

**Министерство по развитию информационных технологий
и коммуникаций Республики Узбекистан**

**Государственное унитарное предприятие Центр научно-технических
и маркетинговых исследований «UNICON.UZ»
(ГУП «UNICON.UZ»)**

**Русско-узбекский толковый словарь
терминов по информационной безопасности**

Переработанное, дополненное второе издание

**O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini
rivojlantirish vazirligi**

**«UNICON.UZ» Fan-texnika va marketing tadqiqotlari markazi
Davlat unitar korxonasi
(«UNICON.UZ» DUK)**

**Axborot xavfsizligiga oid atamalarning
ruscha-o‘zbekcha izohli lug‘ati**

Qayta ishlangan, to‘ldirilgan ikkinchi nashri

**Ўзбекистон Республикаси Ахборот технологиялари
ва коммуникацияларини ривожлантириш вазирлиги**

**«UNICON.UZ» Фан-техника ва маркетинг тадқиқотлари маркази
Давлат унитар корхонаси
(«UNICON.UZ» ДУК)**

**Ахборот хавфсизлигига оид атамаларнинг
русча-ўзбекча изоҳли луғати**

Қайта ишланган, тўлдирилган иккинчи нашри

Toshkent – 2016

Разработан Службой терминологии и словарей ГУП Центр научно-технических и маркетинговых исследований «UNICON.UZ»

Введен в действие приказом Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан от 15.06.2016 г. № 177

Под общей редакцией кандидата технических наук Хасанова Х.П.

Словарь составлен Абрамовой С.И.

переведен и отредактирован
Ахмедовой Ё.Н., Тулягановым Ш.Ш., Адашевой Ш.Ж.

Компьютерный набор: Адашева Ш.Ж.

Рецензент: Ташев К.А.

Texnika fanlari nomzodi X.P.Xasanovning umumiy tahriri ostida.

Lugʻat S.I.Abramova tomonidan tuzildi,

Yo.N.Ahmedova, Sh.Sh.Toʻlaganov, Sh.J.Adashevalar tomonidan
tarjima va tahrir qilindi.

Kompyuter ishlari: Sh.J.Adasheva

Taqrizchi: K.A.Tashev

Техника фанлари номзоди Х.П.Хасановнинг умумий таҳрири остида

Луғат С.И. Абрамова томонидан тузилди,

Ё.Н.Аҳмедова, Ш.Ш.Тўлаганов, Ш.Ж.Адашевлар томонидан
таржима ва таҳрир қилинди.

Компьютер ишлари: Ш.Ж.Адашева

Тақризчи: К.А.Ташев

Содержание

Введение	VI
Список сокращений	X
Русско-узбекский толковый словарь терминов по информационной безопасности	1
Алфавитный указатель терминов на русском языке	582
Алфавитный указатель терминов на узбекском языке (латиница)	615
Алфавитный указатель терминов на узбекском языке (кириллица) . . .	649
Алфавитный указатель терминов на английском языке	683
Список использованных источников	716

Mundarija

Kirish	VII
Qisqartmalar ro‘yxati	X
Axborot xavfsizligiga oid atamalarning ruscha-o‘zbekcha izohli lug‘ati	1
Atamalarning rus tilidagi alifbo ko‘rsatkichi	582
Atamalarning o‘zbek tili (lotin alifbosi) dagi alifbo ko‘rsatkichi	615
Atamalarning o‘zbek tili (kirill alifbosi) dagi alifbo ko‘rsatkichi	649
Atamalarning ingliz tilidagi alifbo ko‘rsatkichi	683
Foydalanilgan manbalar ro‘yxati	716

Мундарижа

Кириш	VIII
Қисқартмалар рўйхати	X
Ахборот хавфсизлигига оид атамаларнинг русча-ўзбекча изоҳли луғати	1
Атамаларнинг рус тилидаги алифбо кўрсаткичи	582
Атамаларнинг ўзбек тилидаги (лотин алифбосидаги) алифбо кўрсаткичи	615
Атамаларнинг ўзбек тилидаги (кирилл алифбосидаги) алифбо кўрсаткичи	649
Атамаларнинг инглиз тилидаги алифбо кўрсаткичи	683
Фойдаланилган манбалар рўйхати	716

Введение

Характерной чертой последних десятилетий прошлого века стало беспрецедентное развитие современных информационно-коммуникационных технологий (ИКТ), включающих новые средства телекоммуникаций, обработки информации и коммуникаций. Уровень развития информатизации общества решающим образом влияет на экономику, обороноспособность и политику и является одной из важных геополитических задач каждого государства.

Революционное воздействие ИКТ касается взаимодействия государственных структур и институтов гражданского общества, экономической и социальной сфер, науки и образования, культуры и образа жизни людей. Многие развитые и развивающиеся страны в полной мере осознали те колоссальные преимущества, которые несет с собой развитие и распространение ИКТ.

Но и у информационной революции, как и у всякого явления, есть обратная сторона медали. Всеобщая компьютеризация основных сфер деятельности и стремительное развитие сети Интернет ведет к появлению широкого спектра внутренних и внешних угроз: нетрадиционных каналов утечки информации и каналов несанкционированного доступа к ней.

В современных условиях проблема защиты информации от несанкционированного доступа, распространения недостоверной информации, нарушения нормального функционирования информационных систем из-за внедрения в них «компьютерных вирусов» становится особенно остро.

Терминология играет значительную роль во всех областях жизнедеятельности общества, и сфера информационной безопасности не является исключением. Русско-узбекский толковый словарь терминов по информационной безопасности является попыткой обобщить имеющуюся терминологию в сфере информационной безопасности и, безусловно, не является исчерпывающим. Словарь – это результат работы специалистов Службы терминологии и словарей, а также других специалистов Центра научно-технических и маркетинговых исследований – «UNICON.UZ» ГУП. Он включает в себя около 1500 терминов, расположенных в алфавитном порядке. В нем отражены термины и определения на русском и узбекском языках и приведены эквиваленты этих терминов на английском языке.

Словарь может быть полезен специалистам в сфере информационных технологий и коммуникаций, руководителям хозяйствующих субъектов при выработке политики информационной безопасности, студентам и аспирантам соответствующих специальностей, а также широкому кругу людей, интересующихся проблемами обеспечения информационной безопасности.

Заранее выражаем признательность за замечания и предложения. Они будут учтены при подготовке очередного издания словаря.

Наш адрес: 100202, г. Ташкент, ул. Богишамол, 7^А.
Государственное унитарное предприятие
«Центр научно-технических и маркетинговых исследований» «UNICON.UZ»,
Служба терминологии и словарей

Kirish

Telekommunikatsiyalar, axborotni qayta ishlash va kommunikatsiyalarning yangi vositalarini ichiga oluvchi zamonaviy axborot-kommunikatsiya texnologiyalari (AKT) ning mislsiz rivojlanishi o'tgan asr so'nggi o'n yilliklarining o'ziga xos xususiyati bo'ldi. Jamiyatni axborotlatirishning rivojlantirish darajasi iqtisodiyotga, mudofaa qobiliyatiga, siyosatga katta ta'sir ko'rsatadi va har bir davlatning muhim geosiyosiy vazifalaridan biri hisoblanadi.

Axborot-kommunikatsiya texnologiyalarining tubdan o'zgartiruvchi ta'siri davlat strukturalari va fuqarolik jamiyati institutlarining o'zaro hamkorligiga, iqtisodiy va ijtimoiy sohalariga, fan va ta'lim, odamlarning turmush tarzi hamda madaniyatiga daxldordir. Rivojlangan va rivojlanayotgan ko'plab mamlakatlarda AKTning rivojlanishi va joriy qilinishi vujudga keltiradigan afzalliklar to'la anglab yetilgan.

Biroq, har bir voqea-hodisada bo'lgani kabi, axborot texnologiyalarining rivojlanishi, joriy qilinishi borasida ham o'ziga xos murakkabliklar mavjud. Jumladan, faoliyatning asosiy sohalarini yalpi kompyuterlashtirish va internet tarmog'ining jadal rivojlanishi ko'plab tashqi va ichki tahdidlar, masalan, axborot chiqib ketishi mumkin bo'lgan noan'anaviy kanallar hamda axborotdan ruxsat etilmagan tarzda foydalana olish kanallari paydo bo'lishiga olib keladi.

Hozirgi sharoitlarda axborotni ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish, ishonchli bo'lmagan axborotning tarqalib ketishi, «kompyuter viruslarining» kiritilishi oqibatida, axborot tizimlari normal ishlashining izdan chiqishi muammosi ayniqsa keskinlashadi.

Atamashunoslik jamiyat hayotining barcha sohalarida, shu jumladan, axborot xavfsizligi sohasida ham sezilarli rol o'ynaydi. Axborot xavfsizligiga oid atamalarning ruscha-o'zbekcha izohli lug'ati axborot xavfsizligi sohasidagi, bu soha bilan bog'liq atamalarni umumlashtirishga bo'lgan dastlabki urinishdir, binobarin, lug'atni mukammal deb bo'lmaydi. Bu lug'at Atamashunoslik va lug'atlar xizmati mutaxassislarining, shuningdek, «UNICON.UZ» – Fan-texnika va marketing tadqiqotlari markazi Davlat unitar korxonasi boshqa bir guruh mutaxassislarining mehnati samarasidir. Lug'at alifbo tartibida joylashtirilgan 1500 ga yaqin atamani o'z ichiga oladi. Lug'atda rus va o'zbek tillaridagi atamalar va ta'riflar hamda shu atamalarning ingliz tilidagi muqobillari keltirilgan.

Lug'atdan axborot texnologiyalari va kommunikatsiyalari sohasida ishlovchi mutaxassislar, xo'jalik yurituvchi subyektlarning rahbarlari axborot xavfsizligi bo'yicha siyosatni ishlab chiqishda, tegishli ixtisoslikdagi talabalar va aspirantlar, shuningdek, axborot xavfsizligini ta'minlash muammolari bilan qiziquvchilarning keng ommasi foydalanishlari mumkin.

Lug'at yuzasidan bildiriladigan fikr-mulohazalar va takliflar uchun oldindan minnatdorchilik bildiramiz. Ular lug'atning keyingi nashrini tayyorlashda hisobga olinadi.

Bizning manzil: 100202, Toshkent sh., Bog'ishamol ko'chasi, 7^A uy
«UNICON.UZ» «Fan-texnika va marketing
tadqiqotlari markazi» Davlat unitar korxonasi,
Atamashunoslik va lug'atlar xizmati

Кириш

Телекоммуникациялар, ахборотни қайта ишлаш ва коммуникацияларнинг янги воситаларини ичига олувчи замонавий ахборот-коммуникация технологиялари (АКТ) нинг мислсиз ривожланиши ўтган аср сўнгги ўн йилликларининг ўзига хос хусусияти бўлди. Жамиятни ахборотлатиришнинг ривожлантириш даражаси иқтисодиётга, муҳофаа қобилиятига, сиёсатга катта таъсир кўрсатади ва ҳар бир давлатнинг муҳим геосиёсий вазифаларидан бири ҳисобланади.

Ахборот-коммуникация технологияларининг тубдан ўзгартирувчи таъсири давлат структуралари ва фуқаролик жамияти институтларининг ўзаро ҳамкорлигига, иқтисодий ва ижтимоий соҳаларига, фан ва таълим, одамларнинг турмуш тарзи ҳамда маданиятига дахлдордир. Ривожланган ва ривожланаётган кўплаб мамлакатларда АКТнинг ривожланиши ва жорий қилиниши вужудга келтирадиган афзалликлар тўла англаб етилган.

Бироқ, ҳар бир воқеа-ҳодисада бўлгани каби, ахборот технологияларининг ривожланиши, жорий қилиниши борасида ҳам ўзига хос мураккабликлар мавжуд. Жумладан, фаолиятнинг асосий соҳаларини ялпи компьютерлаштириш ва интернет тармоғининг жадал ривожланиши кўплаб ташқи ва ички таҳдидлар, масалан, ахборот чиқиб кетиши мумкин бўлган ноанъанавий каналлар ҳамда ахборотдан рухсат этилмаган тарзда фойдалана олиш каналлари пайдо бўлишига олиб келади.

Ҳозирги шароитларда ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш, ишончли бўлмаган ахборотнинг тарқалиб кетиши, «компьютер вирусларининг» киритилиши оқибатида, ахборот тизимлари нормал ишлашининг издан чиқиши муаммоси айниқса кескинлашади.

Атамашунослик жамият ҳаётининг барча соҳаларида, шу жумладан, ахборот хавфсизлиги соҳасида ҳам сезиларли роль ўйнайди. Ахборот хавфсизлигига оид атамаларнинг русча-ўзбекча изоҳли луғати ахборот хавфсизлиги соҳасидаги, бу соҳа билан боғлиқ атамаларни умумлаштиришга бўлган дастлабки уринишдир, бинобарин, луғатни мукамал деб бўлмайди. Бу луғат Атамашунослик ва луғатлар хизмати мутахассисларининг, шунингдек, «UNICON.UZ» – Фан-техника ва маркетинг тадқиқотлари маркази Давлат унитар корхонаси бошқа бир гуруҳ мутахассисларининг меҳнати самарасидир. Луғат алифбо тартибида жойлаштирилган 1500 га яқин атамани ўз ичига олади. Луғатда рус ва ўзбек тилларидаги атамалар ва таърифлар ҳамда шу атамаларнинг инглиз тилидаги муқобиллари келтирилган.

Луғатдан ахборот технологиялари ва коммуникациялари соҳасида ишловчи мутахассислар, хўжалик юритувчи субъектларнинг раҳбарлари ахборот хавфсизлиги бўйича сиёсатни ишлаб чиқишда, тегишли ихтисосликдаги талабалар ва аспирантлар, шунингдек, ахборот хавфсизлигини таъминлаш муаммолари билан қизиқувчиларнинг кенг оммаси фойдаланишлари мумкин.

Луғат юзасидан билдириладиган фикр-мулоҳазалар ва таклифлар учун олдиндан миннатдорчилик билдирамыз. Улар луғатнинг кейинги нашрини тайёрлашда ҳисобга олинади.

Бизнинг манзил: 100202, Тошкент ш., Боғишамол кўчаси, 7^А уй
«UNICON.UZ» «Фан-техника ва маркетинг
тадқиқотлари маркази» Давлат унитар корхонаси,
Атамашунослик ва луғатлар хизмати

Список сокращений
Qisqartmalar ro‘uxati
Қисқартмалар рўйхати

Рус.	Ўзб.	Инглиз.
АИС - автоматизированная информационная система	ААТ - avtomatlashtirilgan axborot tizimi ААТ - автоматлаштирилган ахборот тизими	AIS - automated information system
АРМ - автоматизированные рабочие места	АЮ‘ - avtomatlashtirilgan ish o‘rinlari АИЎ - автоматлаштирилган иш ўринлари	AWS - automated workstation
АС - автоматизированная система	АТ - avtomatlashtirilgan tizim АТ – автоматлаштирилган тизим	AS - automated system
ВОС - взаимодействие открытых систем	ОТВИ - ochiq tizimlarning birgalikda ishlashi ОТБИ - очик тизимларнинг биргаликда ишлаши	OSI - open systems interconnection
ДВБ - достоверная вычислительная база	ИНВ - ishonchli hisoblash bazasi ИХБ - ишончли ҳисоблаш базаси	TCB - trusted computing base
ЗБ - задание по безопасности	ХТ - xavfsizlik bo‘yicha topshiriq ХТ - хавфсизлик бўйича топшириқ	ST - security target
ИВЦ - информационно-вычислительный центр	АНМ - axborot hisoblash markazi АХМ - ахборот ҳисоблаш маркази	DPCC - data-processing computer centre
ИТ - информационная технология	АТ - axborot texnologiyasi АТ - ахборот технологияси	IT - information technology
ОО - объект оценки	ВО - baholash obykti БО - баҳолаш объекти	TOE - target of evaluation
ПЗ - профиль защиты	НР - himoya profili ХП - ҳимоя профили	PP - protection profile
РСО - режимно-секретный орган	МРО - maxfiy-rejimli organ МРО - махфий-режимли орган	RSA - regime and secret authority
СУД - система управления доступом	ФБТ - foydalana olishni boshqarish tizimi ФБТ - фойдалана олишни бошқариш тизими	CAS - controlled access system
УК - управление конфигурацией	КВ - konfiguratsiyani boshqarish КБ - конфигурацияни бошқариш	CM - configuration management
ФБО - функции безопасности объекта оценки	ОХФ - baholash obyektining xavfsizlik funksiyalari ОХФ - баҳолаш объектининг хавфсизлик функциялари	TFS - target security functions of evaluation
ФТБ - функциональные требования безопасности	ФХТ - funksional xavfsizlik talablari ФХТ - функционал хавфсизлик талаблари	FTB - safety function of the object evaluation
ЭВМ - электронная вычислительная машина	ЭНМ - elektron hisoblash mashinasi ЭХМ - электрон ҳисоблаш машинаси	EC - electronic computer

Термин

Определение

А

Аварийный

uz - avariya(viy)

авария(вий)

en - emergency

Определение, характеризующее анализ причин возникновения нежелательных ситуаций в работе системы, основанный на информации, записанной в момент обнаружения нежелательной ситуации.

Nomaqbul vaziyat aniqlangan vaqtda yozilgan axborotga asoslangan, tizim ishida nomaqbul vaziyatlarning yuzaga kelish sabablarining tahlil qilinishini tavsiflovchi ta'rif.

Номақбул вазият аниқланган вақтда ёзилган ахборотга асосланган, тизим ишида номақбул вазиятларнинг юзага келиш сабабларининг таҳлил қилинишини тавсифловчи таъриф.

Автоконтроль целостности

uz - yaxlitlikni avtonazorat

qilish

яхлитликни автоназорат

қилиш

en - integrity authocontrol

Использование в программе специальных алгоритмов, позволяющих после запуска программы определить, были ли внесены изменения в файл, из которого загружена программа, или нет.

Dasturda, dastur ishga tushirilgandan so'ng, dastur yuklangan faylga o'zgartirishlar kiritilgan-kiritilmaganligini aniqlash imkonini beradigan maxsus algoritmlardan foydalanish.

Дастурда, дастур ишга туширилгандан сўнг, дастур юкланган файлга ўзгартиришлар киритилган-киритилмаганлигини аниқлаш имконини берадиган махсус алгоритмлардан фойдаланиш.

Автокорреляция

uz - avtokorrelyatsiya

автокорреляция

en - autocorrelation

Мера подобия различных частей одного и того же множества данных; в контексте проблемы распознавания (идентификации) программ может служить мерой подлинности.

Aynan bir ma'lumotlar to'plami turli qismlarining o'xshashlik o'lchovi; dasturlarni aniqlash (identifikatsiya qilish) muammosi kontekstida haqiqiylik o'lchovi bo'lib xizmat qilishi mumkin.

Айнан бир маълумотлар тўплами турли қисмларининг ўхшашлик ўлчови; дастурларни аниқлаш (идентификация қилиш) муаммоси контекстида ҳақиқийлик ўлчови бўлиб хизмат қилиши мумкин.

A

Авторизация

uz - mualliflashtirish

муаллифлаштириш

en - authorization

1 Предоставление прав, которое включает предоставление доступа на основании прав доступа.

2 Проверка прав доступа пользователя и получение им доступа к ресурсам в соответствии с данными ему правами.

Примечание – Авторизации обычно предшествует процедура аутентификации.

3 Предоставление субъекту прав на доступ к объекту.

4 Предоставление доступа пользователю, программе или процессу.

5 Предоставление доступа к различным системным ресурсам или отказ в доступе.

1 Foydalanish huquqlari asosida foydalanish imkoniyatini taqdim etishdan iborat bo'lgan huquqlarni taqdim etish.

2 Foydalanuvchining foydalana olish huquqlarini tekshirish va unga berilgan huquqlarga muvofiq resurslardan foydalana olishga ruxsat olish.

Izoh – Mualliflashtirish odatda autentifikatsiya protsedurasidan ilgari bo'ladi.

3 Subyektga obyektga kira olish huquqlarini taqdim etish.

4 Foydalanuvchi, dastur yoki jarayonga kira olishni taqdim etish.

5 Turli xildagi tizim resurslaridan foydalanishni taqdim etish yoki foydalanishning rad etilishi. Mualliflashtirish odatda autentifikatsiya protsedurasidan ilgari bo'ladi.

1 Фойдаланиш ҳуқуқлари асосида фойдаланиш имкониятини тақдим этишдан иборат бўлган ҳуқуқларни тақдим этиш.

2 Фойдаланувчининг фойдалана олиш ҳуқуқларини текшириш ва унга берилган ҳуқуқларга мувофиқ ресурслардан фойдалана олишга рухсат олиш.

Изоҳ – Муаллифлаштириш одатда аутентификация процедурасидан илгари бўлади.

3 Субъектга объектга kira олиш ҳуқуқларини тақдим этиш.

4 Фойдаланувчи, дастур ёки жараёнга kira олишни тақдим этиш.

A

Авторизация данных

uz - ma'lumotlarni
mualliflashtirish

маълумотларни
муаллифлаштириш

en - data authorization

Авторизация программы

uz - dasturni mualliflashtirish
дастурни муаллифлаш-
тириш

en - program authorization

Агент (источник) угроз

uz - tahdidlar agenti
(manbai)

таҳдидлар агенти
(манбаи)

en - threat agent

Агрегирование

uz - agregirlash
(birlashtirish)

агрегирлаш
(бирлаштириш)

en - aggregation

5 Турли хилдаги тизим ресурсларидан фойдаланишни тақдим этиш ёки фойдаланишнинг рад этилиши. Муаллифлаштириш одатда аутентификация процедурасидан илгари бўлади.

Определение и установление степени приватности данных в базе данных.

Ma'lumotlar bazasidagi ma'lumotlarning xususiylik darajasini aniqlash va belgilash.

Маълумотлар базасидаги маълумотларнинг хусусийлик даражасини аниқлаш ва белгилаш.

Установление ограничения на доступ к системной или пользовательской программе со стороны других программ и пользователей.

Tizim yoki foydalanuvchi dasturidan boshqa dasturlar yoki foydalanuvchilarning foydalana olishi bo'yicha cheklashlarning o'rnatilishi.

Тизим ёки фойдаланувчи дастуридан бошқа дастурлар ёки фойдаланувчиларнинг фойдалана олиши бўйича чеклашларнинг ўрнатилиши.

Логический объект, который может оказать негативное воздействие на активы.

Aktivlarga salbiy ta'sir qilishi mumkin bo'lgan mantiqiy obyekt.

Активларга салбий таъсир қилиши мумкин бўлган мантиқий объект.

1 Получение чувствительной информации методом сбора и сопоставления информации меньшей чувствительности.

2 Способ получения конфиденциальной (защищаемой) информации на основе обобщения сведений меньшей степени конфиденциальности или открытой информации.

1 Ta'sirchanligi kamroq bo'lgan axborotni to'plash va qiyoslash metodi yordamida ta'sirchan axborotni olish.

A

2 Konfidensiallik darajasi pastroq bo'lgan ma'lumotlarni umumlashtirish yoki ochiq axborot asosida konfidensial (muhofaza qilinadigan) axborotni olish usuli.

1 Таъсирчанлиги камроқ бўлган ахборотни тўплаш ва қиёслаш методи ёрдамида таъсирчан ахборотни олиш.

2 Конфиденциаллик даражаси пастроқ бўлган маълумотларни умумлаштириш ёки очик ахборот асосида конфиденциал (муҳофаза қилинадиган) ахборотни олиш усули.

Администрация

uz - ma'muriyat

маъмурият

en - executive management

Физическое лицо или группа лиц, которым руководящий орган делегировал ответственность за реализацию стратегий и политик, направленных на достижение целей организации.

Примечание – Администрацией иногда называют высшее руководство, в состав которого могут входить генеральный директор, финансовый директор, заместитель генерального директора по информационным технологиям и другие аналогичные роли.

Rahbar organ tashkilot maqsadlariga erishishga yo'naltirilgan strategiyalar va siyosatlarini amalga oshirish uchun javobgarlik vakolatini bergan jismoniy shaxs yoki shaxslar guruhi.

Izoh – Ba'zida tarkibiga Bosh direktor, moliya direktori, Bosh direktorning axborot texnologiyalari bo'yicha o'rinbosari va boshqa shunga o'xshash rollar kirishi mumkin bo'lgan oliy rahbariyat ma'muriyat deb ataladi.

Раҳбар орган ташкилот мақсадларига эришишга йўналтирилган стратегиялар ва сиёсатларни амалга ошириш учун жавобгарлик ваколатини берган жисмоний шахс ёки шахслар гуруҳи.

Изоҳ – Баъзида таркибига Бош директор, молия директори, Бош директорнинг ахборот технологиялари бўйича ўринбосари ва бошқа шунга ўхшаш роллар кириши мумкин бўлган олий раҳбарият маъмурият деб аталади.

Администратор

uz - ma'mur

маъмур

en - administrator

Логический объект, который имеет уровень доверия относительно всех политик, реализуемых ФБО.

Примечание – Не все ПЗ или ЗБ предполагают один и тот

А

же уровень доверия для администраторов. Обычно предполагается, что администраторы придерживаются всегда политик, приведенных в ЗБ ОО. Некоторые из этих политик могут быть обусловлены функциональным назначением ОО, другие – средой функционирования.

OXFda amalga oshiriladigan barcha siyosatlariga nisbatan ishonch darajasiga ega mantiqiy obyekt.

Izoh – Ma'murlar uchun HP yoki XT larning hammasi ham aynan bir ishonch darajasini ko'zda tutmaydi. Odatda, ma'murlar har doim BOning XTda keltirilgan siyosatlarni qo'llab-quvvatlashi taxmin qilinadi. Bu siyosatlarning ayrimlari BOda funksional belgilangan, boshqalari esa ishchi muhiti bo'lishi mumkin.

OXFda amalga oshiriladigan barcha siyosatlariga nisbatan ishonch darajasiga ega mantiqiy obyekt.

Izoh – Ma'murlar uchun HP yoki XT larning hammasi ham aynan bir ishonch darajasini ko'zda tutmaydi. Odatda, ma'murlar har doim BOning XTda keltirilgan siyosatlarni qo'llab-quvvatlashi taxmin qilinadi. Bu siyosatlarning ayrimlari BOda funksional belgilangan, boshqalari esa ishchi muhiti bo'lishi mumkin.

Администратор базы данных

**uz - ma'lumotlar bazasi
ma'muri**

маълумотлар базаси
мамури

en - database administrator

Специальное должностное лицо (группа лиц), имеющий(ие) полное представление о базе данных и отвечающее за ее ведение, использование и развитие. Входит в состав администрации банка данных.

Ma'lumotlar bazasi to'g'risida to'liq tasavvurga ega bo'lgan va bu ma'lumotlar bazasini yuritish, undan foydalanish, uni rivojlantirish yuzasidan javobgar maxsus mansabdor shaxs (shaxslar guruhi). Ma'lumotlar banki ma'muriyati tarkibiga kiradi.

Ma'lumotlar bazasi to'g'risida to'liq tasavvurga ega bo'lgan va bu ma'lumotlar bazasini yuritish, undan foydalanish, uni rivojlantirish yuzasidan javobgar maxsus mansabdor shaxs (shaxslar guruhi). Ma'lumotlar banki ma'muriyati tarkibiga kiradi.

A

Администратор безопасности (защиты)

uz - xavfsizlik (muhofaza qilish) ma'muri

хавфсизлик (муҳофаза қилиш) маъмури

en - security (safety) administrator

1 Полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющий постоянную организационную поддержку функционирования применяемых физических и технических средств защиты.

2 Субъект доступа, ответственный за защиту сети (системы) телекоммуникаций от несанкционированного доступа к информации.

3 Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

1 Tizim xavfsizligini ta'minlash, o'rnatilgan ma'muriy muhofaza choralarini amalga oshirish va ularga rioya qilinishining uzluksizligi uchun javobgar, qo'llaniladigan jismoniy va texnik muhofaza vositalari ishlashini tashkiliy jihatdan muntazam qo'llab-quvvatlanishini amalga oshiruvchi vakolatli vakil (shaxs yoki shaxslar guruhi).

2 Telekommunikatsiyalar tarmog'i (tizimlari)ning axborotdan ruxsat etilmagan tarzda foydalanishdan muhofaza qilinishi yuzasidan javobgar, foydalanish subyekti.

3 Avtomatlashtirilgan tizimning axborotdan ruxsat etilmagan tarzda foydalanishdan muhofaza qilinishi uchun javobgar bo'lgan foydalana olish subyekti.

1 Тизим хавфсизлигини таъминлаш, ўрнатилган маъмурий муҳофаза чораларини амалга ошириш ва уларга риоя қилинишининг узлуксизлиги учун жавобгар, қўлланиладиган жисмоний ва техник муҳофаза воситалари ишлашини ташкилий жиҳатдан мунтазам қўллаб-қувватланишини амалга оширувчи ваколатли вакил (шахс ёки шахслар гуруҳи).

2 Телекоммуникациялар тармоғи (tizimlari)нинг ахборотдан рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиниши юзасидан жавобгар, фойдаланиш субъекти.

3 Автоматлаштирилган тизимнинг ахборотдан рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиниши учун жавобгар бўлган фойдалана олиш субъекти.

А

Администратор доступа

uz - foydalana olish ma'muri
фойдалана олиш маъмури
en - access administrator

Одно из должностных лиц в составе администрации банка данных, отвечающее за организацию доступа пользователей к базам данных.

Ма'lumotlar banki ma'muriyati tarkibidagi, foydalanuvchilarning ma'lumotlar bazasidan erkin foydalanishlarini tashkillashtirish uchun javobgar bo'lgan mansabdor shaxslardan biri.

Маълумотлар банки маъмурияти таркибидаги, фойдаланувчиларнинг маълумотлар базасидан эркин фойдаланишларини ташкиллаштириш учун жавобгар бўлган мансабдор шахслардан бири.

Администратор межсетевого экрана

uz - tarmoqlararo ekran
ma'muri
тармоқлараро экран
маъмури
en - firewall administrator

Лицо, ответственное за сопровождение межсетевого экрана.

Tarmoqlararo ekranning kuzatib borilishi yuzasidan javobgar shaxs.

Тармоқлараро экраннинг кузатиб борилиши юзасидан жавобгар шахс.

Администратор системный

uz - tizim ma'muri
tizim ma'muri
en - system administrator

Лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

Tizimning ekspluatatsiya qilinishi va ishchi holatda saqlab turilishi yuzasidan javobgar shaxs.

Тизимнинг эксплуатация қилиниши ва ишчи ҳолатда сақлаб турилиши юзасидан жавобгар шахс.

Администратор службы безопасности

uz - xavfsizlik xizmati
ma'muri
хавфсизлик хизмати
маъмури
en - security service
administrator

Лицо (или группа лиц), имеющее полное представление об одной или нескольких системах обеспечения безопасности и контролирующее их проектирование и использование.

Bitta yoki bir nechta xavfsizlikni ta'minlash tizimi to'g'risida to'liq tasavvurga ega bo'lgan, ularning loyihalashtirilishini va ulardan foydalanishni nazorat qiluvchi shaxs (yoki shaxslar guruhi).

Битта ёки бир нечта хавфсизликни таъминлаш тизими тўғрисида тўлиқ тасаввурга эга бўлган, уларнинг лойihalаштирилишини ва улардан фойдаланишни назорат қилувчи шахс (ёки шахслар гуруҳи).

A

Администрация банка данных

uz - ma'lumotlar banki
ma'muriyati

маълумотлар банки
маъмурияти

en - databank administration

Группа лиц (подразделение), отвечающих за эксплуатацию банка данных: ведение баз данных, организацию коллективного доступа к ним пользователей и развитие системы.

Ma'lumotlar bankidan foydalanish: ma'lumotlar bazasini yuritish, undan jamoa bo'lib foydalanishni tashkillashtirish va tizimni rivojlantirish yuzasidan javobgar bo'lgan shaxslar guruhi (bo'linma).

Маълумотлар банкидан фойдаланиш: маълумотлар базасини юритиш, ундан жамоа бўлиб фойдаланишни ташкиллаштириш ва тизимни ривожлантириш юзасидан жавобгар бўлган шахслар гуруҳи (бўлинма).

Администрация системы защиты

uz - muhofaza tizimi
ma'muriyati

муҳофаза тизими
маъмурияти

en - security system
administration

Орган управления, устанавливающий политику безопасности и определяющий объекты и субъекты, к которым данная политика применяется.

Xavfsizlik siyosatini belgilaydigan hamda bu siyosat qo'llaniladigan obyekt va subyektlarni aniqlaydigan boshqaruv organi.

Хавфсизлик сиёсатини белгилайдиган ҳамда бу сиёсат қўлланиладиган объект ва субъектларни аниқлайдиган бошқарув органи.

Администрирование базы данных

uz - ma'lumotlar bazasini
boshqarish

маълумотлар базасини
бошқариш

en - database administration

Выполнение функций определения, организации, управления и защиты данных в базе данных.

Ma'lumotlar bazasida ma'lumotlarni belgilash, tashkillashtirish, boshqarish va muhofaza qilish funksiyalarining bajarilishi.

Маълумотлар базасида маълумотларни белгилаш, ташкиллаштириш, бошқариш ва муҳофаза қилиш функцияларининг бажарилиши.

Администрирование средств безопасности

uz - xavfsizlik vositalarini
boshqarish

хавфсизлик воситаларини
бошқариш

en - security facilities
administration

Процесс, включающий распространение информации, необходимой для работы сервисов безопасности, а также сбор и анализ информации об их функционировании. Например, распространение криптографических ключей, установка прав доступа, анализ журнала аудита и т.п.

Xavfsizlik servislarning ishlashi uchun zarur bo'l-

A

gan axborotning tarqatilishini, shuningdek, ularning ishlashi to'g'risidagi axborotni to'plash va tahlil qilishni ichiga oladigan jarayon. Masalan, kriptografik kalitlarning tarqatilishi, foydalana olish huquqining o'rnatilishi, audit jurnalining tahlili va sh.k.

Хавфсизлик сервисларининг ишлаши учун зарур бўлган ахборотнинг тарқатилишини, шунингдек, уларнинг ишлаши тўғрисидаги ахборотни тўплаш ва таҳлил қилишни ичига оладиган жараён. Масалан, криптографик калитларнинг тарқатилиши, фойдалана олиш ҳуқуқининг ўрнатилиши, аудит журналининг таҳлили ва ш.к.

Аккредитация

uz - akkreditlash

аккредитлаш

en - accreditation

Официальное признание технической компетентности предприятия и независимости его от разработчиков, изготовителей (поставщиков) и заказчиков (потребителей) испытываемых средств защиты информации для организации и проведения испытаний в соответствии с требованиями стандартов и иных нормативных документов. Аккредитацию осуществляет специально уполномоченный орган.

Korxonaning texnik kompetentligini hamda uning standartlar va boshqa normativ hujjatlar talablariga muvofiq, sinovlarni tashkil qilish va o'tkazish uchun, sinaladigan axborotni muhofaza qilish vositalarini ishlab chiquvchilar, tayyorlovchilar (yetkazib beruvchilar), buyurtmachilar (iste'molchilar)dan mustaqilligini rasman tan olish. Akkreditlash maxsus vakolatli organ tomonidan amalga oshiriladi.

Корxonанинг техник компетентлигини ҳамда унинг стандартлар ва бошқа норматив ҳужжатлар талабларига мувофиқ, синовларни ташкил қилиш ва ўтказиш учун, sinalадиган ахборотни муҳофаза қилиш воситаларини ишлаб чиқувчилар, тайёрловчилар (етказиб берувчилар), буюртмачилар (истеъмолчилар)дан мустақиллигини расман тан олиш. Аккредитлаш махсус ваколатли орган томонидан амалга оширилади.

A

Аккредитация в области защиты информации

uz - axborotni muhofaza qilish sohasida akkreditlash

ахборотни муҳофаза

қилиш соҳасида аккредитлаш

en - accreditation in the field of information security

Официальное признание полномочий осуществлять какую-либо деятельность в области сертификации защищенных изделий, технических средств и способов защиты информации.

Muhofazalangan mahsulotlar, axborotni muhofaza qilish texnik vositalari va usullarini sertifikatlash sohasida qandaydir faoliyatni amalga oshirish bo'yicha vakolatlarning rasman tan olinishi.

Муҳофазаланган маҳсулотлар, ахборотни муҳофаза қилиш техник воситалари ва усулларини сертификатлаш соҳасида қандайдир фаолиятни амалга ошириш бўйича ваколатларнинг расман тан олинishi.

Активы

uz - aktivlar

активлар

en - assets

Логические объекты, представляющие ценность для владельца ООО.

BOning egasiga qiymatli mantiqiy obyektlar.

BOning egasiga qiymatli mantiqiy obyektlar.

Активы информационные

uz - axborot aktivlari

ахборот активлари

en - information asset

Информация или средства обработки информации юридического лица.

Yuridik shaxsning axboroti yoki axborotni qayta ishlash vositalari.

Юридик шахснинг ахбороти ёки ахборотни қайта ишлаш воситалари.

Алгоритм

uz - algoritim

алгоритм

en - algorithm

Упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Masala(lar)ni cheklangan qadamlarda yechish uchun aniq belgilangan qoidalarning tartiblangan chekli to'plami.

Масала(лар)ни чекланган қадамларда ечиш учун аниқ белгиланган қоидаларнинг тартибланган чекли тўплами.

A

Алгоритм DES трёхкратный

uz - uch martali *DES* algoritmi
уч мартали *DES*
алгоритми
en - 3DES (Triple DES)

Метод шифрования, в котором алгоритм *DES* используется три раза с тремя различными ключами.

DES algoritmidan uch marta uchta turli kalit bilan foydalaniladigan shifrlash metodi.

DES algoritmidan uch marta uchta turli kalit bilan foydalaniladigan shifrlash metodi.

Алгоритм дешифрования

uz - deshifrlash algoritmi
дешифрлаш алгоритми
en - decryption algorithm

Алгоритм, реализующий функцию дешифрования.

Deshifrlash funksiyasini amalga oshiradigan algoritm.

Дешифрлаш функциясини амалга оширадиган алгоритм.

Алгоритм Диффи-Хеллмана

uz - Diffi-Hellman algoritmi
Диффи-Хеллман
алгоритми
en - Diffie-Hellman algorithm

Алгоритм открытого распределения ключей, также называемый экспоненциальным распределением ключей, основанный на использовании односторонней показательной функции.

Kalitlarni ochiq taqsimlash, shuningdek, kalitlarni eksponensial taqsimlash deb nomlanuvchi bir tomonlama ko'rsatkichli funksiyadan foydalanishga asoslangan algoritm.

Калитларни очик тақсимлаш, шунингдек, калитларни экспоненциал тақсимлаш деб номланувчи бир томонлама кўрсаткичли функциядан фойдаланишга асосланган алгоритм.

Алгоритм имитозащищающего кодирования информации

uz - axborotni imitomuhofazalovchi kodlash algoritmi
ахборотни имитомуҳофазаловчи кодлаш алгоритми
en - information encoding imitoprotecting algorithm

Алгоритм преобразования информации с целью контроля целостности.

Yaxlitlikni nazorat qilish maqsadida axborotni o'zgartirish algoritmi.

Yaxlitlikni nazorat qilish maqsadida axborotni ўзгартириш алгоритми.

A

Алгоритм криптографический

uz - kriptografik algoritm

криптографик алгоритм

en - cryptographic algorithm

Математический алгоритм преобразования информации (данных) с целью предотвратить возможность её искажения и защитить от несанкционированного доступа.

Axborot (ma'lumotlar)ni, uning buzib ko'rsatilishi mumkinligining oldini olish va ruxsat etilmagan tarzda foydalanishdan muhofaza qilish maqsadida qayta o'zgartirishning matematik algoritmi.

Ахборот (маълумотлар)ни, унинг бузиб кўрсатилиши мумкинлигининг олдини олиш ва рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш мақсадида қайта ўзгартиришнинг математик алгоритми.

Алгоритм

криптографический асимметричный

uz - asimmetrik kriptografik algoritm

асимметрик криптографик алгоритм

en - asymmetric cryptographic algorithm

Алгоритм выполнения шифрования или соответствующего дешифрования, при котором для шифрования и дешифрования используются разные ключи.

Shifrlash va deshifrlash uchun turli kalitlardan foydalaniladigan, shifrlash yoki tegishli deshifrlashni bajarish algoritmi.

Шифрлаш ва дешифрлаш учун турли калитлардан фойдаланиладиган, шифрлаш ёки тегишли дешифрлашни бажариш алгоритми.

Алгоритм криптографический симметричный

uz - simmetrik kriptografik algoritm

симметрик криптографик алгоритм

en - symmetric cryptographic algorithm

Алгоритм выполнения шифрования или соответствующий алгоритм выполнения дешифрования, в котором для шифрования и дешифрования требуется один и тот же ключ.

Shifrlash va deshifrlash uchun aynan bitta kalitdan foydalaniladigan, shifrlash yoki tegishlicha deshifrlashni bajarish algoritmi.

Шифрлаш ва дешифрлаш учун айнан битта калитдан фойдаланиладиган, шифрлаш ёки тегишлича дешифрлашни бажариш алгоритми.

A

Алгоритм проверки цифровой подписи

uz - raqamli imzoni tekshirish algoritmi

рақамли имзони текшириш алгоритми

en - digital signature checking algorithm

Алгоритм, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы цифровой подписи, а результатом является заключение о правильности или ошибочности цифровой подписи.

Dastlabki ma'lumotlari sifatida imzolangan xabar, tekshirish kaliti va raqamli imzo sxemasi parametrlaridan foydalaniladigan algoritm, raqamli imzoning to'g'riligi yoki xatoligi to'g'risidagi xulosa natija hisoblanadi.

Дастлабки маълумотлари сифатида имзоланган хабар, текшириш калити ва рақамли имзо схемаси параметрларидан фойдаланиладиган алгоритм, рақамли имзонинг тўғрилиги ёки хатолиги тўғрисидаги хулоса натижа ҳисобланади.

Алгоритм СМЕА

uz - *СМЕА* algoritmi

СМЕА алгоритми

en - Cellular Message Encryption Algorithm (СМЕА)

Алгоритм шифрования сообщений в сетях цифровой сотовой связи.

Raqamli sotali aloqa tarmoqlarida xabarlarni shifrlash algoritmi.

Рақамли сотали алоқа тармоқларида хабарларни шифрлаш алгоритми.

Алгоритм

Сторнетт-Хабера

uz - Stornett-Xaber algoritmi

Сторнетт-Хабера алгоритми

en - Stornett Khaber algorithm

Алгоритм, обеспечивающий подпись документов по времени без возможности их подделки.

Hujjatlarning vaqt bo'yicha, ularni qalbakilashtirish imkoniyati bo'lmaydigan tarzda, imzolanishini ta'minlovchi algoritm.

Хужжатларнинг вақт бўйича, уларни қалбакилаштириш имконияти бўлмайдиган тарзда, имзоланишини таъминловчи алгоритм.

Алгоритм формирования цифровой подписи

uz - raqamli imzoni shakllantirish algoritmi

рақамли имзони шакллантириш алгоритми

en - digital signature formation algorithm

Алгоритм, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы цифровой подписи, а в результате формируется цифровая подпись.

Dastlabki ma'lumotlari sifatida xabar, imzo kaliti va raqamli imzo sxemasi parametrlaridan foydalaniladigan algoritm, natijada raqamli imzo shakllanadi.

А

Дастлабки маълумотлари сифатида хабар, имзо калити ва рақамли имзо схемаси параметрларидан фойдаланиладиган алгоритм, натижада рақамли имзо шаклланади.

Алгоритм хэширования односторонний

uz - bir tomonlama xeshlash
algoritmi

бир томонлама хэшлаш
алгоритми

en - single sided hashing
algorithm

Алгоритм хэширования, который обладает свойством практической невозможности восстановления на основе значения хэш-кода исходных данных, из которых этот хэш-код был получен.

Xesh-kod olingan dastlabki ma'lumotlarning xesh-kod qiymati asosida amalda tiklab bo'lmaslik xossasiga ega bo'lgan xeshlash algoritmi.

Хэш-код олинган дастлабки маълумотларнинг хэш-код қиймати асосида амалда тиклаб бўлмаслик хоссасига эга бўлган хэшлаш алгоритми.

Алгоритм шифрования

uz - shifrlash algoritmi

шифрлаш алгоритми

en - encryption algorithm

Алгоритм, реализующий функцию шифрования.

Shifrlash funksiyasini amalga oshiradigan algoritmi.

Шифрлаш функциясини амалга оширадиган алгоритм.

Алгоритм шифрования

данных

uz - ma'lumotlarni shifrlash
algoritmi

маълумотларни шифрлаш
алгоритми

en - data encryption algorithm

Набор математических правил, определяющих содержание и последовательность операций, зависящих от ключевой переменной (ключ шифрования), по преобразованию исходной формы представления информации (открытый текст) к виду, обладающему секретом обратного преобразования (зашифрованный текст).

Axborotni taqdim etishning dastlabki shakli (ochiq matn)ni, qayta o'zgartirish siriga ega ko'rinishga (shifrlangan matn) aylantirish bo'yicha, muhim o'zgaruvchi (shifrlash kaliti)ga bog'liq bo'lgan operatsiyalarning mazmuni va izchilligini belgilaydigan matematik qoidalar to'plami.

Ахборотни такдим этишнинг дастлабки шакли (очик матн)ни, қайта ўзгартириш сирига эга кўринишга (шифрланган матн) айлантериш бўйича, муҳим ўзгарувчи (шифрлаш калити)га боғлиқ бўлган операцияларнинг мазмуни ва изчиллигини белгилайдиган математик қоидалар тўплами.

А

Алгоритм Эль-Гамалы
uz - Al-Jamol algoritmi
Ал-Жамол алгоритми
en - Ale Namale algorithm

Криптосистема, базирующаяся на задаче дискретного логарифмирования, которая может использоваться как для шифрования, так и для аутентификации (цифровой подписи) информации.

Axborotni autentifikatsiya qilish (raqamli imzo) hamda shifrlash uchun foydalaniladigan diskret logarifmlash masalasi asosidagi kriptotizim.

Axborotni autentifikatsiya qilish (raqamli imzo) hamda shifrlash uchun foydalaniladigan diskret logarifmlash masalasi asosidagi kriptotizim.

Амортизация отказов
uz - ishlaymay qolishlar amortizatsiyasi
ишламай қолишлар амортизацияси
en - fail soft

Свойство вычислительной системы, состоящее в способности распознавать изменения окружающей среды и выполнять свои функции в условиях отказа или изъятия части оборудования.

Hisoblash tizimining, atrof muhit o'zgarishini aniqlash va uskuna nosoz bo'lgan yoki uning bir qismi olib tashlangan sharoitda o'z funksiyalarini bajara olishida aks etuvchi xususiyati.

Hisoblash tizimining, atrof muhit o'zgarishini aniqlash va uskuna nosoz bo'lgan yoki uning bir qismi olib tashlangan sharoitda o'z funksiyalarini bajara olishida aks etuvchi xususiyati.

Анализ
uz - tahlil
таҳлил
en - review

Деятельность, предпринимаемая для установления пригодности, адекватности, результативности рассматриваемого объекта для достижения установленных целей.

Belgilangan maqsadlarga erishish yo'lida ko'rilayotgan obyektning yaroqliligini, adekvatligi (o'xshashligi)ni, natijaliligini aniqlash uchun amalga oshiriladigan faoliyat.

Belgilangan maqsadlarga erishish yo'lida ko'rilayotgan obyektning yaroqliligini, adekvatligi (o'xshashligi)ni, natijaliligini aniqlash uchun amalga oshiriladigan faoliyat.

A

Анализ затрат (выгоды)

uz - xarajatlar (foйда)ni tahlil qilish

харажатлар (фойда)ни таҳлил қилиш

en - costbenefit analysis

Стадия в разработке или функционировании системы, на которой определяется стоимость обеспечения требуемого уровня защиты данных в информационной системе. Иногда под этой стоимостью подразумевают ущерб, который может быть нанесен в случае утери или компрометации данных, подлежащих защите.

Tizimni ishlab chiqish yoki ishlashidagi bosqich bo'lib, bunda axborot tizimidagi ma'lumotlarning talab etiladigan darajada muhofaza qilinishini ta'minlash qiymati aniqlanadi. Ba'zida bu qiymat ostida, muhofaza qilinishi lozim bo'lgan ma'lumotlarning yo'qolishi yoki putur yetkazilishi (obro'sizlantirilishi) oqibatida yetkazilishi mumkin bo'lgan zarar tushuniladi.

Тизимни ишлаб чиқиш ёки ишлашидаги босқич бўлиб, бунда ахборот тизимидаги маълумотларнинг талаб этиладиган даражада муҳофаза қилинишини таъминлаш қиймати аниқланади. Баъзида бу қиймат остида, муҳофаза қилиниши лозим бўлган маълумотларнинг йўқолиши ёки путур етказилиши (обрўсизлантирилиши) оқибатида етказилиши мумкин бўлган зарар тушунилади.

Анализ защищенности

uz - muhofaza qilinganlikni tahlil qilish

муҳофаза қилинганликни таҳлил қилиш

en - protection analysis

1 Процесс обнаружения уязвимостей ресурсов автоматизированной системы, а также выработка рекомендаций по их устранению.

2 Проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям по безопасности информации.

1 Avtomatlashtirilgan tizim resurslarining zaif joylarini aniqlash, shuningdek, ularni bartaraf qilish bo'yicha tavsiyalar ishlab chiqish jarayoni.

2 Axborotni muhofaza qilish bo'yicha tadbirlar samaradorligi sifat va miqdor ko'rsatkichlarining axborot xavfsizligi talablariga mos kelishini tekshirish.

1 Автоматлаштирилган тизим ресурсларининг заиф жойларини аниқлаш, шунингдек, уларни бартараф қилиш бўйича тавсиялар ишлаб чиқиш жараёни.

А

Анализ криптографический

uz - kriptografik tahlil qilish

криптографик таҳлил

қилиш

en - cryptanalysis

2 Ахборотни муҳофаза қилиш бўйича тадбирлар самарадорлиги сифат ва миқдор кўрсаткичларининг ахборот хавфсизлиги талабларига мос келишини текшириш.

1 Искусство и наука вскрытия шифра или объекта криптографии любой другой формы.

2 Процесс получения исходного текста по шифрованному без знания ключа или процесс вычисления ключа по исходному и шифрованному тексту.

1 Shifrni yoki har qanday boshqa shakldagi kriptografiya obyektining sirini ochish san'ati va ilmi.

2 Kalitni bilmasdan turib shifrlangan matndan dastlabki matnни olish yoki dastlabki matn va shifrlangan matn bo'yicha kalitni hisoblab chiqarish jarayoni.

1 Шифрни ёки ҳар қандай бошқа шаклдаги криптография объектининг сирини очиш санъати ва илми.

2 Калитни билмасдан туриб шифрланган матндан дастлабки матнни олиш ёки дастлабки матн ва шифрланган матн бўйича калитни ҳисоблаб чиқариш жараёни.

Анализ прерывания

uz - uzilishni tahlil qilish

узилишни таҳлил қилиш

en - interrupt analysis

Функция, выполняемая обработчиком прерываний по коду в старом слове состояния программы (PSW) и состоящая в определении причины прерывания и выборе соответствующей программы его обработки.

(PSW) dastur holati eski so'zidagi kod bo'yicha uzilishlarni qayta ishlovchi tomonidan bajariladigan va uzilish sababini aniqlash hamda uni qayta ishlashning tegishli dasturini tanlashdan iborat funktsiya.

(PSW) dastur holati eski s'zidaagi kod b'yiacha uzilishlarni qayta ishlovchi tomonidan bajariladigan va uzilish sababini aniqlash hamda uni qayta ishlashning tegishli dasturini tanlashdan iborat funktsiya.

A

Анализ программы санкционированный

uz - dasturni ruxsat etilgan
tarzda tahlil qilish

дастурни рухсат этилган
тарзда таҳлил қилиш

en - authorized program
analysis

Анализ, выполняемый для установления расхождения между техническими требованиями и реальными возможностями программы.

Texnik talablar bilan dasturning haqiqiy imkoniyatlari o'rtasidagi farqni belgilash maqsadida bajariladigan tahlil.

Техник талаблар билан дастурнинг ҳақиқий имкониятлари ўртасидаги фарқни белгилаш мақсадида бажариладиган таҳлил.

Анализ риска

uz - riskni tahlil qilish

рискни таҳлил қилиш

en - risk analysis

1 Процесс изучения природы и характера риска и определения уровня риска.

Примечания

1 Анализ риска служит основой для оценки риска и принятия решения об обработке риска.

2 Анализ риска включает в себя количественную оценку риска.

2 Систематическое выполнение процедур идентификации ресурсов системы обработки данных, угроз этим ресурсам и уязвимостей системы к этим угрозам.

3 Процесс определения угроз безопасности системы в целом и отдельным ее компонентам (не только техническим), определения характеристик угроз и потенциального ущерба, который может быть нанесен в случае их реализации, а также разработка мер по защите.

1 Risk tabiati va xarakterini o'rganish va risk darajasini aniqlash jarayoni.

Izohlar

1 Riskni tahlil qilish riskni baholash va riskni qayta ishlash to'g'risida qaror qabul qilinishi uchun asos bo'lib xizmat qiladi.

2 Riskni tahlil qilish riskning miqdor jihatdan baholanishini o'z ichiga oladi.

2 Ma'lumotlarni qayta ishlash tizimi resurslarini, bu resurslarga tahdidlarni va bu tahdidlarga nisbatan tizimning zaifliklarini identifikatsiya qilish protseduralarining muntazam bajarilishi.

3 Umuman tizim xavfsizligiga va uning alohida (nafaqat texnik) komponentlariga tahdidlarni, tahdidlar xarakteristikasini va ular amalga oshirilganda yetkazilishi mumkin bo'lgan potensial zararni aniqlash, shuningdek, muhofaza chora-tadbirlarini ishlab

A

chiqish jarayoni.

1 Риск табиати ва характерини ўрганиш ва риск даражасини аниқлаш жараёни.

Изоҳлар

1 Рискни таҳлил қилиш рискни баҳолаш ва рискни қайта ишлаш тўғрисида қарор қабул қилиниши учун асос бўлиб хизмат қилади.

2 Рискни таҳлил қилиш рискнинг миқдор жиҳатдан баҳоланишини ўз ичига олади.

2 Маълумотларни қайта ишлаш тизими ресурсларини, бу ресурсларга таҳдидларни ва бу таҳдидларга нисбатан тизимнинг заифликларини идентификация қилиш процедураларининг мунтазам бажарилиши.

3 Умуман тизим хавфсизлигига ва унинг алоҳида (нафақат техник) компонентларига таҳдидларни, таҳдидлар характеристикасини ва улар амалга оширилганда етказилиши мумкин бўлган потенциал зарарни аниқлаш, шунингдек, муҳофаза чора-тадбирларини ишлаб чиқиш жараёни.

Анализ риска полный

uz - riskni to‘liq tahlil qilish

рискни тўлиқ таҳлил қилиш

en - full risk analysis

Анализ рисков для информационных систем, предъявляющих повышенные требования в области информационной безопасности (более высокие, чем базовый уровень защищенности).

Примечание – Полный анализ рисков предполагает определение ценности ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер и оценку их эффективности.

Ахборот хавфсизлиги соҳасида ошirilган (муҳофаза қilinganlikning bazaviy darajasiga qaraganda yuqoriroq bo‘lgan) talablar qo‘yadigan axborot tizimlari uchun risklarni tahlil qilish.

Izoh – Risklarni to‘liq tahlil qilish resurslarning qimmatligi aniqlanishini, tahdidlar va zaifliklar baholanishini, adekvat qarshi choralar tanlanishini va ularning samaradorligi baholanishini ko‘zda tutadi.

Ахборот хавфсизлиги соҳасида оширилган (муҳофаза қилинганликнинг базавий даражасига қараганда юқорироқ бўлган) талаблар қўядиган ахборот тизимлари учун рискларни таҳлил қилиш.

Изоҳ – Рискларни тўлиқ таҳлил қилиш ресурсларнинг қимматлилиги аниқланишини, таҳдидлар ва заифликлар баҳоланишини, адекват қарши чоралар танланишини ва уларнинг самарадорлиги баҳоланишини кўзда тутати.

A

Анализ рисков базовый

uz - risklarning asosiy tahlili

рисklarнинг асосий

таҳлили

en - baseline risk analysis

Анализ рисков, проводимый в соответствии с требованиями базового уровня информационной безопасности.

Axborot xavfsizligi asosiy darajasining talablariga muvofiq oʻtkaziladigan riskni tahlil qilish.

Ахборот хавфсизлиги асосий даражасининг талабларига мувофиқ ўтказиладиган рискни таҳлил қилиш.

Анализ трафика

uz - trafikni tahlil qilish

трафикни таҳлил қилиш

en - traffic analysis

Анализ информации, полученной при наблюдении за потоками. Например, анализ наличия, отсутствия, объема, направления и частоты трафика.

Trafik oqimlarini kuzatish paytida olingan axborot tahlili. Masalan, trafik mavjudligi, mavjud emasligi, hajmi, yoʻnalishi va chastotasining tahlili.

Трафик оқимларини кузатиш пайтида олинган ахборот таҳлили. Масалан, трафик мавжудлиги, мавжуд эмаслиги, ҳажми, йўналиши ва частотасининг таҳлили.

Анализ угроз

uz - tahdidlarning tahlili

таҳдидларнинг таҳлили

en - threat analysis

Исследование действий и событий, которые могут неблагоприятно воздействовать на систему обработки данных.

Maʼlumotlarni qayta ishlash tizimiga salbiy taʼsir etishi mumkin boʻlgan harakatlar va hodisalarni tadqiq etish.

Маълумотларни қайта ишлаш тизимига салбий таъсир этиши мумкин бўлган ҳаракатлар ва ҳодисаларни тадқиқ этиш.

Анализ уязвимостей

uz - zaifliklar tahlili

заифликлар таҳлили

en - analysis vulnerability

Деятельность, включающая в себя сканирование TCP- и UDP-портов и идентификацию соответствующих сервисов, удалённую идентификацию операционных систем, выявление уязвимостей сетевых служб, а также генерацию соответствующих отчётов.

A

TCP- va *UDP*-portlarni skanerlashni va tegishli servislar identifikatsiya qilinishini, operatsion tizimlarni masofadan identifikatsiya qilishni, tarmoq xizmatlarining zaif joylarini aniqlashni, shuningdek, tegishli hisobotlar ishlab chiqarishni o‘z ichiga oladigan faoliyat.

TCP- va *UDP*-портларни сканерлашни ва тегишли сервислар идентификация қилинишини, операцион тизимларни масофадан идентификация қилишни, тармоқ хизматларининг заиф жойларини аниқлашни, шунингдек, тегишли ҳисоботлар ишлаб чиқаришни ўз ичига оладиган фаолият.

В системах программирования – алгоритм, выполняющий анализ исходной программы.

Dasturlash tizimlarida – dastlabki dasturning tahlil qilinishini amalga oshiruvchi algoritm.

Дастурлаш тизимларида – дастлабки дастурнинг таҳлил қилинишини амалга оширувчи алгоритм.

Программа, предназначенная для анализа аварийного состояния вычислительной системы и выдачи информации на печать.

Hisoblash tizimining avariya holatini tahlil qilish va axborotni bosishga berish uchun mo‘ljallangan dastur.

Ҳисоблаш тизимининг авария ҳолатини таҳлил қилиш ва ахборотни босишга бериш учун мўлжалланган дастур.

Машинная программа, определяющая возможность возникновения конфликтов в системе в результате прерываний.

Uzilishlar natijasida tizimda konfliktlarning vujudga kelish imkoniyatini belgilovchi mashina dasturi.

Узилишлар натижасида тизимда конфликтларнинг вужудга келиш имкониятини белгиловчи машина дастури.

Анализатор

uz - analizator

анализатор

en - analyzer

Анализатор аварийного состояния

uz - avariya holati analizatori

авария ҳолати

анализатори

en - emergency (disaster situation) analyzer

Анализатор прерываний

uz - uzilishlar analizatori

узилишлар анализатори

en - interrupt analyzer

A

Анализаторы сетевые

uz - tarmoq analizatorlari

тармоқ анализаторлари

en - network anylizers

Программы, осуществляющие «прослушивание» сетевого трафика и автоматическое выделение из трафика имен пользователей, паролей, номеров кредитных карт и другой подобной информации.

Tarmoq trafigini «eshitishni» va trafikdan avtomatik ravishda foydalanuvchilar nomlarining, parollar, kredit kartochkalar raqamlarining va boshqa shunga oʻxshash axborotning ajratib olinishini amalga oshiradigan dasturlar.

Тармоқ трафигини «эшитишни» ва трафикдан автоматик равишда фойдаланувчилар номларининг, пароллар, кредит карточкалар рақамларининг ва бошқа шунга ўхшаш ахборотнинг ажратиб олинисини амалга оширадиган дастурлар.

Антивирус

uz - antivirus

антивирус

en - antivirus

Программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.

Viruslardan himoya qilish, zararlangan dasturiy modullar va tizim sohalarini aniqlash, shuningdek, zararlangan obyektlarning boshlangʻich holatini tiklash uchun moʻljallangan dastur.

Вируслардан ҳимоя қилиш, зарарланган дастурий модуллар ва тизим соҳаларини аниқлаш, шунингдек, зарарланган объектларнинг бошланғич ҳолатини тиклаш учун мўлжалланган дастур.

Аппаратура засекречивания

uz - maxfiylashtirish

apparaturasi

махфийлаштириш

аппаратураси

en - ciphony equipment

Специальные технические устройства для автоматического шифрования и дешифрования телефонных и телеграфных переговоров (сообщений).

Telefon va telegraf soʻzlashuvlarini (xabarlarini) avtomatik ravishda shifrlash va deshifrlash uchun moʻljallangan maxsus texnik qurilmalar.

Телефон ва телеграф сўзлашувларини (хабарларини) автоматик равишда шифрлаш ва дешифрлаш учун мўлжалланган махсус техник қурилмалар.

A

Архивирование

uz - arxivlamoq

архивламоқ

en - archiving

Хранение любых резервных файлов и любых обобщенных документов.

Har qanday rezerv fayllar va umumlashtirilgan hujjatlarni saqlash.

Ҳар қандай резерв файллар ва умумлаштирилган ҳужжатларни сақлаш.

Архивировать

uz - arxivlash

архивлаш

en - to archive

Хранить резервные файлы и любые взаимосвязанные с ними журналы, обычно в течение заданного периода времени.

Rezerv fayllarni va ular bilan o‘zaro bog‘liq bo‘lgan har qanday jurnallarni, odatda belgilangan vaqt davri mobaynida saqlash.

Резерв файлларни ва улар билан ўзаро боғлиқ бўлган ҳар қандай журналларни, одатда белги-ланган вақт даври мобайнида сақлаш.

Атака

uz - hujum

ҳужум

en - attack

1 Попытка уничтожить, раскрыть, изменить, заблокировать, перехватить, получить несанкционированный доступ или несанкционированно использовать активы.

2 Действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей автоматизированной системы.

3 Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности или в целях использования их недостатков.

4 Попытка взлома защиты системы с целью перехвата информации, ее компрометации, нарушения режима сетевого обслуживания и т.д.

5 Попытка преодоления защиты системы.

Примечание – Атака может быть активной, ведущей к изменению данных или пассивной. Тот факт, что атака была осуществлена, не значит, что она успешна. Степень «успеха» атаки зависит от уязвимости системы и эффективности защитных мер.

1 Aktivlarni yo‘q qilish, ochish, o‘zgartirish, blokirovkalash, tutib olish, ruxsat etilmagan foydalanish

A

huquqini olish yoki aktivlardan ruxsatsiz foydalanishga urinish.

2 Buzg‘unchi tomonidan avtomatlashtirilgan tizim zaifliklaridan foydalanish yo‘li bilan tahdidni amalga oshirish harakati.

3 Xavfsizlikni ta‘minlash mexanizmlarini chetlab o‘tish maqsadida yoki ularning kamchiliklaridan foydalanish maqsadida qo‘llaniladigan harakatlar.

4 Axborotni qo‘lga kiritish, unga putur yetkazish (obro‘sizlantirish), tarmoq xizmati rejimini buzish va boshqa maqsadda tizim himoyasini buzishga urinish.

5 Tizim himoyasini yengib o‘tishga urinish. Hujum ma‘lumotlarni o‘zgartirishga olib keluvchi aktiv yoki passiv bo‘lishi mumkin.

Izoh – Hujumning amalga oshirilganligi uning muvaffaqiyatini bildirmaydi. Hujumning «muvaffaqiyat» darajasi tizim qanchalik zaifligiga va muhofaza choralarinig samaradorligiga bog‘liq.

1 Активларни йўқ қилиш, очиш, ўзгартириш, блокировкалаш, тутиб олиш, рухсат этилмаган фойдаланиш ҳуқуқини олиш ёки активлардан рухсатсиз фойдаланишга уриниш.

2 Бузғунчи томонидан автоматлаштирилган тизим заифликларидан фойдаланиш йўли билан таҳдидни амалга ошириш ҳаракати.

3 Хавфсизликни таъминлаш механизмларини четлаб ўтиш мақсадида ёки уларнинг камчиликлари­дан фойдаланиш мақсадида қўлланиладиган ҳаракатлар.

4 Ахборотни қўлга киритиш, унга путур етказиш (обро‘сизлантириш), тармоқ хизмати режимини бузиш ва бошқа мақсадда тизим ҳимоясини бузишга уриниш.

5 Тизим ҳимоясини енгиб ўтишга уриниш. Ҳужум маълумотларни ўзгартиришга олиб келувчи актив ёки пассив бўлиши мумкин.

Изоҳ – Ҳужумнинг амалга оширилганлиги унинг муваффақиятини билдирмайди. Ҳужумнинг «муваффақият» даражаси тизим қанчалик заифлигига ва муҳофаза чораларининг самарадорлигига боғлиқ.

A

Атака активная
uz - faol hujum
фаол хужум
en - active attack

1 Попытка проникновения в систему с изменением содержания передаваемой информации.
2 Реализация активной угрозы безопасности.

1 Tizimga, uzatilayotgan axborotning mazmunini o'zgartirib, kirishga urinish.
2 Xavfsizlikka aktiv tahdidni amalga oshirish.

1 Тизимга, узатилаётган ахборотнинг мазмунини ўзгартириб, киришга уриниш.
2 Хавфсизликка актив таҳдидни амалга ошириш.

Атака аналитическая, атака криптоаналитическая
uz - analitik hujum, kriptanalitik hujum
аналитик хужум, криптоаналитик хужум
en - analytical attack, cryptanalytical attack

Попытка разгадать код или найти ключ, используя аналитические методы.

Примечания

1 Аналитическая атака является противоположностью атаки на основе полного перебора.
2 Примерами аналитических атак являются статистический анализ изображений, поиск недостатков в алгоритме шифрования.

Analitik metodlardan foydalanib, kodni bilib olishga yoki kalitni topishga urinish.

Изохлар

1 Analitik hujum to'liq ajratish asosidagi hujumga qarama-qarshi holat bo'lib hisoblanadi.
2 Tasvirlarni statistik tahlil qilish, shifrlash algoritmidagi kamchiliklarni qidirish analitik hujumlarga misol bo'lib hisoblanadi.

Аналитик методлардан фойдаланиб, кодни билиб олишга ёки калитни топишга уриниш.

Изохлар

1 Аналитик хужум тўлиқ ажратиш асосидаги хужумга қарама-қарши ҳолат бўлиб ҳисобланади.
2 Тасвирларни статистик таҳлил қилиш, шифрлаш алгоритмидаги камчиликларни қидириш аналитик хужумларга мисол бўлиб ҳисобланади.

Атака внутренняя
uz - ichki hujum
ички хужум
en - insider attack

Атака, выполняемая из самой защищенной сети.

Muhofazalangan tarmoqning o'zidan amalga oshiriladigan hujum.

Муҳофазаланган тармоқнинг ўзидан амалга ошириладиган хужум.

A

Атака косвенная

uz - bilvosita hujum

билвосита ҳужум

en - indirect attack

Попытка нарушения защиты системы, основанная на обходе механизма обеспечения безопасности или принуждении системы к неправильному использованию этого механизма.

Xavfsizlikni ta'minlash mexanizmini chetlab o'tishga yoki tizimni ushbu mexanizmdan noto'g'ri foydalanishga majbur qilishga asoslangan, tizim muhofazasini buzishga bo'lgan urinish.

Xavfsizlikni ta'minlash mexanizmini chetlab o'tishga e'ki tizimni ushbu mexanizmdan noto'g'ri foydalanishga majbur qilishga asoslangan, tizim muhofazasini buzishga bo'lgan urinish.

Атака непосредственная

uz - bevosita hujum

бевосита ҳужум

en - direct attack

Попытка нарушения защиты системы, основанная на недостатках базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.

Bazaviy algoritmlar, xavfsizlikni ta'minlash mexanizmi prinsiplari yoki xususiyatlarining kamchiliklariga asoslangan, tizim muhofazasini buzishga bo'lgan urinish.

Базавий алгоритмлар, хавфсизликни таъминлаш механизми принциплари ёки хусусиятларининг камчиликларига асосланган, тизим муҳофазасини бузишга бўлган уриниш.

Атака пассивная

uz - passiv hujum

пассив ҳужум

en - passive attack

Атака, при которой нарушитель не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения.

Примечание – Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

Buzg'unchi uzatilayotgan xabarlarni o'zgartirish hamda jo'natuvchi va oluvchi o'rtasidagi axborot kanaliga o'z xabarlarini qo'yish imkoniyatiga ega bo'lmagan xujum.

A

Izoh – Passiv hujumdan maqsad, faqat uzatiladigan xabarlarни эшитиш ва trafikни tahlil qilish bo‘lishi mumkin.

Бузғунчи узатилаётган хабарларни ўзгартириш ҳамда жўнатувчи ва олувчи ўртасидаги ахборот каналига ўз хабарларини кўйиш имкониятига эга бўлмаган хужум.

Изоҳ – Пассив хужумдан мақсад, фақат узатиладиган хабарларни эшитиш ва трафикни таҳлил қилиш бўлиши мумкин.

Атаки пассивные

uz - passiv hujumlar

пассив хужумлар

en - monitoring attacks

Особая категория атак, во время которых используются пассивные методы анализа, направленные на раскрытие чувствительных внутренних данных ОО, при этом не влияющие на функционирование ОО.

Hujumlarning alohida kategoriyasi, bunday hujumlar paytida BOning ichki sezgir ma'lumotlarini ochishga yo'naltirilgan va BOning ishlashiga ta'sir qilmaydigan, passiv tahlil metodlaridan foydalaniladi.

Хужумларнинг алоҳида категорияси, бундай хужумлар пайтида БОнинг ички сезгир маълумотларини очишга йўналтирилган ва БОнинг ишлашига таъсир қилмайдиган, пассив таҳлил методларидан фойдаланилади.

Атака перебором открытого текста

uz - ochiq matnni tanlash
asosidagi hujum

очиқ матнни танлаш

асосидаги хужум

en - chosen-plaintext attack

Аналитическая атака, когда криптоаналитик может рассматривать неограниченное количество открытого текста сообщения и исследовать соответствующий шифротекст.

Analitik hujum, bunda kriptoanalitik xabarning cheklanmagan miqdordagi ochiq matnlarini ko'rib chiqishi va tegishli shifrmatnni tadqiq qilishi mumkin bo'ladi.

Аналитик хужум, бунда криптоаналитик хабарнинг чекланмаган миқдордаги очиқ матнларини кўриб чиқиши ва тегишли шифрматнни тадқиқ қилиши мумкин бўлади.

A

Атака переполнения

uz - to'ldirib yuborish hujumi
тўлдириб юбориш хужуми
en - flooding attack (overflow)

Создание искусственной перегрузки сетевого оборудования (маршрутизаторов, коммутаторов и др.) за счет введения ложного трафика большого объема.

Katta hajmdagi soxta trafikni kiritish hisobiga tarmoq uskunasing (marshrutizator, kommutator va b.larning) sun'iy ravishda o'ta yuklanishini vujudga keltirish.

Katta hajmdagi soxta trafikni kiritish hisobiga tarmoq uskunasing (marshrutizator, kommutator va b.larning) sun'iy ravishda o'ta yuklanishini vujudga keltirish.

Атака по известному открытому тексту

uz - ma'lum ochiq matn bo'yicha hujum
маълум очик матн бўйича хужум
en - known-plaintext attack

Аналитическая атака, когда криптоаналитик располагает шифротекстом и значительным количеством соответствующего ему открытого текста.

Analitik hujum, bunda kriptoanalitik shifmatn va unga tegishli ochiq matnning ma'lum miqdoriga ega bo'ladi.

Аналитик хужум, бунда криптоаналитик шифр-матн ва унга тегишли очик матннинг маълум миқдorigа эга бўлади.

Атака полным перебором, атака лобовая

uz - to'liq ajratib bajariladigan hujum, ro'paradan qilingan hujum
тўлиқ ажратиб бажариладиган хужум, рўпарадан қилинган хужум
en - exhaustive attack, brute-force attack

Попытка нарушить компьютерную безопасность методом проб и ошибок, перебирая возможные значения паролей или ключей.

Примечание – Атака полным перебором является противоположностью аналитической атаки.

Parol va kalitlarning mumkin bo'lgan qiymatlarini tanlab, sinashlar va xato qilishlar usulida kompyuter xavfsizligini buzishga urinish.

Izoh – To'liq ajratib bajariladigan hujum analitik hujumning aksi hisoblanadi.

Пароль ва калитларнинг мумкин бўлган қийматларини танлаб, синашлар ва хато қилишлар усулида компьютер хавфсизлигини бузишга уришиш.

Изоҳ – Тўлиқ ажратиб бажариладиган хужум аналитик хужумнинг акси ҳисобланади.

А

Атака с известным открытым сообщением

uz - ma'lum ochiq xabar bilan qilinadigan hujum
маълум очик хабар билан қилинадиган ҳужум
en - known-plaintext attack

Вид атаки, при которой злоумышленник имеет доступ к системе и ему известен текст передаваемого сообщения, который он может динамически изменять, пытаясь скрыть зашифрованный текст.

Jinoyatkor tizimga kira oladigan va unga uzatiladigan xabarning matni ma'lum bo'ladigan hujum turi. Jinoyatkor shifrlangan matnni yashirishga uringan holda, uzatiladigan xabar matnini dinamik tarzda o'zgartirishi mumkin.

Жинояткор тизимга кира оладиган ва унга узатиладиган хабарнинг матни маълум бўладиган ҳужум тури. Жинояткор шифрланган матнни яширишга уринган ҳолда, узатиладиган хабар матнни динамик тарзда ўзгартириши мумкин.

Атака с частой сменой пароля

uz - parolni tez-tez o'zgartirish bilan qilinadigan hujum
паролни тез-тез ўзгартириш билан қилинадиган ҳужум
en - leapfrog attack

Вид активной атаки на систему с многоуровневой защитой, во время которой злоумышленник использует чужие идентификационные данные, постоянно их меняет, пытаясь запутать следы, чтобы было невозможно определить, откуда поступил первый вызов.

Ko'p darajali muhofaza tizimiga qilinadigan aktiv hujum turi, bunda jinoyatkor begona identifikatsion ma'lumotlardan foydalanadi, birinchi chaqiruv qayerdan kelganligini aniqlash mumkin bo'lmaydigan tarzda izlarni chigallashtirib, ularni muntazam o'zgartiradi.

Kўп даражали муҳофаза тизимида қилинадиган актив ҳужум тури, бунда жинояткор бегона идентификацион маълумотлардан фойдаланади, биринчи чақирув қаердан келганлигини аниқлаш мумкин бўлмайдиган тарзда изларни чигаллаштириб, уларни мунтазам ўзгартиради.

Атака типа «отказ в обслуживании»

uz - «xizmat ko'rsatishni rad etish» turidagi hujum
«хизмат кўрсатишни рад этиш» туридаги ҳужум
en - denial of service attack

Преднамеренное воздействие на информационную систему или оборудование с целью создания условий, при которых правомерные пользователи не могут получить доступ к предоставляемым системой или оборудованием ресурсам или такой доступ им будет затруднен.

A

Qonuniy foydalanuvchilar tizim yoki uskuna yordamida taqdim etiladigan resurslardan foydalana olmasligi mumkin bo'lgan yoki ularga foydalana olishda qiyinchilik tug'diradigan sharoitlarni yaratish maqsadida axborot tizimiga yoki uskunaga qasddan ta'sir etish.

Қонуний фойдаланувчилар тизим ёки ускуна ёрдамида тақдим этиладиган ресурслардан фойдалана олмаслиги мумкин бўлган ёки уларга фойдалана олишда қийинчилик туғдирадиган шaroитларни яратиш мақсадида ахборот тизимига ёки ускунага қасддан таъсир этиш.

Атака только по шифротексту

uz - faqat shifratn bo'yicha qilinadigan hujum

фақат шифрматн бўйича қилинадиган ҳужум

en - cipher text-only attack

Аналитическая атака, когда криптоаналитик предполагает только шифротекстом.

Analitik hujum, bunda kriptanalitik faqat shifratn-ga ega bo'ladi.

Аналитик ҳужум, бунда криптоаналитик фақат шифрматнга эга бўлади.

Атрибут

uz - atribut

атрибут

en - attribute

Свойство или характеристика объекта, которые могут быть определены количественно или качественно непосредственно человеком или с помощью автоматизированных средств.

Obyektning bevosita inson tomonidan yoki avtomatlashtirilgan vositalar yordamida son yoki sifat jihatidan aniqlanishi mumkin bo'lgan xususiyati yoki xarakteristikasi.

Объектнинг бевосита инсон томонидан ёки автоматлаштирилган воситалар ёрдамида сон ёки сифат жиҳатидан аниқланиши мумкин бўлган хусусияти ёки хarakterистикаси.

Атрибут безопасности

uz - xavfsizlik atributi

хавфсизлик атрибути

en - security attribute

Хarakterистики субъектов, пользователей (в том числе внешних продуктов информационных технологий), объектов, информации, сеансов, и/или ресурсов, используемых при формулировании функциональных требований безопасности и те значения, которые используются при реализации функциональных требований безопасности.

A

Subyektlar, foydalanuvchilar xarakteristikasi (shu jumladan tashqi axborot texnologiyalari mahsulotlari), obyektlar, axborotlar, seanslar va/yoki resurslar, funksional xavfsizlik talablari shakllanishida ishlatiladigan va funksional xavfsizlik talablarini amalga oshirishda foydalaniladigan qiymatlar.

Субъектлар, фойдаланувчилар хarakteristikasi (шу жумладан ташқи ахборот технологиялари маҳсулотлари), объектлар, ахборотлар, сеанслар ва/ёки ресурслар, функционал хавфсизлик талаблари шаклланишида ишлатиладиган ва функционал хавфсизлик талабларини амалга оширишда фойдаланиладиган қийматлар.

Атрибут доступа

uz - foydalana olish atributi

фойдалана олиш атрибути

en - access attribute

Информационный элемент, связанный с объектом защиты и определяющий права доступа субъекта системы к этому объекту. Может принимать значение из заданного множества значений (как правило, «чтение», «запись» и «выполнение»).

Muhofaza obykti bilan bog‘langan va shu obyekt-dan tizim subyekting foydalana olish huquqini belgilovchi axborot elementi. Berilgan ko‘plab qiymatlardan ahamiyatlisini qabul qilishi mumkin (odatda, «o‘qish», «yozish» va «bajarish»).

Муҳофаза объекти билан боғланган ва шу объектдан тизим субъектининг фойдалана олиш ҳуқуқини белгиловчи ахборот элементи. Берилган кўплаб қийматлардан аҳамиятлисини қабул қилиши мумкин (одатда, «ўқиш», «ёзиш» ва «бajarиш»).

Аттестат объекта защиты

uz - muhofaza qilinadigan

obyekt attestati

муҳофаза қилинадиган

объект аттестати

en - protection object certificate

Документ, выдаваемый органом по сертификации или другим специально уполномоченным органом, подтверждающим наличие на объекте защиты необходимых и достаточных условий для выполнения установленных требований и норм эффективности защиты информации.

Sertifikatlash bo‘yicha organ yoki muhofaza qilinadigan obyektida axborotni muhofaza qilishning bel-

A

gilangan talablari va samaradorlik normalari bajarilishi uchun zarur va yetarli shart-sharoitlar mavjudligini tasdiqlaydigan boshqa maxsus vakolatlangan organ tomonidan beriladigan, hujjat.

Сертификатлаш бўйича орган ёки муҳофаза қилинадиган объектда ахборотни муҳофаза қилишнинг белгиланган талаblари ва самарадорлик нормалари бажарилиши учун зарур ва етарли шарт-шароитлар мавжудлигини тасдиқлайдиган бoshqa maxsus vakolatlangan organ tomonidan бериладиган, хужжат.

Аттестация

uz - attestatlash

аттестатлаш

en - attestation

Деятельность по подтверждению соответствия объекта информатизации требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции. Аттестация дает право владельцу объекта информатизации обрабатывать информацию с уровнем секретности, соответствующим уровню безопасности информации.

Axborotlashtirish obyektining davlat standartlari talablariga, sertifikatlash bo'yicha davlat organlari tomonidan, ularning o'z vakolatlari doirasida tasdiqlangan axborot muhofazasi bo'yicha boshqa normativ hujjatlar talablariga muvofiqligini tasdiqlash bo'yicha faoliyat. Attestatlash axborotlashtirish obyektining egasiga axborotni, axborot xavfsizligi darajasiga mos keluvchi maxfiylik darajasida qayta ishlash huquqini beradi.

Axborotlashtirish obyektining davlat standartlari talablariga, sertifikatlash bo'yicha davlat organlari tomonidan, ularning o'z vakolatlari doirasida tasdiqlangan axborot muhofazasi bo'yicha boshqa normativ hujjatlar talablariga muvofiqligini tasdiqlash bo'yicha faoliyat. Attestatlash axborotlashtirish obyektining egasiga axborotni, axborot xavfsizligi darajasiga mos keluvchi maxfiylik darajasida qayta ishlash huquqini beradi.

А

Аттестация в области защиты информации

uz - axborotni muhofaza qilish sohasida attestatlash

ахборотни муҳофаза қилиш соҳасида аттестатлаш

en - attestation in the field of information security

Деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта или процесса требованиям по защите информации.

Obyekt yoki jarayonni muhofaza qilish bo'yicha tashkiliy-texnik tadbirlar kompleksining axborotni muhofaza qilish yuzasidan qo'yiladigan talablarga muvofiqligini belgilash bilan bog'liq faoliyat.

Объект ёки жараёни муҳофаза қилиш бўйича ташкилий-техник тадбирлар комплексининг ахборотни муҳофаза қилиш юзасидан қўйиладиган талабларга мувофиқлигини белгилаш билан боғлиқ фаолият.

Аттестация испытательных лабораторий

uz - sinov laboratoriyalarini attestatlash

синов лабораторияларини аттестатлаш

en - testing laboratories attestation

Удостоверение компетентности испытательных лабораторий и их оснащённости, обеспечивающих проведение на должном техническом уровне всех предусмотренных нормативно-технической документацией испытаний закрепленных видов продукции и/или видов испытаний.

Sinov laboratoriyalarining kompetentligini va ularning normativ-texnik hujjatlarda ko'zda tutilgan birlashtirilgan mahsulot turlari sinovlarini va/yoki sinovlar turlarini tegishli texnik darajada o'tkazishni ta'minlovchi tarzda jihozlanganligini tasdiqlash.

Синов лабораторияларининг компетентлигини ва уларнинг норматив-техник ҳужжатларда кўзда тутилган бириктирилган маҳсулот турлари синовларини ва/ёки синовлар турларини тегишли техник даражада ўтказишни таъминловчи тарзда жиҳозланганлигини тасдиқлаш.

Аттестация объектов информатизации

uz - axborotlashtirish obyektlarini attestatsiya qilish

ахборотлаштириш объектларини аттестация қилиш

en - validation of objects of informatization

Комплекс организационно-технических мероприятий, направленных на определение соответствия фактического состояния защищенности объектов информатизации требованиям государственных стандартов и нормативно-правовых актов в области информационной безопасности.

Axborotlashtirish obyektlari muhofaza qilinganligi haqiqiy holatining axborot xavfsizligi sohasidagi davlat standartlari va normativ-huquqiy hujjatlari talablariga muvofiqligini aniqlashga yo'naltirilgan

A

tashkiliy-texnik chora-tadbirlar kompleksi.

Ахборотлаштириш объектлари муҳофаза қилинганлиги ҳақиқий ҳолатининг ахборот хавфсизлиги соҳасидаги давлат стандартлари ва норматив-ҳуқуқий ҳужжатлари талабларига мувофиқлигини аниқлашга йўналтирилган ташкилий-техник чора-тадбирлар комплекси.

Аудит

uz - audit

аудит

en - audit

1 Систематический, независимый и документированный процесс получения свидетельств аудита и их объективной оценки для определения степени выполнения согласованных критериев аудита.

Примечание – Аудит может быть внутренним, внешним, совместным или комплексным.

2 Процесс получения и анализа записей системного журнала (журнала аудита) с целью установления текущего состояния защищенности системы.

3 Экспертиза автоматизированной системы и всех ее составляющих с целью определения состояния безопасности системы, ее соответствия требованиям действующего законодательства и организационно-распорядительных документов организации.

1 Auditning kelishilgan mezonlarini bajarish darajasini aniqlash uchun audit dalillari va ularning obyektiv bahosini olishning muntazam, mustaqil va hujjatlashtirilgan jarayoni.

Izoh – Audit ichki, tashqi, birgalikda yoki kompleks bo‘lishi mumkin.

2 Tizim muhofazalanganligining kundalik holatini belgilash maqsadida tizim jurnali (audit jurnali) yozuvlarini olish va tahlil qilish jarayoni.

3 Avtomatlashtirilgan tizim va uning barcha tashkil etuvchilarini, tizim xavfsizligining holatini aniqlash, uning amaldagi qonunchilik talablariga va tashkilotning tashkiliy-idora qilish hujjatlariga muvofiqligini aniqlash maqsadida, ekspertiza qilish.

1 Аудитнинг келишилган мезонларини бажариш даражасини аниқлаш учун аудит далиллари ва уларнинг объектив баҳосини олишнинг мунта-

А

зам, мустақил ва ҳужжатлаштирилган жараёни.
Изоҳ – Аудит ички, ташқи, биргаликда ёки комплекс бўлиши мумкин.

2 Тизим муҳофазаланганлигининг кундалик ҳолатини белгилаш мақсадида тизим журнали (аудит журнали) ёзувларини олиш ва таҳлил қилиш жараёни.

3 Автоматлаштирилган тизим ва унинг барча ташкил этувчиларини, тизим хавфсизлигининг ҳолатини аниқлаш, унинг амалдаги қонунчилик талабларига ва ташкилотнинг ташкилий-идора қилиш ҳужжатларига мувофиқлигини аниқлаш мақсадида, экспертиза қилиш.

Аудит безопасности

uz - xavfsizlik auditi

хавфсизлик аудити

en - security audit

Независимый просмотр и анализ записей системы обработки данных и ее работы для проверки на адекватность управляющих функций системы, обеспечения соответствия принятой политике безопасности и операционным процедурам, обнаружения нарушений безопасности и выдачи рекомендаций по любым определенным изменениям в управлении, политике безопасности и процедурах.

Tizimning boshqaruvchi funksiyalarini adekvatlikka tekshirish, qabul qilingan xavfsizlik siyosatiga va operatsion protseduralarga muvofiqligini ta'minlash, xavfsizlikning buzilishlarini aniqlash hamda boshqaruvda, xavfsizlik siyosatida va protseduralarda har qanday muayyan o'zgarishlar bo'yicha tavsiyalar berish maqsadida, ma'lumotlarni qayta ishlash tizimi yozuvlarini va uning ishini mustaqil ko'rib chiqish va tahlil qilish.

Тизимнинг бошқарувчи функцияларини адекватликка текшириш, қабул қилинган хавфсизлик сиёсатига ва операцион процедураларга мувофиқлигини таъминлаш, хавфсизликнинг бузилишларини аниқлаш ҳамда бошқарувда, хавфсизлик сиёсатида ва процедураларда ҳар қандай муайян ўзгаришлар бўйича тавсиялар бериш мақсадида, маълумотларни қайта ишлаш тизими ёзувларини ва унинг ишини мустақил кўриб чиқиш ва таҳлил қилиш.

А

Аудит внешний

uz - tashqi audit

ташқи аудит

en - external audit

Аудиты, обычно называемые «аудитами второй стороны» или «аудитами третьей стороны».

Примечание – Аудиты второй стороны проводятся сторонами, заинтересованными в деятельности организации, например, потребителями или другими лицами от их имени. Аудиты третьей стороны проводятся внешними независимыми организациями.

Odatda, «ikkinchi tomon auditi» yoki «uchinchi tomon auditi» deb nomlanadigan auditlar.

Izoh – Ikkinchi tomon auditlarini tashkilot faoliyatidan manfaatdor bo‘lgan tomonlar, masalan, iste‘molchi yoki ularning nomidan boshqa shaxslar o‘tkazadilar. Tashqi mustaqil tashkilotlar tomonidan uchinchi tomon auditlari o‘tkaziladi.

Odatda, «иккинчи томон аудити» ёки «учинчи томон аудити» деб номланадиган аудитлар.

Изоҳ – Иккинчи томон аудитларини ташкилот фаолиятдан манфаатдор бўлган томонлар, масалан, истеъмолчи ёки уларнинг номидан бошқа шахслар ўтказадилар. Ташқи мустақил ташкилотлар томонидан учинчи томон аудитлари ўтказилади.

Аудит внутренний

uz - ichki audit

ички аудит

en - internal audit

Аудиты, иногда называемые «аудитами первой стороны», которые проводятся обычно самой организацией или от ее имени, для внутренних целей и могут служить основанием для заявления о соответствии.

Ba’zida «birinchi tomon auditi» deb nomlanadigan, odatda, tashkilot tomonidan yoki uning nomidan ichki maqsadlar uchun o‘tkaziladigan va muvofiqlik to‘g‘risida e’lon qilishga asos bo‘lib xizmat qiladigan auditlar.

Баъзида «биринчи томон аудити» деб номланадиган, одатда, ташкилот томонидан ёки унинг номидан ички мақсадлар учун ўтказиладиган ва мувофиқлик тўғрисида эълон қилишга асос бўлиб хизмат қиладиган аудитлар.

Аудит комплексный

uz - kompleks audit

комплекс аудит

en - complex audit

Одновременный аудит двух или более разных систем управления.

Ikki yoki undan ko‘p bo‘lgan turli boshqarish tizimlarining bir vaqtdagi auditi.

Икки ёки ундан кўп бўлган турли бошқариш тизимларининг бир вақтдаги аудити.

А

Аудит компьютерной системы

uz - kompyuter tizimining
auditi

компьютер тизимининг
аудити

en - computer-system audit

Экспертиза процедур, используемых в системе обработки данных, для оценки их эффективности и правильности выполнения, а также выдача рекомендаций по повышению безопасности.

Ma'lumotlarni qayta ishlash tizimida qo'llaniladigan protseduralarni, ularning samaradorligi va to'g'ri bajarilayotganligini baholash yuzasidan ekspertiza qilish, shuningdek, xavfsizlikni oshirish bo'yicha tavsiyalar berish.

Ma'lumotlarni qayta ishlash tizimida qo'llaniladigan protseduralarni, ularning samaradorligi va to'g'ri bajarilayotganligini baholash yuzasidan ekspertiza qilish, shuningdek, xavfsizlikni oshirish bo'yicha tavsiyalar berish.

Аудит совместный

uz - qo'shma audit
qo'shma audit

en - joint audit

Аудит, проводимый совместно двумя или несколькими организациями.

Ikki yoki bir nechta tashkilot bilan birgalikda o'tkaziladigan audit.

Ikki ёки бир нечта ташкилот билан биргаликда ўтказиладиган аудит.

Аудитор безопасности

uz - xavfsizlik auditori
xavfsizlik auditori

en - security auditor

Лицо или процесс, которому разрешен доступ к данным проверки безопасности и создание отчетов о проверке.

Xavfsizlikni tekshirishga oid ma'lumotlardan foydalanish va tekshiruv to'g'risida hisobotlar tuzish ruxsat etilgan shaxs yoki jarayon.

Xavfsizlikni tekshirishga oid ma'lumotlardan foydalanish va tekshiruv to'g'risida hisobotlar tuzish ruxsat etilgan shaxs ёки жараён.

Аутентификатор

uz - autentifikator
аутентификатор

en - authenticator

Средство аутентификации, представляющее отличительный признак пользователя.

Примечание – Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя, которые вводятся в ЭВМ с клавиатуры дисплея, с идентификационной карты или при помощи специального устройства аутентификации по биометрическим данным.

A

Foydalanuvchining farqlovchi belgisini ko'rsatuvchi autentifikatsiya vositasi.

Izoh – Qo'shimcha kodli so'zlar, biometrik ma'lumotlar va foydalanuvchining boshqa farqlovchi belgilari autentifikatsiya vositalari bo'lishi mumkin. Ular elektron hisoblash mashinasiga displey klaviaturasidan, identifikatsion kartadan yoki biometrik ma'lumotlarga qarab autentifikatsiya qilishning maxsus qurilmalari yordamida kiritiladi.

Фойдаланувчининг фарқловчи белгисини кўрсатувчи аутентификация воситаси.

Изоҳ – Қўшимча кодли сўзлар, биометрик маълумотлар ва фойдаланувчининг бошқа фарқловчи белгилари аутентификация воситалари бўлиши мумкин. Улар электрон ҳисоблаш машинасига дисплей клавиатурасидан, идентификацион картадан ёки биометрик маълумотларга қараб аутентификация қилишнинг махсус қурилмалари ёрдамида киритилади.

Аутентификация

uz - autentifikatsiya qilish

аутентификация қилиш

en - authentication

1 Обеспечение уверенности в том, что предъявленный логическим объектом идентификатор является подлинным.

2 Процедура установления подлинности пользователя (абонента сети, отправителя сообщения), программы, устройства или данных (информации, получаемого сообщения, ключа).

1 Mantiqiy obyekt tomonidan taqdim etilgan identifikator haqiqiylikiga ishonch hosil qilinishini ta'minlash.

2 Foydalanuvchining (tarmoq abonentining, xabar jo'natuvchining), dastur, qurilma yoki ma'lumotlarning (axborotning, olinadigan xabarning, kalitning) haqiqiylikini belgilash protsedurasi.

1 Мантикий объект томонидан тақдим этилган идентификатор ҳақиқийлигига ишонч ҳосил қилинишини таъминлаш.

2 Фойдаланувчининг (тармоқ абонентининг, хабар жўнатувчининг), дастур, қурилма ёки маълумотларнинг (ахборотнинг, олинадиган хабарнинг, калитнинг) ҳақиқийлигини белгилаш процедураси.

A

Аутентификация взаимная

uz - o‘zaro autentifikatsiya qilish

ўзаро аутентификация қилиш

en - mutual authentication

Процедура аутентификации, при которой осуществляется одновременно проверка регистрационных данных мобильной и базовой станций.

Autentifikatsiya protsedurasi, unda mobil va bazaviy stansiyalarning ro‘yxatdan o‘tkaziladigan ma’lumotlarini tekshirish bir vaqtda amalga oshiriladi.

Аутентификация процедураси, унда мобил ва базавий станцияларнинг рўйхатдан ўтказиладиган маълумотларини текшириш бир вақтда амалга оширилади.

Аутентификация данных

uz - ma’lumotlarni autentifikatsiya qilish

маълумотларни аутентификация қилиш

en - data authentication

Процесс проверки целостности данных. Например, проверка того, что полученные данные идентичны отправленным данным, а также проверка того, что программа не заражена вирусом.

Ma’lumotlar yaxlitligini tekshirish jarayoni. Masalan, olingan ma’lumotlarning jo‘natilgan ma’lumotlar bilan bir xilligini, shuningdek, dasturda virus bor yoki yo‘qligini tekshirish.

Маълумотлар яхлитлигини текшириш жараёни. Масалан, олинган маълумотларнинг жўнатилган маълумотлар билан бир хиллигини, шунингдек, дастурда вирус бор ёки йўқлигини текшириш.

Аутентификация источника данных

uz - ma’lumotlar manbaini autentifikatsiya qilish

маълумотлар манбаини аутентификация қилиш

en - data origin authentication

Подтверждение подлинности источника полученных данных.

Olingan ma’lumotlar manbaining haqiqiyiligini tasdiqlash.

Олинган маълумотлар манбаининг ҳақиқийлигини тасдиқлаш.

Аутентификация личности, подтверждение подлинности личности

uz - shaxsni autentifikatsiya qilish, shaxsning haqiqiyiligini tasdiqlash

шахсни аутентификация қилиш, шахснинг ҳақиқийлигини тасдиқлаш

Выполнение проверок (например, пароля или токена), позволяющих системе обработки данных распознавать логические объекты.

Ma’lumotlarni qayta ishlash tizimiga mantiqiy obyektlarni aniqlab olish imkonini beradigan tekshiruvlar (masalan, parol yoki token)ning bajarilishi.

Маълумотларни қайта ишлаш тизимига мантиқий

А

en - identity authentication,
identity validation

**Аутентификация
многофакторная**

uz - ko'p faktorli
autentifikatsiya

кўп факторли

аутентификация

en - multi-factor authentication

объектларни аниқлаб олиш имконини берадиган текширувлар (масалан, пароль ёки токен)нинг бажарилиши.

Аутентификация пользователя на основе нескольких независимых факторов (биометрические данные, того, что он знает, и того, чем он владеет, и т.п.).

Примечание – Аутентификация многофакторная представляет гибкий подход, позволяющий организации реализовать устойчивую систему управления доступом на основе использования различных методов аутентификации (одноразовые пароли, сертификаты, контекст и др.).

Foydalanuvchini bir nechta mustaqil faktor (biometrik ma'lumotlar, u biladigan hamda u ega bo'lganlar) asosida autentifikatsiya qilish.

Izoh – Ko'p faktorli autentifikatsiya tashkilotga autentifikatsiya qilishning turli metodlaridan (bir martalik parollar, sertifikatlar, kontekst va boshqalar) foydalanish asosida foydalana olishning barqaror tizimini amalga oshirish imkonini beradigan moslashuvchan yondashuvni o'zida ifodalaydi.

Фойдаланувчини бир нечта мустақил фактор (биометрик маълумотлар, у биладиган ҳамда у эга бўлганлар) асосида аутентификация қилиш.

Изоҳ – Кўп факторли аутентификация ташкилотга аутентификация қилишнинг турли методларидан (бир марталик пароллар, сертификатлар, контекст ва бошқалар) фойдаланиш асосида фойдалана олишнинг барқарор тизимини амалга ошириш имконини берадиган мослашувчан ёндашувни ўзида ифодалайди.

Аутентификация неявная

uz - noaniq autentifikatsiya

ноаниқ аутентификация

en - implicit authentication

Процедура аутентификации, основанная на использовании ключей шифрования, которые генерируются по заданному алгоритму в процессе аутентификации.

Autentifikatsiya qilish jarayonida berilgan algoritm bo'yicha generatsiyalanadigan shifrlash kalitlaridan foydalanishga asoslangan autentifikatsiya qilish protsedurasi.

Аутентификация қилиш жараёнида берилган алгоритм бўйича генерацияланадиган шифрлаш калитларидан фойдаланишга асосланган аутенти-

А

Аутентификация односторонняя

uz - bir tomonlama

autentifikatsiya qilish

бир томонлама

аутентификация қилиш

en - single-side authentication

Аутентификация сильная

uz - kuchli autentifikatsiya

кучли аутентификация

en - strong authentication

Аутентификация слабая

uz - kuchsiz autentifikatsiya

кучсиз аутентификация

en - poor authentication

Аутентификация сообщения

uz - xabarni autentifikatsiya

qilish

хабарни аутентификация

қилиш

en - message authentication

фикация қилиш процедураси.

Аутентификация отправителя или получателя сообщения.

Хабар jo‘natuvchi yoki oluvchini autentifikatsiya qilish.

Хабар жўнатувчи ёки олувчини аутентификация қилиш.

Аутентификация, в процессе которой помимо проверки идентификатора и пароля пользователя используется криптографическое преобразование всей аутентифицируемой информации.

Foydalanuvchining identifikatori va parolini tekshirish jarayonidan tashqari barcha autentifikatsiya qilinadigan axborotni kriptografik o‘zgartirishdan foydalaniladigan autentifikatsiya.

Фойдаланувчининг идентификатори ва паролни текшириш жараёнидан ташқари барча аутентификация қилинадиган ахборотни криптографик ўзгартиришдан фойдаланиладиган аутентификация.

Проверка только идентификатора и пароля пользователя, иницирующего процесс аутентификации.

Autentifikatsiya qilish jarayonini amalga oshiruvchi foydalanuvchining faqat identifikatori va parolini tekshirish.

Аутентификация қилиш жараёнини амалга оширувчи фойдаланувчининг фақат идентификатори ва паролни текшириш.

Верификация того, что сообщение заявленного отправителя было передано предназначенному получателю неповрежденным и неизменным.

Tayinlangan jo‘natuvchining xabari belgilangan oluvchiga shikastlanmasdan va o‘zgartirmasdan uzatilganligini verifikatsiya qilish.

Тайинланган жўнатувчининг хабари белгиланган

A

олувчига шикастланмасдан ва ўзгартирмасдан узатилганлигини верификация қилиш.

Аутентификация явная

uz - aniq autentifikatsiya

аниқ аутентификация

en - explicit authentication

Процедура аутентификации по паролю или с использованием заранее сформированных криптографических ключей, структура которых в процессе аутентификации не изменяется.

Parol bo‘yicha yoki strukturasi autentifikatsiya qilish jarayonida o‘zgarmaydigan, oldindan shakllantirilgan kriptografik kalitlardan foydalanib autentifikatsiya qilish jarayoni.

Пароль бўйича ёки структураси аутентификация қилиш жараёнида ўзгармайдиган, олдиндан шакллантирилган криптографик калитлардан фойдаланиб аутентификация қилиш жараёни.

Аутентичность,

подлинность

uz - haqiqiylik, asllik

ҳақиқийлик, асллик

en - authenticity

1 Свойство, гарантирующее, что логический объект идентичен заявленному.

2 Свойство данных быть подлинными или свойство систем быть способными обеспечить подлинность данных.

1 Mantiqiy obyekt tasdiqlanganiga o‘xshashligini kafolatlovchi xususiyat.

2 Ma’lumotlarning haqiqiy bo‘lish xususiyati yoki tizimlarning ma’lumotlar haqiqiylikini ta’minlay olish xususiyati.

1 Мантикий объект тасдиқланганига ўхшашлигини кафолатловчи хусусият.

2 Маълумотларнинг ҳақиқий бўлиш хусусияти ёки тизимларнинг маълумотлар ҳақиқийлигини таъминлай олиш хусусияти.

Аутсорсинг

uz - autsorsing

аутсорсинг

en - outsource

Передача организацией по договору выполнения части своих функций или процессов специализированной внешней организации.

Примечание – Несмотря на то, что внешняя организация находится за пределами системы управления организации, выполняемые внешней организацией функции или

А

процессы находятся в пределах этой системы управления.

Tashkilot tomonidan shartnoma bo'yicha o'zining funksiyalari yoki jarayonlarining bir qismini bajarishni ixtisoslashtirilgan tashqi tashkilotga berish.

Izoh – Tashqi tashkilot tashkilotning boshqarish tizimlari chegaralaridan tashqarida joylashganligiga qaramay, tashqi tashkilot tomonidan bajariladigan funksiyalar yoki jarayonlar ushbu boshqarish tizimining chegarasida joylashgan.

Ташкилот томонидан шартнома бўйича ўзининг функциялари ёки жараёнларининг бир қисмини бажаришни ихтисослаштирилган ташқи ташкилотга бериш.

Изоҳ – Ташқи ташкилот ташкилотнинг бошқариш тизимлари чегараларидан ташқарида жойлашганлигига қармай, ташқи ташкилот томонидан бажариладиган функциялар ёки жараёнлар ушбу бошқариш тизимининг чегарасида жойлашган.

Б

База вычислительная достоверная

uz - ishonchli hisoblash bazasi
ишончли ҳисоблаш базаси
en - trusted computing base

Совокупность защитных механизмов вычислительной системы, включая программные и аппаратные компоненты, ответственные за поддержание политики безопасности.

Hisoblash tizimi muhofaza mexanizmlarining jami, jumladan, xavfsizlik siyosatini qo'llab-quvvatlash uchun javobgar dasturiy va apparat komponentlar.

Ҳисоблаш тизими муҳофаза механизмларининг жами, жумладан, хавфсизлик сиёсатини қўллаб-қувватлаш учун жавобгар дастурий ва аппарат компонентлар.

База данных распределенная

uz - taqsimlangan ma'lumotlar bazasi
тақсимланган маълумотлар базаси
en - distributed database

База данных, физически распределенная на две или больше компьютерные системы.

Fizik jihatdan ikki yoki undan ortiq kompyuter tizimlariga taqsimlangan ma'lumotlar bazasi.

Физик жиҳатдан икки ёки ундан ортиқ компью-

Б

тер тизимларига тақсимланган маълумотлар базаси.

База информационная

uz - axborot bazasi

ахборот базаси

en - information base

Совокупность описания специальных объектов, существование которых в предметной области предусмотрено в конкретный момент времени или в определенный период времени, и описания текущих состояний связей, представляющих интерес в предметной области.

Predmet sohasida mavjudligi aniq vaqt onida yoki ma'lum vaqt davrida ko'zda tutilgan maxsus obyektlar tavsiflari yig'indisi, predmet sohasida qiziqish uyg'otuvchi aloqalar joriy holatining tavsifi.

Предмет соҳасида мавжудлиги аниқ вақт онида ёки маълум вақт даврида кўзда тutilган махсус объектлар тавсифлари йиғиндиси, предмет соҳасида қизиқиш уйғотувчи алоқалар жорий ҳолатининг тавсифи.

Барьер информационный

uz - axborot to'siq

ахборот тўсиқ

en - information barrier

Совокупность различных препятствий, возникающих на пути распространения и использования информации.

Axborotni tarqatish va undan foydalanish yo'lida yuzaga keladigan turli to'siqlar.

Ахборотни тарқатиш ва ундан фойдаланиш йўлида юзага келадиган турли тўсиқлар.

Барьер коммуникационный

uz - kommunikatsion to'siq

коммуникацион тўсиқ

en - communication barrier

Барьер, возникающий в процессе взаимодействия между системными аналитиками и управленческим персоналом предприятия (учреждения) при разработке и внедрении автоматизированных систем.

Avtomatlashtirilgan tizimlarni ishlab chiqish va joriy qilishda, o'zaro hamkorlik qilish jarayonida tizim analitiklari va korxonalar (muassasa)ning boshqaruv personali o'rtasida yuzaga keladigan to'siq.

Автоматлаштирилган тизимларни ишлаб чиқиш ва жорий қилишда, ўзаро ҳамкорлик қилиш жара-

Б

ёнида тизим аналитиклари ва корхона (муассаса)нинг бошқарув персонали ўртасида юзага келадиган тўсиқ.

Безопасность
uz - xavfsizlik
хавфсизлик
en - security

1 Способность системы или сети обеспечивать защиту, достоверность и надежность хранения информации.

2 Способность объекта противостоять воздействиям случайных и преднамеренных угроз.

1 Tizim yoki tarmoqning, axborotning muhofaza qilinishini, haqiqiylikini va ishonchli saqlanishini ta'minlash qobiliyati.

2 Obyektning tasodifiy va qasddan qilinadigan tahdidlar ta'siriga qarshi tura olish qobiliyati.

1 Тизим ёки тармоқнинг, ахборотнинг муҳофаза қилинишини, ҳақиқийлигини ва ишончли сақла-нишини таъминлаш қобилияти.

2 Объектнинг тасодифий ва қасддан қилинади-ган таҳдидлар таъсирига қарши тура олиш қоби-лияти.

Безопасность автоматизи-
рованной информационной
системы

uz - avtomatlashtirilgan axborot
tizimining xavfsizligi

автоматлаштирилган
ахборот тизимининг
хавфсизлиги

en - automated information
system security

Совокупность мер управления и контроля, защищающая автоматизированную информационную систему от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения этой системы и данных.

Avtomatlashtirilgan axborot tizimiga xizmat ko'rsatishdagi buzilish va bu tizimni hamda ma'lumotlarni ruxsat etilmagan tarzda (qasddan yoki tasodifan) ochish, o'zgartirish yoki buzishdan muhofaza qiluvchi boshqaruv va nazorat chora-tadbirlarining jami.

Автоматлаштирилган ахборот тизими-га хизмат кўрсатишдаги бузилиш ва бу тизимни ҳамда маълумотларни рухсат этилмаган тарзда (қасддан ёки тасодифан) очиш, ўзгартириш ёки бузишдан муҳофаза қилувчи бошқарув ва назорат чора-тад-бирларининг жами.

Безопасность
автоматизированной

Защищенность автоматизированной системы от несанкционированного вмешательства в нор-

Б

системы

uz - avtomatlashtirilgan tizimning xavfsizligi

автоматлаштирилган

тизимнинг хавфсизлиги

en - automated system security

мальный процесс ее функционирования, а также от попыток хищения, незаконной модификации или разрушения ее компонентов.

Avtomatlashtirilgan tizimning, uning normal ishlash jarayoniga ruxsat etilmagan aralashuvdan, shuningdek, tizim komponentlarini o'g'irlash, noqonuniy o'zgartirish yoki buzishdan muhofaza qilinganligi.

Автоматлаштирилган тизимнинг, унинг нормал ишлаш жараёнига рухсат этилмаган аралашувдан, шунингдек, тизим компонентларини ўғирлаш, ноқонуний ўзгартириш ёки бузишдан муҳофаза қилинганлиги.

Безопасность

административная

uz - ma'muriy xavfsizlik

маъмурий хавфсизлик

en - administrative security

Административные меры, направленные на обеспечение компьютерной безопасности. К этим мерам относятся операционные процедуры и процедуры подотчетности, процедуры расследования нарушений безопасности и анализ журналов аудита.

Kompyuter xavfsizligini ta'minlashga qaratilgan ma'muriy chora-tadbirlar. Operatsion protseduralar va hisob berish protseduralari, xavfsizlik buzilishlarini tekshirish hamda audit jurnallarini tahlil qilish protseduralari shunday chora-tadbirlar hisoblanadi.

Компьютер хавфсизлигини таъминлашга қаратилган маъмурий чора-тадбирлар. Операцион процедуралар ва ҳисоб бериш процедуралари, хавфсизлик бузилишларини текшириш ҳамда аудит журналларини таҳлил қилиш процедуралари шундай чора-тадбирлар ҳисобланади.

Безопасность данных

uz - ma'lumotlarning xavfsizligi

маълумотларнинг

хавфсизлиги

1 Компьютерная безопасность применительно к данным.

2 Защищенность данных от несанкционированных действий (случайных или умышленных), приводящих к модификации, раскрытию или

Б

en - data security

разрушению данных.

3 Свойство системы противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации.

1 Ma'lumotlarga nisbatan qo'llaniladigan kompyuter xavfsizligi.

2 Ma'lumotlarning, ma'lumotlar o'zgartirilishiga, fosh bo'lishi yoki buzilishiga olib keluvchi, ruxsat etilmagan ta'sirlardan (tasodifiy yoki qasddan) muhofaza qilinganligi.

3 Tizimning, qayta ishlanadigan va saqlanadigan axborotdan ruxsat etilmagan tarzda foydalanish yo'lidagi urinishlarga qarshi tura olish xususiyati.

1 Маълумотларга нисбатан қўлланиладиган компьютер хавфсизлиги.

2 Маълумотларнинг, маълумотлар ўзгартирилишига, фoш бўлиши ёки бузилишига олиб келувчи, рuxсат этилмаган таъсирлардан (тасодифий ёки қасдан) муҳофаза қилинганлиги.

3 Тизимнинг, қайта ишланадиган ва сақланадиган ахборотдан рuxсат этилмаган тарзда фойдаланиш йўлидаги уринишларга қарши тура олиш хусусияти.

Безопасность информации

uz - axborot xavfsizligi

ахборот хавфсизлиги

en - information security

1 Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

2 Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.

3 Защищенность устройств, процессов, программ, среды и данных, обеспечивающая целостность информации.

Б

1 Axborotning, nomaqbul (axborot munosabatlarining tegishli subyektlari uchun) oshkor qilinishdan (konfidentsialligining buzilishidan), axborotning buzilishi yoki foydalana olish darajasini pasayishdan yoki yo'qotilishdan, shuningdek, noqonuniy ko'paytirilishdan muhofaza qilinganligi.

2 Axborotning, axborot resurslarining va axborot tizimlarining holati, unda talab etiladigan ehtimollikka ko'ra axborotni (ma'lumotlarni) tarqalib ketishidan, o'g'irlash, yo'qotish, ruxsat etilmagan tarzda o'chirish, buzish, o'zgartirish (qalbakilashtirish), nusxa ko'chirish, blokirovka qilish va sh.k. muhofaza qilish ta'minlanadi.

3 Axborotning yaxlitligini ta'minlovchi qurilmalar, jarayonlar, dasturlar, muhit va ma'lumotlarning muhofaza qilinganligi.

1 Ахборотнинг, номақбул (ахборот муносабатларининг тегишли субъектлари учун) ошкор қилинишдан (конфиденциаллигининг бузилишидан), ахборотнинг бузилиши ёки фойдалана олиш даражасини пасайишдан ёки йўқотилишдан, шунингдек, ноқонуний кўпайтирилишдан муҳофаза қилинганлиги.

2 Ахборотнинг, ахборот ресурсларининг ва ахборот тизимларининг ҳолати, унда талаб этиладиган эҳтимолликка кўра ахборотни (маълумотларни) тарқалиб кетишидан, ўғирлаш, йўқотиш, рuxсат этилмаган тарзда ўчириш, бузиш, ўзгартириш (қалбакилаштириш), нусха кўчириш, блокировка қилиш ва ш.к. муҳофаза қилиш таъминланади.

3 Ахборотнинг яхлитлигини таъминловчи қурилмалар, жараёнлар, дастурлар, муҳит ва маълумотларнинг муҳофаза қилинганлиги.

Безопасность информации (данных)

uz - axborot (ma'lumotlar) xavfsizligi

ахборот (маълумотлар) хавфсизлиги

en - security of information (data)

1 Интегральное свойство информации (данных) противостоят случайным или преднамеренным воздействиям (угрозам), наносящим ущерб собственнику информации.

Примечание – Характеристиками безопасности информации (данных) являются конфиденциальность, целостность и доступность, а также неотказуемость, подотчетность, аутентичность

Б

и достоверность.

2 Состояние защищенности информации (данных), обрабатываемых средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

1 Axborot (ma'lumotlar)ning axborot egasiga zarar yetkazuvchi tasodifiy yoki qasddan qilinadigan ta'sirlar (tahdidlar)ga qarshi tura olish integral xususiyati.

Izoh – Axborot (ma'lumotlar) xavfsizligining xarakteristikalarini bo'lib, konfidensiallik, yaxlitlik va foydalana olishlik, shuningdek, rad etolmaslik, hisob berishlik, haqiqiylik va ishonchlik hisoblanadi.

2 Hisoblash texnikasi yoki avtomatlashtirilgan tizim vositalarida qayta ishlanadigan axborot (ma'lumotlar)ning ichki va tashqi tahdidlardan muhofazalan-ganlik holati.

1 Ахборот (маълумотлар)нинг ахборот эгасига зарар етказувчи тасодифий ёки қасдан қилинадиган таъсирлар (тахдидлар)га қарши тура олиш интеграл хусусияти.

Изоҳ – Ахборот (маълумотлар) хавфсизлигининг харақтеристикалари бўлиб, конфиденциаллик, яхлитлик ва фойдалана олишлик, шунингдек, рад этолмаслик, ҳисоб беришлик, ҳақиқийлик ва ишончилиқ ҳисобланади.

2 Ҳисоблаш техникаси ёки автoматлаштирилган тизим воситаларида қайта ишланадиган ахборот (маълумотлар)нинг ички ва ташқи тахдидлардан муҳофазаланганлик ҳолати.

1 Состояние защищенности интересов личности, общества и государства в информационной сфере.

2 Сохранение конфиденциальности, целостности и доступности информации.

Примечание – Можно также выделить и другие, не всегда обязательные, свойства информационной безопасности, например, аутентичность, подотчетность, неотказуемость и достоверность.

3 Совокупность свойств информации и поддерживающей инфраструктуры быть защищенной от случайных или преднамеренных воздействий

Безопасность

информационная

uz - axborot xavfsizligi

ахборот хавфсизлиги

en - information security

Б

естественного или искусственного характера.

1 Axborot sohasida shaxs, jamiyat va davlat manfa-atlarining muhofaza qilinganlik holati.

2 Axborot konfidensialligi, yaxlitligi va undan foydalana olishlikning saqlanishi.

Izoh – Axborot xavfsizligining boshqa, har doim ham shart bo‘lmagan xususiyatlarini, masalan, haqiqiylik, hisobot berishlik, rad etolmaslik va ishonchlilikni ko‘rsatish mumkin.

3 Axborot va ta‘minlovchi infrastrukturaning tabiiy yoki sun‘iy xarakterdagi tasodifiy yoki qasddan qilinadigan ta‘sirlardan muhofaza qilinganlik xususiyatlarining jami.

1 Ахборот соҳасида шахс, жамият ва давлат манфаатларининг муҳофаза қилинганлик ҳолати.

2 Ахборот конфиденциаллиги, яхлитлиги ва undan фойдалана олишликнинг сақланиши.

Изоҳ – Ахборот хавфсизлигининг бошқа, ҳар доим ҳам шарт бўлмаган хусусиятларини, масалан, ҳақиқийлик, ҳисобот беришлик, рад этолмаслик ва ишончлиликни кўрсатиш мумкин.

3 Ахборот ва таъминловчи инфраструктуранинг табиий ёки сунъий характердаги тасодифий ёки қасддан қилинадиган таъсирлардан муҳофаза қилинганлик хусусиятларининг жами.

Безопасность информационной системы

uz - axborot tizimi xavfsizligi

ахборот тизими

хавфсизлиги

en - information system security

1 Свойство информационной системы противостоять попыткам несанкционированного доступа.

2 Совокупность действий и мер, необходимых для обеспечения адекватной защиты системы, включая аппаратно-программные функции, характеристики и средства; операционные и учетные процедуры, средства управления доступом на сервере, удаленных компьютерах и средствах телекоммуникаций; административные мероприятия, физические конструкции и устройства; управление персоналом и коммуникациями системы.

1 Axborot tizimining ruxsat etilmagan tarzda foydalanishga urinishlarga qarshi tura olish xususiyati.

2 Tizimning adekvat muhofazasini ta‘minlash uchun zarur bo‘lgan amallar va chora-tadbirlar jami, jumladan, apparat-dasturiy funksiyalar, xarakteristikalar, vositalar; operatsion va hisobga olish protseduralari,

Б

serverda, olisdagi kompyuterlar hamda telekommunikatsiyalar vositalarida erkin foydalanishni boshqarish vositalari; ma'muriy tadbirlar, fizik konstruksiyalar va qurilmalar; personalni va tizim kommunikatsiyalarini boshqarish.

1 Ахборот тизимининг рухсат этилмаган тарзда фойдаланишга уринишларга қарши тура олиш хусусияти.

2 Тизимнинг адекват муҳофазасини таъминлаш учун зарур бўлган амаллар ва чора-тадбирлар жами, жумладан, аппарат-дастурий функциялар, характеристикалар, воситалар; операцион ва ҳисобга олиш процедуралари, серверда, олисдаги компьютерлар ҳамда телекоммуникациялар восита-ларида эркин фойдаланишни бошқариш восита-лари; маъмурий тадбирлар, физик конструкция-лар ва қурилмалар; персонални ва тизим комму-никацияларини бошқариш.

Безопасность информационной технологии

uz - axborot texnologiyasi xavfsizligi

ахборот технологияси хавфсизлиги

en - information technology security

Безопасность коммуникационная

uz - kommunikatsion xavfsizlik

коммуникацион хавфсизлик

en - communications security

Безопасность компьютерная

uz - kompyuter xavfsizligi

компьютер хавфсизлиги

en - computer security

Защищенность технологического процесса обработки информации.

Axborotni qayta ishlash texnologik jarayonining muhofazalanganligi.

Ахборотни қайта ишлаш технологик жараёнининг муҳофазаланганлиги.

Защищенность коммуникаций (линий и каналов телекоммуникаций) от несанкционированного доступа.

Kommunikatsiyalarning (telekommunikatsiyalar liniyalari va kanallarining) ruxsat etilmagan tarzda foydalanishdan muhofazalanganligi.

Коммуникацияларнинг (телекоммуникациялар линиялари ва каналларининг) рухсат этилмаган тарзда фойдаланишдан муҳофазаланганлиги.

Свойство компьютерных систем противостоять попыткам несанкционированного доступа к обрабатываемой и хранимой информации, вводу информации, приводящей к деструктивным действиям, и навязыванию ложной информации.

Б

Kompyuter tizimlarining, qayta ishlanadigan va saqlanadigan axborotdan ruxsat etilmagan tarzda foydalanish yoʻlidagi urinishlarga, buzgʻunchilik harakatlari olib keluvchi axborotning kiritilishiga hamda soxta axborot majburan kiritilishiga (qabul qilinishiga) qarshi tura olish xususiyati.

Компьютер тизимларининг, қайта ишланадиган ва сақланадиган ахборотдан рухсат этилмаган тарзда фойдаланиш йўлидаги уринишларга, бузгунчилик ҳаракатларига олиб келувчи ахборотнинг киритилишига ҳамда сохта ахборот мажбуран киритилишига (қабул қилинишига) қарши тура олиш хусусияти.

Безопасность

многоуровневая

uz - koʻp darajali xavfsizlik

кўп даражали хавфсизлик

en - multilevel security

Класс систем, содержащих информацию с различными уровнями критичности.

Kritiklik darajasi turlicha boʻlgan axborotni oʻz ichiga olgan tizimlar klassi.

Критиклик даражаси турлича бўлган ахборотни ўз ичига олган тизимлар класси.

Безопасность операционная

uz - operatsion xavfsizlik

операцион хавфсизлик

en - operational data security

Защищенность данных от модификации, разрушения или разглашения (случайных, неавторизованных, либо преднамеренных) во время выполнения операций ввода, обработки или вывода.

Kiritish, qayta ishlash yoki chiqarish operatsiyalarini bajarish vaqtida, maʼlumotlarning oʻzgartirishlardan, buzilishlardan yoki oshkor qilishlardan (tasodifiy, muallif tomonidan boʻlmagan yoki qasddan) muhofaza qilinganligi.

Киритиш, қайта ишлаш ёки чиқариш операцияларини бажариш вақтида, маълумотларнинг ўзгартиришлардан, бузилишлардан ёки ошкор қилишлардан (тасодифий, муаллиф томонидан бўлмаган ёки қасдан) муҳофаза қилинганлиги.

Безопасность программного обеспечения

uz - dasturiy taʼminot

xavfsizligi

дастурий таъминот

Свойство общецелевых (исполнительные программы, утилиты либо средства разработки программного обеспечения) и прикладных программ и средств осуществлять безопасную обработку данных в автоматизированной системе

Б

хавфсизлиги
en - software security

и безопасно использовать ресурсы системы.

Umummaqsadlardagi (bajaruvchi dasturlar, utilitalar yoki dasturiy ta'minotni ishlab chiqish vositalari) hamda amaliy dastur va vositalarning avtomatlashtirilgan tizimda ma'lumotlarning xavfsiz qayta ishlanishini va tizim resurslaridan xavfsiz foydalanishni amalga oshirish xususiyati.

Умуммақсадлардаги (бажарувчи дастурлар, утилиталар ёки дастурий таъминотни ишлаб чиқиш воситалари) ҳамда амалий дастур ва воситаларнинг автоматлаштирилган тизимда маълумотларнинг хавфсиз қайта ишланишини ва тизим ресурсларидан хавфсиз фойдаланишни амалга ошириш хусусияти.

Безопасность процедурная
uz - protseduralar bo'yicha
xavfsizlik

Соответствующие способы управления, используемые с целью обеспечения требуемого уровня безопасности для критичных к защите информации данных.

процедуралар бўйича
хавфсизлик
en - procedural security

Axborotning muhofaza qilinishiga kritik bo'lgan ma'lu-motlar uchun, talab qilinadigan xavfsizlik darajasini ta'minlash maqsadida foydalaniladigan tegishli boshqa-rish usullari.

**Безопасность реальной
открытой системы**
uz - real ochiq tizim
xavfsizligi
реал очик тизим
хавфсизлиги
en - real open system security

Axborotning muhofaza qilinishiga kritik bo'lgan ma'lumotlar uchun, talab qilinadigan xavfsizlik darajasini ta'minlash maqsadida foydalaniladigan tegishli boshqa-rish usullari.

Технологические и административные охранные меры, применяемые в реальной открытой системе для защиты оборудования, программного обеспечения и данных от случайных и преднамеренных модификации, раскрытия и разрушения.

Uskuna, dasturiy ta'minot va ma'lumotlarni, tasodifiy hamda ataylab qilinadigan o'zgartirishlardan, ochish va buzishdan muhofaza qilish uchun, real ochiq tizimda qo'llaniladigan texnologik va ma'muriy himoya chora-tadbirlari.

Ускуна, дастурий таъминот ва маълумотларни, тасодифий ҳамда атайлаб қилинадиган ўзгартиришлардан, очиш ва бузишдан муҳофаза қилиш учун, реал очик тизимда қўлланиладиган технологик ва маъмурий ҳимоя чора-тадбирлари.

Безопасность ресурса авто-

Безопасность ресурса автоматизированной сис-

Б

матизированной системы
uz - avtomatlashtirilgan tizim
resursining xavfsizligi

автоматлаштирилган
тизим ресурсининг
хавфсизлиги

en - automatized system
source security

темы складывается из обеспечения трех его характеристик: конфиденциальности, целостности и доступности.

Конфиденциальность компонента системы заключается в том, что он доступен только тем субъектам доступа (пользователям, программам, процессам), которым предоставлены на то соответствующие полномочия.

Целостность компонента предполагает, что он может быть модифицирован только субъектом, имеющим для этого соответствующие права. Целостность является гарантией корректности (неизменности, работоспособности) компонента в любой момент времени.

Доступность компонента означает, что имеющий соответствующие полномочия субъект может в любое время без особых проблем получить доступ к необходимому компоненту системы (ресурсу).

Avtomatlashtirilgan tizim resursining xavfsizligi uning uchta xarakteristikasini: konfidensialligini, yaxlitligini va foydalana olishlikni ta'minlashdan tashkil topadi.

Tizim komponentining konfidensialligi, unga faqat tegishli vakolati bo'lgan foydalana olish subyektlari (foydalanuvchilar, dasturlar, jarayonlar) kira olishi mumkinligida ifodalanadi.

Komponentning yaxlitligi, u faqat tegishli huquqlari bo'lgan subyekt tomonidagina o'zgartirilishi mumkinligini nazarda tutadi. Yaxlitlik komponentning istalgan vaqt onida to'g'riligi (o'zgarmasligi, ish qobiliyati)ning kafolati hisoblanadi.

Komponentdan foydalana olishlik tegishli vakolatga ega subyekt istalgan vaqtda, hech qanday muammosiz tizim (resurs)ning zarur komponentidan foydalanish uchun ruxsat olishi mumkinligini bildiradi.

Автоматлаштирилган тизим ресурсининг хавфсизлиги унинг учта характеристикасини: конфиденциаллигини, яхлитлигини ва фойдалана олишликни таъминлашдан ташкил топади.

Тизим компонентининг конфиденциаллиги, унга фақат тегишли ваколоти бўлган фойдалана олиш субъектлари (фойдаланувчилар, дастурлар, жара-

Б

ёнлар) кира олиши мумкинлигида ифодаланади. Компонентнинг яхлитлиги, у фақат тегишли хуқуқлари бўлган субъект томонидангина ўзгартирилиши мумкинлигини назарда тутаяди. Яхлитлик компонентнинг исталган вақт онда тўғрилиги (ўзгармаслиги, иш қобилияти)нинг қафолати ҳисобланади.

Компонентдан фойдалана олишлик тегишли ваколатга эга субъект исталган вақтда, ҳеч қандай муаммосиз тизим (ресурс)нинг зарур компонентдан фойдаланиш учун рухсат олиши мумкинлигини билдиради.

Безопасность сети

uz - tarmoq xavfsizligi

тармоқ хавфсизлиги

en - network security

Меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Безопасность информационной сети включает защиту оборудования, программного обеспечения, данных и персонала.

Axborot tarmog'ini ruxsat etilmagan tarzda foydalanishdan, normal ishlashga tasodifiy yoki qasddan bo'ladigan aralashuvlardan, uning komponentlarini buzishga urinishlardan saqlovchi chora-tadbirlar. Axborot tarmog'ining xavfsizligi uskuna, dasturiy ta'minot, ma'lumot va personalning muhofazasini o'z ichiga oladi.

Ахборот тармоғини рухсат этилмаган тарзда фойдаланишдан, нормал ишлашга тасодифий ёки қасддан бўладиган аралашувлардан, унинг компонентларини бузишга уринишлардан сақловчи чора-тадбирлар. Ахборот тармоғининг хавфсизлиги ускуна, дастурий таъминот, маълумот ва персоналнинг муҳофазасини ўз ичига олади.

Безопасность сети

телекоммуникаций

информационная

uz - telekommunikatsiyalar

tarmog'ining axborot

xavfsizligi

телекоммуникациялар

тармоғининг ахборот

Состояние защищенности сети телекоммуникаций от определенного (заданного) множества случайных и преднамеренных воздействий нарушителей (угроз безопасности) на объекты сети, циркулирующие в них данные и информацию управления сетью с целью ознакомления с ними, искажения, уничтожения или блокирования в процессе передачи для дезорганизации процес-

Б

хавфсизлиги

en - information security of telecommunications network

сов функционирования сети телекоммуникаций.

Telekommunikatsiyalar tarmog'ining, buzg'unchilarning tarmoq obyektlariga, ularda aylanadigan ma'lumotlarga va tarmoqni boshqarish axborotiga, ular bilan tanishish, buzib ko'rsatish, yo'q qilish maqsadida bo'ladigan muayyan (berilgan) ko'plab tasodifiy va ataylab qilinadigan ta'sirlaridan (xavfsizlikka tahdidlaridan) yoki uzatish jarayonida telekommunikatsiyalar tarmog'ining ishlash jarayonlarini izdan chiqarish uchun blokirovka qilishdan muhofaza qilinganlik holati.

Телекоммуникациялар тармоғининг, бузгунчиларнинг тармоқ объектларига, уларда айланадиган маълумотларга ва тармоқни бошқариш ахборотига, улар билан танишиш, бузиб кўрсатиш, йўқ қилиш мақсадида бўладиган муайян (берилган) кўплаб тасодифий ва атайлаб қилинадиган таъсирларидан (хавфсизликка таҳдидларидан) ёки узатиш жараёнида телекоммуникациялар тармоғининг ишлаш жараёнларини издан чиқариш учун блокировка қилишдан муҳофаза қилинганлик ҳолати.

Безопасность сети телекоммуникаций общего пользования информационная

uz - umumiy foydalanishdagi telekommunikatsiyalar tarmog'ining axborot xavfsizligi

умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги

en - public switched telecommunications network information security

Состояние (степень) защищенности информационных ресурсов сети телекоммуникаций общего пользования от угроз их информационной безопасности, приводящих к снижению заданного уровня качества служб или к ухудшению заданных качественных характеристик работы сети и, тем самым, к нанесению ущерба ее владельцам или пользователям.

Umumiy foydalanishdagi telekommunikatsiyalar tarmog'i axborot resurslarining, xizmat sifati darajasi-ning pasayishiga yoki tarmoq ishi sifat xarakteristikalarining yomonlashishiga olib keluvchi, shu bilan uning egasi yoki foydalanuvchilarga ziyon yetkazuvchi tahdidlardan muhofaza qilinganlik holati (darajasi).

Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот ресурсларининг, хизмат сифати даражасининг пасайишига ёки тармоқ иши сифат характеристикаларининг ёмонлашишига олиб ке-

Б

Безопасность сети телекоммуникаций технологическая

uz - telekommunikatsiyalar tarmog'ining texnologik xavfsizligi

телекоммуникациялар тармоғининг технологик хавфсизлиги

en - technological security of telecommunications network

Безопасность субъектов информационных отношений

uz - axborot munosabatlari subyektlarining xavfsizligi

ахборот муносабатлари субъектларининг хавфсизлиги

en - information relation subjects security

Безопасность физическая

uz - jismoniy xavfsizlik

жисмоний хавфсизлик
en - physical security

лувчи, шу билан унинг эгаси ёки фойдаланувчиларга зиён етказувчи таҳдидлардан муҳофаза қилинганлик ҳолати (даражаси).

Свойство аппаратно-программного обеспечения сети телекоммуникаций не имеет злоумышленных дефектов диверсионного типа, т.е. средств, способных по истечении определенного времени или по команде извне произвести действия, приводящие к нежелательным последствиям.

Telekommunikatsiyalar tarmog'i apparat-dasturiy ta'minotining, qo'poruvchilik turidagi jinoyatkorona nuqsonlarga, ya'ni ma'lum vaqt o'tgandan so'ng yoki komanda bo'yicha nomaqbul oqibatlarga olib keluvchi harakatni amalga oshirishga qodir vositalarga ega bo'lmaslik xususiyati.

Телекоммуникациялар тармоғи аппарат-дастурий таъминотининг, қўпорувчилик туридаги жинояткорона нуқсонларга, яъни маълум вақт ўтгандан сўнг ёки команда бўйича номақбул оқибатларга олиб келувчи ҳаракатни амалга оширишга қодир воситаларга эга бўлмаслик хусусияти.

Защищенность субъектов информационных отношений от нанесения им материального, морального или иного ущерба путем воздействия на информацию и/или средства ее обработки и передачи.

Axborot munosabatlari subyektlarining, ularga axborot va/yoki uni qayta ishlash va uzatish vositalariga ta'sir etish orqali moddiy, ma'naviy yoki boshqa zarar yetkazilishdan muhofaza qilinganligi.

Ахборот муносабатлари субъектларининг, уларга ахборот ва/ёки уни қайта ишлаш ва узатиш воситаларига таъсир этиш орқали моддий, маънавий ёки бошқа зарар етказилишдан муҳофаза қилинганлиги.

Реализация физических барьеров и контрольных процедур, как превентивная или контрмера против физических угроз (взлома, кражи, террористического акта, а также пожара, наводнения и

Б

т.д.) ресурсам системы и критичной информации.

Tizim resurslari va kritik axborotga jismoniy tahdidlar (buzish, o'g'irlash, terrorchilik akti, shuningdek, yong'in, suv toshqini va b.q.)ga qarshi ogohlantiruvchi yoki qarshi chora kabi jismoniy to'siqlar va nazorat protseduralarini amalga oshirish.

Тизим ресурслари ва критик ахборотга жисмоний таҳдидлар (бузиш, ўғирлаш, террорчилик акти, шунингдек, ёнғин, сув тошқини ва б.қ.)га қарши огоҳлантирувчи ёки қарши чора каби жисмоний тўсиқлар ва назорат процедураларини амалга ошириш.

Биометрия

uz - biometriya

биометрия

en - biometric

Наука об использовании для идентификации личности биологических свойств, например, отпечатков пальцев или голоса.

Shaxsni identifikatsiya qilish uchun biologik xususiyatlardan, masalan, barmoq izlari yoki ovozdan, foydalanish to'g'risidagi fan.

Шахсни идентификация қилиш учун биологик хусусиятлардан, масалан, бармоқ излари ёки овоздан, фойдаланиш тўғрисидаги фан.

Бит достоверности

uz - ishonchlilik biti

ишончлилиқ бити

en - validity bit

Разряд, добавляемый к слову в памяти ЭВМ для указания достоверности информации.

ЕНМ хотирасидаги so'zga axborotning ishonchliligini ko'rsatish uchun qo'shiladigan razryad.

ЭХМ хотирасидаги сўзга ахборотнинг ишончлилигини кўрсатиш учун қўшиладиган разряд.

Бит защиты

uz - muhofaza biti

муҳофаза бити

en - security bit

Двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи.

Xotira kalitidagi, tegishli хотира blokining yozishdan yoki tanlash va yozishdan muhofa qilinishini belgilovchi ikkilik razryad.

Хотира калитидаги, тегишли хотира блокнинг ёзишдан ёки танлаш ва ёзишдан муҳофа қилинишини белгилувчи иккилик разряд.

Бит контроля по четности

Контрольный бит, добавляемый к данным для

Б

uz - juftlik bo'yicha nazorat
biti
жуфтлик бўйича назорат
бити
en - parity check bit, parity bit

контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данные, включая и единицу контрольного бита, всегда была четной или нечетной.

Ma'lumotlarga, ularning ishonchliligini nazorat qilish uchun ma'lumotlarni tashkil etuvchi ikkilik birliklarning yig'indisi, jumladan, nazorat biti birligi, har doim juft yoki toq bo'ladigan tarzda qo'shiladigan nazorat biti.

Маълумотларга, уларнинг ишончилигини назорат қилиш учун маълумотларни ташкил этувчи иккилик бирликларнинг йиғиндиси, жумладан, назорат бити бирлиги, ҳар доим жуфт ёки тоқ бўладиган тарзда қўшиладиган назорат бити.

Бит маски
uz - niqob biti
ниқоб бити
en - mask bit

Сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения или запрета определенных операций либо для проверки или изменения содержимого поля.

Muayyan operatsiyalarga ruxsat etish yoki ularni taqiqlash yoki maydon ichidagini tekshirish yo bo'lmasa o'zgartirish uchun, nol yoki birlik qiymatga o'rnatiladigan bitlar yig'indisi.

Муайян операцияларга рухсат этиш ёки уларни тақиқлаш ёки майдон ичидагини текшириш ё бўлмаса ўзгартириш учун, ноль ёки бирлик қийматга ўрнатиладиган битлар йиғиндиси.

Блок
uz - blok
блок
en - block

1 Совокупность данных, которые вводятся или выводятся одновременно.

2 Последовательность битов, имеющая фиксированную длину.

1 Bir vaqtda kiritiladigan yoki chiqariladigan ma'lumotlar jami.

2 Belgilangan uzunlikka ega bo'lgan bitlar ketma-ketligi.

1 Бир вақтда киритиладиган ёки чиқариладиган маълумотлар жами.

Б

2 Белгиланган узунликка эга бўлган битлар кетма-кетлиги.

Блокирование

uz - blokirovkalash

блокировкалаш

en - blocking

Использование специальных методов защиты данных или программного обеспечения от несанкционированного копирования.

Ruxsat etilmagan tarzda nusxa ko‘chirishga qarshi, ma’lumotlar yoki dasturiy ta’minotni muhofaza qilishning maxsus metodlarini qo‘llash.

Рухсат этилмаган тарзда нусха кўчиришга қарши, маълумотлар ёки дастурий таъминотни муҳофаза қилишнинг махсус методларини қўллаш.

Блокирование доступа (к информации)

uz - foydalana olishni

blokirovkalash (axborotdan)

фойдалана олишни

блокировкалаш (ахборотдан)

en - block access

(to information)

1 Прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей).

2 Создание условий, препятствующих доступу к информации субъекту, имеющему право на него.

Примечание – Создание условий, препятствующих доступу к информации, может быть осуществлено по времени доступа, функциям по обработке информации (видам доступа) и/или доступным информационным ресурсам.

1 Axborotdan foydalanish huquqiga ega bo‘lgan shaxslar (qonuniy foydalanuvchilar)ning undan foydalanishini to‘xtatish yoki qiyinlashtirish.

2 Axborotdan foydalanish huquqiga ega bo‘lgan subyektning axborotdan foydalanishida to‘sqinlik qiladigan sharoitlar yaratish.

Izoh – Axborotdan foydalanishda to‘sqinlik qiladigan sharoitlar yaratish, foydalana olish vaqti bo‘yicha qayta ishlash funksiyalari (foydalana olish turlari) bo‘yicha va/yoki foydalanish mumkin bo‘lgan axborot resurslari bo‘yicha amalga oshirilishi mumkin.

1 Ахборотдан фойдаланиш ҳуқуқига эга бўлган шахслар (қонуний фойдаланувчилар)нинг ундан фойдаланишини тўхтатиш ёки қийинлаштириш.

2 Ахборотдан фойдаланиш ҳуқуқига эга бўлган субъектнинг ахборотдан фойдаланишида тўсқинлик қиладиган шароитлар яратиш.

Изох – Ахборотдан фойдаланишда тўсқинлик қиладиган

Б

шароитлар яратиш, фойдалана олиш вақти бўйича қайта ишлаш функциялари (фойдалана олиш турлари) бўйича ва/ёки фойдаланиш мумкин бўлган ахборот ресурслари бўйича амалга оширилиши мумкин.

Блокирование информации

uz - axborotni blokirovkalash

ахборотни блокировкалаш

en - information blocking

1 Утрата информацией при ее обработке техническими средствами свойства доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней для проведения санкционированных операций по ознакомлению, документированию, модификации или уничтожению.

2 Искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

1 Texnik vositalar bilan qayta ishlashda axborotdagi undan foydalana olish xususiyatining yo'qolishi: tanishish, hujjatlashtirish, o'zgartirish yoki yo'q qilish bo'yicha ruxsat etilgan operatsiyalarni o'tkazish uchun, axborotdan ruxsat etilgan tarzda foydalanishning qiyinlashuvida yoki to'xtatilishida ifodalanadi.

2 Axborotni yo'qotish bilan bog'liq bo'lmagan holda, foydalanuvchilarning axborotdan foydalana olishlarini sun'iy ravishda qiyinlashtirish.

1 Техник воситалар билан қайта ишлашда ахборотдаги ундан фойдалана олиш хусусиятининг йўқолиши: танишиш, хужжатлаштириш, ўзгартириш ёки йўқ қилиш бўйича рухсат этилган операцияларни ўтказиш учун, ахборотдан рухсат этилган tarzda фойдаланишнинг қийинлашувида ёки тўхтатилишида ифодаланadi.

2 Ахборотни йўқотиш билан боғлиқ бўлмаган холда, фойдаланувчиларнинг ахборотдан фойдалана олишларини сунъий равишда қийинлаштириш.

Блокирование логическое

uz - mantiqiy blokirovkalash

мантикий блокировкалаш

en - logical blocking

Блокирование, выполняемое в базах данных на логическом уровне.

Ma'lumotlar bazalarida mantiqiy darajada bajariladigan blokirovkalash.

Маълумотлар базаларида мантикий даражада bajariladigan блокировкалаш.

Б

Блокирование передачи информации (данных)

uz - axborot (ma'lumotlar) uzatilishini blokirovkalash

ахборот (маълумотлар)

узатилишини блокировкаш

en - data transmission blocking

Одно из нарушений из области безопасности информации, выражающееся в прекращении передачи или задержке информации на время, за которое она потеряет ценность для пользователя.

Axborot uzatilishini to'xtatishda yoki vaqtincha ushlab turishda ifodalanadigan, (bu vaqtda u foydalanuvchi uchun o'z qimmatini yo'qotadi) axborot xavfsizligi sohasidagi buzilishlardan biri.

Ахборот узатилишини тўхтатишда ёки вақтинча ушлаб туришда ифодаланадиган, (бу вақтда у фойдаланувчи учун ўз қимматини йўқотади) ахборот хавфсизлиги соҳасидаги бузилишлардан бири.

Блокирование физическое

uz - fizik blokirovkalash

физик блокировкаш

en - physical blocking

Блокирование, выполняемое в базах данных на физическом уровне.

Ma'lumotlar bazalarida fizik darajada bajariladigan blokirovkalash.

Маълумотлар базаларида физик даражада bajariladigan блокировкаш.

Блокировка

uz - blokirovka

блокировка

en - lock, locking

Код, структура данных или программа для управления доступом к данным.

Ma'lumotlardan foydalana olishni boshqarish uchun mo'ljallangan kod, ma'lumotlar strukturasi yoki dastur.

Маълумотлардан фойдалана олишни бошқариш учун мўлжалланган код, маълумотлар структураси ёки дастур.

Блокировка данных

uz - ma'lumotlarni blokirovkalash

маълумотларни

блокировкаш

en - data interlock

Защита файла или его части (блока записи) путем запрещения доступа к ним всех пользователей, за исключением одного.

Bitta foydalanuvchidan tashqari, barcha foydalanuvchilarga kirishni taqiqlash yo'li bilan fayl yoki uning bir qismini (yozuv blokini) muhofaza qilish.

Битта фойдаланувчидан ташқари, барча фойдаланувчиларга киришни тақиқлаш йўли билан файл ёки унинг бир қисмини (ёзув блокини) муҳофаза қилиш.

Б

Блокировка доступа к памяти

uz - хотирага kira olishni blokirovkalash

хотирага кира олишни
блокировкалаш
en - memory lockout

Блокировка записи в память

uz - хотирага yozishni blokirovkalash

хотирага ёзишни
блокировкалаш
en - memory write lockout

Блокировка клавиатуры

uz - klaviaturani blokirovkalash

клавиатурани
блокировкалаш
en - keyboard lockout

Запрещение доступа к ограниченному участку памяти, например, дорожке диска, вследствие обнаруженных на этом участке дефектов. Выполняется программными или аппаратными средствами.

Xotiraning cheklangan uchastkasiga, masalan, disk yoʻlkasiga, bu uchastkada aniqlangan nuqsonlar oqibatida kira olishning taqiqlanishi. Dasturiy yoki apparat vositalar tomonidan bajariladi.

Xotiraning cheklangan uchastkasiga, masalan, disk yoʻlkasiga, bu uchastkada aniqlangan nuqsonlar oqibatida kira olishning taqiqlanishi. Dasturiy yoki apparat vositalar tomonidan bajariladi.

Ситуация при обмене данными, характеризующаяся тем, что запись, читаемая с внешнего носителя, в основную память не переводится.

Maʼlumotlar almashinishda vujudga keladigan vaziyat. Tashqi eltuvchidan oʻqiladigan yozuv asosiy хотирага koʻchirilmasligi bilan tavsiflanadi.

Maʼlumotlar almashinishda vujudga keladigan vaziyat. Tashqi eltuvchidan oʻqiladigan yozuv asosiy хотирага koʻchirilmasligi bilan tavsiflanadi.

1 Запрет на ввод данных в ЭВМ с клавиатуры терминала. Выполняется операционной системой.

2 Игнорирование всех поступающих с клавиатуры сигналов и/или невозможность физического нажатия клавиш.

1 Maʼlumotlarning terminal klaviaturasidan elektron hisoblash mashinasiga kiritilishini taqiqlash. Operatsion tizim tomonidan bajariladi.

2 Klaviaturadan kelayotgan barcha signallarning rad etilishi va/yoki klavishlarni jismoniy bosishning mumkin boʻlmasligi.

1 Maʼlumotlarning terminal klaviaturasidan elektron hisoblash mashinasiga kiritilishini taqiqlash. Operatsion tizim tomonidan bajariladi.

Б

лади.

2 Клавиатурадан келаётган барча сигналларнинг рад этилиши ва/ёки клавишларни жисмоний бошишнинг мумкин бўлмаслиги.

Блокировка локальная

uz - lokal blokirovkalash

локал блокировкалаш

en - local lock

Блокировка с целью защиты ресурсов, приписанных к области, адресуемой отдельным пользователем.

Ayrim foydalanuvchi tomonidan yoʻllanayotgan sohaga tegishli resurslarni muhofaza qilish maqsadida blokirovkalash.

Айрим фойдаланувчи томонидан йўлланаётган соҳага тегишли ресурсларни муҳофаза қилиш мақсадида блокировкалаш.

Блокировка учетной записи

uz - hisobga oid yozuvni

blokirovkalash

хисобга оид ёзувни

блокировкалаш

en - account lockout

Средство защиты пароля пользователя от подбора.

Foydalanuvchining parolini saralashdan muhofaza qilish vositasi.

Фойдаланувчининг паролени саралашдан муҳофаза қилиш воситаси.

Блокнот одноразовый

uz - bir martali bloknot

бир мартали блокнот

en - single-use pad

Криптосистема, также называемая шифром Вернама, использует строку бит, которая генерируется абсолютно случайно. Длина ключевого потока равна длине открытого текста и открытый текст и строка случайных бит комбинируются для выработки шифротекста, используя операцию XOR. Такой алгоритм обладает совершенной секретностью.

Vernam shifri deb ham ataladigan kriptotizim, mutlaqo tasodifan generatsiyalanadigan bit satridan foydalanadi. Kalit oqim uzunligi ochiq matn uzunligiga teng. Tasodifiy bitlar satri va ochiq matn XOR operatsiyasidan foydalanib, shifrmatnni ishlab chiqish uchun kombinatsiyalanadi. Bunday algoritm mutlaqo maxfiy hisoblanadi.

Вернам шифри деб ҳам аталадиган криптотизим, мутлақо тасодифан генерацияланадиган бит сат-

Б

ридан фойдаланади. Калит оким узунлиги очик матн узунлигига тенг. Тасодифий битлар сатри ва очик матн XOR операциясидан фойдаланиб, шифрматни ишлаб чиқиш учун комбинацияланади. Бундай алгоритм мутлақо махфий ҳисобланади.

Бомба временная

uz - vaqt bombasi

вақт бомбаси

en - time bomb

Логическая бомба, которая может быть активирована в определенное время.

Muayyan vaqtda aktivlashtirilishi mumkin bo'lgan mantiqiy bomba.

Муайян вақтда активлаштирилиши мумкин бўлган мантикий бомба.

Бомба логическая

uz - mantiqiy bomba

мантикий бомба

en - logic bomb

1 Вредоносная программа, запуск которой происходит при некотором определенном состоянии системы обработки данных и вызывает повреждение этой системы.

2 Компьютерная программа или фрагмент программы, приводящая к повреждению ресурсов автоматизированной системы (данных, программного или аппаратного обеспечения) и срабатывающая при выполнении некоторого условия.

3 Программа ЭВМ, выполняемая периодически или в определенный момент времени с целью искажения, уничтожения или модификации данных.

1 Ma'lumotlarni qayta ishlash tizimining muayyan bir holatida ishga tushadigan va tizimni ishdan chiqishiga olib keluvchi zararli dastur.

2 Avtomatlashtirilgan tizim resurslarining (ma'lumotlar, dasturiy yoki apparat ta'minot) shikastlanishiga olib keluvchi va ayrim shartlar bajarilganda ishga tushadigan kompyuter dasturi yoki dastur fragmenti.

3 Ma'lumotlarni buzish, yo'q qilish yoki o'zgartirish maqsadida, davriy ravishda yoki muayyan vaqtda bajariladigan EHM dasturi.

1 Маълумотларни қайта ишлаш тизимининг муайян бир ҳолатида ишга тушадиган ва тизимни ишдан чиқишига олиб келувчи зарарли дастур.

Б

2 Автоматлаштирилган тизим ресурсларининг (маълумотлар, дастурий ёки аппарат таъминот) шикастланишига олиб келувчи ва айрим шартлар бажарилганда ишга тушадиган компьютер дастури ёки дастур фрагменти.

3 Маълумотларни бузиш, йўқ қилиш ёки ўзгартириш мақсадида, даврий равишда ёки муайян вақтда бажариладиган ЭХМ дастури.

Бомба почтовая

uz - pochta bombasi

почта бомбаси

en - mail bomb

Блокирование сайта путем вывода из строя почтового сервера посылкой огромного числа писем. Используется для предотвращения получения сайтом писем в ходе атаки или для мести.

Saytni, pochta serverini ko'p sonli xatlarni yuborish orqali posilkasi bilan ishdan chiqarish yo'li bilan blokirovkalash. Sayt orqali hujum chog'ida xatlar olinishini bartaraf qilish yoki o'ch olish maqsadida ishlatiladi.

Сайтни, почта серверини кўп сонли хатларни юбориш орқали посилкаси билан ишдан чиқариш йўли билан блокировкалаш. Сайт орқали хужум чоғида хатлар олинисини бартараф қилиш ёки ўч олиш мақсадида ишлатилади.

Бомба программная

uz - dasturiy bomba

дастурий бомба

en - program bomb

Тайное встраивание в программу команд, которые должны срабатывать один или несколько раз при определенных условиях.

Примечание – Вариантами программной бомбы являются логическая и временная бомбы.

Muayyan sharoitlarda bir yoki bir necha marta ishga tushishi zarur bo'lgan komandalarni dasturga yashirin o'rnatish.

Izoh – Mantiqiy va vaqt bombalari dasturiy bombaning variantlari hisoblanadi.

Муайян шароитларда бир ёки бир неча марта ишга тушиши зарур бўлган командаларни дастурга яширин ўрнатиш.

Изоҳ – Мантикий ва вақт бомбалари дастурий бомбанинг вариантлари ҳисобланади.

Бот

uz - bot

бот

Специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и

Б

en - bot

обычный пользователь.

Примечание – Обычно используется для координации сетевых атак на компьютеры – рассылки спама, хищения персональных данных пользователей, перебора паролей на удаленной системе, атак «отказ в обслуживании» и т.п.

Avtomatik ravishda va/yoki belgilangan jadval bo'yicha oddiy foydalanuvchi kabi va interfeyslar orqali biror-bir harakatni bajaradigan maxsus dastur. Izoh – Odatda, kompyuterlarga bo'ladigan tarmoq hujumlari – spamni yuborish, foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash, olisda tizim parollarini tanlash, «xizmat ko'rsatishni rad etish» hujumlarini muvofiqlashtirish uchun va boshqalarda ishlatiladi.

Автоматик равишда ва/ёки белгиланган жадвал бўйича оддий фойдаланувчи каби ва интерфейс-лар орқали бирор-бир ҳаракатни бажарадиган махсус дастур.

Изоҳ – Одатда, компьютерларга бўладиган тармоқ хужумлари – спамни юбориш, фойдаланувчиларнинг шахсий маълумотларини ўғирлаш, олисда тизим паролларини танлаш, «хизмат кўрсатишни рад этиш» хужумларини мувофиқлаштириш учун ва бошқаларда ишлатилади.

Бот-сеть (ботнет)

uz - bot-tarmoq (botnet)

бот-тармоқ (ботнет)

en - bot-net

Компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами.

Ishga tushirilgan botlari bo'lgan bir qancha xostlardan iborat kompyuter tarmog'i.

Ишга туширилган ботлари бўлган бир қанча хостлардан иборат компьютер тармоғи.

Брешь, лазейка

uz - teshik, tuynuk

тешик, туйнук

en - flaw, loophole

Ошибка при назначении полномочий, упущение при разработке, которые позволяют обойти или вывести из строя механизмы защиты.

Vakolatlarni belgilashdagi, ishlab chiqishdagi xato. Muhofaza mexanizmlarini chetlab o'tish yoki ularni ishdan chiqarish imkonini beradi.

Ваколатларни белгилашдаги, ишлаб чиқишдаги хато. Муҳофаза механизmlарини четлаб ўтиш ёки уларни ишдан чиқариш имконини беради.

В

В

Вакцинирование

uz - vaksinalash

вакциналаш

en - inoculate

Запуск резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса для определения (выявления) заражения, то есть «обманывающих» вирус.

Berilgan (ma'lum bir) virus turi tomonidan zararlanishni aniqlash (topish) uchun foydalaniladigan shart-sharoitlarni imitatsiyalovchi, ya'ni virusni «aldaydigan» rezident vaksina dasturlarni ishga tushirish.

Берилган (маълум бир) вирус тури томонидан зарарланишни аниқлаш (топиш) учун фойдаланиладиган шарт-шароитларни имитацияловчи, яъни вирусни «алдайдиган» резидент вакцина дастурларни ишга тушириш.

Валидация (утверждение)

uz - validatlash (tasdiqlash)

валидатлаш (тасдиқлаш)

en - validation (statement)

Подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного предполагаемого использования или применения, выполнены. Примечания

1 Термин «утверждено» используется для обозначения соответствующего статуса.

2 Условия применения могут быть реальными или смоделированными.

Aniq maqsadlarda foydalanish yoki qo'llash uchun mo'ljallangan talablarning bajarilganligini obyektiv dalillar keltirish yo'li bilan tasdiqlash.

Izohlar

1 «Tasdiqlangan» atamasi tegishli maqomni belgilash uchun ishlatiladi.

2 Qo'llash shartlari real yoki modellashtirilgan bo'lishi mumkin.

Аниқ мақсадларда фойдаланиш ёки қўллаш учун мўлжалланган талабларнинг бажарилганлигини объектив далиллар келтириш йўли билан тасдиқлаш.

Изоҳлар

1 «Тасдиқланган» атамаси тегишли мақомни белгилаш учун ишлатилади.

2 Қўллаш шартлари реал ёки моделлаштирилган бўлиши мумкин.

В

Ведение контроля

uz - nazorat olib borish

назорат олиб бориш

en - auditing

Отслеживание действий пользователей и запись операционной системой в контрольном журнале (*security log*) специальных типов событий, таких, как регистрация в системе, доступ к файлу и т.п.

Foydalanuvchilarning harakatlarini kuzatib borish va operatsion tizim tomonidan nazorat jurnalida (*security log*) tizimda qayd etish, faylga kirish va sh.k. hodisalar maxsus turlarining yozib borilishi.

Фойдаланувчиларнинг ҳаракатларини кузатиб бориш ва операцион тизим томонидан назорат журналида (*security log*) тизимда қайд этиш, файлга кириш ва ш.к. ходисалар махсус турларининг ёзиб борилиши.

Вектор

аутентификационный

uz - autentifikatsion vektor

аутентификацион вектор

en - authentication vector

Совокупность параметров, используемых при аутентификации мобильной станции, например триплет в GSM и квинтет в UMTS.

Mobil stansiyanı autentifikatsiya qilishda qoʻllaniladigan parametrlarning jami, masalan GSM da triplet va UMTS da kvintet.

Мобил станцияни аутентификация қилишда қўлланиладиган параметрларнинг жами, масалан GSM да триплет ва UMTS да квинтет.

Вектор инициализации

uz - initsializatsiya vektori

инициализация вектори

en - initialization vector

Случайное число, которое используется для инициализации процесса шифрования (не является секретным элементом).

Shifrlash jarayonini initsializatsiyalash uchun qoʻllaniladigan tasodifiy son (maxfiy element hisoblanmaydi).

Шифрлаш жараёнини инициализациялаш учун қўлланиладиган тасодифий сон (махфий элемент ҳисобланмайди).

Величина контрольная криптографическая

uz - kriptografik nazorat kattaligi

криптографик назорат

катталиги

en - cryptographic check value

Информация, получаемая в результате криптографического преобразования блока данных.

Ma'lumotlar blokini kriptografik o'zgartirish natijasida olinadigan axborot.

Маълумотлар блокинни криптографик ўзгартириш натижасида олинадиган ахборот.

В

Верификатор

uz - verifikator

верификатор

en - verifier

Объект, требующий аутентифицированной идентификации, или представляющий его. Верификатор включает в себя функции, необходимые для осуществления обменов в целях аутентификации.

Autentifikatsiyalangan identifikatsiya qilish talab qilinadigan yoki uni ko'rsatadigan obyekt. Verifikator autentifikatsiya maqsadlarida almashinuvlarni amalga oshirish uchun zarur bo'lgan funksiyalarni o'z ichiga oladi.

Аутентификацияланган идентификация қилиш талаб қилинадиган ёки уни кўрсатадиган объект. Верификатор аутентификация мақсадларида алмашинувларни амалга ошириш учун зарур бўлган функцияларни ўз ичига олади.

Верификатор

автоматический

uz - avtomatik verifikator

автоматик верификатор

en - mechanical verifier

Схема обеспечения автоматического доказательства правильности программ. Включает генератор условий верификаций и блок доказательства теорем.

Dasturlarning to'g'riligi avtomatik isbotlanishini ta'minlash sxemasi. Verifikatsiyalar shartlari generatori hamda teoremlarni isbotlash blokini ichiga oladi.

Дастурларнинг тўғрилиги автоматик исботланишини таъминлаш схемаси. Верификациялар шартлари генератори ҳамда теоремаларни исботлаш блокини ичига олади.

Верификатор байт-кода

uz - bayt-kod verifikatori

байт-код верификатори

en - byte code verifier

Один из механизмов защиты модели безопасности технологии Java. Позволяет контролировать соответствие байт-кода Java спецификациям Java, приведение типов, переполнение стека и т.д.

Java texnologiyasi xavfsizlik modelini muhofaza qilish mexanizmlaridan biri. Java bayt-kodining Java spetsifikatsiyalariga muvofiqligini, turlar keltirilishini, stek to'ldirilishini va h.k. nazorat qilish imkonini beradi.

Java texnologiyasi xavfsizlik modelini muhofaza qilish mexanizmlaridan biri. Java bayt-kodining Java spetsifikatsiyalariga muvofiqligini, turlar keltirilishini, stek to'ldirilishini va h.k. nazorat qilish imkonini beradi.

В

Верификатор условий

uz - shartlar verifikatori

шартлар верификатори

en - assertion checker

Программа, анализирующая текст другой программы, снабженной условиями и операторами контроля, которые должны выполняться в определенных ее точках, и доказывающая их истинность или ложность при заданных предусловиях.

Dasturning muayyan nuqtalarida bajarilishi kerak boʻlgan nazorat shartlari va operatorlari bilan taʼminlangan boshqa dasturning matnini tahlil qiluvchi hamda berilgan sharoitlarda dasturlarning haqiqiyligini isbotlovchi dastur.

Дастурнинг муайян нуқталарида бажарилиши керак бўлган назорат шартлари ва операторлари билан таъминланган бошқа дастурнинг матнини таҳлил қилувчи ҳамда берилган шароитларда дастурларнинг ҳақиқийлигини исботловчи дастур.

Верификация (проверка)

uz - verifikatlash

(tekshirish)

верификатлаш

(текшириш)

en - verification (check)

Подтверждение посредством представления объективных свидетельств того, что установленные требования были выполнены.

Примечания

1 Термин «верифицировано» используется для обозначения соответствующего статуса.

2 Деятельность по подтверждению может включать такую деятельность, как:

- осуществление альтернативных расчетов;
- сравнение нормативно-технической документации по новому проекту с аналогичной документацией по апробированному проекту;
- проведение испытаний и демонстраций;
- анализ документов до их выпуска.

Belgilangan talablarning bajarilganligini obyektiv dalillar keltirish yoʻli bilan tasdiqlash.

Izohlar

1 «Verifikatlangan» atamasi tegishli maqomni belgilash uchun foydalaniladi.

2 Tasdiqlash boʻyicha faoliyat quyidagi faoliyatlarni oʻz ichiga olishi mumkin:

- alternativ hisoblashlarni amalga oshirish;
- yangi loyiha boʻyicha tuzilgan ilmiy-texnik hujjatlarni sinab koʻrilgan loyihaga tuzilgan oʻxshash hujjatlar bilan taqqoslash;
- sinovlar va koʻrsatishlar oʻtkazish;
- hujjatlarni chiqarishdan oldin tahlil etish.

Белгиланган талабларнинг бажарилганлигини

В

объектив далиллар келтириш йўли билан тасдиқлаш.

Изоҳлар

1 «Верификатланган» атамаси тегишли мақомни белгилаш учун фойдаланилади.

2 Тасдиқлаш бўйича фаолият қуйидаги фаолиятларни ўз ичига олиши мумкин:

- альтернатив ҳисоблашларни амалга ошириш;
- янги лойиҳа бўйича тузилган илмий-техник ҳужжатларни синаб кўрилган лойиҳага тузилган ўхшаш ҳужжатлар билан таққослаш;
- синовлар ва кўрсатишлар ўтказиш;
- ҳужжатларни чиқаришдан олдин таҳлил этиш.

Верифицировать

uz - verifikatsiyalamoq

верификацияламоқ

en - verify

Выполнять строгую детальную проверку с независимым определением ее достаточности.

Примечание – См. также термин «подтверждение». Термин «верифицировать» имеет более глубокий смысл. Он используется в контексте действий оценщика, когда от оценщика требуются независимые усилия.

Yetarliligini mustaqil aniqlash bilan qat'iy batafsil tekshirishni bajarmoq.

Izoh – Shuningdek, «tasdiqlamoq» atamasiga qarang. «Verifikatsiyalash» atamasi chuqur ma'noga ega. Bu atama baholovchidan mustaqil harakatlar talab qilinayotganda, baholovchining harakatlar kontekstida ishlatiladi.

Etarliiligini mustaqil aniqlash bilan qat'iy batafsil tekshirishni bajarmoq.

Izoh – Shuningdek, «tasdiqlamoq» atamasiga qarang. «Verifikatsiyalash» atamasi chuqur ma'noga ega. Bu atama baholovchidan mustaqil harakatlar talab qilinayotganda, baholovchining harakatlar kontekstida ishlatiladi.

Верификация и утверждение

uz - verifikatsiya va tasdiqlash

верификация ва

тасдиқлаш

en - verification and validation, V&V

Полный набор проверок, которым подвергается система для получения гарантий ее соответствия своему назначению.

Примечание – В число таких проверок могут входить жесткий набор функциональных тестов, контроль пропускной способности, проверка надежности и т.д.

Tekshirishlarning to'la to'plami bo'lib, tizimning o'zi mo'ljallangan maqsadlarga muvofiqligini kafolatlash uchun kerak.

Izoh – Funksional testlarni qat'iy tanlash, o'tkazish, qobiliyatini nazorat qilish, ishonchlilikni tekshirish va h.k.

В

shunday tekshirishlar qatoriga kiradi.

Текширишларнинг тўла тўплами бўлиб, тизимнинг ўзи мўлжалланган мақсадларга мувофиқлигини кафолатлаш учун керак.

Изоҳ – Функционал тестларни қатъий танлаш, ўтказиш, қобилиятини назорат қилиш, ишончилиқни текшириш ва ҳ.к. шундай текширишлар қаторига киради.

Вероятность

uz - ehtimollik

ЭҲТИМОЛЛИК

en - likelihood

Характеристика возможности и частоты появления события.

Voqea-hodisaning paydo bo'lish imkoniyati va takrorlanish xarakteristikasi.

Воқеа-ҳодисанинг пайдо бўлиш имконияти ва такрорланиш харақтеристикаси.

Взаимодействие

uz - birgalikda ishlash

биргалиқда ишлаш

en - interaction

Общая деятельность, основанная на коммуникации между логическими объектами.

Mantiqiy obyektlar o'rtasidagi kommunikatsiyaga asoslangan umumiy faoliyat.

Мантикий объектлар ўртасидаги коммуникацияга асосланган умумий фаолият.

Взлом

uz - buzish

бузиш

en - hacking

Перехват начала сеанса связи, как правило, с целью осуществления активной атаки в момент, когда работающий в сети пользователь завершит аутентификацию. В этот момент злоумышленник пытается внедриться в систему как законный пользователь, что позволяет ему контролировать соединение между двумя станциями.

Tarmoqda ishlovchi foydalanuvchi autentifikatsiyani tugatganda, odatda, aktiv hujumni amalga oshirish maqsadida, aloqa seansining boshlanishini tutib olish. Bu vaqtda jinoyatkor tizimga qonuniy foydalanuvchi sifatida kirishga harakat qiladi, bu unga ikkita stansiya o'rtasidagi ulanishni nazorat qilish imkonini beradi.

Тармоқда ишловчи фойдаланувчи аутентификацияни тугатганда, одатда, актив ҳужумни амалга

В

ошириш мақсадида, алоқа сеансининг бошланишини тутиб олиш. Бу вақтда жинояткор тизимга қонуний фойдаланувчи сифатида киришга ҳаракат қилади, бу унга иккита станция ўртасидаги уланишни назорат қилиш имконини беради.

Взлом, вскрытие

криптосистемы

uz - kriptotizimni buzish, ochish

криптотизимни бузиш, очиш

en - cryptosystem

discrimination, hacking

Создание процедуры, позволяющей вызывать отклонения информационного процесса, защищенного криптосистемой, от условий его нормально (штатного) протекания.

Kriptotizim bilan muhofaza qilingan axborot jarayonining uning normal (shtat) kechish sharoitlaridan og‘ishini keltirib chiqarish imkonini beradigan protsedurani yuzaga keltirish.

Криптотизим билан муҳофаза қилинган ахборот жараёнининг унинг нормал (штат) кечиш шароитларидан оғишини келтириб чиқариш имконини берадиган процедурани юзага келтириш.

Взлом компьютерный

uz - kompyuter vositasida buzish

компьютер воситасида бузиш

en - cracking

Несанкционированное проникновение в компьютерную сеть или в чужой компьютер с целью, например, извлечения выгоды, использования чужих данных, удовлетворения личного любопытства.

Manfaat ko‘rish, begonalarning ma’lumotlaridan foydalanish, shaxsiy qiziqishni qanoatlantirish va boshqa maqsadda kompyuter tarmog‘iga yoki begona shaxs kompyuteriga ruxsat etilmagan tarzda kirish.

Манфаат кўриш, бегоналарнинг маълумотларидан фойдаланиш, шахсий қизиқишни қаноатлантириш ва бошқа мақсадда компьютер тармоғига ёки бегона шахс компьютерига рұхсат этилмаган тарзда кириш.

Взломщик

uz - buzuvchi

бузувчи

en - hacker

Лицо, предпринимающее попытку несанкционированного проникновения в защищенную систему.

Muhofazalangan tizimga ruxsat etilmagan tarzda kirishga urinuvchi shaxs.

В

Муҳофазаланган тизимга рухсат этилмаган тарзда киришга уринувчи шахс.

Взрыв

uz - portlash
портлаш
en - blowup

В вычислительных системах – аварийный останов с выдачей сообщения об ошибке, блокирующий дальнейшее выполнение программы.

Hisoblash tizimlarida – xato to‘g‘risida xabar berish bilan, dasturning keyinchalik bajarilishiga to‘sqinlik qiladigan avariyaviy to‘xtash.

Ҳисоблаш тизимларида – хато тўғрисида хабар бериш билан, дастурнинг кейинчалик бажарилишига тўсқинлик қиладиган авариявий тўхташ.

Взрыв комбинированный

uz - kombinatsiyalangan
portlash
комбинацияланган
портлаш
en - combined blowup

В интеллектуальных системах ситуация, когда размер пространства решений увеличивается чрезвычайно быстро с ростом числа элементарных решений. По этой причине метод перебора для поиска решения становится неприемлемым: необходимо использовать эвристические правила. Intellektual tizimlardagi, qarorlarning fazoviy hajmi elementar qarorlarning soni o‘shishi bilan favqulodda tez ko‘payadigan vaziyat. Shu sababga ko‘ra, yechim izlash uchun ajratish usuli to‘g‘ri kelmaydi: evristik qoidalardan foydalanish zarur.

Интеллектуал тизимлардаги, қарорларнинг фазовий ҳажми элементар қарорларнинг сони ўсиши билан фавқулодда тез кўпаядиган вазият. Шу сабабга кўра, ечим излаш учун ажратиш усули тўғри келмайди: эвристик қоидалардан фойдаланиш зарур.

Вид активной атаки

uz - aktiv hujum turi
актив ҳужум тури
en - active attack type

Внедрение злоумышленника между двумя системами для перехвата сообщений и подмены их собственными.

Ikki tizim o‘rtasida, xabarlarni tutib olish va ularni shaxsiy xabarlar bilan almashtirish maqsadida, jinoyatkorni kiritish.

Икки тизим ўртасида, хабарларни тутиб олиш ва уларни шахсий хабарлар билан алмаштириш мақсадида, жинояткорни киритиш.

В

Вид доступа

uz - foydalanish turi

фойдаланиш тури

en - access type

Вид операций, указанной в праве на доступ.

Примечание – В праве на доступ могут быть указаны следующие операции: чтение, запись, выполнение, дополнение, модификация, удаление, создание.

Foydalanish huquqida ko'rsatilgan amallar turi.

Izoh – Foydalanish huquqida quyidagi operatsiyalar ko'rsatishi mumkin: o'qish, yozish, bajarish, to'ldirish, modifikatsiya qilish, o'chirish, yaratish.

Фойдаланиш ҳуқуқида кўрсатилган амаллар тури.

Изоҳ – Фойдаланиш ҳуқуқида қуйидаги операциялар кўрсатилиши мумкин: ўқиш, ёзиш, бажариш, тўлдириш, модификация қилиш, ўчириш, яратиш.

Вирус загрузочный

uz - yuklash virusi

юклаш вируси

en - loading virus

Вирус, заражающий загрузочные части жестких и/или гибких дисков.

Qattiq va yoki yumshoq disklarning yuklanadigan qismlarini zararlaydigan virus.

Қаттиқ ва ёки юмшоқ дискларнинг юкланадиган қисмларини зарарлайдиган вирус.

Вирус (компьютерный)

uz - virus

вирус

en - virus

1 Анонимная программа, которая внедряется в вычислительную систему с целью исказить, модифицировать или уничтожить данные.

2 Программа, которая обладает следующими свойствами: возможностью копирования себя в другие файлы, диски, ЭВМ; возможностью выполнения без явного вызова; возможностью осуществления несанкционированного доступа к информации; возможностью маскировки от попыток обнаружения.

3 Вредоносная программа, способная создавать свои копии или другие вредоносные программы и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия.

1 Hisoblash tizimiga, ma'lumotlarni buzish, o'zgartirish yoki yo'q qilish maqsadida kiritiladigan anonim dastur.

2 Quyidagi xususiyatlarga: o'zini boshqa fayllarga, diskka, EHMga ko'chirish; aniq chaqiruvsiz bajarish; axborotdan ruxsat etilmagan tarzda foydalanishni

В

amalga oshirish; aniqlashga urinishdan maskirovka qilish imkoniyatiga ega dastur.

3 О‘zining nusxasini yoki boshqa zararli dasturlar yarata oladigan va ularni kompyuter fayllariga, tizim sohalariga kiritadigan, shuningdek, boshqa destruktiv xarakatlarni amalga oshiradigan zararli dastur.

1 Ҳисоблаш тизимига, маълумотларни бузиш, ўзгартириш ёки йўқ қилиш мақсадида киритиладиган аноним дастур.

2 Қуйидаги хусусиятларга: ўзини бошқа файлларга, дискка, ЭҲМга кўчириш; аниқ чақирувсиз бажариш; ахборотдан рухсат этилмаган тарзда фойдаланишни амалга ошириш; аниқлашга уришидан маскировка қилиш имкониятига эга дастур.

3 Ўзининг нусхасини ёки бошқа зарarli дастурлар ярата оладиган ва уларни компьютер файлларига, тизим соҳаларига киритадиган, шунингдек, бошқа destruktiv xarakatlarni amalga oshiradigan zararli dastur.

Вирус программный, вирус
uz - dasturiy virus, virus
дастурий вирус, вирус
en - program virus, virus

Специально разработанная вредоносная программа, которая самопроизвольно размножается путем вставления своих возможно измененных копий в другие программы и модификации их при этом, и которая выполняется при вызове инфицированной программы.

Примечание – Вирус часто является причиной искажений или разрушений и, в некоторых случаях, может активизироваться при наступлении определенной даты.

Boshqa dasturlarga o‘zining o‘zgartirilgan nusxalarini qo‘yish yo‘li bilan o‘z-o‘zidan ko‘payadigan, uni o‘zgartiradigan, zararlangan dasturni ochishda amalga oshadigan maxsus ishlab chiqilgan zararli dastur.

Izoh – Virus ko‘pincha buzilishlar yoki ishdan chiqishlarga sabab bo‘ladi hamda ba’zi hollarda ma’lum sana boshlanishi bilan aktivlashishi mumkin.

Бошқа дастурларга ўзининг ўзгартирилган нусхаларини қўйиш йўли билан ўз-ўзидан кўпаядиган, уни ўзгартирадиган, зарарланган дастурни очишда амалга ошадиган махсус ишлаб чиқилган

В

зарарли дастур.

Изоҳ – Вирус кўпинча бузилишлар ёки ишдан чиқишларга сабаб бўлади ҳамда баъзи ҳолларда маълум сана бошланиши билан активлашиши мумкин.

Вирусы неопасные

uz - xavfli bo'lmagan viruslar

хавfli бўлмаган вируслар

en - harmless viruses

Вирусы, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках. Действия таких вирусов проявляются, как правило, в каких-либо графических или звуковых эффектах.

Kompyuter ishiga xalaqit bermaydigan, lekin bo'sh operativ хотира va disklardagi хотира hajmini kamaytiradigan viruslar. Bunday viruslarning ta'siri, odatda, qandaydir grafik yoki tovush effektlarida namoyon bo'ladi.

Компьютер ишига халақит бермайдиган, лекин бўш оператив хотира ва дисклардаги хотира ҳажмини камайтирадиган вируслар. Бундай вирусларнинг таъсири, одатда, қандайдир график ёки товуш эффектларида намоён бўлади.

Вирусы опасные

uz - xavfli viruslar

хавfli вируслар

en - harmful viruses

Вирусы, которые могут привести к различным нарушениям в работе компьютера.

Kompyuter ishida turli buzilishlarga olib kelishi mumkin bo'lgan viruslar.

Компьютер ишида турли бузилишларга олиб келиши мумкин бўлган вируслар.

Вирусы очень опасные

uz - juda xavfli viruslar

жуда хавfli вируслар

en - herceluan viruses

Вирусы, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Ta'sir etishi dasturlarning yo'qotilishiga, ma'lumotlar yo'q bo'lishiga, diskning tizim sohalarida axborot o'chib ketishiga olib kelishi mumkin bo'lgan viruslar.

Таъсир этиши дастурларнинг йўқотилишига, маълумотлар йўқ бўлишига, дискнинг тизим соҳаларида ахборот ўчиб кетишига олиб келиши мумкин бўлган вируслар.

В

Вирусы паразитические

uz - parazit viruslar

паразит вируслар

en - parasitic viruses

Все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, добавляя в него свой код, при этом оставляя сами файлы полностью или частично работоспособными.

Примечание – Код вируса выполняется перед, после или вместе с программой, в зависимости от места внедрения вируса в программу.

Nusxalarini tarqatishda faylga o'zining kodini qo'shgan, fayllarni to'liq yoki qisman ishlash qobiliyatini saqlagan holda, fayllarning ichidagini albat-ta o'zgartiradigan viruslar.

Izoh – Virus kodi virusni dasturga kiritish joyiga bog'liq ravishda dastur oldidan, undan keyin yoki dastur bilan birga bajariladi.

Нусхаларини тарқатишда файлга ўзининг кодини қўшган, файлларни тўлиқ ёки қисман ишлаш қобилиятини сақлаган ҳолда, файлларнинг ичидагини албатта ўзгартирадиган вируслар.

Изоҳ – Вирус коди вирусни дастурга киритиш жойига боғлиқ равишда дастур олдиан, ундан кейин ёки дастур билан бирга бажарилади.

Вирусы перезаписывающие

uz - qayta yozadigan viruslar

қайта ёзадиган вируслар

en - rewriting viruses

Вирусы, записывающие свое тело вместо кода программы, не изменяя названия исполняемого файла, вследствие чего исходная программа перестает запускаться. При запуске программы выполняется код вируса, а не сама программа.

Dastur kodi o'rniga, bajariladigan fayl nomini o'zgartirmagan holda, o'z jismini yozadigan viruslar. Buning oqibatida, dastlabki dasturni ishga tushirish mumkin bo'lmay qoladi. Dasturni ishga tushirishda dasturning o'zi emas, balki virus kodi bajariladi.

Дастур коди ўрнига, бажариладиган файл номи-ни ўзгартирмаган ҳолда, ўз жисмини ёзадиган вируслар. Бунинг оқибатида, дастлабки дастурни ишга тушириш мумкин бўлмай қолади. Дастурни ишга туширишда дастурнинг ўзи эмас, балки вирус коди бажарилади.

Вирусы полиморфные

uz - polimorf viruslar

Вирусы, модифицирующие свой код в зараженных программах таким образом, что два экзем-

В

полиморф вируслар
en - polymorphic viruses

пляра одного и того же вируса могут не совпадать ни в одном бите.

Zararlangan dasturlarda o'z kodini, aynan bir virusning ikkita nusxasi birorta ham bitda mos tushmaydigan qilib o'zgartiradigan viruslar.

Зарарланган дастурларда ўз кодини, айнан бир вируснинг иккита нусхаси бирорта ҳам битда мос тушмайдиган қилиб ўзгартирадиган вируслар.

Вирусы простейшие
uz - oddiy viruslar
оддий вируслар
en - simple viruses

Вирусы, изменяющие содержимое файлов и секторов диска, которые могут быть достаточно легко обнаружены и уничтожены.

Fayllar va disk sektorlarining ichidagini o'zgartiruvchi, oson aniqlanadigan va yo'q qilinadigan viruslar.

Файллар ва диск секторларининг ичидагини ўзгартирувчи, осон аниқланадиган ва йўқ қилинадиган вируслар.

Вирусы резидентные
uz - rezident viruslar
резидент вируслар
en - resident viruses

Вирусы, оставляющие при заражении (инфицировании) компьютера в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.п.) и внедряется в них. Эти вирусы находятся в памяти и остаются активными вплоть до выключения или перезагрузки компьютера.

Kompyuterni zararlashda operativ хотирада o'zining rezident qismini qoldiradigan viruslar. Bu rezident qism operatsion tizimning zararlangan obyektlarga (fayllarga, disklarning yuklash sektorlariga) murojaatini tutib oladi va ularga kiradi. Rezident viruslar хотирада bo'ladi va kompyuter o'chirilgunga yoki qayta yuklangunga qadar aktivligicha qoladi.

Компьютерни зарарлашда оператив хотирада ўзининг резидент қисмини қолдирадиган вирус-

В

лар. Бу резидент қисм операцион тизимнинг зарланган объектларга (файлларга, дискларнинг юклаш секторларига) муружаатини тутиб олади ва уларга киради. Резидент вируслар хотирада бўлади ва компьютер ўчирилгунга ёки қайта юклангунга қадар активлигича қолади.

Вирусы файловые

uz - fayl viruslari

файл вируслари

en - file viruses

Вирусы, записывающие свой код в тело программного файла или документа, содержащего макрокоманды. При этом во время запуска программы (или загрузке документа для редактирования) эти вирусы получают управление.

Примечание – По способу заражения файловые вирусы разделяют на перезаписывающие, паразитические, вирусы-звенья, вирусы-черви, компаньон-вирусы, а так же вирусы, поражающие исходные тексты программ и компоненты программного обеспечения.

O‘z kodini dastur fayliga yoki makrokomandalar bo‘lgan hujjatga yozadigan viruslar. Dasturni ishga tushirishda (yoki hujjatni tahrir qilish uchun yuklashda) viruslar boshqaruvga ega bo‘ladi.

Izoh – Zararlash usuliga ko‘ra, fayl viruslari qayta yozadigan, parazit, zveno viruslar, qurt viruslar, kompanon viruslarga, shuningdek, dasturlarning dastlabki matnini va dasturiy ta‘minot komponentlarini zararlovchi viruslarga ajratiladi.

Ўз кодини дастур файлига ёки макрокомандалар бўлган ҳужжатга ёзадиган вируслар. Дастурни ишга туширишда (ёки ҳужжатни таҳрир қилиш учун юклашда) вируслар бошқарувга эга бўлади.

Изоҳ – Зарарлаш усулига кўра, файл вируслари қайта ёзадиган, паразит, звено вируслар, қурт вируслар, компаньон вирусларга, шунингдек, дастурларнинг дастлабки матнини ва дастурий таъминот компонентларини зарарловчи вирусларга ажратилади.

Вирусы, поражающие

исходный код программ

uz - dasturlarning boshlang‘ich kodini zararlaydigan viruslar

дастурларнинг бошлан-

гич кодини зарарлайдиган

вируслар

en - viruses, attaching program

Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU-файлы) а также VCL и ActiveX компоненты. После компиляции программы оказываются в неё встроенными.

Dasturning boshlang‘ich kodini yoki uning komponentlarini (OBJ-, LIB-, DCU- fayllarni), shuningdek,

В

initial code

VCL hamda ActiveX komponentlarni zararlaydigan viruslar. Kompilyatsiyadan soʻng dasturlar unga kiritilgan boʻladi.

Дастурнинг бошланғич кодини ёки унинг компонентларини (OBJ-, LIB-, DCU- файлларни), шунингдек, VCL ҳамда ActiveX компонентларни зарарлайдиган вируслар. Компиляциядан сўнг дастурлар унга киритилган бўлади.

Вирусы-звенья

uz - zveno viruslar

звено вируслар

en - unit viruses

Вирусы, не изменяющие код программы, а заставляющие операционную систему выполнить собственный код, изменяя адрес местоположения на диске зараженной программы, на собственный адрес. После выполнения кода вируса управление обычно передается вызываемой пользователем программе.

Dastur kodini oʻzgartirmaydigan, balki operasion tizimni zararlangan dastur diskida joylashgan adresni oʻz adresiga oʻzgartirgan holda, oʻzining kodi bajarilishiga majbur qiladigan viruslar. Virus kodi bajarilgandan soʻng, boshqarish odatda, foydalanuvchi tomonidan chaqiriladigan dasturga beriladi.

Дастур кодини ўзгартирмайдиган, балки операцион тизимни зарарланган дастур дискида жойлашган адресни ўз адресига ўзгартирган холда, ўзининг коди бажарилишига мажбур қиладиган вируслар. Вирус коди бажарилгандан сўнг бошқариш одатда, фойдаланувчи томонидан чақириладиган дастурга берилади.

Вирусы-компаньоны

uz - kompanon viruslar

компаньон вируслар

en - companion viruses

Эти вирусы создают свою копию на месте заражаемой программы, но не уничтожают оригинальный файл, а переименовывают или перемещают его. При запуске программы вначале выполняется код вируса, а затем управление передается оригинальной программе.

Nusxasini zararlanadigan dastur oʻrnida yarata-digan, original faylni yoʻq qilmasdan, uni qayta nomlaydigan yoki siljitadigan viruslar. Dasturni ishga tushirishda avval virus kodi bajariladi, keyin boshqaruv original dasturga beriladi.

В

Нусхасини зарарланадиган дастур ўрнида яратадиган, оригинал файлни йўқ қилмасдан, уни қайта номлайдиган ёки силжитадиган вируслар. Дастурни ишга туширишда аввал вирус коди бажарилади, кейин бошқарув оригинал дастурга берилади.

Вирусы-мутанты

uz - mutant viruslar

мутант вируслар

en - mutant viruses

Вирусы, которые содержат алгоритмы шифрования-расшифрования, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Shifrlash-rasshifrovka qilish algoritmlarini ichiga oluvchi viruslar. Bu algoritmlar tufayli, aynan bir virusning nusxalari baytlarning birorta ham takrorlanadigan zanjiriga ega bo'lmaydi.

Шифрлаш-расшифровка қилиш алгоритларини ичига олувчи вируслар. Бу алгоритмлар туфайли, айнан бир вируснинг нусхалари байтларнинг бирорта ҳам такрорланадиган занжирига эга бўлмайди.

Вирусы-невидимки

uz - ko'rinmas viruslar

кўринмас вируслар

en - stealth viruses

1 Трудно обнаруживаемые и обезвреживаемые вирусы, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.

2 Вирусы, использующие специальные алгоритмы, маскирующие их присутствие на диске, а в некоторых случаях и в оперативной памяти.

1 Aniqlanishi va zararsizlantirilishi qiyin bo'lgan viruslar, chunki ular operatsion tizimning zararlangan fayllarga va disk sektorlariga murojaatini tutib oladi va o'z o'rniga diskning zararlanmagan uchastkalarini qo'yadi.

2 O'zining diskda, ba'zi hollarda operativ xotirada mavjudligini niqoblovchi maxsus algoritmlardan foydalanadigan viruslar.

1 Аниқланиши ва зарарсизлантирилиши қийин бўлган вируслар, чунки улар операцион тизим-

В

нинг зарарланган файлларга ва диск секторларига мурожаатини тутиб олади ва ўз ўрнига дискнинг зарарланмаган участкаларини қўяди.

2 Ўзининг дискда, баъзи ҳолларда оператив хотирада мавжудлигини ниқобловчи махсус алгоритмлардан фойдаланадиган вируслар.

Владелец информации

uz - axborot egasi

ахборот эгаси

en - information owner

1 Субъект, осуществляющий владение и пользование информацией и реализующий полномочия и распоряжения в пределах прав, установленных законом и/или собственником информации.

2 Субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

1 Axborotga egalik qilish va undan foydalanishni, qonun bilan va/yoki axborot egasi tomonidan belgilangan huquqlar doirasida vakolat va farmoyishlarni amalga oshiruvchi subyekt.

2 Axborot munosabatlarining, axborot egasi bilan shartnoma bo'yicha axborot resurslariga egalik qilish, farmoyish berish va undan foydalanish huquqiga ega, subyekti.

1 Ахборотга эгалик қилиш ва ундан фойдаланишни, қонун билан ва/ёки ахборот эгаси томонидан белгиланган ҳуқуқлар доирасида ваколат ва фармойишларни амалга оширувчи субъект.

2 Ахборот муносабатларининг, ахборот эгаси билан шартнома бўйича ахборот ресурсларига эгалик қилиш, фармойиш бериш ва ундан фойдаланиш ҳуқуқига эга, субъекти.

Владелец полномочия

uz - vakolat egasi

ваколат эгаси

en - authority holder

Логический объект уровня, которому в данный момент присвоено полномочие.

Ayni paytda vakolat berilgan, darajaning mantiqiy obyekt.

Айни пайтда ваколат берилган, даражанинг мантикий объекти.

Владелец риска

uz - risk egasi

риск эгаси

Физическое лицо или логический объект, несущие ответственность и имеющие полномочия по управлению риском.

В

en - risk owner

Riskni boshqarish bo'yicha javobgar bo'lgan va vakolatga ega jismoniy shaxs yoki mantiqiy obyekt.

Рискни бошқариш бўйича жавобгар бўлган ва ваколатга эга жисмоний шахс ёки мантикий объект.

**Владелец сертификата
подписи**

uz - imzo sertifikatining egasi
имзо сертификатининг
эгаси

en - signature certificate owner

Физическое или юридическое лицо, на имя которого выдан сертификат ключа подписи и которое владеет закрытым ключом электронной цифровой подписи, соответствующим открытому ключу, указанному в сертификате.

Nomiga imzo kalitining sertifikati berilgan, sertifikatda ko'rsatilgan ochiq kalitga mos keluvchi elektron raqamli imzo kalitining yopiq kalitiga egalik qiladigan jismoniy yoki yuridik shaxs.

Номига имзо калитининг сертификати берилган, сертификатда кўрсатилган очик калитга мос келувчи электрон рақамли имзо калитининг ёпик калитига эгалик қиладиган жисмоний ёки юридик шахс.

**Внутренне
непротиворечивый**

uz - ichki qarama-qarshiliksiz
ички қарама-
қаршиликсиз

en - internally consistent

Отсутствие каких-либо явных противоречий между любыми аспектами логического объекта.

Примечание – Относительно документации это означает, что документация не может содержать положения, противоречащие друг другу.

Mantiqiy obyektning istalgan akpektlari orasida biror-bir aniq qarshilikning bo'lmasligi.

Izoh – Hujjatga nisbatan, hujjatda bir-biriga zid holatning bo'lmasligini bildiradi.

Мантикий объектнинг исталган акпектлари орасида бирор-бир аниқ қаршилиқнинг бўлмаслиги.

Изоҳ – Хужжатга нисбатан, хужжатда бир-бирига зид ҳолатнинг бўлмаслигини билдиради.

**Воздействие
дестабилизирующее**
uz - destabillashtiruvchi
ta'sir

дестабиллаштирувчи

Действие, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети телекоммуникаций характера, приводящее к выходу из строя элементов сети.

B

таъсир

en - destabilizing impact

Manbai telekommunikatsiyalar tarmog'iga nisbatan ichki yoki tashqi xarakterdagi fizik yoki texnologik jarayon bo'lgan, tarmoq elementlarining ishdan chiqishiga olib keladigan ta'sir.

Манбаи телекоммуникациялар тармоғига нисбатан ички ёки ташқи характердаги физик ёки технологик жараён бўлган, тармоқ элементларининг ишдан чиқишига олиб келадиган таъсир.

Воздействие злонамеренное
uz - yomon niyatda qilinadigan ta'sir

ёмон ниятда қилинадиган таъсир

en - attack

Действия, предпринимаемые в целях обхода механизмов обеспечения безопасности системы или в целях использования их недостатков.

Примечания

1 При непосредственном злонамеренном воздействии на систему используются недостатки базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.

2 Косвенные злонамеренные воздействия предпринимаются путем обхода механизма безопасности или принуждения системы к неправильному использованию этого механизма.

Tizimning xavfsizlikni ta'minlash mexanizmlarini chetlab o'tish yoki ularning kamchiliklaridan foydalanish maqsadida amalga oshiriladigan harakat.

Izohlar

1 Tizimga bevosita yomon niyatda ta'sir ko'rsatilganda, bazaviy algoritmlarning xavfsizlikni ta'minlash mexanizmining prinsiplari yoki xususiyatlari kamchiliklaridan foydalaniladi.

2 Bilvosita yomon niyatda qilinadigan ta'sir xavfsizlik mexanizmini chetlab o'tish yoki tizimni bu mexanizmdan noto'g'ri foydalanishga majbur qilish orqali amalga oshiriladi.

Тизимнинг хавфсизликни таъминлаш механизмларини четлаб ўтиш ёки уларнинг камчиликларидан фойдаланиш мақсадида амалга оширилган ҳаракат.

Изоҳлар

1 Тизимга бевосита ёмон ниятда таъсир кўрсатилганда, базавий алгоритмларнинг хавфсизликни таъминлаш меха-

В

низмининг принциплари ёки хусусиятлари камчиликларидан фойдаланилади.

2 Билвосита ёмон ниятда қилинадиган таъсир хавфсизлик механизмини четлаб ўтиш ёки тизимни бу механизмдан нотўғри фойдаланишга мажбур қилиш орқали амалга оширилади.

Воздействие на информационный ресурс внешнее

uz - axborot resursiga
ko‘rsatiladigan tashqi ta’sir
ахборот ресурсига кўрсатиладиган ташқи таъсир
en - exposure on information resources

Фактор опасности, вызываемый стихийными бедствиями, мощными электромагнитными излучениями или диверсионными актами и приводящий к нарушению целостности информации или ее блокированию.

Tabiiy ofatlar, kuchli elektromagnit nurlanishlar yoki qo‘poruvchilik harakatlari keltirib chiqaradigan, axborotning yaxlitligi buzilishiga yoki uning blokirovka qilinishiga olib keladigan xavf omili.

Табиий офатлар, кучли электромагнит нурланишлар ёки кўпорувчилик ҳаракатлари келтириб чиқарадиган, ахборотнинг яхлитлиги бузилишига ёки унинг блокировка қилинишига олиб келадиган хавф омили.

Воздействие на информацию непреднамеренное

uz - axborotga qasddan
bo‘lmagan ta’sir
ахборотга қасддан бўлмаган таъсир
en - casual action on information

Ошибка пользователя, сбой технических и программных средств систем, природные явления или иные не целенаправленные на изменение информации действия, приводящие к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Foydalanuvchining xatosi, tizimning texnik va dasturiy vositalaridagi nosozlik, tabiat hodisalari yoki axborotning buzib ko‘rsatilishiga, yo‘q qilinishiga, undan nusxa olinishiga, axborotdan foydalanishni blokirovka qilinishiga, shuningdek, axborot tashuvchining yo‘qolishiga, yo‘q qilinishiga yoki ishlashida uzilishlar kelib chiqishiga olib keladigan, boshqa maqsadga yo‘naltirilmagan, axborotni o‘zgartirishga bo‘lgan harakatlar.

Фойдаланувчининг хатоси, тизимнинг техник ва

В

дастурий воситаларидаги носозлик, табиат ходисалари ёки ахборотнинг бузиб кўрсатилишига, йўқ қилинишига, ундан нусха олинишига, ахборотдан фойдаланишни блокировка қилинишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилишлар келиб чиқишига олиб келадиган, бошқа мақсадга йўналтирилмаган, ахборотни ўзгартиришга бўлган ҳаракатлар.

Воздействие на информацию несанкционированное

uz - axborotga ruxsat etilmagan ta'sir

ахборотга рухсат этилмаган таъсир

en - unauthorized action on information

Воздействие на защищаемую информацию с нарушением установленных прав и/или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Muhofaza qilinadigan axborotga foydalanishning belgilangan huquqlari va/yoki qoidalarini buzgan holda ta'sir etish. Bu, axborotning yo'qolishiga, buzib ko'rsatilishiga, soxtalashtirilishiga, yo'q qilinishiga, axborotdan foydalanishning blokirovka qilinishiga, shuningdek, axborot tashuvchining yo'qolishiga, yo'q qilinishiga yoki ishlashida uzilishlar kelib chiqishiga olib keladi.

Муҳофаза қилинадиган ахборотга фойдаланишнинг белгиланган ҳуқуқлари ва/ёки қоидаларини бузган ҳолда таъсир этиш. Бу, ахборотнинг йўқолишига, бузиб кўрсатилишига, сохталаштирилишига, йўқ қилинишига, ахборотдан фойдаланишнинг блокировка қилинишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилишлар келиб чиқишига олиб келади.

Воздействие с ретрансляцией злонамеренное

uz - retranslyatsiya qilish bilan yomon niyatda qilinadigan ta'sir

ретрансляция қилиш билан ёмон ниятда

Злонамеренное воздействие на аутентификацию, при котором осуществляется перехват обмена аутентификационной информацией и немедленная ее ретрансляция.

Autentifikatsiyaga yomon niyatda ta'sir ko'rsatish. Bunda autentifikatsion axborot almashinuvi tutib

В

қилинадиган таъсир
en - relay attack

olinadi va darhol retranslyatsiya qilinadi.

Аутентификацияга ёмон ниятда таъсир кўрса-тиш. Бунда аутентификацион ахборот алмаши-нуви тутиб олинади ва дарҳол ретрансляция қилинади.

Воздействия негативные
uz - salbiy ta'sir etish
салбий таъсир этиш
en - adverse actions

Воздействия, оказываемые агентом угрозы на актив.

Tahdid agentining aktivga ko'rsatadigan ta'siri.

Таҳдид агентининг активга кўрсатадиган таъси-ри.

Возможности
недекларированные
uz - deklaratsiya (e'lon)
qilinmagan imkoniyatlar
декларация (эълон)
қилинмаган имкониятлар
en - undeclared capabilities

Функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Dasturiy ta'minotning bayon qilinmagan yoki hujjatda bayon qilinganlarga mos kelmaydigan funksional imkoniyatlari. Ulardan foydalanish qayta ishlanadigan axborotning konfidensialligi, tushunarli bo'lishi yoki yaxlitligi buzilishiga olib kelishi mumkin.

Дастурий таъминотнинг баён қилинмаган ёки хужжатда баён қилинганларга мос келмайдиган функционал имкониятлари. Улардан фойдала-ниш қайта ишланадиган ахборотнинг конфиден-циаллиги, тушунарли бўлиши ёки яхлитлиги бу-зилишига олиб келиши мумкин.

Возможности ОО
функциональные
uz - BOning funksional
imkoniyatlari
БОнинг функционал
имкониятлари
en - TOE security functionality

Совокупность функциональных возможностей всех аппаратных, программных и программно-аппаратных средств объекта оценки, которые необходимо использовать для корректной реализации требований.

Talablarni to'g'ri amalga oshirish uchun foydalanish zarur bo'lgan, baholash obyektining barcha apparat, dasturiy va dasturiy-apparat vositalari funksional im-

В

koniyatlarining yigʻindisi.

Талабларни тўғри амалга ошириш учун фойдаланиш зарур бўлган, баҳолаш объектининг барча аппарат, дастурий ва дастурий-аппарат воситалари функционал имкониятларининг йиғиндиси.

Воссоздание данных

uz - ma'lumotlarni yangitdan yaratish

маълумотларни янгитдан яратиш

en - data reconstitution

Метод реставрации данных путем компоновки данных из частей доступных альтернативных источников.

Erkin foydalanish mumkin boʻlgan muqobil manbalarining qismlarini joy-joyiga qoʻyish yoʻli bilan ma'lumotlarni tiklash metodi.

Эркин фойдаланиш мумкин бўлган муқобил манбаларнинг қисмларини жой-жойига қўйиш йўли билан маълумотларни тиклаш методи.

Восстановление базы

данных

uz - ma'lumotlar bazasini tiklash

маълумотлар базасини тиклаш

en - database recovery

1 Полная или частичная повторная загрузка базы данных.

2 Воссоздание содержимого базы данных по резервной копии, выполняемое в случае машинных сбоев или программных ошибок для поддержания целостности данных.

Примечание – Методами и средствами восстановления являются копирование, рестарт с контрольной точки, системный журнал.

1 Ma'lumotlar bazasini to'liq yoki qisman takroran yuklash.

2 Ma'lumotlar bazasini rezerv nusxaga qarab tiklash. Ma'lumotlarning yaxlitligini saqlab turish maqsadida, mashina buzilishlari yoki dasturiy xatoliklar bo'lgan holatlarda bajariladi.

Izoh – Nusxa olish, nazorat nuqtasidan qayta boshlash, tizim jurnali tiklashning metod va vositalari hisoblanadi.

1 Маълумотлар базасини тўлиқ ёки қисман такроран юклаш.

2 Маълумотлар базасини резерв нусхага қараб тиклаш. Маълумотларнинг яхлитлигини сақлаб туриш мақсадида, машина бузилишлари ёки дас-

В

турий хатоликлар бўлган ҳолатларда бажарилади. Изоҳ – Нусха олиш, назорат нуқтасидан қайта бошлаш, тизим журнали тиклашнинг метод ва воситалари ҳисобланади.

Восстановление данных

uz - ma'lumotlarni tiklash

маълумотларни тиклаш

en - data recovery

(reconstruction)

1 Приведение данных к предварительно известному или определенному состоянию.

2 Процесс копирования данных с носителя, содержащего защитную копию данных, на носитель-оригинал в случае нарушения на нем целостности данных.

1 Ma'lumotlarni oldindan ma'lum bo'lgan yoki muayyan bir holatga keltirish.

2 Ma'lumotlarni, ma'lumotlarning himoya nusxasi bo'lgan tashuvchidan original tashuvchiga, ma'lumotlar yaxlitligi buzilgan holda, ko'chirish.

1 Маълумотларни олдиндан маълум бўлган ёки муайян бир ҳолатга келтириш.

2 Маълумотларни, маълумотларнинг ҳимоя нусхаси бўлган ташувчидан оригинал ташувчига, маълумотлар яхлитлиги бузилган ҳолда, кўчириш.

Восстановление обратное

uz - teskari tiklash

тескари тиклаш

en - backward recovery

Использование более поздней версии данных, записанных в журнал, для воссоздания более ранней версии данных.

Ma'lumotlarning jurnalga yozilgan oxirgi versiyasidan ma'lumotlarning dastlabki versiyasini tiklashda foydalanish.

Маълумотларнинг журналга ёзилган охириги версиясидан маълумотларнинг дастлабки версиясини тиклашда фойдаланиш.

Восстановление после отказа

uz - ishlaymay qolishdan

so'ng tiklash

ишламай қолишдан

сўнг тиклаш

en - failure recovery

Процедура возобновления работы вычислительной системы после отказа, исключая выработку системой неверных результатов.

Hisoblash tizimi ishini ishlaymay qolishdan so'ng tiklash protsedurasi tizimning noto'g'ri natijalar chiqarishini istisno qiladi.

Ҳисоблаш тизими ишини ишламай қолишдан

В

сўнг тиклаш процедураси тизимнинг нотўғри натижалар чиқаришини истисно қилади.

Восстановление при исчезновении питающего напряжения

uz - ta'minot kuchlanishi
yo'qolganda tiklash

таъминот кучланиши
йўқолганда тиклаш

en - power fail recovery

Метод борьбы с последствиями отключения напряжения в питающей сети. Система оборудуется устройством контроля линии энергоснабжения, которое обнаруживает любое длительное отклонение напряжения в питающей сети за допустимые пределы и осуществляет прерывание по неисправности в системе питания, когда происходят такие отклонения. Программа обслуживания этого прерывания запоминает дескрипторы всех процессов в энергонезависимой памяти и затем останавливает работу. Когда напряжение в питающей сети восстанавливается, система снова запускается и может восстановить все процессы по их дескрипторам.

Ta'minot manbaida kuchlanishning uzilib qolish oqibatlari bilan kurashish metodi. Tizim elektr ta'minot liniyasini nazorat qiluvchi qurilma bilan jihozlanadi. Qurilma ta'minot manbaidagi kuchlanishning yo'l qo'yiladigan chegaradan har qanday chetga chiqishini aniqlaydi va shunday chetga chiqish yuz berganda, ta'minot tizimida nosozlik bo'yicha uzilishni amalga oshiradi. Bu uzilishga xizmat ko'rsatish dasturini energiyaga bog'liq xotiradagi barcha jarayonlarning deskriptorlari yodda saqlaydi, so'ng ishni to'xtatadi. Ta'minot manbaida kuchlanish tiklanganda, tizim yana ishga tushiriladi va deskriptorlari bo'yicha barcha jarayonlarni tiklaydi.

Таъминот манбаида кучланишнинг узилиб қолиш оқибатлари билан курашиш методи. Тизим электр таъминот линиясини назорат қилувчи қурилма билан жиҳозланади. Қурилма таъминот манбаидаги кучланишнинг йўл қўйиладиган чегарадан ҳар қандай четга чиқишини аниқлайди ва шундай четга чиқиш юз берганда, таъминот тизимида носозлик бўйича узилишни амалга оширади. Бу узилишга хизмат кўрсатиш дастурини энергияга боғлиқ хотирадаги барча жараёнларнинг дескрипторлари ёдда сақлайди, сўнг ишни тўхтатади. Таъминот манбаида кучланиш тикланганда, ти-

В

Восстановление при ошибках

uz - xatolar bo'lganda tiklash
хатолар бўлганда тиклаш
en - error recovery

зим яна ишга туширилади ва дескрипторлари бўйича барча жараёнларни тиклайди.

Процесс исправления или обхода неисправности, позволяющий восстановить предписанное состояние системы.

Tizimning belgilangan holatini tiklash imkoniyatini beradigan, nosozlikni tuzatish yoki aylanib o'tish jarayoni.

Тизимнинг белгиланган ҳолатини тиклаш имкониятини берадиган, носозликни тузатиш ёки айланиб ўтиш жараёни.

Восстановление прямое

uz - bevosita tiklash
бевосита тиклаш
en - forward recovery

Использование более ранней версии данных, записанных в журнал, для воссоздания более поздней версии данных.

Ma'lumotlarning jurnalga yozilgan dastlabki versiyasidan, ma'lumotlarning oxirgi versiyasini tiklashda foydalanish.

Маълумотларнинг журналга ёзилган дастлабки версиясидан, маълумотларнинг охириги версиясини тиклашда фойдаланиш.

Восстановление сети

uz - tarmoqni tiklash
тармоқни тиклаш
en - network recovery

Совокупность действий, выполняемых для восстановления работоспособности вычислительной сети.

Hisoblash tarmog'ining ishlash qobiliyatini tiklash maqsadida bajariladigan amallar jami.

Ҳисоблаш тармоғининг ишлаш қобилиятини тиклаш мақсадида бажариладиган амаллар жами.

Восстановление файла

uz - faylni tiklash
файлни тиклаш
en - file recovery

Процесс восстановления целостности файла после обнаружения в нем ошибок.

Xatoliklar aniqlangandan so'ng, faylning yaxlitligini tiklash jarayoni.

Хатоликлар аниқлангандан сўнг, файлнинг яхлитлигини тиклаш жараёни.

В

Время безопасное

uz - xavfsiz vaqt
хавфсиз вақт
en - security time

Математическое ожидание времени раскрытия системы защиты статистическим апробированием возможных вариантов доступа к данным.

Ma'lumotlardan foydalanishning mumkin bo'lgan variantlarini statistik sinash orqali muhofaza tizimining ochilish vaqtini matematik kutish.

Маълумотлардан фойдаланишнинг мумкин бўлган вариантларини статистик синаш орқали муҳофаза тизимининг очилиш вақтини математик кутиш.

Время восстановления

uz - tiklash vaqti
тиклаш вақти
en - recovery time

Время между моментом обнаружения сбоя и моментом возобновления работы системы (устройства) после восстановления.

Nosozlik aniqlangan payt bilan tiklashdan keyin tizim (qurilma) ishi qayta tiklangan payt orasidagi vaqt.

Носозлик аниқланган пайт билан тиклашдан кейин тизим (қурилма) иши қайта тикланган пайт орасидаги вақт.

Время доступа (обращения)

uz - foydalana olish (murojaat qilish) vaqti
фойдалана олиш
(мурожаат қилиш) вақти
en - access time

Интервал времени между моментом выдачи команды на ввод-вывод данных и моментом начала обмена.

Ma'lumotlarni kiritish-chiqarishga komanda berish payti bilan almashinishning boshlanish payti orasidagi vaqt intervali.

Маълумотларни киритиш-чиқаришга команда бериш пайти билан алмашинишнинг бошланиш пайти орасидаги вақт интервали.

Время жизни

uz - yashash vaqti
яшаш вақти
en - life time

Интервал выполнения программы, в котором программный объект (например, переменная) сохраняет свое значение.

Dastur obyektini (masalan, o'zgaruvchi) o'z ahamiyatini saqlab turadigan, dasturning bajarilish intervali.

Дастур объекти (масалан, ўзгарувчи) ўз аҳамия-

В

Время ремонта

uz - ta'mirlash vaqti

таъмирлаш вақти

en - repair time

тини сақлаб турадиган, дастурнинг бажарилиш интервали.

Время (иногда среднее), необходимое для диагностирования и устранения неполадок либо в технических средствах, либо в программном обеспечении вычислительной системы.

Texnik vositalardagi yoki hisoblash tizimining dasturiy ta'minotidagi nosozliklarni aniqlash va bartaraf qilish uchun zarur bo'lgan (ba'zida o'rtacha) vaqt.

Техник воситалардаги ёки ҳисоблаш тизимининг дастурий таъминотидаги носозликларни аниқлаш ва бартараф қилиш учун зарур бўлган (баъзида ўртача) вақт.

Вскрываетел паролей

uz - parollarni ochuvchi

паролларни очувчи

en - password discriminator

Программа, осуществляющая подбор и обнаружение паролей.

Parollarning tanlanishini va aniqlanishini amalga oshiruvchi dastur.

Паролларнинг танланишини ва аниқланишини амалга оширувчи дастур.

Вторжение

uz - bostirib kirish

бостириб кириш

en - inroad, intrusion

Атака, целью которой является осуществление несанкционированного доступа к информационным ресурсам.

Axborot resurslaridan ruxsat etilmagan tarzda foydalanishni amalga oshirish maqsadidagi hujum.

Ахборот ресурсларидан рухсат этилмаган тарзда фойдаланишни амалга ошириш мақсадидаги хужум.

Вход (в систему)

uz - kirish (tizimga kirish)

кириш (тизимга кириш)

en - logon

Предоставление пользователем идентифицирующих его сведений (например, имени, домена и пароля), проверка подлинности и образование сеанса работы пользователем.

Foydalanuvchi tomonidan, uni identifikatsiya qiluvchi ma'lumotlarning (masalan, nomi, domeni va paroli) taqdim etilishi, haqiqiylikni tekshirish va foyda-

В

lanuvchining ish seansini tashkil qilish.

Фойдаланувчи томонидан, уни идентификация қилувчи маълумотларнинг (масалан, номи, домени ва пароли) тақдим этилиши, ҳақиқийликни текшириш ва фойдаланувчининг иш сеансини ташкил қилиш.

Вход между строк

uz - satrlar orasiga kirish

сатрлар орасига кириш

en - between-the-lines entry

Доступ, полученный нарушителем посредством активного перехвата при кратковременном выключении канала передачи данных, связанного с ресурсами законного пользователя.

Qonuniy foydalanuvchining resurslari bilan bogʻliq boʻlgan, maʼlumotlar uzatish kanalini qisqa vaqtga oʻchirish paytida buzgʻunchi tomonidan aktiv tutib olish vositasida olingan kirish huquqi.

Қонуний фойдаланувчининг ресурслари билан боғлиқ бўлган, маълумотлар узатиш каналини қисқа вақтга ўчириш пайтида бузгунчи томонидан актив тутиб олиш воситасида олинган кириш ҳуқуқи.

Выбор

uz - tanlamoq

танламоқ

en - selection

Выделение одного или нескольких элементов из перечня в компоненте.

Komponentdagi roʻyxatdan bitta yoki bir nechta elementni ajratib koʻrsatilishi.

Компонентдаги рўйхатдан битта ёки бир нечта элементни ажратиб кўрсатилиши.

Выводы аудита

uz - audit xulosalari

аудит хулосалари

en - audit findings

Результаты оценки свидетельств аудита в соответствии с критериями аудита.

Примечание – Данные аудита могут указывать на соответствие или несоответствие критериям аудита или на возможности улучшения.

Audit kriteriyalariga muvofiq audit dalillarini baholash natijalari.

Izoh – Audit maʼlumotlari audit kriteriyalariga mos kelish yoki kelmaslikni yoki yaxshilash imkoniyatlarini koʻrsatadi.

В

Аудит критерийларига мувофиқ аудит далилларини баҳолаш натижалари.

Изоҳ – Аудит маълумотлари аудит критерийларига мос келиш ёки келмаслиқни ёки яхшилаш имкониятларини кўрсатади.

Вызов обратный

uz - qayta chaqiruv

қайта чақирув

en - call-back

Процедура, используемая для аутентификации вызывающего терминала следующим образом: вначале система обработки данных идентифицирует вызывающий терминал, далее происходит разъединение вызова, а затем набирается номер вызывающего терминала.

Chaqiruvchi terminalni autentifikatsiya qilish uchun mo'ljallangan protsedura: dastlab ma'lumotlarni qayta tiklash tizimi chaqiruvchi terminalni identifikatsiya qiladi, keyin chaqiruvning uzilishi yuz beradi, so'ngra chaqiruvchi terminal raqami teriladi.

Чақирувчи терминални аутентификация қилиш учун мўлжалланган процедура: дастлаб маълумотларни қайта тиклаш тизими чақирувчи терминални идентификация қилади, кейин чақирувнинг узилиши юз беради, сўнгра чақирувчи терминал рақами терилади.

Вызов-ответ

uz - chaqiruv-javob

чақирув-жавоб

en - challenge-response

Механизм проверки пароля. Сервер передает клиенту «вызов», тот преобразует его с помощью пароля и результат передает серверу как «ответ». Сервер проверяет, что «ответ» получен из «вызова» при помощи правильного пароля.

Parolni tekshirish mexanizmi. Server mijozga «chaqiruv»ni uzatadi, u parol yordamida uni qayta o'zgartiradi va natijani serverga «javob» sifatida uzatadi. Server «javob» «chaqiruv»dan to'g'ri parol yordamida olinganligini tekshiradi.

Паролни текшириш механизми. Сервер мижозга «чақирув»ни узатади, у пароль ёрдамида уни қайта ўзгартиради ва натижани серверга «жавоб» сифатида узатади. Сервер «жавоб» «чақирув»дан тўғри пароль ёрдамида олинганлигини текширади.

Вызов санкционированный

uz - ruxsat etilgan chaqiruv

Вызов системы, программы или данных, разрешенный данному пользователю. Как правило,

В

рухсат этилган чақирув
en - authorized call

реализуется путем ввода и проверки пароля.

Belgilangan (ma'lum) foydalanuvchiga ruxsat etilgan, tizimni, dastur yoki ma'lumotlarni chaqirish. Odatda, parolni kiritish va uni tekshirish orqali bajariladi.

Белгиланган (маълум) фойдаланувчига рухсат этилган, тизимни, дастур ёки маълумотларни чақириш. Одатда, паролни киритиш ва уни текшириш орқали бажарилади.

Выравнивание сектора
uz - sektorni to'g'rilash
секторни тўғрилаш
en - sector alignment

Метод защиты от копирования, позволяющий при проверке правильности установки секторов от дорожки к дорожке определить, является ли диск несанкционированной копией или нет.

Nusxa ko'chirishdan muhofaza qilish metodi, sektorlarning yo'lkadan yo'lkaga to'g'ri o'rnatilganligini tekshirishda disk ruxsat etilmagan nusxa bo'lib hisoblanishi yoki hisoblanmasligini aniqlash imkonini beradi.

Нусха кўчиришдан муҳофаза қилиш методи, секторларнинг йўлқадан йўлқага тўғри ўрнатилганлигини текширишда диск рухсат этилмаган нусха бўлиб ҳисобланиши ёки ҳисобланмаслигини аниқлаш имконини беради.

Г

Гамма криптостойкая
uz - kriptobardoshli gamma
криптобардошли гамма
en - strong gamma

Гамма, по известному фрагменту которой нельзя определить другие ее фрагменты и восстановить со всеми деталями алгоритм, использованный для ее выработки.

Ma'lum fragmentiga qarab, uning boshqa fragmentlarini aniqlash va uni ishlab chiqish uchun foydalanilgan algoritmnı barcha detallari bilan tiklash mumkin bo'lmagan gamma.

Маълум фрагментига қараб, унинг бошқа фрагментларини аниқлаш ва уни ишлаб чиқиш учун фойдаланилган алгоритмни барча деталлари билан тиклаш мумкин бўлмаган гамма.

Гамма шифра
uz - shifr gammasi

1 Псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму,

Г

шифр гаммаси
en - key stream, gamma of the cipher

для зашифрования и расшифрования данных.

2 Псевдослучайная последовательность элементов данных, вырабатываемая по заданному алгоритму и используемая для зашифрования открытых данных и расшифрования зашифрованных данных путем комбинирования с ними обратной бинарной операции.

1 Ma'lumotlarni shifrlash va rasshifrovka qilish uchun, berilgan algoritm bo'yicha ishlab chiqiladigan psevdotasodifiy ikkilik ketma-ketlik.

2 Berilgan algoritm bo'yicha ishlab chiqiladigan va ochiq ma'lumotlarni shifrlash hamda qaytar binar operatsiyani kombinatsiyalash yo'li bilan shifrlangan ma'lumotlarni rasshifrovka qilish uchun foydalani-ladigan, ma'lumotlar elementlarining psevdotasodi-fiy ketma-ketligi.

1 Маълумотларни шифрлаш ва расшифровка қилиш учун, берилган алгоритм бўйича ишлаб чиқиладиган псевдотасодифий иккилик кетма-кетлик.

2 Берилган алгоритм бўйича ишлаб чиқиладиган ва очик маълумотларни шифрлаш ҳамда қайтар бинар операцияни комбинациялаш йўли билан шифрланган маълумотларни расшифровка қилиш учун фойдаланиладиган, маълумотлар элементларининг псевдотасодифий кетма-кетлиги.

Гаммирование

uz - gammalash

гаммалаш

en - gamming

Процесс наложения по определенному алгоритму гаммы шифра на открытый текст.

Ma'lum algoritmi bo'yicha shifr gammasini ochiq matnga qo'yish jarayoni.

Маълум алгоритми бўйича шифр гаммасини очик матнга қўйиш жараёни.

Гарантированность механизмов защиты информации

uz - axborotni muhofaza qilish mexanizmlarining kafolatlanganligi

ахборотни муҳофаза

Оценка адекватности используемых механизмов защиты информации выбранным функциональным требованиям.

Примечание – Гарантированность определяется эффективностью и корректностью механизмов защиты информации.

Foydalaniladigan axborotni muhofaza qilish mexa-

Г

қилиш механизмларининг
кафолатланганлиги
en - information defence
mechanism security

nizmlarining tanlangan funksional talablarga adekvatligini (mosligini) baholash.

Izoh – Kafolatlanganlik axborotni muhofaza qilish mexanizmlarining samaradorligi va toʻgʻriligi bilan aniqlanadi.

Фойдаланиладиган ахборотни муҳофаза қилиш механизмларининг танланган функционал талабларга адекватлигини (мослигини) баҳолаш.

Изоҳ – Кафолатланганлик ахборотни муҳофаза қилиш механизмларининг самарадорлиги ва тўғрилиги билан аниқланади.

Гарантия
uz - kafolat
кафолат
en - assurance

Мера доверия архитектуре и средствам обеспечения безопасности системы относительно корректности и аккуратности проведения политики безопасности.

Xavfsizlik siyosatini oʻtkazishning toʻgʻriligi va batartibligiga nisbatan arxitektura va tizim xavfsizligini taʼminlash vositalariga ishonch oʻlchovi.

Xavfsizlik siyosatini oʻtkazishning toʻgʻriligi va batartibligiga nisbatan arxitektura va tizim xavfsizligini taʼminlash vositalariga ishonch oʻlchovi.

Генератор ключевого потока
uz - kalit oqimi generatori
калит оқими генератори
en - key stream generator

Алгоритм, вырабатывающий ключевой поток для потоковых криптосистем. Может быть либо детерминированным, чтобы воспроизвести одинаковый ключевой поток на концах отправителя и получателя, либо случайным. Если генератор детерминированный, то он зависит от секретного ключа. Генераторы ключевого потока обычно базируются на комбинациях регистров сдвига и нелинейных булевых функциях. При построении генераторов ключевого потока часто используют криптографические преобразования блочных шифров, например OFB или счетчиковый метод.

Oqimli kriptotizimlar uchun kalit oqimini ishlab chiquvchi algoritm. Yo joʻnatuvchi va oluvchi uchlarida bir xil kalit oqimini qayta ishlab chiqish uchun determinlangan, yo tasodifiy boʻlishi mumkin. Agar generator determinlangan boʻlsa, u maxfiy kalitga bogʻliq boʻladi. Kalit oqimi generatorlari odatda siljish registrlarining kombinatsiyasiga va

Г

nochiziqli Bul funksiyalariga asoslanadi. Kalit oqimi generatorlarini tuzishda ko‘pincha, blokli shifrlarni kriptografik qayta tuzishdan, masalan *OFB* yoki hisoblagichli metoddan foydalaniladi.

Оқимли криптолизимлар учун калит оқимини ишлаб чиқувчи алгоритм. Ё жўнатувчи ва олувчи учларида бир хил калит оқимини қайта ишлаб чиқиш учун детерминланган, ё тасодифий бўлиши мумкин. Агар генератор детерминланган бўлса, у махфий калитга боғлиқ бўлади. Калит оқими генераторлари одатда силжиш регистрларининг комбинациясига ва нозизикли Буль функцияларига асосланади. Калит оқими генераторларини тузишда кўпинча, блокли шифрларни кriptografik қайта тузишдан, масалан *OFB* ёки ҳисоблагичли методдан фойдаланилади.

Генератор случайных паролей

uz - tasodifiy parollar generatori

тасодифий пароллар генератори

en - randompassword generator

Программно-аппаратное средство, представляющее собой генератор случайных чисел, используемых в качестве паролей.

Parollar sifatida foydalaniladigan tasodifiy sonlar generatorini o‘zida ifodalaydigan dasturiy-apparat vosita.

Пароллар сифатида фойдаланиладиган тасодифий сонлар генераторини ўзида ифодаляйдиган дастурий-аппарат восита.

Генерация ключей

uz - kalitlar generatsiyasi

калитлар генерацияси

en - key generation

Процесс генерации криптографических ключей. Согласно правилу Кирхгоффа, стойкость криптографического алгоритма базируется на секретности ключа, поэтому генерация ключей – очень важный процесс, для выполнения которого используются различные методы, например, генераторы случайных и псевдослучайных последовательностей.

Kriptografik kalitlarni generatsiyalash jarayoni. Kirxgoff qoidasiga muvofiq, kriptografik algoritmining o‘zgarmasligi kalitning maxfiyligiga asoslanadi, shuning uchun kalitlar generatsiyasi juda muhim jarayon hisoblanadi, uni bajarish uchun turli metodlardan, masalan, tasodifiy va psevdotasodifiy ketma-

Г

ketlikdagi generatorlardan foydalaniladi.

Криптографик калитларни генерациялаш жараёни. Кирхгофф қоидасига мувофиқ, криптографик алгоритмнинг ўзгармаслиги калитнинг махфийлигига асосланади, шунинг учун калитлар генерацияси жуда муҳим жараён ҳисобланади, уни бажариш учун турли методлардан, масалан, тасодифий ва псевдотасодифий кетма-кетликдаги генераторлардан фойдаланилади.

Граница кодирования

uz - kodlash chegarasi

кодлаш чегараси

en - coding bound

Предел производительности кода, зависимый от таких параметров, как мощность кода, минимальное расстояние Хемминга, длина кодовой комбинации.

Kod unumdorligining chegarasi, u kod quvvati, minimal Хемминг масофаси, kodli kombinatsiya uzunligi kabi parametrlarga bogʻliq.

Код унумдорлигининг чегараси, у код қуввати, минимал Хемминг масофаси, кодли комбинация узунлиги каби параметрларга боғлиқ.

Гриф секретности

uz - maxfiylik grifi

махфийлик грифи

en - security classification

1 Определенный уровень, который необходим в данном конкретном случае для защиты данных или информации от несанкционированного доступа, вместе с указанием этого уровня. Например, «совершенно секретно», «секретно», «конфиденциально».

2 Надпись (штамп) на документе или издании, определяющая особый порядок пользования этим документом.

3 Специальная отметка на носителе информации, свидетельствующая о степени конфиденциальности информации, хранимой на этом носителе.

4 Реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и/или в сопроводительной документации на него.

1 Berilgan muayyan holatda ma'lumotlar yoki axbotni ruxsat etilmagan tarzda foydalanishdan muhofaza qilish uchun zarur boʻlgan aniq belgilangan daraja. Masalan, «mutlaqo maxfiy», «maxfiy», «konfi-

Г

densial».

2 Hujjat yoki nashrdagi, shu hujjatdan foydalanishning muhim tartibini belgilovchi yozuv (tamg'a).

3 Axborot tashuvchidagi, shu tashuvchida saqlanadigan axborotning konfidentsiallik darajasini tasdiqlovchi maxsus belgi.

4 Tashuvchining o'ziga va/yoki unga ilova qilinadigan hujjatlarga qo'yiladigan, ularning eltuvchilarida mavjud bo'lgan ma'lumotlarning maxfiylik darajasini tasdiqlovchi rekvizitlar.

1 Берилган муайян ҳолатда маълумотлар ёки ахборотни рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш учун зарур бўлган аниқ белгиланган даража. Масалан, «мутлақо махфий», «махфий», «конфиденциал».

2 Хужжат ёки нашрдаги, шу хужжатдан фойдаланишнинг муҳим тартибини белгиловчи ёзув (тамға).

3 Ахборот ташувчидаги, шу ташувчида сақланадиган ахборотнинг конфиденциаллик даражасини тасдиқловчи махсус белги.

4 Ташувчининг ўзига ва/ёки унга илова қилинадиган хужжатларга қўйиладиган, уларнинг элтувчиларида mavjud бўлган маълумотларнинг махфийлик даражасини тасдиқловчи реkvизитлар.

Д

Дайджест
uz - dayjest
 дайжест
en - digest

Код фиксированной длины, образующийся в результате обработки с помощью хэш-функции входного потока данных переменной длины. Так, например, алгоритм хэширования SHA-1 создает дайджест размером 20 bit, независимо от размера входного сообщения.

O'zgaruvchan uzunlikdagi ma'lumotlarning kirish oqimini xesh-funksiya yordamida qayta ishlash natijasida hosil bo'ladigan, qat'iy uzunlikdagi kod. Masalan, *SHA-1* xeshlash algoritmi kirish xabarining hajmidan qat'i nazar, 20 bit hajmidagi dayjestni yaratadi.

Ўзгарувчан узунликдаги маълумотларнинг ки-

Д

риш оқимини хэш-функция ёрдамида қайта ишлаш натижасида ҳосил бўладиган, қатъий узунликдаги код. Масалан, SHA-1 хэшлаш алгоритми кириш хабарининг ҳажмидан қатъи назар, 20 bit ҳажмидаги дайжестни яратади.

Данные

uz - ma'lumotlar

маълумотлар

en - data

1 Информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

2 Совокупность заданных величин для основных и производных мер и/или индикаторов.

Примечание – Это определение применительно только в контексте измерения эффективности системы управления информационной безопасностью.

1 Odamning ishtiroki mumkin bo'lgan holda, avtomatik vositalar yordamida, qayta ishlash uchun yaroqli ko'rinishda taqdim etilgan axborot.

2 Asosiy va hosil qilingan me'yorlar va/yoki indikatorlar uchun belgilangan kattaliklar jami.

Izoh – Bu ta'rif faqat axborot xavfsizligini samarali boshqarish tizimi kontekstida qo'llash uchun mo'ljallangan.

1 Odamning ishtiroki mumkin bo'lgan holda, avtomatik vositalar yordamida, qayta ishlash uchun yaroqli ko'rinishda taqdim etilgan axborot.

2 Asosiy va hosil qilingan me'yorlar va/yoki indikatorlar uchun belgilangan kattaliklar jami.

Izoh – Bu ta'rif faqat axborot xavfsizligini samarali boshqarish tizimi kontekstida qo'llash uchun mo'ljallangan.

Данные аутентификационные

uz - autentifikatsion

ma'lumotlar

аутентификацион

маълумотлар

en - authentication data

Информация, используемая для верификации предъявленного идентификатора пользователя.

Foydalanuvchining taqdim etilgan identifikatorini tekshirishda qo'llaniladigan axborot.

Foydalanuvchining taqdim etilgan identifikatorini tekshirishda qo'llaniladigan axborot.

Данные биометрические

uz - biometrik ma'lumotlar

биометрик маълумотлар

en - biometric data

Средства аутентификации, представляющие собой такие персональные отличительные признаки пользователя как тембр голоса, форма кисти руки, отпечатки пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти ЭВМ.

Д

Foydalanuvchining, originallari raqamli ko‘rinishda EHM хотирасида сақланадиган, овоз тембри, qo‘l бармоқларининг шакли, изи ва шулар каби шахсий фарқловчи белгиларини o‘zida ifodalovchi autentifikatsiya qilish vositalari.

Фойдаланувчининг, оригиналлари рақамли кўринишда ЭХМ хотирасида сақланадиган, овоз тембри, қўл бармоқларининг шакли, изи ва шулар каби шахсий фарқловчи белгиларини ўзида ифодаловчи аутентификация қилиш воситалари.

Данные верительные

uz - ishonch ma'lumotlari

ишонч маълумотлари

en - credentials

Данные, передаваемые для установления заявленной подлинности логического объекта.

Mantiqiy obyektning qayd qilingan haqiqiyiligini belgilash uchun uzatiladigan ma'lumotlar.

Мантикий объектнинг қайд қилинган ҳақиқийлигини белгилаш учун узатиладиган маълумотлар.

Данные закрытые

(защищенные)

uz - yopiq (muhofazalangan)

ma'lumotlar

ёпиқ (муҳофазаланган)

маълумотлар

en - private data

Данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой паролей.

Foydalanuvchilarning tor doirasiga mo'ljallangan ma'lumotlar. Qoidaga ko'ra, erkin foydalanishning cheklanishi parollar tizimi orqali amalga oshiriladi.

Фойдаланувчиларнинг тор доирасига мўлжалланган маълумотлар. Қоидага кўра, эркин фойдаланишнинг чекланиши пароллар тизими орқали амалга оширилади.

Данные зашифрованные

uz - shifrlangan ma'lumotlar

шифрланган маълумотлар

en - cipher data

Информация, хранящаяся в памяти ЭВМ в зашифрованном виде, т.е. данные, к которым применен способ криптографической защиты.

Elektron hisoblash mashinasida shifrlangan ko'rinishda saqlanadigan axborot, ya'ni kriptografik muhofaza qilish usullari qo'llanilgan ma'lumotlar.

Электрон ҳисоблаш машинасида шифрланган кўринишда сақланадиган ахборот, яъни криптографик муҳофаза қилиш усуллари қўлланилган маълумотлар.

Данные персональные

1 Сведения о фактах, событиях и обстоятельствах

Д

uz - shaxsiy ma'lumotlar
шахсий маълумотлар
en - personal data

жизни гражданина, позволяющие идентифицировать его личность.

2 Зафиксированная на любом материальном носителе информация о конкретном человеке.

1 Fuqaroning shaxsini identifikatsiya qilish imkonini beruvchi dalillar, voqealar va hayot sharoitlari haqidagi ma'lumotlar.

2 Har qanday moddiy tashuvchida qayd etilgan muayyan odam to'g'risidagi ma'lumot.

1 Fuqaroning shaxsini identifikatsiya qilish imkonini beruvchi dalillar, voqealar va hayot sharoitlari haqidagi ma'lumotlar.

2 Har qanday moddiy tashuvchida qayd etilgan muayyan odam to'g'risidagi ma'lumot.

Данные пользователя

uz - foydalanuvchining
ma'lumotlari
foydalanuvchining
ma'lumotlari
en - user data

Данные для пользователя, которые не влияют на выполнение ФБО.

OXFni bajarishga ta'sir etmaydigan foydalanuvchi uchun ma'lumotlar.

OXFni bajarishga ta'sir etmaydigan foydalanuvchi uchun ma'lumotlar.

Данные проверки безопасности

uz - xavfsizlikni
tekshirish ma'lumotlari
xavfsizlikni
tekshirish ma'lumotlari
en - security audit trail

Данные, которые собраны и могут быть использованы для содействия проведению проверки безопасности.

Xavfsizlikni tekshirishga ko'maklashish maqsadida to'plangan va foydalanilishi mumkin bo'lgan ma'lumotlar

Xavfsizlikni tekshirishga ko'maklashish maqsadida to'plangan va foydalanilishi mumkin bo'lgan ma'lumotlar.

Данные с защитой целостности

uz - yaxlitligi muhofazalangan
ma'lumotlar
yaxlitligi muhofazalangan
ma'lumotlar
en - integrity-protected data

Данные и все соответствующие атрибуты в среде с защитой целостности.

Yaxlitlik muhofazalangan muhitdagi ma'lumotlar va barcha tegishli atributlar.

Yaxlitlik muhofazalangan muhitdagi ma'lumotlar va barcha tegishli atributlar.

uz - maxfiy ma'lumotlar

Закрытые данные, которым присвоен определенный гриф (степень) секретности.

Д

махфий маълумотлар
en - confidential data

Данные теста
uz - test ma'lumotlari
тест маълумотлари
en - test data

**Данные управления
конфигурацией выходные**
uz - konfiguratsiyani boshqarishning chiqish ma'lumotlari
конфигурацияни
бошқаришнинг чиқиш
маълумотлари
en - configuration management
output

Ma'lum bir maxfiylik grifi (darajasi) berilgan yopiq ma'lumotlar.

Маълум бир махфийлик грифи (даражаси) берилган ёпик маълумотлар.

Данные, используемые для контрольной задачи.

Nazorat ishi uchun foydalaniladigan ma'lumotlar.

Назорат иши учун фойдаланиладиган маълумотлар.

Результаты управления конфигурацией, полученные или используемые системой управления конфигурацией.

Примечание – Результатами управления конфигурацией могут быть документы (например, заполненные формуляры, записи системы управления конфигурацией, данные журналов регистрации, выходные данные как на бумажном носителе, так и в электронном виде), а также действия (например, ручное вмешательство, необходимое для выполнения инструкций по управлению конфигурацией). Примерами таких выходных данных управления конфигурацией являются списки конфигурации, планы управления конфигурацией и/или процессы жизненного цикла продукта.

Konfiguratsiyani boshqarish tizimida foydalaniladigan yoki olinadigan konfiguratsiyani boshqarish natijalari.

Izoh – Hujjatlar (masalan, to'ldirilgan formulalar, konfiguratsiyani boshqarish tizimi yozuvlari, ro'yxatga olish jurnallari ma'lumotlari, ham qog'oz shaklida, ham elektron ko'rinishdagi chiqish ma'lumotlari) shuningdek, harakatlar (masalan, konfiguratsiyani boshqarish bo'yicha ko'rsatmalar bajarilishi uchun zarur bo'lgan qo'lda aralashuv) konfiguratsiyani boshqarish natijalari bo'lishi mumkin. Konfiguratsiya ro'yxatlari, konfiguratsiyani boshqarish rejalari va/yoki mahsulot hayotiy sikli jarayonlari konfiguratsiyani boshqarish chiqish ma'lumotlariga misol bo'lib hisoblanadi.

Конфигурацияни бошқариш тизимида фойдаланиладиган ёки олинадиган конфигурацияни бошқариш натижалари.

Изоҳ – Ҳужжатлар (масалан, тўлдирилган формулярлар, конфигурацияни бошқариш тизими ёзувлари, рўйхатга олиш журналлари маълумотлари, ҳам қоғоз шаклида, ҳам электрон кўринишдаги чиқиш маълумотлари) шунингдек,

Д

харакатлар (масалан, конфигурацияни бошқариш бўйича кўрсатмалар бажарилиши учун зарур бўлган қўлда аралашув) конфигурацияни бошқариш натижалари бўлиши мумкин. Конфигурация рўйхатлари, конфигурацияни бошқариш режалари ва ёки маҳсулот ҳаётий цикли жараёнлари конфигурацияни бошқариш чиқиш маълумотларига мисол бўлиб ҳисобланади.

Данные функции безопасности объекта оценки

uz - baholash obyektini xavfsizlik funksiyalarining ma'lumotlari

баҳолаш объекти хавфсизлик функцияларининг маълумотлари

en - target security functions of evaluation data

Данные, необходимые для функционирования объекта оценки, обеспечивающие выполнение ФТБ.

Baholash obyektining ishlashi uchun zarur bo'lgan, FXT bajarilishini ta'minlaydigan ma'lumotlar.

Баҳолаш объектининг ишлаши учун зарур бўлган, ФХТ бажарилишини таъминлайдиган маълумотлар.

Дата и время изменения файла

uz - fayl o'zgartirilgan sana va vaqt

файл ўзгартирилган сана ва вақт

en - data and time stamp

Автоматическая фиксация в заголовке указателя файла даты и времени его создания или последней модификации.

Fayl ko'rsatkichidagi sarlavhada, uni yaratish yoki oxirgi o'zgartirish sanasi hamda vaqtini avtomatik tarzda qayd etish.

Файл кўрсаткичидаги сарлавҳада, уни яратиш ёки охириги ўзгартириш санаси ҳамда вақтини автоматик тарзда қайд этиш.

Действие корректирующее

uz - to'g'rilovchi harakat

тўғриловчи ҳаракат

en - corrective action

Действие, предпринятое для устранения причины обнаруженного несоответствия и предотвращения его повторного возникновения.

Aniqlangan nomuvofiqlik sababini bartaraf etish yoki uning takroran paydo bo'lishining oldini olish uchun amalga oshirilgan ishlar.

Аниқланган номувофиқлик сабабини бартараф этиш ёки унинг такроран пайдо бўлишининг олдини олиш учун амалга оширилган ишлар.

Действие

несанкционированное

uz - ruxsatsiz faoliyat

Действие в нарушение установленных правил.

Belgilangan qoidalarni buzgan holdagi faoliyat.

Д

рухсатсиз фаолият
en - unauthorized action

Действия пользователя
«явные»

uz - foydalanuvchining «ochiq»
harakatlari

фойдаланувчининг
«очик» ҳаракатлари
en - «explicit» user action

Действия пользователя
«скрытые»

uz - foydalanuvchining
«yashirin» harakatlari

фойдаланувчининг
«яширин» ҳаракатлари
en - «convert» user action

Делать заключение

uz - xulosa qilmoq
хулоса қилмоқ

en - determine

Делегирование

uz - vakil qilish
вакил қилиш

Белгиланган қоидаларни бузган ҳолдаги фаолият.

Действия, осуществляемые пользователем, с использованием системных средств.

Foydalanuvchi tomonidan, tizim vositalaridan foydalanib amalga oshiriladigan harakatlar.

Фойдаланувчи томонидан, тизим воситаларидан фойдаланиб амалга ошириладиган ҳаракатлар.

Иные, отличные от «явных», действия, осуществляемые пользователем, в том числе с использованием собственных программ работы с устройствами.

«Oshkor» harakatlardan farq qiluvchi, foydalanuvchi tomonidan, jumladan, qurilmalar bilan ishlash bo'yicha o'z dasturlaridan foydalanib, amalga oshiriladigan harakatlar.

«Ошкор» ҳаракатлардан фарқ қилувчи, фойдаланувчи томонидан, жумладан, қурилмалар билан ишлаш бўйича ўз дастурларидан фойдаланиб, амалга ошириладиган ҳаракатлар.

Подтверждать конкретное заключение, основанное на независимом анализе, выполненном для его получения.

Примечание – В действительности, как правило, при использовании данного термина подразумевается выполнение независимого анализа, при условии, что такой анализ ранее не выполнялся.

Xulosani olish uchun bajarilgan, mustaqil tahlilga asoslangan, aniq xulosani tasdiqlash.

Izoh – Haqiqatda, qoidaga ko'ra, bu atamadan foydalanilganda, bunday tahlil avval bajarilmaganligi sharti bilan, mustaqil tahlil bajarilishi tushuniladi.

Хулосани олиш учун бажарилган, мустақил таҳлилга асосланган, аниқ хулосани тасдиқлаш.

Изоҳ – Ҳақиқатда, қоидага кўра, бу атамадан фойдаланилганда, бундай таҳлил аввал бажарилмаганлиги шarti билан, мустақил таҳлил бажарилиши тушунилади.

Передача полномочия от одного объекта, который владеет данным полномочием, другому объекту.

Д

en - delegation

Vakolatni, ma'lum vakolatga ega bo'lgan obyektдан boshqa obyektga berish.

Ваколатни, маълум ваколатга эга бўлган объектдан бошқа объектга бериш.

Демон

uz - demon

демон

en - demon

Программа, которая незаметно контролирует работу другой программы и время от времени прерывает ее работу, не разрушая саму программу (чаще всего это программа управления периферийными устройствами).

Boshqa dasturning ishini sezdirmay nazorat qiladigan va vaqt-vaqti bilan dasturni (ko'pincha bu periferik (tashqi) qurilmalarni boshqarish dasturi), uning ishini buzmasdan to'xtatadigan dastur.

Бошқа дастурнинг ишини сездирмай назорат қиладиган ва вақт-вақти билан дастурни (кўпинча бу периферик (ташқи) қурилмаларни бошқариш дастури), унинг ишини бузмасдан тўхтатадиган дастур.

Демонстрировать

uz - namoyish etmoq

намоёйиш этмоқ

en - demonstrate

Предоставлять заключение по результатам анализа, менее строгое, чем «доказательство».

Tahlil natijalari bo'yicha, «dalil»ga nisbatan kamroq qat'iy xulosalarni taqdim etish.

Таҳлил натижалари бўйича, «далил»га нисбатан камроқ қатъий хулосаларни тақдим этиш.

Депонирование ключей

uz - kalitlarni saqlash

uchun topshirish

калитларни сақлаш

учун топшириш

en - key escrow

Процесс депонирования ключей, заключающийся в разбиении криптографического ключа на две части, каждая из которых шифруется и передается на хранение доверенным правительственным организациям, обеспечивающим надежное хранение ключевых компонентов в течении срока их действия. Эти компоненты позволяют службам, отвечающим за национальную безопасность, восстанавливать уникальные ключи и выполнять расшифрование сообщений.

Kriptografik kalitlarni ikki qismga ajratib, kalitlarni saqlash uchun topshirish jarayoni, ularning har biri

Д

shifrlanadi va kalit komponentlari, amal qilish muddati davomida ishonchli saqlashni ta'minlovchi ishonchli hukumat tashkilotlariga saqlash uchun topshiriladi. Bu komponentlar milliy xavfsizlik uchun javobgar xizmatlarga noyob kalitlarni tiklash va xabarlarini rasshifrovka qilish imkonini beradi.

Криптографик калитларни икки қисмга ажратиб, калитларни сақлаш учун топшириш жараёни, уларнинг ҳар бири шифрланади ва калит компонентлари, амал қилиш мuddати давомида ишончли сақлашни таъминловчи ишончли ҳукумат ташкilotларига сақлаш учун топширилади. Бу компонентлар миллий хавфсизлик учун жавобгар хизматларга ноёб калитларни тиклаш ва хабарларни расшифровка қилиш имконини беради.

Схематический рисунок модулей системы, на котором показаны вызовы между этими модулями.

Tizim modullarining, shu modullar o'rtasidagi chaqiruvlar ko'rsatilgan sxematik rasmi.

Тизим модулларининг, шу модуллар ўртасидаги чақирувлар кўрсатилган схематик расми.

Схема цифровой подписи, базирующаяся на одноразовых сигнатурах и хэш-функции. Применяется для устранения недостатков схемы одноразовых подписей. Позволяет отказаться от генерации ключевой пары для каждого нового сообщения.

Bir martali signaturalar va xesh-funksiyaga asoslanadigan raqamli imzo sxemasi. Bir martali imzolar sxemasidagi kamchiliklarni bartaraf qilish uchun qo'llaniladi. Har bir yangi xabar uchun kalit juftini generatsiyalashdan voz kechish imkonini beradi.

Бир мартали сигнатуралар ва хэш-функцияга асосланадиган рақамли имзо схемаси. Бир мартали имзолар схемасидаги камчиликларни барта- раф қилиш учун қўлланилади. Ҳар бир янги хабар учун калит жуфтини генерациялашдан воз кечиш имконини беради.

Дерево вызовов

uz - chaqiruvlar daraxti

чақирувлар дарахти

en - call tree

«Дерево» Меркля

uz - Merkl «daraxti»

Меркл «дарахти»

en - Merkle's tree

Д

Дескриптор

uz - deskriptor

дескриптор

en - descriptor

Элемент информационной структуры, который описывает форму или содержание данных, например, дескриптор сигнатуры – описатель последовательности данных на диске, можно использовать для проверки данных на диске.

Ma'lumotlarning shakli yoki mazmunini tavsiflovchi axborot strukturasi elementi, masalan, signatura deskriptori – diskdagi ma'lumotlar ketma-ketligini tavsiflovchidan diskdagi ma'lumotlarni tekshirishda foydalanish mumkin.

Ma'lumotlarning shakli va mazmunini tavsiflovchi axborot strukturasi elementi, masalan, signatura deskriptori – diskdagi ma'lumotlar ketma-ketligini tavsiflovchidan diskdagi ma'lumotlarni tekshirishda foydalanish mumkin.

Дескриптор безопасности

uz - xavfsizlik deskriptori

хавфсизлик дескриптори

en - security descriptor

Атрибут объекта, содержащий информацию для системы безопасности. Включает идентификатор безопасности владельца объекта, дискреционный и системный список контроля доступа.

Xavfsizlik tizimi uchun axborotga ega bo'lgan obyekt atributi. Obyekt egasining xavfsizlik identifikatorini, erkin foydalanishni nazorat qilishning diskretion va tizimga oid ro'yxatlarini o'z ichiga oladi.

Xavfsizlik tizimi uchun axborotga ega bo'lgan obyekt atributi. Obyekt egasining xavfsizlik identifikatorini, erkin foydalanishni nazorat qilishning diskretion va tizimga oid ro'yxatlarini o'z ichiga oladi.

Дешифратор

uz - deshifrator

дешифратор

en - decoder

Логическая схема, преобразующая поразрядное входное двоичное слово (шифр, код) в единственный сигнал на одном из $2n$ выходов этой схемы.

Razryadma razryad kiruvchi ikkilik so'z (shifr, kod) ni sxemaning $2n$ chiqish uchlarining birida birlik signalga o'zgartiruvchi mantiqiy sxema.

Разрядма разряд кирувчи иккилик сўз (шифр, код)ни схеманинг $2n$ чиқиш учларининг бирида бирлик сигналга ўзгартирувчи мантикий схема.

Д

Дешифратор адреса

uz - adres deshifratori

адрес дешифратори

en - address decoder

Дешифрование

uz - deshifrlash

дешифрлаш

en - decryption, decipherment

Деятельность в сфере программного обеспечения незаконная

uz - dasturiy ta'minot

sohasidagi noqonuniy faoliyat

дастурий таъминот

sohasidagi noqonuniy

фаолият

en - software piracy

Преобразователь адреса в управляющие сигналы, направляемые запоминающему устройству.

Adresni, xotirlovchi qurilmaga yuborilayotgan boshqaruvchi signallarga o'zgartirgich.

Адресни, хотирловчи қурилмага юборилаётган бошқарувчи сигналларга ўзгартиргич.

1 Процесс получения из шифротекста соответствующих исходных данных.

Примечание – Шифротекст может быть зашифрован вторично, в этом случае при первом дешифровании исходный открытый текст не может быть восстановлен.

2 Процесс, противоположный шифрованию и связанный с восстановлением исходного текста из зашифрованного при отсутствии ключа шифрования.

1 Shifrmatndan tegishli dastlabki ma'lumotlarni olish jarayoni.

Izoh – Shifrmatn takroran shifrlanishi mumkin, bunda birinchi deshifrlashda dastlabki ochiq matn tiklanmaydi.

2 Shifrlashga qarama-qarshi va shifrlash kaliti mavjud bo'lmaganda, shifrlangan matndan dastlabki matnni tiklash bilan bog'liq jarayon.

1 Шифрланган матндан тегишли дастлабки маълумотларни олиш жараёни.

Изоҳ – Шифрматн такроран шифрланиши мумкин, бунда биринчи дешифрлашда дастлабки очик матн тикланмайди.

2 Шифрлашга қарама-қарши ва шифрлаш калити мавжуд бўлмаганда, шифрланган матндан дастлабки матнни тиклаш билан боғлиқ жараён.

Непредусмотренная документами деятельность лиц, заключающаяся в копировании и распространении программного обеспечения без соответствующей лицензии.

Shaxslarning hujjatlar bilan ko'zda tutilmagan faoliyati bo'lib, tegishli litsenziyasiz dasturiy ta'minotdan nusxa olish va tarqatishda ifodalanadi.

Шахсларнинг ҳужжатлар билан кўзда тутилмаган фаолияти бўлиб, тегишли лицензиясиз дастурий

Д

таъминотдан нусха олиш ва тарқатишда ифодалангани.

Директория

uz - direktoriya

директория

en - directory

Список всех файлов, размещаемых на диске с указанием имени и местонахождения.

Diskda nomi va joylashgan o'rnini ko'rsatib joylashtiriladigan barcha fayllar ro'yxati.

Дискда номи ва жойлашган ўрни кўрсатиб жойлаштирилган барча файллар рўйхати.

Диск основной

uz - asosiy disk

асосий диск

en - key disk

Диск, который необходим для запуска программного продукта на выполнение по частям. Такой диск дает гарантию, что программный продукт адекватен законному оригиналу и не является копией.

Dasturiy mahsulotni qismlarga bo'lib bajarishda ishga tushirish uchun zarur disk. Bunday disk dasturiy mahsulot qonuniy original bilan bir xilligiga, uning nusxasi emasligiga kafolat beradi.

Дастурий маҳсулотни қисмларга бўлиб бажаришда ишга тушириш учун зарур диск. Бундай диск дастурий маҳсулот қонуний оригинал билан бир хиллигига, унинг нусхаси эмаслигига кафолат беради.

Диспетчер доступа, ядро защиты

uz - foydalana olish dispetcheri, muhofaza qilish yadrosi

фойдалана олиш диспетчери, муҳофаза қилиш ядроси

en - reference monitor

1 Защищенная от внешних воздействий совокупность программных и аппаратных средств контроля доступа субъектов к информационным ресурсам в соответствии с установленными правилами.

2 Аппаратные, программные и программно-аппаратные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

1 Belgilangan qoidalarga muvofiq, subyektlarning axborot resurslaridan foydalana olishini nazorat qilishning tashqi ta'sirlardan muhofazalangan dasturiy va apparat vositalarining jami.

2 Foydalana olish dispetcheri konsepsiyasini amalga oshiruvchi muhofaza qilish vositalari kompleksining apparat, dasturiy va dasturiy-apparat elementlari.

Д

1 Белгиланган қоидларга мувофиқ, субъектларнинг ахборот ресурсларидан фойдалана олишини назорат қилишнинг ташқи таъсирлардан муҳофазаланган дастурий ва аппарат воситаларининг жами.

2 Фойдалана олиш диспетчери концепциясини амалга оширувчи муҳофаза қилиш воситалари комплексининг аппарат, дастурий ва дастурий-аппарат элементлари.

Диффейсмент

uz - difeysment

диффейсмент

en - defacement

Искажение веб-страниц. Вид

компьютерного ван-дализма, иногда являющийся для злоумышленника забавой, а иногда средством выражения политических пристрастий.

Примечание – Искажения могут производиться в какой-то части сайта или выражаться в полной замене существующих на сайте страниц (чаще всего, стартовой страницы).

Veb-sahifani buzish. Ayrim hollarda jinoyatkorga ermak uchun, ayrim paytlarda esa siyosiy g‘arazgo‘ylikni ko‘rsatish vositasi hisoblanadigan, kompyuter vandalizm turi.

Izoh – Buzilishlar saytning biron-bir qismida bo‘ladi yoki sayt sahifalarini (ko‘proq, start sahifani) butunlay almashtirishda ko‘rinadi.

Веб-саҳифани бузиш. Айрим ҳолларда жинояткорга эрмак учун, айрим пайтларда эса сиёсий ғаразгўйликни кўрсатиш воситаси ҳисобланадиган, компьютер вандализм тури.

Изоҳ – Бузилишлар сайтнинг бирон-бир қисмида бўлади ёки сайт саҳифаларини (кўпроқ, старт саҳифани) бутунлай алмаштиришда кўринади.

Доверие

uz - ishonch

ишонч

en - assurance

Основание для уверенности в том, что объект оценки соответствует политике функции безопасности.

Baholash obykti xavfsizlik funksiyasi siyosatiga mos kelishi to‘g‘risida ishonch uchun asos.

Баҳолаш объекти хавфсизлик функцияси сиёсатиға мос келиши тўғрисида ишонч учун

Д

Доверие к информации

uz - axborotga bo'lgan ishonch

ахборотга бўлган ишонч

en - assurance to information

асос.

Отсутствие в информации подмены (несанкционированной модификации ее элементов при сохранении целостности).

Ахборотда алмасhtиришларнинг (yaхлитлик saқланishi uchun axborot elementlarini ruхsatsiz o'zgartirishning) bo'lmasligi.

Ахборотда алмаштиришларнинг (yaхлитлик saқланиши uchun axborot elementlarini ruхsatsiz ўzгaртиришнинг) бўлмаслиги.

Доверенная компьютерная система

uz - ishonchli kompyuter tizimi

ишончли компьютер

тизими

en - trusted computer system

Система обработки данных, в которой предусмотрена достаточная компьютерная безопасность с учетом возможности одновременного доступа пользователей к данным с разными грифами секретности и категориями безопасности.

Foydalanuvchilarning turli maxfiylik griflari va xavfsizlik kategoriyalariga ega bo'lgan ma'lumotlardan bir vaqtda foydalana olish imkoniyati hisobga olingan holda, yetarlicha kompyuter xavfsizligi ko'zda tutilgan, ma'lumotlarni qayta ishlash tizimi.

Фойдаланувчиларнинг турли махфийлик грифлари ва хавфсизлик категорияларига эга бўлган маълумотлардан бир вақтда фойдалана олиш имконияти ҳисобга олинган ҳолда, етарлича компьютер хавфсизлиги кўзда тutilган, маълумотларни қайта ишлаш тизими.

Доказательство

uz - dalil

далил

en - evidence

Информация, которая сама по себе или при использовании вместе с другой информацией, может применяться для разрешения спора.

Примечания

1 Конкретными формами доказательств являются цифровые подписи, защитные оболочки и маркеры безопасности.

2 Цифровые подписи используются вместе с методами открытых ключей, тогда как защитные оболочки и маркеры безопасности применяются вместе с методами секретных ключей.

Д

O‘zicha yoki boshqa axborot bilan birga foydalanilganda, bahsni hal qilish uchun qo‘llanilishi mumkin bo‘lgan axborot.

Izohlar

1 Raqamli imzolar, himoya qobiqlari va xavfsizlik markerlari dalilning aniq ko‘rinishlari hisoblanadi.

2 Raqamli imzolaridan ochiq kalitlar metodlari bilan birga foydalaniladi, himoya qobiqlari va xavfsizlik markerlari esa, maxfiy kalitlar metodlari bilan birga qo‘llaniladi.

Ўзича ёки бошқа ахборот билан бирга фойдаланилганда, бахсни ҳал қилиш учун қўлланилиши мумкин бўлган ахборот.

Изоҳлар

1 Рақамли имзолар, ҳимоя қобиклари ва хавфсизлик маркерлари далилнинг аниқ кўринишлари ҳисобланади.

2 Рақамли имзолардан очик калитлар методлари билан бирга фойдаланилади, ҳимоя қобиклари ва хавфсизлик маркерлари эса, махфий калитлар методлари билан бирга қўлланилади.

Доказывать

uz - isbot qilmoq

исбот қилмоқ

en - prove

Демонстрировать соответствие посредством формального анализа в его математическом смысле.

Matematik ma'noda formal tahlil vositasida muvofqlikni namoyon qilish.

Математик маънода формал таҳлил воситасида мувофиқликни намоён қилиш.

Документация по

управлению конфигурацией

uz - konfiguratsiyani boshqarish bo'yicha hujjatlar

конфигурацияни

бошқариш бўйича ҳужжатлар

en - configuration management usage documentation

Часть системы управления конфигурацией, содержащая описание системы управления конфигурацией и руководство по ее использованию, например, справочники, инструкции и/или документация инструментальных средств и процедур.

Konfiguratsiyani boshqarish tizimining, konfiguratsiyani boshqarish tizimining tavsifini va undan foydalanish bo'yicha qo'llanmani, masalan, ma'lumotnomalar, yo'riqnomalar va/yoki instrumental vositalar hujjatlari va protseduralarini tavsiflaydigan qismi.

Конфигурацияни бошқариш тизимининг, конфи-

Д

гурацияни бошқариш тизимининг тавсифини ва ундан фойдаланиш бўйича қўлланмани, масалан, маълумотномалар, йўриқномалар ва ёки инструментал воситалар ҳужжатлари ва процедураларини тавсифлайдиган қисми.

Документация УК

uz - KB hujjat

КБ ҳужжат

en - CM documentation

Комплект документации УК, включающий входные данные УК, список УК (список конфигурации), записи системы УК, план УК и документация по использованию УК.

КВ kirish ma'lumotlarini, КВ ro'yxati (konfiguratsiya ro'yxati)ni, КВ tizimi yozuvlarini, КВ rejasi va KBdan foydalanish bo'yicha hujjatlarni o'z ichiga oladigan KB hujjatlar komplekti.

КБ кириш маълумотларини, КБ рўйхати (конфигурация рўйхати)ни, КБ тизими ёзувларини, КБ режаси ва КБдан фойдаланиш бўйича ҳужжатларни ўз ичига оладиган КБ ҳужжатлар комплекти.

Документы руководящие

uz - rahbariy hujjatlar

раҳбарий ҳужжатлар

en - guidance documentation

Документы, в которых описаны поставка, технологическая подготовка, эксплуатация, управление и/или использование объекта оценки.

Baholash obyektini yetkazib berish, texnologik tay-yorgarlik, ekspluatatsiya qilish, boshqarish va/yoki undan foydalanish tavsiflangan hujjatlar.

Баҳолаш объектини етказиб бериш, технологик тайёргарлик, эксплуатация қилиш, бошқариш ва ёки ундан фойдаланиш тавсифланган ҳужжатлар.

Домен

uz - domen

домен

en - domain

1 Уникальный контекст (например, параметры контроля доступа) исполнения программы, множество объектов, к которым субъект может иметь доступ. Имеет иерархическую структуру.

2 Группа компьютеров, которая использует общий список учетных записей, хранящийся на контроллерах домена.

Д

1 Subyekt foydalana olishi mumkin bo'lgan ko'plab obyektlarning dasturlarini bajarishning noyob konteksti (masalan, erkin foydalanishni nazorat qilish parametrlari). Iyerarxik strukturaga ega.

2 Domen kontrollerlarida saqlanadigan hisobga olinadigan yozuvlarning umumiy ro'yxatidan foydalanadigan kompyuterlar guruhi.

1 Субъект фойдалана олиши мумкин бўлган кўплаб объектларнинг дастурларини бажаришнинг ноёб контексти (масалан, эркин фойдаланишни нazorat қилиш параметрлари). Иерархик структурага эга.

2 Домен контроллерларида сақланадиган ҳисобга олинадиган ёзувларнинг умумий рўйхатидан фойдаланадиган компьютерлар гуруҳи.

Домен безопасности

uz - xavfsizlik domeni

хавфсизлик домени

en - security domain

1 Совокупность пользователей, систем или ресурсов, подчиняющихся единой политике безопасности и единой администрации безопасности.

2 Совокупность ресурсов, к которым активный логический объект имеет право доступа.

1 Yagona xavfsizlik siyosatiga va yagona xavfsizlik ma'muriyatiga bo'ysunuvchi foydalanuvchilar, tizimlar yoki resurslar jami.

2 Aktiv mantiqiy obyekt foydalana olish huquqiga ega resurslar yig'indisi.

1 Ягона хавфсизлик сиёсатига ва ягона хавфсизлик маъмуриятига бўйсунувчи фойдаланувчилар, тизимлар ёки ресурслар жами.

2 Актив мантиқий объект фойдалана олиш ҳуқуқига эга ресурслар йиғиндиси.

Допуск

uz - ruxsat berish

рухсат бериш

en - clearance

Разрешение, выданное лицу на право доступа к данным или информации заданного или более низкого уровня безопасности.

Shaxsga, darajasi belgilangan yoki birmuncha past bo'lgan xavfsizlik ma'lumotlari yoki axborotdan foydalana olish huquqiga berilgan ruxsat.

Д

Шахсга, даражаси белгиланган ёки бирмунча паст бўлган хавфсизлик маълумотлари ёки ахборотдан фойдалана олиш ҳуқуқига берилган рухсат.

Дорожка дополнительная

uz - qo‘shimcha yo‘lka

қўшимча йўлка

en - extra track

Часть метода защиты от копирования, когда на диск сверх стандартного количества дорожек записывается еще одна дорожка.

Nusxa ko‘chirishdan himoya qilish metodining qismi, bunda diskka standart miqdordagi yo‘lkalar ustidan yana bitta yo‘lka yoziladi.

Нусха кўчиришдан ҳимоя қилиш методининг қисми, бунда дискка стандарт миқдордаги йўлкалар устидан яна битта йўлка ёзилади.

Дорожка смещённая

uz - siljigan yo‘lka

силжиган йўлка

en - offset track

Часть метода защиты от копирования, когда дорожка на диск записывается в нестандартную позицию.

Nusxa ko‘chirishdan himoya qilish metodining qismi, bunda diskdagi yo‘lka nostandard pozitsiyaga yoziladi.

Нусха кўчиришдан ҳимоя қилиш методининг қисми, бунда дискдаги йўлка ностандарт позицияга ёзилади.

Дорожка спиральная

uz - spiral yo‘lka

спираль йўлка

en - spiral track

Часть метода защиты от копирования, когда на диск записывается дорожка спиральной формы.

Nusxa ko‘chirishdan himoya qilish metodining qismi, bunda diskka spiral shaklidagi yo‘lka yoziladi.

Нусха кўчиришдан ҳимоя қилиш методининг қисми, бунда дискка спираль шаклидаги йўлка ёзилади.

Дорожка широкая

uz - keng yo‘lka

кенг йўлка

en - wide track

Часть метода защиты от копирования, когда в две или более смежных дорожек на диске записаны одни и те же данные.

Nusxa ko‘chirishdan himoya qilish metodining qismi, bunda diskdagi ikki yoki undan ortiq yonma-yon yo‘lkaga aynan bir xil ma’lumotlar yoziladi.

Д

Нусха кўчиришдан ҳимоя қилиш методининг қисми, бунда дискдаги икки ёки ундан ортиқ ёнма-ён йўлгага айнан бир хил маълумотлар ёзилади.

Доска сообщений

uz - xabarlar taxtasi

хабарлар тахтаси

en - bulletin board

Часть вычислительной системы, реализующая функции электронной почты по рассылке и сбору сообщений.

Hisoblash tizimining, xabarlarini tarqatish va yig'ish bo'yicha elektron pochta funksiyasini amalga oshiruvchi qismi.

Ҳисоблаш тизимининг, хабарларни тарқатиш ва йиғиш бўйича электрон почта функциясини амалга оширувчи қисми.

Достоверность

uz - ishonchlilik

ишончлилиқ

en - authenticity, reliability, validity, adequacy

1 Идентичность объекта защиты заявленному.

2 Степень соответствия данных, хранимых в памяти ЭВМ или документах, реальному состоянию отображаемых ими объектов предметной области.

3 Свойство соответствия предусмотренному поведению или результату.

4 Свойство данных на выходе системы соответствовать данным, поступившим на ее вход.

1 Muhofaza obyektining mavjud obyektga o'xshashligi.

2 Elektron hisoblash mashinalarining xotirasida yoki hujjatlarda saqlanadigan ma'lumotlarning, ular aks ettiradigan predmet sohaning haqiqiy holatiga mos kelish darajasi.

3 Ko'zda tutilgan munosabat yoki natijaga muvofiqlik xususiyati.

4 Tizim chiqishidagi ma'lumotlar xususiyatini uning kirishiga kelgan ma'lumotlarga mos kelish xususiyati.

1 Муҳофаза объектининг мавжуд объектга ўхшашлиги.

2 Электрон ҳисоблаш машиналарининг хотира-сида ёки ҳужжатларда сақланадиган маълумотларнинг, улар акс эттирадиган предмет соҳанинг ҳақиқий ҳолатига мос келиш даражаси.

3 Кўзда тутилган муносабат ёки натижага муво-

Д

фиклик хусусияти.

4 Тизим чиқишидаги маълумотлар хусусиятини унинг киришига келган маълумотларга мос келиш хусусияти.

Достоверность информации

uz - axborotning

ishonchliligi

ахборотнинг

ишончлилиги

en - information actuality,

information integrity

Оценка вероятности отсутствия ошибок в информации.

Axborotda xatoning bo'lmashlik ehtimolligini baholash.

Ахборотда хатонинг бўлмаслик эҳтимоллигини баҳолаш.

Достоверность обработки информации

uz - axborotni qayta ishlash

ishonchliligi

ахборотни қайта ишлаш

ишончлилиги

en - data processing validity

Функция вероятности ошибки, т.е. события, состоящего в том, что информация в системе не совпадает в пределах заданной точности с некоторым ее истинным значением.

Xato ehtimolligi funksiyasi, ya'ni tizimdagi axborot berilgan aniqlik chegarasida axborotning ba'zi haqiqiy qiymati bilan mos tushmasligida ifodalanadigan hodisalar.

Хато эҳтимоллиги функцияси, яъни тизимдаги ахборот берилган аниқлик чегарасида ахборотнинг баъзи ҳақиқий қиймати билан мос тушмаслигида ифодаланадиган ҳодисалар.

Достоверность передачи информации

uz - axborotni uzatishning

ishonchliligi

ахборотни узатишнинг

ишончлилиги

en - data transmission validity

Соответствие принятой информации переданной.

Qabul qilingan axborotning uzatilgan axborotga mos kelishi.

Қабул қилинган ахборотнинг узатилган ахборотга мос келиши.

Достоверность функциональная

uz - funksional ishonchlik

функционал ишончлилик

en - functional reliability

Свойство соответствия безопасности некоторым критериям, определяемым, например, политикой безопасности.

Xavfsizlikning ba'zi kriteriyalarga, masalan, xavfsizlik siyosati bilan belgilanadigan kriteriyalarga mos kelishi xususiyati.

Д

Хавфсизликнинг баъзи критерийларга, масалан, хавфсизлик сиёсати билан белгиланадиган критерийларга мос келиши хусусияти.

Доступ

uz - foydalana olish

фойдалана олиш

en - access

1 Специальный тип взаимодействия между субъектом и объектом, в результате которого создается поток информации от одного к другому.

2 Запрос процесса на открытие объекта для последующего выполнения над ним операций определенного типа.

1 Subyekt va obyekt o'rtasidagi o'zaro hamkorlikning maxsus turi, uning natijasida ularning biridan ikkinchisiga o'tuvchi axborot oqimi paydo bo'ladi.

2 Ma'lum turdagi operatsiyalarni keyinchalik bajarish uchun obyektning ochilishiga so'rov jarayoni.

1 Субъект ва объект ўртасидаги ўзаро ҳамкорликнинг махсус тури, унинг натижасида уларнинг биридан иккинчисига ўтувчи ахборот оқи-ми пайдо бўлади.

2 Маълум турдаги операцияларни кейинчалик бажариш учун объектнинг очилишига сўров жараёни.

Доступ алгоритмический

uz - algoritmik foydalana olish

алгоритмик фойдалана олиш

en - algorithmic access

Доступ, основанный на вычислении адреса по некоторому алгоритму.

Qandaydir algoritm bo'yicha adresni hisoblashga asoslangan foydalana olish.

Қандайдир алгоритм бўйича адресни ҳисоблашга асосланган фойдалана олиш.

Доступ групповой (коллективный)

uz - guruh (jamo'a) bo'lib foydalana olish

гурух (жамоа) бўлиб фойдалана олиш

en - shared access

Совместное использование вычислительной системы двумя или более пользователями в пакетном или интерактивном режимах.

Ikki yoki undan ko'p foydalanuvchining paketli yoki interaktiv rejimda hisoblash tizimidan birgalikda foydalanishi.

Д

Икки ёки ундан кўп фойдаланувчининг пакетли ёки интерактив режимда ҳисоблаш тизимидан биргаликда фойдаланиши.

Доступ дискреционный (избирательный)

uz - diskretsiyon (tanlab)

foydalana olish

дискрецион (танлаб)

фойдалана олиш

en - discretionary (selective)

access

Метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Управление является избирательным в том смысле, что субъект с определенными правами может осуществлять передачу прав любому объекту независимо от установленных ограничений (доступ может быть осуществлен и не напрямую).

Foydalanuvchi, jarayon va/yoki u tegishli bo'lgan guruhni identifikatsiya qilish va tanishga asoslangan, obyektlardan tizim subyektlarining erkin foydalanishini boshqarish metodi. Ma'lum huquqlarga ega subyekt istalgan obyektga, belgilangan cheklashlardan qat'i nazar, huquqlarni berishni amalga oshirishi mumkin bo'lganda, boshqaruv saylanma hisoblanadi (foydalana olish – bevosita bo'lmagan tarzda ham amalga oshirilishi mumkin).

Фойдаланувчи, жараён ва/ёки у тегишли бўлган гуруҳни идентификация қилиш ва танишга асосланган, объектлардан тизим субъектларининг эркин фойдаланишини бошқариш методи. Маълум ҳуқуқларга эга субъект исталган объектга, белгиланган чеклашлардан қатъи назар, ҳуқуқларни беришни амалга ошириши мумкин бўлганда, бошқарув сайланма ҳисобланади (фойдалана олиш – бевосита бўлмаган тарзда ҳам амалга оширилиши мумкин).

Доступ к информации

uz - axborotdan foydalana olish

ахборотдан фойдалана

олиш

en - access to information

1 Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

2 Процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.

Д

1 Axborot bilan tanishish, uni qayta ishlash, xususan, axborotdan nusxa ko‘chirish, o‘zgartirish yoki yo‘q qilish.

2 Axborot bilan tanishish jarayoni, uni shtat texnik vositalaridan foydalanib, hujjatlashtirish, o‘zgartirish yoki yo‘q qilish.

1 Ахборот билан танишиш, уни қайта ишлаш, хусусан, ахборотдан нусха кўчириш, ўзгартириш ёки йўқ қилиш.

2 Ахборот билан танишиш жараёни, уни штат техник воситаларидан фойдаланиб, ҳужжатлаштириш, ўзгартириш ёки йўқ қилиш.

Доступ к информации несанкционированный

uz - axborotdan ruxsatsiz foydalana olish

ахборотдан рухсатсиз фойдалана олиш

en - unauthorized access to information

Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Примечание – Под штатными средствами понимается совокупность программного, программно-аппаратного и аппаратного обеспечения средств вычислительной техники или автоматизированных систем.

Hisoblash texnikasi yoki avtomatlashtirilgan tizim vositalari taqdim etadigan shtat vositalaridan foydalanib, foydalana olishni belgilash qoidalarini buzuvchi axborotdan foydalana olish.

Izoh – Shtat vositalari deganda, hisoblash texnikasi yoki avtomatlashtirilgan tizim vositalarining dasturiy, dasturiy-apparat va apparat ta’minoti majmui tushuniladi.

Ҳисоблаш техникаси ёки автоматлаштирилган тизим воситалари тақдим этадиган штатдаги воситаларидан фойдаланиб, фойдалана олишни белгилаш қоидаларини бузувчи ахборотдан фойдалана олиш.

Изоҳ – Штат воситалари деганда, ҳисоблаш техникаси ёки автоматлаштирилган тизим воситаларининг дастурий, дастурий-аппарат ва аппарат таъминоти мажмуи тушунилади.

Д

Доступ к информации
санкционированный

uz - axborotdan ruxsat etilgan
tarzda foydalana olish

ахборотдан рухсат этил-
ган тарзда фойдалана олиш

en - authorized access to
information

**Доступ к
информационному ресурсу**

uz - axborot resursidan
foydalana olish

ахборот ресурсидан
фойдалана олиш

en - access to information
resource

**Доступ к сведениям,
составляющим
государственные секреты**
uz - davlat siri bo'lgan ma'lumotlardan foydalana olish

давлат сирини бўлган
маълумотлардан фойдалана
олиш

en - access to state secret
information

**Доступ к секретной
информации
несанкционированный**
uz - maxfiy axborotdan ruxsat
etilmagan tarzda foydalana olish

махфий ахборотдан рухсат
этилмаган тарзда фойдалана
олиш

en - unauthorized access to

Доступ к информации, не нарушающий установленные правила разграничения доступа.

Belgilangan erkinfoydalanishni cheklash qoidalari buzilmaydigan tarzda axborotdan foydalana olish.

Белгиланган эркинфойдаланишни чеклаш қоидалари бузилмайдиган тарзда ахборотдан фойдалана олиш.

Получение субъектом доступа возможности манипулировать (использовать, управлять, изменять характеристики и т.п.) данным информационным ресурсом.

Subyektning ma'lum bir axborot resursi bilan manipulyatsiya qilish (foydalanish, boshqarish, xarakteristikalarini o'zgartirish va sh.k.) imkoniyatiga ega bo'lishi.

Субъектнинг маълум бир ахборот ресурси билан манипуляция қилиш (фойдаланиш, бошқариш, характеристикаларини ўзгартириш ва ш.к.) имкониятига эга бўлиши.

Санкционированное полномочным должностным лицом фактическое ознакомление конкретного лица со сведениями, составляющими государственные секреты.

Vakolatli mansabdor shaxs tomonidan ruxsat etilgan tarzda, muayyan shaxsni davlat siri bo'lgan ma'lumotlar bilan tanishtirish.

Ваколатли мансабдор шахс томонидан рухсат этилган тарзда, муайян шахсни давлат сирини бўлган маълумотлар билан таништириш.

Получение секретных сведений лицами, не имеющими права доступа к этим сведениям.

Maxfiy ma'lumotlardan foydalana olish huquqiga ega bo'lmagan shaxslar tomonidan maxfiy ma'lumotlarning olinishi.

Махфий маълумотлардан фойдалана олиш ҳуқуқига эга бўлмаган шахслар томонидан махфий маълумотларнинг олинishi.

Д

secret information

Доступ к файлу

uz - faylga kira olish

файлга кира олиш

en - file access

Просмотр, модификация, замена или удаление файла, а также просмотр и манипулирование его атрибутами.

Faylni ko‘rib chiqish, o‘zgartirish, almashtirish yoki o‘chirib tashlash, shuningdek, uning atributlarini ko‘rib chiqish va ularni manipulyatsiya qilish.

Файлни кўриб чиқиш, ўзгартириш, алмаштириш ёки ўчириб ташлаш, шунингдек, унинг атрибутларини кўриб чиқиш ва уларни манипуляция қилиш.

Доступ мандатный

uz - mandatli foydalana

olish

мандатли фойдалана

олиш

en - mandatory access

Способ управления доступом к объектам, основанный на степени секретности или критичности информации (представленной специальными метками), содержащейся в объекте и формальной проверке полномочий и прав субъекта при доступе к информации данного уровня критичности.

Примечание – Мандатное управление доступом подразумевает, что:

– все субъекты и объекты системы однозначно идентифицированы;

– каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

– каждому объекту системы присвоен базовый уровень безопасности (уровень прозрачности), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

Obyektlardan foydalana olishni boshqarish usuli. Obyektda mavjud bo‘lgan axborotning maxfiylik yoki kritiklik darajasiga, ma’lum bir kritiklik darajasidagi axborotdan foydalana olishda subyektning vakolatlari va huquqlarini rasman tekshirishga asoslangan.

Izoh – Foydalana olishni mandatli boshqarish:

– tizimning barcha subyektlari va obyektlari bir xil identifikatsiya qilinganligini;

– tizimning har bir obyektiga, undagi axborotning qiymatini belgilovchi kritiklik belgisi berilganligini;

– tizimning har bir obyektiga subyekt foydalana olishi mumkin bo‘lgan obyektlar kritiklik belgisining maksimal

Д

qiymatini oʻrnatuvchi bazaviy xavfsizlik darajasi berilishini nazarda tutadi.

Объектлардан фойдалана олишни бошқариш усули. Объектда мавжуд бўлган ахборотнинг махфийлик ёки критиклик даражасига, маълум бир критиклик даражасидаги ахборотдан фойдалана олишда субъектнинг ваколатлари ва ҳуқуқлари-ни расман текширишга асосланган.

Изоҳ – Фойдалана олишни мандатли бошқариш:

– тизимнинг барча субъектлари ва объектлари бир хил идентификация қилинганлигини;

– тизимнинг ҳар бир объектига, ундаги ахборотнинг қийматини белгиловчи критиклик белгиси берилганлигини;

– тизимнинг ҳар бир объектига субъект фойдалана олиши мумкин бўлган объектлар критиклик белгисининг максимал қийматини ўрнатувчи базавий хавфсизлик даражаси берилишини назарда тутати.

Доступ мошеннический

uz - firibgarlik orqali

foydalana olish

фирибгарлик орқали

фойдалана олиш

en - fraud access

Несанкционированное использование услуг сотовой связи путем перепрограммирования серийных номеров сотовых аппаратов.

Sotali apparatlarning seriya raqamlarini qayta dasturlash yoʻli bilan sotali aloqa xizmatlaridan ruxsat etilmagan tarzda foydalanish.

Сотали аппаратларнинг серия рақамларини қайта дастурлаш йўли билан сотали алоқа хизматларидан рухсат этилмаган тарзда фойдаланиш.

Доступ на запись

uz - yozib olishga ruxsat

ёзиб олишга рухсат

en - write access

Право на доступ, при получении которого разрешается записывать данные.

Примечание – Доступ на запись является разрешением на дополнение, модификацию, удаление или создание данных.

Maʼlumotlarni yozib olish uchun ruxsat beradigan foydalana olish huquqi.

Izoh – Yozib olishga ruxsat maʼlumotlarni toʻldirish, oʻzgartirish, oʻchirish yoki yaratishga ruxsat hisoblanadi.

Маълумотларни ёзиб олиш учун рухсат берадиган фойдалана олиш ҳуқуқи.

Изоҳ – Ёзиб олишга рухсат маълумотларни тўлдириш,

Д

Ўзгартириш, ўчириш ёки яратишга рухсат ҳисобланади.

Доступ на чтение

uz - o'qish uchun ruhsat

ўқиш учун рухсат

en - read access

Право на доступ, при получении которого разрешается читать данные.

Ma'lumotlarni o'qish uchun ruhsat beradigan foydalana olish huquqi.

Маълумотларни ўқиш учун рухсат берадиган фойдалана олиш ҳуқуқи.

Доступ неавторизованный

uz - mualliflashtirilmagan

foydalana olish

муаллифлаштирилмаган

фойдалана олиш

en - illegal access

Преднамеренное обращение пользователя к данным, доступ к которым ему не разрешен, с целью их чтения, модификации или разрушения.

Foydalanuvchining, o'qish, o'zgartirish yoki buzish maqsadida, unga erkin foydalanish ruhsat etilmagan ma'lumotlarga ataylab murojaat qilishi.

Фойдаланувчининг, ўқиш, ўзгартириш ёки бузиш мақсадида, унга эркин фойдаланиш рухсат этилмаган маълумотларга атайлаб мурожаат қилиши.

Доступ

несанкционированный

uz - ruhsat etilmagan tarzda

foydalana olish

рухсат этилмаган тарзда

фойдалана олиш

en - unauthorized access

1 Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

2 Доступ к сетевым ресурсам, осуществляемый в обход установленной защиты.

3 Нарушение регламентированного доступа к объекту защиты.

1 Subyektning obyektidan yoki axborotdan, tizimda belgilangan foydalanishni chegaralash qoidalarini buzgan holda foydalana olishi.

2 Tarmoq resurslaridan o'rnatilgan muhofazani chetlab o'tib foydalana olish.

3 Muhofaza obyektidan reglamentlangan tarzda foydalana olishning buzilishi.

1 Субъектнинг объектдан ёки ахборотдан, тизимда белгиланган фойдаланишни чегаралаш қоидаларини бузган ҳолда фойдалана олиши.

2 Тармоқ ресурсларидан ўрнатилган муҳофазани четлаб ўтиб фойдалана олиш.

Д

3 Муҳофаза объектидан регламентланган тарзда фойдалана олишнинг бузилиши.

Доступ при отказе

uz - ishlamay qolishda foydalana olish

ишламай қолишда

фойдалана олиш

en - failure access

Несанкционированный и, как правило, случайный доступ к данным в системе обработки данных, ставший возможным в результате отказа оборудования или программного обеспечения.

Uskuna yoki dasturiy ta'minotning buzilishi natijasida yo'l qo'yilishi mumkin bo'lgan ma'lumotlarni qayta ishlash tizimidagi ma'lumotlardan ruxsat etilmagan tarzda va tasodifiy foydalana olish.

Ускуна ёки дастурий таъминотнинг бузилиши натижасида йўл қўйилиши мумкин бўлган маълумотларни қайта ишлаш тизимидаги маълумотлардан рухсат этилмаган тарзда ва тасодифий фойдалана олиш.

Доступность

uz - foydalana olishlik

фойдалана олишлик

en - availability

1 Свойство данных или ресурсов быть доступными и пригодными к использованию по запросу уполномоченного логического объекта.

2 Возможность за приемлемое время получить от информационной системы требуемую информационную услугу.

3 Состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.

1 Ma'lumotlar yoki resurslarning, vakolatli mantiqiy obyektning so'roviga ko'ra, foydalana olish mumkin bo'lgan va foydalanishga yaroqlilik xususiyati.

2 Maqbul vaqt ichida axborot tizimidan talab qilinadigan axborot xizmatini olish mumkinligi.

3 Axborot va uning tashuvchisining holati, unda foydalanuvchilar tomonidan ular uchun mo'ljallangan axborotning hech qanday qarshiliksiz va o'z vaqtida olinishi ta'minlanadi.

1 Маълумотлар ёки ресурсларнинг, ваколатли мантикий объектнинг сўровига кўра, фойдалана олиш мумкин бўлган ва фойдаланишга яроқли-

Д

лик хусусияти.

2 Мақбул вақт ичида ахборот тизимидан талаб қилинадиган ахборот хизматини олиш мумкинлиги.

3 Ахборот ва унинг ташувчисининг ҳолати, унда фойдаланувчилар томонидан улар учун мўлжалланган ахборотнинг ҳеч қандай қаршиликсиз ва ўз вақтида олинishi таъминланади.

Доступность информации

uz - axborotdan foydalana olishlik

ахборотдан фойдалана олишлик

en - information availability

Состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.

Axborot va uning tashuvchisining holati, unda foydalanuvchilar tomonidan ular uchun mo'ljallangan axborotning hech qanday qarshiliksiz va o'z vaqtida olinishi ta'minlanadi.

Ахборот ва унинг ташувчисининг ҳолати, унда фойдаланувчилар томонидан улар учун мўлжалланган ахборотнинг ҳеч қандай қаршиликсиз ва ўз вақтида олинishi таъминланади.

Доступность системы

uz - tizimdan foydalana olishlik

тизимдан фойдалана олишлик

en - system availability

Свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к информации, имеющих на это надлежащие полномочия.

Tegishli vakolatlari bo'lgan subyektlarning axborotdan o'z vaqtida hech qanday to'siqlarsiz foydalana olishini ta'minlash qobiliyatini tavsiflovchi axborot (uni qayta ishlash vositalari va texnologiyalari) aylanadigan (tarqaladigan) tizimning xususiyati.

Тегишли ваколатлари бўлган субъектларнинг ахборотдан ўз вақтида ҳеч қандай тўсиқларсиз фойдалана олишини таъминлаш қобилиятини тавсифловчи ахборот (уни қайта ишлаш воситалари ва технологиялари) айланадиган (тарқалади-

Д

Драйвер устройства

uz - qurilma drayveri

қурилма драйвери

en - device driver

ган) тизимнинг хусусияти.

Программа, написанная специально для данного устройства с целью обеспечить функцию управления этого устройства со стороны операционной системы.

Operatsion tizim tomonidan shu qurilmani boshqarish funksiyasini ta'minlash maqsadida mazkur qurilma uchun maxsus yozilgan dastur.

Операцион тизим томонидан шу қурилмани бошқариш функциясини таъминлаш мақсадида мазкур қурилма учун махсус ёзилган дастур.

Дыра

uz - teshik

тешик

en - loophole

В вычислительной технике – недоработки, ошибки в программном обеспечении или аппаратуре, позволяющие обойти процессы управления доступом.

Hisoblash texnikasida – dasturiy ta'minot yoki apparaturadagi, foydalana olishni boshqarish jarayonlarini chetlab o'tish imkonini beruvchi xatolar, kamchiliklar.

Ҳисоблаш техникасида – дастурий таъминот ёки аппаратурадаги, фойдалана олишни бошқариш жараёнларини четлаб ўтиш имконини берувчи хатолар, камчиликлар.

Е

Единица измерения

uz - o'lchov birligi

ўлчов бирлиги

en - unit of measurement

Действительная скалярная величина, определенная и принятая по соглашению, с которой можно сравнить любую другую величину того же рода и выразить их отношение в виде числа.

Kelishuv bo'yicha belgilangan va qabul qilingan, ayni har qanday boshqa kattalik taqqoslanishi va ularning nisbati son ko'rinishida ifodalanishi mumkin bo'lgan haqiqiy skalyar kattalik.

Келишув бўйича белгиланган ва қабул қилинган, айни ҳар қандай бошқа катталиқ таққосланиши

Е

ва уларнинг нисбати сон кўринишида ифодалангани мумкин бўлган ҳақиқий скаляр катталиқ.

Ж

Жетон идентификатора личности

uz - shaxs identifikatori jetoni
шахс идентификатори

жетони

en - intelligent token

Миниатюрное устройство, содержащее микропроцессор и память, которое может использоваться в качестве удостоверения личности при работе на терминале.

Tarkibida mikroprotessor va хотира bo‘lgan, terminalda ishlash paytida shaxsiy guvohnoma sifatida foydalanilishi mumkin bo‘lgan ixcham qurilma.

Таркибида микропроцессор ва хотира бўлган, терминалда ишлаш пайтида шахсий гувоҳнома сифатида фойдаланилиши мумкин бўлган ихчам қурилма.

Живучесть

uz - yashovchanlik
яшовчанлик

en - viability

Свойство системы (сети) оставаться работоспособной в условиях внешних воздействий.

Tizim (tarmoq)ning, tashqi ta’sirlar sharoitida ishga layoqatli holatini saqlab qolish xususiyati.

Тизим (тармоқ)нинг, ташқи таъсирлар шароитида ишга лаёқатли ҳолатини сақлаб қолиш хусусияти.

Журнал

uz - jurnal
журнал

en - journal, log

1 В вычислительной технике – набор данных (файл), используемый операционной или иной системой для сбора и учета статистической информации, различных сообщений и других данных.

2 Файл регистрации или список транзакций, происходящих в компьютере или сети, служащий вспомогательным средством для восстановления событий или данных при потере или порче.

1 Hisoblash texnikasida – operatsion yoki boshqa tizim tomonidan statistik axborotni, turli xabarlar va boshqa ma’lumotlarni to‘plash hamda hisobga olish uchun foydalaniladigan ma’lumotlar to‘plami (fayl).

2 Yo‘qolganda yoki buzilganda voqealar yoki ma’-

Ж

lumotlarni tiklash uchun yordamchi vosita bo'lib xizmat qiladigan, kompyuter yoki tarmoqda yuz beradigan tranzaksiyalar ro'yxati yoki qayd etish fayli.

1 Ҳисоблаш техникасида – операцион ёки бошқа тизим томонидан статистик ахборотни, турли хабарлар ва бошқа маълумотларни тўплаш ҳамда ҳисобга олиш учун фойдаланиладиган маълумотлар тўплами (файл).

2 Йўқолганда ёки бузилганда воқеалар ёки маълумотларни тиклаш учун ёрдамчи восита бўлиб хизмат қиладиган, компьютар ёки тармоқда юз берадиган транзакциялар рўйхати ёки қайд этиш файли.

Журнал аудита

uz - audit jurnali

аудит журналли

en - audit trail

1 Данные, собираемые для последующего использования при проведении аудита безопасности.

2 Совокупность записей о выполняемых в системе транзакциях, документирующая процесс обработки информации в системе и позволяющая определить источники возникновения транзакций в системе и последовательность их выполнения системой.

1 Xavfsizlik auditini o'tkazishda foydalanish maqsadida to'planadigan ma'lumotlar.

2 Tizimda amalga oshiriladigan tranzaksiyalar to'g'risidagi yozuvlar yig'indisi. Tizimda axborotning qayta ishlanish jarayonini hujjatlashtiradi, tranzaksiyalarning yuzaga kelish manbalarini va tizim tomonidan ularning bajarilish ketma-ketligini aniqlash imkonini beradi.

1 Xavfsizlik auditini ўтказишда фойдаланиш мақсадида тўпланадиган маълумотлар.

2 Тизимда амалга ошириладиган транзакциялар тўғрисидаги ёзувлар йиғиндиси. Тизимда ахборотнинг қайта ишланиш жараёнини хужжатлаштиради, транзакцияларнинг юзага келиш манбаларини ва тизим томонидан уларнинг бажарилиш кетма-кетлигини аниқлаш имконини беради.

Ж

Журнал восстановления

uz - tiklash jurnali

тиклаш журнали

en - recovery log

Журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в базе данных (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Ma'lumotlar bazasi yoki faylni tiklash imkoniyatini ta'minlovchi jurnal. Ma'lumotlar ishonchli ekanligi va oxirgi rezerv nusxa qilinganligi belgilangan vaqtdan boshlab, ma'lumotlar bazasidagi (fayldagi) barcha o'zgartirishlar to'g'risidagi axborotni ichiga oladi.

Маълумотлар базаси ёки файлни тиклаш имкониятини таъминловчи журнал. Маълумотлар ишончли эканлиги ва охириги резерв нусха қилинганлиги белгиланган вақтдан бошлаб, маълумотлар базасидаги (файлдаги) барча ўзгартиришлар тўғрисидаги ахборотни ичига олади.

Журнал ошибок

uz - xatolar jurnali

хатолар журнали

en - error log

Файл, в который система записывает информацию о сбоях.

Tizim, to'xtab qolishlar to'g'risidagi axborotni yozadigan fayl.

Тизим, тўхтаб қолишлар тўғрисидаги ахборотни ёзадиган файл.

Журнализация

uz - jurnallashtirish

журналлаштириш

en - journalizing

Процесс записи в системный журнал информации о сообщениях, запросах, выполнявшихся программах, использованных наборах данных и других сведений.

Tizim jurnaliga xabarlar, so'rovlar, bajariladigan dasturlar, foydalanilgan ma'lumotlar to'plami to'g'risidagi axborotni va boshqa ma'lumotlarni yozish jarayoni.

Ж

Тизим журналига хабарлар, сўровлар, бажариладиган дастурлар, фойдаланилган маълумотлар тўплами тўғрисидаги ахборотни ва бошқа маълумотларни ёзиш жараёни.

З

Завершение аварийное

uz - avariya viy tugallanish

авариявий тугалланиш

en - abnormal end,abend

1 Незапланированное прерывание обработки данных.

2 Преждевременное завершение работы программы из-за программной или аппаратной ошибки, обнаруженной операционной системой. Сопровождается сообщением об ошибке (в отличие от зависаний).

1 Ma'lumotlarni qayta ishlashning rejalashtirilmagan tarzda to'xtatilishi.

2 Operatsion tizim aniqlagan dastur yoki apparat bilan bog'liq xato tufayli, dastur ishining muddatidan avval tugallanishi. Xato to'g'risidagi xabar ostida boradi (osilib qolishlardan farqli ravishda).

1 Маълумотларни қайта ишлашнинг режалаштирилмаган тарзда тўхтатилиши.

2 Операцион тизим аниқлаган дастур ёки аппарат билан боғлиқ хато туфайли, дастур ишининг муддатидан аввал тугалланиши. Хато тўғрисидаги хабар остида боради (осилиб қолишлардан фарқли равишда).

Зависание программы

uz - dasturning osilib

qolishi

дастурнинг осилиб

қолиши

en - program hang-up

Непредусмотренный останов программы, обусловленный, например, такими причинами, как попытка обращения к устройству, не подключенному к процессору.

Dastur ishining, masalan, protsessorga ulanmagan qurilmaga murojaat qilishga urinish kabi sababga bog'liq ravishda ko'zda tutilmagan to'xtab qolishi.

Дастур ишининг, масалан, процессорга уланмаган қурилмага мурожаат қилишга уриниш каби сабабга боғлиқ равишда кўзда тutilмаган тўхтаб қолиши.

Зависание системы

uz - tizimning osilib

Остановка («замораживание») мультипрограммной системы путем подавления ввода новых за-

qolishi

ТИЗИМНИНГ ОСИЛИБ
КОЛИШИ

en - system quiescing

Зависимость

uz - bog‘liqlik

БОҒЛИҚЛИК

en - dependency

даний.

Multidasturli tizimni yangi topshiriqlar kiritilishini bostirish yo‘li bilan to‘xtatish («muzlatib qo‘yish»).

Мультидастурли тизимни янги топшириқлар киритилишини бостириш йўли билан тўхтатиш («музлатиб қўйиш»).

Взаимосвязь между компонентами, при которой если требование, основанное на зависимом компоненте, включено в профиль защиты, задание по безопасности или пакет, то и требование, основанное на компоненте, который зависит от вышеуказанного компонента, должно, как правило, также включено в профиль защиты, задание по безопасности или пакет.

Komponentlar orasidagi aloqadorlik, bunda bog‘liq bo‘lgan komponentga asoslangan talab, himoya profiliga xavfsizlik bo‘yicha topshiriq yoki paketga kiritilgan bo‘lsa, u holda, yuqorida ko‘rsatilgan komponentga bog‘liq bo‘lgan komponentga asoslangan talab ham, qoidaga ko‘ra, himoya profiliga xavfsizlik bo‘yicha topshiriq yoki paketga kiritilgan bo‘lishi kerak.

Компонентлар орасидаги алоқадорлик, бунда боғлиқ бўлган компонентга асосланган талаб, ҳимоя профилига хавфсизлик бўйича топширик ёки пакетга киритилган бўлса, у ҳолда, юқорида кўрсатилган компонентга боғлиқ бўлган компонентга асосланган талаб ҳам, қоидага кўра, ҳимоя профилига хавфсизлик бўйича топширик ёки пакетга киритилган бўлиши керак.

**Загрузка по линиям
телекоммуникаций**

uz - telekommunikatsiyalar
liniyalari bo‘ylab yuklash

телекоммуникациялар
линиялари бўйлаб юклаш
en - download

Пересылка программного обеспечения по линии телекоммуникаций от одной компьютерной системы к другой, например, от сервера к персональному компьютеру.

Telekommunikatsiyalar liniyasi bo‘ylab dasturiy ta‘minotni bir kompyuter tizimidan boshqasiga, masalan, serverdan shaxsiy kompyuterga o‘tkazish.

Телекоммуникациялар линияси бўйлаб дастурий таъминотни бир компьютер тизимидан бошқасига, масалан, сервердан шахсий компьютерга ўтказиш.

Загрязнение

uz - ifloslanish

ифлосланиш

en - contamination

Введение данных с одним грифом секретности или категорией безопасности в данные с более низким грифом секретности или другой категорией безопасности.

Bitta maxfiylik grifi yoki xavfsizlik kategoriyasidagi ma'lumotlarni maxfiylik grifining darajasi pastroq bo'lgan yoki boshqa xavfsizlik kategoriyasidagi ma'lumotlarga kiritish.

Битта махфийлик грифи ёки хавфсизлик категориясидаги маълумотларни махфийлик грифининг даражаси пастроқ бўлган ёки бошқа хавфсизлик категориясидаги маълумотларга киритиш.

Задание по безопасности

uz - xavfsizlik bo'yicha

topshiriq

хавфсизлик бўйича

топширик

en - security target

1 Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного объекта оценки.

2 Зависимое от реализации изложение потребностей в безопасности для некоторого конкретно определенного объекта оценки.

1 Muayyan baholash obyektini baholash uchun asos sifatida foydalanishga mo'ljallangan, xavfsizlik talablari va spetsifikatsiyalar yig'indisi.

2 Ayrim aniq belgilangan baholash obyektini uchun amalga oshirilishiga bog'liq bo'lgan, xavfsizlik yuzasidan ehtiyojlar bayoni.

1 Muayyan baholash obyektini baholash uchun asos sifatida foydalanishga mo'ljallangan, xavfsizlik talablari va spetsifikatsiyalar yig'indisi.

2 Ayrim aniq belgilangan baholash obyektini uchun amalga oshirilishiga bog'liq bo'lgan, xavfsizlik yuzasidan ehtiyojlar bayoni.

Задача безопасности

uz - xavfsizlik vazifasi

хавфсизлик вазифаси

en - security problem

Формальное изложение, в котором определяется характер и область действия безопасности, которые предполагается адресовать объектам оценки.

Примечание – Задача безопасности включает:

- угрозы, которым должен противостоять объект оценки;
- политики безопасности организации, реализуемые объ-

ектом оценки;

- предположения относительно использования объекта оценки и среды его функционирования.

Baholash obyektiga yo‘llash taxmin qilinadigan xavfsizlik harakatlari sohasi va xarakteri belgilanadigan formal izoh bayon.

Izohlar – Xavfsizlik vazifasi:

- baholash obyektini qarshi tura olishi lozim bo‘lgan tahdidlarni;

- baholash obyektini tomonidan amalga oshiriladigan tashkilotning xavfsizlik siyosatini;

- baholash obyektidan foydalanish hamda ishlash muhitiga oid taxminlarni o‘z ichiga oladi.

Баҳолаш объектига йўллаш тахмин қилинадиган хавфсизлик ҳаракатлари соҳаси ва характери белгиланадиган формал изох баён.

Изоҳлар – Хавфсизлик вазифаси:

- баҳолаш объекти қарши тура олиши лозим бўлган таҳдидларни;

- баҳолаш объекти томонидан амалга ошириладиган ташкilotнинг хавфсизлик сиёсатини;

- баҳолаш объектидан фойдаланиш ҳамда ишлаш муҳитига оид тахминларни ўз ичига олади.

Задача контрольная

uz - nazorat topshirig‘i

назорат топшириғи

en - check problem

Задача с известным решением, используемая для определения правильности работы функционального модуля.

Funksional modul ishi to‘g‘riligini aniqlash uchun foydalaniladigan, yechimi ma‘lum topshiriq.

Функционал модуль иши тўғрилигини аниқлаш учун фойдаланиладиган, ечими маълум топширик.

Задача перехвата

uz - qo‘lga kiritish masalasi

қўлга киритиш масаласи

en - interception problem

Задача получения информации, которая решается на основе обработки перехваченных побочных электромагнитных излучений и наводок.

Axborotni olish masalasi, tutib olingan nomaqbul elektromagnit nurlanishlar va ta’sirlarni qayta ishlash asosida hal etiladi.

Ахборотни олиш масаласи, тутиб олинган нomaқбул электромагнит нурланишлар ва таъсирларни қайта ишлаш асосида ҳал этилади.

Закладка программная

uz - dasturiy oʻrnatma
дастурий ўрнатма
en - software bug

Преднамеренно внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, приводящих к нарушению конфиденциальности, доступности или целостности информации.

Dasturiy taʼminotga ataylab kiritilgan funksional obyektlar, ular maʼlum sharoitlarda (kirish maʼlumotlarida) axborotning konfidensialligi, undan foydalanish yoki yaxlitligi buzilishiga olib keladigan dasturiy taʼminot hujjatlarida tavsiflanmagan funksiyalarning bajarilishini boshlab beradi.

Дастурий таъминотга атайлаб киритилган функционал объектлар, улар маълум шароитларда (кириш маълумотларида) ахборотнинг конфиденциаллиги, ундан фойдаланиш ёки яхлитлиги бузилишига олиб келадиган дастурий таъминот ҳужжатларида тавсифланмаган функцияларнинг бажарилишини бошлаб беради.

Замещение

uz - oʻrnini bosish
ўрнини босиш
en - replay (attack)

Вид атаки в криптосистеме или системе аутентификации, при которой сообщение запоминается и передается вновь позднее, замещая или повторяя первоначальное сообщение.

Kriptotizim yoki autentifikatsiya qilish tizimidagi hujum turi. Bunda xabar yodda saqlanadi va boshlangʻich xabarning oʻrnini bosgan yoki takrorlagan holda, keyinroq yana uzatiladi.

Криптотизим ёки аутентификация қилиш тизимидаги ҳужум тури. Бунда хабар ёдда сақланади ва бошланғич хабарнинг ўрнини босган ёки такрорлаган ҳолда, кейинроқ яна узатилади.

Замок защиты (секретности)

uz - muhofaza (maxfiylik)
qulfi
муҳофаза (махфийлик)
кулфи
en - privacy lock, protection

Программный механизм проверки паролей при обращении к базе данных или ее фрагментам (файлам, областям), обеспечивающий ограничение доступа к записям.

Maʼlumotlar bazasiga yoki uning fragmentlariga

lock

(fayllarga, sohalarga) murojaat qilingandagi parollarni tekshirishning dasturiy mexanizmi. Yozuvlardan foydalanishni cheklaydi.

Замок памяти

uz - хотира qulfi

хотира қулфи

en - memory lock

Маълумотлар базасига ёки унинг фрагментларига (файлларга, соҳаларга) мурожаат қилингандаги паролларни текширишнинг дастурий механизми. Ёзувлардан фойдаланишни чеклайди.

Код в дескрипторе сегмента или страницы виртуальной памяти, используемый системой защиты памяти для ограничения доступа. При этом к сегменту могут обращаться только процессы, имеющие в своем дескрипторе соответствующий ключ.

Xotiraning muhofaza tizimi tomonidan foydalanishni cheklash uchun ishlatiladigan, segment deskriptoridagi kod yoki virtual хотира sahifasi kodi. Bunda segmentga o'z deskriptorida tegishli kalitga ega bo'lgan jarayonlarga murojaat qila oladi.

Хотиранинг муҳофаза тизими томонидан фойдаланишни чеклаш учун ишлатиладиган, сегмент дескрипторидаги код ёки виртуал хотира саҳифаси коди. Бунда сегментга ўз дескрипторида тегишли калитга эга бўлган жараёнларгина мурожаат қила олади.

Замысел защиты информации

uz - axborotni muhofaza

qilish g'oyasi

ахборотни муҳофаза

қилиш ғояси

en - information security plan

Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации на объекте.

Obyektda axborotni muhofaza qilish maqsadlariga erishish uchun zarur bo'lgan tadbirlarning tarkibi, mazmuni, o'zaro aloqadorligi va ketma-ketligini ochib beruvchi asosiy fikr (g'oya).

Объектда ахборотни муҳофаза қилиш мақсадларига эришиш учун зарур бўлган тadbirlarнинг таркиби, мазмуни, ўзаро алоқадорлиги ва кетма-кетлигини очиб берувчи асосий фикр (ғоя).

Записи системы управления конфигурацией

uz - konfiguratsiyani

Выходные данные, получаемые в процессе функционирования системы управления конфигурацией и документирующие основные виды дея-

boshqarish tizimi yozuvlari
 конфигурацияни
 бошқариш тизими ёзувлари
en - configuration management
 system records

тельности по управлению конфигурацией.
 Примечание – Примерами записей системы управления конфигурацией являются формы контроля изменений элементов конфигурации или формы санкционирования доступа к элементам конфигурации.

Konfiguratsiyani boshqarish tizimining ishlash jarayonida olinadigan va konfiguratsiyani boshqarish bo'yicha asosiy faoliyat turlarini hujjatlashtiradigan chiqish ma'lumotlari.

Izoh – Konfiguratsiyani boshqarish tizimi yozuvlariga konfiguratsiya elementlarining o'zgarishlarini nazorat qilish yoki konfiguratsiya elementlariga erkin kira olishga ruxsat berish shakli misol bo'la oladi.

Конфигурацияни бошқариш тизимининг ишлаш жараёнида олинadigan ва конфигурацияни бошқариш бўйича асосий фаолият турларини ҳужжатлаштирадиган чиқиш маълумотлари.

Изоҳ – Конфигурацияни бошқариш тизими ёзувларига конфигурация элементларининг ўзгаришларини назорат қилиш ёки конфигурация элементларига эркин kira олишга рuxсат бериш шакли мисол бўла олади.

Запись контрольная
uz - nazorat yozuvi
 назорат ёзуви
en - control record

Запись, которая содержит контрольные суммы, вычисленные путем суммирования значений из других записей файла. Контрольные суммы могут нести дополнительную информацию или использоваться только для проверки правильности данных.

Fayldagi boshqa yozuvlar qiymatlarini jamlash yo'li bilan hisoblangan nazorat summalarini o'z ichiga oluvchi yozuv. Nazorat summolari qo'shimcha axborotga ega bo'lishi yoki faqat ma'lumotlarning to'g'riligini tekshirish uchun qo'llanilishi mumkin.

Файлдаги бошқа ёзувлар қийматларини жамлаш йўли билан ҳисобланган назорат суммаларини ўз ичига олувчи ёзув. Назорат суммалари қўшимча ахборотга эга бўлиши ёки фақат маълумотларнинг тўғрилигини текшириш учун қўлланилиши мумкин.

Запись учетная
uz - hisobga olish yozuvi
 ҳисобга олиш ёзуви

Информация, идентифицирующая субъект системы безопасности. Указателем на учетную запись является ее идентификатор безопасности.

en - account

Различают учетные записи пользователей, групп, компьютеров и доменов.

Xavfsizlik tizimi subyektini identifikatsiya qiluvchi axborot. Hisobga olish yozuvining ko'rsatkichi bo'lib, uning xavfsizlik identifikatori hisoblanadi. Foydalanuvchilar, guruhlar, kompyuterlar va domenlarning hisobga olish yozuvlari ajratiladi.

Хавфсизлик тизими субъектини идентификация қилувчи ахборот. Ҳисобга олиш ёзувининг кўрсаткичи бўлиб, унинг хавфсизлик идентификатори ҳисобланади. Фойдаланувчилар, гуруҳлар, компьютерлар ва доменларнинг ҳисобга олиш ёзувлари ажратилади.

Заполнение страницы

uz - sahifani to'ldirish

саҳифани тўлдириш

en - page padding

Способ записи в блок данных последней не полностью заполненной страницы незначущей информации.

Ма'lumotlar blokiga ahamiyatli bo'lmagan axborotning oxirgi, to'liq to'ldirilmagan sahifasini yozish usuli.

Маълумотлар блокига аҳамиятли бўлмаган ахборотнинг охириги, тўлиқ тўлдирилмаган саҳифасини ёзиш усули.

Заполнение трафика

uz - trafikni to'ldirish

трафикни тўлдириш

en - traffic padding

Контрмера, при использовании которой средства передачи генерируют ложные данные, чтобы затруднить выполнение анализа трафика или его дешифрование.

Qarshi chora, undan foydalanishda uzatish vositalari trafikni tahlil qilish yoki uning qayta shifrlanishini qiyinlashtirish maqsadida yolg'on ma'lumotlarni generatsiyalaydi.

Қарши чора, ундан фойдаланишда узатиш воситалари трафикни таҳлил қилиш ёки унинг қайта шифрланишини қийинлаштириш мақсадида ёлгон маълумотларни генерациялайди.

Запрос/ответ

uz - so'rov/javob

сўров/жавоб

en - challenge/response

Метод аутентификации, при котором одна сторона посылает шифрованный запрос, а вторая выдает ответ с помощью одного и того же алгоритма аутентификации.

Autentifikatsiya metodi, unga ko‘ra, bir tomon shifrlangan so‘rov jo‘natadi, ikkinchi tomon esa, aynan bitta autentifikatsiya algoritmi yordamida javob beradi.

Аутентификация методи, унга кўра, бир томон шифрланган сўров жўнатади, иккинчи томон эса, айнан битта аутентификация алгоритми ёрдамида жавоб беради.

Засекречивание сведений и их носителей

uz - ma'lumotlar va ularning tashuvchilarini maxfiylashtirish

маълумотлар ва уларнинг ташувчиларини махфийлаштириш

en - classification of information and its bearers

as secret

Введение в предусмотренном законодательством порядке для сведений, составляющих государственные секреты, ограничений на их распространение и на доступ к их носителям.

Qonunda ko‘zda tutilgan tartibda, davlat siri hisoblanadigan ma'lumotlar uchun, ularni tarqatish va tashuvchilardan foydalanish yuzasidan cheklashlar kiritish.

Қонунда кўзда тутилган тартибда, давлат сирини ҳисобланадиган маълумотлар учун, уларни тарқатиш ва ташувчилардан фойдаланиш юзасидан чеклашлар киритиш.

Захватчики паролей

uz - parollarni egallab oluvchilar

паролларни эгаллаб олувчилар

en - password hook

Программы, ворующие пароли путем обманных воздействий на операционную систему.

Operatsion tizimga aldamchi ta'sirlar ko'rsatish orqali parollarni o'g'irlovchi dasturlar.

Операцион тизимга алдамчи таъсирлар кўрсатиш орқали паролларни ўғирловчи дастурлар.

Защивание

uz - sikllash

циклаш

en - cycling

1 Автоматическое объединение конца одной строки с началом другой, когда это касается дисплея или принтера.

2 Автоматическое объединение конечной области постоянных запоминающих устройств с начальной.

1 Bir satr oxirini boshqa satr boshi bilan, bu display yoki printerga taalluqli bo'lganda, avtomatik birlashtirish.

2 Doimiy xotirlovchi qurilmaning oxirgi sohasini boshlang'ich soha bilan avtomatik birlashtirish.

1 Бир сатр охирини бошқа сатр боши билан, бу дисплей ёки принтерга тааллуқли бўлганда, автоматик бирлаштириш.

2 Доимий хотирловчи қурилманинг охириги соҳасини бошланғич соҳа билан автоматик бирлаштириш.

Зашифрование

uz - shifrlash
шифрлаш
en - coding

Процесс применения обратимого преобразования шифра к открытому тексту. Результатом зашифрования является шифротекст.

Shifrnı ochiq matnga o'zgartirishni qo'llash jarayoni. Shifrmatn shifrlash natijasi bo'lib hisoblanadi.

Шифрни очик матнга ўзгартиришни қўллаш жараёни. Шифрматн шифрлаш натижаси бўлиб ҳисобланади.

Защита

uz - muhofaza qilish
муҳофаза қилиш
en - security

Юридические, организационные и технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.

Apparatura, dasturlar va ma'lumotlardan ruxsat etilmagan tarzda foydalanishning oldini olish bo'yicha yuridik, tashkiliy, texnik, shu jumladan, dasturiy chora-tadbirlar.

Аппаратура, дастурлар ва маълумотлардан рұхсат этилмаган тарзда фойдаланишнинг олдини олиш бўйича юридик, ташкилий, техник, шу жумладан, дастурий чора-тадбирлар.

Защита аппаратная

uz - apparat vositasida muhofaza qilish
аппарат воситасида муҳофаза қилиш
en - hardware security

Использование аппаратных средств, например, регистров границ или замков и ключей для защиты данных в ЭВМ.

Apparat vositalardan, masalan, chegaraviy registrlardan yoki qulflar va kalitlardan EHMdagi ma'lumotlarni muhofaza qilish uchun foydalanish.

Аппарат воситалардан, масалан, чегаравий регистрлардан ёки қулфлар ва калитлардан ЭХМ даги маълумотларни муҳофаза қилиш учун фойдаланиш.

Защита

вычислительной сети

uz - hisoblash tarmog'ini muhofaza qilish

хисоблаш тармоғини муҳофаза қилиш

en - network security

Исключение несанкционированного доступа пользователей к элементам и ресурсам сети путем использования аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Apparat, dasturiy va kriptografik muhofaza qilish metodlari hamda vositalaridan, shuningdek tashkiliy tadbirlardan foydalanish yo'li bilan, foydalanuvchilarning tarmoq elementlari hamda resurslaridan ruxsat etilmagan tarzda foydalana olishlariga yo'l qo'y-maslik.

Аппарат, дастурий ва криптографик муҳофаза қилиш методлари ҳамда воситаларидан, шунингдек ташкилий тадбирлардан фойдаланиш йўли билан, фойдаланувчиларнинг тармоқ элементлари ҳамда ресурсларидан рўхсат этилмаган тарзда фойдалана олишларига йўл қўймаслик.

Защита данных

uz - ma'lumotlarni muhofaza qilish

маълумотларни муҳофаза қилиш

en - data protection

1 Реализация административных, технических или физических мер для предотвращения несанкционированного доступа к данным.

2 Меры, предпринимаемые для сохранения данных от нежелательных последствий и действий, которые неумышленно или преднамеренно ведут к модификации, раскрытию или разрушению данных.

1 Ma'lumotlardan ruxsat etilmagan tarzda foydalana olishning oldini olish uchun ma'muriy, texnik yoki jismoniy chora-tadbirlarni amalga oshirish.

2 Ma'lumotlarni, qasddan yoki qasddan bo'lmagan tarzda o'zgartirilishiga, fosh bo'lishiga yoki buzilishiga olib keladigan nomaqbul oqibatlardan va harakatlardan saqlash uchun qo'llaniladigan chora-tadbirlar.

1 Маълумотлардан рўхсат этилмаган тарзда фой-

далана олишнинг олдини олиш учун маъмурий, техник ёки жисмоний чора-тадбирларни амалга ошириш.

2 Маълумотларни, қасддан ёки қасддан бўлмаган тарзда ўзгартирилишига, фoш бўлишига ёки бузилишига олиб келадиган номақбул оқибатлардан ва ҳаракатлардан сақлаш учун қўлланиладиган чора-тадбирлар.

Защита информации (данных)

uz - axborotni (ma'lumotlarni) muhofaza qilish

ахборотни (маълумотларни) муҳофаза қилиш

en - information (data) security

1 Комплекс правовых, организационных и технических (программно-аппаратных) мероприятий, направленных на предотвращение или затруднение нанесения ущерба интересам собственника информации (данных).

2 Меры по предотвращению угроз информационной безопасности и устранению их последствий.

3 Деятельность, направленная на предотвращение утечки защищаемой информации, от несанкционированных и непреднамеренных воздействий на защищаемую информацию.

1 Axborot (ma'lumot) egasi manfaatlariga zarar keltirilishining oldini olish yoki qiyinlashtirishga qaratilgan huquqiy, tashkiliy va texnik (apparat-dasturiy) tadbirlar kompleksi.

2 Axborot xavfsizligiga bo'ladigan tahdidlarning oldini olish va ularning oqibatlarini bartaraf qilish bo'yicha ko'riladigan chora-tadbirlar.

3 Muhofaza qilinadigan axborot chiqib ketishini (yo'qolishini) muhofaza qilinadigan axborotga ruxsat etilmagan va ko'zda tutilmagan ta'sir(lar)ni bartaraf etishga qaratilgan faoliyat.

1 Ахборот (маълумот) эгаси манфаатларига зарар келтирилишининг олдини олиш ёки қийинлаштиришга қаратирилган ҳуқуқий, ташкилий ва техник (аппарат-дастурий) тадбирлар комплекси.

2 Ахборот хавфсизлигига бўладиган таҳдидларнинг олдини олиш ва уларнинг оқибатларини бартараф қилиш бўйича кўриладиган чора-тадбирлар.

3 Муҳофаза қилинадиган ахборот чиқиб кетишини (йўқолишини) муҳофаза қилинадиган ахборотга рухсат этилмаган ва кўзда тутилмаган таъ-

**Защита информации
организационная**

uz - axborotni tashkiliy jihatdan muhofaza qilish

ахборотни ташкилий
жихатдан муҳофаза қилиш

en - organizational security
of information

сир(лар)ни баргараф этишга қаратилган фаолият.

Защита информации при ее обработке техническими средствами, осуществляемая путем принятия административных мер.

Примечание – Административные меры включают выбор места расположения объекта, не подверженного внешним воздействиям, организацию контролируемой (проверяемой) зоны, выполнение правил учета, хранения и обращения секретных (конфиденциальных) документов на различных носителях и другие меры.

Texnik vositalar bilan qayta ishlashda axborotni muhofaza qilish, ma'muriy chora-tadbirlar ko'rish orqali amalga oshiriladi.

Izoh – Ma'muriy chora-tadbirlar tashqi ta'sirga uchramagan obyekt joylashadigan yerning tanlanishini, nazorat qilinadigan (tekshiriladigan) zonani tashkillashtirish, turli tashuvchilardagi maxfiy (konfidensial) hujjatlarni hisobga olib, saqlash va ular bilan ishlash qoidalarini va boshqa chora-tadbirlarni ichiga oladi.

Техник воситалар билан қайта ишлашда ахборотни муҳофаза қилиш, маъмурий чора-тадбирлар кўриш орқали амалга оширилади.

Изоҳ – Маъмурий чора-тадбирлар ташқи таъсирга учрамаган объект жойлашадиган ернинг танланишини, назорат қилинадиган (текшириладиган) зонани ташкиллаштириш, турли ташувчилардаги махфий (конфиденциал) ҳужжатларни ҳисобга олиб, сақлаш ва улар билан ишлаш қоидаларини ва бошқа чора-тадбирларни ичига олади.

**Защита информации
организационно-
техническая**

uz - axborotni tashkiliy-texnik jihatdan muhofaza qilish

ахборотни ташкилий-
техник жихатдан муҳофаза
қилиш

en - organizational and technical
security of information

Защита информации, предусматривающая применение нормативных и методических документов, лицензирование деятельности в области защиты информации, сертификацию защищенных изделий, технических средств и способов защиты, создание на объектах систем защиты информации и аттестацию этих объектов.

Normativ va metodik hujjatlarning qo'llanilishini, axborotni muhofaza qilish sohasida faoliyatni litsenziyalashni, muhofazalangan buyumlar, muhofaza qilishning texnik vositalari hamda usullarini, obyektlarda axborotni muhofaza qilish tizimlari tuzilishini va bu obyektlarning attestatsiya qilinishini ko'zda tutadigan axborotni muhofaza qilish.

Защита информации от несанкционированного воздействия

uz - axborotni ruxsat etilmagan ta'sirdan muhofaza qilish

ахборотни рухсат
этилмаган таъсирдан
муҳофаза қилиш

en - information security from illegal impact

Норматив ва методик ҳужжатларнинг қўлланилишини, ахборотни муҳофаза қилиш соҳасида фаолиятни лицензиялашни, муҳофазаланган буюмлар, муҳофаза қилишнинг техник воситалари ҳамда усуллари, объектларда ахборотни муҳофаза қилиш тизимлари тузилишини ва бу объектларнинг аттестация қилинишини кўзда тутадиган ахборотни муҳофаза қилиш.

Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Axborotni o'zgartirish yuzasidan belgilangan huquqlar va/yoki qoidalar buzilgan holda, axborotning buzib ko'rsatilishiga, yo'q qilinishiga, undan foydalana olishning blokirovkalanishiga, shuningdek, axborot tashuvchining yo'qolishiga, yo'q qilinishiga yoki ishlashida uzilish kelib chiqishiga olib keladigan ta'sirning oldini olishga qaratilgan faoliyat.

Ахборотни ўзгартириш юзасидан белгиланган ҳуқуқлар ва/ёки қоидалар бузилган ҳолда, ахборотнинг бузиб кўрсатилишига, йўқ қилинишига, ундан фойдалана олишнинг блокировкаганишига, шунингдек, ахборот ташувчининг йўқолишига, йўқ қилинишига ёки ишлашида узилиш келиб чиқишига олиб келадиган таъсирнинг олдини олишга қаратилган фаолият.

Защита информации от несанкционированного доступа

uz - axborotni ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish

ахборотни рухсат
этилмаган тарзда фойдалана
олишдан муҳофаза қилиш

Деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных нормативными документами или собственником (владельцем) информации прав или правил доступа к ней.

Manfaatdor subyektning, normativ hujjatlar yoki axborot egasi tomonidan belgilangan huquqlar yoki

en - information security from unauthorized access

axborotdan foydalanish qoidalarini buzib, muhofaza qilinadigan axborotni olishga yo‘l qo‘ymaslikka yo‘naltirilgan faoliyat.

Манфаатдор субъектнинг, норматив ҳужжатлар ёки ахборот эгаси томонидан белгиланган ҳуқуқлар ёки ахборотдан фойдаланиш қоидаларини бузиб, муҳофаза қилинадиган ахборотни олишига йўл қўймасликка йўналтирилган фаолият.

Защита информации от разглашения

uz - axborotni oshkor etilishdan muhofaza qilish

ахборотни ошкор

этилишдан муҳофаза қилиш

en - information security from disclosure

Деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Muhofaza qilinadigan axborotning, bu axborotdan foydalana olish huquqi bo‘lmagan iste‘molchilarga ruxsat etilmagan tarzda yetkazilishining oldini olishga qaratilgan faoliyat.

Муҳофаза қилинадиган ахборотнинг, бу ахборотдан фойдалана олиш ҳуқуқи бўлмаган истеъмолчиларга рухсат этилмаган тарзда етказилишининг олдини олишга қаратилган фаолият.

Защита информации от утечки

uz - axborotni chiqib ketishdan muhofaza qilish

ахборотни чиқиб

кетишдан муҳофаза қилиш

en - information security from leak flow

Деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации.

Oshkor qilish, ruxsat etilmagan tarzda axborotdan foydalana olish va muhofaza qilinadigan axborotni olish natijasida, muhofaza qilinadigan axborotning nazorat qilib bo‘lmaydigan ravishda tarqalib ketishining oldini olishga qaratilgan faoliyat.

Ошкор қилиш, рухсат этилмаган тарзда ахборотдан фойдалана олиш ва муҳофаза қилинадиган ахборотни олиш натижасида, муҳофаза қилинадиган ахборотнинг назорат қилиб бўлмайдиган равишда тарқалиб кетишининг олдини олишга қаратилган фаолият.

Защита информации при ее обработке техническими

Действия, направленные на обеспечение безопасности информации при ее обработке техническими

средствами

uz - axborotni texnik vositalar bilan qayta ishlashda muhofaza qilish

ахборотни техник воситалар билан қайта ишлашда муҳофаза қилиш
en - information security while processing it with technical facilities

Защита информации техническая

uz - axborotni texnik muhofaza qilish

ахборотни техник муҳофаза қилиш
en - technical protection of information

Защита криптографическая

uz - kriptografik muhofaza qilish

криптографик муҳофаза қилиш
en - cryptosecurity, cryptographically security

Защита личной тайны

uz - shaxsiy sirni muhofaza qilish

шахсий сирни муҳофаза қилиш

кими средствами от всех видов угроз и факторов опасности.

Примечание – При обработке информации техническими средствами различают организационную и техническую защиты.

Texnik vositalar bilan qayta ishlashda barcha turdagi tahdidlardan va xavf omillaridan axborotning xavfsizligini ta'minlashga qaratilgan harakat.

Izoh – Axborotni texnik vositalar bilan qayta ishlashda tashkiliy va texnik jihatdan muhofaza qilish farqlanadi.

Техник воситалар билан қайта ишлашда барча турдаги таҳдидлардан ва хавф омилларидан ахборотнинг хавфсизлигини таъминлашга қаратилган ҳаракат.

Изоҳ – Ахборотни техник воситалар билан қайта ишлашда ташкилий ва техник жиҳатдан муҳофаза қилиш фарқланади.

Деятельность, направленная на обеспечение безопасности информации, инженерно-техническими и некриптографическими методами с использованием средств технической защиты информации.

Axborotni texnik muhofaza qilish vositalaridan foydalanib muhandis-texnik va nokriptografik usullar bilan axborot xavfsizligini ta'minlashga yo'naltirilgan faoliyat.

Ахборотни техник муҳофаза қилиш воситаларидан фойдаланиб муҳандис-техник ва нокриптографик усуллар билан ахборот хавфсизлигини таъминлашга йўналтирилган фаолият.

Защита информации (данных) при помощи ее криптографического преобразования.

Axborot (ma'lumotlar)ni, uni kriptografik qayta o'zgartirish yordamida muhofaza qilish.

Ахборот (маълумотлар)ни, уни криптографик қайта ўзгартириш ёрдамида муҳофаза қилиш.

Реализация мер, гарантирующих сохранение личной тайны. К этим мерам относятся защита персональных данных и ограничения на их сбор, обобщение и обработку.

en - privacy protection

Shaxsiy sirning saqlanishini kafolatlovchi chora-tadbirlarning amalga oshirilishi. Bu chora-tadbirlarga shaxsiy ma'lumotlarni muhofaza qilish hamda ularni to'plash, umumlashtirish va qayta ishlanishini cheklashlar kiradi.

Шахсий сирнинг сақланишини кафолатловчи чора-тадбирларнинг амалга оширилиши. Бу чора-тадбирларга шахсий маълумотларни муҳофаза қилиш ҳамда уларни тўплаш, умумлаштириш ва қайта ишланишини чеклашлар кирди.

Защита многоуровневая

uz - ko'p pog'onali himoya

кўп поғонали ҳимоя

en - multilevel protection

Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Konfidensiallikning turli darajasidagi obyektlardan foydalana olishning turli huquqlariga ega subyektlarning foydalana olishi cheklanishi ta'minlanadigan muhofaza.

Конфиденциалликнинг турли даражасидаги объектлардан фойдалана олишнинг турли ҳуқуқларига эга субъектларнинг фойдалана олиши чекланиши таъминланадиган муҳофаза.

Защита накоплением

uz - to'plash bilan muhofaza qilish

тўплаш билан муҳофаза қилиш

en - security by generation

Метод восстановления данных, хранящихся во внешней памяти, состоящий в том, что на дополнительный носитель копируются только те файлы, которые были созданы позднее определенного срока.

Tashqi hotirada saqlanadigan ma'lumotlarni tiklash metodi. Qo'shimcha tashuvchiga ma'lum bir muddatdan keyin yaratilgan fayllar ko'chirilishida ifodalanadi.

Ташқи хотирада сақланадиган маълумотларни тиклаш методи. Қўшимча ташувчига маълум бир муддатдан кейин яратилган файллар кўчирилишида ифодаланеди.

Защита непосредственная

Меры, предусматривающие физическую защиту

uz - bevosita muhofaza qilish
 бевосита муҳофаза қилиш
en - physical security

ресурсов от преднамеренных или случайных угроз.

Resurslarning qasddan qilinadigan yoki tasodifiy tahdidlardan fizik muhofaza qilinishini koʻzda tutadigan chora-tadbirlar.

Ресурсларнинг қасддан қилинадиган ёки тасодифий таҳдидлардан физик муҳофаза қилинишини кўзда тутадиган чора-тадбирлар.

Защита объектов

uz - obyektlarni muhofaza qilish
 объектларни муҳофаза қилиш
en - object protection

Средства защиты объектов (например, файлов, носителей, сейфов), которые могут быть выведены из защищенной области.

Muhofazalangan sohadan chiqarilishi mumkin boʻlgan obyektlarni (masalan, fayllarni, tashuv-chilarni, seyflarni) muhofaza qilish vositalari.

Муҳофазаланган соҳадан чиқарилиши мумкин бўлган объектларни (масалан, файлларни, ташувчиларни, сейфларни) муҳофаза қилиш воситалари.

Защита от записи

uz - yozib olishdan muhofaza qilish
 ёзиб олишдан муҳофаза қилиш
en - write protect

Способ защиты информации на диске, заключающийся в заклеивании метки считывания на дискетах 5,25" и задвижки метки считывания на дискетах 3,5", что предотвращает запись новых данных и сохраняет имеющиеся от разрушения.

Diskdagi axborotni, 5,25" disketalarida solishtirib oʻqish belgisini yopishtirish va 3,5" disketalarida solishtirib oʻqish belgisini surib, muhofaza qilish usuli, bu yangi maʼlumotlar yozib olishning oldini oladi va mavjud maʼlumotlarni yoʻqolishdan saqlaydi.

Дискдаги ахборотни, 5,25" дискеталарида солиштириб ўқиш белгисини ёпиштириш ва 3,5" дискеталарида солиштириб ўқиш белгисини суриб, муҳофаза қилиш усули, бу янги маълумотлар ёзиб олишнинг олдини олади ва мавжуд маълумотларни йўқолишдан сақлайди.

Защита от копирования
uz - nusxa koʻchirilishidan

1 Использование специальных методов для обнаружения или предотвращения несанкциониро-

muhofaza qilish
 nusxa kўчирилишидан
 муҳофаза қилиш
en - copy protection

ванного копирования данных, программного или аппаратно-программного обеспечения.

2 Способ предотвращения копирования информации, записанной на магнитном носителе, например на диске, содержащем программный продукт коммерческого назначения.

1 Ma'lumotlardan, dasturiy yoki dasturiy-apparat ta'minotidan ruxsat etilmagan tarzda nusxa ko'chirilishini aniqlash yoki oldini olish uchun maxsus metodlarning qo'llanilishi.

2 Magnit tashuvchida, masalan, tijorat yo'nalishidagi dasturiy mahsulotga ega diskda, yozilgan axborotdan nusxa ko'chirilishining oldini olish usuli.

1 Маълумотлардан, дастурий ёки дастурий-аппарат таъминотидан рухсат этилмаган тарзда нусха кўчирилишини аниқлаш ёки олдини олиш учун махсус методларнинг қўлланилиши.

2 Магнит ташувчида, масалан, тижорат йўналишидаги дастурий маҳсулотга эга дискда, ёзилган ахборотдан нусха кўчирилишининг олдини олиш усули.

Защита от несанкционированного доступа
uz - ruxsatsiz foydalana
 olishdan muhofaza qilish
 рухсатсиз фойдалана
 олишдан муҳофаза қилиш
en - protection from
 unauthorized access

Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем) информации прав или правил доступа к защищаемой информации.

Muhofaza qilinadigan axborotdan foydalana olishning huquqiy hujjatlari bilan yoki axborot mulkdori (egasi) tomonidan belgilangan huquqlar yoki qoidalar buzilgan holda manfaatdor subyekt tomonidan muhofaza qilinadigan axborotni olishning oldini olish bo'yicha faoliyat.

Муҳофаза қилинадиган ахборотдан фойдалана олишнинг ҳуқуқий ҳужжатлари билан ёки ахборот мулкдори (эгаси) томонидан белгиланган ҳуқуқлар ёки қоидалар бузилган ҳолда манфаатдор субъект томонидан муҳофаза қилинадиган ахборотни олишнинг олдини олиш бўйича фаолият.

Защита от ошибок

uz - xatolardan muhofaza qilish

хатолардан муҳофаза қилиш

en - error protection

1 Совокупность аппаратных и/или программных средств, предотвращающих или уменьшающих возможность появления ошибок.

2 Средства и способы контроля допустимости значений входных параметров.

1 Xatolar paydo bo‘lish imkoniyatini bartaraf qiluvchi yoki kamaytiruvchi apparat va/yoki dasturiy vositalar jami.

2 Kirish parametrlari qiymatlarining yo‘l qo‘yib bo‘lishligini nazorat qilish vositalari va usullari.

1 Хатолар пайдо бўлиш имкониятини бартараф қилувчи ёки камайтирувчи аппарат ва/ёки дастурий воситалар жами.

2 Кириш параметрлари қийматларининг йўл қўйиб бўлишлигини назорат қилиш воситалари ва усуллари.

Защита от чтения

uz - o‘qishdan muhofaza qilish
ўқишдан муҳофаза қилиш

en - read protection

Запрещение обращения к файлу для выполнения операции чтения данных. Разрешается только запись данных.

Ma'lumotlarni o'qish uchun faylga murojaat qilishning taqiqlanishi. Faqat ma'lumotlarni yozishga ruxsat etiladi.

Маълумотларни ўқиш учун файлга мурожаат қилишнинг тақиқланиши. Фақат маълумотларни ёзишга рухсат этилади.

Защита памяти

uz - хотирани muhofaza qilish

хотирани муҳофаза қилиш

en - memory protection,
storage protection

1 Механизм контроля за доступом к какой-либо области памяти с учетом разработанных обращений.

2 Средства и способы предотвращения несанкционированного доступа к некоторым участкам памяти с целью сохранения неизменности записанных данных.

1 Ishlab chiqilgan murojaatlarni hisobga olgan holda, хотиранинг qandaydir qismiga kira olishni mexanik nazorat qilish .

2 Yozilgan ma'lumotlarning doimiyligini saqlash maqsadida, хотиранинг ba'zi bir qismlariga ruxsat

etilmagan tarzda kirishning oldini olish vositalari hamda usullari.

1 Ишлаб чиқилган мурожаатларни ҳисобга олган ҳолда, хотиранинг қандайдир қисмига кира олишни механик назорат қилиш .

2 Ёзилган маълумотларнинг доимийлигини сақлаш мақсадида, хотиранинг баъзи бир қисмларига рухсат этилмаган tarzda киришнинг олдини олиш воситалари ҳамда усуллари.

Защита паролем

uz - parol bilan muhofaza qilish

пароль билан муҳофаза қилиш

en - password protection

1 Механизм управления доступом к системе, обеспечивающий сохранение целостности программного обеспечения в составе системы или сети.

2 Способ защиты данных, при котором для получения доступа к ним необходимо ввести пароль.

1 Tizimdan foydalana olishni boshqarish mexanizmi bo'lib, tizim yoki tarmoq ichida dasturiy ta'minot yaxlitligi saqlanishini ta'minlaydi.

2 Ma'lumotlarni muhofaza qilish usuli, bunda ma'lumotlardan foydalana olish uchun parol kiritish zarur.

1 Tizimdan foydalana olishni boshqarish mexanizmi bo'lib, tizim yoki tarmoq ichida dasturiy ta'minot yaxlitligi saqlanishini ta'minlaydi.

2 Ma'lumotlarni muhofaza qilish usuli, bunda ma'lumotlardan foydalana olish uchun parol kiritish zarur.

Защита поля избирательная

uz - tanlangan maydon muhofazasi

танланган майдон муҳофазаси

en - selective field protection

Защита специальных полей в пределах передаваемого сообщения.

Uzatiladigan xabar doirasida maxsus maydonlarni muhofaza qilish.

Uzatiladigan xabar doirasida maxsus maydonlarni muhofaza qilish.

Защита прав пользователей

uz - foydalanuvchilar huquqlarini muhofaza qilish

foyдаланувчилар ҳуқуқларини муҳофаза қилиш

en - user rights protection

Совокупность правил, методов и средств, направленных на обеспечение беспрепятственного и своевременного доступа пользователей к программам и данным и защиту их информации от использования другими лицами.

Foydalanuvchilarning dasturlar va ma'lumotlardan

to‘sqinliklarsiz hamda o‘z vaqtida foydalana olishlarini ta‘minlashga va ulardagi axborotdan boshqa shaxslar foydalanishidan muhofaza qilishga qaratilgan qoidalar, metodlar hamda vositalar jami.

Фойдаланувчиларнинг дастурлар ва маълумотлардан тўсқинликларсиз ҳамда ўз вақтида фойдалана олишларини таъминлашга ва улардаги ахборотдан бошқа шахслар фойдаланишидан муҳофаза қилишга қаратилган қоидалар, методлар ҳамда воситалар жами.

Защита предупредительная

uz - ogohlantiruvchi
muhofaza qilish

огоҳлантирувчи
муҳофаза қилиш

en - disincentive protection

Организационные меры защиты от копирования, предусматривающие суровый штраф или угрозу штрафа лицу, которое пытается несанкционированно скопировать программу или файл.

Nusxa ko‘chirishdan muhofaza qilish bo‘yicha tashkiliy chora-tadbirlar. Dastur yoki fayldan ruxsat etilmagan tarzda nusxa ko‘chirishga urinadigan shaxs jarimaga tortilishini yoki jarima to‘lash tahdidini ko‘zda tutadi.

Нусха кўчиришдан муҳофаза қилиш бўйича ташкилий чора-тадбирлар. Дастур ёки файлдан рuxсат этилмаган тарзда нусха кўчиришга уринадиган шахс жаримага тортилишини ёки жарима тўлаш тахдидини кўзда тутди.

Защита программы

uz - dasturni muhofaza qilish

дастурни муҳофаза қилиш

en - software lock

(software protection)

Совокупность условий, предотвращающих запуск программы на выполнение.

Dasturning bajarilishi uchun ishga tushirib yuborilishini bartaraf etuvchi shartlarning jami.

Дастурнинг бажарилиши учун ишга тушириб юборилишини бартараф этувчи шартларнинг жами.

Защита системы

uz - tizimni muhofaza qilish

тизимни муҳофаза қилиш

en - system protection

(sistem security)

Совокупность мер, предпринимаемых для исключения несанкционированного доступа к программам и данным системы или случайного вмешательства в ее работу.

3

Dasturlar va tizim ma'lumotlaridan ruxsat etilmagan tarzda foydalana olishni yoki tizim ishiga tasodifiy aralashishni bartaraf etish maqsadida ko'riladigan chora-tadbirlar jami.

Дастурлар ва тизим маълумотларидан рuxсат этилмаган тарзда фойдалана олишни ёки тизим ишига тасодифий аралашини бартараф этиш мақсадида кўриладиган чора-тадбирлар жами.

Защита файла

uz - faylni muhofaza qilish

файлни муҳофаза қилиш

en - file protection

Реализация соответствующих административных, технических или физических мер для предотвращения несанкционированного доступа, модификации или удаления файла.

Faylga ruxsatsiz kirish, uni o'zgartirish yoki o'chirishning oldini olish maqsadida tegishli ma'muriy, texnik yoki fizik chora-tadbirlarni amalga oshirish.

Файлга рuxсатсиз кириш, уни ўзгартириш ёки ўчиришининг олдини олиш мақсадида тегишли маъмурий, техник ёки физик чора-тадбирларни амалга ошириш.

Защита ФБО собственная

uz - OXF shaxsiy himoyasi

ОХФ шахсий ҳимояси

en - TSF self-protection

Свойство архитектуры безопасности, посредством которого ФБО не может быть нарушена посторонним для нее кодом или логическими объектами.

Xavfsizlik arxitekturasining xususiyati bo'lib, uning yordamida OXF uning uchun begona bo'lgan kod yoki mantiqiy obyektlar tomonidan buzilmaydi.

Хавфсизлик архителктурасининг хусусияти бўлиб, унинг ёрдамида ОХФ унинг учун бегона бўлган код ёки мантиқий объектлар томонидан бузилмайди.

Защита физическая

uz - jismoniy muhofaza

жисмоний муҳофаза

en - physical protection

Механизмы и процедуры, предназначенные для защиты компонентов телекоммуникационной или информационной систем и их структуры от физического ущерба, возникающего вследствие умышленных действий злоумышленников или

халатности обслуживающего персонала.

Telekommunikatsiya yoki axborot tizimlari komponentlarini va ularning strukturasi jinoyatkorlarning qasddan qilinadigan harakatlari yoki xizmat ko'rsatuvchi xodimlarning mas'uliyatsizliklari natijasida yetkaziladigan jismoniy zarardan himoya qilish uchun mo'ljallangan mexanizm va protseduralar.

Телекоммуникация ёки ахборот тизимлари компонентларини ва уларнинг структурасини жинояткорларнинг қасддан қилинадиган ҳаракатлари ёки хизмат кўрсатувчи ходимларнинг масъулиятсизликлари натижасида етказиладиган жисмоний зарардан ҳимоя қилиш учун мўлжалланган механизм ва процедуралар.

Защита эшелонированная
uz - birin-ketin joylashtirib muhofaza qilish

бирин-кетин жойлаштириб муҳофаза қилиш
en - defence-in-depth

Концепция системы безопасности, при которой каждая подсистема в сети защищается до максимально возможного уровня.

Xavfsizlik tizimi konsepsiyasi, unda tarmoqdagi har bir kichik tizim mumkin bo'lgan maksimal darajagacha muhofaza qilinadi.

Хавфсизлик тизими концепцияси, унда тармоқдаги ҳар бир кичик тизим мумкин бўлган максимал даражагача муҳофаза қилинади.

Защищенное техническое средство информатизации
uz - himoyalangan axborotlashtirish texnik vositasi

ҳимояланган ахборотлаштириш техник воситаси
en - protected technical facility of informatization

Техническое средство информатизации, в котором реализован комплекс средств защиты от нарушения целостности и утечки по техническим каналам обрабатываемой на них информации.

Qayta ishlanadigan axborot butunligi buzilishdan va texnik kanallar orqali chiqib ketishdan muhofaza qilish vositalari kompleksi bo'lgan axborotlashtirish texnik vositasi.

Қайта ишланадиган ахборот бутунлиги бузилишдан ва техник каналлар орқали чиқиб кетишдан муҳофаза қилиш воситалари комплекси бўлган ахборотлаштириш техник воситаси.

Защищенность

Способность системы противостоять несанкцио-

3

uz - muhofaza qilinganlik
муҳофаза қилинганлик
en - security

нироvanному доступу к захищаемой информации, ее искажению или разрушению.

Tizimning, muhofaza qilinadigan axborotdan ruxsat etilmagan tarzda foydalana olishga, uning buzilishiga yoki unga zarar yetkazilishiga qarshi tura olish qobiliyati.

Тизимнинг, муҳофаза қилинадиган ахборотдан рухсат этилмаган тарзда фойдалана олишга, унинг бузилишига ёки унга зарар етказилишига қарши тура олиш қобилияти.

Заявитель
uz - talabgor
талабгор
en - claimant

Объект, который является администратором доступа в целях аутентификации или представляет его. Заявитель выполняет функции, необходимые для осуществления обменов данными аутентификации от имени администратора доступа.

Autentifikatsiya qilish maqsadida foydalana olish ma'muri hisoblanadigan obyekt. Talabgor foydalana olish ma'muri nomidan autentifikatsiya ma'lumotlari almashinuvini amalga oshirish uchun zarur bo'lgan vazifalarni bajaradi.

Аутентификация қилиш мақсадида фойдалана олиш маъмури ҳисобланадиган объект. Талабгор фойдалана олиш маъмури номидан аутентификация маълумотлари алмашинувини амалга ошириш учун зарур бўлган вазифаларни бажаради.

Заявление о применимости
uz - qo'llanishlik to'g'risidagi bayonot
қўлланишлик
тўғрисидаги баёнот
en - statement of applicability

Документированное заявление, описывающее цели и средства управления, соответствующие и применимые к системе управления информационной безопасности организации.

Tashkilot axborot xavfsizligini boshqarish tizimiga mos keladigan va qo'llaniladigan boshqarish vositalari va maqsadlarni tavsiflovchi hujjatlashtirilgan bayonnoma.

Ташкилот ахборот хавфсизлигини бошқариш тизимига мос келадиган ва қўлланиладиган бошқариш воситалари ва мақсадларни тавсифловчи ҳужжатлаштирилган баённома.

Злоумышленник**uz** - jinoyatkor

жинояткор

en - intruder, malicious user,
hacker

1 Нарушитель, умышленно действующий из корыстных побуждений.

2 Лицо или организация, заинтересованные в получении несанкционированного доступа к информационной системе и ее ресурсам и совершившие преднамеренные действия для их несанкционированного получения и изменения.

3 Лицо, получившее несанкционированный доступ с целью осуществления злонамеренных вызовов.

4 Лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты.

1 G‘arazli niyatda qasddan harakat qiluvchi buzg‘unchi.

2 Axborot tizimi va uning resurslaridan ruxsat etilmagan tarzda foydalanishdan manfaatdar bo‘lgan va ularni ruxsat etilmagan tarzda olish, o‘zgartirish uchun oldindan o‘ylab harakat qilgan shaxs yoki tashkilot.

3 Yomon niyatdagi chaqiruvlarni amalga oshirish maqsadida ruxsat etilmagan foydalana olishga ega bo‘lgan shaxs.

4 Muhofaza obyektining axborot xavfsizligi buzilishini anglagan holda harakat qiluvchi shaxs.

1 Ғаразли ниятда қасддан ҳаракат қилувчи бузғунчи.

2 Ахборот тизими ва унинг ресурсларидан рұхсат этилмаган тарзда фойдаланишдан манфаатдар бўлган ва уларни рұхсат этилмаган тарзда олиш, ўзгартириш учун олдиндан ўйлаб ҳаракат қилган шахс ёки ташкилот.

3 Ёмон ниятдаги чақирувларни амалга ошириш мақсадида рұхсат этилмаган фойдалана олишга эга бўлган шахс.

4 Муҳофаза объектнинг ахборот хавфсизлиги бузилишини англаган ҳолда ҳаракат қилувчи шахс.

**Злоупотребление
компьютерное****uz** - kompyuter suiiste'molligi

компьютер

суиистеъмоллиги

en - computer abuse

Умышленное или случайное несанкционированное действие, которое влияет на компьютерную безопасность системы обработки данных или нарушает ее.

Ma'lumotlarni qayta ishlash tizimining kompyuter xavfsizligiga ta'sir etadigan yoki uni buzadigan, qasddan yoki tasodifiy ruxsat berilmagan harakat.

Маълумотларни қайта ишлаш тизимининг компьютер хавфсизлигига таъсир этадиган ёки уни бузадиган, қасдан ёки тасодифий рухсат берилмаган ҳаракат.

**Знак защитный
специальный**

uz - maxsus muhofaza belgisi
махсус муҳофаза белгиси
en - special security mark

Сертифицированное и зарегистрированное в установленном порядке изделие, предназначенное для контроля несанкционированного доступа к объектам защиты путем определения подлинности и целостности самого знака или композиции «Специальный защитный сигналподложка» по критериям соответствия характерным признакам.

Belgining o‘zini haqiqiyiligini va yaxlitligini aniqlash yoki xarakterli alomatlariga mos kelishlik mezonlari bo‘yicha, «Maxsus muhofaza belgisi – taglik» kompozitsiyasini aniqlash yo‘li bilan muhofaza qilindigan obyektlardan ruxsat etilmagan tarzda foydalana olishni nazorat qilish uchun mo‘ljallangan, belgilangan tartibda sertifikatlangan va ro‘yxatga olingan buyum.

Белгининг ўзини ҳақиқийлигини ва яхлитлигини аниқлаш ёки хarakterли аломатларга мос келишлик мезонлари бўйича, «Махсус муҳофаза белгиси – таглик» композициясини аниқлаш йўли билан муҳофаза қилинадиган объектлардан рухсат этилмаган тарзда фойдалана олишни назорат қилиш учун мўлжалланган, белгиланган тартибда сертификатланган ва рўйхатга олинган буюм.

**Знак соответствия в области
защиты информации**

uz - axborotni muhofaza qilish sohasidagi muvofiqlik belgisi
ахборотни муҳофаза қилиш соҳасидаги мувофиқлик белгиси
en - compliance mark in the field of information security

Защищенный в установленном порядке знак, применяемый или выданный в соответствии с правилами системы сертификации, указывающий, что обеспечивается необходимая уверенность в том, что данное защищенное изделие, техническое средство или способ защиты информации соответствует конкретному стандарту или другому нормативному документу.

Sertifikatlash tizimi qoidalariga muvofiq beriladigan yoki qo‘llaniladigan, berilgan muhofazalangan buyum, texnik vosita yoki axborotni muhofaza qilish

usuli muayyan standartga yoki boshqa normativ hujjatga mos kelishini ko'rsatadigan, belgilangan tartibda muhofazalangan belgi.

Сертификатлаш тизими қоидаларига мувофиқ берилладиган ёки қўлланиладиган, берилган муҳофазаланган буюм, техник восита ёки ахборотни муҳофаза қилиш усули муайян стандартга ёки бошқа норматив ҳужжатга мос келишини кўрсатадиган, белгиланган тартибда муҳофазаланган белги.

Значение атрибута

uz - atribut qiymati

атрибут қиймати

en - attribute value

Тип атрибута, который обозначает конкретный экземпляр класса информации, например, персональные имена, и является частью атрибута.

Axborot klassining ma'lum bir nusxasini, masalan, shaxsiy nomlarni belgilaydigan atribut turi. Atributning bir qismi hisoblanadi.

Ахборот классининг маълум бир нусхасини, масалан, шахсий номларни белгиладиган атрибут тури. Атрибутнинг бир қисми ҳисобланади.

Значение контрольное криптографическое

uz - kriptografik nazorat

qiymati

криптографик назорат қиймати

en - cryptographic checkvalue

Информация, определяемая в ходе криптографического преобразования блока данных и предназначенная для контроля целостности передаваемой информации.

Ma'lumotlar blokini kriptografik qayta o'zgartirishda aniqlanadigan va uzatiladigan axborotning yaxlitligini nazorat qilish uchun mo'ljallangan axborot.

Маълумотлар блокини криптографик қайта ўзгартиришда аниқланадиган ва узатиладиган ахборотнинг яхлитлигини назорат қилиш учун мўлжалланган ахборот.

Значение начальной установки

uz - boshlang'ich o'rnatish

qiymati

бошланғич ўрнатиш

Последовательность символов, используемая для установки генератора ключевого потока в заданное положение.

Kalit oqimi generatorini berilgan (ma'lum bir)

қиймати
en - initialization value

holatga oʻrnatish uchun qoʻllaniladigan simvollar ketma-ketligi.

Значение секретное коллективное

uz - jamoaviy maxfiy qiymat
 жамоавий махфий қиймат
en - shared secret

Калит оқими генераторини берилган (маълум бир) ҳолатга ўрнатиш учун қўлланиладиган символлар кетма-кетлиги.

Ключ системы защиты для криптографических алгоритмов.

Muhofaza qilish tizimining, kriptografik algoritmlar uchun moʻljallangan kaliti.

Муҳофаза қилиш тизимининг, криптографик алгоритмлар учун мўлжалланган калити.

Зона

uz - zona
 зона
en - protected area

Область, защищенная системой безопасности.

Xavfsizlik tizimi bilan muhofaza qilingan soha.

Хавфсизлик тизими билан муҳофаза қилинган соҳа.

Зона безопасности

uz - xavfsizlik zonasi
 хавфсизлик зонаси
en - security zone

1 Пространство, в пределах которого обеспечивается требуемый уровень защиты информации.

2 Механизм, определенный в браузере Microsoft Internet Explorer компании Microsoft, позволяющий задавать настройки безопасности для групп Интернет-серверов.

Примечание – Для каждой из зон возможно использовать различные уровни безопасности, определяющие возможные действия, допустимые для этого сервера (запуск Java-апплетов, управляющих элементов ActiveX, установление защищенного соединения по протоколу SSL и т.п.).

1 Axborot muhofaza qilinishining talab etiladigan darajasi ta'minlanadigan makon.

2 Internet-serverlar guruhi uchun xavfsizlik sozlashlari oʻrnatilishiga imkon beruvchi Microsoft kompaniyasining Microsoft Internet Explorer brauzerida belgilangan mexanizm.

Izoh – Zonalarning har biri uchun shu server uchun yoʻl qoʻyiladigan, mumkin boʻlgan harakatlarni belgilovchi xavfsizlikning turli darajalarini qoʻllash mumkin (*Java*-appletlarini, *ActiveX* boshqaruvchi elementlarini ishga tushirish, *SSL* protokoli boʻyicha muhofazalangan ulanishni oʻrnatish va

sh.k.).

1 Ахборот муҳофаза қилинишининг талаб этиладиган даражаси таъминладиган макон.

2 Интернет-серверлар гуруҳи учун хавфсизлик созланишлари ўрнатилишига имкон берувчи Microsoft компаниясининг Microsoft Internet Explorer браузерда белгиланган механизм.

Изоҳ – Зоналарнинг ҳар бири учун шу сервер учун йўл қўйилладиган, мумкин бўлган ҳаракатларни белгиловчи хавфсизликнинг турли даражаларини қўллаш мумкин (Java-апплетларини, ActiveX бошқарувчи элементларини ишга тушириш, SSL протоколи бўйича муҳофазаланган уланишни ўрнатиш ва ш.к.).

Зона контролируемая

uz - nazorat qilinadigan zona

назорат қилинадиган зона

en - under control zone

Территория вокруг технического средства обработки информации, в пределах которой не допускается несанкционированное пребывание посторонних лиц и транспортных средств.

Axborotni qayta ishlash texnik vositasi atrofidagi hudud, uning chegarasida begona shaxslarning va transport vositalarining ruxsat etilmagan tarzda bo‘lishiga yo‘l qo‘yilmaydi.

Ахборотни қайта ишлаш техник воситаси атрофидаги худуд, унинг чегарасида бегона шахсларнинг ва транспорт воситаларининг рухсат этилмаган тарзда бўлишига йўл қўйилмайди.

Зона опасная 1

uz - 1-xavfli zona

1-хавfli зона

en - 1 danger area

Пространство вокруг технического средства обработки информации, в пределах которого на случайных антеннах наводится опасный сигнал выше допустимого нормированного уровня. В зоне 1 запрещается размещение случайных антенн, имеющих выход по токопроводящим коммуникациям за пределы контролируемой зоны.

Axborotni qayta ishlash texnik vositasining atrofidagi maydon bo‘lib, uning doirasida tasodifiy antennalarda yo‘l qo‘yiladigan normalangan darajadan yuqori bo‘lgan xavfli signal hosil qilinadi. Birinchi zonada, tok o‘tkazadigan kommunikatsiyalar orqali nazorat qilinadigan zonadan

3

tashqariga chiqishi bo'lgan tasodifiy antennalarni joylashtirish taqiqlanadi.

Ахборотни қайта ишлаш техник воситасининг атрофидаги майдон бўлиб, унинг доирасида тасодифий антенналарда йўл қўйиладиган нормаланган даражадан юқори бўлган хавфли сигнал ҳосил қилинади. Биринчи зонада, ток ўтказадиган коммуникациялар орқали назорат қилинадиган зонадан ташқарига чиқиши бўлган тасодифий антенналарни жойлаштириш тақиқланади.

Зона опасная 2

uz - 2-xavfli zona

2-xavfli zona

en - 2 danger area

Пространство вокруг технического средства обработки информации, в пределах которого отношение опасный сигнал/помеха для составляющих напряженности электромагнитного поля превышает допустимое нормированное значение.

Axborotni qayta ishlash texnik vositasining atrofidagi maydon bo'lib, uning doirasida elektromagnit maydon kuchlanganligini tashkil etuvchilar uchun xavfli signal/xalaqit nisbati yo'l qo'yiladigan normalangan qiymatdan oshadi.

Ахборотни қайта ишлаш техник воситасининг атрофидаги майдон бўлиб, унинг доирасида электромагнит майдон кучланганлигини ташкил этувчилар учун хавфли сигнал/халақит нисбати йўл қўйиладиган нормаланган қийматдан ошади.

И

Идентификатор

uz - identifikator

идентификатор

en - identity

1 Представление однозначной идентификации логического объекта (например, пользователя, процесса или диска) в контексте соответствующего объекта оценки.

Примечание – Примером такого представления может быть строка символов. Для человека-пользователя представлением может быть его полное или сокращенное имя, либо (личный) псевдоним.

2 Код или символическое имя, однозначно характеризующее объект и позволяющее выделить его

И

среди множества других объектов. Идентификатор может указывать на тип сети, протокол, номер порта и др.

3 Средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

1 Tegishli baholash obykti kontekstida mantiqiy obyekt (masalan, foydalanuvchi, jarayon yoki disk) qat'iy identifikatsiya qilinganligining taqdim etilishi. Izoh – Bunga simvollar qatori misol sifatida ko'rsatilishi mumkin. Foydalanuvchi-odam uchun uning to'liq yoki qisqartirilgan ismi, yo (shaxsiy) laqabi ko'rsatilishi mumkin.

2 Obyektni tavsiflovchi va uni boshqa ko'plab obyektlar orasida ajratib ko'rsatish imkonini beruvchi kod yoki ramziy nom. Identifikator tarmoq turini, protokolini, port raqamini va b.q. ko'rsatishi mumkin.

3 Foydalana olish subyekti yoki obyektining farqli belgisini aks ettiruvchi, foydalana olishni identifikatsiya qilish vositasi. Foydalanuvchilar uchun foydalana olishni identifikatsiya qilishning asosiy vositasi parol hisoblanadi.

1 Тегишли баҳолаш объекти контекстида мантикий объект (масалан, фойдаланувчи, жараён ёки диск) қатъий идентификация қилинганлигининг тақдим этилиши.

Изоҳ – Бунга символлар қатори мисол сифатида кўрсатилиши мумкин. Фойдаланувчи-одам учун унинг тўлиқ ёки қисқартирилган исми, ё (шахсий) лақаби кўрсатилиши мумкин.

2 Объектни тавсифловчи ва уни бошқа кўплаб обyekтлар орасида ажратиб кўрсатиш имконини берувчи код ёки рамзий ном. Идентификатор тармоқ турини, протоколинн, порт рақамини ва б.қ. кўрсатиши мумкин.

3 Фойдалана олиш субъекти ёки объектининг фарқли белгисини акс эттирувчи, фойдалана олишни идентификация қилиш воситаси. Фойдаланувчилар учун фойдалана олишни идентифика-

И

Идентификатор безопасности

uz - xavfsizlik identifikatori

хавфсизлик

идентификатори

en - security identifier

Идентификатор безопасности общеизвестный

uz - hammaga ma'lum

xavfsizlik identifikatori

хаммага маълум

хавфсизлик идентификатори

en - well-known security

identifier

Идентификатор диагностического сообщения

uz - diagnostik xabar

identifikatori

диагностик хабар

идентификатори

en - diagnostic message

identifier

Идентификатор доступа

uz - foydalana olish

identifikatori

фойдалана олиш

идентификатори

en - access identifier

ция қилишнинг асосий воситаси пароль ҳисобланади.

Глобальный уникальный идентификатор субъекта системы безопасности. Различают идентификаторы безопасности учетных записей и общеизвестные идентификаторы безопасности.

Xavfsizlik tizimi subyektining global noyob identifikatori. Hisobga olinadigan yozuvlarning xavfsizlik identifikatorlari va hammaga ma'lum xavfsizlik identifikatorlari farqlanadi.

Хавфсизлик тизими субъектининг глобал ноёб идентификатори. Ҳисобга олинadиган ёзувларнинг хавфсизлик идентификаторлари ва ҳаммага маълум хавфсизлик идентификаторлари фарқланади.

Идентификатор безопасности с фиксированным численным значением и назначением для системы защиты.

Muhofaza tizimi uchun qayd qilingan sonli qiymatga va belgilanishga ega xavfsizlik identifikatori.

Муҳофаза тизими учун қайд қилинган сонли қийматга ва белгиланишга эга хавфсизлик идентификатори.

Код сообщения, выдаваемого системной программой в ответ на обнаруженную ошибку.

Tizim dasturi tomonidan aniqlangan xatoga javoban beriladigan xabar kodi.

Тизим дастури томонидан аниқланган хатога жавобан берилadиган хабар коди.

Уникальный признак субъекта или объекта доступа.

Foydalana olish subyekti yoki obyektining noyob belgisi.

И

Идентификатор задачи

uz - vazifa identifikatori

вазифа идентификатори

en - task identifier

Фойдалана олиш субъекти ёки объектининг ноёб белгиси.

Символьный код, приписываемый выполняющейся или готовой к выполнению задаче.

Bajariladigan yoki bajarishga tayyor vazifaga beriladigan ramziy kod.

Бажариладиган ёки бажаришга тайёр вазифага берилладиган рамзий код.

Идентификатор

относительный

uz - nisbiy identifikator

нисбий идентификатор

en - relative identifier

Младшая часть идентификатора безопасности. В пределах домена идентификаторы безопасности имеют одинаковую старшую часть, а относительный идентификатор принимает последовательно возрастающие значения, начиная с 1000.

Xavfsizlik identifikatorining kichik qismi. Domen doirasida xavfsizlik identifikatorlari bir xil katta qismga ega, nisbiy identifikator esa 1000 dan boshlab ketma-ket ko‘payuvchi qiymatni oladi.

Хавфсизлик идентификаторининг кичик қисми. Домен доирасида хавфсизлик идентификаторлари бир хил катта қисмга эга, нисбий идентификатор эса 1000 дан бошлаб кетма-кет кўпаювчи қийматни олади.

Идентификатор

пользователя

uz - foydalanuvchining identifikatori

фойдаланувчининг идентификатори

en - user identifier, user ID

1 Последовательность символов или изображение, которое используется системой обработки данных для идентификации пользователя.

2 Персональное обозначение (имя, код и т.п.), позволяющее однозначно выделить идентифицируемый субъект (объект) среди всех других в полном множестве субъектов (объектов).

3 Символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы.

1 Foydalanuvchini identifikatsiya qilish uchun ma'lumotlarni qayta ishlash tizimida foydalaniladigan tasvir yoki simvollar ketma-ketligi.

И

2 Barcha boshqa subyektlar (obyektlar)ning to'liq ko'pligi o'rtasida identifikatsiya qilinuvchi subyekt (obyekt)ni bir xil ajratishga imkon beradigan xususiy belgilanish (nom, kod va sh.k.).

3 Alohida shaxsga yoki shaxslar guruhiga beriladigan hamda hisoblash tizimi resurslaridan foydalanishga ruxsat beradigan ramziy nom.

1 Фойдаланувчини идентификация қилиш учун маълумотларни қайта ишлаш тизимида фойдаланиладиган тасвир ёки символлар кетма-кетлиги.

2 Барча бошқа субъектлар (объектлар)нинг тўлиқ кўплиги ўртасида идентификация қилинувчи субъект (объект)ни бир хил ажратишга имкон берадиган хусусий белгиланиш (ном, код ва ш.к.).

3 Алоҳида шахсга ёки шахслар гуруҳига бериладиган ҳамда ҳисоблаш тизими ресурсларидан фойдаланишга рухсат берадиган рамзий ном.

Идентификатор

пользователя сети

uz - tarmoqdan foydalanuvchi identifikatori

тармоқдан фойдаланувчи идентификатори

en - network user identifier

Уникальный код, используемый для идентификации пользователя службой коммутации пакетов.

Paketlarni kommutatsiyalash xizmati tomonidan foydalanuvchini identifikatsiya qilish uchun ishlatiladigan noyob kod.

Пакетларни коммутациялаш хизмати томонидан фойдаланувчини идентификация қилиш учун ишлатиладиган ноёб код.

Идентификация

uz - identifikatsiya qilish

идентификация қилиш

en - identification

1 Присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

2 Процесс распознавания определенных компонентов системы, обычно с помощью уникальных имен (идентификаторов), воспринимаемых системой.

3 Выяснение личности пользователя с целью предоставления ему определенного набора прав и привилегий при работе с системой, например,

И

определение соответствующих пользователю идентификаторов безопасности.

1 Foydalana olish subyektlari va obyektlariga identifikator berish va/yoki taqdim etilayotgan identifikatorni o'zlashtirilgan identifikatorlar ro'y-xati bilan solishtirish.

2 Tizimning ayrim komponentlarini, odatda tizimda qabul qilinadigan noyob nomlar (identifikatorlar) yordamida aniqlash jarayoni.

3 Foydalanuvchining shaxsini, unga tizim bilan ishlashda huquq va imtiyozlarning ma'lum to'plamini berish maqsadida aniqlash, masalan, foydalanuvchiga taalluqli xavfsizlik identifikatorini belgilash.

1 Фойдалана олиш субъектлари ва объектларига идентификатор бериш ва/ёки тақдим этилаётган идентификаторни ўзлаштирилган идентификаторлар рўйхати билан солиштириш.

2 Тизимнинг айрим компонентларини, одатда тизимда қабул қилинадиган ноёб номлар (идентификаторлар) ёрдамида аниқлаш жараёни.

3 Фойдаланувчининг шахсини, унга тизим билан ишлашда ҳуқуқ ва имтиёзларнинг маълум тўпламини бериш мақсадида аниқлаш, масалан, фойдаланувчига тааллуқли хавфсизлик идентификаторини белгилаш.

**Идентификация
аутентифицированная**
uz - autentifikatsiya qilingan
identifikatsiya

аутентификация
қилинган идентификация
en - authenticated identity

Идентификация риска
uz - riskni identifikatsiya
qilish

Отличительный идентификатор администратора доступа, удостоверяемый путем аутентификации.

Autentifikatsiya qilish yo'li bilan tasdiqlanadigan erkin foydalanish ma'murining farqlovchi identifikatori.

Аутентификация қилиш йўли билан тасдиқландиган эркин фойдаланиш маъмурининг фарқловчи идентификатори.

Процесс определения, составления перечня и описания риска.

Примечания

И

рискни идентификация
қилиш
en - risk identification

1 Идентификация риска может включать в себя источники риска, события, их причины и возможные последствия.
2 Идентификация риска может также включать в себя теоретический анализ, анализ хронологических данных, экспертных оценок и потребностей заинтересованных сторон.

Riskni aniqlash, ro‘yxatini tuzish va tavsiflash jarayoni.

Izohlar

1 Riskni identifikatsiya qilish riskning manbalarini, hodisalarini, ularning sabablari va ro‘y berishi mumkin bo‘lgan oqibatlarini o‘z ichiga oladi.

2 Riskni identifikatsiya qilish, shuningdek, xronologik ma’lumotlar tahlilini, ekspert baholashlarni va manfaatdor tomonlarning ehtiyojlarini o‘z ichiga oladi.

Рискни аниқлаш, рўйхатини тузиш ва тавсифлаш жараёни.

Изоҳлар

1 Рискни идентификация қилиш рискнинг манбаларини, ҳодисаларини, уларнинг сабаблари ва рўй бериши мумкин бўлган оқибатларини ўз ичига олади.

2 Рискни идентификация қилиш, шунингдек, хронологик маълумотлар таҳлилин, эксперт баҳолашларни ва манфаатдор томонларнинг эҳтиёжларини ўз ичига олади.

Идентификация сервисов
uz - servislarni
identifikatsiya qilish
сервисларни
идентификация қилиш
en - identifying services

Сопоставление выявленных открытых портов активным компонентам сетевого взаимодействия.

Aniqlangan ochiq portlarni tarmoq o‘zaro ishlaydigan aktiv komponentiga solishtirish.

Аниқланган очик портларни тармоқ ўзаро ишлайдиган актив компонентиға солиштириш.

Идентификация терминала
uz - terminalni
identifikatsiya qilish
терминални
идентификация қилиш
en - terminal identification

Процесс автоматической передачи на абонентский терминал установленного идентификатора, относящегося к удаленному абонентскому терминалу (терминалам), с которым (которыми) установлено соединение.

Ulanish o‘rnatilgan uzoqdagi abonent terminali (terminallari)ga taalluqli belgilangan identifikatorni abonent terminaliga avtomatik uzatish jarayoni.

Уланиш ўрнатилган узоқдаги абонент терминали (терминаллари)га тааллуқли белгиланган

И

идентификаторни абонент терминалига автоматик узатиш жараёни.

Избыточность

uz - ortiqchalik
ортиқчалик
en - redundancy

Введение в систему дополнительных компонентов сверх минимально необходимого их числа с целью повышения надежности системы. Различают избыточность аппаратную, информационную, алгоритмическую.

Tizimga uning ishonchliligini oshirish maqsadida, minimal zarur sonidan ko'p bo'lgan qo'shimcha komponentlarni kiritish. Apparat, axborot, algoritm ortiqchaligi farq qilinadi.

Тизимга унинг ишончилигини ошириш мақсадида, минимал зарур сонидан кўп бўлган қўшимча компонентларни киритиш. Аппарат, ахборот, алгоритм ортиқчалиги фарқ қилинади.

Избыточность кода

uz - kodning ortiqchaligi
коднинг ортиқчалиги
en - code redundancy

Разность между средним числом битов, используемых для кодирования одного сообщения источника, и минимально возможным числом битов, полученным из теоремы Шеннона.

Манбанинг бир хабарини кодлаш учун қўлланиладиган битларнинг о'ртача сони ва Шеннон теоремасидан олинган битларнинг mumkin bo'lgan eng kam soni o'rtasidagi farq.

Манбанинг бир хабарини кодлаш учун қўлланиладиган битларнинг ўртача сони ва Шеннон теоремасидан олинган битларнинг mumkin bo'lgan eng kam soni o'rtasidagi farq.

Излучение побочное

uz - yondosh nurlanish
ёндош нурланиш
en - compromising emanation

Нежелательно излучаемые сигналы, при перехвате и анализе которых может быть раскрыта обрабатываемая или передаваемая чувствительная информация.

Примечание – Например, побочными излучениями могут быть акустические и электромагнитные излучения.

Nomaqbul nurlanadigan signallar, ular ushlab qolinganda va tahlil qilinganda qayta ishlanadigan yoki uzatiladigan ta'sirchan axborot fosh etilishi mumkin. Izoh – Masalan, akustik va elektromagnit nurlanishlar

И

nomaqbul nurlanish bo‘lib hisoblanishi mumkin.

Номақбул нурланадиган сигналлар, улар ушлаб қолинганда ва таҳлил қилинганда қайта ишланадиган ёки узатиладиган таъсирчан ахборот фoш этилиши мумкин.

Изоҳ – Масалан, акустик ва электромагнит нурланишлар номақбул нурланиш бўлиб ҳисобланиши мумкин.

Изменение формата

uz - formatni o‘zgartirish

форматни ўзгартириш

en - format alteration

Использование нестандартного формата диска для защиты от копирования, в этом случае диск не может быть прочитан стандартными утилитами копирования.

Diskning nostandart formatidan nusxa ko‘chirishdan himoya qilishda foydalanish, bunda diskni nusxa ko‘chirishning standart utilitalari o‘qiy olmaydi.

Дискнинг ностандарт форматидан нусха кўчиришдан ҳимоя қилишда фойдаланиш, бунда дискни нусха кўчиришнинг стандарт утилиталари ўқий олмайди.

Измерение

uz - o‘lchash

ўлчаш

en - measurement

Процесс определения значения.

Примечание – В контексте информационной безопасности для выполнения процесса определения значения требуется информация об эффективности системы управления информационной безопасностью и взаимодействующих с ней средств управления, используемых методе измерения, функции измерения, аналитической модели и критериях принятия решения.

Qiyamatni aniqlash jarayoni.

Izoh – Axborot xavfsizligi kontekstida qiymatni aniqlash jarayonini bajarish uchun, axborot xavfsizligini boshqarish tizimining va u bilan birga ishlaydigan boshqarish vositalarining samaradorligi, foydalaniladigan o‘lchash usuli, o‘lchash funksiyasi, tahliliy model va qaror qabul qilish mezonlari to‘g‘risidagi axborot kerak bo‘ladi.

Қийматни аниқлаш жараёни.

Изоҳ – Ахборот хавфсизлиги контекстида қийматни аниқлаш жараёнини бажариш учун, ахборот хавфсизлигини бошқариш тизимининг ва у билан бирга ишлайдиган бошқариш воситаларининг самарадорлиги, фойдаланиладиган ўлчаш усули, ўлчаш функцияси, таҳлилий модель ва қарор қабул қилиш мезонлари тўғрисидаги ахборот

И

керак бўлади.

Имитация

uz - imitatsiya

имитация

en - imitation

Составная часть технической дезинформации, осуществляемая путем искусственного воспроизведения ложных объектов и технических демаскирующих признаков.

Texnik yolgʻon xabar tarqatishning tarkibiy qismi, soxta obyektlar va texnik demaskirovka qiluvchi belgilarni sunʻiy qayta tiklash yoʻli bilan amalga oshiriladi.

Техник ёлгон хабар тарқатишнинг таркибий қисми, сохта объектлар ва техник демаскировка қилувчи белгиларни сунъий қайта тиклаш йўли билан амалга оширилади.

Имитация экрана

uz - ekran imitatsiyasi

экран имитацияси

en - screen mimic

Маскировка экрана, обычно связанная с высвечиванием ничего не подозревающему пользователю ложного экрана опроса для перехвата его имени и пароля.

Hech narsadan gumon qilmagan foydalanuvchiga, uning nomi va parolini bilib olish uchun soxta soʻroq ekranini yoritish bilan bogʻliq ekran maskirovkasi.

Ҳеч нарсадан гумон қилмаган фойдаланувчига, унинг номи ва паролени билиб олиш учун сохта сўроқ экранини ёритиш билан боғлиқ экран маскировкаси.

Имитовставка

uz - imitoqoʻshimcha

имитокўшимча

en - imitoinserter

Отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Ochiq maʼlumotlar va kalitdan maʼlum qoidaga koʻra olingan hamda shifrlangan maʼlumotlarga imitomuhofazani taʼminlash uchun qoʻshilgan, qayd qilingan uzunlikdagi axborot boʻlagi.

Очиқ маълумотлар ва калитдан маълум қоидага кўра олинган ҳамда шифрланган маълумотларга

И

имитомуҳофазани таъминлаш учун қўшилган, қайд қилинган узунликдаги ахборот бўлаги.

Имитозащита

uz - imitomuhofaza

имитомуҳофаза

en - imitation (simulation)

of protection

1 Аппаратные, аппаратно-программные или программные средства защиты системы шифрованной связи от навязывания ложных данных.

2 Защита системы шифрованной связи от навязывания ложных данных.

1 Shifrlangan aloqa tizimini yolgʻon maʼlumotlar majburan kiritilishidan (qabul qilinishidan) saqlashning apparat, apparat-dasturiy yoki dasturiy muhofaza vositalari.

2 Shifrlangan aloqani yolgʻon maʼlumotlarning ortiqcha oʻrnatilishidan muhofaza qilish tizimi.

1 Шифрланган алоқа тизимини ёлғон маълумотлар мажбуран киритилишидан (қабул қилинишидан) сақлашнинг аппарат, аппарат-дастурий ёки дастурий муҳофаза воситалари.

2 Шифрланган алоқани ёлғон маълумотларнинг ортиқча ўрнашишидан муҳофаза қилиш тизими.

Имитостойкость

uz - imitobardoshlilik

имитобардошлилик

en - mimic resistance

Способность противостоять активным атакам со стороны злоумышленника, целью которых является навязывание ложного или подмена передаваемого сообщения или хранимых данных.

Maqsadi yolgʻon xabarni majburan kiritish (qabul qilish) yoki uzatiladigan axborotni yoki saqlanadigan maʼlumotlarni almashtirib qoʻyish boʻlgan, jinoyatkorning aktiv hujumlariga qarshi tura olish qobiliyati.

Мақсади ёлғон хабарни мажбуран киритиш (қабул қилиш) ёки узатиладиган ахборотни ёки сақланадиган маълумотларни алмаштириб қўйиш бўлган, жинояткорнинг актив ҳужумларига қарши тура олиш қобилияти.

Имя уникальное

uz - noyob nom

ноёб ном

en - distinguished name

Текстовый идентификатор объекта в каталоге, построенном по спецификации X.500. Включает имена контейнерных объектов каталога, в которых находится данный объект, и имя самого объекта.

И

Obyektning, X.500 spetsifikatsiyasi bo'yicha tuzilgan katalogdagi matnli identifikatori. Katalogning, shu obyekt bo'lgan konteynerli obyektlari nomini va obyektning o'z nomini ichiga oladi.

Объектнинг, X.500 спецификацияси бўйича тuzилган каталогдаги матнли идентификатори. Каталогнинг, шу объект бўлган контейнерли объекtlari номини ва объектнинг ўз номини ичига олади.

Индикатор

uz - indikator
индикатор
en - indicator

Мера, позволяющая оценить соответствующие атрибуты, полученные из аналитической модели, разработанной для определенных информационных потребностей.

Muayyan axborot ehtiyojlari uchun ishlab chiqilgan tahliliy modeldan olingan tegishli atributlarni baholash imkonini beradigan o'lchov.

Муайян ахборот эhtiёжлари учун ишлаб чиқилган тахлилий моделдан олинган тегишли атрибутларни баҳолаш имконини берадиган ўлчов.

Инженерия программная

uz - dasturiy injeneriya
дастурий инженерия
en - software engineering

Приложение систематического, упорядоченного, измеримого подхода к разработке и сопровождению программного обеспечения.

Dasturiy ta'minotni ta'minlashga va ishlab chiqishga bo'lgan tizimli, tartiblashtirilgan, o'lchanadigan yondashuv ilovasi.

Дастурий таъминотни таъминлашга ва ишлаб чиқишга бўлган тизимли, тартиблаштирилган, ўлчанадиган ёндашув иловаси.

Инженерия социальная

uz - ijtimoiy injeneriya
ижтимоий инженерия
en - social engineering

Метод несанкционированного доступа к информации или системам хранения информации без использования технических средств, основанный на знании человеческой природы, особенностях принятия решения людьми и социальной психологии.

Inson tabiatini bilishga, odamlar tomonidan qaror

И

qabul qilish xususiyatlariga va ijtimoiy psixologiyaga asoslangan, texnik vositalardan foydalanmasdan axborotdan yoki axborotni saqlash tizimlaridan ruxsatsiz foydalana olish usuli.

Инсон табиатини билишга, одамлар томонидан қарор қабул қилиш хусусиятларига ва ижтимоий психологияга асосланган, техник воситалардан фойдаланмасдан ахборотдан ёки ахборотни сақлаш тизимларидан рухсатсиз фойдалана олиш усули.

Инсталлятор

uz - installator

инсталлятор

en - installer

Компьютерная программа, которая устанавливает файлы, например, приложения, драйверы, или другое программное обеспечение, на компьютер. Некоторые инсталляторы специально сделаны для установки содержащихся в них файлов; другие же являются универсальными и работают, считывая содержимое комплекта программного обеспечения, которое необходимо установить.

Fayllarni, masalan, kompyuterga ilova, drayverlar yoki boshqa dasturiy ta'minotni o'rnatuvchi kompyuter dasturi. Ayrim installatorlar ulardagi mavjud fayllarni o'rnatish uchun maxsus ishlangan; boshqalari universal hisoblanadi va o'rnatish zarur bo'lgan dasturiy ta'minot komplektini hisobga olib ishlaydi.

Файлларни, масалан, компьютерга илова, драйверлар ёки бошқа дастурий таъминотни ўрнатувчи компьютер дастури. Айрим инсталляторлар улардаги мавжуд файлларни ўрнатиш учун махсус ишланган; бошқалари универсал ҳисобланadi ва ўрнатиш зарур бўлган дастурий таъминот комплектини ҳисобга олиб ишлайди.

Инсталляция

uz - installatsiya

инсталляция

en - installation

Процесс установки ОО в эксплуатационную среду и приведение его в рабочее состояние, выполняемый человеком-пользователем.

Примечание – Этот процесс обычно выполняется только один раз после получения и приемки ОО.

Foydalanuvchi-odam tomonidan bajariladigan, BOni

И

qo'llaniladigan muhitga o'rnatish hamda uni ishchi holatga keltirish jarayoni.

Izoh – Bu jarayon odatda, faqat bir marta BOni qabul qilgandan va olingandan keyin bajariladi.

Фойдаланувчи-одам томонидан бажариладиган, BOni қўлланиладиган муҳитга ўрнатиш ҳамда уни ишчи ҳолатга келтириш жараёни.

Изоҳ – Бу жараён одатда, фақат бир марта BOni қабул қилгандан ва олингандан кейин бажарилади.

Интерпретация

uz - interpretatsiya (talqin)
интерпретация (талқин)

en - interpretation

Анализ команд или операторов программы и не-медленное их выполнение.

Komandalar yoki dastur operatorlarining tahlili, ularning darhol bajarilishi.

Командалар ёки дастур операторларининг таҳлили, уларнинг дарҳол бажарилиши.

Интерпретация

программная

uz - dasturiy interpretatsiya
дастурий интерпретация

en - software interpretation

Способ защиты управляющей программы от не-санкционированной модификации путем загрузки ее в измененной форме с помощью кодового оптимизатора.

Kodli optimizator yordamida o'zgartirilgan shaklda yuklash yo'li bilan, boshqaruvchi dasturni ruxsat etilmagan o'zgartirishdan muhofaza qilish usuli.

Кодли оптимизатор ёрдамида ўзгартирилган шаклда юклаш йўли билан, бошқарувчи дастурни рұхсат этилмаган ўзгартиришдан муҳофаза қилиш усули.

Интерфейс

uz - interfeys
интерфейс

en - interface

Средства взаимодействия с компонентом или модулем.

Komponent yoki modul bilan birga ishlash vositasi.

Компонент ёки модуль билан бирга ишлаш воситаси.

Интерфейс (в системах обработки данных)

uz - interfeys (ma'lumotlarni qayta ishlash tizimlarida)

Определенный набор услуг, представляемых процессором.

Protsessor taqdim etadigan xizmatlarning ma'lum bir

И

интерфейс (маълумотлар-ни қайта ишлаш тизимларида)

en - interface (in data processing systems)

Интерфейс функции безопасности объекта оценки

uz - baholash obyektini xavfsizlik funksiyasining interfeysi

баҳолаш объекти хавфсизлик функциясининг интерфейси

en - target security functions of evaluation interface

Интерфейс функциональный

uz - funksional interfeysi

функционал интерфейс

en - functional interface

to'plami.

Процессор тақдим этадиган хизматларнинг маълум бир тўплами.

Средства, с помощью которых внешние логические объекты (или субъекты в ОО, но вне ФБО) передают/получают данные от/из ФБО, а также пользуются сервисами ФБО.

Tashqi mantiqiy obyektlar (yoki OXFda bo'lmagan BO subyektlar) OXFdan/ga ma'lumotlar uzatadigan/oladigan, shuningdek, OXF xizmatlaridan foydalanadigan vositalar.

Ташқи мантикий объектлар (ёки ОХФда бўлмаган БО субъектлар) ОХФдан/га маълумотлар узатадиган/олададиган, шунингдек, ОХФ хизматларидан фойдаланадиган воситалар.

Внешний интерфейс, предоставляющий пользователю доступ к функциональным возможностям ОО, которые непосредственно не задействованы в выполнении функциональных требований безопасности.

Примечание – В составном ОО – это интерфейсы, предоставляемые базовым компонентом, которые необходимы зависимому компоненту для поддержания функционирования составного ОО.

Foydalanuvchiga BOning, funksional xavfsizlik talblarini bajarishda bevosita qatnashmaydigan funksional imkoniyatlaridan foydalanishiga imkon beradigan tashqi interfeysi.

Izoh – Tarkibiy BOda – bu, bazaviy komponent taqdim etadigan, bog'liq komponentga tarkibiy BO ishlashini ta'minlash uchun zarur bo'lgan interfeyslardir.

Фойдаланувчига БОнинг, функционал хавфсизлик талабларини бажаришда бевосита қатнашмайдиган функционал имкониятларидан фойдаланишига имкон берадиган ташқи интерфейс.

Изоҳ – Таркибий БОда – бу, базавий компонент тақдим этадиган, боғлиқ компонентга таркибий БО ишлашини таъминлаш учун зарур бўлган интерфейслардир.

И

Информация

uz - axborot

ахборот

en - information

1 Сведения о фактах, событиях, процессах и явлениях в некоторой предметной области, включенные в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях и используемые (необходимые) для оптимизации принимаемых решений в процессе управления объектами данной предметной области.

2 Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

1 Axborotni qayta ishlash tizimiga kiritilgan yoki turli tashuvchilarda turli shakllarda taqdim etishda uning natijasi bo'lib hisoblanadigan va ushbu predmet sohasining boshqaruv obyektini jarayonida qabul qilinadigan qarorlarni optimallashtirish uchun (zarur bo'lgan) ishlatiladigan faktlar, voqealar, jarayonlar va hodisalar to'g'risidagi ma'lumotlar.

2 Taqdim etish shaklidan qat'i nazar, shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar.

1 Axborotni qayta ishlash tizimiga kiritilgan barcha turli tashuvchilarda turli shakllarda taqdim etishda uning natijasi bo'lib hisoblanadigan va ushbu predmet sohasining boshqaruv obyektini jarayonida qabul qilinadigan qarorlarni optimallashtirish uchun (zarur bo'lgan) ishlatiladigan faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar.

2 Taqdim etish shaklidan qat'i nazar, shaxslar, predmetlar, faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar.

Информация (для процесса обработки данных)

uz - axborot (ma'lumotlarni

qayta ishlash jarayoni uchun)

ахборот (маълумотларни

қайта ишлаш жараёни учун)

en - information (in data

processing)

Любые знания о предметах, фактах, понятиях и т.д. проблемной области, которыми обмениваются пользователи системы обработки данных.

Ma'lumotlarni qayta ishlash tizimi foydalanuvchilari almashinadigan, muammoli soha predmetlari, faktlari, tushunchalari va b.q. haqidagi har qanday bilimlar.

И

Маълумотларни қайта ишлаш тизими фойдаланувчилари алмашинадиган, муаммоли соҳа предметлари, фактлари, тушунчалари ва б.қ. ҳақидаги ҳар қандай билимлар.

Информация

аутентификации

uz - autentifikatsiya axboroti

аутентификация ахбороти

en - authentication information

1 Информация, используемая для установления достоверности идентификационной информации, предъявленной логическим объектом.

2 Информация, используемая для установления подлинности личности, за которую выдает себя пользователь.

1 Mantiqiy obyekt tomonidan taqdim etilgan identifikatsion axborotning ishonchliligini aniqlash uchun foydalaniladigan axborot.

2 Foydalanuvchi shaxsining haqiqiylikini aniqlash uchun foydalaniladigan axborot.

1 Мантикий объект томонидан тақдим этилган идентификацион ахборотнинг ишончлилигини аниқлаш учун фойдаланиладиган ахборот.

2 Фойдаланувчи шахсининг ҳақиқийлигини аниқлаш учун фойдаланиладиган ахборот.

Информация безопасности

uz - xavfsizlik axboroti

хавфсизлик ахбороти

en - security information

Информация, необходимая для реализации услуг обеспечения безопасности.

Xavfsizlikni ta'minlash xizmatlarini amalga oshirish uchun zarur bo'lgan axborot.

Xavfsizlikni ta'minlash xizmatlarini amalga oshirish uchun zarur bo'lgan axborot.

Информация

документированная

uz - hujjatlashtirilgan

axborot

хужжатлаштирилган

ахборот

en - documented information

1 Информация, зафиксированная на материальном носителе и обладающая реквизитами, позволяющими ее идентифицировать.

2 Информация, необходимая для управления и функционирования организации, а также материальный носитель, на котором она содержится.

Примечание – Документированная информация может быть представлена в любой форме и на любом носителе, она может быть получена из любого источника.

1 Moddiy tashuvchida qayd etilgan va uni identifi-

И

katsiya qilish imkonini beradigan rekvizitlarga ega axborot.

2 Tashkilotni boshqarish va uning ishlashi uchun zarur axborot, shuningdek, axborot saqlanadigan moddiy tashuvchi.

Izoh – Hujjatlashtirilgan axborot har qanday shaklda va har qanday tashuvchida taqdim etilishi, shuningdek, har qanday manbadan olinishi mumkin.

1 Моддий ташувчида қайд этилган ва уни идентификация қилиш имконини берадиган реkvизитларга эга ахборот.

2 Ташкилотни бошқариш ва унинг ишлаши учун зарур ахборот, шунингдек, ахборот сақланадиган моддий ташувчи.

Изоҳ – Ҳужжатлаштирилган ахборот ҳар қандай шаклда ва ҳар қандай ташувчида тақдим этилиши, шунингдек, ҳар қандай манбадан олинishi мумкин.

Информация защищаемая

uz - muhofaza qilinadigan axborot

муҳофаза қилинадиган ахборот

en - secured information

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями нормативных документов или требованиями, устанавливаемыми собственником информации.

Mulkchilik predmeti hisoblanadigan va normativ hujjatlar talablari yoki axborot egasi tomonidan belgilanadigan talablarga muvofiq muhofaza qilinishi kerak bo'lgan axborot.

Мулкчилик предмети ҳисобланадиган ва норматив ҳужжатлар талаблари ёки ахборот эгаси томонидан белгиланадиган талабларга мувофиқ муҳофаза қилиниши керак бўлган ахборот.

Информация

конфиденциальная

uz - konfidensial axborot

конфиденциал ахборот

en - confidential information

1 Документированная информация, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Республики Узбекистан.

2 Информация, имеющая ограничения на право доступа к ней со стороны пользователей и, как следствие, требующая защиты от несанкционированного к ней доступа.

И

3 Служебная, профессиональная, промышленная, коммерческая или иная информация, правовой режим которой устанавливается ее собственником на основе законодательства и которая требует защиты.

1 Davlat siri hisoblanadigan ma'lumotlar bo'lmagan hujjatlashtirilgan axborot, undan foydalanish O'zbekiston Respublikasi qonunlariga muvofiq chegaralanadi.

2 Foydalanuvchilar tomonidan erkin foydalanish huquqi cheklangan va ruxsat etilmagan tarzda foydalana olishdan muhofaza qilinishi talab etiladigan axborot.

3 Xizmatga oid, professional, sanoat, tijoratga oid yoki huquqiy rejimi egasi tomonidan qonunchilikka asosan belgilanadigan va muhofaza qilinishi talab etiladigan axborot.

1 Давлат сирин ҳисобланадиган маълумотлар бўлмаган ҳужжатлаштирилган ахборот, ундан фойдаланиш Ўзбекистон Республикаси қонунларига мувофиқ чегараланadi.

2 Фойдаланувчилар томонидан эркин фойдаланиш ҳуқуқи чекланган ва рұхсат этилмаган тарзда фойдалана олишдан муҳофаза қилиниши талаб этиладиган ахборот.

3 Хизматга оид, профессионал, саноат, тижоратга оид ёки ҳуқуқий режими эгаси томонидан қонunchиликка асосан белгиланадиган ва муҳофаза қилиниши талаб этиладиган ахборот.

Информация некритичная (несекретная)

uz - kritik (maxfiy) bo'lmagan axborot

критик (махфий)

бўлмаган ахборот

en - unclassified information

1 Информация, не нуждающаяся в защите от раскрытия.

2 Информация, которая не представляет собой государственную, служебную, коммерческую или личную тайны и может быть опубликована в открытой печати.

1 Ochilishdan muhofaza qilishga ehtiyoj bo'lmagan axborot.

2 Davlat, xizmat, tijorat sirlarini yoki shaxsiy sirni ichiga olmaydigan, ochiq matbuotda e'lon qilinishi

И

mumkin bo'lgan axborot.

1 Очилишдан муҳофаза қилишга эҳтиёж бўлмаган ахборот.

2 Давлат, хизмат, тижорат сирларини ёки шахсий сирни ичига олмайдиган, очик матбуотда эълон қилиниши мумкин бўлган ахборот.

Информация ограниченного доступа

uz - foydalana olinishi

cheklangan axborot

фойдалана олинishi

чекланган ахборот

en - limited access information

Документированная информация, содержащая сведения, составляющие государственные секреты и конфиденциальную информацию, доступ к которой ограничивается в соответствии с законодательством.

Davlat sirlari va konfidensial axborotdan iborat ma'lumotlarga ega bo'lgan hujjatlashtirilgan axborot, ulardan foydalana olish qonun hujjatlariga muvofiq chegaralanadi.

Давлат сирлари ва конфиденциал ахборотдан иборат маълумотларга эга бўлган ҳужжатлаштирилган ахборот, улардан фойдалана олиш қонун ҳужжатларига мувофиқ чегараланади.

Информация остаточная

uz - qoldiq axborot

қолдиқ ахборот

en - residual information

Информация на запоминающем устройстве, оставшаяся от формально удалённых операционной системой данных или из-за физических свойств запоминающих устройств.

Formal jihatdan operatsion tizim tomonidan o'chirilgan ma'lumotlardan yoki xotirlovchi qurilmalarning fizik xususiyatlari sababli ularda qolgan axborot.

Формал жиҳатдан операцион тизим томонидан ўчирилган маълумотлардан ёки хотирловчи қурилмаларнинг физик хусусиятлари сабабли уларда қолган ахборот.

Информация персональная

uz - shaxsiy axborot

шахсий ахборот

en - private information

Сведения, которые не подлежат огласке. Их распространение по каналам телекоммуникаций требует соблюдения специальных мер безопасности.

Oshkor qilinishi mumkin bo'lmagan axborot. Ularni

И

telekommunikatsiya kanallari orqali tarqatish maxsus xavfsizlik choralariga rioya qilinishini talab etadi.

Ошкор қилиниши мумкин бўлмаган ахборот. Уларни телекоммуникация каналлари орқали тарқатиш махсус хавфсизлик чораларига риоя қилинишини талаб этади.

Информация чувствительная (критичная)

uz - ta'sirchan (kritik)

axborot

таъсирчан (критик)

ахборот

en - sensitive information

Информация, которая определена уполномоченным органом как нуждающаяся в защите, потому что ее раскрытие, модификация, уничтожение или сокрытие нанесет ощутимый ущерб кому-то или чему-то.

Ochilishi, o'zgartirilishi, yo'q qilinishi yoki yashirilishi kimgadir yohud nimagadir sezilarli ziyon yetkazishi mumkin bo'lganligi uchun, vakolatlangan organ tomonidan muhofaza qilinishi zarur deb belgilangan axborot.

Очилиши, ўзгартирилиши, йўқ қилиниши ёки яширилиши кимгадир ёҳуд нимагадир сезиларли зиён етказиши мумкин бўлганлиги учун, ваколатланган орган томонидан муҳофаза қилиниши зарур деб белгиланган ахборот.

Инфраструктура открытых ключей

uz - ochiq kalitlar

infrastrukturasi

очиқ калитлар

инфраструктураси

en - public key infrastructure

Технология передачи шифрованных данных по открытым каналам телекоммуникаций с использованием двух логически связанных ключей: открытого, который известен всем, и закрытого, который знает только определенный пользователь.

Mantiqiy bog'langan ikkita: hammaga ma'lum bo'lgan ochiq va faqat ma'lum foydalanuvchi biladigan yopiq kalitlardan foydalanib, ochiq telekommunikatsiyalar kanallari orqali shifrlangan ma'lumotlarni uzatish texnologiyasi.

Мантиқий боғланган иккита: ҳаммага маълум бўлган очиқ ва фақат маълум фойдаланувчи биладиган ёпиқ калитлардан фойдаланиб, очиқ телекоммуникациялар каналлари орқали шифрланган маълумотларни узатиш технологияси.

И

Инфраструктура управления привилегиями

uz - imtiyozlarni boshqarish
strukturası

имтиёзларни бошқариш
структураси

en - privilege management
infrastructure

Инфраструктура, способная поддерживать управление привилегиями при поддержке комплексной услуги авторизации и при взаимодействии с инфраструктурой открытых ключей.

Kompleks mualliflashtirish xizmati ko‘magida hamda ochiq kalitlar infrastrukturası bilan o‘zaro hamkorlikda imtiyozlarni boshqarish ta‘minlanadigan infrastruktura.

Комплекс муаллифлаштириш хизмати кўмагида ҳамда очик калитлар инфраструктураси билан ўзаро ҳамкорликда имтиёзларни бошқариш таъминланадиган инфраструктура.

Инцидент

uz - insident

инцидент

en - incident

Любое событие, которое приводит или может привести к незапланированному прерыванию услуги или к снижению ее качества.

Примечание – Примером инцидента является сбой в одном из элементов инфраструктуры.

Xizmatlarning rejalashtirilmagan tarzda uzilishiga yoki uning sifati pasayishiga olib keladigan yoki olib kelishi mumkin bo‘lgan har qanday hodisa.

Izoh – Masalan, infrastruktura elementlaridan biridagi uzilish insidentga misol bo‘ladi.

Хизматларнинг режалаштирилмаган тарзда узилишига ёки унинг сифати пасайишига олиб келадиган ёки олиб келиши мумкин бўлган ҳар қандай ҳодиса.

Изоҳ – Масалан, инфраструктура элементларидан биридаги узилиш инцидентга мисол бўлади.

Инцидент информационной безопасности

uz - axborot xavfsizligi
insidenti

ахборот хавфсизлиги
инциденти

en - information security
incident

Еди́нчиное событие́ или ряд нежелательных или непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации бизнес-операций и угрозы информационной безопасности.

Yagona hodisa yoki axborot xavfsizligining, biznes-operatsiyalarning obro‘sizlanish va axborot xavfsizligiga tahdid ehtimoli katta bo‘lgan qator nomaqbul yoki ko‘zda tutilmagan hodisalari.

Ягона ҳодиса ёки ахборот хавфсизлигининг, биз-

И

нес-операцияларнинг обрўсизланиш ва ахборот хавфсизлигига таҳдид эҳтимоли катта бўлган қатор номақбул ёки кўзда тутилмаган ҳодисалари.

Случайное или умышленное нарушение целостности данных.

Искажение данных

uz - ma'lumotlarning buzilishi

маълумотларнинг бузилиши

en - data corruption

Ma'lumotlar yaxlitligining tasodifan yoki qasddan buzilishi.

Маълумотлар яхлитлигининг тасодифан ёки қасддан бузилиши.

Искажение информации

uz - axborotning buzilishi

ахборотнинг бузилиши

en - information distortion

Случайная или преднамеренная несанкционированная модификация информации при ее обработке (передаче) техническими средствами в результате внешних воздействий (помех), сбоя в работе аппаратуры или ошибочных действий обслуживающего персонала.

Tashqi ta'sirlar (xalaqitlar), apparatura ishidagi to'xtashlar yoki xizmat ko'rsatuvchi personalning noto'g'ri harakatlari natijasida axborotni texnik vositalar yordamida qayta ishlash (uzatish)da axborotning tasodifiy yoki qasddan ruxsat etilmagan tarzda o'zgartirilishi.

Ташқи таъсирлар (халақитлар), аппаратура ишидаги тўхташлар ёки хизмат кўрсатувчи персоналнинг нотўғри ҳаракатлари натижасида ахборотни техник воситалар ёрдамида қайта ишлаш (узатиш)да ахборотнинг тасодифий ёки қасддан рўхсат этилмаган тарзда ўзгартирилиши.

Использование вычислительной системы

злоумышленное

uz - hisoblash tizimidan qasddan foydalanish

ҳисоблаш тизимидан қасддан фойдаланиш

en - computer fraud

Любая деятельность, направленная на манипулирование информацией внутри вычислительной системы с целью личной выгоды, обычно финансовой.

Shaxsiy, odatda moliyaviy foyda olish maqsadida hisoblash tizimi ichida axborot bilan manipulyatsiya qilishga qaratilgan har qanday faoliyat.

Шахсий, одатда молиявий фойда олиш мақсадида ҳисоблаш тизими ичида ахборот билан манипу-

И

Использование ловушек

uz - tuzoqlardan foydalanish

тузоқлардан фойдаланиш

en - entrapment

ляция қилишга қаратилган ҳар қандай фаолият.

Умышленная установка очевидных брешей в системе обработки данных, предназначенных для обнаружения попыток проникновения или введения в заблуждение нарушителя, когда он воспользуется этими брешами.

Ma'lumotlarni qayta ishlash tizimiga, oshkora kamchiliklarni (zaifliklarni) atayin kiritish. Buzg'unchi bu kamchiliklardan (zaifliklardan) foydalanganda, uni chalg'itish uchun yoki kirishga urinishlarni aniqlash uchun mo'ljallangan.

Маълумотларни қайта ишлаш тизимига, ошкора камчиликларни (заифликларни) атайин киритиш. Бузғунчи бу камчиликлардан (заифликлардан) фойдаланганда, уни чалғитиш учун ёки киришга уринишларни аниқлаш учун мўлжалланган.

Использование

объекта повторное

uz - obyektдан takror

foydalanish

объектдан такрор

фойдаланиш

en - object reuse

Переназначение и повторное использование пространства памяти (например, страницы фрейма, сектора диска, магнитной ленты), которое ранее содержало в себе один или несколько объектов. Для поддержания безопасности это пространство при выделении его под новый объект не должно содержать информации о старом объекте.

Avval bitta yoki bir nechta obyektни o'z ichiga olgan хотира майдонини (масалан, фрейм саҳифалари, диск сектори, магнит лентаси) қайта тайинлаш ва ундан такрор фойдаланиш. Хавфсизликни таъминлаш учун бу майдон, уни янги объектга ажратишда, эски объект то'ғ'рисидаги ахборотга эга бўлмаслиги керак.

Аввал битта ёки бир нечта объектни ўз ичига олган хотира майдонини (масалан, фрейм саҳифалари, диск сектори, магнит лентаси) қайта тайинлаш ва ундан такрор фойдаланиш. Хавфсизликни таъминлаш учун бу майдон, уни янги объектга ажратишда, эски объект тўғ'рисидаги ахборотга эга бўлмаслиги керак.

Исправление

uz - tuzatish

тузатиш

Внесение изменений в программу или набор данных путем обновления, добавления или удаления отдельных частей (фрагментов).

И

en - correction

Dasturga o'zgartirishlar kiritish yoki ayrim qismlar (fragmentlar)ni yangilash, qo'shish yoki olib tashlash yo'li bilan ma'lumotlar to'plash.

Дастурга ўзгартиришлар киритиш ёки айрим қисмлар (фрагментлар)ни янгилаш, қўшиш ёки олиб ташлаш йўли билан маълумотлар тўплаш.

Испытание

uz - sinov

СИНОВ

en - test, testing

Проверка системы или ее компонента путем реального выполнения каких-либо задач.

Qandaydir vazifani aniq bajarish yo'li bilan tizimni yoki uning komponentini tekshirish.

Қандайдир вазифани аниқ бажариш йўли билан тизимни ёки унинг компонентини текшириш.

Испытание на проникновение

uz - suqulib kirishga sinash

суқулиб киришга синаш

en - penetration test

Испытание системы с целью проверки средств ее защиты (в частности от несанкционированного доступа).

Muhofaza qilish vositalarini tekshirish maqsadida tizimni sinab ko'rish (xususan, ruxsat etilmagan tarzda foydalana olishdan).

Муҳофаза қилиш воситаларини текшириш мақсадида тизимни синаб кўриш (хусусан, рухсат этилмаган тарзда фойдалана олишдан).

Исследования специальные

uz - maxsus tadqiqotlar

махсус тадқиқотлар

en - special study

1 Исследования, которые проводятся на объекте эксплуатации технических средств обработки информации с целью определения соответствия системы защиты информации требованиям стандартов и других нормативных документов, а также для выработки соответствующих рекомендаций по доведению системы защиты до требуемого уровня.

2 Деятельность по выявлению с использованием контрольноизмерительной аппаратуры возможных технических каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем и оценка соответствия защиты информации требованиям нормативных документов по защите информации.

1 Axborotni qayta ishlash texnik vositalarini ekspluatatsiya qilish obyektida axborotni muhofaza qi-

И

lish tizimining standartlar va normativ hujjatlar talablariga mos kelishini aniqlash, shuningdek, muhofaza qilish tizimini talab qilinadigan darajagacha yetkazish bo'yicha tegishli tavsiyalar ishlab chiqish maqsadida olib boriladigan tadqiqotlar.

2 Nazorat-o'lchash apparaturasidan foydalanib, muhofaza qilinadigan axborot asosiy va yordamchi texnik vositalar hamda tizimlardan chiqib ketishi mumkin bo'lgan texnik kanallarni aniqlash va axborotni muhofaza qilishning shu mazmundagi normativ hujjatlar talablariga mos kelishini baholash bo'yicha faoliyat.

1 Ахборотни қайта ишлаш техник воситаларини эксплуатация қилиш объектида ахборотни муҳофаза қилиш тизимининг стандартлар ва норматив хужжатлар талабларига мос келишини аниқлаш, шунингдек, муҳофаза қилиш тизимини талаб қилинадиган даражагача етказиш бўйича тегишли тавсиялар ишлаб чиқиш мақсадида олиб бориладиган тадқиқотлар.

2 Назорат-ўлчаш аппаратурасидан фойдаланиб, муҳофаза қилинадиган ахборот асосий ва ёрдамчи техник воситалар ҳамда тизимлардан чиқиб кетиши мумкин бўлган техник каналларни аниқлаш ва ахборотни муҳофаза қилишнинг шу мазмундаги норматив хужжатлар талабларига мос келишини баҳолаш бўйича фаолият.

Источник

uz - manba

манба

en - source

Материальный объект или субъект, способный накапливать, хранить, преобразовывать и выдавать информацию в виде сообщений или сигналов различной физической природы.

Turli fizik tabiatdagi xabarlar yoki signallar ko'rinishidagi axborotni to'plash, saqlash, o'zgartirish va berishi mumkin bo'lgan moddiy obyekt yoki subyekt.

Турли физик табиатдаги хабарлар ёки сигналлар кўринишидаги ахборотни тўплаш, сақлаш, ўзгартириш ва бериши мумкин бўлган моддий объект ёки субъект.

Источник информации

комбинаторный

uz - kombinator

Источник, на выходе которого может появиться одна из последовательностей, принадлежащая заданному конечному множеству, например, мно-

И

axborot manbai
комбинатор
ахборот манбаи
en - combinatorial source

жество векторов фиксированного веса Хемминга.

Chiqishida berilgan cheklovchi ko'plikka taalluqli ketma-ketliklardan biri paydo bo'lishi mumkin bo'lgan manba, masalan, Хемминг qayd vazni vektorlarining to'plami.

Чиқишида берилган чекловчи кўпликка тааллуқли кетма-кетликлардан бири пайдо бўлиши мумкин бўлган манба, масалан, Хемминг қайд вазни векторларининг тўплами.

Источники
коррелированные
uz - o'zaro bog'langan manbalar
ўзаро боғланган манбалар
en - correlated sources

Источники, порождающие статистически зависимые последовательности символов.

Simvollarning statistik bog'liq ketma-ketligini yuzaga keltiruvchi manbalar.

Символларнинг статистик боғлиқ кетма-кетлигини юзага келтирувчи манбалар.

Источники угроз
uz - tahdidlar manbalari
тахдидлар манбалари
en - threat source

Потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Potensial antropogen, texnogen yoki tabiiy (stixiyali) xavfsizlikka bo'lgan tahdidlarni tarqatuvchilar.

Потенциал антропоген, техноген ёки табиий (стихийали) хавфсизликка бўлган тахдидларни тарқатувчилар.

Исчерпывающий
uz - mukammal
мукаммал
en - exhaustive

Характеристика методики, используемой при выполнении анализа или деятельности согласно однозначно изложенному плану.

Tahlilni bajarishda foydalaniladigan yoki bayon qilingan rejaga muvofiq faoliyatning metodika tavsifi.

Таҳлилни бажаришда фойдаланиладиган ёки баён қилинган режага мувофиқ фаолиятнинг методика тавсифи.

Итерация
uz - iteratsiya
итерация
en - iteration

Использование одного и того же компонента для выражения двух или более различных требований.

И

Aynan bir komponentdan ikki yoki undan ortiq turli talabni ifodalash uchun foydalanish.

Айнан бир компонентдан икки ёки undan ортик турли талабни ифодалаш учун фойдаланиш.

К

Канал

uz - kanal

канал

en - channel

1 Маршрут передачи информации.

2 Часть системы телекоммуникаций, связывающая между собой источник и приемник сообщений.

1 Axborotni uzatish marshruti.

2 Telekommunikatsiyalar tizimining, manba va xabarlar qabul qilgichni o‘zaro bog‘lovchi qismi.

1 Ахборотни узатиш маршрути.

2 Телекоммуникациялар тизимининг, манба ва хабарлар қабул қилгични ўзаро боғловчи қисми.

Канал временный скрытый

uz - vaqtga bog‘liq bo‘lgan

kanal

вақтга боғлиқ бўлган

канал

en - covert timing channel

Скрытый канал, в котором один процесс передает информацию другому посредством модуляции доступа к системным ресурсам (например, времени занятости центрального процессора) таким образом, что эта модуляция может распознаваться и детектироваться другим процессом.

Yashirin kanal, unda bir jarayon axborotni boshqasiga tizim resurslaridan (masalan, markaziy protsesorning bandlik vaqtidan) foydalanishni modulyatsiyalash vositasida, bu modulyatsiyalash boshqa jarayon tomonidan aniqlanishi va detektorlanishi mumkin bo‘ladigan tarzda uzatadi.

Яширин канал, унда бир жараён ахборотни бошқасига тизим ресурсларидан (масалан, марказий процессорнинг бандлик вақтидан) фойдаланишни модуляциялаш воситасида, бу модуляциялаш бошқа жараён томонидан аниқланиши ва детекторланиши мумкин бўладиган тарзда узатади.

Канал доверенный

uz - ishonchli kanal

Средство взаимодействия между ФБО и другим доверенным продуктом ИТ, обеспечивающее не-

К

ишончли канал
en - trusted channel

обходимую для этого степень уверенности.

OXF va ATning boshqa ishonchli mahsuloti orasidagi, zarur qat'iylik darajasini ta'minlovchi, birgalikda ishlash vositasi.

OXF va ATning boshqa ishonchli mahsuloti orasidagi, zarur qat'iylik darajasini ta'minlovchi, birgalikda ishlash vositasi.

Канал защищенный
uz - muhofazalangan kanal
муҳофазаланган канал
en - secure channel

Именованный канал между службами Netlogon и компьютерами домена. При образовании защищенного канала создается ключ сеанса, применяемый для проверки подлинности передаваемых по каналу сообщений и для шифрования части передаваемой информации.

Domen kompyuterlarining va *Netlogon* xizmatlari o'rtasidagi nomlangan kanal. Muhofazalangan kanalni hosil qilishda kanal bo'yicha uzatiladigan xabarlarining haqiqiylikini tekshirish va uzatilayotgan axborotning bir qismini shifrlash uchun qo'llaniladigan seans kaliti yaratiladi.

Домен компьютерларининг ва *Netlogon* хизматлари ўртасидаги номланган канал. Муҳофазаланган канални ҳосил қилишда канал бўйича узатиладиган хабарларнинг ҳақиқийлигини текшириш ва узатилаётган ахборотнинг бир қисмини шифрлаш учун қўлланиладиган сеанс калити яратилади.

Канал связи внутренний
uz - ichki aloqa kanali
ички алоқа канали
en - internal communication channel

Канал связи между разделенными частями объекта оценки.

Baholash obyektining bo'lingan qismlari orasidagi aloqa kanali.

Баҳолаш объектининг бўлинган қисмлари орасидаги алоқа канали.

Канал с защитой целостности
uz - yaxlitlik muhofazalangan kanal
яхлитлик

Канал телекоммуникаций, к которому была применена услуга обеспечения безопасности.

Xavfsizlikni ta'minlash xizmati qo'llanilgan telekommunikatsiyalar kanali.

К

муҳофазаланган канал

en - integrity-protected channel

Хавфсизликни таъминлаш хизмати қўлланилган телекоммуникациялар канали.

Канал скрытый

uz - yashirin kanal

яширин канал

en - covert channel

1 Канал передачи, который может быть использован для передачи данных способом, нарушающим политику безопасности.

2 Недекларированный канал передачи, который позволяет пользователю скрытно нарушать многоуровневую политику разграничения доступа и требования ненаблюдаемости для ОО.

1 Ма'lumotlarni, xavfsizlik siyosatini buzadigan usulda uzatish uchun qo'llanilishi mumkin bo'lgan uzatish kanali.

2 Foydalanuvchiga yashirin tarzda ko'p darajali kira olishni cheklash siyosatini va BO uchun kuzatib bo'lmaslik talabini buzishga imkon beradigan deklaratsiya qilinmagan uzatish kanali.

1 Маълумотларни, хавфсизлик сиёсатини бузадиган усулда узатиш учун қўлланилиши мумкин бўлган узатиш канали.

2 Фойдаланувчига яширин тарзда кўп даражали кира олишни чеклаш сиёсатини ва БО учун кузатиб бўлмаслик талабини бузишга имкон берадиган декларация қилинмаган узатиш канали.

Канал с памятью скрытый

uz - хотирага эга

yashirin kanal

хотирага эга

яширин канал

en - covert storage channel

Скрытый канал, обеспечивающий прямую или косвенную запись в пространство памяти одним процессом и чтение этой информации другим процессом.

Примечание – Скрытый канал с памятью обычно связан с использованием ресурсов ограниченного объема, (например, секторов на диске), которые разделяются двумя субъектами с различными уровнями безопасности.

Xotira maydoniga bir jarayon tomonidan bevosita yoki bilvosita yozishni va bu axborotning boshqa jarayon tomonidan o'qilishini ta'minlovchi yashirin kanal.

Ilova – Yashirin kanal xavfsizlik darajasi turlicha bo'lgan ikkita subyekt bilan ajratiladigan cheklangan hajmdagi resurslardan (masalan, diskdagi sektorlardan) foydalanish bilan

К

bog'liq.

Хотира майдонига бир жараён томонидан бевосита ёки билвосита ёзишни ва бу ахборотнинг бошқа жараён томонидан ўқилишини таъминловчи яширин канал.

Илова – Яширин канал хавфсизлик даражаси турлича бўлган иккита субъект билан ажратилдиган чекланган хажмдаги ресурслардан (масалан, дискдаги секторлардан) фойдаланиш билан боғлиқ.

Канал утечки информации

uz - axborot chiqib

ketadigan kanal

ахборот чиқиб

кетадиган канал

en - covert channel

1 Канал коммуникаций, позволяющий процессу передавать информацию путем, нарушающим безопасность системы.

2 Неконтролируемый физический путь от источника информации, выходящий за пределы объекта защиты или круга лиц, обладающих защищаемыми сведениями, посредством которого возможно неправомерное получение и/или воздействие на защищаемую информацию.

1 Jarayonga, axborotni tizim xavfsizligi buziladigan yo'l bilan uzatish imkonini beruvchi kommunikatsiya kanali.

2 Muhofaza obyektini yoki muhofaza qilinadigan ma'lumotlarga ega bo'lgan shaxslar doirasidan tashqariga chiquvchi, axborot manбайдan boshlanadigan fizik yo'l. Uning vositasida muhofaza qilinadigan axborotni noqonuniy olish va/yoki unga ta'sir o'tkazish mumkin bo'ladi.

1 Жараёнга, ахборотни тизим хавфсизлиги бузиладиган йўл билан узатиш имконини берувчи коммуникация канали.

2 Муҳофаза объекти ёки муҳофаза қилинадиган маълумотларга эга бўлган шахслар доирасидан ташқарига чиқувчи, ахборот манбаидан бошланадиган физик йўл. Унинг воситасида муҳофаза қилинадиган ахборотни ноқонуний олиш ва/ёки унга таъсир ўтказиш мумкин бўлади.

Канал утечки информации

технический

uz - axborot chiqib

ketadigan texnik kanal

ахборот чиқиб

Физическая среда распространения сигналов, несущих конфиденциальную информацию, выходящая за пределы охраняемой территории.

Konfidensial axborotni tashuvchi signallarni tarqat-

К

кетидаган техник канал
en - technical convert channel

ishning, qo‘riqlanayotgan hududdan tashqariga chiquvchi fizik muhiti.

Кардер
uz - karder
кардер
en - carder

Конфиденциал ахборотни ташувчи сигналларни тарқатишнинг, қўриқланаётган худуддан ташқарига чиқувчи физик мухити.

Мошенник («виртуальный вор»), занимающийся аферами с пластиковыми картами.

Plastik kartalar bilan bog‘liq qalbaki ishlar bilan shug‘ullanuvchi firibgar («virtual o‘g‘ri»).

Пластик карталар билан боғлиқ қалбаки ишлар билан шуғулланувчи фирибгар («виртуал ўғри»).

Карта идентификационная (кодовая)

uz - identifikatsion (kodli) karta

идентификацион
(кодли) карта
en - ID card (code)

Перфорированная бумажная или магнитная карта с нанесенным на ней кодовым словом (паролем), предназначенная для идентификации доступа пользователя к информационному ресурсу.

Foydalanuvchining axborot resursidan foydalana olishini identifikatsiya qilish uchun mo‘ljallangan, kodli so‘z (parol) tushirilgan, perforatsiyalangan qog‘oz yoki magnit karta.

Фойдаланувчининг ахборот ресурсидан фойдалана олишини идентификация қилиш учун мўлжалланган, кодли сўз (пароль) туширилган, перфорацияланган қоғоз ёки магнит карта.

Карта интеллектуальная

uz - intellektual karta
интеллектуал карта
en - smart card

Миниатюрная пластиковая карточка с расширенными функциональными возможностями, реализованная на микропроцессорной основе и используемая при работе с терминалом для идентификации личности.

Keng funksional imkoniyatlarga ega bo‘lgan, mikroprotessor asosidagi, shaxsni identifikatsiya qilish uchun terminal bilan ishlashda foydalaniladigan ixcham plastik kartochka.

Кенг функционал имкониятларга эга бўлган, микропроцессор асосидаги, шахсни идентификация қилиш учун терминал билан ишлашда фойдала-

К

ниладиган ихчам пластик карточка.

Карта копирования

uz - nusxa ko‘chirish kartasi
нусха кўчириш картаси
en - copy card

Электронное устройство, которое будучи включенным в компьютер, позволяет копировать защищенное программное обеспечение из оперативной памяти на диск.

Kompyuterga kiritilgach, muhofazalangan dasturiy ta‘minotni operativ хотирадан дискка ко‘чирish имконини берадиган электрон қурилма.

Компьютерга киритилгач, муҳофазаланган дастурий таъминотни оператив хотирадан дискка кўчириш имконини берадиган электрон қурилма.

Карта с микропроцессором

uz - mikroprotessorli karta
микропроцессорли карта
en - chip card

Пластмассовая карточка типа кредитной, но имеющая встроенные запоминающее устройство и микропроцессор (или специализированную логическую схему).

Kredit kartochka turidagi, lekin ichida хотирловчи қурилма ва микропроцессори (yoki ixtisoslashtirilgan mantiqiy sxema) bo‘lgan plastmassa kartochka.

Кредит карточка туридаги, лекин ичида хотирловчи қурилма ва микропроцессори (ёки ихтисослаштирилган мантикий схема) бўлган пластмасса карточка.

Категория безопасности

uz - xavfsizlik kategoriyasi
хавфсизлик категорияси
en - security category

Неиерархическое группирование чувствительной информации, используемое для управления доступом к данным, более точного, чем при использовании только иерархического грифа секретности.

Faqat iyerarxik maxfiylik grifini qo‘llashdan ko‘ra, juda aniq bo‘lgan ma‘lumotlardan erkin foydalanishni boshqarishda qo‘llaniladigan nozik axborotni noiyerarxik guruhlash.

Фақат иерархик махфийлик грифини қўллашдан кўра, жуда аниқ бўлган маълумотлардан эркин фойдаланишни бошқаришда қўлланиладиган но-

К

зик ахборотни ноиерархик гурухлаш.

Категория безопасности информации

uz - axborot xavfsizligi kategoriyasi

ахборот хавфсизлиги категорияси

en - information security category

Уровень безопасности информации, определяемый установленными нормами в зависимости от важности (ценности) информации.

Оʻrnatilgan normalarga koʻra, axborotning muhimligiga (qimmatliligiga) bogʻliq holda belgilanadigan axborot xavfsizligi darajasi.

Ўрнатилган нормаларга кўра, ахборотнинг муҳимлигига (қимматлилигига) боғлиқ ҳолда белгиланадиган ахборот хавфсизлиги даражаси.

Категория допуска, допуск

uz - ruxsat berish kategoriyasi, ruxsat berish

рухсат бериш категорияси, рухсат бериш

en - security clearance, clearance

Разрешение, выданное лицу на право доступа к данным или информации заданного или более низкого уровня безопасности.

Shaxsga muayyan yoki juda past darajadagi xavfsizlik maʼlumotlari yoki axborotidan foydalanish huquqi berilgan ruxsat.

Шахсга муайян ёки жуда паст даражадаги хавфсизлик маълумотлари ёки ахборотидан фойдаланиш ҳуқуқи берилган рухсат.

Категория доступа

uz - erkin foydalanish kategoriyasi

эркин фойдаланиш категорияси

en - access category

Категория, присваиваемая логическим объектам, на основании которой они получают разрешение на использование ресурсов.

Mantiqiy obyektarga beriladigan kategoriya, uning asosida obyektlar resurslardan foydalanish uchun ruxsat oladilar.

Мантикий объектларга бериладиган категория, унинг асосида объектлар ресурслардан фойдаланиш учун рухсат оладилар.

Категория защиты информации

uz - axborotni muhofaza qilish

Качественный показатель, отражающий степень важности защиты информации в выбранной шкале ценностей.

К

kategoriyasi

ахборотни муҳофаза
қилиш категорияси

en - information protection
category

**Категория
конфиденциальности**

uz - konfidensiallik

kategoriyasi

конфиденциаллик
категорияси

en - sensitivity

**Категория управления
доступом**

uz - erkin foydalanishni
boshqarish kategoriyasi

эркин фойдаланишни
бошқариш категорияси

en - access control category

Качество

uz - sifat

сифат

en - quality

Tanlangan ahamiyatlilik shkalasida axborotni muhofaza qilish muhimlik darajasini aks ettiruvchi sifat ko'rsatkichi.

Танланган аҳамиятлилик шкаласида ахборотни муҳофаза қилиш муҳимлик даражасини акс эттирувчи сифат кўрсаткичи.

Характеристика ресурса, определяющая его ценность или значимость и способная включать в себя его уязвимость.

Resursning, uning muhimligini yoki ahamiyatligini belgilovchi va o'z ichiga resurs zaifligini olish xarakteristikasi.

Ресурснинг, унинг муҳимлигини ёки аҳамиятлилигини белгиловчи ва ўз ичига ресурс заифлигини олиш характеристикаси.

Языковые элементы, предназначенные для определения правил, предохраняющих от несанкционированных операций.

Ruxsat etilmagan operatsiyalardan saqlovchi qoidalarni aniqlash uchun mo'ljallangan til elementlari.

Рухсат этилмаган операциялардан сақловчи қоидаларни аниқлаш учун мўлжалланган тил элементлари.

Совокупность свойств изделия, обуславливающих его пригодность удовлетворять определенные потребности в соответствии с его назначениями.

Примечание – Качество определяется показателями качества такими, как надежность, точность, полнота, быстродействие и т.п.

O'zining mo'ljallanishiga muvofiq, mahsulotning ma'lum ehtiyojlarni qondirishga yaroqliligini asoslovchi xossalari jami.

Пояснение – Сифат ишончлilik, aniqlik, to'liqlik, tezkorlik va sh.k. sifat ko'rsatkichlari bilan belgilanadi.

К

Ўзининг мўлжалланишига мувофиқ, маҳсулотнинг маълум эҳтиёжларни қондиришга яроқлилигини асословчи хоссалари жами.

Илова – Сифат ишончилилик, аниқлик, тўлиқлик, тезкорлик ва ш.к. сифат кўрсаткичлари билан белгиланади.

Качество данных

uz - ma'lumotlarning sifati

маълумотларнинг сифати

en - data quality

Совокупность свойств данных, обеспечивающих их пригодность для решения определенных задач.

К показателям качества данных относятся: точность, полнота, адекватность, непротиворечивость, защищенность и др.

Ma'lumotlarning muayyan vazifalarni bajarish uchun yaroqliligini ta'minlovchi xossalari jami. Aniqlik, to'liqlik, adekvatlik, ziddiyatsizlik, muhofaza qilinganlik ma'lumotlarning sifat ko'rsatkichlari hisoblanadi.

Маълумотларнинг муайян вазифаларни бажариш учун яроқлилигини таъминловчи хоссалари жами. Аниқлик, тўлиқлик, адекватлик, зиддиятсизлик, муҳофаза қилинганлик маълумотларнинг сифат кўрсаткичлари ҳисобланади.

Качество документации

uz - hujjatlar sifati

хужжатлар сифати

en - documentation quality

Характеристика документации, определяемая полнотой и точностью описания программного обеспечения, наглядностью и удобочитаемостью материала, что позволяет быстро его осваивать и эффективно использовать.

Hujjatlarning, dasturiy ta'minotning to'liq va aniq tavsifi, materialning ravshan va o'qishga qulayligi bilan belgilanadigan (bu uni tez o'zlashtirish va undan unumli foydalanishga imkon beradi) xarakteristikasi.

Хужжатларнинг, дастурий таъминотнинг тўлиқ ва аниқ тавсифи, материалнинг равшан ва ўқишга қулайлиги билан белгиланадиган (бу уни тез ўзлаштириш ва ундан унумли фойдаланишга имкон беради) характеристикаси.

Квадрат Бофорта

uz - Bofort kvadrati

Многоалфавитная криптосистема, аналогичная криптосистеме Виженера. Строками квадрата яв-

К

Бофорт квадрати
en - Beaufirt square

ляются строки квадрата Виженера, записанные в обратном порядке. Криптосистема названа в честь адмирала Фрэнсиса Бофорта.

Vijener kriptotizimiga o‘xshash ko‘p alifboli kriptotizim. Teskari tartibda yozilgan Vijener kvadrati satrlari kvadrat satrlari hisoblanadi. Kriptotizim admiral Frensis Bofort sharafiga nomlangan.

Виженер крiптотизимига ўхшаш кўп алифболи крiптотизим. Тескари тартибда ёзилган Виженер квадрати сатрлари квадрат сатрлари ҳисобланади. Криптотизим адмирал Фрэнсис Бофорт шарафига номланган.

Квадрат Виженера
uz - Vijener kvadrati
Виженер квадрати
en - Vigenera square

Одна из наиболее известных многоалфавитных криптосистем. Квадрат Виженера представляет собой квадратную матрицу с n^2 элементами, где n – число символов используемого алфавита. Каждая строка квадрата заполняется циклическим сдвигом алфавита на один символ. Ключом шифрования является так называемое ключевое слово, которое меняется аналогично криптосистеме Цезаря от шага к шагу. Каждый столбец может быть рассмотрен как криптосистема Цезаря с ключами 0, 1, ..., 25. Так как ключевое слово обычно короче открытого текста, то оно используется периодически.

Ko‘p alifboli mashhur kriptotizimlardan biri. Vijener kvadrati n^2 elementlar bo‘lgan kvadrat matritsani ifodalaydi, bunda n – foydalaniladigan alifbo simvollarining soni. Kvadratning har bir satri alifboni bir simvolga siklik siljitish bilan to‘ldiriladi. Qadamdan qadamgacha Sezar kriptotizimiga o‘xshash o‘zgaradigan kalit so‘z shifrlash kaliti hisoblanadi. Har bir ustun 0, 1, ..., 25 kalitlari bo‘lgan Sezar kriptotizimi sifatida qaralishi mumkin. Kalit so‘z, odatda ochiq matndan qisqa bo‘lgani uchun, undan davriy ravishda foydalaniladi.

Кўп алифболи машхур крiптотизимлардан бири. Виженер квадрати n^2 элементлар бўлган квадрат

К

матрицани ифодалайди, бунда n – фойдаланиладиган алифбо символларининг сони. Квадратнинг ҳар бир сатри алифбони бир символга циклик силжитиш билан тўлдирилади. Қадамдан қадамгача Цезар криптолизимига ўхшаш ўзгарадиган калит сўз шифрлаш калити ҳисобланади. Ҳар бир устун 0, 1, ..., 25 калитлари бўлган Цезар криптолизими сифатида қаралиши мумкин. Калит сўз, одатда очиқ матндан қисқа бўлгани учун, ундан даврий равишда фойдаланилади.

Квадрат Полибия

uz - Polibiy kvadrati

Полибий квадрати

en - Polybius checkerboard

Одноалфавитная криптосистема, описанная греческим историком Полибием. Представляет собой квадрат 5×5 . Каждый символ открытого текста заменяется на пару символов, указывающих на столбец и строку, в которых расположен символ открытого текста.

Gre'k tarixchisi Polibiy tomonidan tavsiflangan bir alifboli kriptotizim. O'zida 5×5 kvadratni ifodalaydi. Ochiq matnning har bir simvoli ochiq matnning simvoli joylashgan ustun va satrni ko'rsatuvchi juft simvollar bilan almashtiriladi.

Грек тарихчиси Полибий томонидан тавсифланган бир алифболи криптолизим. Ўзида 5×5 квадратни ифодалайди. Очиқ матннинг ҳар бир симболи очиқ матннинг симболи жойлашган устун ва сатрни кўрсатувчи жуфт символлар билан алмаштирилади.

Квинтет

uz - kvintet

квинтет

en - quintet

Аутентификационный вектор в UMTS, состоящий из пяти компонентов – RAND, XRES, CK, IK и AUTN.

Beshta komponent – RAND, XRES, CK, IK va AUTN dan tashkil topgan, UMTS dagi autentifikatsion vektor.

Бешта компонент – RAND, XRES, CK, IK ва AUTN дан ташкил топган, UMTS даги аутентификацион вектор.

К

Кейлоггер

uz - keylogger

кейлоггер

en - keylogger

Программа или аппаратное устройство, предназначенное для перехвата клавиатурного ввода.

Примечание – Кейлоггер осуществляет распознавание скан-кодов нажатых клавиш и скрытое сохранение и/или скрытую передачу их по какому-либо каналу.

Klaviaturadan kiritishni tutib olish uchun mo'ljallangan apparat qurilma yoki dastur.

Izoh – Keylogger bosilgan klavishlar skan-kodlarini aniqlashni ular yashirin saqlanishini va/yoki qandaydir kanal orqali uzatilishini amalga oshiradi.

Клавиатурадан киритишни тутиб олиш учун мўлжалланган аппарат қурилма ёки дастур.

Изоҳ – Кейлоггер босилган клавишлар скан-кодларини аниқлашни улар яширин сақланишини ва/ёки қандайдир канал орқали узатилишини амалга оширади.

Кибербезопасность

uz - kiberxavfsizlik

киберхавфсизлик

en - cybersecurity

Совокупность инструментов, политик, руководящих указаний, подходов к управлению рисками, обучения, распространения лучшего опыта, страхования, технологий информационной безопасности и информационных технологий, которые могут использоваться для защиты ресурсов пользователей в информационной среде.

Axborot muhitida foydalanuvchilar resurslarini muhofaza qilish uchun ishlatilishi mumkin bo'lgan vositalar, yo'llar, rahbariy ko'rsatmalar, ehtimoliy xavflarni boshqarishga yondashuvlar, o'rgatishlar, eng yaxshi tajribani tarqatish, sug'urta, axborot xavfsizligi texnologiyalari va axborot texnologiyalarining jami.

Ахборот мухитида фойдаланувчилар ресурсларини муҳофаза қилиш учун ишлатилиши мумкин бўлган воситалар, йўллар, раҳбарий кўрсатмалар, эҳтимолий хавфларни бошқаришга ёндашувлар, ўргатишлар, энг яхши тажрибани тарқатиш, сугурта, ахборот хавфсизлиги технологиялари ва ахборот технологияларининг жами.

Киберпреступление

uz - kiberjinoyat

кибержиноят

en - cybercrime

Любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети.

К

Kompyuter tizimi yoki tarmog‘i yordamida, kompyuter tizimi yoki tarmog‘i doirasida yoki kompyuter tizimi yoki tarmog‘iga qarshi sodir etilishi mumkin bo‘lgan har qanday jinoyat.

Компьютер тизими ёки тармоғи ёрдамида, компьютер тизими ёки тармоғи доирасида ёки компьютер тизими ёки тармоғига қарши содир этилиши мумкин бўлган ҳар қандай жиноят.

Кибертерроризм

uz - kiberterrorizm

кибертерроризм

en - cyberterrorism

Преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов.

Submilliy guruhlar yoki maxfiy agentlar tomonidan noharbiy nishonlarga nisbatan kuch ishlatilishida ifodalangan, axborot, kompyuter tizimlariga, kompyuter dasturlari va ma'lumotlarga siyosiy asoslangan qasddan qilinadigan hujumlar.

Субмиллий гуруҳлар ёки махфий агентлар томонидан ҳарбий нишонларга нисбатан куч ишлатилишида ифодаланган, ахборот, компьютер тизимларига, компьютер дастурлари ва маълумотларга сиёсий асосланган қасдан қилинадиган ҳужумлар.

Класс

uz - klass

класс

en - class

Группа семейств, объединенных общим назначением.

Umumiy vazifa bilan birlashtirilgan turkumlar guruhi.

Умумий вазифа билан бирлаштирилган туркумлар гуруҳи.

Класс защищенности средств вычислительной техники (автоматизиро-

Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного

К

ванной системы)

uz - hisoblash texnikasi vositalarining (avtomatlashtirilgan tizimning) muhofaza qilinganlik klassi

хисоблаш техникаси воситаларининг (автоматлаштирилган тизимнинг) муҳофаза қилинганлик класси

en - security class of facilities of computing machinery (computer-based system)

Класс идентификатора

uz - identifikator klassi

идентификатор класси

en - naming class

доступа к информации.

Hisoblash texnikasi vositalari (avtomatlashtirilgan tizim)ni axborotdan ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish bo'yicha talablarning muayyan yig'indisi.

Ҳисоблаш техникаси воситалари (автоматлаштирилган тизим)ни ахборотдан рўхсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш бўйича талабларнинг муайян йиғиндиси.

Категория, определяющая способ связи идентификатора со значением и способ его использования.

Identifikatorning qiymat bilan bog'lanish va undan foydalanish usulini belgilovchi kategoriya.

Идентификаторнинг қиймат билан боғланиш ва ундан фойдаланиш усулини белгиловчи категория.

Классификация

uz - klassifikatsiyalash (tasniflash)

классификациялаш (таснифлаш)

en - classification

Сортировка информации по категориям безопасности.

Axborotni xavfsizlik kategoriyalari bo'yicha saralash.

Ахборотни хавфсизлик категориялари бўйича саралаш.

Класс рисков

uz - risklar klassi

рисklar класси

en - risk category

Множество угроз информационной безопасности, выделенных по определенному признаку, например, относящихся к определенной подсистеме или типу ресурса.

Ma'lum bir, masalan, muayyan kichik tizimga yoki resurs turiga tegishli belgiga qarab ajratilgan, axborot xavfsizligiga bo'ladigan ko'plab tahdidlar.

Маълум бир, масалан, муайян кичик тизимга ёки ресурс турига тегишли белгига қараб ажратилган, ахборот хавфсизлигига бўладиган кўплаб таҳдид-

К

Клонирование

uz - klonlash

клонлаш

en - cloning

лар.

1 Изготовление сотового телефона-двойника с чужим номером путем его перепрограммирования.

2 Неправомочное изготовление телефонов или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок.

1 Qayta dasturlash yo‘li bilan, begona raqamli sotali o‘xshash telefonni tayyorlash.

2 Telefonlar yoki abonentlarning qalbaki identifikatori bo‘lgan telefon to‘lov kartalari, raqamlar va to‘lov belgilarini vakolatga ega bo‘lmagan holda tayyorlash.

1 Қайта дастурлаш йўли билан, бегона рақамли сотали ўхшаш телефонни тайёрлаш.

2 Телефонлар ёки абонентларнинг қалбаки идентификатори бўлган телефон тўлов карталари, рақамлар ва тўлов белгиларини ваколатга эга бўлмаган ҳолда тайёрлаш.

Ключ анонимности

uz - anonimlik kaliti

анонимлик калити

en - anonymity key

Вспомогательный ключ, используемый в процедуре аутентификации через шифрование (не связан с абонентом).

Autentifikatsiya qilish protsedurasida shifrlash orqali foydalaniladigan yordamchi kalit (abonent bilan bog‘lanmagan).

Аутентификация қилиш процедурасида шифрлаш орқали фойдаланиладиган ёрдамчи калит (абонент билан боғланмаган).

Ключ аутентификации

uz - autentifikatsiya qilish kaliti

аутентификация қилиш

калити

en - authentication key, A-KEY

1 Уникальное кодовое слово, хранящееся в памяти сотового телефона. Используется для аутентификации и генерирования ключей шифрования в сетях USDC и CDMA-450.

2 Закрытый или открытый ключ шифрования, который используется для аутентификации абонента. Каждый абонент радиосети обладает индивидуальным ключом аутентификации, запрограммированным при инициализации радиостанции.

К

1 Sotali telefon xotirasida saqlanadigan noyob kodli soʻz. *USDC* va *CDMA-450* tarmoqlarida shifrlash kalitlarini autentifikatsiya qilish va generatsiyalash uchun ishlatiladi.

2 Abonentni autentifikatsiya qilish uchun ishlatiladigan yopiq yoki ochiq shifrlash kaliti. Radiotarmoqning har bir abonentni radiostansiyani initsializatsiya qilishda dasturlashtirilgan individual autentifikatsiya qilish kalitiga ega boʻladi.

1 Sotali telefon xotirasida saqlanadigan noʻb kodli sʻz. *USDC* va *CDMA-450* tarmoqlarida shifrlash kalitlarini autentifikatsiya qilish va generatsiyalash uchun ishlatiladi.

2 Abonentni autentifikatsiya qilish uchun ishlatiladigan yopiq yoki ochiq shifrlash kaliti. Radiotarmoqning har bir abonentni radiostansiyani initsializatsiya qilishda dasturlashtirilgan individual autentifikatsiya qilish kalitiga ega boʻladi.

Ключ базы данных
uz - maʼlumotlar bazasi kaliti

маълумотлар базаси
калити

en - database key

Ключ, присвоенный системой управления базами данных и однозначно идентифицирующий запись базы данных.

Boshqaruv tizimi tomonidan maʼlumotlar bazasiga berilgan va maʼlumotlar bazasi yozuvini qatʼiy identifikatsiya qiluvchi kalit.

Бошқарув тизими томонидан маълумотлар базасига берилган ва маълумотлар базаси ёзувини қатъий идентификация қилувчи калит.

Ключ вторичный
uz - ikkilamchi kalit

иккиламчи калит
en - secondary key

1 Ключ, получаемый путем логического преобразования основного сообщения и какого-либо входного параметра, например, серийного номера абонентской станции.

2 Способ защиты программного обеспечения, в котором первый криптографический ключ открывает доступ ко второму ключу, являющемуся ключом для дешифрования программного обеспечения.

1 Asosiy xabarni va biror bir kirish parametrini, masa-

К

lan, abonent stansiyasining seriya raqamini mantiqiy qayta o'zgartirish yo'li bilan olinadigan kalit.

2 Dasturiy ta'minotni muhofaza qilish usuli, unda birinchi kriptografik kalit dasturiy ta'minotni deshifrovka qilish uchun kalit hisoblanadigan ikkinchi kalitdan foydalana olish uchun yo'l ochadi.

1 Асосий хабарни ва бирор бир кириш параметрини, масалан, абонент станциясининг серия рақамини мантиқий қайта ўзгартириш йўли билан олинadigan калит.

2 Дастурий таъминотни муҳофаза қилиш усули, unda биринчи криптографик калит дастурий таъминотни дешифровка қилиш учун калит ҳисобlanadigan иккинчи калитдан фойдалана олиш учун йўл очади.

Ключ закрытый

uz - yopiq kalit

ёпиқ калит

en - private key

1 Один из ключей несимметричной системы шифрования. Используется при расшифровании сообщений и формировании электронной подписи.

2 Закрытая (секретная) часть пары криптографических ключей в системе шифрования с открытым ключом.

1 Nosimmetrik shifrlash tizimining kalitlaridan biri. Xabarlarini rasshifrovka qilishda va elektron imzoni shakllantirishda ishlatiladi.

2 Ochiq kalitli shifrlash tizimidagi juft kriptografik kalitlarning yopiq (maxfiy) qismi.

1 Носимметрик шифрлаш тизимининг калитларидан бири. Хабарларни расшифровка қилишда ва электрон имзони шакллантиришда ишлатилади.

2 Очиқ калитли шифрлаш тизимидаги жуфт криптографик калитларнинг ёпиқ (махфий) қисми.

Ключ защиты памяти

uz - хотирани muhofaza

qilish kaliti

хотирани муҳофаза қилиш калити

en - protection key

Код, присваиваемый блоку памяти, выделенному программе, и используемый для обращения программы к памяти в целях ее защиты. Должен совпадать с ключом защиты; при несовпадении задание завершается аварийно.

Dastur uchun ajratilgan хотира blokiga berilgan va muhofaza qilish maqsadida dastur хотирага murojaat qilishi uchun ishlatiladigan kod. Muhofaza kaliti bilan

К

mos kelishi kerak; mos kelmaganda topshiriq avariya bilan tugaydi.

Дастур учун ажратилган хотира блокига берилган ва муҳофаза қилиш мақсадида дастур хотирага мурожаат қилиши учун ишлатиладиган код. Муҳофаза калити билан мос келиши керак; мос келмаганда топшириқ авария билан тугайди.

Ключ (криптографический)

uz - kalit (kriptografik)

калит (криптографик)

en - cryptographic key

1 Последовательность символов, управляющая операциями шифрования и дешифрования.

2 Параметр криптографического алгоритма, последовательность символов, обеспечивающая возможность шифрования и расшифрования.

3 Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра.

1 Shifrlash va deshifrlash amallarini boshqaruvchi simvollar ketma-ketligi.

2 Kriptografik algoritm parametri, shifrlash va rasshifrovka qilish imkonini ta'minlaydigan simvollar ketma-ketligi.

3 Shifrning ko'plab almashtirishlaridan aniq bir almashtirishni belgilovchi ma'lumotlar jami.

1 Шифрлаш ва дешифрлаш амалларини бошқарувчи символлар кетма-кетлиги.

2 Криптографик алгоритм параметри, шифрлаш ва расшифровка қилиш имконини таъминлайдиган символлар кетма-кетлиги.

3 Шифрнинг кўплаб алмасhtiришларидан аниқ бир алмасhtiришни белгилувчи маълумотлар жами.

Ключ личный

uz - shaxsiy kalit

шахсий калит

en - private key

Ключ, предназначенный для дешифрования и используемый только его владельцем.

Deshifrlash uchun mo'ljallangan va faqat uning egasi tomonidan foydalaniladigan kalit.

Дешифрлаш учун мўлжалланган ва фақат унинг эгаси томонидан фойдаланиладиган калит.

Ключ общий

Секретный ключ в симметричной криптосистеме,

К

uz - umumiy kalit
умумий калит
en - public key

совместно используемый двумя или несколькими пользователями.

Simmetrik kriptotizimdagı, ikki yoki bir nechta foydalanuvchi tomonidan birgalikda ishlatiladigan maxfiy kalit.

Симметрик криптолизимдаги, икки ёки бир нечта фойдаланувчи томонидан биргаликда ишлатиладиган махфий калит.

Ключ открытый
uz - ochiq kalit
очиқ калит
en - public key

1 Ключ, который предназначен для использования любым логическим объектом для зашифрованной связи с владельцем соответствующего личного ключа.

2 Один из ключей асимметричной системы шифрования. Он не является секретом, но вычислить по нему соответствующий закрытый ключ нельзя. Применяется для шифрования сообщений и при проверке электронной подписи.

3 Ключ, используемый в асимметричной криптосистеме и доступный всем пользователям системы.

4 Общий криптографический ключ, который доступен всем пользователям и служит для расшифровки сообщений или верификации цифровых подписей.

1 Istalgan mantiqiy obyekt tomonidan tegishli shaxsiy kalit egasi bilan shifrlangan aloqani ochishda foydalanish uchun mo'ljallangan kalit.

2 Asimmetrik shifrlash tizimi kalitlaridan biri. U maxfiy hisoblanmaydi, lekin unga ko'ra tegishli yopiq kalitni hisoblash mumkin emas. Xabarlarini shifrlash va elektron imzoni tekshirishda qo'llaniladi.

3 Asimmetrik kriptotizimda qo'llaniladigan va tizimning barcha foydalanuvchilari erkin foydalana olishi uchun qulay bo'lgan kalit.

4 Barcha foydalanuvchilar erkin foydalana oladigan va xabarlarini rasshifrovka qilish yoki raqamli imzolarni verifikatsiya qilish uchun xizmat qiladigan umumiy kriptografik kalit.

1 Исталган мантиқий объект томонидан тегишли

К

шахсий калит эгаси билан шифрланган алоқани очишда фойдаланиш учун мўлжалланган калит.

2 Асимметрик шифрлаш тизими калитларидан бири. У махфий ҳисобланмайди, лекин унга кўра тегишли ёпиқ калитни ҳисоблаш мумкин эмас. Хабарларни шифрлаш ва электрон имзони текширишда қўлланилади.

3 Асимметрик криптотизимда қўлланиладиган ва тизимнинг барча фойдаланувчилари эркин фойдалана олиши учун қулай бўлган калит.

4 Барча фойдаланувчилар эркин фойдалана оладиган ва хабарларни расшифровка қилиш ёки рақамли имзоларни верификация қилиш учун хизмат қиладиган умумий криптографик калит.

Ключ разблокирования PIN-кода

uz - *PIN*-kodni blokirovkadan chiqarish kaliti

PIN-кодни блокировкадан чиқариш калити

en - PIN unblocking key, PUK

Специальный код в сети GSM, используемый для разблокировки SIM-карт.

GSM tarmogʻidagi, *SIM*-kartalarni blokirovkadan chiqarish uchun ishlatiladigan maxsus kod.

GSM тармоғидаги, *SIM*-карталарни блокировкадан чиқариш учун ишлатиладиган махсус код.

Ключ раундовый

uz - raund kaliti

раунд калити

en - round key

Секретный элемент, получаемый из ключа криптоалгоритма, и используемый шифром Файстеля и аналогичными криптоалгоритмами на одном раунде шифрования.

Kriptoalgoritm kalitidan olinadigan va shifrlashning bir raundida Faistel shifri hamda oʻxshash kriptoalgoritmalar tomonidan foydalaniladigan maxfiy element.

Криптоалгоритм калитидан олинадиган ва шифрлашнинг бир раундида Файстел шифри ҳамда ўхшаш криптоалгоритмлар томонидан фойдаланиладиган махфий элемент.

Ключ сеансовый

uz - seans kaliti

сеанс калити

en - session key

Криптографический ключ, используемый для шифрования в течение ограниченного промежутка времени, равного одному сеансу; после окончания передачи ключ автоматически стирается.

Bir seansga teng boʻlgan cheklangan vaqt oraliqida shifrlash uchun ishlatiladigan kriptografik kalit; uzatish tugagandan soʻng kalit avtomatik ravishda oʻchib

К

ketadi.

Бир сеансга тенг бўлган чекланган вақт оралиғида шифрлаш учун ишлатиладиган криптографик калит; узатиш тугагандан сўнг калит автоматик равишда ўчиб кетади.

Ключ секретный

uz - maxfiy kalit

махфий калит

en - secret key

1 Ключ, который предназначен для использования при шифровании и дешифровании ограниченным числом корреспондентов.

2 Ключ, используемый в симметричной криптосистеме и разделяемый между объектами или субъектами, которые устанавливают защищенное взаимодействие.

3 Ключ, используемый в асимметричной криптосистеме и известный, как правило, только одному объекту системы.

4 Ключ шифрования, принадлежащий только одному абоненту и предназначенный для конфиденциального доступа к защищенным данным.

5 Ключ, значение которого система использует для определения того, должен ли защищенный ресурс быть доступным процессу, выдавшему данное значение ключа.

1 Shifrlash va deshifrlashda korrespondentlarning cheklangan soni foydalanishi uchun mo'ljallangan kalit.

2 Simmetrik kriptotizimda ishlatiladigan va muhofazalangan o'zaro hamkorlikni o'rnatuvchi obyektlar yoki subyektlar o'rtasida taqsimlanadigan kalit.

3 Asimmetrik kriptotizimda ishlatiladigan va odatda, tizimning faqat bir obyektiga ma'lum bo'lgan kalit.

4 Faqat bir abonentga tegishli va muhofazalangan ma'lumotlardan konfidensial tarzda foydalana olish uchun mo'ljallangan shifrlash kaliti.

5 Qiymatidan, tizim muhofazalangan resursdan kalitning bu qiymatini bergan jarayon foydalana olishi yoki olmasligini aniqlash uchun foydalaniladigan kalit.

1 Шифрлаш ва дешифрлашда корреспондентларнинг чекланган сони фойдаланиши учун мўлжалланган калит.

К

2 Симметрик криптолизимда ишлатиладиган ва муҳофазаланган ўзаро ҳамкорликни ўрнатувчи объектлар ёки субъектлар ўртасида тақсимланадиган калит.

3 Асимметрик криптолизимда ишлатиладиган ва одатда, тизимнинг фақат бир объектига маълум бўлган калит.

4 Фақат бир абонентга тегишли ва муҳофазаланган маълумотлардан конфиденциал тарзда фойдалана олиш учун мўлжалланган шифрлаш калити.

5 Қийматидан, тизим муҳофазаланган ресурсдан калитнинг бу қийматини берган жараён фойдалана олиши ёки олмаслигини аниқлаш учун фойдаланиладиган калит.

Ключ системный

uz - tizim kaliti

тизим калити

en - system key

Ключ, обеспечивающий защиту системных средств от несанкционированного доступа.

Tizim vositalarining ruxsat etilmagan tarzda erkin foydalanishdan muhofaza qilinishini ta'minlaydigan kalit.

Тизим воситаларининг рухсат этилмаган тарзда эркин фойдаланишдан муҳофаза қилинишини таъминлайдиган калит.

Ключ скрытый

uz - yashirin kalit

яширин калит

en - sealed key

Ключ шифрования, который в явном виде не хранится на станции, а воспроизводится каждый раз с помощью криптографических алгоритмов.

Stansiyada ochiq ko'rinishda saqlanmaydigan, har safar kriptografik algoritmlar yordamida qayta ishlab chiqiladigan shifrlash kaliti.

Станцияда очик кўринишда сақланмайдиган, ҳар сафар криптографик алгоритмлар ёрдамида қайта ишлаб чиқиладиган шифрлаш калити.

Ключ стойкий

uz - barqaror kalit

барқарор калит

en - strong key

Ключ, длина которого достаточна для построения практически стойкой криптосистемы.

Uzunligi amalda barqaror kriptotizim tuzish uchun yetarli bo'lgan kalit.

Узунлиги амалда барқарор криптолизим тузиш

К

учун етарли бўлган калит.

Ключ управления доступом

uz - foydalana olishni

boshqarish kaliti

фойдалана олишни

бошқариш калити

en - access control key

Значение, предъявляемое процессом системе управления базами данных и сравниваемое ею с соответствующим значением с целью предотвращения несанкционированного доступа к данным.

Jarayon tomonidan ma'lumotlar bazasi boshqarish tizimiga beriladigan va ma'lumotlardan ruxsat etilmagan tarzda erkin foydalanishning oldini olish maqsadida, tegishli qiymat bilan solishtiriladigan qiymat.

Жараён томонидан маълумотлар базаси бошқариш тизимига бериладиган ва маълумотлардан рұхсат этилмаган тарзда эркин фойдаланишнинг олдини олиш мақсадида, тегишли қиймат билан солиштирилладиган қиймат.

Ключ целостности

uz - yaxlitlik kaliti

яхлитлик калити

en - integrity key

Ключ шифрования, применяемый для защиты информации от модификации или замены либо в процессе передачи по сети.

Axborotni o'zgartirilishdan yoki almashtirilishdan yo tarmoq orqali uzatish jarayonida muhofaza qilish uchun qo'llaniladigan shifrlash kaliti.

Ахборотни ўзгартирилишдан ёки алмаштирилишдан ё тармоқ орқали узатиш жараёнида муҳофаза қилиш учун қўлланиладиган шифрлаш калити.

Ключ шифрования

uz - shifrlash kaliti

шифрлаш калити

en - encryption key

1 Параметр алгоритмов шифрования и расшифрования.

2 Специальным образом сформированная случайная последовательность, имеющая сравнительно небольшую длину и используемая для управления процессом шифрования.

3 Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования информации, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

1 Shifrlash va rasshifrovka qilish algoritmlarining parametri.

К

2 Nisbatan uncha katta bo‘lmagan uzunlikka ega bo‘lgan va shifrlash jarayonini boshqarish uchun ishlatiladigan maxsus shakllantirilgan tasodifiy ketma-ketlik.

3 Axborotni kriptografik qayta o‘zgartirish algoritmi ayrim parametrlarining, bu algoritm uchun mumkin bo‘lgan o‘zgartirishlar ichidan bitta o‘zgartirish tanlanishini ta’minlovchi aniq maxfiy holati.

1 Шифрлаш ва расшифровка қилиш алгоритмларининг параметри.

2 Нисбатан унча катта бўлмаган узунликка эга бўлган ва шифрлаш жараёнини бошқариш учун ишлатиладиган махсус шакллантирилган тасодифий кетма-кетлик.

3 Ахборотни криптографик қайта ўзгартириш алгоритми айрим параметрларининг, бу алгоритм учун мумкин бўлган ўзгартиришлар ичидан битта ўзгартириш танланишини таъминловчи аниқ махфий ҳолати.

Книга кодировочная

uz - kod kitobi

код китоби

en - code book

Книга, используемая при преобразовании открытого текста в закодированную форму (криптограмму).

Ochiq matnni kodlangan shaklga (kriptogrammaga) aylantirishda foydalaniladigan kitob.

Очиқ матнни кодланган шаклга (криптограммага) айланттиришда фойдаланиладиган китоб.

Код

uz - kod

код

en - code

1 Множество преобразований элементов открытого текста (буквы, сочетания букв, слова и т.п.) группами символов (букв, цифр или других знаков). Является специальным типом шифра.

2 Правило преобразования сообщения из одного (исходного) алфавита в другой (объектный), обычно без каких-либо потерь информации.

1 Ochiq matn elementlarini (harflar, harflar birikmasi, so‘z va sh.k.) simvollar guruhlarini (harflar, raqamlar yoki boshqa belgilar) bilan ko‘plab qayta o‘zgartirish. Shifrnin maxsus turi hisoblanadi.

2 Xabarni bir (dastlabki) alifbodan boshqasiga (obyekt) axborotni hech qanday yo‘qotishlarsiz qayta

К

oʻzgartirish qoidasi.

1 Очiq матн элементларини (харфлар, харфлар бирикмаси, сўз ва ш.к.) символлар гуруҳлари (харфлар, рақамлар ёки бошқа белгилар) билан кўплаб қайта ўзгартириш. Шифрнинг махсус тури ҳисобланади.

2 Хабарни бир (дастлабки) алифбодан бошқасига (объект) ахборотни ҳеч қандай йўқотишларсиз қайта ўзгартириш қоидаси.

Код аутентификации

uz - autentifikatsiya qilish
kodi

аутентификация
қилиш коди

en - authentication code

Код фиксированной длины (имитовставка), вырабатываемый из данных с использованием секретного ключа и добавляемый к данным с целью обнаружения факта изменений хранимых или передаваемых по каналу телекоммуникаций данных.

Махфий калитдан фойдаланиб маълумотлардан олинadigan va saqlanadigan yoki telekommunikatsiyalar kanali orqali uzatiladigan ma'lumotlarning o'zgartirilish faktini aniqlash maqsadida, ma'lumotlarga qo'shiladigan qat'iy uzunlikdagi kod (imitoqo'shimcha).

Махфий калитдан фойдаланиб маълумотлардан олинadigan va saqlanadigan yoki telekommunikatsiyalar kanali orqali uzatiladigan ma'lumotlarning o'zgartirilish faktini aniqlash maqsadida, ma'lumotlarga qo'shiladigan qat'iy uzunlikdagi kod (imitoqo'shimcha).

Код аутентификации сообщений

uz - xabarlarni autentifikatsiya
qilish kodi

xabarlarни аутенти-
фикация қилиш коди

en - message authentication
code

1 Последовательность битов, являющаяся функцией обоих данных (открытого текста или шифротекста) и секретного ключа, которая присоединяется к данным, чтобы обеспечить аутентификацию данных.

Примечание – Функция, используемая для генерации кода аутентификации сообщений, обычно является односторонней функцией.

2 Код фиксированной длины, формируемый по заданному алгоритму из случайного входного потока и ключа шифрования.

1 Ikkala ma'lumotning (ochiq matn yoki shifratn)

К

hamda maxfiy kalitning funksiyasi bo'lgan bitlar ketma-ketligi. Ma'lumotlarni autentifikatsiya qilishni ta'minlash uchun ularga qo'shiladi.

Izoh – Xabarlarni autentifikatsiya qilish kodini generatsiyalash uchun foydalaniladigan funksiya, ko'pchilik hollarda, bir tomonlama funksiya hisoblanadi.

2 Berilgan algoritm bo'yicha tasodifiy kirish oqimi va shifrlash kalitidan tuziladigan, qayd qilingan uzunlikdagi kod.

1 Иккала маълумотнинг (очик матн ёки шифр-матн) ҳамда махфий калитнинг функцияси бўлган битлар кетма-кетлиги. Маълумотларни аутентификация қилишни таъминлаш учун уларга қўшилади.

Изоҳ – Хабарларни аутентификация қилиш кодини генерациялаш учун фойдаланиладиган функция, кўпчилик ҳолларда, бир томонлама функция ҳисобланади.

2 Берилган алгоритм бўйича тасодифий кириш оқими ва шифрлаш калитидан тузиладиган, қайд қилинган узунликдаги код.

Код изменяющийся во времени

uz - vaqtda o'zgaruvchi kod
вақтда ўзгарувчи код
en - time variant code

Код, слова которого некоторым образом изменяются в процессе работы.

So'zlari ish jarayonida biror-bir tarzda o'zgaradigan kod.

Сўзлари иш жараёнида бирор-бир тарзда ўзгарадиган код.

Кодирование

uz - kodlash
кодлаш
en - coding

Процесс преобразования исходного алфавита в объектный.

Dastlabki alifboni obyektli alifboga qayta o'zgartirish jarayoni.

Дастлабки алифбони объектли алифбога қайта ўзгартириш жараёни.

Кодирование источника

uz - manbani kodlash
манбани кодлаш
en - source coding

Использование в рамках заданного алфавита кодов переменной длины с целью уменьшения числа символов в сообщении до минимума, необходимого для представления всей информации сообщения или по крайней мере для обеспечения

К

условий такого сокращения.

Berilgan alifbo doirasida o'zgaruvchan uzunlikdagi kodlardan, xabardagi simvollar sonini, xabardagi butun axborotni taqdim etish yoki hech bo'lmaganda bunday qisqartirish shartlarini ta'minlash uchun zarur bo'lgan eng kam darajagacha kamaytirish maqsadida foydalanish.

Берилган алифбо доирасида ўзгарувчан узунликдаги кодлардан, хабардаги символлар сонини, хабардаги бутун ахборотни тақдим этиш ёки ҳеч бўлмаганда бундай қисқартириш шартларини таъминлаш учун зарур бўлган энг кам даражагача камайтириш мақсадида фойдаланиш.

Кодирование канальное
uz - kanal bo'yicha kodlash
канал бўйича кодлаш
en - channel coding

1 Использование кодов с обнаружением ошибок или кодов с исправлением ошибок для обеспечения надежной передачи по каналу телекоммуникаций.

2 Способ передачи зашифрованных сообщений, при котором каждое сообщение дешифрируется и перекодируется вновь после каждого этапа его пересылки.

1 Telekomunikatsiyalar kanali orqali ishonchli uzatishni ta'minlash uchun, xatolarni aniqlovchi kodlardan yoki xatolarni tuzatuvchi kodlardan foydalanish.

2 Shifrlangan xabarlarni uzatish usuli, bunda har bir xabar deshifrovka qilinadi va uni qayta jo'natishning har bir bosqichidan so'ng yana qayta kodlanadi.

1 Телекоммуникациялар канали орқали ишончли узатишни таъминлаш учун, хатоларни аниқловчи кодлардан ёки хатоларни тuzатувчи кодлардан фойдаланиш.

2 Шифрланган хабарларни узатиш усули, бунда ҳар бир хабар дешифровка қилинади ва уни қайта жўнатишнинг ҳар бир босқичидан сўнг яна қайта кодланади.

Кодирование с использованием флага
uz - bayroqdan foydalanib kodlash

Добавление к коду некоторой последовательности символов, которая не является кодовым словом и в процессе работы может быть использована как разделитель между словами.

К

байрокдан фойдаланиб
кодлаш
en - flag coding

Kodga kodli soʻz hisoblanmaydigan va ish jarayonida soʻzlar oʻrtasida boʻluvchi sifatida ishlatiladigan simvollarning biror-bir ketma-ketligini qoʻshish.

Кодга кодли сўз ҳисобланмайдиган ва иш жараёнида сўзлар ўртасида бўлувчи сифатида ишлатиладиган символларнинг бирор-бир кетма-кетлигини қўшиш.

**Кодирование с критерием
верности**
uz - ishonchlilik kriteriysi bilan
kodlash
ишончлилиқ критерийси
билан кодлаш
en - coding with fidelity criterion

Такое преобразование сообщения источника в кодовое слово, при котором после обратного преобразования получают некоторое другое сообщение, близкое к исходному в смысле заданного критерия верности.

Manba xabarini kodli soʻzga qayta oʻzgartirish, bunda teskari oʻzgartirishdan soʻng, dastlabki xabarga berilgan ishonchlilik kriteriysi maʼnosida yaqin boʻlgan qandaydir boshqa xabar olinadi.

Манба хабарини кодли сўзга қайта ўзгартириш, бунда тескари ўзгартиришдан сўнг, дастлабки хабарга берилган ишончлилиқ критерийси маъносида яқин бўлган қандайдир бошқа хабар олинади.

Код каскадный
uz - kaskadli kod
каскадли код
en - cascade code

Код с исправлением ошибок, который можно рассматривать как результат последовательного применения нескольких других кодов.

Bir nechta boshqa kodni ketma-ket qoʻllash natijasi sifatida qaralishi mumkin boʻlgan xatolarni tuzatuvchi kod.

Бир нечта бошқа кодни кетма-кет қўллаш натижаси сифатида қаралиши мумкин бўлган хатоларни тuzатувчи код.

Код контрольный
uz - nazorat kodi
назорат коди
en - check code

Код, позволяющий автоматически обнаруживать, локализовать и устранять ошибки в передаваемых данных.

Uzatiladigan maʼlumotlardagi xatolarni avtomatik

К

tarzda aniqlash, tarqalishiga yo‘l qo‘ymaslik va bartaraf qilish imkonini beradigan kod.

Узатиладиган маълумотлардаги хатоларни автоматик тарзда аниқлаш, тарқалишига йўл қўймаслик ва бартараф қилиш имконини берадиган код.

Код контрольный (проверочный)

uz - nazorat (tekshirish) kodi
назорат (текшириш) коди
en - checking code

Машинные команды, которые читают часть диска, чтобы определить, не является ли он несанкционированной копией.

Ruxsat etilmagan tarzda ko‘chirib olingan nusxa emasligini aniqlash uchun, diskning bir qismini o‘qiydigan mashina komandalari.

Рухсат этилмаган тарзда кўчириб олинган нусха эмаслигини аниқлаш учун, дискнинг бир қисмини ўқийдиган машина командалари.

Код обнаружения манипуляции

uz - manipulyatsiyani
aniqlash kodi
манипуляцияни
аниқлаш коди
en - manipulation detection
code

Последовательность битов, являющаяся функцией данных, к которым она добавлена, чтобы можно было обнаруживать наличие манипуляции.
Примечания

1 Полученное сообщение (данные плюс код обнаружения манипуляции) может быть зашифровано, чтобы обеспечить секретность или аутентификацию данных.

2 Функция, используемая для генерации кода обнаружения манипуляции, должна быть общедоступной.

Manipulyatsiya mavjudligini aniqlash mumkin bo‘lishi uchun, o‘zi qo‘shilgan ma’lumotlarning funksiyasi bo‘lgan bitlar ketma-ketligi.

Izohlar

1 Olingan xabar (ma’lumotlar+manipulyatsiyani aniqlash kodi) ma’lumotlarning maxfiyligini yoki autentifikasiya qilinishini ta’minlash maqsadida shifrlanishi mumkin.

2 Manipulyatsiyani aniqlash kodini generatsiya qilish uchun qo‘llaniladigan funksiya umumfoydalanadigan bo‘lishi kerak.

Манипуляция мавжудлигини аниқлаш мумкин бўлиши учун, ўзи қўшилган маълумотларнинг функцияси бўлган битлар кетма-кетлиги.

Изохлар

1 Олинган хабар (маълумотлар+манипуляцияни аниқлаш коди) маълумотларнинг махфийлигини ёки аутентификация қилинишини таъминлаш мақсадида шифрланиши

К

мумкин.

2 Манипуляцияни аниқлаш кодини генерация қилиш учун қўлланиладиган функция умумфойдаланадиган бўлиши керак.

Код операции

uz - operatsiya kodi

операция коди

en - operation code

Код с контролем на четность

uz - juftlikni nazorat

qilish kodi

жуфтликни назорат

қилиш коди

en - parity check code

Команда ЭВМ на уровне машинного кода.

Mashina kodi darajasidagi EHM komandasi.

Машина коди даражасидаги ЭХМ командаси.

Двоичный код, в котором к каждой кодовой комбинации присоединяется дополнительный контрольный разряд, что позволяет сохранить принятую в системе одну и ту же четность двоичных блоков.

Ikkilik kod, unda har bir kodli kombinatsiyaga qo'shimcha nazorat razryadi qo'shiladi, bu ikkilik blok-larning tizimda qabul qilingan aynan bir juftligini saqlash imkonini beradi.

Иккилик код, унда ҳар бир кодли комбинацияга қўшимча назорат разряди қўшилади, бу иккилик блоklarнинг тизимда қабул қилинган айнан бир жуфтлигини сақлаш имконини беради.

Код с минимальной избыточностью

uz - minimal ortiqchalikka

ega kod

минимал ортиқчаликка

эга код

en - minimum redundancy code

Как правило, под этим подразумевается код, построенный по процедуре Хаффмана. В общем случае «оптимальный» код с точки зрения средней длины кодового слова, сложность реализации кодирования не рассматривается.

Qoidaga ko'ra, bunda Xaffman protsedurasi bo'yicha tuzilgan kod tushuniladi. Umumiy holda kodli so'z-ning o'rtacha uzunligi nuqtai nazaridan qaraganda «optimal» kod, kodlashni amalga oshirishning murakkabligi ko'rib chiqilmaydi.

Қоидага кўра, бунда Хаффман процедураси бўйича тузилган код тушунилади. Умумий ҳолда кодли сўзнинг ўртача узунлиги нуқтаи назаридан қараганда «оптимал» код, кодлашни амалга оширишнинг мураккаблиги кўриб чиқилмайди.

Код с минимальным расстоянием

uz - minimal oraliqli kod

Избыточный код, в котором переход от одного допустимого значения к следующему сопровождается минимальным изменением в кодовой

К

минимал оралиқли код
en - minimum distance code

комбинации. Позволяет обнаруживать в передаваемых данных только одиночные ошибки.

Ortiqcha kod, unda yo‘l qo‘yiladigan bir qiymatdan keyingisiga o‘tish kodli kombinatsiyadagi minimal o‘zgarish bilan boradi. Uzatiladigan ma’lumotlarda faqat yakka xatolarni aniqlash imkonini beradi.

Ортиқча код, унда йўл қўйиладиган бир қийматдан кейингисига ўтиш кодли комбинациядаги минимал ўзгариш билан боради. Узатиладиган маълумотларда фақат якка хатоларни аниқлаш имконини беради.

Код с переменной скоростью
uz - o‘zgaruvchan tezlikli kod
ўзгарувчан тезликли код
en - variable-rate code

Код, используемый при описании сверхточных кодов, у которых длина кодовых подблоков изменяется во времени, а длина информационных подблоков остается постоянной.

Kodli qism bloklarning uzunligi vaqt bo‘yicha o‘zgaradigan, axborot qism bloklarining uzunligi doimiylicha qoladigan yuqori aniqlikdagi kodlarni tavsiflashda qo‘llaniladigan kod.

Кодли қисм блокларнинг узунлиги вақт бўйича ўзгарадиган, ахборот қисм блокларининг узунлиги доимийлигича қоладиган юқори аниқликдаги кодларни тавсифлашда қўлланиладиган код.

Код установления подлинности сообщения
uz - xabarning haqiqiyiligini o‘rnatish kodi

хабарнинг ҳақиқийлигини ўрнатиш коди
en - message authentication code

Код, присоединяемый к сообщению отправителем, который является результатом обработки сообщения через процесс криптографии.

Xabarga jo‘natuvchi tomonidan qo‘shiladigan, kriptografiya jarayoni orqali xabarni qayta ishlash natijasi hisoblanadigan kod.

Хабарга жўнатувчи томонидан қўшиладиган, криптография жараёни орқали хабарни қайта ишлаш натижаси ҳисобланадиган код.

Код Хаффмана
uz - Xaffman kodi
Хаффман коди

Префиксный код, в котором длина кодовой комбинации обратно пропорциональна частоте появления кодируемого элемента (чем чаще встре-

К

en - Huffman code

чається елемент, тем короче кодовая комбинация).

Prefiksli kod, unda kodli kombinatsiyaning uzunligi kodlashtiriladigan elementning paydo bo'lish chastotasiga teskari proporsional (element qancha ko'p uchrasa, kodli kombinatsiya shuncha qisqa).

Префиксли код, унда кодли комбинациянинг узунлиги кодлаштирилладиган элементнинг пайдо бўлиш частотасига тескари пропорционал (элемент қанча кўп учраса, кодли комбинация шунча қисқа).

Код Хемминга

uz - Xemming kodi

Хемминг коди

en - Hamming code

Код с минимальной избыточностью, обеспечивающий исправление одиночных ошибок.

Yakka xatolarning tuzatilishini ta'minlovchi minimal ortiqchalikka ega kod.

Якка хатоларнинг тузатилишини таъминловчи минимал ортиқчаликка эга код.

Коды Боуза-Чоудхури-Хокенгема

uz - Bouz-Choudhuri-

Xokengem kodlari

Боуз-Чоудхури-Хокенгем кодлари

en - Bose-Chaudhuri-

Nocquenghem codes

Семейство двоичных линейных блочных кодов с исправлением ошибок. Эти коды весьма эффективны, но главное их преимущество состоит в простоте кодирования/декодирования (с использованием сдвиговых регистров). Коды БЧХ используются и в качестве циклических кодов.

Xatolarni tuzatuvchi ikkilik chizikli blokli kodlar turkumi. Bu kodlar ancha samarador, lekin ularning asosiy afzalligi kodlash/dekodlashning oddiyligida (siljish registrlaridan foydalanib). BChX kodlari siklik kodlar sifatida ham ishlatiladi.

Хатоларни тузатувчи иккилик чизикли блокли кодлар туркуми. Бу кодлар анча самарадор, лекин уларнинг асосий афзаллиги кодлаш/декодлашнинг оддийлигида (силжиш регистрларидан фойдаланиб). БЧХ кодлари циклик кодлар сифатида ҳам ишлатилади.

Коды Голея

uz - Goley kodlari

Голей кодлари

Семейство совершенных линейных блочных кодов с исправлением ошибок. Коды Голея можно рассматривать как циклические коды.

К

en - Golay codes

Xatolarni tuzatuvchi chiziqli blokli kodlar turkumi. Goley kodlari siklik kod sifatida ham ko‘rib chiqilishi mumkin.

Хатоларни тузатувчи чизиқли блокли кодлар туркуми. Голей кодлари циклик код сифатида ҳам кўриб чиқилиши мумкин.

Коды Гоппы

uz - Gopp kodlari

Гопп кодлари

en - Goppa codes

Коды, исправляющие ошибки, используемые в различных криптосистемах. Использование кодов Гоппы основано на том факте, что декодирование кодов Гоппы возможно осуществить вручную, в то время как декодирование линейных блочных кодов, под которые «маскируются» коды Гоппы является NP-полной задачей и трудно выполнимо.

Turli kriptotizimlarda ishlatiladigan, xatolarni tuzatuvchi kodlar. Gopp kodlaridan foydalanish Gopp kodlarini dekodlashni qo‘lda amalga oshirish mumkinligiga asoslangan (Gopp kodlari «yashirinadigan») chiziqli blokli kodlarni dekodlash. NP to‘liq vazifa bo‘lib, uni bajarish juda qiyin.

Турли криптотизимларда ишлатиладиган, хатоларни тузатувчи кодлар. Гопп кодларидан фойдаланиш Гопп кодларини декодлашни қўлда амалга ошириш мумкинлигига асосланган (Гопп кодлари «яширинадиган») чизиқли блокли кодларни декодлаш. NP тўлиқ вазифа бўлиб, уни бажариш жуда қийин.

Коды, исправляющие ошибки

uz - xatolarni tuzatuvchi kodlar

хатоларни тузатувчи кодлар

en - error-correction code

Избыточные коды, использование которых позволяет с большой вероятностью не только обнаруживать, но и исправлять возникшие при передаче информации ошибки.

Ortiqcha kodlar, ulardan foydalanish katta ehtimollik bilan, axborot uzatishda sodir bo‘ladigan xatolarni nafaqat aniqlash, balki tuzatish imkonini ham beradi.

Ортиқча кодлар, улардан фойдаланиш катта эҳтимоллик билан, ахборот узатишда содир бўладиган хатоларни нафақат аниқлаш, балки тузатиш имконини ҳам беради.

Коды Рид-Мюллера

uz - Rid-Myuller kodlari

Рид-Мюллер кодлари

Семейство двоичных циклических блоковых кодов с исправлением ошибок.

К

en - Reed-Muller codes,
RM codes

Xatolarni tuzatuvchi ikkilik siklik blokli kodlar turkumi.

Коды Рида-Соломона

uz - Rid-Solomon kodlari

Рид-Соломон кодлари

en - Reed-Solomon codes,
RS codes

Хатоларни тuzатувчи иккилик циклик блокли кодлар туркуми.

Важное семейство линейных блоковых кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут быть отнесены к циклическим кодам.

Xatolarni tuzatuvchi chiziqli blokli kodlarning, xatolar paketlarini tuzatish uchun ayniqsa qulay bo'lgan, muhim turkumi. Ular siklik kodlarga taalluqli bo'lishi mumkin.

Хатоларни тuzатувчи чизикли блокли кодларнинг, хатолар пакетларини тuzатиш учун айниқса қулай бўлган, муҳим туркуми. Улар циклик кодларга тааллуқли бўлиши мумкин.

Коды с повторением

uz - takrorlanuvchi kodlar

такрорланувчи кодлар

en - repetition codes

Семейство совершенных циклических блоковых кодов с исправлением ошибок, в котором ключевые слова формируются просто r -кратным повторением слов сообщения. Если данные коды рассматривать как коды с параметрами (n, k) , то для любого k у них $n = rk$.

Xatolarni tuzatuvchi mukammal siklik blokli kodlar turkumi, unda kalit so'zlar xabardagi so'zlarni r marta oddiy takrorlash bilan shakllanadi. Agar bu kodlarni (n, k) parametrlarga ega kodlar deb qaralsa, ularda istalgan k uchun $n = rk$ bo'ladi.

Хатоларни тuzатувчи мукаммал циклик блокли кодлар туркуми, унда калит сўзлар хабардаги сўзларни r марта оддий такрорлаш билан шаклланади. Агар бу кодларни (n, k) параметрларга эга кодлар деб қаралса, уларда исталган k учун $n = rk$ бўлади.

Коллизия

uz - kolliziya

КОЛЛИЗИЯ

Событие, при котором хэш-функции от разных сообщений совпадают.

Turli xabarlarning xesh-funksiyasi bir-biriga mos ke-

К

en - collision

ladigan hodisa.

Турли хабарларнинг хэш-функцияси бир-бирига мос келадиган ҳодиса.

Команда перехода в режим шифрования

uz - shifrlash rejimiga o'tish komandasi

шифрлаш режимига ўтиш командаси

en - ciphering mode command

Команда, передаваемая базовой станцией и инициирующая установление режима шифрования в мобильной станции.

Bazaviy stansiya tomonidan uzatiladigan va mobil stansiyada shifrlash rejimi o'rnatilishini boshlab beruvchi komanda.

Базавий станция томонидан узатиладиган ва мобил станцияда шифрлаш режими ўрнатилишини бошлаб берувчи команда.

Компетентность

uz - kompetentlik

компетентлик

en - competence

Способность применять знания и навыки для достижения желаемых результатов.

Istalgan natijalarga erishish uchun bilim va ko'nikmalarni qo'llash qobiliyati.

Исталган натижаларга эришиш учун билим ва кўникмаларни қўллаш қобилияти.

Компилятор

uz - kompilyator

компилятор

en - compiler

Транслятор, предназначенный для выполнения компиляции.

Kompilyatsiyani bajarish uchun mo'ljallangan translyator.

Компиляцияни бажариш учун мўлжалланган транслятор.

Комплекс средств защиты

uz - muhofaza qilish

vositalari kompleksi

муҳофаза қилиш

воситалари комплекси

en - trusted computing base

Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или систем от несанкционированного доступа к информации и к объектам сферы информационных технологий и коммуникаций.

Hisoblash texnikasi vositalari yoki tizimlarining axborotdan hamda axborot texnologiyalari va kommunikatsiyalar sohasi obyektlaridan ruxsat etilmagan tarzda foydalana olishdan muhofaza qilinishini ta'minlash uchun yaratiladigan va tutib turiladigan dasturiy hamda texnik vositalar jami.

К

Ҳисоблаш техникаси воситалари ёки тизимларининг ахборотдан ҳамда ахборот технологиялари ва коммуникациялар соҳаси объектларидан рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилинишини таъминлаш учун яратилдиган ва тутиб туриладиган дастурий ҳамда техник воситалар жами.

Комплексность защиты

uz - muhofazaning

kompleksliligi

муҳофазанинг

комплекслилиги

en - security complexity

Принцип защиты, предусматривающий мероприятия против всех опасных видов и средств технической разведки.

Texnik razvedkaning barcha xavfli turlari va vositalariga qarshi tadbirlarni ko'zda tutuvchi muhofaza qilish prinsipi.

Техник разведканинг барча хавфли турлари ва воситаларига қарши тадбирларни кўзда тутувчи муҳофаза қилиш принципи.

Компонент

uz - komponent

компонент

en - component

Наименьшая выбираемая совокупность элементов, на которой могут быть основаны требования.

Talablar asoslanadigan, elementlarning eng kam tanlanadigan to'plami.

Талаблар асосланадиган, элементларнинг энг кам танланадиган тўплами.

Компонент базовый

uz - bazaviy komponent

базавий компонент

en - base component

Логический объект составного ОО, который предоставляет сервисы и ресурсы зависимому компоненту и который сам может быть предметом оценки.

Tarkibiy BOning, bog'liq bo'lgan komponentga servislar va resurslar taqdim etadigan va o'zi ham baholash predmeti bo'ladigan mantiqiy obyekt.

Таркибий БОнинг, боғлиқ бўлган компонентга сервислар ва ресурслар тақдим этадиган ва ўзи ҳам баҳолаш предмети бўладиган мантикий объект.

Компонент зависимый

uz - bog'liq bo'lgan komponent

боғлиқ бўлган компонент

Логический объект в составном ОО, который сам является предметом оценки, зависящий от базового компонента в части предоставления серви-

К

en - dependent component

сов.

Tarkibiy BO, o'zi baholash predmeti hisoblanadigan, xizmatlar ko'rsatish qismida bazaviy komponentga bog'liq bo'lgan mantiqiy obyekt.

Таркибий БО, ўзи баҳолаш предмети ҳисобланадиган, хизматлар кўрсатиш қисмида базавий компонентга боғлиқ бўлган мантиқий объект.

Компонент объекта оценки

uz - baholash obyektining komponenti

баҳолаш объектининг
компоненти

en - component target of evaluation

Успешно оцененный ОО, являющийся частью другого составного ОО.

Boshqa BO tarkibiy qismi hisoblanadigan, muvaffaqiyatli baholangan BO.

Бошқа БО таркибий қисми ҳисобланадиган, муваффақиятли баҳоланган БО.

Компоновка, обобщение

uz - komponovka qilish, umumlashtirish

компоновка қилиш,
умумлаштириш

en - linkage, fusion

Целенаправленное объединение данных или информации одной системы обработки данных с данными или информацией другой системы для получения защищенной информации.

Muhofaza qilingan axborotni olish uchun, ma'lumotlarni qayta ishlash bitta tizimining axborot yoki ma'lumotlarini boshqa tizimning axborot yoki ma'lumotlari bilan aniq bir maqsadni ko'zlagan holda birlashtirish.

Муҳофаза қилинган ахборотни олиш учун, маълумотларни қайта ишлаш битта тизимнинг ахборот ёки маълумотларини бошқа тизимнинг ахборот ёки маълумотлари билан аниқ бир мақсадни кўзлаган ҳолда бирлаштириш.

Компрометация

uz - komprometatsiya (obro'sizlantirish)

компрометация
(обрўсизлантириш)

en - compromise

1 Раскрытие криптографических ключей или конфиденциальной информации.

2 Утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.).

3 Нарушение компьютерной безопасности, в результате чего программы или данные могут быть модифицированы, уничтожены или могут стать доступными неполномочным логическим объек-

К

там.

1 Kriptografik kalitlar yoki konfidensial axborotni ochish.

2 Kritik axborotni yo‘qotish yoki uning mualliflashtirilmagan subyektlar (shaxslar, dasturlar, jarayonlar va b.q.) tomonidan olinishi.

3 Kompyuter xavfsizligining buzilishi, uning natijasida dastur yoki ma‘lumotlar o‘zgartirilishi, yo‘q qilinishi yoki vakolatga ega bo‘lmagan mantiqiy obyektlar uchun ochiq bo‘lib qolishi mumkin.

1 Криптографик калитлар ёки конфиденциал ахборотни очиш.

2 Критик ахборотни йўқотиш ёки унинг муаллифлаштирилмаган субъектлар (шахслар, дастурлар, жараёнлар ва б.қ.) томондан олинishi.

3 Компьютер хавфсизлигининг бузилиши, унинг натижасида дастур ёки маълумотлар ўзгартирилиши, йўқ қилиниши ёки ваколатга эга бўлмаган мантикий объектлар учун очик бўлиб қолиши мумкин.

Компрометация информации

uz - axborotga putur yetkazish (axborotni obro‘sizlantirish)

ахборотга путур етказиш (ахборотни обрўсизлантириш)

en - information compromise

Утечка или разглашение конфиденциальной информации, либо получение ее неавторизованными субъектами.

Konfidensial axborotning chiqib ketishi (yo‘qolishi) yoki oshkor bo‘lishi yoki mualliflashtirilmagan subyektlar tomonidan olinishi.

Конфиденциал ахборотнинг чиқиб кетиши (йўқолиши) ёки ошкор бўлиши ёки муаллифлаштирилмаган субъектлар томондан олинishi.

Конверт цифровой

uz - raqamli konvert

рақамли конверт

en - digital envelope

1 Данные, добавляемые к сообщению и позволяющие предполагаемому получателю проверять целостность содержания сообщения.

2 Механизм, в котором для шифрования сообщений используется симметричная криптосистема, а для шифрования секретных ключей – асимметричная. Таким образом, долговременный ключ принадлежит асимметричной криптосистеме, а сеансовый – симметричной криптосистеме.

К

1 Хабарга qo‘shimcha qilinadigan hamda mo‘ljallangan oluvchiga xabar mazmunining yaxlitligini tekshirish imkonini beradigan ma’lumotlar.

2 Xabarlarni shifrlash uchun simmetrik kriptotizimdan, maxfiy kalitlarni shifrlash uchun esa asimmetrik kriptotizimdan foydalaniladigan mexanizm. Shu tarzda uzoq muddatli kalit asimmetrik kriptotizimga, seansli kalit simmetrik kriptotizimga tegishli bo‘ladi.

1 Хабарга қўшимча қилинадиган ҳамда мўлжалланган олувчига хабар мазмунининг яхлитлигини текшириш имконини берадиган маълумотлар.

2 Хабарларни шифрлаш учун симметрик кriptotizimдан, махфий калитларни шифрлаш учун эса асимметрик кriptotizimдан фойдаланиладиган механизм. Шу тарзда узоқ муддатли калит асимметрик кriptotizimga, сеансли калит симметрик кriptotizimga тегишли бўлади.

Контейнер

uz - konteyner

контейнер

en - container

1 Файл, предназначенный для сокрытия тайных сообщений.

2 Любая информация, предназначенная для сокрытия тайных сообщений.

1 Maxfiy xabarlarni yashirish uchun mo‘ljallangan fayl.

2 Maxfiy xabarlarni yashirish uchun mo‘ljallangan har qanday axborot.

1 Махфий хабарларни яшириш учун мўлжалланган файл.

2 Махфий хабарларни яшириш учун мўлжалланган ҳар қандай ахборот.

Контрмера

uz - qarshi chora

қарши чора

en - countermeasure

Действие, устройство, процедура, метод или другая мера, которая предназначена для сведения к минимуму уязвимости.

Harakat, qurilma, protsedura, metod yoki zaifligini eng kam darajaga keltirish uchun mo‘ljallangan

К

boshqa chora-tadbir.

Ҳаракат, қурилма, процедура, метод ёки заифлигини энг кам даражага келтириш учун мўлжалланган бошқа чора-тадбир.

Контроллер безопасности сети с централизованным управлением

uz - markazlashtirilgan tarzda boshqariladigan tarmoq xavfsizlik kontrolleri

марказлаштирилган тарзда бошқариладиган тармоқ хавфсизлик контроллери

en - centralized security controller

Способ обеспечения безопасности сети, при котором основные функции безопасности реализуются в одном узле (ячейке) сети – центральном контроллере сети.

Тармоқ хавфсизлигини таъминлаш усули, бунда асосий хавфсизлик funksiyalari тармоқнинг бitta uzелida (yacheykasida) – markaziy kontrollerida amalga oshiriladi.

Тармоқ хавфсизлигини таъминлаш усули, бунда асосий хавфсизлик функциялари тармоқнинг битта узелида (ячейкасида) – марказий контроллерида амалга оширилади.

Контроллер дисковый

uz - disk kontrolleri

диск контроллери

en - disk controller

Устройство, которое подключает к ЭВМ один или несколько дисководов и управляет их работой.

ЕНМга бitta yoki bir nechta diskovodni ulaydigan va ularning ishini boshqaradigan qurilma.

ЭХМга битта ёки бир нечта дисководни улайдиган ва уларнинг ишини бошқарадиган қурилма.

Контроллер домена

uz - domen kontrolleri

домен контроллери

en - domain controller

Компьютер, на котором хранится список учетных записей домена, выполняющий проверку пароля при сквозной проверке подлинности.

Нақiqiylikni yalpi tekshirishda parolning tekshirilishini bajaradigan, domenning hisobga olish yozuvlari ro‘uxati saqlanadigan kompyuter.

Ҳақиқийликни ялпи текширишда паролнинг текширилишини бажарадиган, доменнинг ҳисобга олиш ёзувлари рўйхати сақланадиган компьютер.

Контроль

uz - nazorat

Совокупность действий, позволяющих получать независимый обзор и анализ системных записей

К

назорат
en - control

и активности системы с целью установления ее текущего состояния безопасности.

Tizim xavfsizligining joriy holatini aniqlash maqsadida, mustaqil obzor va tizim yozuvlarining tahlilini hamda tizim faolligini olish imkonini beruvchi amallar jami.

Тизим хавфсизлигининг жорий ҳолатини аниқлаш мақсадида, мустақил обзор ва тизим ёзувларининг таҳлилини ҳамда тизим фаоллигини олиш имконини берувчи амаллар жами.

Контроль битов
uz - bitlarni nazorat qilish
битларни назорат қилиш
en - bit counting

Метод защиты от копирования, при котором диск распознается как оригинал, если некоторая дорожка (или другая область) содержит определенное число битов.

Nusxa ko'chirishdan muhofaza qilish metodi, unga ko'ra, yo'lka (yoki boshqa soha) bitlarning ma'lum sonini o'z ichiga olsa, disk original sifatida aniqlanadi.

Нусха кўчиришдан муҳофаза қилиш методи, унга кўра, йўлка (ёки бошқа соҳа) битларнинг маълум сонини ўз ичига олса, диск оригинал сифатида аниқланади.

Контроль данных
uz - ma'lumotlarni nazorat qilish
маълумотларни назорат қилиш
en - data control

Проверка достоверности и целостности данных. Различают синтаксический, семантический и прагматический контроль.

Ma'lumotlarning ishonchliligi va yaxlitligini tekshirish. Sintaksis, semantik va pragmatik nazorat farq qilinadi.

Маълумотларнинг ишончлилиги ва яхлитлигини текшириш. Синтаксис, семантик ва прагматик назорат фарқ қилинади.

Контроль доступа
uz - foydalana olishni

Процесс, который ограничивает доступ к ресурсам автоматизированной системы в соответствии

К

nazorat qilish
фойдалана олишни
назорат қилиш
en - access control

Контроль дублированием
uz - takrorlash orqali
nazorat qilish
такроплаш орқали
назорат қилиш
en - duplication control

Контроль избыточным циклическим кодом
uz - ortiqcha siklik kod bilan nazorat qilish
ортиқча циклик код билан назорат қилиш
en - cyclic redundancy control

с требуемой моделью защиты.

Talab qilinadigan muhofaza qilish modeliga muvofiq, avtomatlashtirilgan tizim resurslaridan erkin foydalanishni cheklaydigan jarayon.

Талаб қилинадиган муҳофаза қилиш моделига мувофиқ, автоматлаштирилган тизим ресурсларидан эркин фойдаланишни чеклайдиган жараён.

Контроль двух тождественных процессов посредством сравнения их результатов. Полное совпадение результатов свидетельствует об отсутствии ошибок.

Ikkita bir-biriga o'xshash jarayonni ularning natijalarini solishtirish vositasida, nazorat qilish. Natijalarning to'liq mos kelishi xatolarning yo'qligidan dalolat beradi.

Иккита бир-бирига ўхшаш жараённи уларнинг натижаларини солиштириш воситасида, назорат қилиш. Натижаларнинг тўлиқ мос келиши хатоларнинг йўқлигидан далолат беради.

1 Один из способов автоматического контроля целостности данных при их передаче и хранении. Вычисленное с помощью разновидности полиномиального кода (т.е. по более сложным правилам, чем контрольная сумма) число помещается в конце записи в памяти, используется для контроля целостности данных при операциях чтения/записи или при передаче по каналам телекоммуникаций.

2 Способ продольного контроля данных, который обеспечивает коррекцию ошибок.

1 Ma'lumotlarni uzatish va saqlashda ularning yaxlitligini avtomatik nazorat qilish usullaridan biri. Polinomial kodning bir turi yordamida hisoblangan (ya'ni, nazorat summasiga qaraganda murakkabroq qoidalar bo'yicha) son xotiradagi yozuvning oxirida joylashtiriladi, o'qish/yozish operatsiyalarida yoki telekommunikatsiyalar kanallari orqali uzatishda ma'lumotlarning yaxlitligini nazorat qilish uchun foydalaniladi.

К

2 Ma'lumotlarni bo'ylama nazorat qilish usuli, xatolarning tuzatilishini ta'minlaydi.

1 Ma'lumotlarni uzatish va saqlashda ularning yaxlitligini avtomatik nazorat qilish usullaridan biri. Полиномиал коднинг бир тури ёрдамида ҳисобланган (яъни, нazorat суммасига қараганда мураккаброқ қоидалар бўйича) сон хотирадаги ёзувнинг охирида жойлаштирилади, ўқиш/ёзиш операцияларида ёки телекоммуникациялар каналлари орқали узатишда маълумотларнинг yaxlitligini nazorat qilish uchun фойдаланилади.

2 Ma'lumotlarni бўйлама nazorat qilish usuli, xatolarning tuzatilishini ta'minlaydi.

Контроль избыточным кодом продольный

uz - ortiqcha kod bilan bo'ylama nazorat qilish

ортиқча код билан бўйлама нazorat qilish

en - longitudinal redundancy control

Метод контроля целостности данных при чтении/записи на магнитную ленту – контрольные суммы считаются для блока данных по каждой дорожке.

O'qish/magnit tasmaga yozishda ma'lumotlar yaxlitligini nazorat qilish metodi, nazorat summalari har bir yo'lka bo'yicha ma'lumotlar bloki uchun hisoblanadi.

Ўқиш/магнит тасмага ёзишда маълумотлар yaxlitligini nazorat qilish metodi, nazorat summalari har bir yo'lka bo'yicha ma'lumotlar bloki uchun hisoblanadi.

Контроль качества

uz - sifatni nazorat qilish

сифатни нazorat qilish

en - quality control

Использование методов выборки, проверки и испытания на всех уровнях разработки системы с целью выпуска бездефектного оборудования и программного обеспечения.

Tizimni ishlab chiqishning barcha bosqichlarida nuqsonsiz uskuna va dasturiy ta'minot chiqarish maqsadida tanlash, tekshirish va sinash metodlaridan foydalanish.

Тизимни ишлаб чиқишнинг барча босқичларида нуқсонсиз ускуна ва дастурий таъминот чиқариш мақсадида танлаш, текшириш ва синаш методларидан фойдаланиш.

Контроль нажатия клавиш

Определение правильности ввода данных с по-

К

uz - klavishlar bosilishini nazorat qilish

клавишлар босилишини

назорат қилиш

en - keystroke verification

мощью метода повторного ввода тех же самых данных с клавиатуры.

Ma'lumotlarning to'g'ri kiritilayotganligini, aynan shu ma'lumotlarni klaviaturadan takroran kiritish usuli yordamida aniqlash.

Маълумотларнинг тўғри киритилаётганлигини, айнан шу маълумотларни клавиатурадан такроран киритиш усули ёрдамида аниқлаш.

Контроль по избыточности

uz - ortiqchalik bo'yicha nazorat qilish

ортиқчалик бўйича

назорат қилиш

en - redundancy control

Контроль, выполняемый или с помощью резервированных технических средств, или на основе избыточной информации и обеспечивающий выдачу сведений о наличии определенных ошибок.

Rezervlangan texnik vositalar yordamida yoki ortiqcha axborot asosida bajariladigan va ayrim xatolar mavjudligi haqida ma'lumotlar olinishini ta'minlaydigan nazorat.

Резервланган техник воситалар ёрдамида ёки ортиқча ахборот асосида бажариладиган ва айрим хатолар мавжудлиги ҳақида маълумотлар олиншини таъминлайдиган назорат.

Контроль по избыточности циклический

uz - ortiqchalik bo'yicha siklik nazorat

ортиқчалик бўйича

циклик назорат

en - cyclic redundancy control

Контроль по избыточности, в котором дополнительные цифры или символы генерируются циклическим алгоритмом.

Ortiqchalik bo'yicha nazorat bo'lib, qo'shimcha raqamlar yoki simvollar siklik algoritm bilan generatsiyalanadi.

Ортиқчалик бўйича назорат бўлиб, қўшимча рақамлар ёки символлар циклик алгоритм билан генерацияланади.

Контроль по остатку, контроль по модулю n

uz - qoldiq bo'yicha nazorat, n moduli bo'yicha nazorat

қолдиқ бўйича назорат,

n модули бўйича назорат

en - residue check,

Простой метод обнаружения ошибок, основанный на анализе некоторого набора данных или участка программы. Если этот набор представляет собой совокупность блоков длиной m bit, то берется сумма по модулю n , где $n = 2^{**}m$, и ставится в конец набора. Позднее (например, после пересылки набора данных в другое место) можно

К

modulo- n - check

осуществить повторное вычисление контрольной суммы; при этом будут выявлены одиночные ошибки на уровне битов. Простейшим вариантом метода ($m = 1, n = 2$) является контроль четности.

Xatolarni aniqlashning, ma'lumotlarning ayrim to'plami yoki dasturning ayrim qismini tahlil qilishga asoslangan, oddiy metodi. Agar bu to'plam, m bit uzunlikdagi bloklarning jamini o'zida ifodalasa, n moduli bo'yicha summa olinadi, bunda $n = 2^{*}m$, va to'planning oxiriga qo'yiladi. Keyinchalik (masalan, ma'lumotlar to'plami boshqa joyga o'tkazilgach) nazorat summasini takroriy hisoblashni amalga oshirish mumkin, bunda bitlar darajasidan ayrim xatolar aniqlanadi. ($m = 1, n = 2$) metodining oddiy varianti juftlikni nazorat qilish hisoblanadi.

Хатоларни аниқлашнинг, маълумотларнинг айрим тўплами ёки дастурнинг айрим қисмини таҳлил қилишга асосланган, оддий методи. Агар бу тўплам, m bit узунликдаги блокларнинг жамини ўзида ифодаласа, n модули бўйича сумма олинади, бунда $n = 2^{*}m$, ва тўпламнинг охирига қўйилади. Кейинчалик (масалан, маълумотлар тўплами бошқа жойга ўтказилгач) назорат суммасини такрорий ҳисоблашни амалга ошириш мумкин, бунда битлар даражасидан айрим хатолар аниқланади. ($m = 1, n = 2$) методининг оддий варианты жуфтликни назорат қилиш ҳисобланади.

**Контроль по четности
продольный**

uz - juftlik bo'yicha
bo'ylama nazorat

жуфтлик бўйича
бўйлама назорат

en - longitudinal parity check

Контроль по четности на строке двоичных цифр, которые являются членами набора, формирующего матрицу.

Matritsani shakllantiruvchi to'plam bo'lagi hisoblanadigan ikkilik raqamlar satrida juftlik bo'yicha nazorat qilish.

Матрицани шаклантирувчи тўплам бўлаги ҳисобланадиган иккилик рақамлар сатрида жуфтлик бўйича назорат қилиш.

К

Контроль по четности поперечный

uz - juftlik bo'yicha

ko'ndalang nazorat

жуфтлик бўйича

кўндаланг назорат

en - transverse parity check

Контроль по четности на столбце двоичных цифр, которые являются членами набора, формирующего матрицу.

Matritsani shakllantiruvchi to'plam bo'lagi hisoblanadigan ikkilik raqamlar ustunida juftlik bo'yicha nazorat qilish.

Матрицани шакллантирувчи тўплам бўлаги ҳисобланадиган иккилик рақамлар устунда жуфтлик бўйича назорат қилиш.

Контроль правильности

uz - to'g'rilikni nazorat

qilish

тўғрилиқни назорат

қилиш

en - validity check

Любая проверка соответствия некоторого объекта установленным ограничениям. Например, если какое-либо значение элемента данных вводится программой, то обычно этой программой осуществляется проверка значения на соответствие заданному диапазону.

Qandaydir obyektning belgilangan cheklashlarga muvofiqligini har qanday tekshirish. Masalan, ma'lumotlar elementining biror-bir qiymati dastur tomonidan kiritilsa, odatda, shu dastur tomonidan qiymatning berilgan diapazonga muvofiqligini tekshirish amalga oshiriladi.

Қандайдир объектнинг белгиланган чеклашларга мувофиқлигини ҳар қандай текшириш. Масалан, маълумотлар элементининг бирор-бир қиймати дастур томонидан киритилса, одатда, шу дастур томонидан қийматнинг берилган диапазонга мувофиқлигини текшириш амалга оширилади.

Контроль продольный (циклический)

uz - bo'ylama (siklik) nazorat

бўйлама (циклик) назорат

en - longitudinal repundancy check

Контроль за счет избыточности, при котором контрольная сумма вычисляется для всего блока данных, как правило, с помощью циклических кодов.

Ortiqchalik hisobiga nazorat qilish, bunda nazorat summasi siklik kodlar yordamida butun ma'lumotlar bloki uchun hisoblab chiqiladi.

Ортиқчалик ҳисобига назорат қилиш, бунда назорат суммаси циклик кодлар ёрдамида бутун маълумотлар блоқи учун ҳисоблаб чиқилади.

К

Контроль работы с данными

uz - ma'lumotlar bilan ishlashni nazorat qilish

маълумотлар билан ишлашни назорат қилиш

en - manipulation detection

Процедура, позволяющая выявить, подвергался ли блок данных случайным или преднамеренным воздействиям.

Ma'lumotlar bloki tasodifiy yoki qasddan qilingan ta'sirlar ostida bo'lgan yoki bo'lmaganligini aniqlash imkonini beradigan protsedura.

Маълумотлар блоки тасодифий ёки қасддан қилинган таъсирлар остида бўлган ёки бўлмаганлигини аниқлаш имконини берадиган процедура.

Контроль средств защиты

uz - muhofaza vositalarini nazorat qilish

муҳофаза воситаларини назорат қилиш

en - security audit

Инспекция системных записей и работы персонала с целью проверки функционирования систем защиты, их соответствия принятой политике безопасности и требованиям эксплуатации, а также выработки соответствующих рекомендаций.

Muhofaza tizimlarining ishlashini, ularning ekspluatatsiya qilish talablariga va qabul qilingan xavfsizlik siyosatiga muvofiqligini tekshirish, shuningdek, tegishli tavsiyalarni ishlab chiqish maqsadida, tizim yozuvlari va personal ishini nazorat qilish.

Муҳофаза тизимларининг ишлашини, уларнинг эксплуатация қилиш талабларига ва қабул қилинган хавфсизлик сиёсатига мувофиқлигини текшириш, шунингдек, тегишли тавсияларни ишлаб чиқиш мақсадида, тизим ёзувлари ва персонал ишини назорат қилиш.

Контроль четности

uz - juftlikni nazorat qilish

жуфтликни назорат қилиш

en - parity check

Метод контроля данных, при котором сумма по модулю 2 двоичных единиц в машинном слове, включая контрольный разряд, должна иметь определенное значение: быть всегда четной или нечетной. Неравенство суммы этому значению говорит об ошибке в данных.

Ma'lumotlarni nazorat qilish metodi, unda mashina so'zidagi ikkilik birliklarning ikki moduli bo'yicha summasi, nazorat razryadini qo'shgan holda, ma'lum qiymatga ega bo'lishi kerak: har doim juft yoki har doim toq bo'lishi kerak. Summaning bu qiymatga teng kelmasligi ma'lumotlarda xato borligini bildiradi.

К

Маълумотларни назорат қилиш методи, унда машина сўзидаги иккилик бирликларнинг икки модули бўйича суммаси, назорат разрядини қўшган ҳолда, маълум қийматга эга бўлиши керак: ҳар доим жуфт ёки ҳар доим тоқ бўлиши керак. Сумманинг бу қийматга тенг келмаслиги маълумотларда хато борлигини билдиради.

Контроль эффективности защиты информации

uz - axborotni muhofaza qilish samaradorligini nazorat qilish

ахборотни муҳофаза қилиш самарадорлигини назорат қилиш

en - information security performance management

Проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Axborotni muhofaza qilish bo'yicha tadbirlar samaradorligining, belgilangan talablarga yoki muhofaza qilish samaradorligi normalariga muvofiqligini tekshirish.

Ахборотни муҳофаза қилиш бўйича тадбирлар самарадорлигининг, белгиланган талабларга ёки муҳофаза қилиш самарадорлиги нормаларига мувофиқлигини текшириш.

Конфиденциальность

uz - konfidensiallik

конфиденциаллик

en - confidentiality

1 Свойство информации быть недоступной или закрытой для неавторизованных лиц, логических объектов или процессов.

2 Субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

3 Состояние информации и ее носителя, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

4 Невозможность получения несанкционированного доступа к информации в результате перехвата и других несанкционированных действий.

1 Axborotning avtorizatsiya qilinmagan shaxslar, mantiqiy obyektlar yoki jarayonlar uchun foydalanib bo'lmazlik yoki yopiqlik xususiyati.

К

2 Axborotdan foydalanish huquqiga ega subyektlar doirasiga cheklovlar kiritish zarurligini ko'rsatuvchi va tizimning (muhitning) ko'rsatilgan axborotni undan erkin foydalanish huquqi bo'lmagan subyektlardan sir saqlash zarurligini ta'minlovchi, subyektiv aniqlanadigan (qo'shib yoziladigan) axborot xarakteristikasi (xususiyati).

3 Axborot va uning tashuvchisining holati, bunda u bilan ruxsat etilmagan tarzda tanishishning yoki ruxsat etilmagan tarzda hujjatlashtirish (nusxa ko'chirish)ning oldini olish ta'minlanadi.

4 Tutib olish va boshqa ruxsat etilmagan harakatlar natijasida axborotdan ruxsat etilmagan tarzda foydalana olishning mumkin bo'lmashligi.

1 Ахборотнинг авторизация қилинмаган шахслар, мантиқий объектлар ёки жараёнлар учун фойдаланиб бўлмаслик ёки ёпиклик хусусияти.

2 Ахборотдан фойдаланиш ҳуқуқига эга субъектлар доирасига чекловлар киритиш зарурлигини кўрсатувчи ва тизимнинг (муҳитнинг) кўрсатилган ахборотни ундан эркин фойдаланиш ҳуқуқи бўлмаган субъектлардан сир сақлаш зарурлигини таъминловчи, субъектив аниқланадиган (қўшиб ёзиладиган) ахборот хarakteristikasi (хусусияти).

3 Ахборот ва унинг ташувчисининг ҳолати, бунда у билан рuxсат этилмаган тарзда танишишнинг ёки рuxсат этилмаган тарзда ҳужжатлаштириш (нусха кўчириш)нинг олдини олиш таъминланади.

4 Тутиб олиш ва бошқа рuxсат этилмаган ҳаракатлар натижасида ахборотдан рuxсат этилмаган тарзда фойдалана олишнинг мумкин бўлмаслиги.

Конфиденциальность информации

uz - axborotning

konfidensialligi

axborotning

konfidensialligi

en - information confidentiality

Состояние информации и ее носителей, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Axborot va uni tashuvchilarning holati, bunda u bilan ruxsat etilmagan tarzda tanishishning yoki ruxsat

К

etilmagan tarzda hujjatlashtirish (nusxa ko'chirish)-ning oldini olish ta'minlanadi.

Ахборот ва уни ташувчиларнинг ҳолати, бунда у билан рухсат этилмаган тарзда танишишнинг ёки рухсат этилмаган тарзда ҳужжатлаштириш (нусаха кўчириш)нинг олдини олиш таъминланади.

Конфиденциальность трафика

uz - trafikning

konfidensialligi

трафикнинг

конфиденциаллиги

en - traffic confidentiality

Услуги конфиденциальности, обеспечивающие защиту от анализа трафика (потока сообщений).

Trafik (xabarlar oqimi)ni tahlildan muhofaza qilinishini ta'minlovchi konfidensiallik xizmatlari.

Трафик (хабарлар оқими)ни таҳлилдан муҳофаза қилинишини таъминловчи конфиденциаллик хизматлари.

Концепция диспетчера доступа

uz - erkin foydalanish

dispatcheri konsepsiyasi

эркин фойдаланиш

диспетчера концепцияси

en - reference monitor concept

Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях субъектов к объектам.

Abstrakt mashinaga taalluqli, erkin foydalanishni boshqarish konsepsiyasi, u subyektlarning obyektlariga barcha murojaatlarida vositachilik qiladi.

Абстракт машинага тааллуқли, эркин фойдаланишни бошқариш концепцияси, у субъектларнинг объектларга барча мурожаатларида воситачилик қилади.

Концепция доступа

uz - erkin foydalanish

konsepsiyasi

эркин фойдаланиш

концепцияси

en - access concept

Модель управления доступом, осуществляемая в абстрактной ЭВМ, которая посредничает при всех обращениях субъектов к информационным ресурсам. Существуют следующие концепции доступа: дискреционное управление, мандатное управление, многоуровневая защита.

Abstrakt EHMda amalga oshiriladigan, erkin foydalanishni boshqarish modeli, u subyektlarning axborot resurslariga qiladigan barcha murojaatlarida vositachilik qiladi. Quyidagi erkin foydalanish konsepsiyalari mavjud: diskretsiyon boshqarish, mandatli boshqarish, ko'p darajali muhofaza.

К

Абстракт ЭХМда амалга ошириладиган, эркин фойдаланишни бошқариш модели, у субъектларнинг ахборот ресурсларига қиладиган барча муурожаатларида воситачилик қилади. Қуйидаги эркин фойдаланиш концепциялари мавжуд: дискрецион бошқариш, мандатли бошқариш, кўп даражали муҳофаза.

Концепция защиты информации

uz - axborotni muhofaza qilish konsepsiyasi
ахборотни муҳофаза қилиш концепцияси
en - information security concept

Концепция монитора ссылок

uz - havolalar monitori konsepsiyasi
ҳаволалар монитори концепцияси
en - reference monitor concept

Концепция обеспечения информационной безопасности

uz - axborot xavfsizligini ta'minlash konsepsiyasi
таъминлаш концепцияси
en - information security provision concept

Система взглядов и общих технических требований по защите информации.

Axborotni muhofaza qilish bo'yicha qarashlar va umumiy texnik talablar tizimi.

Ахборотни муҳофаза қилиш бўйича қарашлар ва умумий техник талаблар тизими.

Концепция контроля доступа, базирующаяся на понятии абстрактной машины, разделяющей все попытки доступа субъектов к объектам. Находит практическую реализацию в виде ядра безопасности.

Subyektlarning obektlardan erkin foydalanish yo'lidagi barcha urinishlarini taqsimlovchi abstrakt mashina tushunchasiga asoslangan, erkin foydalanishni nazorat qilish konsepsiyasi. Xavfsizlik yadrosi ko'rinishida amalga oshiriladi.

Субъектларнинг объектлардан эркин фойдаланиш йўлидаги барча уринишларини тақсимловчи абстракт машина тушунчасига асосланган, эркин фойдаланишни назорат қилиш концепцияси. Хавфсизлик ядроси кўринишида амалга оширилади.

Документ, определяющий общую систему взглядов на проблему обеспечения информационной безопасности в автоматизированной системе обработки информации и путях ее решения с учетом накопленного опыта и современных тенденций ее развития. Концепция обеспечения информационной безопасности является составной частью концепции безопасности организации.

К

Axborotni qayta ishlash avtomatlashtirilgan tizimida axborot xavfsizligini ta'minlash muammosiga, uni to'plangan tajriba va rivojlanishining zamonaviy tendensiyalarini hisobga olgan holda hal qilish yo'llariga qarashlarning umumiy tizimini belgilovchi hujjat. Axborot xavfsizligini ta'minlash konsepsiyasi tashkilot xavfsizligi konsepsiyasining tarkibiy qismi hisoblanadi.

Ахборотни қайта ишлаш автоматлаштирилган тизимида ахборот хавфсизлигини таъминлаш муаммосига, уни тўпланган тажриба ва ривожланишининг замонавий тенденцияларини ҳисобга олган ҳолда ҳал қилиш йўлларига қарашларнинг умумий тизимини белгиловчи ҳужжат. Ахборот хавфсизлигини таъминлаш концепцияси ташкилот хавфсизлиги концепциясининг таркибий қисми ҳисобланади.

Копировщик побитовый

uz - bitma-bit nusxa

ko'chiruvchi

битма-бит нусха

кўчирувчи

en - bit copier

Программа, предназначенная для побитового считывания информации с дисков.

Axborotni disklardan bitma-bit o'qish uchun mo'ljallangan dastur.

Ахборотни дисклардан битма-бит ўқиш учун мўлжалланган дастур.

Корреляция взвешенная

uz - baholangan korrelyatsiya

баҳоланган корреляция

en - enhanced correlation

Метод анализа данных, применяемый к последовательности данных в различных программах с целью надежного отделения от фоновой корреляции.

Ma'lumotlarni tahlil qilish metodi, turli dasturlarda fonli korrelyatsiyadan ishonchli ajratish maqsadida, ma'lumotlar ketma-ketligiga nisbatan qo'llaniladi.

Маълумотларни таҳлил қилиш методи, турли дастурларда фонли корреляциядан ишончли ажратиш мақсадида, маълумотлар кетма-кетлигига нисбатан қўлланилади.

Коэффициент сжатия в источнике сообщений

uz - xabarlar manbaidagi

zichlash koeffitsiyenti

Отношение длин сообщения до и после его сжатого кодирования.

Xabarlar uzunligining, uni zichlab kodlashdan

К

хабарлар манбаидаги
зичлаш коэффициенти
en - source compressing factor

**Коэффициент экранирова-
ния технического средства
обработки информации**

uz - axborotni qayta ishlash
texnik vositasini ekranlash
koeffitsiyenti

ахборотни қайта ишлаш
техник воситасини экранлаш
коэффициенти

en - information processing
hardware screening factor

oldingi va keyingi nisbati.

Хабарлар узунлигининг, уни зичлаб кодлашдан олдинги ва кейинги нисбати.

1 Степень ослабления воздействия внешних электромагнитных излучений на электронные элементы технического средства обработки информации через электромагнитное поле за счет соответствующего выбора базовых несущих конструкций и применения других аппаратных способов защиты.

2 Степень ослабления воздействия внешних электромагнитных излучений на электронные элементы технического средства обработки информации через проводящие коммуникации, гальванически подключаемые к техническому средству.

1 Bazaviy tutib turuvchi konstruksiyalarni tegish-
licha tanlash va muhofaza qilishning boshqa apparat
usullarini qo'llash hisobiga, elektromagnit maydon
orqali axborotni qayta ishlash texnik vositalarining
elektron elementlariga qaratilgan tashqi elektromag-
nit nurlanishlar ta'sirini pasaytirish darajasi.

2 Texnik vositalarga galvanik ulanadigan o'tkazuv-
chi kommunikatsiyalar orqali axborotni qayta ishlash
texnik vositalarining elektron elementiga qaratilgan
tashqi elektromagnit nurlanishlar ta'sirini pasaytirish
darajasi.

1 Базавий тутиб турувчи конструкцияларни тегишлича танлаш ва муҳофаза қилишнинг бошқа аппарат усулларини қўллаш ҳисобига, электромагнит майдон орқали ахборотни қайта ишлаш техник воситаларининг электрон элементларига қаратилган ташқи электромагнит нурланишлар таъсирини пасайтириш даражаси.

2 Техник воситаларга гальваник уланадиган ўтказувчи коммуникациялар орқали ахборотни қайта ишлаш техник воситаларининг электрон элементига қаратилган ташқи электромагнит нурланишлар таъсирини пасайтириш даражаси.

К

Кракер

uz - kraker

кракер

en - craker

Разновидность хакеров, специализирующихся в области прикладного программного обеспечения. Деятельность кракеров обычно преследует корыстные цели и связана с несанкционированным доступом к «чужой» информации, в том числе и конфиденциальной.

Amaliy dasturiy ta'minot sohasida ixtisoslashgan hakerlarning bir turi. Krakerlarning faoliyati odatda, g'arazli maqsadlarga yo'naltirilgan va «begona» axborotdan, jumladan, konfidensial axborotdan ruxsat etilmagan tarzda foydalanish bilan bog'liq.

Амалий дастурий таъминот соҳасида ихтисослашган хакерларнинг бир тури. Кракерларнинг фаолияти одатда, ғаразли мақсадларга йўналтирилган ва «бегона» ахборотдан, жумладан, конфиденциал ахборотдан рухсат этилмаган тарзда фойдаланиш билан боғлиқ.

Крекинг

uz - kreking

крекинг

en - cracking

Акт проникновения в компьютерную систему или сеть.

Компьютер tizimiga yoki tarmoqqa suqulib kirish harakati.

Компьютер тизимиға ёки тармоққа суқулиб кириш ҳаракати.

Криптоалгоритм

uz - kriptoalgoritm

криптоалгоритм

en - cryptalgorithm

Алгоритм, с помощью которого осуществляется логическое преобразование исходного сообщения (открытого текста) в зашифрованную последовательность знаков.

Algoritm, uning yordamida dastlabki xabar (ochiq matn)ni belgilarning shifrlangan ketma-ketligiga mantiqiy qayta o'zgartirish amalga oshiriladi.

Алгоритм, унинг ёрдамида дастлабки хабар (очик матн)ни белгиларнинг шифрланган кетма-кетлигига мантиқий қайта ўзгартириш амалга оширилади.

К

Криптоанализ

uz - kriptotahlil

криптотахлил

en - cryptanalysis

1 Анализ криптографической системы и/или ее входов и выходов с целью получения чувствительной информации, включая открытый текст.

2 Наука о методах раскрытия и/или подделки данных.

3 Изучение системы защиты сообщений и/или исследование ее входных и выходных сообщений с целью выделить скрытые переменные или истинные данные, включая исходный текст.

1 Ta'sirchan axborotni, jumladan, ochiq matnni olish maqsadida, kriptografik tizimni va/yoki uning kirishlari hamda chiqishlarini tahlil qilish.

2 Ma'lumotlarni ochish va/yoki qalbakilashtirish metodlari haqidagi fan.

3 Yashirin o'zgaruvchan yoki haqiqiy ma'lumotlarni, jumladan, dastlabki matnni ajratish maqsadida xabarlarini muhofaza qilish tizimini o'rganish va/yoki uning kirish va chiqish xabarlarini tekshirish.

1 Ta'sirchan axborotni, jumladan, ochiq matnni olish maqsadida, kriptografik tizimni va/ёки uning kirishlari hamda chiqishlarini tahlil qilish.

2 Ma'lumotlarni ochish va/ёки qalbakilashtirish metodlari haqidagi fan.

3 Yashirin ўzgaruvchan ёки haqiqiy ma'lumotlarni, jumladan, dastlabki matnni ajratish maqsadida xabarlarini muhofaza qilish tizimini o'rganish va/ёки uning kirish va chiqish xabarlarini tekshirish.

Криптоанализ

дифференциальный

uz - differensial

kriptotahlil

дифференциал

криптотахлил

en - differential cryptanalysis

Метод криптоанализа, который может применяться для повторяющихся блочных шифров. Данный метод криптоанализа базируется на методе криптоанализа по выбранному открытому тексту и анализирует отличия между двумя открытыми текстами, зашифрованными на одном ключе. Каждому из возможных ключей назначается вероятность его «правильности» и в конечном счете вычисляется используемый ключ.

Takrorlanuvchi blokli shifrlar uchun qo'llaniladigan

К

kriptotahlil metodi. Bu kriptotahlil metodi tanlangan ochiq matn bo'yicha kriptotahlil metodiga asoslanadi va bir kalitda shifrlangan ikki ochiq matn o'rtasidagi farqni tahlil qiladi. Mumkin bo'lgan kalitlarning har biriga uning «to'g'riligi» ehtimoli belgilanadi va pirovardida foydalaniladigan kalit hisoblab chiqariladi.

Такрорланувчи блокли шифрлар учун қўлланиладиган криптоаҳлил методи. Бу криптоаҳлил методи танланган очик матн бўйича криптоаҳлил методига асосланади ва бир калитда шифрланган икки очик матн ўртасидаги фарқни таҳлил қилади. Мумкин бўлган калитларнинг ҳар бирига унинг «тўғрилиги» эҳтимоли белгиланади ва пировардида фойдаланиладиган калит ҳисоблаб чиқарилади.

Криптоанализ линейный

uz - chiziqli kriptotahlil

чизикли криптоаҳлил

en - linear cryptanalysis

Метод криптоанализа, который может применяться для блочных шифров. Данный метод криптоанализа базируется на методе криптоанализа по известному открытому тексту.

Blokli shifrlar uchun qo'llanilishi mumkin bo'lgan kriptotahlil metodi. Bu kriptotahlil metodi ma'lum ochiq matn bo'yicha kriptotahlil metodiga asoslanadi.

Блокли шифрлар учун қўлланилиши мумкин бўлган криптоаҳлил методи. Бу криптоаҳлил методи маълум очик матн бўйича криптоаҳлил методига асосланади.

Криптографическая стойкость

uz - kriptografik

bardoshlilik

криптографик

бардошлилик

en - cryptostrength

1 Характеристика шифра, определяющая его стойкость к расшифровке информации без знания ключа.

2 Свойство криптографической системы, характеризующее ее способность противостоять атакам злоумышленника, как правило, с целью получить ключ, открытое сообщение или навязать ложное сообщение.

3. Устойчивость криптографического алгоритма к его криптоанализу.

1 Shifrning, kalitni bilmasdan turib axborotni ras-

К

shifrovka qilishga bardoshlilikini belgilovchi xarakteristikasi.

2 Kriptografik tizimning, jinoyatkorning kalitni, ochiq xabarni olish yoki yolgʻon xabarni kiritish maqsadida qiladigan hujumlariga qarshi tura olish qobiliyatini tavsiflovchi xossasi.

3 Kriptografik algoritmning kriptotahlilga bardoshlilikigi.

1 Шифрнинг, калитни билмасдан туриб ахборотни расшифровка қилишга бардошлилигини белгиловчи характеристикаси.

2 Криптографик тизимнинг, жинояткорнинг калитни, очик хабарни олиш ёки ёлгон хабарни киритиш мақсадида қиладиган ҳужумларига қарши тура олиш қобилиятини тавсифловчи хоссаси.

3 Криптографик алгоритмнинг кriptотahlilga бардошлилиги.

Криптография

uz - kriptografiya

криптография

en - cryptography

1 Дисциплина, охватывающая принципы, средства и методы преобразования данных для сокрытия их семантического содержания, предотвращения их несанкционированного использования или необнаруживаемой модификации.

2 Наука о методах обеспечения секретности и/или подлинности данных при их передаче по каналам телекоммуникаций или хранения.

3 Принципы, средства и методы преобразования информации к непонятному виду, а также восстановления информации к виду, пригодному для восприятия.

1 Ma'lumotlarning semantik mazmunini yashirish, ulardan ruxsat etilmagan tarzda foydalanish yoki ularning aniqlab bo'lmaydigan o'zgartirilishini oldini olish maqsadida, ma'lumotlarni o'zgartirish prinsiplari, vositalari va metodlarini, qamrab oluvchi fan.

2 Ma'lumotlarni telekommunikatsiyalar kanallari orqali uzatishda yoki saqlashda, ularning maxfiyligi va/yoki haqiqiyiligini ta'minlash metodlari haqidagi fan.

3 Axborotni tushunarsiz ko'rinishga keltirish prin-

К

siplari, vositalari va metodlari, shuningdek, uni qabul qilish uchun yaroqli ko‘rinishga qayta tiklash.

1 Маълумотларнинг семантик мазмунини яшириш, улардан рухсат этилмаган тарзда фойдаланиш ёки уларнинг аниқлаб бўлмайдиган ўзгартирилишини олдини олиш мақсадида, маълумотларни ўзгартириш принциплари, воситалари ва методларини, қамраб олувчи фан.

2 Маълумотларни телекоммуникациялар каналлари орқали узатишда ёки сақлашда, уларнинг махфийлиги ва/ёки ҳақиқийлигини таъминлаш методлари ҳақидаги фан.

3 Ахборотни тушунарсиз кўринишга келтириш принциплари, воситалари ва методлари, шунингдек, уни қабул қилиш учун яроқли кўринишга қайта тиклаш.

Криптография многоуровневая

uz - ko‘p darajali
kriptografiya

кўп даражали
криптография

en - multilevel cryptography

Механизм, который заключается в специальном методе построения криптографических ключей для симметричных криптосистем. Криптосистема, реализующая данный механизм, устроена так, что первый криптографический ключ может быть выбран произвольно, в то время как выбор всех последующих ключей должен подчиняться определенному закону.

Simmetrik kriptotizimlar uchun kriptografik kalitlarni tuzishning maxsus metodidan iborat mexanizm. Ushbu mexanizmni amalga oshiruvchi kriptotizim, keyingi kalitlarning barchasini tanlash ma'lum qonunga bo'ysunishi kerak bo'lgan vaqtda birinchi kriptografik kalit ixtiyoriy tanlanishi mumkin bo'lgan tarzda, tuzilgan.

Симметрик криптотизимлар учун криптографик калитларни тузишнинг махсус методидан иборат механизм. Ушбу механизмни амалга оширувчи криптотизим, кейинги калитларнинг барчасини танлаш маълум қонунга бўйсунishi керак бўлган вақтда биринчи криптографик калит ихтиёрий танланиши мумкин бўлган тарзда, тузилган.

К

Криптография квантовая

uz - kvant kriptografiyasi

квант криптографияси

en - quantum cryptography

Криптографический механизм, заключающийся в использовании принципов квантовой физики. Для передачи сообщений используются фотоны, что позволяет гарантировать невозможность со стороны криптоаналитика модификации информации или нарушения процесса ее передачи. В настоящий момент практического применения квантовая криптография не имеет; используется только в качестве эксперимента.

Kvant fizikasi prinsiplaridan foydalanishga asoslangan kriptografik mexanizm. Xabarlarni uzatish uchun fotonlardan foydalaniladi, bu kriptoolitik tomonidan axborotni o'zgartirish yoki uni uzatish jarayonini buzish mumkin bo'lmashligini kafolatlaydi. Hozirgi vaqtda kvant kriptografiyasi qo'llanilmaydi; faqat eksperiment sifatida ishlatiladi.

Квант физикаси принципларидан фойдаланишга асосланган криптографик механизм. Хабарларни узатиш учун фотонлардан фойдаланилади, бу криптоаналитик томонидан ахборотни ўзгартириш ёки уни узатиш жараёнини бузиш мумкин бўлмаслигини кафолатлайди. Ҳозирги вақтда квант криптографияси қўлланилмайди; фақат эксперимент сифатида ишлатилади.

Криптография на эллиптических кривых

uz - elliptik egri chiziq

асосидаги кriptografiya

эллиптик эгри чизик

асосидаги криптография

en - elliptic-curve cryptography

Быстро развивающееся направление асимметричного шифрования и электронной цифровой подписи. Здесь все вычисления (например, выбор значения ключа) производятся над точками эллиптической кривой, т.е., например, вместо обычного сложения двух чисел выполняется по определённым правилам сложение двух точек кривой, при этом в качестве результата получается третья точка.

Asimmetrik shifrlash va elektron raqamli imzoning tez rivojlanib borayotgan yo'nalishi. Bunda barcha hisoblashlar (masalan, kalitning qiymatini tanlash) elliptik egri chiziq nuqtalari ustida amalga oshiriladi, ya'ni, masalan, ikkita sonni oddiy qo'shish o'rniga, ma'lum qoidalarga ko'ra egri chiziqning ikki nuqtasini qo'shish bajariladi, bunda natija sifatida uchinchi nuqta olinadi.

К

Асимметрик шифрлаш ва электрон рақамли имзонинг тез ривожланиб бораётган йўналиши. Бунда барча ҳисоблашлар (масалан, калитнинг қийматини танлаш) эллиптик эгри чизик нуқталари устида амалга оширилади, яъни, масалан, иккита сонни оддий қўшиш ўрнига, маълум коидаларга кўра эгри чизикнинг икки нуқтасини қўшиш бажарилади, бунда натижа сифатида учинчи нуқта олинади.

Криптография с открытым ключом

uz - ochiq kalitli

kriptografiya

очик калитли

криптография

en - public-key cryptography

1 Криптография, в которой для шифрования и дешифрования используется как открытый ключ, так и соответствующий ему личный ключ.

Примечание – Если открытый ключ используется для шифрования, то соответствующий ему личный ключ должен использоваться для дешифрования, и наоборот.

2 Метод шифрования, использующий пару ключей, один из которых является открытым, а второй – секретным.

1 Shifrlash va deshifrlash uchun ochiq kalit kabi, unga mos keladigan shaxsiy kalitdan foydalaniladigan kriptografiya.

Izoh – Agar ochiq kalit shifrlash uchun foydalanilsa, unga mos keladigan shaxsiy kalitdan deshifrlash uchun foydalaniladi, va aksincha.

2 Biri ochiq, ikkinchisi yopiq bo‘lgan juft kalitlardan foydalaniladigan shifrlash metodi.

1 Шифрлаш ва дешифрлаш учун очик калит каби, унга мос келадиган шахсий калитдан фойдаланиладиган криптография.

Изоҳ – Агар очик калит шифрлаш учун фойдаланилса, унга мос келадиган шахсий калитдан дешифрлаш учун фойдаланилади, ва аксинча.

2 Бири очик, иккинчиси ёпиқ бўлган жуфт калитлардан фойдаланиладиган шифрлаш методи.

Криптография симметричная

uz - simmetrik kriptografiya

симметрик криптография

en - symmetric cryptography

Криптография, в которой для шифрования и дешифрования используется один и тот же ключ.

Shifrlash va deshifrlash uchun bitta kalitdan foydalaniladigan kriptografiya.

Шифрлаш ва дешифрлаш учун битта калитдан фойдаланиладиган криптография.

К

Криптология
uz - kriptologiya
криптология
en - cryptology

Наука о создании и анализе систем безопасного хранения и передаче информации по каналам связи. Криптологию принято делить на две части – криптографию и криптоанализ.

Axborotni xavfsiz saqlash va aloqa kanallari bo‘ylab uzatish tizimini yaratish hamda tahlil qilish haqidagi fan. Kriptologiya ikki qismga – kriptografiya va kriptotahlilga bo‘linadi.

Ахборотни хавфсиз сақлаш ва алоқа каналлари бўйлаб узатиш тизимини яратиш ҳамда таҳлил қилиш ҳақидаги фан. Криптология икки қисмга – криптография ва криптоаҳлилга бўлинади.

Криптосистема
uz - kriptotizim
криптотизим
en - cryptosystem

1 Совокупность используемых документов, устройств, оборудования и методов, обеспечивающая шифрование или дешифрование.

2 Совокупность организационных, технических и программных средств, обеспечивающих криптографическое преобразование информации и/или управление, в том числе автоматизированное, процессом изготовления и распределения криптографических ключей.

1 Shifrlash yoki deshifrlashni ta'minlashda foydalaniladigan hujjatlar, qurilmalar, uskunalar va metodlar jami.

2 Axborotning kriptografik o'zgartirilishini va/yoki kriptografik kalitlarni tayyorlash va taqsimlash jarayoni boshqarilishini, jumladan, avtomatlashtirilgan tarzda, ta'minlovchi tashkiliy, texnik va dasturiy vositalar jami.

1 Шифрлаш ёки дешифрлашни таъминлашда фойдаланиладиган ҳужжатлар, қурилмалар, ускуналар ва методлар жами.

2 Ахборотнинг криптографик ўзгартирилишини ва ёки криптографик калитларни тайёрлаш ва тақсимлаш жараёни бошқарилишини, жумладан, автоматлаштирилган тарзда, таъминловчи ташкилий, техник ва дастурий воситалар жами.

К

Криптосистема Габидулина
uz - Gabidulin kriptotizimi

Габидулин криптотизими

en - Gabidulin's cryptosystem

Криптосистема, основанная на кодах, исправляющих ошибки в ранговой метрике.

Rang (daraja) metrikasida xatolarni tuzatuvchi kodlarga asoslangan kriptotizim.

Ранг (даража) метрикасида хатоларни тuzатувчи кодларга асосланган криптотизим.

Криптосистема Крук
uz - Kruk kriptotizimi

Крук криптотизими

en - Crook's cryptosystem

Криптосистема, основанная на кодах, исправляющих ошибки. В ней устранены недостатки криптосистемы Мак Эллиса.

Xatolarni tuzatuvchi kodlarga asoslangan kriptotizim. Unda Mak Ellis kriptotizimining kamchiliklari bartaraf qilingan.

Хатоларни тuzатувчи кодларга асосланган криптотизим. Унда Мак Эллис криптотизимининг камчиликлари бартараф қилинган.

Криптосистема Мак Эллиса
uz - Mak Ellis kriptotizimi

Мак Эллис криптотизими

en - Mac Alice cryptosystem

Криптосистема, основанная на кодах, исправляющих ошибки. Ей присущи два недостатка: большая длина ключа и большая избыточность (длина шифротекста вдвое превышает длину сообщения).

Xatolarni tuzatuvchi kodlarga asoslangan kriptotizim. Uning o'ziga xos ikki kamchiligi bor: kalit uzunligining katta bo'lishi va katta ortiqchalik (shifrmatn uzunligi xabar uzunligidan ikki marta oshadi).

Хатоларни тuzатувчи кодларга асосланган криптотизим. Унинг ўзига хос икки камчилиги бор: калит узунлигининг катта бўлиши ва катта ортиқчалик (шифрматн узунлиги хабар узунлигидан икки марта ошади).

Криптосистема
Нидеррайтера

uz - Niderrayter kriptotizimi

Нидеррайтер

криптотизими

en - Nidderrighter's cryptosystem

Криптосистема, основанная на кодах, исправляющих ошибки.

Xatolarni tuzatuvchi kodlarga asoslangan kriptotizim.

Хатоларни тuzатувчи кодларга асосланган криптотизим.

К

Криптосистема потоковая самосинхронизирующаяся

uz - oʻz-oʻzidan sinxronlanuvchi oqimli kriptotizim

ўз-ўзидан синхронланувчи оқимли криптотизим
en - data-flow selfsynchronizing cryptosystem

Потоковая криптосистема, характеризуемая тем, что каждый знак ключевого потока в любой момент времени определяется фиксированным числом предшествующих знаков шифротекста.

Kalit oqimining har bir belgisi vaqtning istalgan onida shifratn oldingi belgilarining qayd qilingan soni orqali aniqlanishi bilan tavsiflanadigan oqimli kriptotizim.

Калит оқимининг ҳар бир белгиси вақтнинг исталган онда шифрматн олдинги белгиларининг қайд қилинган сони орқали аниқланиши билан тавсифланадиган оқимли криптотизим.

Криптосистема потоковая синхронизирующаяся

uz - sinxronlanuvchi oqimli kriptotizim

синхронланувчи оқимли криптотизим
en - data-flow synchronizing cryptosystem

Потоковая криптосистема, в которой ключевой поток вырабатывается независимо от открытого текста и шифротекста. Если какой-либо символ шифротекста потерян при передаче, то получатель должен пересинхронизировать свой ключевой поток, отбросив соответствующий символ ключевого потока для правильного расшифрования последующих знаков шифротекста.

Kalit oqimi ochiq matn va shifratnga bogʻliq boʻlmagan tarzda ishlab chiqiladigan oqim kriptotizimi. Shifratnning biror-bir simvoli uzatishda yoʻqolgan boʻlsa, oluvchi shifr matnning keyingi belgilarini toʻgʻri rasshifrovka qilish uchun, kalit oqimining tegishli simvolini olib tashlab, oʻzining kalit oqimini qayta sinxronlashi kerak.

Калит оқими очик матн ва шифрматнга боғлиқ бўлмаган тарзда ишлаб чиқиладиган оқим криптотизими. Шифрматннинг бирор-бир симболи узатишда йўқолган бўлса, олувчи шифр матннинг кейинги белгиларини тўғри расшифровка қилиш учун, калит оқимининг тегишли символини олиб ташлаб, ўзининг калит оқимини қайта синхронлаши керак.

К

Криптосистема с эллиптическими кривыми

uz - elliptik egri chiziqli kriptotizim

эллиптик эгри чизиқли крiптотизим

en - cryptosystem with elliptic curve

Криптосистема с временным раскрытием
uz - vaqtga qarab ochiladigan kriptotizim

вақтга қараб очиладиган крiптотизим

en - cryptosystem with temporary disclosure

Криптосистема, основанная на математическом аппарате эллиптических кривых из теории чисел.

Sonlar nazariyasidan olingan elliptik egri chiziqning matematik apparatiga asoslangan kriptotizim.

Сонлар назариясидан олинган эллиптик эгри чизиқларнинг математик аппаратига асосланган крiптотизим.

Криптографическая система, которая позволяет расшифровать защищенное сообщение только по истечении заданного интервала времени. В настоящий момент существует два варианта реализации таких систем:

- шарады с временным замком;
- использование доверенных агентов, принимающих на себя обязательства не раскрывать информацию в течение заданного интервала времени.

В случае использования агентов возникает проблема доверия к ним, которая может быть частично решена за счет применения механизма разделения секретов.

Faqat berilgan vaqt intervali tugagandan soʻng muhofazalangan axborotni rasshifrovka qilish imkonini beradigan kriptografik tizim. Hozirgi vaqtda bunday tizimlarni amalga oshirishning ikkita varianti mavjud:

- vaqtinchalik qulflovchi sharadalar;
- berilgan vaqt intervali mobaynida axborotni ochmaslik majburiyatini zimmasiga olgan ishonchli agentlardan foydalanish. Agentlardan foydalanishga toʻgʻri kelganda ularga nisbatan ishonch muammosi yuzaga keladi, buni sirlarni taqsimlash mexanizmini qoʻllash hisobiga qisman hal qilish mumkin.

Фақат берилган вақт интервали тугагандан сўнг муҳофазаланган ахборотни расшифровка қилиш имконини берадиган криптографик тизим. Ҳозирги вақтда бундай тизимларни амалга оширишнинг иккита варианты мавжуд:

К

– вақтинчалик кулфловчи шарадалар;
– берилган вақт интервали мобайнида ахборотни очмаслик мажбуриятини зиммасига олган ишончли агентлардан фойдаланиш. Агентлардан фойдаланишга тўғри келганда уларга нисбатан ишонч муаммоси юзага келади, буни сирларни тақсимлаш механизмини қўллаш ҳисобига қисман ҳал қилиш мумкин.

Криптосистема с открытым ключом

uz - ochiq kalitli

kriptotizim

очик калитли

криптотизим

en - public key cryptosystem

Криптографическая система, в которой используется два ключа: секретный и открытый, причем ни один из ключей не может быть вычислен из другого за приемлемое время. Секретный ключ должен содержаться в тайне, в то время как открытый ключ может быть разослан всем абонентам, с которыми осуществляется взаимодействие. Такие криптосистемы, также называются двухключевыми и асимметричными. Одним из основных применений таких систем является управление ключами и создание электронной цифровой подписи.

Ikkita – maxfiy va ochiq kalitdan foydalaniladigan kriptografik tizim. Shuni hisobga olish kerakki, kalitlarning birortasi ham, maqbul vaqt ichida boshqasidan hisoblab chiqarilishi mumkin emas. Maxfiy kalit sir saqlanishi kerak, ochiq kalit o‘zaro hamkorlik qilinadigan barcha abonentlarga yuborilishi mumkin. Bunday kriptotizimlar, shuningdek, ikki kalitli va asimmetrik kriptotizimlar deb ham nomlanadi. Bunday tizimlar kalitlarni boshqarishda va elektron raqamli imzoni yaratishda qo‘llaniladi.

Иккита – махфий ва очик калитдан фойдаланиладиган криптографик тизим. Шунингдек, калитларнинг бирортаси ҳам, мақбул вақт ичида бoshқасидан ҳисоблаб чиқарилиши мумкин эмас. Махфий калит сир сақланиши керак, очик калит ўзаро ҳамкорлик қилинадиган барча абонентларга юборилиши мумкин. Бундай криптотизимлар, шунингдек, икки калитли ва асимметрик криптотизимлар деб ҳам номланadi. Бундай тизимлар калитларни бoshқаришда ва электрон рақамли имзони яратишда қўлланилади.

К

Криптосистема с секретным ключом

uz - maxfiy kalitli kriptotizim

махфий калитли кriptотизим

en - private key cryptosystem

Криптографическая система, в которой один и тот же криптографический ключ используется для зашифрования и расшифрования информации. Такие криптосистемы также называются одноключевыми, симметричными, обычными, двусторонними или классическими. Криптографические системы с секретным ключом делятся на блочные и поточные криптосистемы.

Kriptografik tizim, bunda aynan bitta kriptografik kalitdan axborotni shifrlash va rasshifrovka qilish uchun foydalaniladi. Bunday kriptotizimlar bir kalitli, simmetrik, oddiy, ikki tomonlama yoki klassik deb ham ataladi. Maxfiy kalitli kriptografik tizimlar blokli va oqimli kriptotizimlarga bo‘linadi.

Криптографик тизим, бунда айнан битта криптографик калитдан ахборотни шифрлаш ва расшифровка қилиш учун фойдаланилади. Бундай кriptотизимлар бир калитли, симметрик, оддий, икки томонлама ёки классик деб ҳам аталади. Махфий калитли криптографик тизимлар блокли ва оқимли кriptотизимларга бўлинади.

Критерии аудита

uz - audit kriteriyalari

аудит критерийлари

en - audit criteria

Совокупность политик, процедур или требований.

Примечание – Критерии аудита используются в качестве ориентира, с которым сравниваются свидетельства аудита.

Ҳо‘ллар, protseduralar yoki talablar yig‘indisi.

Izoh – Audit kriteriyalaridan audit dalillari solishtiriladigan orientir sifatida foydalaniladi.

Йўллар, процедуралар ёки талаблар йиғиндиси.

Изоҳ – Аудит критерийларидан аудит далиллари солиштирилладиган ориентир сифатида фойдаланилади.

Критерии приемки

uz - qabul qilib olish kriteriyalari

қабул қилиб олиш критерийлари

en - acceptance criteria

Критерии, применяемые при выполнении процедур приемки (например, успешный просмотр документации или успешное тестирование программного обеспечения, программно-аппаратных или аппаратных средств).

Qabul qilib olish protsedurasini bajarishda qo‘llaniladigan kriteriyalar (masalan, hujjatlarni muvaffaqiyatli

К

ko‘rib chiqish yoki dasturiy ta‘minotni, dasturiy apparat vositalarini muvaffaqiyatli testlash).

Қабул қилиб олиш процедурасини бажаришда қўлланиладиган критерийлар (масалан, ҳужжатларни муваффақиятли кўриб чиқиш ёки дастурий таъминотни, дастурий-аппарат ёки аппарат воситаларини муваффақиятли тестлаш).

Критерии принятия решений

uz - qarorlar qabul qilish kriteriyalari

қарорлар қабул қилиш критерийлари

en - decision criteria

Пороговые и заданные величины или эталоны, используемые для определения потребности в деятельности или дальнейшем исследовании, или для описания уровня достоверности данного результата.

Ishda yoki keyingi tadqiqotdagi ehtiyojni aniqlash yoki ushbu natija ishonchlilik darajasini tavsiflash uchun ishlatiladigan chegaraviy va berilgan kattaliklar yoki etalonlar.

Ишда ёки кейинги тадқиқотдаги эҳтиёжни аниқлаш ёки ушбу натижа ишончлилиқ даражасини тавсифлаш учун ишлатиладиган чегаравий ва берилган катталиқлар ёки эталонлар.

Критерии риска

uz - risk kriteriyalari

риск критерийлари

en - risk criteria

Признаки, по которым оценивают значимость риска.

Примечания

1 Критерии риска основываются на целях организации, а также на внешней и внутренней ситуации.

2 Критерии риска могут быть взяты из стандартов, законов, политик и других требований.

Riskning ahamiyatini baholaydigan belgilar.

Изоҳлар

1 Risk kriteriyalari tashkilot maqsadlariga, shuningdek, ichki va tashqi vaziyatlarga asoslanadi.

2 Risk kriteriyalari standartlar, qonunlar, siyosatlar va boshqa talablardan olinishi mumkin.

Рискнинг аҳамиятини баҳолайдиган белгилар.

Изоҳлар

1 Риск критерийлари ташкилот мақсадларига, шунингдек, ички ва ташқи вазиятларга асосланади.

2 Риск критерийлари стандартлар, қонунлар, сиёсатлар ва бошқа талаблардан олинishi мумкин.

К

Критичность

uz - kritiklik

критиклик

en - criticality, criticalness

1 Требования к достаточности определенной информации или ресурсов, обрабатывающих информацию, для ведения дел.

2 Характеристика ресурса, которая косвенно выражает его значение или важность.

1 Ishlarni yuritish uchun, muayyan axborot yoki axbotni qayta ishlovchi resurslarning yetarliligiga qo'yiladigan talablar.

2 Resursning, uning ahamiyatini yoki muhimligini bilvosita ifodalaydigan xarakteristikasi.

1 Ishlarni yuritish uchun, muayyan axborot yoki axbotni qayta ishlovchi resurslarning yetarliligiga qo'yiladigan talablar.

2 Resursning, uning ahamiyatini yoki muhimligini bilvosita ifodalaydigan xarakteristikasi.

Кэширование паролей

uz - parollarni keshlash

паролларни кэшлаш

en - password caching

Хранение паролей и других сведений о пользователе на локальном компьютере.

Lokal kompyuterda parollarni va foydalanuvchi haqidagi boshqa ma'lumotlarni saqlash.

Локал компьютерда паролларни ва фойдаланувчи хақидаги бошқа маълумотларни сақлаш.

Л

«Лечение» вируса

uz - virusni «davolash»

вирусни «даволаш»

en - virus treatment

Процесс удаления вируса из зараженного им объекта и восстановления состояния этого объекта (файла, загрузочной части диска и т.д.), существовавшего до заражения вирусом.

Zararlangan obyektдан virusni chiqarib tashlash va bu obyektning (faylning, disk yuklanadigan qismining) virus bilan zararlanguga qadar bo'lgan holatini tiklash jarayoni.

Zararlangan obyektдан virusni chiqarib tashlash va bu obyektning (faylning, disk yuklanadigan qismining) virus bilan zararlanguga qadar bo'lgan holatini tiklash jarayoni.

Лицензиар в области защиты информации
uz - axborotni muhofaza qilish sohasidagi litsenziar

ахборотни муҳофаза қилиш соҳасидаги лицензиар
en - licensor in the information protection field

Лицензиат в области защиты информации
uz - axborotni muhofaza qilish sohasidagi litsenziat

ахборотни муҳофаза қилиш соҳасидаги лицензиат
en - licensee in the information protection field

Лицензирование
uz - litsenziyalash
лицензиялаш
en - licensing

Лицензирование в области защиты информации
uz - axborotni muhofaza qilish sohasida litsenziyalash
ахборотни муҳофаза қилиш соҳасида лицензиялаш
en - licensing in the information protection field

Сторона в лицензионном соглашении, передающая право на проведение работ в области защиты информации.

Litsenziya kelishuvidagi, axborotni muhofaza qilish sohasida ishlarni olib borish huquqini beradigan tomon.

Лицензия келишувидаги, ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини берадиган томон.

Сторона в лицензионном соглашении, получившая право на проведение работ в области защиты информации.

Litsenziya kelishuvidagi, axborotni muhofaza qilish sohasida ishlarni olib borish huquqini oladigan tomon.

Лицензия келишувидаги, ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини оладиган томон.

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации.

Axborotni muhofaza qilish sohasida ishlarni olib borish huquqini berish yoki olishdan iborat faoliyat.

Ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини бериш ёки олишдан иборат фаолият.

Деятельность, заключающаяся в передаче или получении прав на проведение работ в области защиты информации, оформленная лицензионным соглашением (договором), и осуществлении контроля за лицензиатом.

Litsenziya kelishuvi (shartnomasi) bilan rasmiylashtirilgan, axborotni muhofaza qilish sohasida ishlarni olib borish huquqini berish yoki olishda, litsenziat ustidan nazoratni amalga oshirishda ifodalanadigan faoliyat.

Лицензия келишуви (шартномаси) билан расмийлаштирилган, ахборотни муҳофаза қилиш соҳасида ишларни олиб бориш ҳуқуқини бериш ёки олишда, лицензиат устидан назоратни амалга оширишда ифодаланадиган фаолият.

Лицензирование

обязательное

uz - majburiy litsenziyalash

мажбурий лицензиялаш

en - compulsory licence

Юридическое постановление, которое требует от любого лица получить лицензию на определенный срок независимо от того, желает или нет лицо, выдающее лицензии, предоставить ее.

Har bir shaxsdan, litsenziyani beradigan shaxs uni taqdim etishni xohlash yoki xohlamasligidan qat'i nazar, litsenziya olishni talab etadigan yuridik qaror.

Ҳар бир шахсдан, лицензияни берадиган шахс уни тақдим этишни хоҳлаш ёки хоҳламаслигидан қатъи назар, лицензия олишни талаб этадиган юридик қарор.

Лицензия

uz - litsenziya

лицензия

en - license

1 Разрешение, выдаваемое государственными органами, на право продажи или предоставления услуг.

2 Оформленный документ на право владение собственностью.

3 Оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

1 Davlat organlari tomonidan xizmatlarni sotish yoki taqdim etish huquqini beradigan ruxsat.

2 Mulkchilikka egalik qilish huquqini beradigan rasmiylashtirilgan hujjat.

3 Axborotni muhofaza qilish sohasida u yoki bu ishlarni olib borish huquqi uchun berilgan, tegishli ravishda rasmiylashtirilgan ruxsatnoma.

1 Давлат органлари томонидан хизматларни сотиш ёки тақдим этиш ҳуқуқини берадиган рухсат.

2 Мулкчиликка эгалик қилиш ҳуқуқини берадиган расмийлаштирилган ҳужжат.

3 Ахборотни муҳофаза қилиш соҳасида у ёки бу ишларни олиб бориш ҳуқуқи учун берилган, тегишли равишда расмийлаштирилган рухсатнома.

Лицензия свободная

uz - erkin litsenziya
эркин лицензия
en - free license

Открытая публикация программы в журнале, книге или частном сообщении, равносильная разрешению на использование.

Dasturning, foydalanish uchun ruxsatga teng kuchga ega jurnal, kitob yoki xususiy xabarda ochiq e'lon qilinishi.

Дастурнинг, фойдаланиш учун рухсатга тенг кучга эга журнал, китоб ёки хусусий хабарда очик эълон қилиниши.

Лицензия упакованная

uz - joylangan litsenziya
жойланган лицензия
en - shrink-wrap license

Лицензия на программный продукт, доступная для чтения и вступающая в силу при вскрытии упаковки программного продукта.

Dasturiy mahsulot uchun berilgan, o'qish uchun qulay bo'lgan va dasturiy mahsulot o'rami ochilganda kuchga kiradigan litsenziya.

Дастурий маҳсулот учун берилган, ўқиш учун қулай бўлган ва дастурий маҳсулот ўрами очилганда кучга кирадиган лицензия.

Лицензия установочная

uz - yo'l-yo'riq ko'rsatuvchi
litsenziya
йўл-йўриқ кўрсатувчи
лицензия
en - site license

Лицензия на множественное копирование программного средства.

Dasturiy vositadan ko'plab nusxa ko'chirish uchun beriladigan litsenziya.

Дастурий воситадан кўплаб нусха кўчириш учун бериладиган лицензия.

Ловушка

uz - tuzoq
тузоқ
en - honeypot, penetration
entraption

Программа, которая эмулирует работу определенных сервисов (почтовых, Telnet и т.п.) на компьютере, тщательно протоколирующем при этом любые действия злоумышленника.

Jinoyatkorning har qanday harakatini sinchiklab protokollashtiradigan kompyuterdagi ma'lum servislar (pochta, Telnet va sh.k.) ishini tezlashtiradigan dastur.

Жинояткорнинг ҳар қандай ҳаракатини синчиклаб протоколлаштирадиган компьютердаги маълум сервислар (почта, Telnet ва ш.к.) ишини тезлаштирадиган дастур.

Ловушка сброса

uz - chiqarib tashlash tuzog‘i
чиқариб ташлаш тузоғи
en - reset trapping

Программный способ отвести любую попытку прерывания штатной работы компьютера, чтобы избежать возврата управления пользователю.

Boshqaruvning foydalanuvchiga qaytishining oldini olish maqsadida, kompyuterning shtat rejimida ishlashini buzadigan har qanday urinishni yo‘qqa chiqarishning dasturiy usuli.

Boshqaruvning foydalanuvchiga qaytishining oldini olish maqsadida, kompyuterning shtat rejimida ishlashini buzadigan har qanday urinishni yo‘qqa chiqarishning dasturiy usuli.

Люк

uz - lyuk
люк
en - trapdoor

1 Скрытый программный или аппаратный механизм, обычно создаваемый для тестирования и поиска неисправностей, который позволяет обойти механизмы компьютерной безопасности.

2 Скрытая или недокументированная точка входа в автоматизированную систему. Может применяться для обхода системы защиты.

3 Блок, скрытый в большой программе, который разрешает пользователю преодолеть систему защиты или позволяет использовать ресурсы системы в штатном режиме.

1 Kompyuter xavfsizligi mexanizmlarini chetlab o‘tish imkonini beruvchi, asosan testlash va nosozliklarni izlab topish uchun yaratiladigan yashirin dasturiy yoki apparat mexanizm.

2 Avtomatlashtirilgan tizimga kirishning yashirin yoki hujjatlashtirilgan nuqtasi. Muhofaza tizimini chetlab o‘tishda qo‘llash mumkin.

3 Katta dasturga yashiringan, foydalanuvchiga muhofaza tizimidan o‘tishga ruxsat beradigan yoki tizim resurslaridan shtat rejimida foydalanish imkonini beradigan blok.

1 Kompyuter xavfsizligi mexanizmlarini chetlab o‘tish imkonini beruvchi, asosan testlash va nosozliklarni izlab topish uchun yaratiladigan yashirin dasturiy yoki apparat mexanizm.

2 Avtomatlashtirilgan tizimga kirishning yashirin yoki hujjatlashtirilgan nuqtasi. Muhofaza tizimini chetlab o‘tishda qo‘llash mumkin.

Люк эксплуатационный

uz - ekspluatatsion lyuk

эксплуатацион люк

en - maintenance hatch

3 Катта дастурга яширинган, фойдаланувчига муҳофаза тизимидан ўтишга рухсат берадиган ёки тизим ресурсларидан штат режимида фойдаланиш имконини берадиган блок.

Люк в программном обеспечении, который облегчает обслуживание, предоставляя дополнительные возможности для входа в программу в недокументированных точках или без обычных проверок.

Dasturiy ta'minotdagi lyuk, dasturga hujjatlashtiril-magan nuqtalardan yoki odatdagi tekshiruvlarsiz ki-rish uchun qo'shimcha imkoniyatlarni taqdim etgan holda, xizmat ko'rsatishni yengillashtiradi.

Дастурий таъминотдаги люк, дастурга хужжатлаштирилмаган нуқталардан ёки одатдаги текширувларсиз кириш учун қўшимча имкониятларни тақдим этган ҳолда, хизмат кўрсатишни енгиллаштиради.

М

Макровирус

uz - makrovirus

макровирус

en - macro-virus

Файловый вирус, существующий в виде макрокоманды для определенного приложения. При открытии зараженного файла вирус прикрепляет себя к приложению и заражает все файлы, к которым обращается программа.

Ma'lum bir ilova (dastur) uchun makrokomanda ko'rinishida mavjud bo'lgan fayl virusi. Zararlangan fayl ochilganda, virus ilovaga yopishib, dastur murojaat qiladigan barcha fayllarni zararlaydi.

Маълум бир илова (дастур) учун макрокоманда кўринишида мавжуд бўлган файл вирусини. Зарарланган файл очилганда, вирус иловага ёпишиб, дастур мурожаат қиладиган барча файлларни зарарлайди.

Мандат

uz - mandat

мандат

en - ticket, capability

1 Представление одного или нескольких прав на доступ к объекту.

Примечание – Мандат является разрешением на доступ.

2 Элемент матрицы доступа, определяющий тип

М

доступа определенного субъекта к определенному объекту. Каждый раз мандат выдается субъекту динамически – при запросе доступа. Поскольку распространение мандатов происходит очень динамично, и они могут размещаться непосредственно внутри объектов, то вследствие этого контроль за ним очень затруднен. В чистом виде этот механизм используется редко. Однако реализация других механизмов контроля доступа часто осуществляется с помощью мандатов.

3 Представимая форма полномочия, обладание которой подтверждает право на доступ к ресурсу системы.

4 Информация, передаваемая для подтверждения требуемой идентичности какого-либо объекта.

1 Obyektdan erkin foydalanish uchun bitta yoki bir nechta huquqlarni taqdim etish.

Izoh – Mandat erkin foydalanishga ruxsat berish hisoblanadi.

2 Ma'lum subyektning ma'lum obyektdan foydalanish turini belgilovchi, erkin foydalanish matritsasi elementi. Har safar mandat subyektga dinamik ravishda – erkin foydalanish so'ralganda beriladi. Mandatlarni tarqatish juda ham o'zgaruvchan tarzda yuz berishi sababli, ular bevosita obyektlar ichida joylashishi mumkin, buning oqibatida ularni nazorat qilish juda ham qiyin. Sof ko'rinishda bu mexanizmdan juda kam foydalaniladi. Biroq, erkin foydalanishni nazorat qilishning boshqa mexanizmlari ko'pincha mandatlar yordamida amalga oshiriladi.

3 Taqdim etiladigan vakolat shakli, unga egalik qilish tizim resursidan erkin foydalanish huquqini tasdiqlaydi.

4 Qandaydir obyektning talab etiladigan identikligini (o'xshashligini) tasdiqlash uchun uzatiladigan axborot.

1 Объектдан эркин фойдаланиш учун битта ёки бир нечта ҳуқуқларни тақдим этиш.

Изоҳ – Мандат эркин фойдаланишга рухсат бериш ҳисобланади.

2 Маълум субъектнинг маълум объектдан фойда-

М

ланиш турини белгиловчи, эркин фойдаланиш матрицаси элементи. Ҳар сафар мандат субъектга динамик равишда – эркин фойдаланиш сўралганда берилади. Мандатларни тарқатиш жуда ҳам ўзгарувчан тарзда юз бериши сабабли, улар бево-сита объектлар ичида жойлашиши мумкин, бу-нинг оқибатида уларни назорат қилиш жуда ҳам қийин. Соф кўринишда бу механизмдан жуда кам фойдаланилади. Бирок, эркин фойдаланишни назорат қилишнинг бошқа механизмлари кўпин-ча мандатлар ёрдамида амалга оширилади.

3 Тақдим этиладиган ваколат шакли, унга эгалик қилиш тизим ресурсидан эркин фойдаланиш ҳу-қуқини тасдиқлайди.

4 Қандайдир объектнинг талаб этиладиган иден-тиклигини (ўхшашлигини) тасдиқлаш учун уза-тиладиган ахборот.

Маркер

uz - marker

маркер

en - token

1 Электронный носитель содержания.

2 Короткий код для представления распознавае-мых слов, например, служебных слов языка, кон-стант и т.п.

1 Elektron mazmun tashuvchi.

2 Aniqlanadigan soʻzlarni, masalan, tilning xizmatga oid soʻzlarini, konstantalarni va sh.k., taqdim etish uchun moʻljallangan qisqa kod.

1 Электрон мазмун ташувчи.

2 Аниқланадиган сўзларни, масалан, тилнинг хизматга оид сўзларини, константаларни ва ш.к., тақдим этиш учун мўлжалланган қисқа код.

Маркер безопасности

uz - xavfsizlik markeri

хавфсизлик маркери

en - security token

Набор данных, передаваемых между объектами телекоммуникаций, который защищен одной или несколькими услугами безопасности, вместе с информацией безопасности, которая используется при их предоставлении.

Telekommunikatsiyalar obyektleri oʻrtasida uza-tiladigan, maʼlumotlarni taqdim etishda foy- dalaniladigan xavfsizlik axboroti bilan birga, bitta yoki bir nechta xavfsizlik xizmati tomonidan muhofazalangan, maʼlumotlar toʻplami.

М

Телекоммуникациялар объектлари ўртасида узатиладиган, маълумотларни такдим этишда фойдаланиладиган хавфсизлик ахбороти билан бирга, битта ёки бир нечта хавфсизлик хизмати томонидан муҳофазаланган, маълумотлар тўплами.

Маркер доступа

uz - foydalana olish markeri
фойдалана олиш маркери
en - access token

Структура данных, связанная с процессом и являющаяся его «пропуском» к ресурсам операционной системы. В частности, включает все идентификаторы безопасности запустившего процесс пользователя.

Jarayon bilan bog'liq va uning operatsion tizim resurslaridan foydalana olishi uchun «ruxsatnomasi» hisoblanadigan, ma'lumotlar strukturasi. Xususan, jarayonni ishga tushirgan foydalanuvchining barcha xavfsizlik identifikatorlarini o'z ichiga oladi.

Жараён билан боғлиқ ва унинг операцион тизим ресурсларидан фойдалана олиши учун «рухсатномаси» ҳисобланадиган, маълумотлар структураси. Хусусан, жараёни ишга туширган фойдаланувчининг барча хавфсизлик идентификаторларини ўз ичига олади.

Маркировка по времени

uz - vaqt bo'yicha belgi qo'yish
вақт бўйича белги қўйиш
en - time stamping

Метод защиты информации от ее замены или модификации в процессе передачи, основанный на включении в каждое сообщение временных меток, однозначно связанных с данными.

Axborotni uzatish jarayonida almashtirilish yoki o'zgartirilishdan muhofaza qilish metodi. Har bir xabarga ma'lumotlar bilan qat'iy bog'liq bo'lgan vaqtinchalik belgilarni kiritishga asoslanadi.

Ахборотни узатиш жараёнида алмаштирилиш ёки ўзгартирилишдан муҳофаза қилиш методи. Ҳар бир хабарга маълумотлар билан қатъий боғлиқ бўлган вақтинчалик белгиларни киритишга асосланади.

М

Маршрут доверенный

uz - ishonchli yoʻnalish
ишончли йўналиш
en - trusted path

Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую для этого степень уверенности.

Foydalanuvchi va OXF oʻrtasidagi, zarur boʻlgan qatʼiylik darajasini taʼminlaydigan birgalikda ishlash vositasi.

Фойдаланувчи ва ОXF ўртасидаги, зарур бўлган қатъийлик даражасини таъминлайдиган биргаликда ишлаш воситаси.

Маршрут достоверный

uz - ishonchli marshrut
ишончли маршрут
en - trusted path

Механизм, с помощью которого пользователь за терминалом может взаимодействовать непосредственно с ДВБ. Он может быть активизирован только пользователем или ДВБ, его работа не может быть прервана, имитирована или нарушена недостоверным программным обеспечением.

Foydalanuvchi terminaldan keyin ИВБ bilan, bevosita birgalikda ishlashi mumkin boʻlgan mexanizm. U faqat foydalanuvchi yoki ИВБ tomonidan aktivlashtirilishi mumkin, uning ishi ishonchsiz dasturiy taʼminot bilan toʻxtatilishi, imitatsiya qilinishi yoki buzilishi mumkin emas.

Фойдаланувчи терминалдан кейин ИХБ билан, бевосита биргаликда ишлаши мумкин бўлган механизм. У фақат фойдаланувчи ёки ИХБ томонидан активлаштирилиши мумкин, унинг иши ишончсиз дастурий таъминот билан тўхтатилиши, имитация қилиниши ёки бузилиши мумкин эмас.

Маска доступа

uz - foydalana olish niqobi
фойдалана олиш ниқоби
en - access mask

Двоичное число, отдельные биты которого соответствуют разным типам доступа.

Ayrim bitlari foydalana olishning har-xil turlariga mos keladigan ikkilik son.

Айрим битлари фойдалана олишнинг ҳар-хил турларига мос келадиган иккилик сон.

М

Маскарад

uz - maskarad

маскарад

en - masquerade

1 Попытка какого-либо логического объекта выдать себя за другой логический объект для получения несанкционированного доступа.

2 Попытка получить доступ к системе, объекту или выполнение других действий субъектом, не обладающим полномочиями на соответствующее действие и выдающим себя за другого, которому эти действия разрешены.

3 Попытка несанкционированного проникновения в сеть путем имитации работы какого-либо легитимного пользователя.

1 Ruxsat etilmagan tarzda foydalana olish uchun biror-bir mantiqiy obyektning o'zini boshqa mantiqiy obyekt qilib ko'rsatishga urinishi.

2 Tegishli harakatlarni amalga oshirishga vakolatlari bo'lmagan va o'zini bu harakatlar ruxsat berilgan boshqa shaxs qilib ko'rsatadigan subyekt tomonidan, tizimdan, obyektдан erkin foydalanishga urinish yoki boshqa harakatlarning bajarilishi.

3 Qandaydir qonuniy foydalanuvchining ishini imitatsiya qilish yo'li bilan tarmoqqa ruxsat etilmagan tarzda kirishga urinish.

1 Рухсат этилмаган тарзда фойдалана олиш учун бирор-бир мантикий объектнинг ўзини бошқа мантикий объект қилиб кўрсатишга уриниши.

2 Тегишли ҳаракатларни амалга оширишга ваколатлари бўлмаган ва ўзини бу ҳаракатлар рухсат берилган бошқа шахс қилиб кўрсатадиган субъект томонидан, тизимдан, объектдан эркин фойдаланишга уриниш ёки бошқа ҳаракатларнинг bajarilishi.

3 Қандайдир қонуний фойдаланувчининг ишини имитация қилиш йўли билан тармоққа рухсат этилмаган тарзда киришга уриниш.

Маскиратор

uz - maskirator

маскиратор

en - maskirator

Средство защиты информации, реализующее математический алгоритм преобразования информации, не использующее секретного ключа или передающее (хранящее) его вместе с сообщением.

Axborotni o'zgartirishning matematik algoritmini amalga oshiradigan, maxfiy kalitdan foydalanmaydi-

М

gan yoki uni xabar bilan birga uzatadigan (saqlaydigan) axborotni muhofaza qilish vositasi.

Ахборотни ўзгартиришнинг математик алгоритмини амалга оширадиган, махфий калитдан фойдаланмайдиган ёки уни хабар билан бирга узатадиган (сақлайдиган) ахборотни муҳофаза қилиш воситаси.

Маскировка

uz - niqoblash

ниқоблаш

en - masking

Метод защиты объектов, основанный на использовании действий, вследствие которых объект становится недоступным (скрытым) или труднодоступным для злоумышленников.

Obyektlarni muhofaza qilish metodi, obyektни jinoyatkorlar uchun egallab bo'lmaydigan (yashirin) yoki kirish qiyin bo'ladigan holatga olib keladigan harakatlardan foydalanishga asoslangan.

Объектларни муҳофаза қилиш методи, объектни жинояткорлар учун эгаллаб бўлмайдиган (яширин) ёки кириш қийин бўладиган ҳолатга олиб келадиган ҳаракатлардан фойдаланишга асосланган.

Матрица доступа

uz - foydalana olish

matritsasi

фойдалана олиш

матрицаси

en - access matrix

1 Таблица, отображающая правила разграничения доступа и предназначенная для описания свойств избирательного доступа. Представляет собой матрицу, в которой объекту системы соответствует столбец, а субъекту – строка. На пересечении столбца и строки матрицы указывается права доступа субъекта к объекту.

2 Таблица, отображающая правила доступа субъектов к информационным ресурсам, данные о которых хранятся в диспетчере доступа.

3 Системная структура данных, представленная в виде таблицы, столбцы которой помечены идентификаторами всех существующих в системе ресурсов, а строки – идентификаторами всех зарегистрированных в системе пользователей. На пересечении каждого столбца таблицы с каждой ее строкой администратором системы проставляется специальный указатель разрешенного конкретному пользователю типа доступа к данному объекту.

M

1 Erkin kira olishni cheklash huquqini aks ettiruvchi va tanlaydigan kirishning xususiyatlarini tasvirlash uchun mo'ljallangan jadval. Tizim obyektiga ustun, subyektiga esa, satr mos keladigan matritsani o'zida aks ettiradi. Matritsaning ustun va satrlari kesishgan joyda subyektning obyektidan erkin foydalanish huquqi ko'rsatiladi.

2 Subyektlarning axborot resurslaridan erkin foydalanish qoidalarini aks ettiradigan jadval.

3 Jadval ko'rinishida taqdim etilgan, ma'lumotlarning tizimli strukturasi. Jadvalning ustunlari tizimda mavjud bo'lgan barcha resurslarning identifikatorlari bilan, satrlar esa tizimda qayd etilgan barcha foydalanuvchilarning identifikatorlari bilan belgilangan. Jadval har bir ustunining har bir satr bilan kesishish joyida tizim ma'muri tomonidan berilgan obyektidan erkin foydalanish turining muayyan foydalanuvchiga ruxsat etilgan maxsus ko'rsatkichi qo'yiladi.

1 Эркин кира олишни чеклаш ҳуқуқини акс эттирувчи ва танлайдиган киришнинг хусусиятларини тасвирлаш учун мўлжалланган жадвал. Тизим объектига устун, субъектига эса, сатр мос келадиган матрицани ўзида акс эттиради. Матрицанинг устун ва сатрлари кесишган жойда субъектнинг объектдан эркин фойдаланиш ҳуқуқи кўрсатилади.

2 Субъектларнинг ахборот ресурсларидан эркин фойдаланиш қоидаларини акс эттирадиган жадвал.

3 Жадвал кўринишида тақдим этилган, маълумотларнинг тизимли структураси. Жадвалнинг устунлари тизимда мавжуд бўлган барча ресурсларнинг идентификаторлари билан, сатрлар эса тизимда қайд этилган барча фойдаланувчиларнинг идентификаторлари билан белгиланган. Жадвал ҳар бир устунининг ҳар бир сатр билан кесишиш жойида тизим маъмури томонидан берилган объектдан эркин фойдаланиш турининг муайян фойдаланувчига рухсат этилган махсус кўрсаткичи кўйилади.

М

Матрица полномочий

uz - vakolatlar matritsasi
ваколатлар матрицаси
en - privilege matrix

Таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно защищаемых данных.

Elementlari muayyan obyektning muhofaza qilinadigan ma'lumotlarga nisbatan huquqlarini (vakolatlarini, imtiyozlarini) belgilaydigan jadval.

Элементлари муайян объектнинг муҳофаза қилинадиган маълумотларга нисбатан ҳуқуқларини (ваколатларини, имтиёзларини) белгилайдиган жадвал.

Мера

uz - o'lchov
ўлчов
en - measure

Переменная, значение которой присваивается в процессе измерения.

Примечание – Термин «меры» используется для определения совокупности базовых и производных мер, а также индикаторов.

Qiymati o'lchash jarayonida beriladigan o'zgaruvchi. Izoh – «O'lchov» atamasidan bazaviy va hosila o'lchovlar, shuningdek, indikatorlar jamini aniqlash uchun foydalaniladi.

Қиймати ўлчаш жараёнида бериладиган ўзгарувчи.

Изоҳ – «Ўлчов» атамасидан базавий ва ҳосила ўлчовлар, шунингдек, индикаторлар жамини аниқлаш учун фойдаланилади.

Мера основная (базовая)

uz - asosiy (bazaviy) o'lchov
асосий (базавий) ўлчов
en - base measure

Мера, определенная в терминах атрибута и метода его количественного определения.

Примечание – Основная мера функционально независима от других мер.

Atribut va uni miqdoriy aniqlash usulining atamalarida belgilangan o'lchov.

Izoh – Asosiy o'lchov funksional jihatdan boshqa o'lchovlarga bog'liq bo'lmaydi.

Атрибут ва уни миқдорий аниқлаш усулининг атамаларида белгиланган ўлчов.

Изоҳ – Асосий ўлчов функционал жиҳатдан бошқа ўлчовларга боғлиқ бўлмайди.

М

Мера производная

uz - hosila o'Ichov

хосила ўлчов

en - derived measure

Мера, которая определяется как функция двух или более значений основных мер.

Asosiy o'Ichovlarning ikki yoki undan ortiq qiymatining funksiyasi sifatida aniqlanadigan o'Ichov.

Асосий ўлчовларнинг икки ёки ундан ортиқ қийматининг функцияси сифатида аниқланадиган ўлчов.

Мероприятие по защите информации

uz - axborotni muhofaza

qilish bo'yicha tadbir

ахборотни муҳофаза

қилиш бўйича тадбир

en - information protective

measures

Совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

Axborotni muhofaza qilish usullari va vositalarini ishlab chiqish va/yoki amaliy qo'llashga yo'naltirilgan harakatlar jami.

Ахборотни муҳофаза қилиш усуллари ва воситаларини ишлаб чиқиш ва/ёки амалий қўллашга йўналтирилган ҳаракатлар жами.

Меры защиты информации организационные

uz - axborotni muhofaza

qilishning tashkiliy

chora-tadbirlari

ахборотни муҳофаза

қилишнинг ташкилий

чора-тадбирлари

en - organizational information

protective measures

Меры, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Ma'lumotlarni qayta ishlash tizimining ishlash jarayonini, tizim resurslaridan foydalanishni, personal faoliyatini, shuningdek, foydalanuvchilarning tizim bilan o'zaro hamkorlik tartibini, tizimda aylanuvchi axborot xavfsizligiga tahdidlarni amalga oshirish qiyin bo'ladigan yoki bunday imkoniyat bartaraf etiladigan tarzda tartibga soladigan chora-tadbirlar.

Маълумотларни қайта ишлаш тизимининг ишлаш жараёнини, тизим ресурсларидан фойдаланишни, персонал фаолиятини, шунингдек, фойдаланувчиларнинг тизим билан ўзаро ҳамкорлик тартибини, тизимда айланувчи ахборот хавфсизлигига таҳдидларни амалга ошириш қийин бўладиган ёки бундай имконият бартараф этиладиган тарзда тартибга соладиган чора-тадбирлар.

М

Меры защиты информации правовые

uz - axborotni muhofaza qilishning huquqiy chora-tadbirlari

ахборотни муҳофаза қилишнинг ҳуқуқий чора-тадбирлари

en - legal information protective measures

Действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие тем самым неправомерному ее использованию и являющиеся сдерживающим фактором для потенциальных нарушителей.

Mamlakatda amal qiluvchi axborot bilan ishlash qoidalarini va ularning buzilishi uchun javobgarlikni, shu bilan undan noqonuniy foydalanishga toʻsqinlik qiladigan va potensial buzgʻunchilarni toʻxtatib turuvchi omil hisoblanadigan, qonunlar, farmoyishlar va boshqa normativ-huquqiy aktlar.

Мамлакатда амал қилувчи ахборот билан ишлаш қоидаларини ва уларнинг бузилиши учун жавобгарликни, шу билан ундан ноқонуний фойдаланишга тўсқинлик қиладиган ва потенциал бузғунчиларни тўхтатиб турувчи омил ҳисобланадиган, қонунлар, фармойишлар ва бошқа норматив-ҳуқуқий актлар.

Меры защиты информации технические

uz - axborotni muhofaza qilishning texnik chora-tadbirlari

ахборотни муҳофаза қилишнинг техник чора-тадбирлари

en - technical information protective measures

Различные электронные устройства и специальные программы, входящие в состав автоматизированной системы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Avtomatlashtirilgan tizim tarkibiga kiruvchi, (mustaqil yoki boshqa vositalar bilan birgalikda) axborotni muhofaza qilish (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan erkin foydalanishni cheklash, hodisalarni qayd qilish, axborotni kriptografik yopish va b.q.) funksiyalarini bajaruvchi turli elektron qurilmalar va maxsus dasturlar.

Автоматлаштирилган тизим таркибига кирувчи, (мустакил ёки бошқа воситалар билан биргаликда) ахборотни муҳофаза қилиш (фойдаланувчи-

М

ларни идентификациялаш ва аутентификация қилиш, ресурслардан эркин фойдаланишни чеклаш, ходисаларни қайд қилиш, ахборотни криптографик ёпиш ва б.қ.) функцияларини бажарувчи турли электрон қурилмалар ва махсус дастурлар.

Меры защиты информации физические

uz - axborotni muhofaza qilishning jismoniy chora-tadbirlari

ахборотни муҳофаза қилишнинг жисмоний чора-тадбирлари

en - physical information protective measures

Разного рода механические, электро- или электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам автоматизированной системы и защищаемой информации, а также технические средства визуального наблюдения, телекоммуникаций и охранной сигнализации.

Avtomatlashtirilgan tizim va muhofaza qilinayotgan axborot komponentlariga potensial buzg'unchilarning suqulib kirishi va foydalanishining mumkin bo'lgan yo'llariga jismoniy to'siq yaratish uchun maxsus mo'ljallangan har xil turdagi mexanik, elektr yoki elektron-mexanik qurilmalar va inshootlar, shuningdek telekommunikatsiya va qo'riqlash signalizatsiyasi, vizual kuzatish texnik vositalari.

Автоматлаштирилган тизим ва муҳофаза қилинаётган ахборот компонентларига потенциал бузғунчиларнинг суқулиб кириши ва фойдаланишининг мумкин бўлган йўлларига жисмоний тўсиқ яратиш учун махсус мўлжалланган ҳар хил турдаги механик, электр ёки электрон-механик қурилмалар ва иншоотлар, шунингдек телекоммуникация ва қўриқлаш сигнализацияси, визуал кузатиш техник воситалари.

Метка безопасности

uz - xavfsizlik belgisi
хавфсизлик белгиси
en - security mark

Маркировка, связанная с ресурсом (которым может быть блок данных), определяющая имя или обозначение атрибутов безопасности данного ресурса.

Resurs (ma'lumotlar bloki bo'lishi mumkin) bilan bog'langan, berilgan resurs xavfsizlik atributlarining nomini yoki belgilanishini aniqlaydigan markalash.

М

Метка грифа

uz - grif belgisi

гриф белгиси

en - security label

Ресурс (маълумотлар блоки бўлиши мумкин) билан боғланган, берилган ресурс хавфсизлик атрибутларининг номини ёки белгиланишини аниқлайдиган маркалаш.

Указатель, непосредственно связанный с той информацией, к которой он относится, например, как часть протокола передачи информации.

O‘zi tegishli axborot bilan bevosita, masalan, axborotni uzatish protokolining bir qismi sifatida, bog‘liq bo‘lgan ko‘rsatkich.

Ўзи тегишли ахборот билан бевосита, масалан, ахборотни узатиш протоколининг бир қисми сифатида, боғлиқ бўлган кўрсаткич.

Метка идентификационная

uz - identifikatsion belgi

идентификацион белги

en - identification mark

Подлинная информация (имя автора, программы) в закодированном или зашифрованном виде.

Kodlangan yoki shifrlangan ko‘rinishdagi haqiqiy axborot (muallif, dastur nomi).

Кодланган ёки шифрланган кўринишдаги ҳақиқий ахборот (муаллиф, дастур номи).

Метка конфиденциальности

uz - konfidensiallik belgisi

конфиденциаллик белгиси

en - confidentiality mark

Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Obyektda mavjud bo‘lgan axborotning konfidensialligini tavsiflovchi axborot elementi.

Объектда мавжуд бўлган ахборотнинг конфиденциаллигини тавсифловчи ахборот элементи.

Метод аутентификации

асимметричный

uz - asimmetrik autentifikatsiya qilish metodi

асимметрик аутентификация қилиш методи

en - asymmetric authentication method

Метод аутентификации, при котором не вся информация аутентификации используется обеими сторонами совместно.

Autentifikatsiya qilish axborotining barchasidan ikkala tomon birgalikda foydalanmaydigan autentifikatsiya qilish metodi.

Аутентификация қилиш ахборотининг барчасидан иккала томон биргаликда фойдаланмайдиган аутентификация қилиш методи.

М

Метод аутентификации симметричный

uz - simmetrik autentifikatsiya qilish metodi

симметрик аутентификация қилиш методи

en - symmetric authentication method

Метод записи с частичным разрушением памяти

uz - хотирани qisman buzib yozish metodi

хотирани қисман бузиб ёзиш методи

en - corruptable store method

Метод защиты информации криптографический

uz - axborotni muhofaza qilishning kriptografik usuli

ахборотни муҳофаза қилишнинг криптографик усули

en - cryptographic method of information protection

Метод измерения

uz - o'lchash usuli

ўлчаш усули

en - measurement method

Метод аутентификации, при котором оба объекта совместно используют общую информацию аутентификации.

Ikkala obyekt umumiy autentifikatsiya axborotidan birgalikda foydalanadigan autentifikatsiya qilish metodi.

Иккала объект умумий аутентификация ахборотидан биргаликда фойдаланадиган аутентификация қилиш методи.

Метод, позволяющий создать уникальный рисунок кристалла памяти путем управления процессом ее частичного разрушения.

Xotiraning qisman buzilish jarayonini boshqarish yo'li bilan, uning kristall noyob shaklini yaratishga imkon beruvchi metod.

Хотиранинг қисман бузилиш жараёнини бошқариш йўли билан, унинг кристалл ноёб шаклини яратишга имкон берувчи метод.

Метод защиты информации, основанный на принципах шифрования и/или электронной цифровой подписи.

Примечание – Криптографический метод может быть реализован программными, аппаратными и аппаратно-программными средствами.

Shifrlash va/yoki elektron raqamli imzo prinsiplariga asoslangan, axborotni muhofaza qilish usuli.

Izoh – Kriptografik usul dasturiy, apparat va apparat-dasturiy vositalar yordamida amalga oshirilishi mumkin.

Шифрлаш ва/ёки электрон рақамли имзо принципларига асосланган, ахборотни муҳофаза қилиш усули.

Изоҳ – Криптографик усул дастурий, аппарат ва аппарат-дастурий воситалар ёрдамида амалга оширилиши мумкин.

Логическая последовательность операций, описанная в общем виде и используемая для измерения атрибута с помощью определенной шкалы.

Примечание – Вид метода измерения зависит от характера операций, используемых при измерении атрибута. Раз-

М

личают два вида метода измерения:

- субъективный: количественная оценка включает человеческую оценку;
- объективный: количественная оценка основана на математических правилах.

Umumiy ko‘rinishda tavsiflangan va ma’lum shkala yordamida atributni o‘lchash uchun foydalaniladigan operatsiyalarning mantiqiy ketma-ketligi.

Izoh – O‘lchash usulining turi atributni o‘lchashda foydalaniladigan operatsiyalar xarakteriga bog‘liq. O‘lchash usulining ikkita turi bor:

- subyektiv: inson bahosini o‘z ichiga olgan miqdoriy baho;
- obyektiv: matematik qoidalarga asoslangan miqdoriy baho.

Умумий кўринишда тавсифланган ва маълум шкала ёрдамида атрибутни ўлчаш учун фойдаланиладиган операцияларнинг мантикий кетма-кетлиги.

Изоҳ – Ўлчаш усулининг тури атрибутни ўлчашда фойдаланиладиган операциялар хактерига боғлиқ. Ўлчаш усулининг иккита тури бор:

- субъектив: инсон баҳосини ўз ичига олган миқдорий баҳо;
- объектив: математик қоидаларга асосланган миқдорий баҳо.

Метод Казиски

uz - Kaziski metodi

Казиски методи

en - Kazisky's method

Метод криптоанализа, позволяющий вычислять период многоалфавитных криптосистем при помощи обнаружения одинаковых слов в шифротексте. Если период многоалфавитной криптосистемы становится известным, то криптоанализ может быть сведен к криптоанализу одноалфавитных систем.

Shifratndagi bir xil so‘zlarni aniqlash yordamida ko‘p alifboli kriptotizim davrini hisoblash imkonini beruvchi kriptotahlil metodi. Agar ko‘p alifboli kriptotizim davri ma’lum bo‘lsa, kriptotahlil bir alifboli tizimlar kriptotahliliga keltiriladi.

Шифратндаги бир хил сўзларни аниқлаш ёрдамида кўп алифболи кriptотизим даврини ҳисоблаш имконини берувчи кriptотаҳлил методи. Агар кўп алифболи кriptотизим даври маълум бўлса, кriptотаҳлил бир алифболи тизимлар кriptотаҳлилига келтирилади.

М

Метод счетчиковый

uz - hisoblagich metodi
хисоблагич методи
en - counter method

Режим использования блочного шифра, похожий на режим OFB, но на вход регистра подается не результат шифрования, а некий счетчик, состояние которого увеличивается на константу, обычно единицу.

OFB rejimiga o'xshash, blokli shifrdan foydalanish rejimi, registr kirishiga shifrlash natijasi emas, holati konstantaga, odatda, bittaga ko'payadigan hisoblagich uzatiladi.

OFB rejimiga ўхшаш, блокли шифрдан фойдаланиш режими, регистр киришига шифрлаш натижаси эмас, ҳолати константага, одатда, биттага кўпаядиган ҳисоблагич узатилади.

Методы внешних вторжений

uz - tashqi bostirib kirishlar yo'llari
ташқи бостириб киришлар йўллари
en - external intrusions techniques

Совокупность способов достижения поставленной цели, отличительной особенностью которых является нахождение источника воздействия во внешней среде.

Примечание – Внешние вторжения могут использовать следующие методы: подсоединение к линии (активное или пассивное); перехват излучений; маскирование под полномочных пользователей системы или под ее компоненты; обход механизмов аутентификации или управления доступом.

Tashqi muhitda ta'sir manbaini topish o'ziga xos xususiyati hisoblanadigan, qo'yilgan maqsadlarga erishish usullari jami.

Izoh – Tashqi bostirib kirishlarda quyidagi usullardan foydalanilishi mumkin: liniyaga (aktiv yoki passiv) ulanish; nurlanishni tutib olish; tizim vakolatli foydalanuvchisi yoki uning komponentlari ostida niqoblanish; autentifikatsiya yoki kira olishni boshqarish mexanizmlarini chetlab o'tish.

Ташқи муҳитда таъсир манбаини топиш ўзига хос хусусияти ҳисобланадиган, қўйилган мақсадларга эришиш усуллари жами.

Изоҳ – Ташқи бостириб киришларда қуйидаги усуллардан фойдаланилиши мумкин: линияга (актив ёки пассив) уланиш; нурланишни тутиб олиш; тизим ваколатли фойдаланувчиси ёки унинг компонентлари остида ниқобланиш; аутентификация ёки кира олишни бошқариш механизмларини четлаб ўтиш.

М

Механизм информационной безопасности сети телекоммуникаций общего пользования

uz - umum foydalanishdagi telekommunikatsiyalar tarmogʻining axborot xavfsizligi mexanizmi

умум фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги механизми

en - public switched telecommunications network information security mechanism

Аппаратно-программные и организационные средства системы обеспечения информационной безопасности сети телекоммуникаций общего пользования, реализующие в соответствии с заданной политикой информационной безопасности сети, один или несколько аспектов защиты от угроз информационной безопасности сети в соответствии с одним из трех, перекрывающих друг друга классов защиты: предотвращение воздействия нарушения, обнаружение последствий, причиненных злоумышленником, восстановление (ликвидация) этих последствий.

Примечание – К механизмам информационной безопасности сети телекоммуникаций общего пользования при защите процесса передачи сообщений в сети относятся: механизм контроля доступа, механизм аутентификации сообщений, механизм обменной аутентификации.

Tarmoqning belgilangan axborot xavfsizligi siyosatiga muvofiq, bir-birini toʻldiruvchi uchta – buzish koʻrsatadigan taʼsirning oldini olish, jinoyatkor tomonidan yetkazilgan oqibatlarni aniqlash, bu oqibatlarni tiklash (bartaraf qilish) kabi, muhofaza qilish klassining biriga muvofiq, tarmoqni axborot xavfsizligiga boʻladigan tahdidlardan muhofaza qilishning bitta yoki bir nechta aspektini amalga oshiradigan umumiy foydalanishdagi telekommunikatsiyalar tarmogʻi axborot xavfsizligini taʼminlash tizimining apparat-dasturiy va tashkiliy vositalari.

Izoh – Tarmoqda xabarlar uzatish jarayonini muhofaza qilishda umumiy foydalanishdagi telekommunikatsiyalar tarmogʻi axborot xavfsizligi mexanizmlariga erkin foydalanishni nazorat qilish mexanizmi, xabarlarni autentifikatsiya qilish mexanizmi, almashuv autentifikatsiya mexanizmi kiradi.

Tarmoqning belgilangan axborot xavfsizligi siyosatiga muvofiq, bir-birini toʻldiruvchi uchta – buzish koʻrsatadigan taʼsirning oldini olish, jinoyatkor tomonidan yetkazilgan oqibatlarni aniqlash, bu oqibatlarni tiklash (bartaraf qilish) kabi, muhofaza qilish klassining biriga muvofiq, tarmoqni axborot xavfsizligiga boʻladigan tahdidlardan muhofaza qilishning bitta yoki bir nechta aspektini amalga oshiradigan

М

умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг аппарат-дастурий ва ташкилий воситалари.

Изоҳ – Тармоқда хабарлар узатиш жараёнини муҳофаза қилишда умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлиги механизмларига эркин фойдаланишни назорат қилиш механизми, хабарларни аутентификация қилиш механизми, алмашув аутентификация механизми киради.

Механизм контроля доступа

uz - foydalana olishni

nazorat qilish mexanizmi

фойдалана олишни

назорат қилиш механизми

en - access control mechanism

Оборудование или программное обеспечение, процедуры системы, процедуры администратора и их различные комбинации, которые обнаруживают, предотвращают несанкционированный доступ и разрешают законный в автоматизированных системах.

Ruxsat etilmagan tarzda foydalana olishni aniqlaydigan, bartaraf qiladigan va avtomatlashtirilgan tizimlarda qonuniy foydalanishga ruxsat beradigan uskuna yoki dasturiy ta'minot, tizim protsedurasi, ma'mur protsedurasi va ularning turli xil kombinatsiyalari.

Рухсат этилмаган тарзда фойдалана олишни аниқлайдиган, бартараф қиладиган ва автоматлаштирилган тизимларда қонуний фойдаланишга рухсат берадиган ускуна ёки дастурий таъминот, тизим процедураси, маъмур процедураси ва уларнинг турли хил комбинациялари.

Микроб

uz - mikro

микроб

en - microbe

Программа, которая способна рассылаться самостоятельно по электронной почте всем адресатам каждого списка доставки.

Elektron pochta orqali har bir eltib berish ro'yxatidagi adresatlarga mustaqil tarzda tarqalish qobiliyatiga ega bo'lgan dastur.

Электрон почта орқали ҳар бир элтиб бериш рўйхатидаги адресатларга мустақил тарзда тарқалиш қобилиятига эга бўлган дастур.

М

Минимум привилегий
uz - imtiyozlar minimumi
имтиёзлар минимуми
en - least privilege

1 Наделение субъектов только теми правами на доступ, которые им необходимы для выполнения конкретных задач.

2 Один из основополагающих принципов организации системы защиты, гласящий, что каждый субъект должен иметь минимально возможный набор привилегий, необходимый для решения поставленных перед ним задач.

Примечание – Следование этому принципу предохраняет от нарушений, возможных в результате злого умысла, ошибки или несанкционированного использования привилегий.

1 Subyektlarga ularning aniq vazifalarni bajarishlari uchun zarur boʻlgan erkin foydalanish huquqlarini berish.

2 Har bir subyekt oʻz oldiga qoʻygan vazifalarni hal qilish uchun zarur imtiyozlarning minimal darajada mumkin boʻlgan toʻplamiga ega boʻlishi kerak deb hisoblovchi muhofaza tizimini tashkil qilishning eng muhim prinsiplaridan biri.

Izoh – Bu prinsipga rioya qilish yovuz niyat, xato yoki imtiyozlardan ruxsat etilmagan tarzda foydalana olish natijasida sodir boʻlishi mumkin boʻlgan buzilishlardan saqlaydi.

1 Субъектларга уларнинг аниқ вазифаларни бажаришлари учун зарур бўлган эркин фойдаланиш ҳуқуқларини бериш.

2 Ҳар бир субъект ўз олдига қўйган вазифаларни ҳал қилиш учун зарур имтиёзларнинг минимал даражада мумкин бўлган тўпламига эга бўлиши керак деб ҳисобловчи муҳофаза тизимини ташкил қилишнинг энг муҳим принципларидан бири.

Изоҳ – Бу принципга риоя қилиш ёвуз ният, хато ёки имтиёзлардан рухсат этилмаган тарзда фойдалана олиш натижасида содир бўлиши мумкин бўлган бузилишлардан сақлайди.

Модель аналитическая
uz - tahliliy model
таҳлилий модель
en - analytical model

Алгоритм или формула, объединяющие одну или несколько основных и/или производных мер с соответствующими критериями принятия решения.

Qaror qabul qilishning tegishli mezonlariga ega bitta yoki bir nechta asosiy va/yoki hosil qilingan meʼyorni birlashtiruvchi algoritm yoki formula.

М

Қарор қабул қилишнинг тегишли мезонларига эга битта ёки бир нечта асосий ва/ёки ҳосил қилинган меъёрни бирлаштирувчи алгоритм ёки формула.

Модель Белла-Лападула

uz - Bella-Lapadula modeli

Белла-Лападула модели

en - Bella-Lapadula model

Формальная модель описания политики безопасности с использованием теории автоматов, и описывающая множество правил управления доступом. В этой модели компоненты системы делятся на объекты и субъекты. Вводится понятие безопасного состояния и доказывается, что если каждый переход сохраняет безопасное состояние (то есть переводит систему из безопасного состояния в другое безопасное состояние), то согласно принципу индукции система является безопасной.

Avtomatlar nazariyasidan foydalanib, xavfsizlik siyosatini tavsiflashning formal modeli va erkin foydalanishni boshqarishning ko'plab qoidalarini tavsiflovchi formal model. Bu modelda tizim komponentlari obyektlar va subyektlarga bo'linadi. Xavfsizlik holati tushunchasi kiritiladi, har bir o'tish xavfsizlik holatini saqlab qolsa (ya'ni, tizimni xavfsiz holatdan boshqa xavfsiz holatga o'tkazadi), induksiya prinsipiga muvofiq, tizim xavfsiz hisoblanishi isbot qilinadi.

Автоматлар назариясидан фойдаланиб, хавфсизлик сиёсатини тавсифлашнинг формал модели ва эркин фойдаланишни бошқаришнинг кўплаб қоидаларини тавсифловчи формал модель. Бу моделда тизим компонентлари объектлар ва субъектларга бўлинади. Хавфсизлик ҳолати тушунчаси киритилади, ҳар бир ўтиш хавфсизлик ҳолатини сақлаб қолса (яъни, тизимни хавфсиз ҳолатдан бошқа хавфсиз ҳолатга ўтказди), индукция принципига мувофиқ, тизим хавфсиз ҳисобланиши исбот қилинади.

М

Модель данных

иерархическая

uz - iyerarxik ma'lumotlar modeli

иерархик маълумотлар модели

en - hierarchical data model

Модель данных для представления данных иерархической структуры.

Iyerarxik struktura ma'lumotlarini taqdim etish uchun yaratiladigan ma'lumotlar modeli.

Иерархик структура маълумотларини тақдим этиш учун яратиладиган маълумотлар модели.

Модель жизненного цикла

uz - hayotiy sikl modeli

ҳаётӣй цикл модели

en - life-cycle model

Описание стадий и их взаимосвязей друг с другом, которые используются при управлении жизненным циклом определенного объекта, а также описание последовательности этих стадий и их высокоуровневых характеристик.

Belgilangan obyektning hayotiy siklini boshqarishda ishlatiladigan, o'zaro bir-biri bilan bog'langan bosqichlar tavsifi, shuningdek, ushbu bosqichlar ketma-ketligini va ularning yuqori darajadagi xarakteristikalarini tavsiflash.

Белгиланган объектнинг ҳаётӣй циклини бошқаришда ишлатиладиган, ўзаро бир-бири билан боғланган босқичлар тавсифи, шунингдек, ушбу босқичлар кетма-кетлигини ва уларнинг юқори даражадаги характеристикаларини тавсифлаш.

Модель защиты

uz - muhofaza qilish modeli

муҳофаза қилиш модели

en - protection model

Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и/или организационных мер защиты от несанкционированного доступа.

Dasturiy-texnik vositalar kompleksi va/yoki ruxsat etilmagan foydalana olishdan muhofaza qilish tashkiliy chora-tadbirlarining mavhum (formallashtirilgan yoki formallashtirilmagan) tavsifi.

Дастурий-техник воситалар комплекси ва/ёки рухсат этилмаган фойдалана олишдан муҳофаза қилиш ташкилий чора-тадбирларининг мавҳум (формаллаштирилган ёки формаллаштирилмаган) тавсифи.

М

Модель информационных угроз (техническими средствами)

uz - axborot tahdidlari (texnik vositalar bilan amalga oshiriladigan) modeli

ахборот таҳдидлари (техник воситалар билан амалга ошириладиган) модели

en - information treats model (by technical facilities)

Формализованное описание технических каналов утечки, сведения о методах и средствах реализации информационных угроз.

Ахборот чиқиб кетадиган техник каналларнинг формаллаштирилган тавсифи, ахборот таҳдидларини амалга оширишнинг методлари ҳамда воситалари то‘ғ‘risidagi ma‘lumotlar.

Ахборот чиқиб кетадиган техник каналларнинг формаллаштирилган тавсифи, ахборот таҳдидларини амалга оширишнинг методлари ҳамда воситалари тўғ‘risidaги маълумотлар.

Модель концептуальная

uz - konseptual model

концептуал модель

en - conceptual model

Формальное представление проблемной области на понятийном уровне.

Muammoli sohaning tushuncha darajasida formal taqdim etilishi.

Муаммоли соҳанинг тушунча даражасида формал тақдим этилиши.

Модель нарушителя правил разграничения доступа

uz - foydalana olishni belgilash qoidalarini buzuvchining modeli

фойдалана олишни белгилаш қоидаларини бузувчининг модели

en - security policy violator model

Абстрактное (формализованное или не формализованное) описание нарушителя правил разграничения доступа.

Foydalana olishni belgilash qoidalarini buzuvchining abstrakt (formallashtirilgan yoki formallashtirilmagan) tavsifi.

Фойдалана олишни белгилаш қоидаларини бузувчининг абстракт (формаллаштирилган ёки формаллаштирилмаган) тавсифи.

Модель политики безопасности формальная

uz - formal xavfsizlik siyosati modeli

формал хавфсизлик сиёсати модели

en - formal security policy model

Математически строгое описание политики безопасности, подразумевающее описание начального состояния системы, способы перехода системы из одного состояния в другое, а также определение безопасного состояния. Примером формальной модели является модель Белла-Лападула.

Tizim boshlang‘ich holati tavsifini, tizimning bir ho-

M

latdan ikkinchi holatga o'tish usullarini, shuningdek, xavfsiz holat aniqlanishini nazarda tutuvchi, xavfsizlik siyosatining qat'iy matematik tavsifi. Bella-Lapadula modeli formal modelga misol bo'ladi.

Тизим бошланғич ҳолати тавсифини, тизимнинг бир ҳолатдан иккинчи ҳолатга ўтиш усулларини, шунингдек, хавфсиз ҳолат аниқланишини назарда тутувчи, хавфсизлик сиёсатининг қатъий математик тавсифи. Белла-Лападула модели формал моделга мисол бўлади.

Модель угроз

uz - tahdidlar modeli

тахдидлар модели

en - threat model

Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Axborot xavfsizligi tahdidlari xarakteristikalarini yoki xususiyatlarining fizik, matematik, tavsifiy taqdim etilishi.

Ахборот хавфсизлиги таҳдидлари хактеристикалари ёки хусусиятларининг физик, математик, тавсифий тақдим этилиши.

Модификация

uz - o'zgartirish

ўзгартириш

en - modification

Неавторизованное изменение данных в базах данных или в файлах автоматизированной системы, изменение алгоритмов используемых программ с целью выполнения некоторой дополнительной несанкционированной обработки.

Avtomatlashtirilgan tizim fayllaridagi yoki ma'lumotlar bazasidagi ma'lumotlarning mualliflashtirilmagan tarzda o'zgartirilishi, foydalaniladigan dasturlar algoritmlarining ba'zi bir qo'shimcha, ruxsat etilmagan tarzda qayta ishlashni bajarish maqsadida, o'zgartirilishi.

Автоматлаштирилган тизим файлларидаги ёки маълумотлар базасидаги маълумотларнинг муаллифлаштирилмаган тарзда ўзгартирилиши, фойдаланиладиган дастурлар алгоритмларининг баъзи бир қўшимча, рухсат этилмаган тарзда қайта ишлашни бажариш мақсадида, ўзгартирилиши.

М

Модификация информации

uz - axborotni o'zgartirish

ахборотни ўзгартириш

en - information modification

Несанкционированное изменение содержания или объема информации на ее носителях при обработке техническими средствами.

Texnik vositalar bilan qayta ishlashda, tashuvchilardagi axborotning mazmuni yoki hajmini ruxsat etilmagan tarzda o'zgartirilishi.

Техник воситалар билан қайта ишлашда, ташувчилардаги ахборотнинг мазмуни ёки ҳажмини рухсат этилмаган тарзда ўзгартирилиши.

Модуль защиты

интеллектуальный

uz - intellektual muhofaza

qilish moduli

интеллектуал муҳофаза

қилиш модули

en - smart protection card

Аппаратно-программная схема защиты программного обеспечения, характеризующаяся высоким уровнем защищенности и использующая процессор.

Dasturiy ta'minotni muhofaza qilishning, yuqori darajada muhofazalanganlik bilan tavsiflanuvchi hamda protsessordan foydalanuvchi apparat-dasturiy sxemasi.

Дастурий таъминотни муҳофаза қилишнинг, юқори даражада муҳофазаланганлик билан тавсифланувчи ҳамда процессордан фойдаланувчи аппарат-дастурий схемаси.

Модуль идентификации

абонента (SIM-карта)

uz - abonentni identifikatsiyalash moduli (SIM-karta)

абонентни идентификациялаш модули (SIM-карта)

en - subscriber identification module, SIM

Пластиковая карточка с микрочипом, в памяти которой хранятся идентификационный номер, ключ аутентификации и криптографический алгоритм, необходимый для реализации процедуры аутентификации.

Mikrochipli plastik kartochka, uning хотирасида аутентификация процедурасини амалга ошириш учун зарур бўлган идентификацион рақам, аутентификация калити ва криптографик алгоритм сақланади.

Микрочипли пластик карточка, унинг хотирасида аутентификация процедурасини амалга ошириш учун зарур бўлган идентификацион рақам, аутентификация калити ва криптографик алгоритм сақланади.

М

Модуль идентификационный сменный

uz - identifikatsion

almashtiriladigan modul

идентификацион

алмаштириладиган модуль

en - removable user identity

module, R-UIM

Разновидность смарт-карты, которая может быть легко удалена из одного абонентского аппарата и вставлена в другой.

Bir abonent apparatidan oson olinadigan va boshqasiga qo'yiladigan smart-kartaning bir turi.

Бир абонент аппаратидадан осон олинадиган ва бошқасига қўйиладиган смарт-картанинг бир тури.

Модуль услуг пользователя идентификационный

uz - identifikatsion foydalanuvchi xizmatlari moduli

идентификацион фойдаланувчи хизматлари модули

идентификацион фойдаланувчи хизматлари модули

en - user services identity module

Универсальная смарт-карта в сети UMTS, являющаяся аналогом SIM-карты в GSM, но с более широким набором услуг.

GSM dagi *SIM*-kartaga o'xshash, lekin xizmatlarning keng to'plamiga ega bo'lgan, *UMTS* tarmog'idagi universal smart-karta.

*GSM*даги *SIM*-картага ўхшаш, лекин хизматларнинг кенг тўпламига эга бўлган, *UMTS* тармоғидаги универсал смарт-карта.

Монитор (программа)

uz - monitor (dastur)

монитор (дастур)

en - monitor (software)

Резидентно находящаяся в оперативной памяти утилита, которая позволяет выявлять «подозрительные» действия пользовательских программ: изменение и переименование выполняемых программ (COM- и EXE-файлов), запись на диск по абсолютному адресу, форматирование диска и т.д.

Operativ хотирада rezidentlik bilan joylashgan utilita. Foydalanuvchilar dasturlarining «shubhali» harakatlarini aniqlash: bajariladigan dasturlarning (*COM* va *EXE* fayllarning) o'zgartirilishini yoki qayta nomlanishini, absolyut adres bo'yicha diskka yozish, diskni formatlash va h.k. aniqlash imkonini beradi.

Оператив хотирада резидентлик билан жойлашган утилита. Фойдаланувчилар дастурларининг «шубҳали» ҳаракатларини аниқлаш: бажариладиган дастурларнинг (*COM* ва *EXE* файлларнинг) ўзгартирилишини ёки қайта номланишини, абсолют адрес бўйича дискка ёзиш, дискни форматлаш ва ҳ.к. аниқлаш имконини беради.

М

Монитор ссылок

uz - havolalar monitori

хаволалар монитори

en - reference monitor concept

Концепция контроля доступа, базирующаяся на понятии абстрактной машины, разделяющей все попытки доступа субъектов к объектам. Находит практическую реализацию в виде ядра безопасности.

Subyektlarning obyektlardan erkin foydalanish uchun boʻlgan barcha urinishlarini ajratuvchi abstrakt mashina tushunchasiga asoslanuvchi, erkin foydalanishni nazorat qilish konsepsiyasi. Yadro xavfsizligi koʻrinishida amalga oshiriladi.

Субъектларнинг объектлардан эркин фойдаланиш учун бўлган барча уринишларини ажратувчи абстракт машина тушунчасига асосланувчи, эркин фойдаланишни назорат қилиш концепцияси. Ядро хавфсизлиги кўринишида амалга оширилади.

Мониторинг

uz - monitoring

мониторинг

en - monitoring

Определение состояния системы, процесса или деятельности.

Примечание – Для определения состояния возможно будет необходимо его контролировать, наблюдать или критически оценивать.

Tizim, jarayon yoki faoliyat holatini aniqlash.

Izoh – Holatni aniqlash uchun, balki uni nazorat qilish, kuzatish yoki kritik baholash zarur boʻlishi mumkin.

Тизим, жараён ёки фаолият ҳолатини аниқлаш.

Изоҳ – Ҳолатни аниқлаш учун, балки уни назорат қилиш, кузатиш ёки критик баҳолаш зарур бўлиши мумкин.

Мошенничество

uz - firibgarlik

фирибгарлик

en - fraud

1 Любые незаконные действия, связанные с использованием ресурсов мобильной сети связи без надлежащей оплаты за эфирное время, например путем предоставления ложных сведений.

2 Любые незаконные преднамеренные действия, связанные с использованием услуг телекоммуникаций без надлежащей оплаты, с целью получения выгоды.

1 Efir vaqti uchun tegishli toʻlovlarsiz, masalan, yolgʻon maʼlumotlarni taqdim etish yoʻli bilan mobil aloqaning tarmogʻi resurslaridan foydalanish bilan bogʻliq har qanday noqonuniy harakat.

М

2 Foyda olish maqsadida lozim darajadagi to'lovlar-siz telekommunikatsiyalar xizmatlaridan foydalanish bilan bog'liq bo'lgan har qanday noqonuniy ataylab qilingan harakatlar.

1 Эфир вақти учун тегишли тўловларсиз, масалан, ёлғон маълумотларни тақдим этиш йўли билан мобил алоқанинг тармоғи ресурсларидан фойдаланиш билан боғлиқ ҳар қандай ноқонуний ҳаракат.

2 Фойда олиш мақсадида лозим даражадаги тўловларсиз телекоммуникациялар хизматлари-дан фойдаланиш билан боғлиқ бўлган ҳар қандай ноқонуний атайлаб қилинган ҳаракатлар.

Мошенничество внутреннее

uz - ichki firibgarlik

ички фирибгарлик

en - internal fraud

Использование служащими своего служебного положения для получения выгоды лично или че-рез третьих лиц путем передачи им технических сведений конфиденциального характера.

Xizmatchilar tomonidan uchinchi shaxslarga konfi-densial xarakterdagi texnik ma'lumotlarni uzatish yo'li bilan, shaxsan yoki ushbu shaxslar orqali foyda olish uchun o'z xizmat mavqeidan foydalanishi.

Хизматчилар томонидан учинчи шахсларга кон-фиденциал характердаги техник маълумотларни узатиш йўли билан, шахсан ёки ушбу шахслар орқали фойда олиш учун ўз хизмат мавқеидан фойдаланиши.

Мошенничество

компьютерное

uz - kompyuter firibgarligi

компьютер фирибгарлиги

en - computer fraud

Мошенничество, совершенное с помощью или при непосредственном использовании системы обработки данных или компьютерной сети.

Ma'lumotlarni qayta ishlash tizimi yoki kompyuter tarmog'i yordamida yoki undan bevosita foydalan-gan holda sodir etilgan firibgarlik.

Маълумотларни қайта ишлаш тизими ёки ком-пьютер тармоғи ёрдамида ёки ундан бевосита фойдаланган ҳолда содир этилган фирибгарлик.

М

Мошенничество процедурное

uz - protsedura firibgarligi
процедура фирибгарлиги
en - procedural fraud

Неправомерное использование роуминга и других сетевых процедур (например, биллинга) с целью уменьшения оплаты услуг связи.

Aloqa xizmatlari to'lovini kamaytirish maqsadida, rouming va boshqa tarmoq protseduralaridan (masalan, billingdan) vakolatsiz foydalanish.

Алоқа хизматлари тўловини камайтириш мақсадида, роуминг ва бошқа тармоқ процедураларидан (масалан, биллингдан) ваколатсиз фойдаланиш.

Мошенничество с карточками предоплаты

uz - oldindan to'lov kartochkalar bilan bog'liq firibgarlik
олдиндан тўлов
карточкалари билан боғлиқ
фирибгарлик
en - prepaid fraud

Любые действия, связанные с незаконными способами пополнения счета с помощью предоплаченных карточек.

Oldindan to'langan kartochkalar yordamida hisobni to'ldirishning noqonuniy usullari bilan bog'liq har qanday harakatlar.

Олдиндан тўланган карточкалар ёрдамида ҳисобни тўлдиришнинг ноқонуний усуллари билан боғлиқ ҳар қандай ҳаракатлар.

Мошенничество с контрактами

uz - kontraktlar bilan bog'liq firibgarlik
контрактлар билан
боғлиқ фирибгарлик
en - subscription fraud

Преднамеренное указание ложных сведений при заключении контракта с оператором сети мобильной связи.

Mobil aloqa tarmog'i operatori bilan kontrakt tuzishda yolg'on ma'lumotlarni ataylab ko'rsatish.

Мобил алоқа тармоғи оператори билан контракт тузишда ёлғон маълумотларни атайлаб кўрсатиш.

Мошенничество с украденным телефоном

uz - o'g'irlangan telefon bilan bog'liq firibgarlik
ўғирланган телефон билан
боғлиқ фирибгарлик
en - stolen phone fraud

Несанкционированное использование украденного или потерянного сотового телефона обычно до тех пор, пока владелец не заявит о его пропаже, а оператор не заблокирует номер.

O'g'irlangan yoki yo'qotilgan sotali telefondan, egasi uni yo'qotgani to'g'risida xabar bergungacha, operator esa raqamni blokirovka qilgungacha, ruxsat etilmagan tarzda foydalanish.

М

Ўғирланган ёки йўқотилган сотали телефондан, эгаси уни йўқотгани тўғрисида хабар бергунгача, оператор эса рақамни блокировка қилгунгача, рухсат этилмаган тарзда фойдаланиш.

Мошенничество, основанное на умении общения

uz - muloqot qila olishga asoslangan firibgarlik

мулоқот қила олишга асосланган фирибгарлик

en - fraud based on communication ability

Искусство обмана пользователей или администраторов сетей путем выведывания у них сведений, необходимых для незаконного доступа в сеть; обычно осуществляется путем обращения к ним от имени авторизованного пользователя.

Foydalanuvchilar yoki tarmoq ma'murlarini, ulardan tarmoqdan noqonuniy foydalana olish uchun zarur bo'lgan ma'lumotlarni bilib olish yo'li bilan aldash mahorati; odatda, mualliflashtirilgan foydalanuvchi nomidan ularga murojaat qilish orqali amalga oshiriladi.

Фойдаланувчилар ёки тармоқ маъмурларини, улардан тармоқдан ноқонуний фойдалана олиш учун зарур бўлган маълумотларни билиб олиш йўли билан алдаш маҳорати; одатда, муаллифлаштирилган фойдаланувчи номидан уларга мурожаат қилиш орқали амалга оширилади.

Н

Наблюдатель

uz - kuzatuvchi
кузатувчи

en - lurker

1 Человек, занимающийся тайным просмотром.

2 Лицо, читающее письма на электронной доске объявлений, но не принимающее никакого участия в их обсуждениях и не отправляющее туда свои письма.

1 Yashirin ko'rib chiqish bilan shug'ullanuvchi odam.

2 Elektron e'lonlar taxtasidagi xatlarni o'quvchi, lekin ularning muhokamasida ishtirok etmaydigan va u yerga o'zining xatlarini yubormaydigan shaxs.

1 Яширин кўриб чиқиш билан шуғулланувчи одам.

2 Электрон эълонлар тахтасидаги хатларни ўқувчи, лекин уларнинг муҳокамасида иштирок этмайдиган ва у ерга ўзининг хатларини юбормайдиган шахс.

Н

Наблюдение

uz - kuzatish

кузатиш

en - lurking

Чтение группы новостей без участия в их обсуждении.

Yangiliklar turkumini, ularning muhokamasida ishtirok etmasdan, o'qish.

Янгиликлар туркумини, уларнинг муҳокамасида иштирок этмасдан, ўқиш.

Надежность

информационная

uz - axborotning

ishonchliligi

ахборотнинг

ишончлилиги

en - information reliability

1 Способность алгоритма или программы правильно выполнять свои функции при различных ошибках в исходных данных.

2 Способность информационной системы обеспечивать целостность хранящихся в ней данных.

1 Algoritm yoki dasturning, dastlabki ma'lumotlarda turli xatolar bo'lganda, o'z funksiyalarini to'g'ri bajarish qobiliyati.

2 Axborot tizimining, unda saqlanadigan ma'lumotlar yaxlitligini ta'minlash qobiliyati.

1 Алгоритм ёки дастурнинг, дастлабки маълумотларда турли хатолар бўлганда, ўз функцияларини тўғри бажариш қобилияти.

2 Ахборот тизимининг, унда сақланадиган маълумотлар яхлитлигини таъминлаш қобилияти.

Надежность сети

uz - tarmoqning ishonchliligi

тармоқнинг ишончлилиги

en - network reliability

Свойство сети сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях использования и технического обслуживания.

Tarmoqning, berilgan rejimlarda va foydalanish hamda texnik xizmat ko'rsatish sharoitlarida, talab qilinadigan funksiyalarni bajarish qobiliyatini tavsiflovchi barcha parametrlar qiymatlarini belgilangan chegarada vaqt bo'yicha saqlash xususiyati.

Тармоқнинг, берилган режимларда ва фойдаланиш ҳамда техник хизмат кўрсатиш шароитларида, талаб қилинадиган функцияларни бажариш қобилиятини тавсифловчи барча параметрлар қийматларини белгиланган чегарада вақт бўйича сақлаш хусусияти.

Н

Назначение

uz - tayinlamoq
тайинламоқ
en - assignment

Спецификация определенного параметра в компоненте или требовании.

Komponentdagi yoki talablardagi muayyan parametrlar tasnifi.

Компонентдаги ёки талаблардаги муайян параметрлар таснифи.

Нападение

uz - hujum
хужум
en - hijacking

Попытка злоумышленника разрушить систему безопасности сервера путем передачи серии сетевых пакетов, фальсифицирующих действия законного клиента.

Jinoyatkorning, serverning xavfsizlik tizimini qonuniy mijozlarning harakatini soxtalashtiruvchi tarmoq paketlarining turkumini uzatish yoʻli bilan buzishga urinishi.

Жинояткорнинг, сервернинг хавфсизлик тизими-ни қонуний мижозларнинг ҳаракатини сохталаштирувчи тармоқ пакетларининг туркумини узатиш йўли билан бузишга уриниши.

Нарушение защиты

uz - muhofaza qilishning buzilishi
муҳофаза қилишнинг бузилиши
en - security breach

Обход системы компьютерной безопасности или вывод из строя какого-либо ее элемента, результатом которого может быть проникновение в систему обработки данных.

Kompyuter xavfsizligi tizimini chetlab oʻtish yoki uning biror-bir elementini ishdan chiqarish, natijada maʼlumotlarni qayta ishlash tizimiga kirib olish mumkin boʻladi.

Компьютер хавфсизлиги тизимини четлаб ўтиш ёки унинг бирор-бир элементини ишдан чиқариш, натижада маълумотларни қайта ишлаш тизимига кириб олиш мумкин бўлади.

Нарушение целостности

uz - yaxlitlikning buzilishi
яхлитликнинг бузилиши
en - integrity violation

Искажение содержимого записей файла или базы данных, которое происходит вследствие машинных сбоев, программных ошибок, а также ошибочных действий пользователей.

Н

Fayl yozuvlari yoki ma'lumotlar bazasi tarkibidagilarning mashina bilan bog'liq uzilishlar, dasturdagi xatolar, shuningdek, foydalanuvchilarning noto'g'ri harakatlari oqibatida yuz beradigan o'zgarishi.

Файл ёзувлари ёки маълумотлар базаси таркибидагиларнинг машина билан боғлиқ узилишлар, дастурдаги хатолар, шунингдек, фойдаланувчиларнинг нотўғри ҳаракatlari оқибатида юз берадиган ўзгариши.

Нарушитель
uz - buzg'unchi
бузғунчи
en - intruder

Лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

Tizim resurslaridan ruxsat etilmagan tarzda foydalana olishga (bu resurs bilan ishlashda uning uchun taqiqlangan harakatlarni bajarishga urinish) xato, bilmaslik oqibatida yoki yovuz niyatda (o'z manfaatlari yo'lida) yoki shunchaki (o'yin yoki o'zini namoyon qilish maqsadida) uringan (urinib ko'rgan) va buning uchun turli xil imkoniyatlar, metodlar va vositalardan foydalangan shaxs (subyekt).

Тизим ресурсларидан рухсат этилмаган тарзда фойдалана олишга (бу ресурс билан ишлашда унинг учун тақиқланган ҳаракатларни бажаришга уриниш) хато, билмаслик оқибатида ёки ёвуз ниятда (ўз манфаатлари йўлида) ёки шунчаки (ўйин ёки ўзини намоен қилиш мақсадида) уринган (уриниб кўрган) ва бунинг учун турли хил имкониятлар, методлар ва воситалардан фойдаланган шахс (субъект).

Нарушитель правил
разграничения доступа
uz - foydalana olishni belgilash qoidalarini buzuvchi

1 Субъект доступа, осуществляющий несанкционированный доступ к информации.
2 Лицо, осуществляющее несанкционированный доступ к информационному ресурсу с использова-

Н

фойдалана олишни
белгилаш қоидаларини
бузувчи
en - security policy violator

Невозможность обхода (ФБО)

uz - chetlab o'tishni iloji
yo'qligi (OXF)
четлаб ўтишни иложи
йўқлиги (OXF)
en - non-bypassability of the
TSF

Недоверие взаимное

uz - o'zaro ishonchsizlik
ўзаро ишончсизлик
en - mutual distrust

нием штатных технических средств.

1 Axborotdan ruxsatsiz foydalana olishni amalga oshiruvchi foydalana olish subyekti.

2 Shtat texnik vositalar yordamida axborot resursidan ruxsat etilmagan tarzda erkin foydalanadigan shaxs.

1 Ахборотдан рухсатсиз фойдалана олишни амалга оширувчи фойдалана олиш субъекти.

2 Штат техник воситалар ёрдамида ахборот ресурсидан рухсат этилмаган тарзда эркин фойдаланадиган шахс.

Свойство архитектуры безопасности, посредством которого все связанные с ФТБ действия выполняются через ФБО.

Xavfsizlik arxitekturasining xususiyati, uning yordamida FXT bilan bog'liq barcha harakatlar OXF orqali bajariladi.

Хавфсизлик архитектурасининг хусусияти, унинг ёрдамида ФХТ билан боғлиқ барча ҳаракатлар ОXF орқали бажарилади.

Отношения между взаимодействующими логическими объектами, когда ни один из них не полагается на безошибочность или надежность выполнения функций другим логическим объектом относительно некоторых свойств.

Birgalikda ishlaydigan mantiqiy obyektlar o'rtasidagi munosabat, bunda ulardan birortasi ham boshqa mantiqiy obyekt tomonidan ba'zi xususiyatlarga nisbatan funksiyalarning bajarilishini xatosiz yoki ishonchli deb hisoblamaydi.

Биргаликда ишлайдиган мантиқий объектлар ўртасидаги муносабат, бунда улардан бирортаси ҳам бошқа мантиқий объект томонидан баъзи хусусиятларга нисбатан функцияларнинг бажарилишини хатосиз ёки ишончли деб ҳисобламайди.

Н

Незащищенность

uz - muhofaza qilinmaganlik
муҳофаза қилинмаганлик
en - insecurity

Возможность использования конкретной уязвимости системы обработки данных при проведении конкретной атаки.

Muayyan hujum amalga oshirilganda ma'lumotlarni qayta ishlash tizimining muayyan zaifligidan foydalanish imkoniyati.

Muayyan hujum amalga oshirilganda ma'lumotlarni qayta ishlash tizimining muayyan zaifligidan foydalanish imkoniyati.

Неотказуемость

uz - rad etib bo'lmazlik
рад этиб бўлмаслик
en - non-repudiation

1 Возможность доказать возникновение определенного события или действия и определить иницирующие их логические объекты.

2 Процедура обмена электронными документами с гарантированной доставкой сообщений. В результате такой процедуры отправитель не может отрицать факт передачи, а получатель то, что сообщение не было доставлено в срок.

1 Muayyan hodisa yoki faoliyatning yuzaga kelishini isbotlash va ularni initsiatsiya qiluvchi mantiqiy obyektlarni aniqlash imkoniyati.

2 Xabarlarni kafolatli yetkazib berish bilan elektron hujjatlarni almashish protsedurasi. Bunday protsedura natijasida jo'natuvchi uzatish faktini, oluvchi esa xabar muddatida yetkazilmaganligini rad etolmaydi.

1 Muayyan hodisa yoki faoliyatning yuzaga kelishini isbotlash va ularni initsiatsiya qiluvchi mantiqiy obyektlarni aniqlash imkoniyati.

2 Xabarlarni kafolatli yetkazib berish bilan elektron hujjatlarni almashish protsedurasi. Bunday protsedura natijasida jo'natuvchi uzatish faktini, oluvchi esa xabar muddatida yetkazilmaganligini rad etolmaydi.

Непрерывность информационной безопасности

uz - axborot xavfsizligining uzluksizligi
ахборот хавфсизлигининг узлуксизлиги
en - information security continuity

Процессы и процедуры, обеспечивающие непрерывность функционирования информационной безопасности.

Axborot xavfsizligi ishlashining uzluksizligi ta'minlanadigan jarayonlar va protseduralar.

Axborot xavfsizligi ishlashining uzluksizligi ta'minlanadigan jarayonlar va protseduralar.

Н

Непризнание участия

uz - ishtirokni tan olmaslik

ishtirokni tan olmaslik

en - repudiation

1 Отрицание одним из логических объектов, участвующих в обмене данными, полного или частичного своего участия в этом обмене.

Примечание – В описании методов и механизмов часто используется термин «неотказуемость», который подразумевает, что ни один из взаимодействующих логических объектов не может отрицать свое участие в обмене данными.

2 Отрицание одной из сторон участия в информационном обмене, а также факта получения сообщений в электронном виде.

1 Ma'lumotlar almashinishda ishtirok etadigan mantiqiy obyektlardan birining, bu almashinishda o'zining ishtirokini to'liq yoki qisman tan olmasligi.

Izoh – Metod va mexanizmlarning bayonida, ko'pchilik hollarda, birgalikda ishlaydigan mantiqiy obyektlardan birontasi ham ma'lumotlar almashinishdagi o'zining ishtirokini rad eta olmasligi nazarda tutilgan «rad etolmaslik» atamasidan foydalaniladi.

2 Tomonlardan birining axborot almashinishda o'z ishtirokini, shuningdek, xabarlarini elektron ko'rinishda olganlik faktini rad etishi.

1 Ma'lumotlar almashinishda ishtirok etadigan mantiqiy obyektlardan birining, bu almashinishda o'zining ishtirokini to'liq yoki qisman tan olmasligi.

Izoh – Metod va mexanizmlarning bayonida, ko'pchilik hollarda, birgalikda ishlaydigan mantiqiy obyektlardan birontasi ham ma'lumotlar almashinishdagi o'zining ishtirokini rad eta olmasligi nazarda tutilgan «rad etolmaslik» atamasidan foydalaniladi.

2 Tomonlardan birining axborot almashinishda o'z ishtirokini, shuningdek, xabarlarini elektron ko'rinishda olganlik faktini rad etishi.

Непротиворечивый

uz - ziddiyatsizlik

ziddiyatsizlik

en - consistent

Характеристика связи между двумя или более логическими объектами, указывающая на отсутствие между ними каких-либо явных противоречий.

Ikki yoki undan ko'p mantiqiy obyekt orasidagi bog'langanlik xarakteristikasi, ular orasida qandaydir ochiq ziddiyatlar yo'qligini ko'rsatadi.

Ikki ёки undan ko'p mantiqiy obyekt orasidagi bog'langanlik xarakteristikasi, ular orasida qandaydir ochiq ziddiyatlar yo'qligini ko'rsatadi.

Н

дайдир очик зиддиятлар йўқлигини кўрсатади.

Несоответствие

uz - nomuvofiqlik
номувофиклик
en - nonconformity

Невыполнение требования.

Talablarning bajarilmasligi.

Талабларнинг бажарилмаслиги.

Нестойкость

uz - bardoshsizlik
бардошсизлик
en - nonpersistence

Возможность несанкционированного ознакомления криптоаналитиками с алгоритмом при генерации, распространении и хранении ключей.

Kalitlarni generatsiyalash, tarqatish va saqlashda kriptanalitiklarning algoritm bilan ruxsat etilmagan tarzda tanishish imkoniyati.

Калитларни генерациялаш, тарқатиш ва сақлашда криптоаналитикларнинг алгоритм билан рухсат этилмаган тарзда танишиш имконияти.

Неформальный

uz - norasmiy
норасмий
en - informal

Выраженный на естественном языке.

Tabiiy tilda ifodalangan.

Табиий тилда ифодаланган.

Нечувствительность к отказам

uz - ishlaymay qolishlarga ta'sirchan bo'lmaslik
ишламай қолишларга таъсирчан бўлмаслик
en - fault tolerance

Свойство программы или системы сохранять правильность функционирования при наличии ошибок или отказов.

Dastur yoki tizimning, xatolar mavjud bo'lgan yoki ishlaymay qolishlar sharoitida to'g'ri ishlashini saqlab qolish xususiyati.

Дастур ёки тизимнинг, хатолар мавжуд бўлган ёки ишламай қолишлар шароитида тўғри ишлашини сақлаб қолиш хусусияти.

Номер идентификационный персональный

uz - shaxsiy identifikatsiya raqami
шахсий идентификация рақами
en - personal identification number

1 Уникальный код, хранимый на смарт-карте и используемый для аутентификации личности пользователя.

2 Персональный код некоторого лица, обеспечивающий ему возможность входа в систему с управляемым доступом.

3 Вид пароля, который должен быть указан терминалу вместе, например, с магнитной картой

Н

для получения доступа к системе.

1 Smart-kartada saqlanadigan va foydalanuvchining shaxsini autentifikatsiya qilish uchun ishlatiladigan poyob kod.

2 Qandaydir shaxsning, unga boshqariladigan tizimga kirish imkonini beradigan shaxsiy kodi.

3 Tizimga kirishga ruxsat olish uchun magnit karta bilan birga terminalga ko'rsatiladigan parol turi.

1 Смарт-картада сақланадиган ва фойдаланувчининг шахсини аутентификация қилиш учун ишлатиладиган ноёб код.

2 Қандайдир шахснинг, унга бошқариладиган тизимга кириш имконини берадиган шахсий коди.

3 Тизимга киришга рухсат олиш учун магнит карта билан бирга терминалга кўрсатиладиган пароль тури.

Номер порядковый

uz - tartib raqami

тартиб рақами

en - sequence number

Текущий номер пакета или сообщения, с помощью которого приемник всегда информирован о порядке поступления данных; позволяет обнаружить подмену данных в процессе передачи.

Paket yoki xabarning joriy raqami, uning yordamida qabul qilgich har doim ma'lumotlarning kelib tushish tartibi to'g'risida xabardor bo'ladi; uzatish jarayonida ma'lumotlar almashtirilganligini aniqlashga imkon beradi.

Пакет ёки хабарнинг жорий рақами, унинг ёрдамида қабул қилгич ҳар доим маълумотларнинг келиб тушиш тартиби тўғрисида хабардор бўлади; узатиш жараёнида маълумотлар алмаштирилганлигини аниқлашга имкон беради.

Норма безопасности

uz - xavfsizlik normasi

хавфсизлик нормаси

en - safety standard

Количественное значение критерия безопасности информации, устанавливаемое в зависимости от категории безопасности.

Xavfsizlik kategoriyasiga bog'liq ravishda o'rnatiladigan, axborot xavfsizligi kriteriyining miqdor qiymati.

Хавфсизлик категориясига боғлиқ равишда ўрнатиладиган, ахборот хавфсизлиги критерийининг

Н

Нормы эффективности защиты информации

uz - axborotni muhofaza qilish samaradorligining normalari

ахборотни муҳофаза қилиш самарадорлигининг нормалари

en - information security efficiency rates

Носители информации

uz - axborot tashuvchilar

ахборот ташувчилар

en - data carrier

микдор қиймати.

Значения показателей эффективности защиты информации, установленные нормативными документами.

Normativ hujjatlar bilan belgilangan axborotni muhofaza qilish samaradorligi ko'rsatkichlarining qiymatlari.

Норматив ҳужжатлар билан белгиланган ахборотни муҳофаза қилиш самарадорлиги кўрсаткичларининг қийматлари.

Материальные объекты (в т.ч. и люди), предназначенные для хранения, обработки и передачи информации.

Axborotni saqlash, qayta ishlash va uzatish uchun mo'ljallangan moddiy obyektlar (shu jumladan, odamlar).

Ахборотни сақлаш, қайта ишлаш ва узатиш учун мўлжалланган моддий объектлар (шу жумладан, одамлар).

Н

**Носители сведений,
являющиеся государст-
венными секретами**

uz - davlat siri hisoblanadigan
ma'lumotlarni tashuvchilar

давлат сири ҳисобла-
надиган маълумотларни
ташувчилар

en - bearers of state secrets

Физические лица и материальные объекты, в том числе физические поля, в которых сведения, составляющие государственные секреты, отражаются в виде памяти, символов, образов, сигналов, технических решений и процессов.

Davlat sirlarini tashkil qiladigan ma'lumotlar хотира, simvollar, obrazlar, signallar, texnik yechimlar va jarayonlar ko'rinishida aks etadigan, jismoniy shaxslar, moddiy obyektlar, shu jumladan, fizik maydonlar.

Давлат сирларини ташкил қиладиган маълумотлар хотира, символлар, образлар, сигналлар, техник ечимлар ва жараёнлар кўринишида акс этадиган, жисмоний шахслар, моддий объектлар, шу жумладан, физик майдонлар.

Нотаризация

uz - notariallashtirish

нотариаллаштириш

en - notarization

Регистрация данных доверенной третьей стороной, которая обеспечит впоследствии подтверждение таких их характеристик, как содержимое, отправитель, время и получатель.

Ma'lumotlarni uchinchi ishonchli tomondan qayd etilishi, bu esa keyinchalik ularning ichidagi, jo'natuvchi, vaqt va oluvchi kabi tavsiflarining tasdiqlanishini ta'minlaydi.

Маълумотларни учинчи ишончли томондан қайд этилиши, бу эса кейинчалик уларнинг ичидаги, жўнатувчи, вақт ва олувчи каби тавсифларининг тасдиқланишини таъминлайди.

О

Область предметная

uz - predmet soha

предмет соҳа

en - universe of discourse

Совокупность всех объектов, которые были, есть или будут в выбранной части реального или условного мира представлять интерес с точки зрения их описания.

Real yoki shartli olamning tanlangan qismida ularni tavsiflash nuqtai nazaridan qiziqish uyg'otadigan,

О

ilgari bo‘lgan, hozirda mavjud va mavjud bo‘ladigan, barcha obyektларning jami.

Реал ёки шартли оламнинг танланган қисмида уларни тавсифлаш нуқтаи назаридан қизиқиш уйғотадиган, илгари бўлган, ҳозирда мавжуд ва мавжуд бўладиган, барча объектларнинг жами.

Область применения

внешняя

uz - tashqi qo‘llanish sohasi

ташқи қўлланиш соҳаси

en - external context

Внешние условия, в которых организация работает и достигает своих целей.

Примечание – Внешняя область применения может включать в себя:

- внешнюю среду, связанную с культурной, социальной, политической, законодательной, регулирующей, экономической, природной или конкурентной сферой на международном, национальном, региональном или местном уровнях;

- ключевые критерии и тенденции, которые могут воздействовать на достижение установленных целей организации;

- взаимоотношения с внешними заинтересованными сторонами, восприятие ими риска, а также значимость для организации этих заинтересованных сторон.

Tashkilot ishlaydigan va o‘z maqsadlariga erishadigan tashqi sharoitlar.

Izoh – Tashqi qo‘llanish sohasi:

- xalqaro, milliy, mintaqaviy yoki mahalliy darajalarda madaniy, ijtimoiy, siyosiy, qonunchilik, tartibga soluvchi, iqtisodiy, tabiiy yoki raqobatbardosh soha bilan bog‘liq tashqi muhitni;

- tashkilotning belgilangan maqsadlariga erishish uchun ta’sir ko‘rsatishi mumkin bo‘lgan asosiy mezonlar va tendensiyalarni;

- tashqi manfaatdor tomonlar bilan o‘zaro aloqani, ularning riskni idrok qilishini, shuningdek, ushbu manfaatdor tomonlarning tashkilot uchun ahamiyatini o‘z ichiga olishi mumkin.

Ташкилот ишлайдиган ва ўз мақсадларига эришадиган ташқи шароитлар.

Изоҳ – Ташқи қўлланиш соҳаси:

- халқаро, миллий, минтақавий ёки маҳаллий даражаларда маданий, ижтимоий, сиёсий, қонунчилик, тартибга солувчи, иқтисодий, табиий ёки рақобатбардош соҳа билан боғлиқ ташқи муҳитни;

- ташкилотнинг белгиланган мақсадларига эришиш учун таъсир кўрсатиши мумкин бўлган асосий меzonлар ва

О

Область применения внутренняя

uz - ichki qoʻllanish sohasi
ichki qoʻllanish sohasi
en - internal context

тенденцияларни;

- ташки манфаатдор томонлар билан ўзаро алоқани, уларнинг рискни идрок қилишини, шунингдек, ушбу манфаатдор томонларнинг ташкилот учун аҳамиятини ўз ичига олиши мумкин.

Внутренние условия, в которых организация работает и достигает своих целей.

Примечание – Внутренняя область применения может включать в себя:

- управление, организационную структуру, обязанности и подотчетность;
- политику, цели и задачи, а также стратегию их достижения;
- возможности организации с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (формальные и неформальные);
- взаимоотношения с внутренними заинтересованными сторонами, восприятие ими риска и значимость для организации этих заинтересованных сторон;
- культуру организации;
- стандарты, руководящие принципы и модели работы, принятые в организации;
- форму и объем договорных отношений.

Tashkilot ishlaydigan va oʻz maqsadlariga erishadigan ichki sharoitlar.

Izoh – Ichki qoʻllanish sohasi:

- boshqaruv, tashkiliy struktura, majburiyatlar va hisobot berishni;
- siyosat, maqsadlar va vazifalar, shuningdek ularga erishish strategiyasini;
- resurslar va bilimlar nuqtai nazaridan tashkilot imkoniyatlarini (masalan, kapital, vaqt, xodimlar, jarayonlar, tizimlar va texnologiyalar);
- axborot tizimlarini, axborot oqimlarini va qarorlar (ham rasmiy, ham norasmiy) qabul qilish jarayonlarini;
- ichki manfaatdor tomonlar bilan oʻzaro aloqani, ularning riskni idrok qilishi va ushbu manfaatdor tomonlarning tashkilot uchun ahamiyatini;
- tashkilot madaniyatini;
- tashkilot tomonidan qabul qilingan standartlar, ishga rahbarlik qilish prinsiplari va modellarini;
- shartnomaviy munosabatlar shakli va hajmini oʻz ichiga olishi mumkin.

О

Ташкилот ишлайдиган ва ўз мақсадларига эришадиган ички шароитлар.

Изоҳ – Ички қўлланиш соҳаси:

- бошқарув, ташкилий структура, мажбуриятлар ва ҳисобот беришни;
- сиёсат, мақсадлар ва вазифалар, шунингдек уларга эришиш стратегиясини;
- ресурслар ва билимлар нуқтаи назаридан ташкилот имкониятларини (масалан, капитал, вақт, ходимлар, жараёнлар, тизимлар ва технологиялар);
- ахборот тизимларини, ахборот оқимларини ва қарорлар (ҳам расмий, ҳам норасмий) қабул қилиш жараёнларини;
- ички манфаатдор томонлар билан ўзаро алоқани, уларнинг рискни идрок қилиши ва ушбу манфаатдор томонларнинг ташкилот учун аҳамиятини;
- ташкилот маданиятини;
- ташкилот томонидан қабул қилинган стандартлар, ишга раҳбарлик қилиш принциплари ва моделларини;
- шартномавий муносабатлар шакли ва ҳажмини ўз ичига олиши мумкин.

Обеспечение программное безопасное

uz - xavfsiz dasturiy ta'minot
хавфсиз дастурий

таъминот

en - security software

Общечеловеческие и прикладные программы и средства, осуществляющие безопасную обработку данных в системе или сети и безопасно используемые ресурсы системы.

Tizim yoki tarmoqda ma'lumotlarning xavfsiz qayta ishlanishini amalga oshiruvchi, tizim resurslaridan xavfsiz foydalanuvchi umumiy maqsadlardagi hamda amaliy dastur va vositalar.

Тизим ёки тармоқда маълумотларнинг хавфсиз қайта ишланишини амалга оширувчи, тизим ресурсларидан хавфсиз фойдаланувчи умумий мақсадлардаги ҳамда амалий дастур ва воситалар.

Обеспечение программное достоверное

uz - ishonchli dasturiy ta'minot
ишончли дастурий

таъминот

en - trusted software

Программное обеспечение, входящее в ДВБ.

ИНВга кирувчи дастурий таъминот.

ИХБга кирувчи дастурий таъминот.

Обеспечивать

uz - ta'minlamoq

таъминламоқ

Гарантировать стойкие причинно-следственные связи между действием и его последствиями.

О

en - ensure

Harakat va uning oqibatlari orasidagi qat'iy sabab-oqibat bog'lanishni kafolatlash.

Харакат ва унинг оқибатлари орасидаги қатъий сабаб-оқибат боғланишни кафолатлаш.

Область блокирования

uz - blokirovkalash sohasi
блокировкалаш соҳаси
en - locking unit

Часть базы данных (запись, область, файл), открытая для монопольной обработки одной программой и недоступная до момента закрытия другим программам.

Ma'lumotlar bazasining, bitta dastur tomonidan monopoli (yakka) qayta ishlash uchun ochiq bo'lgan, yopilish paytigacha boshqa dasturlar foydalana olmaydigan qismi (yozuv, soha, fayl).

Маълумотлар базасининг, битта дастур томонидан монопол (якка) қайта ишлаш учун очик бўлган, ёпилиш пайтигача бошқа дастурлар фойдалана олмайдиган қисми (ёзув, соҳа, файл).

Обман

uz - aldov
алдов
en - spoof

Выполнение действий, направленных на введение в заблуждение пользователя, наблюдателя (например, оператора перехвата сообщений) или ресурса.

Foydalanuvchini, kuzatuvchini (masalan, xabar-larni tutib oluvchi operatorni) yoki resursni chalg'itishga yo'naltirilgan harakatlarni bajarish.

Фойдаланувчини, кузатувчини (масалан, хабарларни тутиб олувчи операторни) ёки ресурсни чалғитишга йўналтирилган ҳаракатларни бажариш.

Обмен аутентификацией

uz - autentifikatsiya
almashinish
аутентификация
алмашиниш
en - authentication exchange

Механизм, предназначенный для подтверждения подлинности какого-либо логического объекта путем обмена информацией.

Axborot almashinuv yo'li bilan qandaydir mantiqiy obyektning haqiqiyligini tasdiqlash uchun mo'ljallangan mexanizm.

Ахборот алмашинув йўли билан қандайдир мантикий объектнинг ҳақиқийлигини тасдиқлаш учун

О

Обмен данными

uz - ma'lumotlar almashinuvi

маълумотлар алмашинуви

en - data communication

мўлжалланган механизм.

Процедура приема и передачи данных, включая кодирование, декодирование буферизацию и проверку.

Ma'lumotlarni qabul qilish va uzatish protsedurasi, jumladan, kodlash, dekodlash, buferlash va tekshirish.

Маълумотларни қабул қилиш ва узатиш процедураси, жумладан, кодлаш, декодлаш, буферлаш ва текшириш.

Обмен данными безопасности

uz - xavfsizlik ma'lumotlari almashinuvi

хавфсизлик маълумотлари

алмашинуви

en - security exchange

Передача или последовательность передач данных управления-протокола-приложения между открытыми системами, являющихся частью работы одного или нескольких механизмов обеспечения безопасности.

Ochiq tizimlar o'rtasida boshqarish-protokol ilova ma'lumotlarini uzatish yoki uzatishlar ketma-ketligi. Bitta yoki bir nechta xavfsizlikni ta'minlash mexanizmlarining ishi hisoblanadi.

Очиқ тизимлар ўртасида бошқариш-протокол-илова маълумотларини узатиш ёки узатишлар кетма-кетлиги. Битта ёки бир нечта хавфсизликни таъминлаш механизмларининг иши ҳисобланади.

Обмен информацией и консультации относительно риска

uz - axbotorlar almashinish va risk yuzasidan maslahatlashuvlar

ахборотлар алмашиниш

ва риск юзасидан

маслаҳатлашувлар

en - risk communication and consultation

Непрерывные итеративные процессы, выполняемые организацией для обеспечения, распространения или получения информации и участия в диалоге с заинтересованными сторонами по вопросам, относящимся к управлению рисками.

Примечания

1 Информация может относиться к существованию, природе, форме, вероятности, значимости, оценке, приемлемости и обработке риска.

2 Консультации являются двухсторонним процессом обмена информацией между организацией и ее заинтересованными сторонами по проблеме до принятия решения или определения действий по этой проблеме.

Консультация – это:

- процесс, который способствует принятию решения на

О

основе убеждения, а не под давлением;

- процесс, который предшествует процессу принятия решения, но не объединяется с ним.

Axborot bilan ta'minlash, uni taqsimlash yoki olish uchun va risklarni boshqarishga taalluqli masalalar bo'yicha manfaatdor tomonlar bilan muloqotda ishtirok etish uchun tashkilotda bajariladigan uzluksiz iterativ jarayonlar.

Izohlar

1 Axborot risklarning mavjudligi, tabiati, shakli, ehtimolligi, ahamiyati baholanishi, qabul qilinishi va qayta ishlanishiga tegishli bo'lishi mumkin.

2 Maslahatlashuvlar ushbu muammo bo'yicha qaror qabul qilingunga qadar yoki bu muammo bo'yicha ishlarni belgilab olishdan avval, tashkilot bilan manfaatdor tomonlar o'rtasida axborot almashinuvining ikki tomonlama jarayonidir.

Maslahatlashuv – bu:

- majburlash asosida emas, balki ishontirish asosida qaror qabul qilishga yordam beradigan jarayon;

- qarorni qabul qilishdan oldin keladigan, ammo u bilan birlashmaydigan jarayon.

Ахборот билан таъминлаш, уни тақсимлаш ёки олиш учун ва рискларни бошқаришга тааллуқли масалалар бўйича манфаатдор томонлар билан мулоқотда иштирок этиш учун ташкilotда бажариладиган узлуксиз итератив жараёнлар.

Изоҳлар

1 Ахборот рискларнинг мавжудлиги, табиати, шакли, эҳтимоллиги, аҳамияти баҳоланиши, қабул қилиниши ва қайта ишланишига тегишли бўлиши мумкин.

2 Маслаҳатлашувлар ушбу муаммо бўйича қарор қабул қилингунга қадар ёки бу муаммо бўйича ишларни белгилаб олишдан аввал, ташкilot билан манфаатдор томонлар ўртасида ахборот алмашинувининг икки томонлама жараёнидир.

Маслаҳатлашув – бу:

- мажбурлаш асосида эмас, балки ишонтириш асосида қарор қабул қилишга ёрдам берадиган жараён;

- қарорни қабул қилишдан олдин келадиган, ammo у билан бирлашмайдиган жараён.

Обмен ключами

uz - kalitlar almashinuvi

калитлар алмашинуви

en - key exchange

Обмен между объектами открытыми ключами, которые должны использоваться для кодирования связи между этими объектами.

Obyektlar o'rtasida, bu obyektlar orasida bog'la-

О

nishni kodlash uchun foydalanilishi kerak bo'lgan ochiq kalitlarni almashinish.

Объектлар ўртасида, бу объектлар орасида боғланишни кодлаш учун фойдаланилиши керак бўлган очик калитларни алмашиниш.

Обмен при установлении подлинности

uz - haqiqiylikni aniqlashdagi almashish

хақиқийликни

аниқлашдаги алмашиниш

en - authentication exchange

Механизм, предназначенный для установления подлинности какого-либо объекта посредством обмена информацией.

Axborot almashinuvi yordamida qandaydir obyektning haqiqiyligini aniqlash uchun mo'ljallangan mexanizm.

Ахборот алмашинуви ёрдамида қандайдир объектнинг ҳақиқийлигини аниқлаш учун мўлжалланган механизм.

Обнаружение атак

uz - hujumlarni aniqlash

хужумларни аниқлаш

en - attack detection

Механизм, используемый для обнаружения атак на объекты системы.

Tizim obyektlariga bo'ladigan hujumlarni aniqlash uchun qo'llaniladigan mexanizm.

Тизим объектларига бўладиган хужумларни аниқлаш учун қўлланиладиган механизм.

Обнаружение манипуляции

uz - manipulyatsiyani

aniqlash

манипуляцияни аниқлаш

en - manipulation detection

Процедура, которая используется для обнаружения случайной или умышленной модификации данных.

Ma'lumotlarning tasodifan yoki qasddan qilinadigan o'zgartirishlarni aniqlash uchun qo'llaniladigan protsedura.

Маълумотларнинг тасодифан ёки қасдан қилинадиган ўзгартиришларни аниқлаш учун қўлланиладиган процедура.

Обновление ключей

быстрое

uz - kalitlarni tez yangilash

калитларни тез янгилаш

en - key freshness

Метод защиты от вскрытия ключевой информации, при котором в каждом новом сеансе связи ключи обновляются, при этом ни один из них повторно не используется.

Kalitli axborotni ochishdan muhofaza qilish metodi,

О

unga ko‘ra, har bir yangi aloqa seansida kalitlar yangilanadi, bunda kalitlarning hech qaysisi takroran ishlatilmaydi.

Калитли ахборотни очишдан муҳофаза қилиш методи, унга кўра, ҳар бир янги алоқа сеансида калитлар янгиланади, бунда калитларнинг ҳеч қайсиси такrorан ишлатилмайди.

Оборудование

криптографическое

uz - kriptografik uskuna

криптографик ускуна

en - cryptographic equipment

Аппаратные, программно-аппаратные, программные комплексы и средства для шифрования, расшифрования, изготовления шифрключей и защиты от несанкционированного доступа, реализующие криптографические алгоритмы и предназначенные для защиты информации при ее передаче, обработке и хранении.

Kriptografik algoritmlarni amalga oshiruvchi, shifrlash, rasshifrovka qilish, shifr kalitlarni tayyorlash, ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish va axborotni uzatish, qayta ishlash va saqlashda muhofaza qilish uchun mo‘ljallangan apparat, dasturiy-apparat, dasturiy kompleks va vositalar.

Криптографик алгоритмларни амалга оширувчи, шифрлаш, расшифровка қилиш, шифр калитларни тайёрлаш, рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш ва ахборотни узатиш, қайта ишлаш ва сақлашда муҳофаза қилиш учун мўлжалланган аппарат, дастурий-аппарат, дастурий комплекс ва воситалар.

Обоснование строгое

uz - qat’iy asos

қатъий асос

en - justification

Заклучение, полученное при выполнении анализа.

Tahlilni bajarishda olingan hulosa.

Таҳлилни бажаришда олинган ҳулоса.

Обработка информации в автоматизированной системе

uz - avtomatlashtirilgan tizimda axborotni qayta ishlash

автоматлаштирилган

tizimda axborotni qayta ishlash

Совокупность операций (сбор, накопление, хранение, преобразование, отображение, выдача и т.п.), осуществляемых над информацией (сведениями, данными) с использованием средств автоматизированной системы.

Avtomatlashtirilgan tizim vositalaridan foydalanib axborot (ma’lumotlar) ustida amalga oshiriladigan

О

en - information processing in the automated system

operatsiyalar (yig'ish, to'plash, saqlash, o'zgartirish, aks ettirish, uzatish va sh.k.) jami.

Автоматлаштирилган тизим воситаларидан фойдаланиб ахборот (маълумотлар) устида амалда ошириладиган операциялар (йиғиш, тўплаш, сақлаш, ўзгартириш, акс эттириш, узатиш ва ш.к.) жами.

Обработка риска

uz - riskni qayta ishlash

рискни қайта ишлаш

en - risk treatment

Процесс модификации риска.

Примечания

1 Обработка риска может включать в себя:

- исключение риска путем принятия решения не начинать или не продолжать деятельность, в процессе или в результате которой может возникнуть опасное событие;
- принятие или повышение риска для обеспечения более широких возможностей;
- устранение источников риска;
- изменение вероятности опасного события;
- изменение последствий опасного события;
- разделение риска с другой стороной или сторонами (путем включения в контракты или финансирования обработки риска);
- обоснованное решение о сохранении риска.

2 Обработка риска может включать в себя устранение, предотвращение или снижение риска.

3 При обработке риска могут возникнуть новые риски и могут измениться существующие риски.

Riskni modifikatsiyalash jarayoni.

Izohlar

1 Riskni qayta ishlash:

- risk jarayoni yoki uning natijasida xavfli hodisa yuzaga kelishi mumkin bo'lgan faoliyatni boshlamaslik yoki davom ettirmaslik to'g'risida qaror qabul qilish yordamida riskning oldi olinishini;
- yanada keng imkoniyatlarni ta'minlash uchun riskning qabul qilinishini yoki riskning oshirilishini;
- risk manbai bartaraf etilishini;
- xavfli hodisa ehtimolligi o'zgarishini;
- xavfli hodisa oqibatlari o'zgarishini;
- boshqa tomon yoki tomonlar bilan riskning taqsimlanishini (shartnomalarga kiritish va riskni qayta ishlashni moliyalashtirish yo'li bilan);
- riskni saqlash to'g'risida asoslangan qarorni o'z ichiga olishi mumkin.

2 Riskni qayta ishlash riskning bartaraf etilishi, oldi olinishi yoki kamaytirilishini o'z ichiga olishi mumkin.

3 Riskni qayta ishlashda yangi risklar vujudga kelishi yoki mavjud risklar o'zgartirilishi mumkin.

О

Рискни модификациялаш жараёни.

Изоҳлар

1 Рискни қайта ишлаш:

- риск жараёни ёки унинг натижасида хавfli ҳодиса юзга келиши мумкин бўлган фаолиятни бошламаслик ёки давом эттирмаслик тўғрисида қарор қабул қилиш ёрдамида рискнинг олди олинишини;
- янада кенг имкониятларни таъминлаш учун рискнинг қабул қилинишини ёки рискнинг оширилишини;
- риск манбаи бартараф этилишини;
- хавfli ҳодиса эҳтимоллиги ўзгаришини;
- хавfli ҳодиса оқибатлари ўзгаришини;
- бошқа томон ёки томонлар билан рискнинг тақсимла-нишини (шартномаларга киритиш ва рискни қайта ишлашни молиялаштириш йўли билан);
- рискни сақлаш тўғрисида асосланган қарорни ўз ичига олиши мумкин.

2 Рискни қайта ишлаш рискнинг бартараф этилиши, олди олиниши ёки камайтирилишини ўз ичига олиши мумкин.

3 Рискни қайта ишлашда янги рисклар вужудга келиши ёки мавжуд рисклар ўзгартирилиши мумкин.

Обработка рисков

uz - risklarni qayta ishlash

рискларни қайта ишлаш

en - risk treatment

Процесс выбора и внедрения мер по изменению рисков.

Risklarni o'zgartirish bo'yicha o'lchovlar tanlash va joriy qilish jarayoni.

Рискларни ўзгартириш бўйича ўлчовлар танлаш ва жорий қилиш жараёни.

Образ

uz - obraz

образ

en - image

Точная копия совокупности данных (возможно, в другой среде хранения информации), на основе которой может быть восстановлен оригинал данных.

Ma'lumotlar jamining aniq nusxasi (axborotni saqlashning boshqa muhitida), uning asosida ma'lumotlarning originali tiklanishi mumkin.

Маълумотлар жамининг аниқ нусхаси (ахборотни сақлашнинг бошқа мухитида), унинг асосида маълумотларнинг оригинали тикланиши мумкин.

Объект

uz - obyekt

объект

1 Отдельный элемент, характеризующийся посредством измерения его атрибутов.

2 Логический объект, доступ к которому контро-

О

en - object

лируется.

Например, файл, программа, область оперативной памяти, собранные и хранимые персональные данные.

3 Пассивный компонент системы, хранящий, принимающий или передающий информацию, доступ к которому регламентируется правилами разграничения доступа.

Примечание – Доступ к объекту подразумевает доступ к содержащейся в нем информации. Примеры объектов: записи, блоки, страницы, сегменты, файлы, директории и программы, а также отдельные биты, байты, слова, поля; различные устройства (терминалы, принтеры, дисководы и т.д.); различные сетевые устройства (отдельные узлы, кабели и т.д.).

1 Atributlarini o'lchash yordamida tavsiflanadigan alohida element.

2 Foydalanilishi nazorat qilinadigan mantiqiy obyekt.

Masalan, fayl, dastur, operativ xotira doirasi; yig'ilgan va saqlanayotgan shaxsiy ma'lumotlar.

3 Axborotni saqlovchi, qabul qiluvchi yoki uzatuvchi tizimning passiv komponenti, undan foydalana olish erkin foydalanishni cheklash qoidalari bilan tartibga solinadi.

Izoh – Obyektdan foydalana olishda unda saqlanayotgan axborotdan erkin foydalanishni anglatadi. Obyektlar: yozuvlar, bloklar, sahifalar, segmentlar, fayllar, direktoriyalar va dasturlar, shuningdek, alohida bitlar, baytlar, so'zlar, maydonlar; turli qurilmalar (terminallar, printerlar, diskovodlar va h.k.); turli tarmoq qurilmalari (alohida uzellar, kabellar va h.k.).

1 Атрибутларини ўлчаш ёрдамида тавсифланадиган алоҳида элемент.

2 Фойдаланилиши назорат қилинадиган мантиқий объект.

Масалан, файл, дастур, оператив хотира доираси; йиғилган ва сақланаётган шахсий маълумотлар.

3 Ахборотни сақловчи, қабул қилувчи ёки узатувчи тизимнинг пассив компоненти, ундан фойдалана олиш эркин фойдаланишни чеклаш қоидалари билан тартибга солинади.

Изоҳ – Объектдан фойдалана олишда унда сақланаётган ахборотдан эркин фойдаланишни англатади. Объектлар:

О

ёзувлар, блоклар, саҳифалар, сегментлар, файллар, директориялар ва дастурлар, шунингдек, алоҳида битлар, байтлар, сўзлар, майдонлар; турли қурилмалар (терминаллар, принтерлар, дисководлар ва ҳ.к.); турли тармоқ қурилмалари (алоҳида узеллар, кабеллар ва ҳ.к.).

Объект анализа

uz - tahlil obyektı

таҳлил объекти

en - review object

Анализируемый специфический элемент.

Tahlil qilinadigan spetsifik element.

Таҳлил қилинадиган специфик элемент.

Объект безопасности

uz - xavfsizlik obyektı

хавфсизлик объекти

en - security object

Пассивная системная составляющая, к которой применяется политика безопасности.

Xavfsizlik siyosati qo‘llaniladigan, tizimning passiv tashkil etuvchisi.

Хавфсизлик сиёсати қўлланиладиган, тизимнинг пассив ташкил этувчиси.

Объект вычислительной техники

uz - hisoblash texnikasi

obyektı

ҳисоблаш техникаси

объекти

en - computer technology object

Стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации.

Примечание – К объектам вычислительной техники относятся АС, АРМ, ИВЦ и другие комплексы средств вычислительной техники, а также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

O‘zida axborotni qayta ishlashning muayyan funksiyalarini bajarish uchun mo‘ljallangan hisoblash texnikasi vositalarining kompleksini ifodalovchi statSIONAR yoki ko‘chma obyekt.

Izoh – Hisoblash texnikasi obyektlariga AT, AIO‘, АНМ va hisoblash texnikasi vositalarining boshqa komplekslari, shuningdek, axborotni qayta ishlashning mustaqil funksiyalarini bajaradigan, hisoblash texnikasining alohida vositalari ham kiradi.

Ўзида ахборотни қайта ишлашнинг муайян функцияларини бажариш учун мўлжалланган ҳисоблаш техникаси воситаларининг комплексини ифодаловчи стационар ёки кўчма объект.

Изоҳ – Ҳисоблаш техникаси объектларига АТ, АИЎ,

О

АХМ ва ҳисоблаш техникаси воситаларининг бошқа комплекслари, шунингдек, ахборотни қайта ишлашнинг мустақил функцияларини бажарадиган, ҳисоблаш техникасининг алоҳида воситалари ҳам киради.

Объект доступа

uz - foydalana olish obyektı

фойдалана олиш объекти

en - access object

Единица информационного ресурса системы, доступ к которой регламентируется правилами разграничения доступа.

Tizimning axborot resursi birligi, undan foydalana olish erkin foydalanishni chegaralash qoidalari bilan tartibga solinadi.

Тизимнинг ахборот ресурси бирлиги, ундан фойдалана олиш эркин фойдаланишни чегаралаш қоидалари билан тартибга солинади.

Объект защиты информации

uz - axborotni muhofaza

qilish obyektı

ахборотни муҳофаза

қилиш объекти

en - information security object

Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Axborotni muhofaza qilish bo'yicha qo'yilgan maqsadga muvofiq muhofaza qilinishi zarur bo'lgan axborot yoki axborot tashuvchi, yoki axborot jarayoni.

Ахборотни муҳофаза қилиш бўйича қўйилган мақсадга мувофиқ муҳофаза қилиниши зарур бўлган ахборот ёки ахборот ташувчи, ёки ахборот жараёни.

Объект информатизации

uz - axborotlashtirish obyektı

ахборотлаштириш

объекти

en - object of informatization

Информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, а также помещения, предназначенные для ведения переговоров, в т.ч. конфиденциальных.

Turli daraja va maqsadlardagi axborot tizimlari, telekommunikatsiya tarmoqlari, axborotni qayta ishlash texnik vositalari, bu vositalar o'rnatilgan va ekspluatatsiya qilinadigan, shuningdek, muzokaralar, shu jumladan, konfidensial muzokaralar olib borish

О

uchun mo'ljallangan xonalar.

Турли даража ва мақсадлардаги ахборот тизимлари, телекоммуникация тармоқлари, ахборотни қайта ишлаш техник воситалари, бу воситалар ўрнатилган ва эксплуатация қилинадиган, шунингдек, музокаралар, шу жумладан, конфиденциал музокаралар олиб бориш учун мўлжалланган хоналар.

Объект информатизации защищенный

uz - muhofazalangan axbotor obyekti

муҳофазаланган ахборот объекти

en - protected informatics object

Объект информатизации, соответствующий требованиям стандартов и других нормативных документов по обеспечению безопасности обрабатываемой информации.

Qayta ishlanadigan axborotning xavfsizligini ta'minlash bo'yicha standartlar va boshqa normativ hujjatlarning talablariga mos keladigan axborotlashtirish obyekti.

Қайта ишланадиган ахборотнинг хавфсизлигини таъминлаш бўйича стандартлар ва бошқа норматив ҳужжатларнинг талабларига мос келадиган ахборотлаштириш объекти.

Объект информационного обмена

uz - axborot almashinish obyekti

ахборот алмашиниш объекти

en - information exchange object

Пассивная единица информационного обмена. Например, информационный пакет данных, файл, каталог, электронное письмо, пароль, электронная подпись и др.

Axborot almashinishning passiv birligi. Masalan, ma'lumotlarning axborot paketi, fayl, katalog, elektron xat, parol, elektron imzo va boshqalar.

Ахборот алмашинишнинг пассив бирлиги. Масалан, маълумотларнинг ахборот пакети, файл, каталог, электрон хат, пароль, электрон имзо ва бошқалар.

Объект информационной безопасности сети телекоммуникаций общего пользования

uz - umumiy foydalanishdagi telekommunikatsiyalar

Объект(ы) сети телекоммуникаций общего пользования, воздействия злоумышленника на который(ые) могут привести к реализации угрозы информационной безопасности сети телекоммуникаций общего пользования.

О

**tarmogʻi axborot xavfsizligi
obyekti**

**умумий фойдаланиш-
даги телекоммуникациялар
тармоғи ахборот
хавфсизлиги объекти**
**en - public switched
telecommunications network
information security object**

Umumiy foydalanishdagi telekommunikatsiyalar tarmogʻi obyekt(lar)i, jinoyatkorning unga (ularga) boʻladigan taʼsiri umumiy foydalanishdagi telekommunikatsiyalar tarmogʻining axborot xavfsizligiga tahdid amalga oshirilishiga olib kelishi mumkin.

Умумий фойдаланишдаги телекоммуникациялар тармоғи объект(лар)и, жинояткорнинг унга (уларга) бўладиган таъсири умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлигига таҳдид амалга оширилишига олиб келиши мумкин.

Объект конечный

uz - oxirgi obyekt
охирги объект
en - terminal object

Субъект, который имеет сертификат и использует свой личный ключ не для целей подписи сертификатов, или объект, который является доверенной стороной.

Sertifikati boʻlgan, oʻzining shaxsiy kalitidan sertifikatlarni imzolash maqsadlarida foydalanmaydigan subyekt yoki ishonchli tomon hisoblanadigan obyekt.

Сертификати бўлган, ўзининг шахсий калитидан сертификатларни имзолаш мақсадларида фойдаланмайдиган субъект ёки ишончли томон ҳисобланадиган объект.

**Объект логический
внешний**

uz - tashqi mantiqiy obyekt
ташқи мантиқий объект
en - external entity

Человек или объект ИТ, находящийся вне объекта оценки и осуществляющий с ним взаимодействие.

Примечание – Внешний логический объект может также называться пользователем.

Baholash obyektidan tashqarida boʻlgan va u bilan birgalikda ishlaydigan odam yoki AT obyektı.

Izoh – Tashqi mantiqiy obyektıni foydalanuvchi deb nomlasa ham boʻladi.

Баҳолаш объектидан ташқарида бўлган ва у билан биргаликда ишлайдиган одам ёки АТ объекти.

Изоҳ – Ташқи мантиқий объектни фойдаланувчи деб номласа ҳам бўлади.

Объект оценки

1 Совокупность аппаратных, программных и/или

О

uz - baholash obyekt
баҳолаш объекти
en - target of evaluation

программно-аппаратных средств возможно в комплекте с руководством.

2 Подлежащий оценке продукт ИТ с руководствами администратора и пользователя.

1 Apparat, dasturiy va/yoki dasturiy-apparat vositalarning qoʻllanma bilan komplekt yigʻindisi.

2 Baholanishi zarur boʻlgan, foydalanuvchi va maʼmur qoʻllanmasiga ega AT mahsuloti.

1 Apparat, dasturiy va/ёки dasturiy-apparat vositalarнинг қўлланма билан комплект йиғиндиси.

2 Баҳоланиши зарур бўлган, фойдаланувчи ва маъмур қўлланмасига эга АТ маҳсулоти.

Объект оценки составной

uz - tarkibiy baholash
obyekti
таркибий баҳолаш
объекти
en - composed target of
evaluation

ОО, состоящий из двух или более компонентов, которые были успешно оценены.

Muvaffaqiyatli baholangan ikkita yoki koʻproq komponentlardan tuzilgan BO.

Муваффақиятли баҳоланган иккита ёки кўпроқ компонентлардан тузилган БО.

Объекты информатики

uz - informatika obyektleri
информатика объектлари
en - information science objects

Автоматизированные системы различного назначения, системы телекоммуникаций, отображения и размножения вместе с помещениями, в которых они установлены, а также отдельные технические средства обработки информации и помещения, предназначенные для ведения конфиденциальных переговоров.

Turli maqsadlardagi avtomatlashtirilgan tizimlar, telekommunikatsiyalarni tasvirlash, koʻpaytirish tizimlari ular oʻrnatilgan xonalar bilan birga, shuningdek, axborotni qayta ishlash ayrim texnik vositalari hamda konfidensial muzokaralar olib borish uchun moʻljallangan xonalar.

Турли мақсадлардаги автоматлаштирилган тизимлар, телекоммуникацияларни тасвирлаш, кў-

О

пайтириш тизимлари, улар ўрнатилган хоналар билан бирга, шунингдек, ахборотни қайта ишлаш айрим техник воситалари ҳамда конфиденциал музокаралар олиб бориш учун мўлжалланган хоналар.

Объекты режимные

uz - rejimli obyektlar
режимли объектлар
en - secret entities

Организации, технологическое производство, отчеты которых содержат сведения, составляющие государственные секреты.

Texnologik ishlab chiqarishi, hisobotlari davlat siri hisoblanadigan ma'lumotlarni o'z ichiga oladigan tashkilotlar.

Технологик ишлаб чиқариши, ҳисоботлари давлат сирини ҳисобланадиган маълумотларни ўз ичига оладиган ташкилотлар.

Объём аудита

uz - audit hajmi
аудит ҳажми
en - audit scope

Продолжительность и границы аудита.

Auditning davomiyligi va chegaralari.

Аудитнинг давомийлиги ва чегаралари.

Объяснять

uz - izohlamoq
изоҳламоқ
en - explain

Аргументировать причины выбора образа действия.

Примечание – Этот термин отличается от терминов «демонстрировать» и «описывать». Предназначен для ответа на вопрос «почему?» без приведения доказательств того, что был выбран наиболее оптимальный образ действия.

Harakat tarzini tanlash sabablarini isbotlamoq.

Izoh – Bu atama «namoyish qilmoq» va «tavsiflamoq» atamalaridan farq qiladi. «Nima uchun» so'rog'iga javob bo'lib, isbotsiz eng optimal harakat tarzi uchun mo'ljallangan.

Ҳаракат тарзини танлаш сабабларини исботламоқ.

Изоҳ – Бу атама «намойиш қилмоқ» ва «тавсифламоқ» атамаларидан фарқ қилади. «Нима учун» сўроғига жавоб бўлиб, исботсиз энг оптимал ҳаракат тарзи учун мўлжалланган.

Один звонок

uz - bitta qo'ng'iroq
битта қўнғироқ

Метод мошенничества, при котором сотовый телефон звонит только один раз, а если владелец перезванивает на определившийся телефонный но-

O

en - wan-giri

мер, то мошенник через некоторое время высыла-ет ему счет на солидную сумму.

Firibgarlik metodi, bunda sotali telefon faqat bir marta jiringlaydi, agar uning egasi aniqlangan telefon raqamiga qayta qo'ng'iroq qilsa, firibgar ma'lum vaqt o'tgandan so'ng unga katta miqdordagi summaga hisob yuboradi.

Фирибгарлик методи, бунда сotalи телефон фақат бир марта жиринглайди, агар унинг эгаси аниқланган телефон рақамига қайта қўнғирок қилса, фирибгар маълум вақт ўтгандан сўнг унга катта миқдордаги суммага ҳисоб юборди.

Операция (над компонентом)

uz - operatsiya (komponent ustida)

операция (компонент устида)

en - operation

Модификация или повторение компонента.

Примечание – Разрешенные операции над компонентами: «назначение», «итерация», «уточнение» и «выбор».

Komponentning takrorlanishi yoki o'zgartirilishi.

Izoh – Komponentlar ustida ruxsat etilgan operatsiyalar: «tayinlamoq», «iteratsiya», «aniqlamoq» va «tanlamoq».

Компонентнинг такрорланиши ёки ўзгартирилиши.

Изоҳ – Компонентлар устида рухсат этилган операциялар: «тайинламоқ», «итерация», «аниқламоқ» ва «танламоқ».

Операция (над объектом)

uz - operatsiya (obyekt ustida)

операция (объект устида)

en - operation

Действие определенного типа, выполняемое субъектом над объектом.

Subyektning obyekt ustida bajaradigan aniq turdagi harakati.

Субъектнинг объект устида бажарадиган аниқ турдаги ҳаракати.

Описывать

uz - tavsiflamoq

тавсифламоқ

en - describe

Предоставлять подробное описание конкретного логического объекта.

Aniq mantiqiy obyektning to'liq tavsifini taqdim etmoq.

О

Аниқ мантиқий объектнинг тўлиқ тавсифини тақдим этмоқ.

Определение риска

uz - riskni aniqlash

рискни аниқлаш

en - risk assessment

Процесс, включающий идентификацию риска, анализ риска и оценку риска.

Riskni identifikatsiya qilish, risk tahlili va riskni baholashni ichiga oladigan jarayon.

Рискни идентификация қилиш, риск таҳлили ва рискни баҳолашни ичига оладиган жараён.

Определение рисков

uz - risklarni aniqlash

рискларни аниқлаш

en - risk assessment

Процесс, включающий анализ и оценку рисков.

Risklarni tahlil qilish va baholashni ichiga oladigan jarayon.

Рискларни таҳлил қилиш ва баҳолашни ичига оладиган жараён.

Определение жизненного цикла

uz - hayotiy siklni aniqlash

ҳаётий циклни аниқлаш

en - life-cycle definition

Определение модели жизненного цикла.

Hayotiy sikl modelini aniqlash.

Ҳаётий цикл моделини аниқлаш.

Определитель события

uz - hodisani aniqlagich

ходисани аниқлагич

en - event discriminator

Функция, которая обеспечивает первоначальный анализ события, имеющего отношение к обеспечению безопасности, и вызывает, по мере необходимости, проверку безопасности и/или сигнал тревоги.

Xavfsizlikni ta'minlashga aloqasi bo'lgan hodisaning dastlabki tahlilini ta'minlaydigan va zaruratga qarab, xavfsizlik va/yoki trevoga signali tekshirishini keltirib chiqaradigan funktsiya.

Хавфсизликни таъминлашга алоқаси бўлган ходисанинг дастлабки таҳлилини таъминлайдиган ва заруратга қараб, хавфсизлик ва/ёки тревога сигнали текширилишини келтириб чиқарадиган функция.

Орган

uz - organ

орган

en - authority

Объект, ответственный за выдачу сертификатов. Определены два типа органов: орган сертификации, который выдает сертификаты открытых ключей, и орган по присвоению атрибутов, ко-

О

торый выдает сертификаты атрибутов.

Sertifikatlar berilishi yuzasidan javobgar obyekt. Organlarning ikki turi: ochiq kalitlar sertifikatlarini beradigan sertifikatlash organi hamda atributlar sertifikatlarini beradigan atributlar organi belgilangan.

Сертификатлар берилиши юзасидан жавобгар объект. Органларнинг икки тури: очик калитлар сертификатларини берадиган сертификатлаш органи ҳамда атрибутлар сертификатларини берадиган атрибутлар органи белгиланган.

Орган безопасности

uz - xavfsizlik organi

хавфсизлик органи

en - security authority

1 Объект, ответственный за определение, реализацию и выполнение политики безопасности.

2 Объект, ответственный за управление политической безопасности в домене безопасности.

3 Администратор, ответственный за реализацию политики безопасности.

1 Xavfsizlik siyosatining belgilanishi, amalga oshirilishi va bajarilishi yuzasidan javobgar obyekt.

2 Xavfsizlik domenida xavfsizlik siyosatini boshqarish yuzasidan javobgar obyekt.

3 Xavfsizlik siyosati amalga oshirilishi yuzasidan javobgar ma'mur.

1 Xavfsizlik siyosatining belgilanishi, amalga oshirilishi va bajarilishi yuzasidan javobgar obyekt.

2 Xavfsizlik domenida xavfsizlik siyosatini boshqarish yuzasidan javobgar obyekt.

3 Xavfsizlik siyosati amalga oshirilishi yuzasidan javobgar ma'mur.

Орган оценки

uz - baholash organi

баҳолаш органи

en - evaluation authority

Организация, которая устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах определенного сообщества.

Tashkilotlarning muayyan hamjamiyati doirasida o'tkaziladigan, baholash sifatini nazorat qiluvchi va standartlarni belgilovchi tashkilot.

Ташкилотларнинг муайян ҳамжамияти доирасида ўтказиладиган, баҳолаш сифатини назорат қилув-

О

Орган по присвоению атрибутов

uz - atributlar beruvchi organ
атрибутлар берувчи орган
en - attribute authority

чи ва стандартларни белгиловчи ташкилот.

1 Орган, который назначает полномочия путем выдачи сертификатов атрибутов.

2 Объект, которому один или несколько объектов доверяют создание и подпись сертификатов атрибутов.

1 Atributlar sertifikatlarini berish yo‘li bilan vakolatlar belgilovchi organ.

2 Bitta yoki bir nechta obyekt atributlar sertifikatlarini tuzish va imzolanishini ishonib topshiradigan obyekt.

1 Атрибутлар сертификатларини бериш йўли билан ваколатлар белгиловчи орган.

2 Битта ёки бир нечта объект атрибутлар сертификатларини тузиш ва имзоланишини ишониб топширадиган объект.

Орган по сертификации в области защиты информации

uz - axborotni muhofaza qilish sohasida sertifikatlash organi
ахборотни муҳофаза қилиш соҳасида сертификатлаш органи
en - certification authority in field of information security

Орган, проводящий сертификацию защищенных изделий, технических средств и способов защиты информации на соответствие конкретному стандарту или другому документу.

Muhofazalangan buyumlar, axborotni muhofaza qilish texnik vositalari va usullarining ma’lum bir standartga yoki boshqa hujjatga muvofiqlik sertifikatsiyasini o‘tkazuvchi organ.

Муҳофазаланган буюмлар, ахборотни муҳофаза қилиш техник воситалари ва усулларининг маълум бир стандартга ёки бошқа ҳужжатга мувофиқлик сертификациясини ўтказувчи орган.

Орган регистрации

uz - ro‘uxatga olish organi
рўйхатга олиш органи
en - registration authority

1 Какой-либо объект, отвечающий за идентификацию и аутентификацию субъектов сертификатов, но не являющийся органом сертификации и органом по присвоению атрибутов.

2 Орган, которому предоставлено право и доверено предоставлять услугу регистрации.

1 Sertifikatlar subyektlarini identifikatsiyalash va autentifikatsiya qilish yuzasidan javobgar, biroq, sertifikatlash organi ham, atributlar berish organi ham bo‘lmagan qandaydir obyekt.

О

2 Ro'yxatga olish xizmatini taqdim etish huquqi berilgan va ishonib topshirilgan organ.

1 Сертификатлар субъектларини идентификациялаш ва аутентификация қилиш юзасидан жавобгар, бироқ, сертификатлаш органи ҳам, атрибутлар бериш органи ҳам бўлмаган қандайдир объект.

2 Рўйхатга олиш хизматини тақдим этиш ҳуқуқи берилган ва ишониб топширилган орган.

Орган режимно-секретный (PCO)

uz - maxfiy-rejimli organ

(MRO)

махфий-режимли орган

(MPO)

en - regime and secret authority

(RSA)

Самостоятельное структурное подразделение, разрабатывающее и осуществляющее мероприятия по обеспечению режима секретности и проводящее постоянный контроль за его соблюдением в организациях, где ведутся секретные работы.

Maxfiylik rejimini ta'minlash bo'yicha tadbirlarni ishlab chiquvchi va amalga oshiruvchi hamda maxfiy ishlar yuritiladigan tashkilotlarda unga rioya qilinishini muntazam tekshirib turadigan mustaqil tashkiliy bo'linma.

Махфийлик режимини таъминлаш бўйича тadbirlарни ишлаб чиқувчи ва амалга оширувчи ҳамда махфий ишлар юритиладиган ташкilotларда унга rioya қилинишини мунтазам текшириб турадиган мустақил ташкилий бўлинма.

Орган руководящий

uz - rahbarlik qiluvchi organ

раҳбарлик қилувчи орган

en - governing body

Физическое лицо или группа лиц, ответственных за соответствующие результаты деятельности организации.

Примечание – Руководящим органом может быть совет директоров.

Tashkilot faoliyatining tegishli natijalari uchun javobgar jismoniy shaxs yoki shaxslar guruhi.

Izoh – Direktorlar kengashi rahbarlik qiluvchi organ bo'lishi mumkin.

Ташкilot фаолиятининг тегишли натижалари учун жавобгар жисмоний шахс ёки шахслар гуруҳи.

Изоҳ – Директорлар кенгаши раҳбарлик қилувчи орган

О

бўлиши мумкин.

Орган сертификации

uz - sertifikatlash organi

сертификатлаш органи

en - certification authority

1 Орган, которому одним или более пользователями доверено создавать и распределять сертификаты открытых ключей.

2 Объект, которому доверено (в контексте политики обеспечения безопасности) создавать сертификаты безопасности, содержащие один или более классов данных, относящихся к обеспечению безопасности.

1 Bitta yoki bir nechta foydalanuvchi tomonidan ochiq kalitlar sertifikatlarini tuzish va taqsimlash ishonib topshirilgan organ.

2 Xavfsizlikni ta'minlashga taalluqli bo'lgan ma'lumotlarning bitta yoki undan ortiq klassini ichiga olgan xavfsizlik sertifikatlarini tuzish ishonib topshirilgan obyekt (xavfsizlikni ta'minlash siyosati kontekstida).

1 Битта ёки бир нечта фойдаланувчи томонидан очик калитлар сертификатларини тузиш ва тақсимлаш ишониб топширилган орган.

2 Хавфсизликни таъминлашга тааллуқли бўлган маълумотларнинг битта ёки undan ortiq klassini ichiga olgan xavfsizlik sertifikatlarini tuzish ishonib topshirilgan obyekt (xavfsizlikni ta'minlash siyosati kontekstida).

Организация

uz - tashkilot

ташкilot

en - organization

Физическое лицо или группа лиц, выполняющие определенные функции, несущие определенную ответственность, а также обладающие определенными полномочиями и взаимоотношениями, необходимыми для достижения определенных целей.

Muayyan funksiyalarni bajaruvchi, ma'lum javobgarlik yuklangan, shuningdek, muayyan maqsadlarga erishish uchun vakolatlar va o'zaro munosabatlarga ega bo'lgan jismoniy shaxs yoki shaxslar guruhi.

Муайян функцияларни бажарувчи, маълум жавобгарлик юкланган, шунингдек, муайян мақсадларга эришиш учун ваколатлар ва ўзаро муноса-

О

батларга эга бўлган жисмоний шахс ёки шахслар гуруҳи.

Ответ ожидаемый

uz - kutilgan javob

кутилган жавоб

en - expected response, XRES

Отклик, вычисляемый в сети с использованием того же алгоритма, что и ответ мобильной станции. Если XRES и SRES совпадают, то аутентификация завершается успешно.

Mobil stansiyaning javobi kabi algoritmdan foydalanib, tarmoqda hisoblab chiqariladigan javob. Agar XRES va SRES mos kelsa, autentifikatsiya qilish muvaffaqiyatli tugaydi.

Мобил станциянинг жавоби каби алгоритмдан фойдаланиб, тармоқда ҳисоблаб чиқариладиган жавоб. Агар XRES ва SRES мос келса, аутентификация қилиш муваффақиятли тугайди.

Отказ в обслуживании

uz - xizmat ko'rsatishni

rad etish

хизмат кўрсатишни

рад этиш

en - denial of service

1 Прекращение санкционированного доступа к ресурсам или задержка выполнения операций, критичных ко времени.

2 Любое действие или последовательность действий, которая приводит любую часть системы к выходу из строя, при котором та перестаёт выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т.д.

3 Отказ в предоставлении ресурсов законным пользователям вследствие нарушения режима сетевого обслуживания. Обычно возникает при введении в сеть фиктивного трафика или ложных запросов, которые хотя и отбрасываются, но загружают сеть ненужной информацией.

1 Resurslardan ruxsat etilgan tarzda foydalana olishning to'xtatilishi yoki vaqtga nisbatan kritik operat-siyalar bajarilishining kechikishi.

2 Tizimning har qanday qismini safdan chiqaradigan va bunda tizim o'z funksiyalarini bajarishni to'xtatadigan har qanday harakat yoki harakatlar ketma-ketligi. Buning sababi, ruxsat etilmagan tarzda foydalana olish, xizmat ko'rsatishdagi kechikishlar va b.q. bo'lishi mumkin.

3 Tarmoq xizmat ko'rsatish rejimining buzilishi natijasida resurslarning qonuniy foydalanuvchilarga taqdim etilishini rad etish. Odatda, tarmoqqa soxta trafik

О

yoki yolg'on so'rovlar kiritilganda paydo bo'ladi, garchi ular olib tashlansada, tarmoqni keraksiz axborot bilan band qilib qo'yadi.

1 Ресурслардан рухсат этилган тарзда фойдалана олишнинг тўхтатилиши ёки вақтга нисбатан критик операциялар бажарилишининг кечикиши.

2 Тизимнинг ҳар қандай қисмини сафдан чиқарадиган ва бунда тизим ўз функцияларини бажаришни тўхтатадиган ҳар қандай ҳаракат ёки ҳаракатлар кетма-кетлиги. Бунинг сабаби, рухсат этилмаган тарзда фойдалана олиш, хизмат кўрсатишдаги кечикишлар ва б.к. бўлиши мумкин.

3 Тармоқ хизмат кўрсатиш режимининг бузилиши натижасида ресурсларнинг қонуний фойдаланувчиларга тақдим этилишини рад этиш. Одатда, тармоққа сохта трафик ёки ёлғон сўровлар киритилганда пайдо бўлади, гарчи улар олиб ташлансада, тармоқни кераксиз ахборот билан банд қилиб қўяди.

Нарушение работы сети, обусловленное одновременной атакой злоумышленников на разные ее элементы, производимой с большого числа компьютеров.

Tarmoq ishining jinoyatkorlarning, ko'p sonli kompyuterlardan chiqariladigan tarmoqning turli elementlariga bir vaqtda hujum qilishi bilan bog'liq bo'lgan buzilishi.

Тармоқ ишининг жинояткорларнинг, кўп сонли компьютерлардан чиқариладиган тармоқнинг турли элементларига бир вақтда хужум қилиши билан боғлиқ бўлган бузилиши.

Отрицание причастности к какому-либо документу или сообщению.

Qandaydir hujjat yoki xabarga aloqadorlikni rad etish.

Қандайдир хужжат ёки хабарга алоқадорликни рад этиш.

Ответ мобильной станции на полученное случайное число RAND.

Отказ в обслуживании распределенный

uz - xizmat ko'rsatishni taqsimlangan rad etish

хизмат кўрсатишни тақсимланган рад этиш

en - distributed denial of service

Отказ от авторства

uz - mualliflikni rad etish

муаллифликни рад этиш

en - refusal of authorship

Отклик ожидаемый

uz - kutilgan javob

кутилган жавоб

О

en - signer response

Olingan *RAND* tasodifiy soniga mobil stansiyaning javobi.

Олинган *RAND* тасодифий сонига мобил станциянинг жавоби.

Отладчик

uz - sozlovchi

созловчи

en - debugger

Программа или устройство, предназначенные для выявления ошибок в программном обеспечении.

Dasturiy ta'minotdagi xatolarni aniqlash uchun mo'ljallangan dastur yoki qurilma.

Дастурий таъминотдаги хатоларни аниқлаш учун мўлжалланган дастур ёки қурилма.

Отношение

uz - munosabat

муносабат

en - relationship

Воспринимаемая связь между объектами в предметной области.

Predmet sohasidagi obyektlar o'rtasida qabul qilinadigan aloqadorlik (bog'lanish).

Предмет соҳасидаги объектлар ўртасида қабул қилинадиган алоқадорлик (боғланиш).

Отношения доверительные

uz - ishonchli munosabatlar

ишончли муносабатлар

en - trust relationships

Несимметричная логическая связь между двумя доменами, позволяющая системе безопасности одного домена (доверяющего, *trusting*) использовать в качестве субъектов учетные записи другого домена (доверяемого, *trusted*).

Ikki domen o'rtasidagi, bir domen (ishonuvchi, *trusting*) xavfsizlik tizimiga boshqa domen (ishonch bildirilayotgan, *trusted*) hisob yozuvlaridan subyekt sifatida foydalanish imkonini beradigan nosimmetrik mantiqiy aloqa.

Икки домен ўртасидаги, бир домен (ишонувчи, *trusting*) хавфсизлик тизимига бошқа домен (ишонч билдирилаётган, *trusted*) ҳисоб ёзувларидан субъект сифатида фойдаланиш имконини берадиган носимметрик мантикий алоқа.

«Отпечаток» цифровой

uz - raqamli «iz»

рақамли «из»

en - digital fingerprint

Характеристика элемента данных, например, криптографическое контрольное значение или результат выполнения односторонней функции хэширования в отношении данных.

О

Ma'lumotlar elementining xarakteristikasi, masalan, kriptografik nazorat qiymati yoki ma'lumotlarga nisbatan bir tomonlama xeshlash funksiyasini bajarish natijasi.

Маълумотлар элементининг хактеристикаси, масалан, криптографик назорат қиймати ёки маълумотларга нисбатан бир томонлама хэшлаш функциясини бажариш натижаси.

Оценка

uz - baho

баҳо

en - evaluation

Оценка профиля защиты, задания по безопасности или объекта оценки по определенным критериям.

Xavfsizlik bo'yicha topshiriq yoki baholash obyektining muayyan kriteriyalar bo'yicha himoya profilining bahosi.

Хавфсизлик бўйича топшириқ ёки баҳолаш объектининг муайян критерийлар бўйича ҳимоя профилининг баҳоси.

Оценка безопасности

uz - xavfsizlikni baholash

хавфсизликни баҳолаш

en - security evaluation

Проверка системы с целью определения степени ее соответствия установленной модели защиты, стандарту обеспечения защиты и техническим условиям.

Tizimni, belgilangan muhofaza modeliga, muhofaza qilishni ta'minlash standarti va texnik shartlarga mos kelish darajasini aniqlash maqsadida tekshirish.

Тизимни, белгиланган муҳофаза моделига, муҳофаза қилишни таъминлаш стандарти ва техник шартларга мос келиш даражасини аниқлаш мақсадида текшириш.

Оценка качества

программного изделия

uz - dasturiy mahsulot sifatini baholash

дастурий маҳсулот

сифатини баҳолаш

en - program quality estimation

Комплекс мероприятий, включающий выбор показателей качества, отбор или разработку методов определения количественных значений этих показателей, установление базовых значений показателей, расчет реальных значений показателей, сравнение базовых значений с расчетными.

Sifat ko'rsatkichlari tanlanishini, bu ko'rsat-kich-

O

larning miqdor qiymatlarini tanlash va aniqlash metodlari ishlab chiqilishini, ko'rsatkichlarning bazaviy qiymatlari belgilanishini, ko'rsatkichlarning haqiqiy qiymatlarini hisoblash, bazaviy qiymatlarni hisoblangan qiymatlar bilan taqqoslashni ichiga oladigan tadbirlar kompleksi.

Сифат кўрсаткичлари танланишини, бу кўрсаткичларнинг миқдор қийматларини танлаш ва аниқлаш методлари ишлаб чиқилишини, кўрсаткичларнинг базавий қийматлари белгиланишини, кўрсаткичларнинг ҳақиқий қийматларини ҳисоблаш, базавий қийматларни ҳисобланган қийматлар билан таққослашни ичига оладиган тadbirlar комплекси.

Оценка риска

uz - riskni baholash

рискни баҳолаш

en - risk evaluation

1 Процесс сравнения результатов анализа риска с критериями риска для определения риска и/или приемлемости, или допустимости его величины.

Примечание – Сравнительная оценка риска может быть использована при принятии решения об обработке риска.

2 Метод анализа угроз и слабых сторон, известных и предполагаемых, позволяющий определить размер ожидаемого ущерба и степень его приемлемости для работы системы (сети).

3 Идентификация рисков, выбор параметров для их описания и получения оценок по этим параметрам.

1 Riskni tahlil qilish natijalarini risk va/yoki uning kattaligi maqbul yoki yo'l qo'yib bo'lishligini aniqlash uchun risk kriteriyalari bilan taqqoslash jarayoni.

Izoh – Riskni qiyosiy baholashdan riskni qayta ishlash to'g'risida qaror qabul qilishda foydalanilishi mumkin.

2 Ma'lum bo'lgan va taxmin qilinayotgan tahdidlar va zaif tomonlarni tahlil qilish metodi. Kutilayotgan zarar miqdorini va uning tizim ishi uchun maqbullik darajasini aniqlash imkonini beradi.

3 Risklarni identifikatsiya qilish, ularni tavsiflash uchun parametrlar tanlash va bu parametrlar bo'yicha baho olish.

1 Riskni taхлил қилиш натижаларини риск ва/ёки унинг катталиги мақбул ёки йўл қўйиб бўлишлигини аниқлаш учун риск критерийлари

О

билан таққослаш жараёни.

Изоҳ – Рискни қиёсий баҳолашдан рискни қайта ишлаш тўғрисида қарор қабул қилишда фойдаланилиши мумкин.

2 Маълум бўлган ва тахмин қилинаётган таҳдидлар ва заиф томонларни таҳлил қилиш методи. Кутилаётган зарар миқдорини ва унинг тизим иши учун мақбуллик даражасини аниқлаш имконини беради.

3 Рискларни идентификация қилиш, уларни тавсифлаш учун параметрлар танлаш ва бу параметрлар бўйича баҳо олиш.

Очистка

uz - tozalash

тозалаш

en - clearing

Перезапись категорированных данных на носитель данных, имеющий определенный гриф секретности и категорию защиты, для того, чтобы этот носитель данных можно было неоднократно использовать для записи данных, имеющих тот же самый гриф секретности и категорию защиты.

Kategoriyalashtirilgan ma'lumotlarni muayyan maxfiylik grifiga hamda muhofaza qilish kategoriyasiga ega bo'lgan ma'lumot tashuvchiga, uni xuddi shunday maxfiylik grifi va muhofaza qilish kategoriyasidagi ma'lumotlarni bir necha marta yozib olishda foydalanish mumkin bo'lishi uchun, qayta yozish.

Категориялаштирилган маълумотларни муайян махфийлик грифига ҳамда муҳофаза қилиш категориясига эга бўлган маълумот ташувчига, уни худди шундай махфийлик грифи ва муҳофаза қилиш категориясидаги маълумотларни бир неча марта ёзиб олишда фойдаланиш мумкин бўлиши учун, қайта ёзиш.

Ошибка (преднамеренная) умышленная

uz - ataylab (qasddan) qilingan
хато

атайлаб (қасддан)

қилинган хато

en - intentional error

Ошибка, преднамеренно внесенная в программу или данные.

Dastur yoki ma'lumotlarga qasddan kiritilgan xato.

Дастур ёки маълумотларга қасддан киритилган хато.

Ошибка данных

uz - ma'lumotlarning xatoligi

маълумотларнинг

Ошибочное представление одного или нескольких исходных данных, которое может стать причиной аварийного завершения программы либо

О

хатолиги

en - data error

оказаться необнаруженным, но результаты нормально завершившейся программы будут при этом неверными.

Bitta yoki bir nechta boshlang'ich ma'lumotning xato taqdim etilishi. Dastur avariya viy tugallanishiga sababchi bo'lishi yoki aniqlanmay qolishi mumkin, ammo normal tugallangan dastur natijalari bu holda noto'g'ri bo'ladi.

Битта ёки бир нечта бошланғич маълумотнинг хато тақдим этилиши. Дастур авариявий тугалланишига сабабчи бўлиши ёки аниқланмай қолиши мумкин, ammo нормал тугалланган дастур натижалари бу ҳолда нотўғри бўлади.

Ошибка кратковременная

uz - qisqa muddatli xato

қисқа муддатли хато

en - soft error

Ошибка из-за случайных обстоятельств, сбой.

Tasodifiy holatlar, natijasida yuzaga keladigan xato, uzilish.

Тасодифий ҳолатлар, натижасида юзага келадиган хато, узилиш.

Ошибка

невосстанавливаемая

uz - tiklab bo'lmaydigan xato

тиклаб бўлмайдиган хато

en - unrecoverable error

Ошибка, последствия которой не могут быть устранены средствами вычислительной системы автоматически и требуют вмешательства оператора.

Oqibatlarini hisoblash tizimi vositalari bilan avtomatik ravishda bartaraf etib bo'lmaydigan, operatorning aralashuvi talab etiladigan xato.

Оқибатларини ҳисоблаш тизими воситалари билан автоматик равишда бартараф этиб бўлмайдиган, операторнинг аралашуви талаб этиладиган хато.

Ошибка некорректируемая

uz - tuzatib bo'lmaydigan xato

тузатиб бўлмайдиган хато

en - uncorrectable error

Ошибка в сообщении, которая не может быть исправлена средствами корректирующего кода.

Xabardagi, tuzatuvchi kod vositalari bilan tuzatish mumkin bo'lmagan xato.

Хабардаги, тузатувчи код воситалари билан тузатиш мумкин бўлмаган хато.

Ошибка неповторяющаяся

Несистематическая ошибка, возникающая вслед-

О

(нерегулярная, перемежающаяся, случайная)

uz - takrorlanmaydigan (munta-zam bo'lmagan, vaqt-vaqti bilan uchraydigan, tasodifiy) xato

такропланмайдиган

(мунтазам бўлмаган, вақт-вақти билан учрайдиган, тасодифий) хато

en - temporary (intermittent, soft, transient) error

Ошибка семантическая

uz - semantik xato

семантик хато

en - semantic error

Ошибка фатальная

uz - fatal xato

фатал хато

en - fatal error

Ошибка четности

uz - juftlik xatosi

жуфтлик хатоси

en - parity error

ствии самоустраняющихся машинных отказов, сбоев и других случайных обстоятельств.

О'з-о'зидан бартараф бўладиган машина бузилишлари, то'хтаб қолишлар ва бoшқа тасодифий ҳолатлар оқибатда пайдо бўлувчи номунтазам хато.

Ўз-ўзидан бартараф бўладиган машина бузилишлари, тўхтаб қолишлар ва бошқа тасодифий ҳолатлар оқибатида пайдо бўлувчи номунтазам хато.

Ошибка программирования, возникающая из-за непонимания смысла, значения или действия той или иной конструкции программирования.

Dasturlashdagi xato dasturlash u yoki bu konstruk-siyasining ma'nosini, ahamiyatini yoki ishini tushun-maslik tufayli yuzaga keladi.

Дастурлашдаги хато дастурлаш у ёки бу конст-рукциясининг маъносини, аҳамиятини ёки иши-ни тушунмаслик тўфайли юзага келади.

Ошибка, при появлении которой дальнейшее вы-полнение программы приводит к бессмысленным результатам.

Paydo bo'lishi dasturning bajarilishida noaniq (ma'-nosiz) natijalarga olib keladigan xato.

Пайдо бўлиши дастурнинг бажарилишида ноаниқ (маъносиз) натижаларга олиб келадиган хато.

Ошибка в данных, обнаруживаемая в процессе их хранения или передачи путем контроля на четность.

Ma'lumotlardagi, ularni saqlash yoki juftlikni nazorat qilish orqali uzatish jarayonida aniqlanadigan xato.

Маълумотлардаги, уларни сақлаш ёки жуфтлик-ни назорат қилиш орқали узатиш жараёнида аниқланадиган хато.

П

П

Пакет

uz - paket

пакет

en - package

1 Поименованная группа функциональных требований безопасности или требований доверия.

Примечание – Примерами пакетов доверия являются оценочные уровни доверия.

2 Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия.

1 Xavfsizlikning funksional talablari yoki ishonch talablarining nomma-nom ko‘rsatilgan guruhlari.

Izoh – Ishonch paketlariga misol bo‘lib, ishonchni baholovchi darajalari hisoblanadi.

2 Ko‘p marta foydalanishga mo‘ljallangan funksional komponentlar yoki ishonch komponentlarining yig‘indisi.

1 Xavfsizlikning funksional talablari ёки ишонч талабларининг номма-ном кўрсатилган гурухлари.

Изоҳ – Ишонч пакетларига мисол бўлиб, ишончни баҳоловчи даражалари ҳисобланади.

2 Кўп марта фойдаланишга мўлжалланган функционал компонентлар ёки ишонч компонентларининг йиғиндиси.

Пакет доверия составной

uz - tarkibiy ishonch paketi

таркибий ишонч пакети

en - composed assurance package

Пакет доверия, включающий требования доверия к безопасности (в основном требования класса АСО) и занимающий некоторое положение на заданной в шкале доверия.

Xavfsizlikning ishonch talablari bo‘lgan, (asosan, ASO klassi talablari) va ishonch shkalasida joylashgan ishonch paketi.

Xavfsizlikning ishonch talablari бўлган, (асосан, АСО класси талаблари) ва ишонч шкаласида жойлашган ишонч пакети.

Пакеты-убийцы

uz - qotil paketlar

қотил пакетлар

en - packets - killer

Метод вывода из строя информационной системы путем посылки ей Ethernet- или IP-пакетов, которые используют ошибки в сетевых программах для аварийного завершения работы этой системы.

Tizimning ishini avariyaaviy tugatish uchun tarmoq dasturlaridagi xatolardan foydalanadigan *Ethernet* yoki *IP*-paketlarini yuborish yo‘li bilan, axborot

II

tizimini ishdan chiqarish metodi.

Тизимнинг ишини авариявий тугатиш учун тармоқ дастурларидаги хатолардан фойдаланадиган Ethernet ёки IP-пакетларини юбориш йўли билан, ахборот тизимини ишдан чиқариш методи.

Память с защитой

uz - himoyaga ega хотира

химояга эга хотира

en - protected storage

Память, имеющая специальные средства защиты от несанкционированного доступа к любой из ее ячеек.

Istalgan yacheykasiga ruxsat etilmagan tarzda kira olishdan muhofaza qiluvchi maxsus vositalari bo'lgan хотира.

Исталган ячейкасига рухсат этилмаган тарзда кира олишдан муҳофаза қилувчи махсус воситалари бўлган хотира.

Память только для записи

uz - faqat yozish uchun хотира

фақат ёзиш учун хотира

en - write - only memory

Тип памяти со следующими свойствами: после записи новой информации прежняя может быть восстановлена только с помощью внутренних механизмов самого чипа; данные никогда не распространяются за пределы чипа и не могут появиться на шинах, внешних по отношению к чипу.

Yangi axborot yozilgandan so'ng oldingisi faqat chipning ichki mexanizmlari yordamida tiklanishi mumkin bo'lgan; ma'lumotlar hech qachon chipdan tashqarida tarqatilmaydigan va chipga nisbatan tashqi hisoblanadigan shinalarda paydo bo'lmaydigan хотира turi.

Янги ахборот ёзилгандан сўнг олдингиси фақат чипнинг ички механизмлари ёрдамида тикланиши мумкин бўлган; маълумотлар ҳеч қачон чипдан ташқарида тарқатилмайдиган ва чипга нисбатан ташқи ҳисобланадиган шиналарда пайдо бўлмайдиган хотира тури.

Паролирование

uz - parollashtirish

пароллаштириш

en - determination of password

Один из методов ограничения доступа к компьютерной системе и ее файлам.

Kompyuter tizimi va uning fayllariga kira olishni cheklash metodlaridan biri.

П

Компьютер тизими ва унинг файлларига кира олишни чеклаш методларидан бири.

Пароль

uz - parol

пароль

en - password

1 Последовательность символов, которая используется как информация аутентификации.

2 Идентификатор субъекта доступа, являющийся его (субъекта) секретом.

3 Секретная информация аутентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

4 Средство идентификации доступа, представляющее собой кодовое слово в буквенной, цифровой или буквенно-цифровой форме, которое вводится в ЭВМ перед началом диалога с ней с клавиатуры терминала или при помощи идентификационной (кодовой) карты.

1 Autentifikatsiya qilish axboroti sifatida foydalaniladigan belgilar ketma-ketligi.

2 Erkin foydalanish subyektining identifikatori bo'lib, subyektning siri hisoblanadi.

3 Foydalanuvchining muhofaza qilingan ma'lumotlardan erkin foydalanishi uchun ega bo'lishi kerak bo'lgan belgilar satrini o'zida aks ettiruvchi maxfiy autentifikatsiya qilish axboroti.

4 Elektron hisoblash mashinasiga terminal klaviaturasidan yoki identifikatsion (kodli) karta yordamida kiritiladigan, harf, harf-raqam yoki raqam shaklidagi kodli so'zni o'zida ifodalovchi, erkin foydalanishni identifikatsiyalovchi vosita.

1 Аутентификация қилиш ахбороти сифатида фойдаланиладиган белгилар кетма-кетлиги.

2 Эркин фойдаланиш субъектининг идентификатори бўлиб, субъектнинг сирини ҳисобланади.

3 Фойдаланувчининг муҳофаза қилинган маълумотлардан эркин фойдаланиши учун эга бўлиши керак бўлган белгилар сатрини ўзида акс эттирувчи махфий аутентификация қилиш ахбороти.

4 Электрон ҳисоблаш машинасига терминал клавиатурасидан ёки идентификацион (кодли) карта ёрдамида киритиладиган, ҳарф, ҳарф-рақам

П

ёки рақам шаклидаги кодли сўзни ўзида ифодаловчи, эркин фойдаланишни идентификацияловчи восита.

Пароль главный

uz - asosiy parol
асосий пароль
en - main password

1 Корневое слово, являющееся общим для определенного набора паролей.
2 Пароль, предназначенный для защиты каталога паролей.

1 Parollarning ma'lum bir to'plami uchun umumiy bo'lgan o'zak so'z.
2 Parollar katalogini muhofaza qilish uchun mo'ljallangan parol.

1 Паролларнинг маълум бир тўплами учун умумий бўлган ўзак сўз.
2 Пароллар каталогини муҳофаза қилиш учун мўлжалланган пароль.

Пароль одноразовый

uz - bir martali parol
бир мартали пароль
en - single-use password

Пароль с очень коротким сроком действия, обычно изменяемый после каждого входа в сеть.

Tarmoqqa har bir kirishdan so'ng o'zgaradigan, amal qilish muddati juda qisqa bo'lgan parol.

Тармоққа ҳар бир киришдан сўнг ўзгарадиган, амал қилиш муддати жуда қисқа бўлган пароль.

Пассивное скрятие

uz - passiv yashirish
пассив яшириш
en - passive hiding

Способ технической защиты информации, состоящий в ослаблении энергетических характеристик сигналов, полей или в уменьшении концентраций веществ.

Axborotni texnik muhofaza qilish usuli, signallar, maydonlar energetik xarakteristikalarini susaytirish yoki moddalar konsentratsiyasini kamaytirishdan iborat.

Ахборотни техник муҳофаза қилиш усули, сигналлар, майдонлар энергетик характеристикаларини сусайтириш ёки моддалар концентрациясини камайтиришдан иборат.

Перебор номеров

циклический
uz - raqamlarni siklik

Скрытное клонирование с циклическим перебором номеров телефонов-двойников, при котором каждый последующий вызов осуществляется с новым

II

saralash
рақамларни циклик
саралаш
en - tumbling

номером.

O‘xshash telefonlarning raqamlarini siklik saralash bilan yopiq klonlash, unda har bir keyingi chaqiruv yangi raqam bilan amalga oshiriladi.

Ўхшаш телефонларнинг рақамларини циклик саралаш билан ёпиқ клонлаш, унда ҳар бир кейинги чақирув янги рақам билан амалга оширилади.

Перебор полный
uz - to‘liq saralash
тўлиқ саралаш
en - exhaustive search

Основной метод поиска правильного криптографического ключа из множества всех возможных ключей путем его полного перебора. Число возможных ключей можно сократить, если найдены уязвимости алгоритма шифрования или выработки ключей.

To‘g‘ri kriptografik kalitni barcha mumkin bo‘lgan kalitlar ichidan uni to‘liq saralash yo‘li bilan izlashning asosiy metodi. Shifrlash algoritmi yoki kalitlarni ishlab chiqishda zaifliklar topilganda, kalitlar sonini qisqartirish mumkin bo‘ladi.

Tўғри криптографик калитни барча мумкин бўлган калитлар ичидан уни тўлиқ саралаш йўли билан излашнинг асосий методи. Шифрлаш алгоритми ёки калитларни ишлаб чиқишда заифликлар топилганда, калитлар сонини қисқартириш мумкин бўлади.

**Передача в пределах
объекта оценки**
uz - baholash obykti
doirasida uzatish
баҳолаш объекти
доирасида узатиш
en - internal target of
evaluation transfer

Передача данных между разделенными частями объекта оценки.

Ma‘lumotlarni baholash obyektining bo‘lingan qismlari orasida uzatish.

Маълумотларни баҳолаш объектининг бўлинган қисмлари орасида узатиш.

II

Передача за пределы объекта оценки

uz - baholash obyektini doirasidan tashqariga uzatish

баҳолаш объекти

доирасидан ташқарига узатиш

en - transfers outside of the target of evaluation

Опосредованная ФБО передача данных логическим объектам, не контролируемым ФБО.

OXF nazorat qilmaydigan, mantiqiy obyektlarga OXF bevosita ifodalangan ma'lumotlarni uzatish.

OXF nazorat qilmaydigan, mantiqiy obyektlarga OXF bevosita ifodalangan ma'lumotlarni uzatish.

Передача между функциями безопасности объекта оценки

uz - baholash obyektini xavfsizlik funksiyalari orasida uzatish

баҳолаш объектини

хавфсизлик функциялари

орасида узатиш

en - inter target security functions of evaluation transfers

Передача данных между объектом оценки и функциональными возможностями безопасности других доверенных продуктов ИТ.

Ma'lumotlarni baholash obyektini hamda ATning boshqa ishonchli mahsulotlari xavfsizligining funksional imkoniyatlari orasida uzatish.

Ma'lumotlarni baholash obyektini hamda ATning boshqa ishonchli mahsulotlari xavfsizligining funksional imkoniyatlari orasida uzatish.

Передача права

uz - huquqni berish

хуқуқни бериш

en - assignment of right

Законная передача владельцем права интеллектуальной собственности другому лицу.

Intellektual mulkchilik huquqining egasi tomonidan boshqa shaxsga qonuniy berilishi.

Интеллектуал мулкчилик ҳуқуқининг эгаси томонидан бошқа шахсга қонуний берилиши.

Перемешивание

uz - aralash tirib yuborish

аралаштириб юбориш

en - confusion

Свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифротекстом.

Shifrovchi o'zgartirishning ma'lumotlar elementlari o'rtasidagi aloqadorlikni murakkablashtirish xossasi. Bu narsa, ochiq matn, kalit va shifrmavn o'rtasidagi funksional va statistik bog'lanishning tiklanishini qiyinlashtiradi.

Шифрловчи ўзгартиришнинг маълумотлар эле-

П

ментлари ўртасидаги алоқадорликни мураккаб-лаштириш хоссаси. Бу нарса, очик матн, калит ва шифрматн ўртасидаги функционал ва статистик боғланишнинг тикланишини қийинлаштиради.

Переполнение

uz - to‘lib ketish

тўлиб кетиш

en - overflow

Случайный или умышленный ввод большого объема данных, результатом которого является отказ в обслуживании.

Ma'lumotlarning katta hajmini tasodifan yoki qasddan kiritish, uning natijasida xizmat ko'rsatishning rad etilishi yuz beradi.

Ma'lumotlarning katta hajmini tasodifan yoki qasddan kiritish, uning natijasida xizmat ko'rsatishning rad etilishi yuz beradi.

Переполнение-SYN

uz - SYN to‘lib ketish

SYN тўлиб кетиш

en - SYN overflow

Метод вывода системы из строя путем послыки ей такого числа SYN-пакетов, которое не может обработать сетевой драйвер.

Tarmoq drayveri qayta ishlay olmaydigan miqdorda SYN paketlarni yuborish orqali tizimni ishdan chiqarish metodi.

Tarmoq drayveri qayta ishlay olmaydigan miqdorda SYN paketlarni yuborish orqali tizimni ishdan chiqarish metodi.

Перестановка

uz - o‘rnini (tartibini)

almashtirish

ўрнини (тартибини)

алмаштириш

en - permutation

1 Криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

2 Шифрование, при котором биты или символы переставляются по некоторой схеме.

Примечание – Полученный шифротекст называется шифром перестановки.

1 Ma'lumotlar blokidagi ayrim bitlar yoki simvolarning o'tish tartibini o'zgartirish bilan bog'liq kriptografik operatsiya.

2 Bitlar yoki belgilar ma'lum sxema bo'yicha almashtiriladigan shifrlash.

Izoh – Olingan shifratn o'rnini almashtirish shifri deb ataladi.

II

1 Маълумотлар блокадаги айрим битлар ёки символларнинг ўтиш тартибини ўзгартириш билан боғлиқ криптографик операция.

2 Битлар ёки белгилар маълум схема бўйича алмаштириладиган шифрлаш.

Изоҳ – Олинган шифрматн ўрнини алмаштириш шифри деб аталади.

Перехват информации

uz - axborotni qo‘lga kiritish

ахборотни қўлга киритиш

en - wiretapping

Тайное подключение нелегального устройства к какой-либо части линии телекоммуникаций, чтобы получать, модифицировать или вставлять данные.

Ma'lumotlarni olish, o'zgartirish yoki kiritish maqsadida, telekommunikatsiyalar liniyasining biror-bir qismiga yashirin qurilmani bildirmasdan ulash.

Маълумотларни олиш, ўзгартириш ёки киритиш мақсадида, телекоммуникациялар линиясининг бирор-бир қисмига яширин қурилмани билдирмасдан улаш.

Перехват информации

активный

uz - axborotni aktiv

tutib qolish

ахборотни актив

тутиб қолиш

en - active wiretapping

Подключение нелегального устройства к линии телекоммуникаций с целью модифицировать или вставить данные.

Ma'lumotlarni o'zgartirish yoki kiritish maqsadida, telekommunikatsiyalar liniyasiga yashirin qurilmani ulash.

Маълумотларни ўзгартириш ёки киритиш мақсадида, телекоммуникациялар линиясига яширин қурилмани улаш.

Перехват информации

пассивный

uz - axborotni passiv

tutib qolish

ахборотни пассив

тутиб қолиш

en - passive wiretapping

Подключение нелегального устройства к линии телекоммуникаций для получения данных.

Ma'lumotlar olish maqsadida telekommunikatsiyalar liniyasiga yashirin qurilmani ulash.

Маълумотлар олиш мақсадида телекоммуникациялар линиясига яширин қурилмани улаш.

Перехват сообщений

uz - xabarlarni tutib qolish

хабарларни тутиб қолиш

en - message wiretapping

Несанкционированное подключение специального терминала к линии телекоммуникаций, прием и использование сообщений, циркулирующих между абонентскими пунктами и ЭВМ.

Maxsus terminalni telekommunikatsiyalar liniyasiga

II

ruxsatsiz ulash, abonent punktlari bilan EHM o'rtasida aylanadigan xabarlarini qabul qilish va ulardan foydalanish.

Махсус терминални телекоммуникациялар линиясига рухсатсиз улаш, абонент пункtlари билан ЭХМ ўртасида айланадиган хабарларни қабул қилиш ва улардан фойдаланиш.

Перечень сведений, подлежащих засекречиванию

uz - maxfiylashtirilishi zarur bo'lgan ma'lumotlar ro'yxati

махфийлаштирилиши зарур бўлган маълумотлар рўйхати

en - list of information to be classified as secret

Документ, утвержденный в установленном порядке, определяющий степень секретности сведений, разглашение которых может нанести ущерб интересам Республики Узбекистан.

Belgilangan tartibda tasdiqlangan, tarqatilishi O'zbekiston Respublikasi manfaatlariga ziyon yetkazishi mumkin bo'lgan ma'lumotlarning maxfiylik darajasini belgilovchi hujjat.

Белгиланган тартибда тасдиқланган, тарқатилиши Ўзбекистон Республикаси манфаатларига зиён етказиши мумкин бўлган маълумотларнинг махфийлик даражасини белгиловчи ҳужжат.

Период действия ключа

uz - kalitning amal qilish davri kalitning amal qilish davri

даври

en - life cycle

Интервал времени, в течение которого гарантируется необходимая защищенность без смены криптографического ключа.

Vaqt intervali, uning mobaynida kriptografik kalit almashtirilmasdan, zarur muhofazalanganlik kafolatlanadi.

Вақт интервали, унинг мобайнида криптографик калит алмаштирилмасдан, зарур муҳофазаланганлик кафолатланади.

Период доступа

uz - foydalanish davri

фойдаланиш даври

en - access period

Временной интервал, в течение которого действуют права доступа.

Foydalanish uchun ko'rsatilgan huquqlar amal qiladigan vaqt intervali.

Фойдаланиш учун кўрсатилган ҳуқуқлар амал қиладиган вақт интервали.

Печать

uz - muhr

муҳр

en - seal

Криптографическое контрольное значение, которое обеспечивает поддержку целостности, но не защищает от подлога, осуществляемого получателем (т.е. не обеспечивает фиксацию авторства).

II

Kriptografik nazorat qiymati bo‘lib, yaxlitlik saqlanib turishini ta‘minlaydi, lekin oluvchi tomonidan amalga oshiriladigan qalbakilashtirishdan muhofaza qila olmaydi (ya‘ni, mualliflik qayd etilishini ta‘minlay olmaydi).

Криптографик назорат қиймати бўлиб, яхлитлик сақланиб туришини таъминлайди, лекин олувчи томонидан амалга ошириладиган қалбакилаштиришдан муҳофаза қила олмайди (яъни, муаллифлик қайд этилишини таъминлай олмайди).

Пиггибекинг физический

uz - jismoniy piggibeking
жисмоний пиггибекинг
en - to tailgate

Несанкционированный проход через контролируемую дверь вслед за полномочным лицом.

Vakolatli shaxs ortidan nazorat qilinadigan eshik orqali ruxsat etilmagan tarzda o‘tish.

Ваколатли шахс ортидан назорат қилинадиган эшик орқали рухсат этилмаган тарзда ўтиш.

Пиггибекинг электронный

uz - elektron piggibeking
электрон пиггибекинг
en - electronic piggyback

Несанкционированный доступ к системе обработки данных по легальному соединению полномочного пользователя.

Vakolatli foydalanuvchining qonuniy bog‘lanishi orqali ma‘lumotlarni qayta ishlash tizimidan ruxsat etilmagan tarzda foydalana olish.

Ваколатли фойдаланувчининг қонуний боғланиши орқали маълумотларни қайта ишлаш тизимидан рухсат этилмаган тарзда фойдалана олиш.

Пират телефонный (взломщик телефонных сетей)

uz - telefon qaroqchisi
(telefon tarmoqlarini buzuvchi)
телефон қароқчиси (телефон тармоқларини бузувчи)
en - phreaker

Мошенник, являющийся, как правило, профессиональным связистом с навыками хакера. Создает электронные устройства, позволяющие ему подключаться к телефонным сетям и использовать их ресурсы без надлежащей оплаты.

Xaker malakasiga ega professional aloqachi bo‘lgan firibgar. Telefon tarmoqlariga ulanish va ularning resurslaridan tegishli to‘lovlarsiz foydalanish imkonini beradigan elektron qurilmalarni yaratadi.

II

Пиратство программное

uz - dasturiy qarqochilik
дастурий қарқочилик
en - software piracy

Хакер малакасига эга профессионал алоқачи бўлган фирибгар. Телефон тармоқларига уланиш ва уларнинг ресурсларидан тегишли тўловларсиз фойдаланиш имконини берадиган электрон қурилмаларни яратади.

Неправомерное использование, копирование или распространение лицензионных программных продуктов, являющихся авторским произведением.

Mualliflik asari hisoblanadigan litsenzion dasturiy mahsulotlardan noqonuniy foydalanish, nusxa ko‘chirish yoki tarqatish.

Mualliflik asari hisoblanadigan litsenzion dasturiy mahsulotlardan noqonuniy foydalanish, nusxa ko‘chirish yoki tarqatish.

План обеспечения непрерывной работы и восстановления функционирования

uz - uzluksiz ishlashni ta‘minlash va tiklash rejasi
узлуксиз ишлашни таъминлаш ва тиклаш режаси
en - contingency plan
(backup plan, recovery plan)

План реагирования на опасные ситуации, резервного копирования и последующих восстановительных процедур, являющийся частью программы защиты и обеспечивающий доступность основных ресурсов системы и непрерывность обработки в кризисных ситуациях.

Muhofaza qilish dasturining bir qismi hisoblanadigan hamda tizimning asosiy resurslaridan foydalanishni va krizisli vaziyatlarda qayta ishlashning uzluksizligini ta‘minlovchi, xavfli vaziyatlarga javob berish, rezerv nusxa ko‘chirish va keyingi tiklash protseduralari rejasi.

Muhofaza qilish dasturining bir qismi hisoblanadigan hamda tizimning asosiy resurslaridan foydalanishni va krizisli vaziyatlarda qayta ishlashning uzluksizligini ta‘minlovchi, xavfli vaziyatlarga javob berish, rezerv nusxa ko‘chirish va keyingi tiklash protseduralari rejasi.

План управления конфигурацией

Описание использования системы управления конфигурацией для объекта оценки.

П

uz - konfiguratsiyani

boshqarish rejasi

конфигурацияни

бошқариш режаси

en - configuration management
plan

Плата копирования

uz - nusxa ko'chirish platasi

нусха кўчириш платаси

en - copy card

Baholash obyektlari uchun konfiguratsiyani boshqarish tizimidan foydalanish tavsifi.

Баҳолаш объектлари учун конфигурацияни бошқариш тизимдан фойдаланиш тавсифи.

Электронное устройство, которое после установки в ЭВМ позволяет копировать защищенное программное обеспечение из оперативной памяти на диск.

Elektron hisoblash mashinasiga o'rnatilgandan so'ng, operativ хотирадан diskka muhofazalangan dasturiy ta'minotni ko'chirish imkonini beradigan elektron qurilma.

Электрон ҳисоблаш машинасига ўрнатилгандан сўнг, оператив хотирадан дискка муҳофазаланган дастурий таъминотни кўчириш имконини берадиган электрон қурилма.

Повтор

uz - takror(lash)

такрор(лаш)

en - replay

Простейший вид сетевой атаки, когда злоумышленник перехватывает сообщение и повторяет его, не изменяя, в более позднее время.

Tarmoqqa qilinadigan hujumning oddiy turi, bunda jinoyatkor xabarni tutib oladi va uni o'zgartirmasdan, birmuncha kechroq takrorlaydi.

Тармоққа қилинадиган ҳужумнинг оддий тури, бунда жинояткор хабарни тутиб олади ва уни ўзгартирмасдан, бирмунча кечроқ такрорлайди.

Подглядывание из-за плеча

uz - yelka osha yashirincha

qarash

елка оша яширинча қараш

en - keeking behind shoulder

Кража паролей или PIN-кодов путем наблюдения за их набором на клавиатуре.

Parollar yoki PIN-kodlarni, ularning klaviaturada terilishini kuzatish yo'li bilan o'g'irlash.

Пароллар ёки PIN-кодларни, уларнинг клавиатурада терилишини кузатиш йўли билан ўғирлаш.

Подготовка

Стадия жизненного цикла продукта, включающая

П

uz - tayyorgarlik
тайёргарлик
en - preparation

приемку поставленного ОО потребителем и его инсталляцию.

Mahsulot hayotiy siklining bosqichi, yetkazib berilgan BOning iste'molchi tomonidan qabul qilib olinishini va uning installyatsiyasini ichiga oladi.

Маҳсулот ҳаётӣй циклининг босқичи, етказиб берилган БОнинг истеъмолчи томонидан қабул қилиб олинисини ва унинг инсталляциясини ичига олади.

Подделка
uz - soxtalashtirish
сохталаштириш
en - tampering

Модификация злоумышленником содержания перехваченных пакетов, приводящая к потере целостности.

Jinoyatkor tomonidan tutib olingan paketlar mazmunining, ularning yaxlitligi buzilishiga olib keladigan tarzda, o'zgartirilishi.

Жинояткор томонидан тутиб олинган пакетлар мазмунининг, уларнинг яхлитлиги бузилишига олиб келадиган тарзда, ўзгартирилиши.

Подделка информации
uz - axborotni
soxtalashtirish
ахборотни
сохталаштириш
en - data corruption

Умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

Axborotni, raqobatchi oldida ma'lum foyda (afzallik) olish yoki unga zarar yetkazish maqsadida, texnik vositalar bilan qayta ishlashda, atayin ruxsat etilmagan tarzda o'zgartirish.

Ахборотни, рақобатчи олдида маълум фойда (афзаллик) олиш ёки унга зарар етказиш мақсадида, техник воситалар билан қайта ишлашда, атайин рухсат этилмаган тарзда ўзгартириш.

Подотчетность
uz - hisob berishlik
ҳисоб беришлик
en - accountability

1 Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

2 Свойство автоматизированной системы, позволяющее фиксировать деятельность ее субъектов

II

и ассоциировать их с индивидуальными идентификаторами для последующего выявления нарушений безопасности и ответственных за эти нарушения.

3 Возможность для ответственных за защиту информации лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.

4 Свойство реальной открытой системы, заключающееся в способности контролировать действия пользователей и ресурсов с целью последующего выявления нарушений безопасности и ответственных за эти нарушения.

1 Har qanday mantiqiy obyektning harakatlarini qat'iy kuzatishni ta'minlaydigan xususiyat.

2 Avtomatlashtirilgan tizimning, tizim subyektlari faoliyatini qayd qilishga hamda ularni xavfsizlik buzilishlari va bu buzilishlar uchun javobgarlarni kelgusida aniqlash uchun ularning individual identifikatorlari bilan assotsiatsiyalash imkonini beruvchi xususiyati.

3 Axborotning muhofaza qilinishi yuzasidan javobgar bo'lgan shaxslar uchun axborot tizimi xavfsizligi buzilish jarayonini yoki buzishga urinishlarni tiklash imkoniyati.

4 Real ochiq tizimning, xavfsizlik buzilishlarini va ular yuzasidan javobgarlarni aniqlash maqsadida, foydalanuvchilarning harakatini va resurslarni nazorat qilishida ifodalanadigan xususiyati.

1 Ҳар қандай мантиқий объектнинг ҳаракатларини қатъий кузатишни таъминлайдиган хусусият.

2 Автоматлаштирилган тизимнинг, тизим субъектлари фаолиятини қайд қилишга ҳамда уларни хавфсизлик бузилишлари ва бу бузилишлар учун жавобгарларни келгусида аниқлаш учун уларнинг индивидуал идентификаторлари билан ассоциациялаш имконини берувчи хусусияти.

3 Ахборотнинг муҳофаза қилиниши юзасидан жавобгар бўлган шахслар учун ахборот тизими хавфсизлиги бузилиш жараёнини ёки бузишга уринишларни тиклаш имконияти.

II

4 Реал очик тизимнинг, хавфсизлик бузилишларини ва улар юзасидан жавобгарларни аниқлаш мақсадида, фойдаланувчиларнинг ҳаракатини ва ресурсларни назорат қилишида ифодаланадиган хусусияти.

Подпись бесспорная

uz - aniq imzo

аниқ имзо

en - indisputable signature

Схема цифровой подписи, использующая протокол отрицания, который позволяет предотвратить отказ подписывающего от своего сообщения.

Inkor qilish protokolidan foydalaniladigan raqamli imzo sxemasi imzo chekuvchining o'z xabarini inkor etishining oldini olish imkonini beradi.

Инкор қилиш протоколидан фойдаланиладиган рақамли имзо схемаси имзо чекувчининг ўз хабарини инкор этишининг олдини олиш имконини беради.

Подпись групповая

uz - guruhiy imzo

гурухий имзо

en - group signature

Схема цифровой подписи, предложенная в 1991 году Чомом и Ван Хейстом, позволяющая любому члену группы подписать сообщение таким образом, чтобы при проверке можно было установить, что сообщение подписано одним из членов группы, без конкретизации личности подписывающего.

1991 yilda Chom va Van Heyst tomonidan taklif qilingan raqamli imzo sxemasi, guruhning istalgan a'zosiga xabarni, tekshirish paytida, xabar guruh a'zolaridan biri tomonidan imzo chekuvchining shaxsini aniqlashtirilmasdan imzolanganini aniqlash mumkin bo'ladigan tarzda imzolash imkonini beradi.

1991 йилда Чом ва Ван Хейст томонидан таклиф қилинган рақамли имзо схемаси, гуруҳнинг исталган аъзосига хабарни, текшириш пайтида, хабар гуруҳ аъзоларидан бири томонидан имзо чекувчининг шахсини аниқлаштирилмасдан имзоланганини аниқлаш мумкин бўладиган тарзда имзолаш имконини беради.

Подпись кода

uz - kod yozuvi

Механизм, позволяющий подписывать программное обеспечение, распространяемое по се-

II

код ёзуви
en - code signature

тям общего пользования. Это позволяет аутентифицировать автора программного обеспечения и гарантировать, что в процессе передачи код не модифицировался.

Umumiy foydalanish tarmoqlari bo‘ylab tarqatiladigan dasturiy ta’minotni imzolash imkonini beruvchi mexanizm. Bu, dasturiy ta’minot muallifini autentifikatsiya qilish va uzatish jarayonida kodning o‘zgartirilmasligini kafolatlash imkonini beradi.

Умумий фойдаланиш тармоқлари бўйлаб тарқатиладиган дастурий таъминотни имзолаш имконини берувчи механизм. Бу, дастурий таъминот муаллифини аутентификация қилиш ва узатиш жараёнида коднинг ўзгартирилмаслигини кафолатлаш имконини беради.

**Подпись
самопроверяющаяся**
uz - o‘z-o‘zini tekshirish
imzosi
ўз-ўзини текшириш
имзоси
en - self-verifying signature

Цифровая подпись, подлинность которой может быть проверена в любое время без согласия подписывающего лица. К этой категории может быть отнесена любая цифровая подпись с открытым ключом.

Haqiqiyliги imzo chekuvchi shaxsning rozilgisiz istalgan vaqtda tekshirilishi mumkin bo‘lgan raqamli imzo. Bu kategoriyaga ochiq kalitli istalgan raqamli imzo kiritilishi mumkin.

Ҳақиқийлиги имзо чекувчи шахснинг розилигисиз исталган вақтда текширилиши мумкин бўлган рақамли имзо. Бу категорияга очик калитли исталган рақамли имзо киритилиши мумкин.

Подпись слепая
uz - ko‘r-ko‘rona imzo
кўр-кўрона имзо
en - blind signature

Механизм электронной цифровой подписи, используемый в платежной системе DigiCash и основанный на применении случайного множителя (blinding factor).

DigiCash to‘lov tizimida ishlatiladigan va tasodifiy ko‘paytiruvchini (blinding factor) qo‘llashga asoslangan elektron raqamli imzo mexanizmi.

DigiCash тўлов тизимида ишлатиладиган ва тасо-

II

дифий кўпайтирувчини (blinding factor) қўллашга асосланган электрон рақамли имзо механизми.

Подпись цифровая

uz - raqamli imzo

рақамли имзо

en - digital signature

1 Данные, добавляемые к сообщению и позволяющие получателю сообщения проверять подлинность отправителя.

2 Последовательность данных, добавляемая к блоку данных или к результату его криптографического преобразования, которая позволяет получателю данных проверить источник и целостность блока данных, а также защиту от подлога или подделки.

1 Хабарга qo'shimcha qilinadigan hamda xabar oluvchiga jo'natuvchining haqiqiyiligini tekshirish imkonini beruvchi ma'lumotlar.

2 Ma'lumotlar blokiga yoki uni kriptografik qayta o'zgartirish natijasiga qo'shimcha qilinadigan ma'lumotlar ketma-ketligi, u ma'lumotlar oluvchisiga manba va ma'lumotlar blokining yaxlitligini tekshirish, shuningdek, soxtalashtirishdan yoki almashtirishdan muhofaza qilish imkonini beradi.

1 Хабарга қўшимча қилинадиган ҳамда хабар олувчига жўнатувчининг ҳақиқийлигини текшириш имконини берувчи маълумотлар.

2 Маълумотлар блокига ёки уни криптографик қайта ўзгартириш натижасига қўшимча қилинадиган маълумотлар кетма-кетлиги, у маълумотлар олувчисига манба ва маълумотлар блокнинг яхлитлигини текшириш, шунингдек, сохталаштиришдан ёки алмаштиришдан муҳофаза қилиш имконини беради.

Подпись цифровая

одноразовая

uz - bir martali raqamli

imzo

бир мартали рақамли

имзо

en - one-shot digital signature

Схема, в которой для любого сообщения цифровая подпись может быть использована только один раз, т.е. для каждого нового сообщения требуется новая пара ключей. Достоинством такой схемы является быстрота, недостатком – необходимость опубликования большого количества информации (открытых ключей), т.к. каждая подпись используется только один раз.

Har qanday xabar uchun raqamli imzo faqat bir

II

marta ishlatilishi mumkin bo'lgan sxema, ya'ni har bir yangi xabar uchun kalitlarning yangi jufti talab qilinadi. Bunday sxemaning afzalligi uning tezkorligi hisoblanadi, kamchiligi – katta miqdordagi axborotni (ochiq kalitlarni) e'lon qilish zarurligi, chunki har bir imzo faqat bir marta ishlatiladi.

Har qanday xabar uchun raqamli imzo faqat bir marta ishlatilishi mumkin bo'lgan sxema, ya'ni har bir yangi xabar uchun kalitlarning yangi jufti talab qilinadi. Bunday sxemaning afzalligi uning tezkorligi hisoblanadi, kamchiligi – katta miqdordagi axborotni (ochiq kalitlarni) e'lon qilish zarurligi, chunki har bir imzo faqat bir marta ishlatiladi.

Подпись цифровая электронная

uz - elektron raqamli imzo

электрон рақамли имзо

en - digital signature

Механизм, позволяющий на основе криптографических методов надежно установить авторство и подлинность информации (сообщения или документа).

Kriptografik metodlar asosida mualliflikni va axborot (xabar yoki hujjat)ning haqiqiyligini ishonchli belgilashga imkon beruvchi mexanizm.

Криптографик методлар асосида муаллифликни ва ахборот (хабар ёки ҳужжат)нинг ҳақиқийлигини ишончли белгилашга имкон берувчи механизм.

Подслушивание

uz - yashirin eshitish

яширин эшитиш

en - eavesdropping

1 Перехват злоумышленником передаваемой по сети информации с целью выявления и последующей эксплуатации слабых мест системы защиты.

2 Любые действия, связанные с перехватом конфиденциальной информации, в том числе за счет приема излучений по побочным каналам.

1 Jinoyatkor tomonidan, tarmoq bo'ylab uzatiladigan axborotni, muhofaza tizimining zaif joylarini aniqlash va keyinchalik undan foydalanish maqsadida, qo'lga kiritish.

2 Konfidensial axborotni qo'lga kiritish bilan bog'liq, har qanday harakatlar shu jumladan, qo'shni kanallar orqali nurlanishlarni qabul qilish hisobiga.

П

1 Жинойткор томонидан, тармоқ бўйлаб узатиладиган ахборотни, муҳофаза тизимининг заиф жойларини аниқлаш ва кейинчалик ундан фойдаланиш мақсадида, қўлга киритиш.

2 Конфиденциал ахборотни қўлга киритиш билан боғлиқ, ҳар қандай ҳаракатлар, шу жумладан, қўшни каналлар орқали нурланишларни қабул қилиш ҳисобига.

Подстановка

uz - oʻrniga qoʻyish

ўрнига қўйиш

en - substitution

1 Шифрование, при котором последовательность битов или символов заменяется другой последовательностью битов или символов.

Примечание – Полученный шифротекст называется шифром подстановки.

2 Криптографическая операция, связанная с замещением одного блока другим и использующая определенный код.

1 Bitlar yoki simvollar ketma-ketligi boshqa bitlar yoki simvollar ketma-ketligi bilan almashtiriladigan shifrlash.

Izoh – Olingan shifratn oʻrniga qoʻyish shifri deb ataladi.

2 Bir blokni boshqasi bilan almashtirish bilan bogʻliq va maʼlum koddan foydalanuvchi kriptografik operatsiya.

1 Битлар ёки символлар кетма-кетлиги бошқа битлар ёки символлар кетма-кетлиги билан алмаштириладиган шифрлаш.

Изоҳ – Олинган шифратн ўрнига қўйиш шифри деб аталади.

2 Бир блокни бошқаси билан алмаштириш билан боғлиқ ва маълум коддан фойдаланувчи криптографик операция.

Подстановка

(заполнение) трафика

uz - trafikni oʻrniga qoʻyish

(toʻldirish)

трафикни ўрнига қўйиш

(тўлдириш)

en - traffic padding

1 Установление поддельных соединений, генерация фальшивых блоков данных и/или отдельных фальшивых данных внутри блоков данных.

2 Генерирование ложных событий связи, ложных блоков данных и/или ложных данных в пределах блоков данных.

1 Soxta ulanishlarni aniqlash, qalbaki maʼlumotlar bloklarini va/yoki maʼlumotlar bloki ichidagi alohida

II

qalbaki ma'lumotlarni generatsiyalash.

2 Ma'lumotlar bloki doirasida noto'g'ri aloqa voqealarini, noto'g'ri ma'lumotlar blokini va/yoki noto'g'ri ma'lumotlarni generatsiyalash.

1 Сохта уланишларни аниқлаш, қалбаки маълумотлар блокларини ва/ёки маълумотлар блоки ичидаги алоҳида қалбаки маълумотларни генерациялаш.

2 Маълумотлар блоки доирасида нотўғри алоқа воқеаларини, нотўғри маълумотлар блокини ва/ёки нотўғри маълумотларни генерациялаш.

Подсчет побитовый

uz - bitma-bit hisoblash

битма-бит ҳисоблаш

en - bit counting

Метод защиты от копирования, при котором диск распознается как оригинал, если некоторая дорожка (или другая область) содержит определенное число битов.

Nusxa olinishdan muhofaza qilish metodi bo'lib, qandaydir yo'lka (yoki boshqa soha) bitlarning muayyan sonini ichiga olganda, disk original sifatida aniqlanadi.

Нусха олинишдан муҳофаза қилиш методи бўлиб, қандайдир йўлка (ёки бошқа соҳа) битларнинг муайян сонини ичига олганда, диск оригинал сифатида аниқланади.

Подтверждать

uz - tasdiqlamoq

тасдиқламоқ

en - confirm

Заявлять о том, что нечто было детально рассмотрено с независимым определением достаточности.

Примечание – Требуемый уровень детализации зависит от типа предмета рассмотрения. Этот термин применим только к действиям оценщика.

Yetarlilikni mustaqil aniqlash bilan nimanidir batafsil ko'rilganligini bildirish.

Izoh – Detallashtirishning talab etilayotgan darajasi qarab chiqiladigan predmet turiga bog'liq bo'ladi. Bu atama faqat baholovchining harakatida qo'llaniladi.

Етарlilikни мустақил аниқлаш билан ниманидир батафсил кўрилганлигини билдириш.

Изоҳ – Деталлаштиришнинг талаб этилаётган даражаси қараб чиқиладиган предмет турига боғлиқ бўлади. Бу

II

Подтверждение подлинности

uz - haqiqiylikni tasdiqlash

ҳақиқийликни тасдиқлаш

en - authentication

Показатели защищенности средств вычислительной техники (автоматизирован- ной системы)

uz - hisoblash texnikasi vositalarining (avtomatlashtirilgan tizimning) muhofaza qilinganlik ko'rsatkichlari

хисоблаш техникаси
воситаларининг (автомат-
лаштирилган тизимнинг)
муҳофаза қилинганлик
кўрсаткичлари

en - protection criteria of facilities of computing machinery (computer-based system)

Показатель эффективности защиты информации

uz - axborotni muhofaza qilishning samaradorlik ko'rsatkichi

ахборотни муҳофаза
қилишнинг самарадорлик
кўрсаткичи

en - efficiency factor of

атама фақат баҳоловчининг ҳаракатида қўлланилади.

Механизм, направленный на подтверждение подлинности и предусматривающий обмен информацией.

Haqiqiylikni tasdiqlashga yo'naltirilgan va axborot almashinuvi ko'zda tutiladigan mexanizm.

Ҳақиқийликни тасдиқлашга йўналтирилган ва ахборот алмашинуви кўзда тутилдиган механизм.

Характеристика средств вычислительной техники (автоматизированной системы), влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности средств вычислительной техники (автоматизированной системы).

Muhofaza qilinganlik ko'rsatkichlarini aks ettiruvchi va hisoblash texnikasi vositalari (avtomatlashtirilgan tizim) ning muhofaza qilinganlik klassiga muvofiq daraja va kenglik bo'yicha o'zgaradigan talablarning ma'lum guruhi bilan tavsiflanadigan hisoblash texnikasi vositalari (avtomatlashtirilgan tizim)ning xarakteristikasi.

Муҳофаза қилинганлик кўрсаткичларини акс эттирувчи ва хисоблаш техникаси воситалари (автоматлаштирилган тизим) нинг муҳофаза қилинганлик классига мувофиқ даража ва кенглик бўйича ўзгарадиган талабларнинг маълум гуруҳи билан тавсифланадиган хисоблаш техникаси воситалари (автоматлаштирилган тизим)нинг харақтеристикаси.

Мера или характеристика для оценки эффективности защиты информации.

Axborotni muhofaza qilish samaradorligini baholash o'lchovi yoki xarakteristikasi.

Ахборотни муҳофаза қилиш самарадорлигини баҳолаш ўлчови ёки харақтеристикаси.

П

information security

Поле (диска) адресное

uz - adresli (disk) maydoni

адресли (диск) майдони

en - address field (disk)

Поле данных

uz - ma'lumotlar maydoni

маълумотлар майдони

en - data field

**Поле управления
аутентификацией**

uz - autentifikatsiyani
boshqarish maydoni

аутентификацияни

бошқариш майдони

en - authentication
management field

Политика

uz - siyosat

сиёсат

en - policy

Политика безопасности

uz - xavfsizlik siyosati

хавфсизлик сиёсати

en - security policy

Начальная область сектора на диске, в которой указано число дорожек и секторов.

Diskdagi sektorning, yo'laklar va sektorlar soni ko'rsatilgan boshlang'ich sohasi.

Дискдаги секторнинг, йўлкалар ва секторлар соҳаси кўрсатилган бошланғич соҳаси.

Часть дискового пространства (сектора) для размещения данных, которому предшествует адрес.

Disk maydoni (sektori)ning, adres undan oldin keladigan ma'lumotlarni joylashtirish uchun mo'ljallangan qismi.

Диск майдони (сектори)нинг, адрес ундан олдин келадиган маълумотларни жойлаштириш учун мўлжалланган қисми.

Поле данных, используемое для проверки аутентичности сообщения.

Xabarning autentikligini (haqiqiyligini) tekshirish uchun qo'llaniladigan ma'lumotlar maydoni.

Хабарнинг аутентиклигини (ҳақиқийлигини) текшириш учун қўлланиладиган маълумотлар майдони.

Цели и распоряжения организации, формально выраженные ее высшим руководством.

Tashkilotning oliy rahbariyati tomonidan rasmiy ifodalangan umumiy maqsad va farmoyishlari.

Ташкилотнинг олий раҳбарияти томонидан расмий ифодаланган умумий мақсад ва фармойишлари.

1 План или программа действий, принятая для обеспечения компьютерной безопасности.

2 Набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение защищаемой информации в системе. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

II

3 Набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного подмножества объектов и субъектов безопасности.

4 Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

5 Свод законов, норм, правил, практических рекомендаций и приёмов, которые регулируют в данной организации обработку, защиту и распространение значимой информации.

1 Kompyuter xavfsizligini ta'minlash uchun qabul qilingan harakatlar rejasi yoki dasturi.

2 Qonunlar, qoidalar va amaliy tavsiyanomalar to'plami, unga asosan tizimdagi muhofaza qili-nayotgan axborotni boshqarish, muhofaza qilish va taqsimlash yo'lga qo'yiladi. U, turli vaziyatlarda tizim o'zini qanday tutishini belgilagan holda, axborotni qayta ishlash jarayonining barcha xususiyatlarini qamrab oladi.

3 Xavfsizlik obyektlari va subyektlari berilgan ko'pligining xavfsizligini ta'minlash prosedura va mexanizmlarini belgilovchi qoidalar to'plami.

4 Tizimning ma'lum tahdidlardan muhofaza qilinishini ta'minlashda tayanish mumkin bo'lgan kriteriylarning, ayniqsa, operativ kriteriylarning formal belgilanishi.

5 Tashkilotda ahamiyatli axborotning qayta ishlani-shini, muhofaza qilinishini va tarqatilishini tartibga soladigan qonunlar, normalar, qoidalar, amaliy tavsiyalar va usullar to'plami.

1 Компьютер хавфсизлигини таъминлаш учун қабул қилинган ҳаракатлар режаси ёки дастури.

2 Қонунлар, қоидалар ва амалий тавсияномалар тўплами, унга асосан тизимдаги муҳофаза қилинаётган ахборотни бошқариш, муҳофаза қилиш ва тақсимлаш йўлга қўйилади. У, турли вазиятларда тизим ўзини қандай тутишини белгилаган ҳолда, ахборотни қайта ишлаш жараёнининг барча хусусиятларини қамраб олади.

3 Хавфсизлик объектлари ва субъектлари берил-

II

ган кўплигининг хавфсизлигини таъминлаш процедура ва механизмларини белгиловчи қоидалар тўплами.

4 Тизимнинг маълум таҳдидлардан муҳофаза қилинишини таъминлашда таяниш мумкин бўлган критерийларнинг, айниқса, оператив критерийларнинг формал белгиланиши.

5 Ташкилотда аҳамиятли ахборотнинг қайта ишланишини, муҳофаза қилинишини ва тарқатилишини тартибга соладиган қонунлар, нормалар, қоидалар, амалий тавсиялар ва усуллар тўплами.

Политика безопасности идентификационная

uz - identifikatsion xavfsizlik siyosati

идентификацион хавфсизлик сиёсати

en - identity-based security policy

Политика безопасности, основанная на идентифицирующих свойствах и/или атрибутах пользователей сети, группы пользователей сети, используемых ресурсов сети.

Foydalaniladigan tarmoq resurslarining, tarmoq foydalanuvchilarining, foydalanuvchilar guruhining identifikatsiyalovchi xossalari va/yoki atributlariga asoslangan xavfsizlik siyosati.

Фойдаланиладиган тармоқ ресурсларининг, тармоқ фойдаланувчиларининг, фойдаланувчилар гуруҳининг идентификацияловчи хоссалари ва/ёки атрибутларига асосланган хавфсизлик сиёсати.

Политика безопасности инструкционная

uz - instruksion xavfsizlik siyosati

инструкцион хавфсизлик сиёсати

en - rule-based security policy

Методика безопасности, основанная на общих правилах, обязательных для всех пользователей АИС.

ААТ barcha foydalanuvchilari uchun majburiy bo'lgan umumiy qoidalarga asoslangan, xavfsizlik metodikasi.

ААТ барча фойдаланувчилари учун мажбурий бўлган умумий қоидаларга асосланган, хавфсизлик методикаси.

Политика безопасности организации

uz - tashkilotning xavfsizlik siyosati

ташкilotнинг хавфсизлик сиёсати

en - organizational security

Совокупность правил, процедур или рекомендаций по безопасности в организации.

Примечание – Политика может относиться к определенной среде функционирования.

Tashkilotdagi xavfsizlik bo'yicha qoidalar, protseduralar yoki tavsiyalar jami.

Izoh – Siyosat muayyan ishlash muhitiga taalluqli bo'ladi.

II

policy

Политика информационной безопасности сети телекоммуникаций общего пользования

uz - umumiy foydalanishdagi telekommunikatsiyalar tar-mog'ining axborot xavfsizligi siyosati

умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги сиёсати
en - public switched telecommunications network information security policy

Политика управления доступом

uz - foydalana olishni boshqarish siyosati

фойдалана олишни бошқариш сиёсати
en - access control policy

Ташкилотдаги хавфсизлик бўйича қоидалар, процедуралар ёки тавсиялар жами.

Изоҳ – Сиёсат муайян ишлаш муҳитига тааллуқли бўлади.

Совокупность требований и правил для объекта (объектов) информационной безопасности сети телекоммуникаций общего пользования, выработанных администрацией сети, в целях противодействия определенным угрозам информационной безопасности сети, с учетом ценности защищаемых ресурсов и стоимости системы обеспечения информационной безопасности сети телекоммуникаций общего пользования.

Tarmoq ma'muri tomonidan, muhofaza qilinadigan resurslarning qiymati va umumiy foydalanishdagi telekommunikatsiyalar tarmog'i axborot xavfsizligini ta'minlash tizimining bahosini hisobga olib, tarmoqning axborot xavfsizligiga bo'ladigan ma'lum tahdidlarga qarshi harakat qilish maqsadida ishlab chiqilgan, umumiy foydalanishdagi telekommunikatsiyalar tarmog'i axborot xavfsizligi obyekt (obyekt-lari) uchun mo'ljallangan talablar va qoidalarining jami.

Тармоқ маъмури томонидан, муҳофаза қилинадиган ресурсларнинг қиймати ва умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизимининг баҳосини ҳисобга олиб, тармоқнинг ахборот хавфсизлигига бўладиган маълум таҳдидларга қарши ҳаракат қилиш мақсадида ишлаб чиқилган, умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлиги объекти (объектлари) учун мўлжалланган талаблар ва қоидаларининг жами.

Набор правил, определяющих условия, при которых доступ может иметь место.

Foydalana olish o'z o'rniga ega bo'lishi mumkin bo'lgan sharoitlarni belgilaydigan qoidalar to'plami.

Фойдалана олиш ўз ўрнига эга бўлиши мумкин

П

бўлган шароитларни белгилайдиган қоидалар тўплами.

Политика функции безопасности

uz - xavfsizlik funksiyasi siyosati

хавфсизлик функцияси сиёсати

en - security function policy

Совокупность правил, описывающих конкретный режим безопасности, реализуемый функциями безопасности объекта оценки, и выраженных в виде совокупности функциональных требований безопасности.

Baholash obyektini xavfsizlik funksiyalari amalga oshiradigan aniq xavfsizlik rejimini tavsiflaydigan va funksional xavfsizlik talablari yigʻindisi koʻrinishida ifodalangan qoidalar jami.

Баҳолаш объекти хавфсизлик функциялари амалга оширадиган аниқ хавфсизлик режимини тавсифлайдиган ва функционал хавфсизлик талаблари йиғиндиси кўринишида ифодаланган қоидалар жами.

Полномочие

uz - vakolat

ваколат

en - authority

1 Представление идентификации объекта или класса объектов и всех разрешенных видов доступа к этим объектам.

Примечание – Полномочие может быть реализовано в форме мандата.

2 Знак, используемый в качестве идентификатора для какого-либо ресурса, причем обладание таким знаком подтверждает право доступа к ресурсам.

1. Obyektni yoki obyektlar klassini identifikatsiya qilishni va ushbu obyektlardan erkin foydalanishning barcha ruxsat etilgan turlarini taqdim etish.

Izoh – Vakolat mandat shaklida amalga oshirilishi mumkin.

2 Qandaydir resurs uchun identifikator sifatida foydalaniladigan belgi. Bunday belgiga ega boʻlishlik resurslardan foydalana olish huquqini tasdiqlaydi.

1. Obyektni ёки obyektlar klassini identifikatsiya qilishni va ushbu obyektlardan erkin foydalanishning barcha ruxsat etilgan turlarini taqdim etish.

Изоҳ – Ваколат мандат шаклида амалга оширилиши мумкин.

2 Қандайдир ресурс учун идентификатор сифа-

П

тида фойдаланиладиган белги. Бундай белгига эга бўлишлик ресурслардан фойдалана олиш ҳуқуқини тасдиқлайди.

Полный

uz - to‘la

тўла

en - complete

Свойство, обеспечивающее наличие всех необходимых частей логического объекта.

Примечание – Относительно документации это означает, что вся необходимая информация включена в документацию на таком уровне детализации, который не требует каких-либо дополнительных пояснений.

Mantiqiy obyektни barcha zarur qismlari bilan ta‘minlaydigan xossasi.

Izoh – Hujjatga nisbatan, barcha zarur axborot hujjatga hech qanday qo‘shimcha tushuntirish talab etilmaydigan detallash-tirish darajasida kiritilganligini bildiradi.

Мантикий объектни барча зарур қисмлари билан таъминлайдиган хоссаси.

Изоҳ – Хужжатга нисбатан, барча зарур ахборот хужжатга ҳеч қандай қўшимча тушунтириш талаб этилмайдиган деталлаштириш даражасида киритилганлигини билдиради.

Полубайт

uz - yarim bayt

ярим байт

en - nibble

Часть слова длиной четыре бита.

To‘rt bit uzunlikdagi so‘zning qismi.

Тўрт бит узунликдаги сўзнинг қисми.

Полуформальный

uz - yarimformal

яримформал

en - semiformal

Выраженный на языке с ограниченным синтаксисом и определенной семантикой.

Cheklangan sintaksis va belgilangan semantika tilida ifodalangan.

Чекланган синтаксис ва белгиланган семантика тилида ифодаланган.

Пользователь

uz - foydalanuvchi

фойдаланувчи

en - user

Любой логический объект (человек-пользователь или внешний объект ИТ) вне объекта оценки, который взаимодействует с объектом оценки.

Baholash obyektini bilan birgalikda ishlaydigan, baholash obyektidan tashqarida bo‘lgan har qanday mantiqiy obyekt (foydalanuvchi-odam yoki AT tashqi obyektini).

П

Баҳолаш объекти билан биргаликда ишлайдиган, баҳолаш объектидан ташқарида бўлган ҳар қандай мантикий объект (фойдаланувчи-одам ёки АТ ташқи объекти).

Пользователь

авторизованный

uz - mualliflashtirilgan

foydalanuvchi

муаллифлаштирилган

фойдаланувчи

en - authorized user

Пользователь, наделенный определенными правами и привилегиями.

Ma'lum huquq va imtiyozlarga ega foydalanuvchi.

Маълум ҳуқуқ ва имтиёзларга эга фойдаланувчи.

Пользователь

зарегистрированный

uz - ro'uxatga olingan

foydalanuvchi

рўйхатга олинган

фойдаланувчи

en - registered user

1 Пользователь, имеющий приоритетный номер в данной системе коллективного пользования.

2 Пользователь, включенный в график работ на ЭВМ.

1 Berilgan jamoa bo'lib foydalanish tizimida ustuvor raqamga ega bo'lgan foydalanuvchi.

2 ENMdagı ishlar grafigiga kiritilgan foydalanuvchi.

1 Берилган жамоа бўлиб фойдаланиш тизимида устувор рақамга эга бўлган фойдаланувчи.

2 ЭХМдаги ишлар графигига киритилган фойдаланувчи.

Пользователь (потребитель) информации

uz - axborotdan foydalanuvchi

(axborot iste'molchisi)

ахборотдан фойдаланувчи

(ахборот истеъмолчиси)

en - information user

1 Субъект, обращающийся к информационным ресурсам за получением необходимой ему информации и пользующийся ею.

2 Юридическое или физическое лицо, обладающее полномочиями доступа к информации.

3 Субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

1 Axborot resurslariga zarur axborotni olish va undan foydalanish uchun murojaat qiluvchi subyekt.

2 Axborotdan foydalana olish vakolatiga ega yuridik yoki jismoniy shaxs.

3 Axborotdan erkin foydalanishning belgilangan hu-

II

quq va qoidalariga muvofiq yoki ularni buzgan holda, axborot egasi yoki vositachisidan olingan axborotdan foydalanuvchi subyekt.

1 Ахборот ресурсларига зарур ахборотни олиш ва ундан фойдаланиш учун мурожаат қилувчи субъект.

2 Ахборотдан фойдалана олиш ваколатига эга юридик ёки жисмоний шахс.

3 Ахборотдан эркин фойдаланишнинг белгиланган ҳуқуқ ва қоидаларига мувофиқ ёки уларни бузган ҳолда, ахборот эгаси ёки воситачисидан олинган ахборотдан фойдаланувчи субъект.

Пользователь легальный
uz - qonuniy foydalanuvchi
қонуний фойдаланувчи
en - legal user

Пользователь, имеющий законные основания для доступа к заданным ресурсам и сервисам.

Berilgan resurslar va servislardan erkin foydalanish uchun qonuniy asosga ega boʻlgan foydalanuvchi.

Берилган ресурслар ва сервислардан эркин фойдаланиш учун қонуний асосга эга бўлган фойдаланувчи.

**Пользователь
уполномоченный**
uz - vakolatli foydalanuvchi
ваколатли фойдаланувчи
en - authorised user

Пользователь объекта оценки, которому в соответствии с политикой функции безопасности разрешено выполнять какую-либо операцию.

Xavfsizlik funksiyasi siyosatiga muvofiq, har qanday operatsiyani bajarishga ruxsat etilgan, baholash obyekti foydalanuvchisi.

Хавфсизлик функцияси сиёсатига мувофиқ, ҳар қандай операцияни бажаришга рухсат этилган, баҳолаш объекти фойдаланувчиси.

Понятный
uz - tushunarli
тушунарли
en - coherent

Логически упорядоченный и имеющий очевидный смысл.

Примечание – Относительно документации это означает, что имеющийся текст и структура документа понятны для заявленной целевой аудитории.

Mantiqiy tartiblashtirilgan va aniq mazmunga ega boʻlgan.

II

Izoh – Hujjatga nisbatan, hujjatning matn va strukturasi e'lon qilingan maqsadli auditoriya uchun tushunarli bo'lishini bildiradi.

Мантикий тартиблаштирилган ва аниқ мазмунга эга бўлган.

Изоҳ – Хужжатга нисбатан, хужжатнинг матн ва структураси эълон қилинган мақсадли аудитория учун тушунарли бўлишини билдиради.

Попытка доступа к информации

неавторизованная

uz - axborotdan mualliflashtirilmagan tarzda foydalanishga urinish

ахборотдан муаллифлаштирилмаган тарзда фойдаланишга уриниш

en - hacking

Попытка нарушения защиты прямая

uz - muhofazani bevosita buzishga urinish

муҳофазани бевосита бузишга уриниш

en - direct attack

Портал обеспечения безопасности кабельный

uz - kabelli xavfsizlikni ta'minlash portali

кабелли хавфсизликни таъминлаш портали

en - cable security portal

Попытка получить доступ к информации за счет обхода (обмана) средств контроля доступа в сети.

Tarmoqdan erkin foydalanishni nazorat qiluvchi vositalarni chetlab o'tish (aldash) hisobiga axborotdan foydalana olishga urinib ko'rish.

Тармоқдан эркин фойдаланишни назорат қилувчи воситаларни четлаб ўтиш (алдаш) ҳисобига ахборотдан фойдалана олишга уриниб кўриш.

Попытка нарушения защиты системы, основанная на недостатках базовых алгоритмов, принципов или свойств механизма обеспечения безопасности.

Bazaviy algoritmlarning, xavfsizlikni ta'minlash mexanizmi prinsiplari yoki xususiyatlarining kamchiliklariga asoslangan, tizim muhofazasini buzishga bo'lgan urinish.

Базавий алгоритмларнинг, хавфсизликни таъминлаш механизми принциплари ёки хусусиятларининг камчиликларига асосланган, тизим муҳофазасини бузишга бўлган уриниш.

Функциональный элемент, управляющий обеспечением безопасности и функциями преобразования между коаксиальным гибридным волоконным кабелем и домом.

Xavfsizlik ta'minlanishini hamda koaksial gibrid tolali kabel bilan uy o'rtasida o'zgartirish funksiyala-

II

rini boshqaruvchi funksional element.

Хавфсизлик таъминланишини ҳамда коаксиал гибрид толали кабель билан уй ўртасида ўзгартириш функцияларини бошқарувчи функционал элемент.

Последовательность команд

uz - komandalar

ketma-ketligi

командалар

кетма-кетлиги

en - command sequence

Совокупность команд или зарезервированных слов в программах на языке высокого уровня или множество кодов операций в программах на машинном языке.

Yuqori darajali dasturlardagi komandalar yoki rezervlangan soʻzlar jami yoki mashina tili dasturlaridagi operatsiyalarning koʻplab kodlari (kodlar koʻpligi).

Юқори даражали дастурлардаги командалар ёки резервланган сўзлар жами ёки машина тили дастурларидаги операцияларнинг кўплаб кодлари (кодлар кўплиги).

Последовательность сверхдлинная

uz - oʻta uzun ketma-ketlik

ўта узун кетма-кетлик

en - knapsack

Псевдослучайная последовательность с высокой криптостойкостью и сверхдлинным периодом повторения.

Yuqori kriptobardoshlik va oʻta uzun takrorlanish davriga ega psevdotasodifiy ketma-ketlik.

Юқори криптобардошлик ва ўта узун такрорланиш даврига эга псевдотасодифий кетма-кетлик.

Последствие

uz - oqibat

оқибат

en - consequence

Результат воздействия события на цели.

Примечания

1 Результатом воздействия события может быть одно или несколько последствий.

2 Последствия могут быть определенными или неопределенными, могут быть ранжированы от позитивных до негативных.

3 Последствия могут быть выражены качественно или количественно.

4 Первоначальные последствия могут вызвать эскалацию дальнейших последствий по принципу «домино».

Voqea-hodisaning maqsadlarga taʼsir koʻrsatishining natijasi.

Izohlar

1 Voqea-hodisaning taʼsir koʻrsatish natijasi bitta yoki bir

II

nechta oqibat bo'lishi mumkin.

2 Oqibatlar ma'lum yoki noma'lum bo'lishi, ijobiydan salbiygacha qarab farqlanishi mumkin.

3 Oqibatlar sifat va miqdor jihatdan ifodalanishi mumkin.

4 Boshlang'ich oqibatlar «domino» prinsipi bo'yicha keyingi oqibatlar ko'payishini keltirib chiqarishi mumkin.

Воқеа-ходисанинг мақсадларга таъсир кўрсатишининг натижаси.

Изоҳлар

1 Воқеа-ходисанинг таъсир кўрсатиш натижаси битта ёки бир нечта оқибат бўлиши мумкин.

2 Оқибатлар маълум ёки номаълум бўлиши, ижобийдан салбийгача қараб фарқланиши мумкин.

3 Оқибатлар сифат ва миқдор жиҳатдан ифодаланиши мумкин.

4 Бошланғич оқибатлар «домино» принципи бўйича кейинги оқибатлар кўпайишини келтириб чиқариши мумкин.

Посредник

uz - vositachi

воситачи

en - proxy

Приложение, выполняемое на шлюзе, которое передает пакеты между авторизованным клиентом и внешним хостом. Посредник принимает запросы от клиента на определенные сервисы Интернет, а затем, действуя от имени клиента (т.е. выступая его посредником), устанавливает соединения для полученного запрошенного сервиса. Все шлюзы прикладного уровня используют связанные с приложениями программы-посредники. Большинство шлюзов сеансового уровня канальные посредники, которые обеспечивают те же функции перенаправления запросов, но поддерживают большую часть сервисов TCP/IP.

Shlyuzda bajariladigan, mualliflashtirilgan mijoz va tashqi xost o'rtasida paketlarni uzatuvchi ilova (dastur). Vositachi Internetning ma'lum servislari uchun mijozdan so'rov qabul qiladi, keyin, mijoz nomidan harakat qilib (ya'ni uning vositachisi bo'lib), rasmiy ravishda so'rab olingan servis uchun ulanishni o'rnatadi. Amaliy darajadagi barcha shlyuzlar ilovalar bilan bog'liq dastur-vositalardan foydalanadi. Seans darajasidagi ko'pchilik shlyuzlar so'rovlarni qayta yo'naltirishning aynan bir xil funksiyalarini ta'minlaydigan, lekin TCP/IP servislari-ning katta qismini tutib turadigan kanal vositachi-

П

laridir.

Шлюзда бажариладиган, муаллифлаштирилган мижоз ва ташқи хост ўртасида пакетларни узатувчи илова (дастур). Воситачи Интернетнинг маълум сервислари учун мижоздан сўров қабул қилади, кейин, мижоз номидан ҳаракат қилиб (яъни унинг воситачиси бўлиб), расмий равишда сўраб олинган сервис учун уланишни ўрнатади. Амалий даражадаги барча шлюзлар иловалар билан боғлиқ дастур-воситалардан фойдаланади. Сеанс даражасидаги кўпчилик шлюзлар сўровларни қайта йўналтиришнинг айнан бир хил функцияларини таъминлайдиган, лекин ТСП/IP сервисларининг қатта қисмини тутиб турадиган канал воситачиларидир.

Поставка

uz - yetkazib berish

етказиб бериш

en - delivery

Передача готового ОО из производственной среды потребителю.

Примечание – Эта стадия жизненного цикла продукта может включать упаковку и хранение в месте разработки, но не включает транспортировку незаконченного ОО или части ОО между различными разработчиками или разными местами разработки.

Tayyor BO ni ishlab chiqarish muhitidan iste'molchiga uzatish.

Izoh – Mahsulot hayotiy siklining bu bosqichi ishlab chiqish joyida o'rash va saqlashni ichiga olishi mumkin, biroq, tugallanmagan BO yoki BO qismlari turli ishlab chiquvchilar yoki turli ishlab chiqish joylari orasida tashilishini ichiga olmaydi.

Тайёр БО ни ишлаб чиқариш мухитидан истеъмолчига узатиш.

Изоҳ – Маҳсулот ҳаётий циклининг бу босқичи ишлаб чиқиш жойида ўраш ва сақлашни ичига олиши мумкин, бироқ, тугалланмаган БО ёки БО қисmlари турли ишлаб чиқувчилар ёки турли ишлаб чиқиш жойлари орасида ташилишини ичига олмайди.

Потенциал атаки

uz - hujum potensiali

ҳужум потенциали

en - attack potential

Мера усилия, которое нужно затратить на атаку объекта оценки, выраженная в показателях компетентности, ресурсов и мотивации нарушителя.

Baholash obyektiga hujum qilishda ishlatish uchun kerak bo'lgan, buzg'unchining kompetentlik, resurslar va motivatsiya ko'rsatkichlarida ifodalangan kuch

П

o'Ichovi.

Баҳолаш объектига ҳужум қилишда ишлатиш учун керак бўлган, бузгунчининг компетентлик, ресурслар ва мотивация кўрсаткичларида ифодаланган куч ўлчови.

Потеря или искажение информации

uz - axborotning yo'qotilishi yoki buzib ko'rsatilishi

ахборотнинг йўқотилиши

ёки бузиб кўрсатилиши

en - loss or corruption of information

Нарушение целостности переданных данных путем несанкционированного удаления, вставки, изменения порядка следования, повторного использования или задержки.

Ruxsat etilmagan tarzda chiqarib tashlash, kiritish, o'tish tartibini o'zgartirish, takror foydalanish yoki ushlab qolish yo'li bilan, uzatilgan ma'lumotlar yaxlitligining buzilishi.

Рухсат этилмаган тарзда чиқариб ташлаш, киритиш, ўтиш тартибини ўзгартириш, такрор фойдаланиш ёки ушлаб қолиш йўли билан, узатилган маълумотлар яхлитлигининг бузилиши.

Поток ключевой

uz - kalit oqimi

калит оқими

en - keystream

Длинная псевдослучайная последовательность, налагаемая на преобразуемое открытое сообщение с помощью побитового суммирования по модулю два.

Ikkining moduli bo'yicha bitma-bit jamlash yordamida o'zgartiriladigan ochiq xabarga qo'yiladigan uzun psevdotasodifiy ketma-ketlik.

Иккиннинг модули бўйича битма-бит жамлаш ёрдамида ўзгартириладиган очик хабарга қўйиладиган узун псевдотасодифий кетма-кетлик.

Потоки информационные

uz - axborot oqimlari

ахборот оқимлари

en - information flow

Совокупность передаваемой информации между двумя и более взаимодействующими объектами.

Ikki va undan ortiq o'zaro hamkorlik qiluvchi obyekt o'rtasida uzatiladigan axborot jami.

Икки ва ундан ортиқ ўзаро ҳамкорлик қилувчи объект ўртасида узатиладиган ахборот жами.

П

Потребность информационная

uz - axborotga bo'lgan ehtiyoj
ахборотга бўлган эҳтиёж
en - information need

Права пользователя

uz - foydalanuvchining
huquqlari
фойдаланувчининг
хуқуқлари
en - usr rights

Правила доступа

uz - foydalana olish
qoidalari
фойдалана олиш
қоидалари
en - access rule

Правила политики безопасности

uz - xavfsizlik siyosati

Достоверные знания, необходимые для управления целями, задачами, рисками и проблемами.

Maqsadlar, vazifalar, risklar va muammolarni boshqarish uchun zarur bo'ladigan haqiqiy bilimlar.

Мақсадлар, вазифалар, рисклар ва муаммоларни бошқариш учун зарур бўладиган ҳақиқий билимлар.

Возможность произвести вход в систему определенного типа и наличие тех или иных привилегий.

Ma'lum turdagi tizimga kirishni amalga oshirish imkoniyati va u yoki boshqa imtiyozlarning mavjudligi.

Маълум турдаги тизимга киришни амалга ошириш имконияти ва у ёки бошқа имтиёзларнинг мавжудлиги.

1 Совокупность правил, регламентирующих порядок и условия доступа к защищаемой информации и ее носителям.

2 Правила, установленные для осуществления доступа субъекта к информационному ресурсу с использованием штатных технических средств.

1 Muhofaza qilinadigan axborot va uning tashuvchilaridan foydalana olish tartibi va shartlarini qat'iy tartibga soladigan qoidalar jami.

2 Shtat texnik vositalaridan foydalangan holda, subyektning axborot resursidan foydalana olishini amalga oshirish maqsadida o'rnatilgan qoidalar.

1 Muhofaza qilinadigan axborot va uning tashuvchilaridan foydalana olish tartibi va shartlarini qat'iy tartibga soladigan qoidalar jami.

2 Shtat texnik vositalaridan foydalangan holda, subyektning axborot resursidan foydalana olishini amalga oshirish maqsadida o'rnatilgan qoidalar.

Местная информация, которая с учетом выбранных услуг безопасности определяет механизмы безопасности для применения, включая все пара-

II

qoidalari
xavfsizlik siёsati
қоидалари
en - security policy rules

метры, необходимые для работы данного механизма.

Tanlab olingan xavfsizlik xizmatlarini hisobga olgan holda, qo'llash uchun xavfsizlik mexanizmlarini, jumladan, ushbu mexanizmning ishlashi uchun zarur bo'lgan barcha parametrlarni belgilaydigan mahalliy axborot.

Танлаб олинган хавфсизлик хизматларини ҳисобга олган ҳолда, қўллаш учун хавфсизлик механизмларини, жумладан, ушбу механизмнинг ишлаши учун зарур бўлган барча параметрларни белгилайдиган маҳаллий ахборот.

**Правила разграничения
доступа**

uz - foydalana olishni
belgilash qoidalari
фойдалана олишни
белгилаш қоидалари
en - access demarcation rules

Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Foydalana olish subyektlarining foydalana olish obyektidan foydalana olish huquqlarini tartibga soluvchi qoidalar jami.

Фойдалана олиш субъектларининг фойдалана олиш объектидан фойдалана олиш ҳуқуқларини тартибга солувчи қоидалар жами.

Право авторское

uz - mualliflik huquqi
муаллифлик ҳуқуқи
en - copyright

Исключительное право, предоставляемое законом автору или его представителю, на воспроизведение, публикацию и копирование оригинальной работы.

Qonun tomonidan muallifga yoki uning vakiliga original ishni qayta tiklash, e'lon qilish va nusxa ko'chirish uchun taqdim etiladigan yagona huquq.

Қонун томонидан муаллифга ёки унинг вакилига оригинал ишни қайта тиклаш, эълон қилиш ва нусха кўчириш учун тақдим этиладиган ягона ҳуқуқ.

Право доступа

uz - foydalana olish huquqi
фойдалана олиш ҳуқуқи
en - access right

Совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Qonuniy hujjatlar yoki axborot egasi, mulkdori tomonidan belgilangan, muhofaza qilinadigan

II

axborotdan foydalanish qoidalarining jami.

Қонуний ҳужжатлар ёки ахборот эгаси, мулкдори томонидан белгиланган, муҳофаза қилинадиган ахборотдан фойдаланиш қоидаларининг жами.

Право доступа к записи

uz - yozuvdan foydalana olish huquqi

ёзувдан фойдалана олиш ҳуқуқи

en - write access control

Предоставление субъекту полномочий на запись (модификацию) определенной информации.

Subyektga ma'lum axborotni yozish (o'zgartirish) uchun vakolat berish.

Субъектга маълум ахборотни ёзиш (ўзгартириш) учун ваколат бериш.

Право доступа к чтению

uz - o'qish imkoniyatini olish huquqi

ўқиш имкониятини олиш ҳуқуқи

en - read access control

Предоставление субъекту полномочий на чтение определенной информации.

Subyektga ma'lum axborotni o'qish uchun vakolat berish.

Субъектга маълум ахборотни ўқиш учун ваколат бериш.

Право на доступ

uz - foydalana olish huquqi

фойдалана олиш ҳуқуқи

en - access right

Разрешение субъекту на получение доступа к определенному объекту для выполнения операции определенного вида.

Примечание – Примером права на доступ является разрешение на чтение файла, но не на запись в него.

Aniq turdagi amalni bajarish uchun subyektga muayyan obyektдан foydalana olish uchun ruxsat berish.

Izoh – Foydalana olish huquqiga faylga yozish emas, balki faylni o'qish uchun ruxsat hisoblanadi.

Аниқ турдаги амални бажариш учун субъектга муайян объектдан фойдалана олиш учун рухсат бериш.

Изоҳ – Фойдалана олиш ҳуқуқига файлга ёзиш эмас, балки файлни ўқиш учун рухсат ҳисобланади.

Предоставление права на доступ

Выдача разрешения (санкции) на использование определенных программ и данных.

II

uz - foydalana olish huquqlarini taqdim etish

фойдалана олиш

хуқуқларини тақдим этиш

en - authorization

Представление реализации

uz - amalga oshirishning taqdim etilishi

amalg'a oshirishning taqdim etilishi

амалга оширишнинг тақдим этилиши

тақдим этилиши

en - implementation

representation

Muayyan dasturlar va ma'lumotlardan foydalanishga ruxsat (sanksiya) berish.

Muayyan dasturlar va ma'lumotlardan foydalanishga ruxsat (sanksiya) beriш.

Наименее абстрактное представление ФБО, именно которое используется при создании собственно ФБО без дополнительной корректировки проекта.

Примечание – Примерами частей представления реализации являются исходный код, который затем компилируется, или схемы аппаратных средств, используемые при их производстве.

OXF yaratilishida loyihani ortiqcha to'g'rilashlarsiz ishlatiladigan, OXFning eng kam abstrakt taqdim etilishi.

Izoh – Keyin kompilyatsiya qilinadigan boshlang'ich kod yoki ularni ishlab chiqarishda qo'llaniladigan apparat vositalarning sxemalari amalga oshirish taqdim etilishining qismlari hisoblanadi.

OXF yaratilishida loyihani ortiqcha tug'rilashlarsiz ishlatiladigan, OXFning eng kam abstrakt taqdim etilishi.

Izoh – Keyin kompilyatsiya qilinadigan boshlang'ich kod yoki ularni ishlab chiqarishda qo'llaniladigan apparat vositalarning sxemalari amalga oshirish taqdim etilishining qismlari hisoblanadi.

Предъявление пароля

uz - parolni ko'rsatish

паролни кўрсатиш

en - sign-on

Завершение идентификации и установления подлинности пользователя.

Identifikatsiyalashning tugallanishi va foydalanuvchining haqiqiyligini o'rnatish.

Идентификациялашнинг тугалланиши ва фойдаланувчининг ҳақиқийлигини ўрнатиш.

Преобразование информации криптографическое

uz - axborotni kriptografik o'zgartirish

axborotni kriptografik o'zgartirish

ахборотни криптографик ўзгартириш

Процесс преобразования информации, основанный на применении криптографических методов (зашифрование и расшифрование, выработка и проверка электронной цифровой подписи, выработка и проверка хэш-функции).

Kriptografik metodlarni (shifrlash va rasshifrovka qilish elektron raqamli imzo hamda xesh-funksiyani

II

en - cryptographic transformation of information

Преобразования криптографические

uz - kriptografik o'zgartirishlar

криптографик ўзгартиришлар
en - cryptographic transformation

Препятствие

uz - to'siq tўsiq

en - interference

Прерывание

uz - uzilish uzilish

en - interrupt

Прерывание соединения
uz - bog'lanishning uzilishi

ishlab chiqish va tekshirish) qo'llashga asoslangan axborotni o'zgartirish jarayoni.

Криптографик методларни (шифрлаш ва расшифровка қилиш электрон рақамли имзо ҳамда хэш-функцияни ишлаб чиқиш ва текшириш) қўллашга асосланган ахборотни ўзгартириш жараёни.

Совокупность операций шифрования и дешифрования данных, а также перешифрования данных при смене шифра.

Ma'lumotlarni shifrlash va deshifrlash operatsiyalarining yig'indisi, shuningdek, shifr almashganda ma'lumotlarni qayta shifrlash.

Маълумотларни шифрлаш ва дешифрлаш операцияларининг йиғиндиси, шунингдек, шифр алмашганда маълумотларни қайта шифрлаш.

Метод организационного, технического, программного преграждения доступа к защищаемой информации и объекту.

Muhofaza qilinadigan axborot va obyektдан foydalanishga tashkiliy, texnik, dasturiy jihatdan to'siqinlik qilish metodi.

Муҳофаза қилинадиган ахборот ва объектдан фойдалана олишга ташкилий, техник, дастурий жиҳатдан тўсқинлик қилиш методи.

Сигнал, по которому компьютер прекращает выполнение программы и начинает выполнять служебную программу.

Компьютер dasturning bajarilishini to'xtatadigan va xizmat dasturi bajarilishini boshlaydigan signal.

Компьютер дастурнинг бажарилишини тўхтатадиган ва хизмат дастури бажарилишини бошлайдиган сигнал.

Разъединение, производимое в нарушение установленных процедур.

П

боғланишнинг узилиши
en - aborted connection

Примечание – Прерывание соединения может дать возможность другим логическим объектам получить несанкционированный доступ.

O‘rnatilgan protseduralar buzilgan holda amalga oshiriladigan uzib qo‘yish.

Izoh – Bog‘lanishning uzilishi boshqa mantiqiy obyektlarga ruxsat etilmagan tarzda foydalana olish imkoniyatini berishi mumkin.

Ўрнатилган процедуралар бузилган ҳолда амалга ошириладиган узиб қўйиш.

Изоҳ – Боғланишнинг узилиши бошқа мантикий объектларга рұхсат этилмаган тарзда фойдалана олиш имкониятини бериши мумкин.

**Преступление
компьютерное**
uz - kompyuter jinoyati
компьютер жинояти
en - computer crime

1 Осуществление несанкционированного доступа к информационному ресурсу, его модификация (подделка) или уничтожение с целью получения имущественных выгод для себя или для третьего лица, а также для нанесения имущественного ущерба своему конкуренту.

2 Преступление, совершённое с помощью или при непосредственном использовании системы обработки данных или компьютерной сети.

1 Axborot resursidan ruxsat etilmagan tarzda foydalana olish, uni o‘zgartirish (qalbakilashtirish) yoki o‘zi uchun yo uchinchi shaxs uchun mulkiy foyda olish, shuningdek, o‘z raqibiga mulkiy zarar yetkazish maqsadida bu resursni yo‘q qilish.

2 Ma’lumotlarni qayta ishlash tizimi yoki kompyuter tarmog‘i yordamida yoki undan bevosita foydalangan holda sodir etilgan jinoyat.

1 Axborot resursidan ruxsat etilmagan tarzda foydalana oliش, uni ўзгартириш (қалбакилаштириш) ёки ўзи учун ё учинчи шахс учун мулкий фойда олиш, шунингдек, ўз рақибига мулкий зарар етказиш мақсадида бу ресурсни йўқ қилиш.

2 Маълумотларни қайта ишлаш тизими ёки компьютер тармоғи ёрдамида ёки ундан бевосита фойдаланган ҳолда содир этилган жиноят.

Приватность

Запрет на вмешательство в личную жизнь или дела

II

uz - privatlik, xususiylik
 приватлик, хусусийлик
en - privacy

частного лица, если в результате этого вмешательства производятся чрезмерные или противозаконные накопление и использование данных этого лица.

Xususiy shaxsning shaxsiy hayoti yoki ishiga aralashuv natijasida shu shaxs ma'lumotlarini to'plash va ulardan foydalanish favqulodda yoki qonunga xilof ravishda bo'lganda bu aralashuvni taqiqlash.

Xususiy shaxsning shaxsiy hayoti yoki ishiga aralashuv natijasida shu shaxs ma'lumotlarini to'plash va ulardan foydalanish favqulodda yoki qonunga xilof ravishda bo'lganda bu aralashuvni taqiqlash.

Привилегии
uz - imtiyozlar
 имтиёзлар
en - privileges

Право выполнять привилегированные, т.е. доступные ограниченному кругу пользователей запросы к операционной системе. Например, запрос на изменение системного времени.

Operatsion tizimga yuborilgan imtiyozli, ya'ni cheklangan doiradagi foydalanuvchilar uchun mumkin bo'lgan so'rovlarni bajarish huquqi. Masalan, tizim vaqtini o'zgartirishga so'rov.

Operatsion tizimga yuborilgan imtiyozli, ya'ni cheklangan doiradagi foydalanuvchilar uchun mumkin bo'lgan so'rovlarni bajarish huquqi. Masalan, tizim vaqtini o'zgartirishga so'rov.

Пригодный/непригодный
uz - yaroqli/yaroqsiz
 яроқли/яроқсиз
en - stun/unstun

Функция, позволяющая сделать украденную радиостанцию непригодной для использования злоумышленником.

O'g'irlangan radiostansiyani jinoyatkor foydalanishi uchun yaroqsiz holatga keltirish imkonini beruvchi funksiya.

O'g'irlangan radiostansiyani jinoyatkor foydalanishi uchun yaroqsiz holatga keltirish imkonini beruvchi funksiya.

Признак объекта демас-

Технический демаскирующий признак, обуслов-

П

кирующий косвенный

uz - obyektning demaskirovkalovchi bilvosita belgisi

объектнинг

демаскировкаловчи билвосита белгиси

en - indirect unmask object characteristics

ленный действием обеспечивающих сил и средств или изменением окружающей среды в результате функционирования объекта защиты. К косвенным демаскирующим признакам относятся визуально-оптические признаки деятельности объекта, а также химическое или радиоактивное заражение местности.

Ta'minlovchi kuch va vositalarning harakati yoki muhofaza obyektining ishlashi natijasida atrof muhitning o'zgarishi bilan bog'liq demaskirovkalovchi texnik belgi. Bilvosita demaskirovkalovchi belgilarga obyekt faoliyatining vizual-optik belgilari, shuningdek, joyning kimyoviy yoki radioaktiv zararlanishi kiradi.

Ta'minlovchi kuch va vositalarning harakati yoki muhofaza obyektining ishlashi natijasida atrof muhitning o'zgarishi bilan bog'liq demaskirovkalovchi texnik belgi. Bilvosita demaskirovkalovchi belgilarga obyekt faoliyatining vizual-optik belgilari, shuningdek, joyning kimyoviy yoki radioaktiv zararlanishi kiradi.

Принуждение

uz - majburlash

мажбурлаш

en - enforcement

Метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Muhofaza metodi, bunga ko'ra foydalanuvchilar va tizim personalni moddiy, ma'muriy yoki jinoiy javobgarlik tahdidi ostida muhofaza qilinadigan axborotni qayta ishlash, uzatish va undan foydalanish qoidalariga rioya qilishga majbur bo'ladilar.

Muhofaza metodi, bunga ko'ra foydalanuvchilar va tizim personalni moddiy, ma'muriy yoki jinoiy javobgarlik tahdidi ostida muhofaza qilinadigan axborotni qayta ishlash, uzatish va undan foydalanish qoidalariga rioya qilishga majbur bo'ladilar.

П

Принцип «положено знать»
uz - «bilish zarur» prinsipi
«билиш зарур» принципи
en - need-to-know

1 Обоснованное требование предполагаемого получателя ознакомиться с необходимыми данными, получить к ним доступ или овладеть любой чувствительной информацией, содержащейся в этих данных.

2 Необходимость иметь доступ, знать или обладать специальной информацией для выполнения своих служебных обязанностей.

1 Faraz qilingan oluvchining zarur ma'lumotlar bilan tanishish, ulardan erkin foydalanishga ruxsat olish yoki ushbu ma'lumotlardagi istalgan ta'sirchan axborotga ega bo'lishning asoslangan talabi.

2 O'z xizmat vazifalarini bajarish uchun maxsus axborotdan erkin foydalanish huquqiga ega bo'lish, uni bilish yoki unga egalik qilishning zarurligi.

1 Фараз қилинган олувчининг зарур маълумотлар билан танишиш, улардан эркин фойдаланишга рухсат олиш ёки ушбу маълумотлардаги исталган таъсирчан ахборотга эга бўлишнинг асосланган талаби.

2 Ўз хизмат вазифаларини бажариш учун махсус ахборотдан эркин фойдаланиш ҳуқуқига эга бўлиш, уни билиш ёки унга эгалик қилишнинг зарурлиги.

Принцип Кирхгофа
uz - Kirxgof prinsipi
Кирхгоф принципи
en - Kirchhoff principal

Принцип построения криптографических алгоритмов, согласно которому в секрете держится только определенный набор их параметров (ключ), а все остальное может быть открытым без снижения стойкости алгоритма ниже допустимой величины.

Kriptografik algoritmlarni tuzish prinsipi. Unga ko'ra, bu algoritmlarning ma'lum bir to'plami (kalit) sir tutiladi, qolgan barchasi esa, algoritm bardoshliligini yo'l qo'yiladigan miqdordan pasaytirmasdan, ochiq bo'lishi mumkin.

Криптографик алгоритмларни тузиш принципи. Унга кўра, бу алгоритмларнинг маълум бир тўплами (калит) сир тугилади, қолган барчаси эса, алгоритм бардошлилигини йўл қўйиладиган миқдордан пасайтирмасдан, очиқ бўлиши мумкин.

П

Принятие риска

uz - riskni qabul qilish

riskni qabul qiliش

en - risk acceptance

1 Решение принять риск.

2 Решение администрации считать приемлемым некоторый уровень риска, как правило, по техническим или финансовым причинам.

1 Riskni qabul qilish qarori.

2 Ma'muriyatning qoida bo'yicha texnik yoki moliyaviy sabablarga ko'ra riskning ba'zi bir darajasini ma'qul deb hisoblaydigan qarori.

1 Riskni qabul qiliش qarori.

2 Ma'muriyatning qoida bo'yicha texnik e'ki moliyaviy sabablarga ko'ra riskning ba'zi bir darajasini ma'qul deb hisoblaydigan qarori.

Проверка безопасности

uz - xavfsizlikni tekshirish

xavfsizlikni tekshirish

en - security inspection

Независимый просмотр, изучение системных журналов и наблюдение за функционированием с целью определения достаточности средств контроля системы, соответствия принятой политике безопасности и процедурам обработки данных, обнаружения нарушений безопасности, выработки рекомендаций по изменению средств контроля и процедур безопасности.

Tizimni nazorat qilish vositalarining yetarliligini, qabul qilingan xavfsizlik siyosatiga va ma'lumotlarni qayta ishlash protseduralariga mosligini, xavfsizlik buzilishlarini aniqlash, nazorat vositalari va xavfsizlik protseduralarini o'zgartirish bo'yicha tavsiyalar ishlab chiqish maqsadida, tizim jurnallarini mustaqil ko'rib chiqish, o'rganish va ishlashi ustidan kuzatish olib borish.

Tizimni nazorat qiliش vositalarining yetarliligini, qabul qilingan xavfsizlik siyosatiga va ma'lumotlarni qayta ishlash protseduralariga mosligini, xavfsizlik buzilishlarini aniqlash, nazorat vositalari va xavfsizlik protseduralarini o'zgartirish bo'yicha tavsiyalar ishlab chiqish maqsadida, tizim jurnallarini mustaqil ko'rib chiqish, o'rganish va ishlashi ustidan kuzatish olib borish.

П

Проверка достоверности данных

uz - ma'lumotlarning ishonchliligini tekshirish
маълумотларнинг ишончилигини текшириш
en - data validation

Процесс, используемый для определения точности данных, их полноты или соответствия заданным критериям.

Примечание – Проверка достоверности данных может включать проверки их форматов и полноты, контрольные тесты ключа, проверки корректности и ограничений.

Ma'lumotlarning aniqligini, ularning to'liqligini yoki berilgan kriteriyalarga mosligini aniqlash uchun qo'llaniladigan jarayon.

Izoh – Ma'lumotlarning ishonchliligini tekshirish ularning formatlarini va to'liqligini tekshirish, kalitning nazorat testlari, to'g'riligini va cheklashlarni tekshirishdan iborat.

Маълумотларнинг аниқлигини, уларнинг тўлиқлигини ёки берилган критерийларга мослигини аниқлаш учун қўлланиладиган жараён.

Изоҳ – Маълумотларнинг ишончилигини текшириш уларнинг форматларини ва тўлиқлигини текшириш, калитнинг назорат тестлари, тўғрилигини ва чеклашларни текширишдан иборат.

Проверка криптографическая

uz - kriptografik tekshiruv
криптографик текширув
en - cryptographic verification

Процесс извлечения информации с помощью криптографического преобразования.

Kriptografik o'zgartirish yordamida axborot olish jarayoni.

Криптографик ўзгартириш ёрдамида ахборот олиш жараёни.

Проверка ограничения

uz - cheklashni tekshirish
чеклашни текшириш
en - limit check

Проверка, выполняемая, чтобы определить, находятся ли значения данных выше или ниже заданного значения или достигли установленного ограничения.

Ma'lumotlarning qiymatlari berilgan qiymatdan yuqorida yoki quyida turganligini yoki belgilangan cheklashga yetganligini aniqlash maqsadida bajariladigan tekshirish.

Маълумотларнинг қийматлари берилган қийматдан юқорида ёки қуйида турганлигини ёки белгиланган чеклашга етганлигини аниқлаш мақсадида бажариладиган текшириш.

П

Проверка подлинности

uz - haqiqiylikni tekshirish

хақиқийликни текшириш

en - authentication

Процедура, удостоверяющая, что пользователь именно тот, за кого себя выдает. В простейшем случае проверяется знание пользователем пароля, хранящегося в его учетной записи.

Foydalanuvchining, o'zini aynan shu odam deb ko'rsatishligini tasdiqlovchi protsedura. Oddiy holda foydalanuvchining, uning hisobga olish yozuvida saqlanadigan, parolni bilishi tekshiriladi.

Фойдаланувчининг, ўзини айнан шу одам деб кўрсатишлигини тасдиқловчи процедура. Оддий ҳолда фойдаланувчининг, унинг ҳисобга олиш ёзувида сақланадиган, паролни билиши текширилади.

Проверка подлинности сквозная

uz - ishonchlilikni yalpi

tekshirish

ишончлиликни ялпи

текшириш

en - throughout authentication

Проверка подлинности, при которой компьютер входа передает сведения, идентифицирующие пользователя, на другой компьютер.

Ishonchlilikni tekshirish, bunda kirish kompyuteri foydalanuvchini identifikatsiya qiluvchi axborotni boshqa kompyuterga uzatadi.

Ишончлиликни текшириш, бунда кириш компютери фойдаланувчини идентификация қилувчи ахборотни бошқа компютерга узатади.

Проверка правильности (данных) на входе

uz - kirishda (ma'lumotlarning)

to'g'riligini tekshirish

киришда (маълумотларнинг)

тўғрилигини

текшириш

en - input (data) validation

Процесс, используемый, чтобы определить неточность данных на входе, их незавершенность или нелогичность.

Ma'lumotlarning kirishda noaniqligini, ularning tugallanmay qolganligini yoki mantiqiy emasligini aniqlash maqsadida foydalaniladigan jarayon.

Маълумотларнинг киришда ноаниқлигини, уларнинг тугалланмай қолганлигини ёки мантиқий эмаслигини аниқлаш мақсадида фойдаланиладиган жараён.

Проверка системы

uz - tizimni tekshirish

тизимни текшириш

en - system checkout

Исследование процедур, используемых в системе, чтобы оценить их эффективность и правильность, а также рекомендовать усовершенствования.

Tizimda foydalaniladigan protseduralarni, ularning samaradorligini va to'g'riligini baholash, shuningdek, takomillashtirishni tavsiya etish maqsadida o'rganish.

П

Тизимда фойдаланиладиган процедураларни, уларнинг самарадорлигини ва тўғрилигини баҳолаш, шунингдек, такомиллаштиришни тавсия этиш мақсадида ўрганиш.

Программа

uz - dastur

дастур

en - program, programme

Последовательность операторов, предназначенных для реализации на ЭВМ.

ЕНМда amalga oshirish uchun mo‘ljallangan, operatorlar ketma-ketligi.

ЭХМда амалга ошириш учун мўлжалланган, операторлар кетма-кетлиги.

Программа антивирусная

uz - virusga qarshi dastur

вирусга қарши дастур

en - anti-virus program

Программа, предназначенная для обнаружения вирусов и, возможно, предлагающая удалить или удаляющая их.

Viruslarni aniqlash uchun mo‘ljallangan va ularni yo‘q qilish taklifini berishi mumkin bo‘lgan yoki yo‘q qiluvchi dastur.

Вирусларни аниқлаш учун мўлжалланган ва уларни йўқ қилиш таклифини бериши мумкин бўлган ёки йўқ қилувчи дастур.

Программа вредоносная

uz - zararli dastur

зарарли дастур

en - malicious logic

Программа, реализованная аппаратным, программно-аппаратным или программным способом и предназначенная для выполнения каких-либо несанкционированных или злоумышленных действий.

Примечание – Примерами вредоносных программ являются логическая бомба, троянская программа, вирус, червь.

Apparat, dasturiy-apparat yoki dasturiy usulda amalga oshirilgan va biror-bir ruxsat etilmagan yoki jinoyatkorona harakatlarni bajarish uchun mo‘ljallangan dastur.

Izoh – Zararli dasturlarga mantiqiy bomba, troyan oti, virus, qurt misol bo‘la oladi.

Аппарат, дастурий-аппарат ёки дастурий усулда амалга оширилган ва бирор-бир рухсат этилмаган ёки жинояткорона ҳаракатларни бажариш учун мўлжалланган дастур.

Изоҳ – Зарарли дастурларга мантиқий бомба, троян оти, вирус, қурт мисол бўла олади.

П

Программа

диагностическая

uz - diagnostik dastur

диагностик дастур

en - diagnostic routine

1 Программа запуска тестов для выявления возможных и реальных неисправностей в системе.

2 Программа, предназначенная для обнаружения, локализации и описания неисправностей технического оборудования или ошибок программ.

1 Tizimdagi mumkin bo'lgan va real nosozliklarni aniqlash uchun testlarni ishga tushirish dasturi.

2 Texnik uskuna nosozliklarini yoki dasturdagi xatoliklarni aniqlash, bartaraf etish va tavsiflash uchun mo'ljallangan dastur.

1 Tizimdaги mumkin бўлган ва реал носозликларни аниқлаш учун тестларни ишга тушириш дастури.

2 Техник ускуна носозликларини ёки дастурдаги хатоликларни аниқлаш, бартараф этиш ва тавсифлаш учун мўлжалланган дастур.

Программа самозагрузки

uz - o'z-o'zidan yuklash dasturi

ўз-ўзидан юклаш дастури

en - bootstrap

Минимальное множество команд, необходимое для загрузки операционной системы.

Operatsion tizimni yuklash uchun zarur bo'lgan komandalarning minimal ko'pligi.

Операцион тизимни юклаш учун зарур бўлган командаларнинг минимал кўплиги.

Программа-вакцина

uz - vaksina-dastur

вакцина-дастур

en - vaccine program

Программа, которая модифицирует другие программы и диски таким образом, что это не отражается на их работе, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными.

Boshqa dasturlar va diskarni, ularning ishiga ta'sir qilmaydigan darajada o'zgartiradigan dastur. Biroq, vaksinatsiya manbai bo'lgan virus bu dasturlar yoki disklar zararlanib bo'lgan deb hisoblaydi.

Бошқа дастурлар ва дискларни, уларнинг ишига таъсир қилмайдиган даражада ўзгартирадиган дастур. Бироқ, вакцинация манбаи бўлган вирус бу дастурлар ёки дисклар зарарланиб бўлган деб ҳисоблайди.

Программа TEMPEST

uz - TEMPEST dasturi

TEMPEST дастури

Программа изучения и анализа побочных электромагнитных сигналов, излучаемых электрическим и электронным оборудованием.

II

en - TEMPEST program

Elektr va elektron uskuna nurlantiradigan qo‘shimcha elektromagnit signallarni o‘rganish va tahlil qilish dasturi.

Электр ва электрон ускуна нурлантирадиган қўшимча электромагнит сигналларни ўрганиш ва таҳлил қилиш дастури.

Программы бесплатные

uz - bepul dasturlar

бепул дастурлар

en - freeware

Распространяемые бесплатно программы. Бесплатные программы не эквивалентны общедоступным программам, так как их разработчик сохраняет авторское право.

Bepul tarqatiladigan dasturlar. Bepul dasturlar, ularni ishlab chiquvchi mualliflik huquqini saqlab qolganligi tufayli, umumfoydalanish dasturlariga ekvivalent bo‘lmaydi.

Бепул тарқатиладиган дастурлар. Бепул дастурлар, уларни ишлаб чиқувчи муаллифлик ҳуқуқини сақлаб қолганлиги тўфайли, умумфойдаланиш дастурларига эквивалент бўлмайди.

Программы

доктора-реvisоры

uz - doktor-revizor dasturlar

доктор-реvisor дастурлар

en - doctor-inspector program

Программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут в случае изменений автоматически вернуть их в исходное состояние.

Fayllardagi va disklarning tizim sohalaridagi o‘zgarishlarni aniqlabgina qolmay, balki o‘zgarishlar yuz berganda ularni dastlabki holatga avtomatik ravishda qaytaradigan dasturlar.

Файллардаги ва дискларнинг тизим соҳаларидаги ўзгаришларни аниқлабгина қолмай, балки ўзгаришлар юз берганда уларни дастлабки ҳолатга автоматик равишда қайтарадиган дастурлар.

Программы общедоступные

uz - umumfoydalanish dasturlari

умумфойдаланиш

дастурлари

en - common access software

Программы, которые распространяются и используются бесплатно.

Bepul tarqatiladigan va foydalaniladigan dasturlar.

Бепул тарқатиладиган ва фойдаланиладиган дастурлар.

II

Программы-детекторы

uz - detektor dasturlar

детектор дастурлар

en - detector software

Программы, позволяющие обнаруживать файлы, зараженные одним из нескольких известных вирусов. Многие из этих программ имеют режимы лечения или уничтожения зараженных файлов.

Ma'lum bo'lgan bir qancha viruslarning biri bilan zararlangan fayllarni aniqlash imkonini beradigan dasturlar. Bu dasturlardan ko'pchiligi zararlangan fayllarni tuzatish yoki yo'q qilish rejimlariga ega.

Maълум бўлган бир қанча вирусларнинг бири билан зарарланган файлларни аниқлаш имконини берадиган дастурлар. Бу дастурлардан кўпчилиги зарарланган файлларни тузатиш ёки йўқ қилиш режимларига эга.

Программы-ревизоры

uz - revizor dasturlar

ревизор дастурлар

en - inspector programs

Программы, с помощью которых можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщается пользователю.

Shunday dasturlarki, ularning yordamida dasturlarning va disklar tizim sohalarining holatini dastlabki holat bilan taqqoslash mumkin. Aniqlangan nomuvofiqliklar to'g'risida foydalanuvchiga xabar qilinadi.

Шундай дастурларки, уларнинг ёрдамида дастурларнинг ва дисклар тизим соҳаларининг ҳолатини дастлабки ҳолат билан таққослаш мумкин. Аниқланган номувофиқликлар тўғрисида фойдаланувчига хабар қилинади.

Программы-фильтры

uz - filtr dasturlar

фильтр дастурлар

en - filter programs

Программы, располагающиеся резидентно в оперативной памяти компьютера и перехватывающие те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, а также сообщающие о них пользователям.

Kompyuterning operativ xotirasida rezident tarzda joylashgan va operatsion tizimga qilingan, viruslar ko'payish va zarar yetkazish uchun foydalanadigan murojaatlarni tutib oladigan, shuningdek, ular to'g'risida foydalanuvchiga xabar beradigan dasturlar.

II

Компьютернинг оператив хотирасида резидент тарзда жойлашган ва операцион тизимга қилинган, вируслар кўпайиш ва зарар етказиш учун фойдаланадиган мурожаатларни тутиб оладиган, шунингдек, улар тўғрисида фойдаланувчига хабар берадиган дастурлар.

Продажа вызовов

uz - chaqiruvlarni sotish

чақирувларни сотиш

en - call selling

Вид криминальной деятельности, при котором злоумышленник получает прибыль, продавая дорогостоящие вызовы со значительными скидками, используя одну или несколько линий телекоммуникаций с максимальной загрузкой, организуя нелегальные «телефонные переговорные пункты».

Jinoiy faoliyat turi, bunda jinoyatkor maksimal yuklanishdagi bitta yoki bir nechta telekommunikatsiyalar liniyasidan foydalangan holda, yashirin «telefon soʻzlashuv punktlari»ni tashkil qilib, baland narxli chaqiruvlarni katta chegirma bilan sotib, foyda oladi.

Жиноий фаолият тури, бунда жинояткор максимал юкланишдаги битта ёки бир нечта телекоммуникациялар линиясидан фойдаланган ҳолда, яширин «телефон сўзлашув пунктлари»ни ташкил қилиб, баланд нархли чақирувларни катта чегирма билан сотиб, фойда олади.

Продукт ИТ доверенный

uz - ishonchli AT mahsuloti

ишончли АТ маҳсулоти

en - trusted IT product

Продукт ИТ, находящийся вне ОО, функциональные требования безопасности которого в административном порядке согласованы с ОО, и который предположительно выполняет свои функциональные требования безопасности правильно.

Примечание – Примером доверенного продукта ИТ является отдельно оцененный продукт.

Baholash obyektida joylashmagan, xavfsizlikning funksional talablari BO bilan ma'muriy tartibda keli-shilgan hamda o'zining funksional xavfsizlik talablarini taxminan to'g'ri bajaradigan AT mahsuloti.

Izoh – АТning ishonchli mahsulotiga alohida baholangan mahsulot misol bo'lishi mumkin.

П

Баҳолаш объектида жойлашмаган, хавфсиз-ликнинг функционал талаблари БО билан маъмурий тартибда келишилган ҳамда ўзининг функционал хавфсизлик талабларини тахминан тўғри бажарадиган АТ маҳсулоти.

Изоҳ – АТнинг ишончли маҳсулотига алоҳида баҳоланган маҳсулот мисол бўлиши мумкин.

Проект системы управления информационной безопасности

uz - axborot xavfsizligini boshqarish tizimining loyihasi

ахборот хавфсизлигини бошқариш тизимининг лойиҳаси

en - information security management system project

Структурированные виды деятельности, принимаемые организацией при внедрении системы управления информационной безопасности.

Axborot xavfsizligini boshqarish tizimini joriy etishda tashkilot tomonidan amalga oshiriladigan, strukturalangan faoliyat turlari.

Ахборот хавфсизлигини бошқариш тизимини жорий этишда ташкилот томонидан амалга ошириладиган, структураланган фаолият турлари.

Производство

uz - ishlab chiqarish
ишлаб чиқариш

en - production

Стадия жизненного цикла, следующая за стадией «разработка», и заключающаяся в преобразовании представления реализации в реализацию ОО, то есть в состояние, пригодное для поставки потребителю.

Примечание – Эта стадия может включать производство, интеграцию, генерацию, внутреннюю транспортировку, хранение и маркировку ОО.

Hayotiy siklning «ishlab chiqish» bosqichidan keyin keladigan va amalga oshirish taqdim etilishini BOni amalga oshirishga, ya'ni iste'molchiga yetkazib berish uchun yaroqli holatga aylantirishda ifodalanadigan bosqichi.

Izoh – Bu bosqich ichiga BOni ishlab chiqarish, integratsiya, generatsiya, ichki tashishni, saqlash va markalashni oladi.

Ҳаётий циклнинг «ишлаб чиқариш» босқичидан кейин келадиган ва амалга ошириш тақдим этилишини БОни амалга оширишга, яъни истеъмолчига етказиб бериш учун яроқли ҳолатга айлантдиришда ифодаланадиган босқичи.

Изоҳ – Бу босқич ичига БОни ишлаб чиқариш, интеграция, генерация, ички ташишни, сақлаш ва маркалашни олади.

П

Проникновение

uz - suqulib kirish

суқулиб кириш

en - penetration

1 Успешное преодоление механизмов защиты системы.

2 Несанкционированный доступ к системе обработки данных.

1 Tizimning muhofaza qilish mexanizmlarini muvaffaqiyatli yengib o'tish.

2 Ma'lumotlarni qayta ishlash tizimiga ruxsat etilmagan tarzda kirish.

1 Tizimning muhofaza qilish mexanizmlarini muvaffaqiyatli engib o'tish.

2 Ma'lumotlarni qayta ishlash tizimiga ruxsat etilmagan tarzda kirish.

Проследивать,

сопоставлять

uz - kuzatmoq, taqqoslamoq

кузатмоқ, таққосламоқ

en - trace

Выполнять неформальный анализ соответствия между двумя логическими объектами с минимальным уровнем строгости.

Eng kam talabchanlik bilan ikkita mantiqiy obyekt o'rtasidagi muvofiqlikning norasmiy tahlilini bajarish.

Eng kam talabchanlik bilan ikkita mantiqiy obyekt o'rtasidagi muvofiqlikning norasmiy tahlilini bajarish.

Прослушивание

uz - eshitish

эшитиш

en - eavesdropping

1 Несанкционированный перехват информационных излучений.

2 Перехват злоумышленником передаваемой по сети информации с целью выявления и последующего использования слабых мест системы защиты.

1 Axborot nurlanishlarini ruxsat etilmagan tarzda tutib olish.

2 Muhofaza qilish tizimining sust joylarini aniqlash va undan keyinchalik foydalanish maqsadida tarmoq bo'yicha uzatiladigan axborotni jinoyatkor tomonidan qo'lga kiritilishi.

1 Axborot nurlanishlarini ruxsat etilmagan tarzda tutib olish.

2 Muhofaza qilish tizimining sust joylarini aniqlash va undan keyinchalik foydalanish maqsadida tarmoq bo'yicha uzatiladigan axborotni jinoyatkor tomonidan qo'lga kiritilishi.

П

Просмотр

uz - ko‘rib chiqish

кўриб чиқиш

en - browsing

Поиск информации, нередко преследующий цель получения несанкционированного доступа к конфиденциальным данным и представляющий в этом случае угрозу для системы.

Axborot izlash bo‘lib, ko‘pincha konfidensial ma‘lumotlardan ruxsat etilmagan tarzda foydalanishni maqsad qilib qo‘yadi, shu tufayli tizim uchun xavf tug‘diradi.

Ахборот излаш бўлиб, кўпинча конфиденциал маълумотлардан рухсат этилмаган тарзда фойдаланишни мақсад қилиб қўяди, шу туфайли тизим учун хавф туғдиради.

Противодействие

сетевым угрозам

uz - tarmoq tahdidlariga

qarshi turish

тармоқ таҳдидларига

қарши туриш

en - network threat

counteraction

Комплекс мер безопасности, предназначенный для защиты сетевой инфраструктуры от атак злоумышленников.

Tarmoq infrastrukturasini jinoyatkorlarning hujumlaridan muhofaza qilish uchun mo‘ljallangan xavfsizlik choralari kompleksi.

Тармоқ инфраструктурасини жинояткорларнинг хужумларидан муҳофаза қилиш учун мўлжалланган хавфсизлик чоралари комплекси.

Противостоять

uz - qarama-qarshi turmoq

(qarshi turmoq)

карама-қарши турмоқ

(қарши турмоқ)

en - counter

Уменьшать воздействие конкретной угрозы, но не обязательно устранять ее полностью.

Аниқ таҳдидларнинг таъсирини камайтириш, бироқ, бутунлай бартараф этиш шарт эмас.

Аниқ таҳдидларнинг таъсирини камайтириш, бироқ, бутунлай бартараф этиш шарт эмас.

Протокол безопасной

передачи данных

uz - ma‘lumotlarni xavfsiz

uzatish protokoli

маълумотларни хавфсиз

узатиш протоколи

en - secure sockets layer

Протокол, используемый для окончного шифрования трафика на прикладном уровне.

Amaliy darajada trafikni oxirgi shifrlash uchun foydalaniladigan protokol.

Амалий даражада трафикни охирги шифрлаш учун фойдаланиладиган протокол.

П

Протокол

криптографический

uz - kriptografik protokol

криптографик протокол

en - cryptographic protocol

1 Алгоритм, посредством которого две или более стороны обмениваются некоторой информацией и который гарантирует безопасность обмениваемой информации. Такой алгоритм использует криптографические преобразования и обычно базируется на криптографии с открытыми ключами.

2 Набор правил и процедур, определяющих использование криптоалгоритма и ключей шифрования.

3 Протокол, предусматривающий взаимодействие двух и более сторон с использованием криптографических алгоритмов.

1 Algoritm, uning vositasida ikki yoki undan ortiq tomon qandaydir axborotni almashinadi va almashinadigan axborotning xavfsizligi kafolatlanadi. Bunday algoritm kriptografik o'zgartirishlardan foydalanadi va odatda, ochiq kalitli kriptografiyaga asoslanadi.

2 Kriptoalgoritmdan va shifrlash kalitlaridan foydalanishni belgilaydigan qoidalar va protseduralar to'plami.

3 Kriptografik algoritmlardan foydalangan holda, ikki va undan ko'p tomonning o'zaro ishlashini ko'zda tutuvchi protokol.

1 Алгоритм, унинг воситасида икки ёки ундан ортиқ томон қандайдир ахборотни алмашинади ва алмашинадиган ахборотнинг хавфсизлиги кафолатланади. Бундай алгоритм криптографик ўзгартиришлардан фойдаланади ва одатда, очик калитли криптографияга асосланади.

2 Кристоалгоритмдан ва шифрлаш калитларидан фойдаланишни белгилайдиган қоидалар ва процедуралар тўплами.

3 Криптографик алгоритмлардан фойдаланган ҳолда, икки ва ундан кўп томоннинг ўзaro ишлашини кўзда тутувчи протокол.

Протокол отрицания

uz - inkor qilish protokoli

инкор қилиш протоколи

en - denial protocol

Тип протокола, не позволяющий подписывающему лицу отказаться от подписанного сообщения.

II

Imzo chekuvchi shaxsga imzolangan xabarni rad qilishiga yo‘l qo‘ymaydigan protokol turi.

Имзо чекувчи шахсга имзоланган хабарни рад қилишига йўл қўймайдиган протокол тури.

Протокол распределения ключей

uz - kalitlarni taqsimlash protokoli

калитларни тақсимлаш протоколи

en - key distribution protocol

Протокол, в результате выполнения которого взаимодействующие стороны (пользователи, группы пользователей) получают необходимые для функционирования криптографической системы ключи.

Bajarilishi natijasida birgalikda ishlaydigan tomonlar (foydalanuvchilar, foydalanuvchilar guruhi) kriptografik tizim ishlashi uchun zarur bo‘lgan kalitlarni oladigan protokol.

Бажарилиши натижасида биргаликда ишлайдиган томонлар (фойдаланувчилар, фойдаланувчилар гуруҳи) криптографик тизим ишлаши учун зарур бўлган калитларни оладиган протокол.

Протокол с арбитром

uz - arbitrli protokol

арбитрли протокол

en - protocol with arbiter

Криптографический протокол, в котором используется одна или несколько незаинтересованных доверенных сторон (арбитров). Доверенность означает, что все участники протокола признают, что любые утверждения или действия арбитра истинны и корректны.

Bir yoki bir nechta manfaatdor bo‘lmagan vakolatli tomonlar (atributlar) dan foydalaniladigan kriptografik protokol. Vakolatnoma, protokolning barcha ishtirokchilari arbitrning har qanday tasdiqlashi yoki harakatlari to‘g‘ri va haqiqiy ekanligini tan olishlarini bildiradi.

Бир ёки бир нечта манфаатдор бўлмаган ваколатли томонлар (атрибутлар) дан фойдаланиладиган криптографик протокол. Ваколатнома, протоколнинг барча иштирокчилари арбитранинг ҳар қандай тасдиқлаши ёки ҳаракатлари тўғри ва ҳақиқий эканлигини тан олишларини билдиради.

II

Протокол с третейским судьей

uz - manfaatdor boʻlmagan hakam protokoli

манфаатдор бўлмаган хакам протоколи

en - protocol with arbitrator

Протокол, аналогичный протоколу с арбитром, но в отличие от последнего, третейский судья появляется только в случае возникновения спорных ситуаций между участниками протокола. Третейский судья, в отличие от арбитра, не участвует напрямую в протоколе, однако существуют данные, которые позволяют третейскому судье определить обман.

Arbitrli protokolga oʻxshash protokol, lekin undan farqli ravishda manfaatdor boʻlmagan hakam faqat protokol ishtirokchilari oʻrtasida bahsli holatlar yuz bergan hollardagina paydo boʻladi. Manfaatdor boʻlmagan hakam, arbitrdan farqli ravishda, toʻgʻridan-toʻgʻri protokolda ishtirok etmaydi, lekin manfaatdor boʻlmagan hakamga aldovni aniqlash uchun imkon beradigan maʼlumotlar mavjud boʻladi.

Арбитрли протоколга ўхшаш протокол, лекин ундан фарқли равишда манфаатдор бўлмаган хакам фақат протокол иштирокчилари ўртасида баҳсли ҳолатлар юз берган ҳоллардагина пайдо бўлади. Манфаатдор бўлмаган хакам, арбитрдан фарқли равишда, тўғридан-тўғри протоколда иштирок этмайди, лекин манфаатдор бўлмаган хакамга алдовни аниқлаш учун имкон берадиган маълумотлар мавжуд бўлади.

Протокол, самообеспечивающий законность

uz - qonuniylikni oʻzi taʼminlaydigan protokol

қонунийликни ўзи таъминлайдиган протокол

en - self maintain law protocol

Один из лучших типов криптографических протоколов, позволяющих обойтись без третьей стороны. В данном типе протокола он сам гарантирует соблюдение всех правил. Такой протокол построен так, что в случае возникновения обмана с одной стороны, другая сторона всегда может определить это.

Kriptografik protokollarning uchinchi tomonga ehtiyoj boʻlmagan eng yaxshi turlaridan biri. Protokol barcha qoidalarga rioya qilinishini kafolatlaydi. Bunday protokol bir tomonda aldov paydo boʻlganda, boshqa tomon har doim buni aniqlashi mumkin boʻlgan tarzda tuzilgan.

Криптографик протоколларнинг учинчи томонга эҳтиёж бўлмаган энг яхши турларидан бири.

П

Протокол барча қоидаларга риоя қилинишини кафолатлайди. Бундай протокол бир томонда алдов пайдо бўлганда, бошқа томон ҳар доим буни аниқлаши мумкин бўлган тарзда тузилган.

Протоколы

uz - protokollar

протоколлар

en - protocols

1 Набор правил и форматов семантических и синтаксических, позволяющих различным компонентам системы обмениваться информацией (например, узлам сети).

2 Согласованные процедуры передачи данных между различными объектами вычислительной системы.

1 Tizimning turli komponentlariga (masalan, tarmoq uzellariga) axborot almashinishi uchun imkon beruvchi semantik va sintaksik qoidalar, formatlar to'plami.

2 Hisoblash tizimining turli obyektlari o'rtasida ma'lumotlar uzatishning kelishilgan protseduralari.

1 Tizimning turli komponentlariga (masalan, tarmoq uzellariga) axborot almashinishi uchun imkon beruvchi semantik va sintaksik qoidalar, formatlar to'plami.

2 Hisoblash tizimining turli obyektlari o'rtasida ma'lumotlar uzatishning kelishilgan protseduralari.

Профиль защиты

uz - himoya profili

ҳимоя профили

en - protection profile

1 Не зависящая от реализации (не связанная с реализацией) совокупность требований безопасности для некоторой категории объектов оценки, отвечающей специфическим потребностям потребителя.

2 Функционально полный, прошедший апробацию, стандартизированный набор требований, предназначенный для многократного использования.

1 Amalga oshirish bilan bog'liq bo'lmagan, iste'molchining spetsifik ehtiyojlariga javob beradigan, qandaydir kategoriyadagi baholash obyektlari uchun mo'ljallangan, xavfsizlik talablarining jami.

2 Funktsional jihatdan to'la, aprobatsiyadan o'tgan, ko'p marotaba foydalanish uchun mo'ljallangan, standartlashtirilgan talablar to'plami.

II

1 Амалга ошириш билан боғлиқ бўлмаган, истеъмолчининг специфик эҳтиёжларига жавоб берадиган, қандайдир категориядаги баҳолаш объектлари учун мўлжалланган, хавфсизлик талабларининг жами.

2 Функционал жиҳатдан тўла, апробациядан ўтган, кўп маротаба фойдаланиш учун мўлжалланган, стандартлаштирилган талаблар тўплами.

Профиль полномочий

uz - vakolatlar profili

ваколатлар профили

en - authorized profile

Список защищаемых объектов системы и прав доступа к ним, ассоциированный с каждым объектом. При обращении к объекту профиль субъекта проверяется на наличие соответствующих прав доступа. Профиль представляется в виде строки матрицы доступа.

Nar bir subyekt bilan assotsiatsiyalangan tizimning muhofaza qilinadigan obyektlari va ulardan erkin foydalanish huquqlari ro‘yxati. Obyektga murojaat qilishda subyekt profili foydalanishning tegishli huquqlari mavjudligiga tekshiriladi. Profil erkin foydalanish matritsasining satri ko‘rinishida taqdim etiladi.

Ҳар бир субъект билан ассоциацияланган тизимнинг муҳофаза қилинадиган объектлари ва улардан эркин фойдаланиш ҳуқуқлари рўйхати. Объектга мурожаат қилишда субъект профили фойдаланишнинг тегишли ҳуқуқлари мавжудлигига текширилади. Профиль эркин фойдаланиш матрицасининг сатри кўринишида тақдим этилади.

Профиль пользователя

uz - foydalanuvchining profili

фойдаланувчининг профили

en - user profile

1 Описание пользователя, обычно используемое для управления доступом.

Примечание – Профиль пользователя может содержать такие данные как идентификатор пользователя, имя пользователя, пароль, права на доступ и другие атрибуты.

2 Образец деятельности пользователя, который может использоваться для обнаружения изменений в его деятельности.

1 Odatda, erkin foydalanishni boshqarish uchun qo‘llaniladigan foydalanuvchining tavsifi.

Izoh – Foydalanuvchining profili foydalanuvchining identif-

II

ikator, foydalanuvchining nomi, parol, erkin foydalanish huquqi va boshqa atributlardan iborat bo'lishi mumkin.

2 Foydalanuvchi faoliyatining namunasi foydalanuvchining faoliyatidagi o'zgarishlarni aniqlash uchun qo'llaniladi.

1 Одатда, эркин фойдаланишни бошқариш учун қўлланиладиган фойдаланувчининг тавсифи.

Изоҳ – Фойдаланувчининг профили фойдаланувчининг идентификатори, фойдаланувчининг номи, пароль, эркин фойдаланиш ҳуқуқи ва бошқа атрибутлардан иборат бўлиши мумкин.

2 Фойдаланувчи фаолиятининг намунаси фойдаланувчининг фаолиятидаги ўзгаришларни аниқлаш учун қўлланилади.

Проход через систему защиты, обходной путь

uz - muhofaza tizimi orqali o'tish, aylanma yo'l

муҳофаза тизими орқали ўтиш, айланма йўл

en - security trapdoor, bypass path

Процедура резервирования

uz - rezervlash protsedurasi

резервлаш процедураси

en - backup procedure

Процедуры

восстановительные

uz - tiklovchi protseduralar

тикловчи процедуралар

en - recovery procedures

Блок обхода, встроенный в систему шифрования.

Shifrlash tizimiga kiritilgan chetlab o'tish bloki.

Шифрлаш тизимига киритилган четлаб ўтиш блоки.

Процедура, предусматривающая реставрацию данных после сбоя или аварии. Например, создание резервных файлов.

To'xtab qolish yoki avariya dan keyin ma'lumotlarning qayta tiklanishini ko'zda tutuvchi protsedura. Masalan, rezerv fayllarni yaratish.

T'uxtab qolish ёки авариядан кейин маълумотларнинг қайта тикланишини кўзда тутувчи процедура. Масалан, резерв файлларни яратиш.

Действия, предпринимаемые для восстановления способности системы обрабатывать информацию, а также восстановление наборов данных после аварии или сбоя.

Tizimning axborotni qayta ishlash qobiliyatini tiklash uchun qilinadigan harakatlar, shuningdek, avariya yoki to'xtab qolishdan so'ng ma'lumotlar to'p-

II

lamlarini tiklash.

Тизимнинг ахборотни қайта ишлаш қобилятини тиклаш учун қилинадиган ҳаракатлар, шунингдек, авария ёки тўхтаб қолишдан сўнг маълумотлар тўпламларини тиклаш.

Процедуры приемки

uz - qabul qilib olish
protseduralari

қабул қилиб олиш
процедуралари

en - acceptance procedures

Процедуры, выполняемые последовательно при приемке вновь созданных или модифицированных элементов конфигурации в составе ОО или при переводе их на следующую стадию жизненного цикла.

Примечание – Эти процедуры идентифицируют роли или лица, ответственные за приемку и критерии принятия решения о приемке.

BO tarkibida konfiguratsiyaning yangi yaratilgan yoki o'zgartirilgan elementlarini qabul qilishda yoki ularni hayotiy siklning keyingi bosqichiga o'tkazishda ketma-ket bajariladigan protseduralar.

Izoh – Bu protseduralar qabul qilishga mas'ul bo'lgan rollar yoki shaxslarni va qabul qilib olish to'g'risida qaror qabul qilish kriteriyalarini identifikatsiyalaydi.

BO tarkibida konfiguratsiyaning yangi yaratilgan ёки ўзгартирилган элементларини қабул қилишда ёки уларни ҳаётий циклнинг кейинги босқичига ўтказишда кетма-кет бажариладиган процедуралар.

Изоҳ – Бу процедуралар қабул қилишга масъул бўлган роллар ёки шахсларни ва қабул қилиб олиш тўғрисида қарор қабул қилиш кriterийларини идентификациялайди.

Процесс

uz - jarayon
жараён

en - process

1 Объект операционной системы, включающий, помимо прочего, защищенную область памяти с исполняемым кодом и данными, один или несколько потоков исполнения и главный маркер доступа.

2 Выполняющаяся программа.

3 Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

1 Xotiraning bajariluvchi kodlar va ma'lumotlar bilan muhofazalangan sohasini, bir yoki bir nechta bajarish oqimini hamda foydalanishning bosh marke-

II

rini o‘z ichiga oluvchi operatsion tizim obyektii.

2 Bajarilayotgan dastur.

3 Kirishlarni chiqishlarga o‘zgartiruvchi o‘zaro bog‘langan va o‘zaro harakat qiluvchi faoliyat turlari yig‘indisi.

1 Хотиранинг бажарилувчи кодлар ва маълумотлар билан муҳофазаланган соҳасини, бир ёки бир нечта бажариш оқимини ҳамда фойдаланишнинг бош маркерини ўз ичига олувчи операцион тизим объекти.

2 Бажарилаётган дастур.

3 Киришларни чиқишларга ўзгартирувчи ўзаро боғланган ва ўзаро ҳаракат қилувчи фаолият турлари йиғиндиси.

Процесс управления риском

uz - riskni boshqarish jarayoni

riskni бошқариш

жараёни

en - risk management process

Взаимосвязанные действия по обмену информацией, консультациям, установлению целей, области применения, идентификации, исследованию, оценке, обработке, мониторингу и анализу риска, выполняемые в соответствии с политикой, процедурами и методами управления организации.

Примечание – Термин «процесс» используется для полного описания управления риском. Элементы в пределах процесса управления риском называют «деятельностью».

Tashkilotni boshqarish siyosati, protseduralari va usullariga muvofiq bajariladigan, axborot almashinuvi, maslahatlashuvlar, maqsadlarni belgilash, qo‘llash sohasi, riskni identifikatsiya qilish, tadqiq qilish, baholash, qayta ishlash, monitoring va tahlil qilish bo‘yicha o‘zaro bog‘langan xatti-harakatlar.

Izoh – Riskni boshqarishni to‘liq tavsiflash uchun «jarayon» atamasidan foydalaniladi. Riskni boshqarish jarayoni doirasidagi elementlar «faoliyat» deb ataladi.

Ташкилотни бошқариш сиёсати, процедуралари ва усулларига мувофиқ бажариладиган, ахборот алмашинуви, маслаҳатлашувлар, мақсадларни белгилаш, қўллаш соҳаси, рискни идентификация қилиш, тадқиқ қилиш, баҳолаш, қайта ишлаш, мониторинг ва таҳлил қилиш бўйича ўзаро боғланган хатти-ҳаракатлар.

Изоҳ – Рискни бошқаришни тўлиқ тавсифлаш учун

II

«жараён» атамасидан фойдаланилади. Рискни бошқариш жараёни доирасидаги элементлар «фаолият» деб аталади.

Процессы информационные

uz - axborot jarayonlari

ахборот жараёнлари
en - informational process

Процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Axborotni yig‘ish, qayta ishlash, to‘plash, saqlash, izlash va tarqatish jarayonlari.

Ахборотни йиғиш, қайта ишлаш, тўплаш, сақлаш, излаш ва тарқатиш жараёнлари.

Прошивка сети

uz - tarmoqdan kirib olish

тармоқдан кириб олиш
en - network weaving

Способ проникновения, при котором используются различные сети телекоммуникаций с целью получить доступ к системе обработки данных и при этом избежать обнаружения и определения местонахождения.

Suqulib kirish usuli, bunda ma’lumotlarni qayta ishlash tizimiga kira olish yo‘lini topish maqsadida telekommunikatsiyalarning turli tarmoqlaridan foydalaniladi, joylashgan o‘rin aniqlanishi mumkin bo‘lgan hollarning oldi olinadi.

Suqulib kirish usuli, bunda ma’lumotlarni qayta ishlash tizimiga kira olish yo‘lini topish maqsadida telekommunikatsiyalarning turli tarmoqlaridan foydalaniladi, joylashgan o‘rin aniqlanishi mumkin bo‘lgan hollarning oldi olinadi.

Пункт обработки данных запасной

uz - ma’lumotlarni qayta
ishlash zaxira punkti

маълумотларни қайта
ишлаш захира пункти
en - cold site

Возможно минимальное количество оборудования, необходимого для инсталляции и задействования резервной системы обработки данных.

Instalyatsiya va ma’lumotlarni qayta ishlash rezerv tizimi ishga tushirilishi uchun zarur uskuning mumkin bo‘lgan minimal miqdori.

Инсталляция ва маълумотларни қайта ишлаш резерв тизими ишга туширилиши учун зарур ускунинг мумкин бўлган минимал миқдори.

Пункт обработки данных резервный

uz - ma’lumotlarni qayta
ishlash rezerv punkti

маълумотларни қайта
ишлаш резерв пункти

Полностью оборудованный вычислительный центр, который обеспечивает возможность немедленной альтернативной обработки данных.

Ma’lumotlarni zudlik bilan muqobil qayta ishlash imkonini beruvchi, to‘liq jihozlangan hisoblash markazi.

П

en - hot site

Путь доступа

uz - kira olish (foydalana olish) yo‘li

кира олиш (фойдалана олиш) йўли

en - access path

Маълумотларни зудлик билан муқобил қайта ишлаш имконини берувчи, тўлиқ жиҳозланган ҳисоблаш маркази.

Последовательность элементов данных, которые используются системой управления базой данных для доступа к записям или другим элементам данных, хранящимся в базе данных.

Ma'lumotlar elementlarining ketma-ketligi, ular ma'lumotlar bazasini boshqarish tizimi tomonidan yozuvlardan yoki ma'lumotlar bazasida saqlanadigan ma'lumotlarning boshqa elementlaridan erkin foydalanishda qo'llaniladi.

Маълумотлар элементларининг кетма-кетлиги, улар маълумотлар базасини бошқариш тизими томонидан ёзувлардан ёки маълумотлар базасида сақланадиган маълумотларнинг бошқа элементларидан эркин фойдаланишда қўлланилади.

Путь обхода системы защиты

uz - muhofaza qilish tizimini chetlab o'tish yo‘li

муҳофаза қилиш тизимини четлаб ўтиш йўли

en - trapdoor

Результат действия, при котором объект системы претерпевает изменение, для того чтобы позволить злоумышленнику оказать несанкционированное влияние на команду или на predetermined событие или на последовательность событий. Например, проверка пароля может быть изменена таким образом, что помимо своего обычного результата она подтверждает также правильность пароля злоумышленника.

Harakat natijasi bo'lib, bunda tizim obyektini jinoyatkorga komandaga yoki oldindan belgilangan voqega yoki voqealar ketma-ketligiga ruxsat etilmagan tarzda ta'sir ko'rsatish imkonini beradigan darajada o'zgaradi. Masalan, parolni tekshirish shunday o'zgartirilishi mumkinki, u o'zining odatdagi natijasidan tashqari, jinoyatkor parolining to'g'riligini ham tasdiqlaydi.

Ҳаракат натижаси бўлиб, бунда тизим объекти жинояткорга командага ёки олдиндан белгиланган воқеага ёки воқеалар кетма-кетлигига рухсат этилмаган тарзда таъсир кўрсатиш имконини

П

Путь проникновения

uz - suqulib kirish yo‘li
сукулиб кириш йўли
en - penetration route

берадиган даражада ўзгаради. Масалан, паролни текшириш шундай ўзгартирилиши мумкинки, у ўзининг одатдаги натижасидан ташқари, жинояткор паролининг тўғрилигини ҳам тасдиқлайди.

Последовательность несанкционированных действий пользователя при его проникновении в защищенную систему.

Muhofazalangan tizimga suqulib kirish paytida, foydalanuvchi ruxsat etilmagan harakatlarining ketma-ketligi.

Муҳофазаланган тизимга сукулиб кириш пайтида, фойдаланувчи рухсат этилмаган ҳаракатларининг кетма-кетлиги.

Путь сертификата

uz - sertifikat yo‘li
сертификат йўли
en - certification path

Упорядоченная последовательность сертификатов объектов в информационном дереве каталога, которая вместе с открытым ключом первоначального объекта данного пути может быть обработана для получения открытого ключа конечного объекта данного пути.

Obyektlar sertifikatlarining, katalogning axborot daraxtidagi tartiblashtirilgan ketma-ketligi bo‘lib, berilgan yo‘l boshlang‘ich obyektining ochiq kaliti bilan birga shu yo‘l oxirgi obyektining ochiq kalitini olish maqsadida qayta ishlanishi mumkin.

Объектлар сертификатларининг, каталогнинг ахборот дарахтидаги тартиблаштирилган кетма-кетлиги бўлиб, берилган йўл бошланғич объектининг очик калити билан бирга шу йўл охириги объектининг очик калитини олиш мақсадида қайта ишланиши мумкин.

«Пятна родимые»

uz - «xol»
«хол»
en - birthmarks

Присущие автору в процессе написания программы особенности стиля: типичные ошибки, избыточные данные и характерные черты программирования, позволяющие выявить очевидность заимствования.

Dasturni yozish jarayonida muallifga xos uslubning xossasi: tipik xatolar, o‘zlashtirmaning ayonligini aniqlashga imkon beruvchi ortiqcha ma’lumotlar va dasturlashdagi xarakterli xususiyatlar.

П

Дастурни ёзиш жараёнида муаллифга хос услубнинг хоссаси: типик хатолар, ўзлаштирманинг аёнлигини аниқлашга имкон берувчи ортикча маълумотлар ва дастурлашдаги характерли хусусиятлар.

Р

Работа секретная

uz - maxfiy ish

махфий иш

en - secret work

Научно-исследовательские, опытно-конструкторские, проектные, технологические, изыскательские и иные работы (в том числе работы студентов, дипломников, диссертантов), а также любые сведения, предусмотренные в перечне сведений, подлежащих засекречиванию.

Ilmiy-tadqiqot, tajriba-konstruktorlik, loyiha, texnologik, qidiruv va boshqa ishlar (shu jumladan, talabalar, diplomniklar, dissertantlarning ishlari), shuningdek, maxfiylashtirish lozim bo'lgan ma'lumotlar ro'yxatida ko'zda tutilgan har qanday ma'lumot.

Илмий-тадқиқот, тажриба-конструкторлик, лойиҳа, технологик, қидирув ва бошқа ишлар (шу жумладан, талабалар, дипломниклар, диссертантларнинг ишлари), шунингдек, махфийлаштириш лозим бўлган маълумотлар рўйхатида кўзда тутилган ҳар қандай маълумот.

Работоспособность сети

uz - tarmoqning ish

qobiliyati

тармоқнинг иш

қобилияти

en - network capability

Свойство сети выполнять заданные функции в соответствии с установленными требованиями.

Tarmoqning, berilgan funksiyalarni belgilangan talablarga muvofiq bajarish xususiyati.

Тармоқнинг, берилган функцияларни белгиланган талабларга мувофиқ бажариш хусусияти.

Радиокиллер

uz - radiokiller

радиокиллер

en - radio killer

Специальная команда, переданная оператором транкинговой сети на абонентскую станцию (обычно похищенную) и вызывающая в ней необратимые изменения, делающие ее непригодной к работе.

Tranking tarmoq operatori tomonidan abonent stansiyasiga (odatda, o'g'irlangan) uzatilgan va unda,

Р

uni ishga yaroqsiz qiluvchi, qaytarib bo'lmaydigan o'zgarishlar paydo qiladigan maxsus komanda.

Транкинг тармоқ оператори томонидан абонент станциясига (одатда, ўғирланган) узатилган ва унда, уни ишга яроқсиз қилувчи, қайтариб бўлмайдиган ўзгаришлар пайдо қиладиган махсус команда.

Радиус (опасной) зоны

uz - (xavfli) zona radiusi
(хавфли) зона радиуси
en - dangerous area radius

Радиус сферы, охватывающий зону 1 или зону 2.

1- yoki 2-zonani qamrab oluvchi sfera radiusi.

1- ёки 2-зонани қамраб олувчи сфера радиуси.

Разбиение на модули

uz - modullarga bo'lish
модуларга бўлиш
en - modular decomposition

Процесс разбиения системы на компоненты для облегчения проектирования, разработки и оценки.

Loyihalashni, ishlab chiqishni va baholashni yengillashtirish maqsadida, tizimni komponentlarga ajratish jarayoni.

Лойиҳалашни, ишлаб чиқишни ва баҳолашни енгиллаштириш мақсадида, тизимни компонентларга ажратиш жараёни.

Развертывание ключа

uz - kalitni ochib ko'rsatish
калитни очиб кўрсатиш
en - key scheduling

Процедура выработки последовательности раундовых ключей из ключа шифрования. Обычно суммарный объем раундовых ключей значительно превышает размер ключа шифрования.

Shifrlash kalitidan raundli kalitlar ketma-ketligini ishlab chiqish protsedurasi. Odatda, raundli kalitlarning jami hajmi shifrlash kalitining o'lchamidan ancha ko'p bo'ladi.

Шифрлаш калитидан раундли калитлар кетма-кетлигини ишлаб чиқиш процедураси. Одатда, раундли калитларнинг жами ҳажми шифрлаш калитининг ўлчамидан анча кўп бўлади.

Разглашение информации

uz - axborotning oshkor bo'lishi
ахборотнинг ошкор

Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Р

бўлиши

en - information disclosure

Muhofaza qilinadigan axborotning, bunday axborotdan erkin foydalanish huquqi bo'lmagan iste'molchilarga ruxsat etilmagan tarzda yetkazilishi.

Муҳофаза қилинадиган ахборотнинг, бундай ахборотдан эркин фойдаланиш ҳуқуқи бўлмаган истеъмолчиларга рухсат этилмаган тарзда етказилиши.

Разграничение доступа

uz - erkin foydalanishni

chegaralash

эркин фойдаланишни

чегаралаш

en - access isolation

1 Порядок использования ресурсов системы, при котором субъекты получают доступ к объектам в строгом соответствии с установленными правилами.

2 Наделение каждого пользователя (субъекта доступа) индивидуальными правами по доступу к информационному ресурсу и проведению операций по ознакомлению с информацией, ее документированию, модификации и уничтожению.

Примечание – Разграничение доступа может осуществляться по различным моделям, построенным по тематическому признаку или по грифу секретности разрешенной к пользованию информации.

1 Tizim resurslaridan foydalanish tartibi, bunda subyektlar belgilangan qoidalarga qat'iy muvofiq holda obyektlardan foydalana oladilar.

2 Har bir foydalanuvchiga (foydalanish subyektiga) axborot resursidan erkin foydalanish, axborot bilan tanishish, uni hujjatlashtirish, o'zgartirish va yo'q qilish bo'yicha operatsiyalarni amalga oshirish yuzasidan alohida huquqlar berish.

Izoh – Erkin foydalanishni belgilash tematik belgiga ko'ra qurilgan turli modellar yoki foydalanish ruxsat etilgan axborotning maxfiylik grifi bo'yicha amalga oshirilishi mumkin.

1 Тизим ресурсларидан фойдаланиш тартиби, бунда субъектлар белгиланган қоидаларга қатъий мувофиқ ҳолда объектлардан фойдалана оладилар.

2 Ҳар бир фойдаланувчига (фойдаланиш субъектига) ахборот ресурсларидан эркин фойдаланиш,

Р

ахборот билан танишиш, уни ҳужжатлаштириш, ўзгартириш ва йўқ қилиш бўйича операцияларни амалга ошириш юзасидан алоҳида ҳуқуқлар бериш.

Изоҳ – Эркин фойдаланишни белгилаш тематик белгига кўра қурилган турли моделлар ёки фойдаланиш рухсат этилган ахборотнинг махфийлик грифи бўйича амалга оширилиши мумкин.

Разграничение обязанностей

uz - majburiyatlarning

aniq belgilab olinishi

мажбуриятларнинг

аниқ белгилаб олинishi

en - separation of duties

Разделение ответственности в отношении чувствительной информации таким образом, чтобы действующее в одиночку лицо, могло скомпрометировать безопасность только ограниченной части системы обработки данных.

Ta'sirchan axborotga nisbatan javobgarlikning bo'linishi, bu jarayon shunday tarzda bajariladiki, bunda bir o'zi harakat qilayotgan shaxs ma'lumotlarni qayta ishlash tizimi cheklangan qismini xavfsizligiga putur yetkazish (xavfsizligini obro'sizlantirishi) mumkin.

Таъсирчан ахборотга нисбатан жавобгарликнинг бўлиниши, бу жараён шундай тарзда бажариладики, бунда бир ўзи ҳаракат қилаётган шахс маълумотларни қайта ишлаш тизими чекланган қисмини хавфсизлигига путур етказиш (хавфсизлигини обрўсизлантириши) мумкин.

Разделение

uz - ajratish

ажратиш

en - division

Деление данных на изолированные блоки, управление безопасностью которых производится отдельно, с целью уменьшения риска. Например, чтобы ограничить воздействие на весь проект производится разделение данных главного проекта на блоки, соответствующие разделам проекта, каждый из которых имеет собственную систему безопасности.

Ma'lumotlarni izolyatsiyalangan bloklarga bo'lish. Riskni kamaytirish maqsadida, ularning xavfsizligini boshqarish alohida amalga oshiriladi. Masalan, butun loyihaga ta'sirni cheklash uchun, bosh loyiha ma'lumotlari loyihaning o'z xavfsizlik tizimiga ega bo'lgan, har bir tegishli bo'limiga mos keladigan

Р

bloklarga ajratiladi.

Маълумотларни изоляцияланган блоklarга бўлиш. Рискни камайтириш мақсадида, уларнинг хавфсизлигини бошқариш алоҳида амалга оширилади. Масалан, бутун лойиҳага таъсирни чеклаш учун, бош лойиҳа маълумотлари лойиҳанинг ўз хавфсизлик тизимига эга бўлган, ҳар бир тегишли бўлимига мос келадиган блоklarга ажратилади.

Разделение доменов

uz - domenlarga bo'lish

доменларга бўлиш

en - domain separation

Свойство архитектуры безопасности, посредством которого ФБО определяет отдельные домены безопасности для каждого пользователя и ФБО, а также исключает возможность влияния каких-либо процессов пользователя на содержание домена безопасности другого пользователя или ФБО.

Xavfsizlik arxitekturasi xususiyati, OXF vositasida har bir foydalanuvchi hamda OXF uchun xavfsizlikning alohida domenlarini belgilaydi, shuningdek, boshqa foydalanuvchi va OXFning xavfsizlik domenlariga foydalanuvchining biror-bir jarayonga bo'lgan ta'sirini yo'q qiladi.

Xavfsizlik arxitekturasi xususiyati, OXF vositasida har bir foydalanuvchi hamda OXF uchun xavfsizlikning alohida domenlarini belgilaydi, shuningdek, boshqa foydalanuvchi va OXFning xavfsizlik domenlariga foydalanuvchining biror-bir jarayonga bo'lgan ta'sirini yo'q qiladi.

Разделение на уровни

uz - darajalarga bo'lish

даражаларга бўлиш

en - layering

Метод проектирования, при котором отдельные группы модулей (уровни) иерархически организованы таким образом, чтобы один уровень зависел только от уровней ниже его в иерархии сервисов и предоставлял свои сервисы только уровням выше его в иерархии.

Modullarning ayrim (darajalari) guruhlari bir daraja servislar iyerarxiasida faqat o'zidan quyidagi darajalar bog'liq bo'ladigan va o'z xizmatlarini iyerarxiyada faqat o'zidan yuqoridagi darajalarga ko'rsata-

Р

digan qilib iyerarxik tashkillashtirilgan loyihalash metodi.

Модуларнинг айрим (даражалари) гуруҳлари бир даража сервислар иерархиясида фақат ўзидан қуйидаги даражалар боғлиқ бўладиган ва ўз хизматларини иерархияда фақат ўзидан юқоридаги даражаларга кўрсатадиган қилиб иерархик ташкиллаштирилган лойиҳалаш методи.

Разделение привилегий

uz - imtiyozlarning taqsimlanishi

имтиёзларнинг тақсимланиши

en - privilege sharing

Принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Ma'lumotlarni muhofaza qilish mexanizmini ochish prinsipi, bunda erkin foydalanish (kirish) uchun bir emas, balki ikkita parolni (masalan, ikkita shaxs tomonidan) ko'rsatish zarur bo'ladi.

Маълумотларни муҳофаза қилиш механизми-ни очиш принципи, бунда эркин фойдаланиш (кириш) учун бир эмас, балки иккита паролни (масалан, иккита шахс томонидан) кўрсатиш зарур бўлади.

Разделение риска

uz - risk taqsimoti

риск тақсимооти

en - risk sharing

Форма обработки риска, включающая согласованное распределение риска между несколькими сторонами.

Примечания

1 Законодательные или обязательные требования могут ограничить, запретить или обязать проведение разделения риска.

2 Разделение риска может представлять собой страхование или иметь форму договора (контракта).

3 Степень, до которой риск зависит от точности и однозначности условий договоров по разделению риска.

4 Перенос риска является формой разделения риска.

Bir nechta tomonlar orasida riskning kelishilgan holda taqsimlanishini ichiga oladigan riskni qayta ishlash shakli.

Izohlar

1 Qonuniy yoki majburiy talablar, risk taqsimlanishi o'tkazilishini cheklashi, ta'qiqlashi yoki buyurishi mumkin.

Р

2 Riskning taqsimlanishi o'zida sug'urta qilishni ifodalashi yoki shartnoma (kontrakt) shaklini olishi mumkin.

3 Risk taqsimlanishi bo'yicha shartnoma shartlarida riskning aniqligi va mazmunan bir hilligiga bog'liq bo'lgungacha bo'lgan daraja.

4 Riskni ko'chirish riskni tasqiqlash shakli hisoblanadi.

Бир нечта томонлар орасида рискнинг келишилган ҳолда тақсимланишини ичига оладиган рискни қайта ишлаш шакли.

Изоҳлар

1 Қонуний ёки мажбурий талаблар, риск тақсимланиши ўтказилишини чеклаши, таъқиқлаши ёки буюриши мумкин.

2 Рискнинг тақсимланиши ўзида суғурта қилишни ифодалаши ёки шартнома (контракт) шаклини олиши мумкин.

3 Риск тақсимланиши бўйича шартнома шартларида рискнинг аниқлиги ва мазмунан бир ҳиллигига боғлиқ бўлгунгача бўлган даража.

4 Рискни кўчириш рискни тақсимлаш шакли ҳисобланади.

Разделение секретов

uz - sirlarning taqsimlanishi
сирларнинг

тақсимланиши

en - secret sharing scheme

Схема разделения секрета, основная идея которой – разделить секретный ключ между несколькими субъектами, чтобы собравшись вместе, они могли восстановить ключ из нескольких частей.

Sirni taqsimlash sxemasi, uning asosiy g'oyasi maxfiy kalitni bir nechta subyekt o'rtasida, ular birga to'planib, kalitni bir nechta qismlardan tiklashlari mumkin bo'ladigan tarzda ajratishda ifodalanadi.

Сирни тақсимлаш схемаси, унинг асосий ғояси махфий калитни бир нечта субъект ўртасида, улар бирга тўпланиб, калитни бир нечта қисмлардан тиклашлари мумкин бўладиган тарзда ажратишда ифодаланadi.

Разметка дорожек

спиральная

uz - yo'lkalarni spiral bo'yicha
belgilab chiqish

йўлкаларни спираль
бўйича белгилаб чиқиш

en - spiral tracking

Метод защиты от копирования, в котором используется для чтения данных только часть каждой дорожки, при этом головка, читающая содержимое диска, будет двигаться к центру приблизительно по спирали.

Nusxa ko'chirishdan muhofaza qilish metodi, unda ma'lumotlarni o'qish uchun har bir yo'lkaning faqat

Р

bir qismidan foydalaniladi, bunda disk ichidagilarni o'quvchi kallak markazga taxminan spiral bo'yicha harakat qiladi.

Нусха кўчиришдан муҳофаза қилиш методи, унда маълумотларни ўқиш учун ҳар бир йўлканинг фақат бир қисмидан фойдаланилади, бунда диск ичидагиларни ўқувчи каллак марказга тахминан спираль бўйича ҳаракат қилади.

Разметка ложная

uz - chalg'ituvchi belgi

чалғитувчи белги

en - bad tracking

Способ защиты от копирования, при использовании которого на диске специально записываются дефектные секторы.

Nusxa ko'chirishdan muhofaza qilish metodi, undan foydalanilganda diskda nuqsonli sektorlar maxsus yozib olinadi.

Нусха кўчиришдан муҳофаза қилиш методи, ундан фойдаланилганда дискда нуқсонли секторлар махсус ёзиб олинади.

Разработка

uz - ishlab chiqish

ишлаб чиқиш

en - development

Стадия жизненного цикла продукта, связанная с созданием представленной реализации ОО.

Примечание – Во всех требованиях класса ALC термин «разработка» и связанные с ним термины (разработчик, разрабатывать) используются в более широком смысле и означают как разработку, так и производство.

Mahsulot hayotiy siklining, BOni amalga oshirishni taqdim etishda yaratilishi bilan bog'liq bosqichi. Izoh – ALC turkumidagi barcha talablarda «ishlab chiqish» atamasi va u bilan bog'liq bo'lgan (ishlab chiquvchi, ishlab chiqish) atamaları keng ma'noda ishlatiladi, ham ishlab chiqish, ham ishlab chiqarishni bildiradi.

Маҳсулот ҳаётий циклининг, БОни амалга оширишни тақдим этишда яратилиши билан боғлиқ босқичи.

Изоҳ – ALC туркумидаги барча талабларда «ишлаб чиқиш» атамаси ва у билан боғлиқ бўлган (ишлаб чиқувчи, ишлаб чиқиш) атамалари кенг маънода ишлатилади, ҳам ишлаб чиқиш, ҳам ишлаб чиқаришни билдиради.

Разработчик

uz - ishlab chiquvchi

ишлаб чиқувчи

en - developer

Организация, ответственная за разработку ОО.

BOni ishlab chiqishga mas'ul tashkilot.

БОни ишлаб чиқишга масъул ташкилот.

Р

Разрешение

uz - ruxsat

рухсат

en - permission

Набор типов доступа, используемый в административных программах при формировании списков контроля доступа.

Erkin foydalanish turlari to'plami erkin foydalanishni nazorat qilish ro'yxatini shakllantirishda ma'muriy dasturlarda qo'llaniladi.

Эркин фойдаланиш турлари тўплами эркин фойдаланишни назорат қилиш рўйхатини шакллантиришда маъмурий дастурларда қўлланилади.

Все права на доступ субъекта к некоторому объекту.

Разрешение на доступ

uz - erkin foydalanishga ruxsat

эркин фойдаланишга

рухсат

en - access permission

Subyektning qandaydir obyektдан erkin foydalani-shini ta'minlaydigan barcha huquqlar.

Субъектнинг қандайдир объектдан эркин фойдаланишини таъминлайдиган барча ҳуқуқлар.

Разрушение информации

uz - axborotning buzilishi

ахборотнинг бузилиши

en - information destruction

1 Любое состояние данных независимо от причины, которое делает невозможным использование информации.

2 Стирание информации, хранящейся в памяти ЭВМ.

1 Qanday sabab bo'lishidan qat'i nazar, ma'lumotlarning, axborotdan foydalanish imkoniyatini yo'qqa chiqaradigan, har qanday holati.

2 EHM хотирасида сақланадиган ахборотнинг о'chirib yuborilishi.

1 Қандай сабаб бўлишидан қатъи назар, маълумотларнинг, ахборотдан фойдаланиш имкониятини йўққа чиқарадиган, ҳар қандай ҳолати.

2 ЭҲМ хотирасида сақланадиган ахборотнинг ўчириб юборилиши.

Разрушение секретной информации

uz - maxfiy axborotning

buzilishi

махфий ахборотнинг

бузилиши

en - secret information

Неправомерное или преднамеренное изменение, искажение или уничтожение информации в результате неисправности технических средств, несовершенства и ошибок программного обеспечения, халатности обслуживающего персонала, стихийных бедствий или действий злоумышленников (нарушителей).

Р

destruction

Texnik vositalarning nosozligi, dasturiy ta'minotning takomillashmaganligi va xatolari, xizmat ko'rsatuvchi personalning mas'uliyatsizligi, tabiiy ofatlar yoki jinoyatkorlar (buzg'unchilar) harakatlari natijasida, axborotning noqonuniy yoki qasddan o'zgartirilishi, buzilishi yoki yo'q qilinishi.

Техник воситаларнинг носозлиги, дастурий таъминотнинг такомиллашмаганлиги ва хатолари, хизмат кўрсатувчи персоналнинг масъулиятсизлиги, табиий офатлар ёки жинояткорлар (бузгунчилар) ҳаракатлари натижасида, ахборотнинг ноқонуний ёки қасддан ўзгартирилиши, бузилиши ёки йўқ қилиниши.

Разрыв линии

uz - liniyaning uzilishi

линиянинг узилиши

en - line disconnect

Метод проведения атаки на систему, при котором пользователь выходит из системы либо злоумышленник разрывает линию телекоммуникаций, но система продолжает работу с злоумышленником как с легальным пользователем.

Tizimga qilinadigan hujumni amalga oshirish metodi, bunda foydalanuvchi tizimdan chiqadi yoki jinoyatkor telekommunikatsiyalar liniyasini uzib qo'yadi, biroq tizim jinoyatkor bilan ochiq foydalanuvchi bilan bo'lganidek ishlashni davom ettiraveradi.

Тизимга қилинадиган ҳужумни амалга ошириш методи, бунда фойдаланувчи тизимдан чиқади ёки жинояткор телекоммуникациялар линиясини узиб қўяди, бироқ тизим жинояткор билан очик фойдаланувчи билан бўлганидек ишлашни давом эттираверади.

Разряд защиты

uz - muhofaza razryadi

муҳофаза разряди

en - protection bit

Один из дополнительных разрядов промежуточных результатов, обеспечивающих сохранение точности.

Aniqlik saqlanib qolishini ta'minlaydigan oraliq natijalarning qo'shimcha razryadlaridan biri.

Аниқлик сақланиб қолишини таъминлайдиган оралик натижаларнинг қўшимча разрядларидан бири.

Р

Рандомизация

uz - randomizatsiya(lash)

рандомизация(лаш)

en - randomisation

Преобразование исходных данных перед или во время зашифрования с использованием псевдослучайной последовательности данных, имеющее целью скрыть наличие в них, например, наличие идентичных блоков.

Ma'lumotlarda identik bloklar mavjudligini yashirish maqsadida, ma'lumotlarning psevdotasodifiy ketma-ketligidan foydalanib, shifrlashdan oldin yoki shifrlash paytida boshlang'ich ma'lumotlarni o'zgartirish.

Маълумотларда идентик блоклар мавжудлигини яшириш мақсадида, маълумотларнинг псевдотасодифий кетма-кетлигидан фойдаланиб, шифрлашдан олдин ёки шифрлаш пайтида бошлангич маълумотларни ўзгартириш.

Раскрытие

uz - ochilish (fosh etilish)

очилиш (фош этилиш)

en - disclosure, reveal

Операция частичного или полного удаления ранее примененной защиты.

Ilgari qo'llanilgan muhofazani qisman yoki to'liq olib tashlash operatsiyasi.

Ilgari qullanilgan muhofazani qisman ёки to'liq olib tashlash operatsiyasi.

Раскрытие информации

uz - axborotning fosh

etilishi

ахборотнинг фош

этилиши

en - disclosure of information

1 Нарушение компьютерной безопасности, в результате которого данные становятся доступны полномочным логическим объектам.

2 Несанкционированный или потенциальный просмотр информации.

1 Kompyuter xavfsizligining buzilishi, uning natijasida ma'lumotlar vakolatga ega bo'lmagan mantiqiy obyektlarga ochiq bo'lib qoladi.

2 Axborotni yashirin yoki ruxsat etilmagan tarzda ko'rib chiqish.

1 Kompyuter xavfsizligining buzilishi, uning natijasida ma'lumotlar vakolatga ega bo'lmagan mantiqiy obyektlarga ochiq bo'lib qoladi.

2 Axborotni yashirin ёки ruxsat etilmagan tarzda ko'rib chiqish.

Распределение ключей

1 Один из основных механизмов управления

Р

uz - kalitlarni taqsimlash
калитларни тақсимлаш
en - key distribution, key
management

ключами. Может реализовываться различными способами. Для симметричных криптосистем возможны варианты доставки ключей абонентам:

- по защищенным каналам, например, при помощи фельдъегерской службы;
- частями по разным каналам;
- через центр распределения ключей.

Для асимметричных криптосистем можно использовать механизм открытого распределения ключей.

2 Совокупность правил, определяющих порядок генерации криптографических ключей, рассылки пользователям, хранения и аннулирования.

1 Kalitlarni boshqarishning asosiy mexanizmlaridan biri. Turli xil usullar bilan amalga oshirilishi mumkin. Simmetrik kriptotizimlar uchun abonentlarga kalitlarni yetkazib berishning quyidagi variantlari mavjud:

- muhofazalangan kanallar bo‘ylab, masalan feldyegeerlik xizmati yordamida;
- turli kanallar bo‘ylab qismlarga bo‘lib;
- kalitlarni taqsimlash markazi orqali.

Asimmetrik kriptotizimlar uchun kalitlarni ochiq taqsimlash mexanizmidan foydalanish mumkin.

2 Kriptografik kalitlarni generatsiyalash, foydalanuvchilarga yuborish, saqlash va bekor qilish tartibini belgilovchi qoidalar to‘plami.

1 Калитларни бошқаришнинг асосий механизмларидан бири. Турли хил усуллар билан амалга оширилиши мумкин. Симметрик кriptотизимлар учун абонентларга калитларни етказиб беришнинг қуйидаги вариантлари мавжуд:

- муҳофазаланган каналлар бўйлаб, масалан фельдъегерлик хизмати ёрдамида;
- турли каналлар бўйлаб қисмларга бўлиб;
- калитларни тақсимлаш маркази орқали.

Асимметрик кriptотизимлар учун калитларни очик тақсимлаш механизmidан фойдаланиш мумкин.

2 Криптографик калитларни генерациялаш, фойдаланувчиларга юбориш, сақлаш ва бекор қилиш

Р

Распределение ключей открытое

uz - kalitlarni ochiq
taqsimlash

калитларни очик

тақсимлаш

en - public key distribution

тартибини белгиловчи қоидалар тўплами.

1 Механизм распределения криптографических ключей по незащищенным каналам телекоммуникаций.

2 Протокол, позволяющий двум абонентам выработать общий секретный ключ путем обмена сообщениями по открытому каналу телекоммуникаций без передачи какой-либо общей секретной информации, распределяемой заранее.

1 Muhofazalanmagan telekommunikatsiyalar kanallari bo'yicha kriptografik kalitlarni taqsimlash mexanizmi.

2 Ikkita abonentga, oldindan taqsimlanadigan qandaydir umumiy maxfiy axborotni uzatmasdan turib, ochiq telekommunikatsiyalar kanali orqali xabarlarini almashinish yo'li bilan, umumiy maxfiy kalit ishlab chiqish imkonini beradigan protokol.

1 Muhofazalanmagan telekommunikatsiyalar kanallari b'uyicha kriptografik kalitlarini taqsimlash mexanizmi.

2 Ikkita abonentga, oldindan taqsimlanadigan qandaydir umumiy maxfiy axborotni uzatmasdan turib, ochiq telekommunikatsiyalar kanali orqali xabarlarini almashinish yo'li bilan, umumiy maxfiy kalit ishlab chiqish imkonini beradigan protokol.

Рассеивание

uz - tarqalish

тарқалиш

en - diffusion

Процесс шифрования, при котором изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста.

Shifrlash jarayoni, bunda ochiq matnning har qanday belgisini yoki kalitni o'zgartirish shifrmtn belgilarining ko'plab soniga ta'sir ko'rsatadi, bu esa ochiq matnning statistik xususiyatlarini berkitadi.

Шифрлаш жараёни, бунда очик матннинг ҳар қандай белгисини ёки калитни ўзгартириш шифрматн белгиларининг кўплаб сонига таъсир кўрсатади, бу эса очик матннинг статистик хусусиятларини беркитади.

Р

Рассекречивание сведений и их носителей

uz - ma'lumotlarni va ularni tashuvchilarni oshkor qilish

маълумотларни ва уларни ташувчиларни ошкор қилиш
en - declassification of information and its carriers

Снятие ранее введенных в предусмотренном законодательством порядке ограничений на распространение сведений, составляющих государственные секреты, и на доступ к их носителям.

Qonunchilikda ko'zda tutilgan tartibda oldin kiritilgan, davlat siri hisoblanadigan ma'lumotlarni tarqatishga va ularni tashuvchilardan foydalana olishga bo'lgan cheklovlarni olib tashlash.

Р

Рассылка спама

uz - spamni yuborish
спамни юбориш
en - spamming

Қонунчиликда кўзда тутилган тартибда олдин киритилган, давлат сири ҳисобланадиган маълумотларни тарқатишга ва уларни ташувчилардан фойдалана олишга бўлган чекловларни олиб ташлаш.

Рассылка незапрашиваемых данных, которые перегружают систему.

Tizimni o'ta band qiladigan, so'ralmagan ma'lumotlarni yuborish.

Тизимни ўта банд қиладиган, сўралмаган маълумотларни юбориш.

Расширение

uz - kengaytirish
кенгайтириш
en - extension

Добавление в задание по безопасности или профиль защиты требований, отсутствующих в соответствующих стандартах.

Tegishli standartlarda bo'lmagan talablarning xavfsizlik bo'yicha topshiriqqa yoki himoya profiliga qo'shilishi.

Тегишли стандартларда бўлмаган талабларнинг хавфсизлик бўйича топшириққа ёки ҳимоя профилига қўшилиши.

Расшифрование

uz - rasshifrovkalash
расшифровкалаш
en - deciphering

1 Процесс противоположный шифрованию и связанный с восстановлением исходного текста из зашифрованного с использованием известного ключа.

2 Процесс обратного преобразования шифротекста в открытый текст.

Р

1 Shifrlashga qarama-qarshi va dastlabki matni ma'lum kalitdan foydalanib, shifrlangan matndan tiklash bilan bog'liq jarayon.

2 Shifrmatni ochiq matnga teskari qayta o'zgartirish jarayoni.

1 Шифрлашга қарама-қарши ва дастлабки матни маълум калитдан фойдаланиб, шифрланган матндан тиклаш билан боғлиқ жараён.

2 Шифрматни очик матнга тескари қайта ўзгартириш жараёни.

Раунд

uz - raund

раунд

en - round

Один шаг шифрования в шифре Файстеля и близких ему по архитектуре шифрах, в ходе которого одна или несколько частей шифруемого блока данных подвергается модификации.

Faystel shifridagi va arxitektura jihatdan unga yaqin bo'lgan shifrlardagi shifrlashning bitta qadami. Shifrlash jarayonida shifrlanadigan blokning bir yoki bir nechta qismi o'zgarishga uchraydi.

Файстел шифридаги ва архитектура жиҳатдан унга яқин бўлган шифрлардаги шифрлашнинг битта қадами. Шифрлаш жараёнида шифрланадиган блокнинг бир ёки бир нечта қисми ўзгаришга учрайди.

Регистрация

uz - qayd qilish

қайд қилиш

en - log-on

Процедура входа пользователя в систему с указанием идентификационного кода или пароля для получения доступа в систему (сеть).

Foydalanuvchining, tizimdan (tarmoqdan) erkin foydalanish uchun identifikatsion kod yoki parolni ko'rsatgan holda, kirish protsedurasi.

Фойдаланувчининг, тизимдан (тармоқдан) эркин фойдаланиш учун идентификацион код ёки паролни кўрсатган ҳолда, кириш процедураси.

Регистрация деятельности

uz - faoliyatni qayd qilish

фаолиятни қайд қилиш

uz - activity registration

Отслеживание действий субъекта доступа или злоумышленника в системе.

Tizimda erkin foydalanish subyektining yoki jinoyatkorning harakatlarini kuzatish.

Р

Регистрация открытого ключа

uz - ochiq kalitni ro'uxatga olish

очик калитни рўйхатга олиш

en - public key registry

Регистрация пользователя

uz - foydalanuvchini ro'uxatga olish

фойдаланувчини рўйхатга олиш

en - user registration

Регистр постоянный запоминающий

uz - doimiy хотирловчи registr

доимий хотирловчи регистр

en - permanent memory register

Регламентация

uz - qat'iy belgilash

катъий белгилаш

en - regulation

Тизимда эркин фойдаланиш субъектининг ёки жинойткорнинг ҳаракатларини кузатиш.

Процесс фиксации открытых ключей, обеспечивающий достоверную информацию лицу, осуществляющему запрос, с целью предотвратить фальсификацию значения открытого ключа.

Ochiq kalitning qiymati qalbakilashtirilishini bartaraf qilish maqsadida, so'rovni amalga oshiruvchi shaxsga ishonchli axborotni ta'minlovchi, ochiq kalitlarni ro'uxatga olish jarayoni.

Очик калитнинг қиймати қалбакилаштирилишини бартараф қилиш мақсадида, сўровни амалга оширувчи шахсга ишончли ахборотни таъминловчи, очик калитларни рўйхатга олиш жараёни.

Учет входа пользователя в систему с указанием кода идентификации или пароля для получения доступа в систему.

Foydalanuvchining tizimga kirishini, tizimdan erkin foydalanish uchun identifikatsiya kodi yoki parolni ko'rsatgan holda, hisobga olish.

Фойдаланувчининг тизимга киришини, тизимдан эркин фойдаланиш учун идентификация коди ёки паролни кўрсатган ҳолда, ҳисобга олиш.

Техническое устройство, содержащее данные, которые могут быть прочитаны, но не могут быть изменены.

O'qish mumkin bo'lgan, lekin o'zgartirish mumkin bo'lmagan ma'lumotlarni o'z ichiga oluvchi texnik qurilma.

Ўқиш мумкин бўлган, лекин ўзгартириш мумкин бўлмаган маълумотларни ўз ичига олувчи техник қурилма.

Метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

Р

Ахборотни муҳофаза қилиш методи. Муҳофаза қилинаётган ахборотни автоматлаштирилган қайта ишлаш, уни сақлаш ва узатишнинг шундай шароитлари yaratiladiki, natijada ахборотдан рuxsat etilmagan tarzda foydalana olish imkoniyatlari minimumga keltiriladi.

Ахборотни муҳофаза қилиш методи. Муҳофаза қилинаётган ахборотни автоматлаштирилган қайта ишлаш, уни сақлаш ва узатишнинг шундай шароитлари yaratiladiki, natijada ахборотдан рuxsat etilmagan tarzda foydalana olish imkoniyatlari minimumga keltiriladi.

Режим использования защищенный

uz - muhofazalangan foydalanish rejimi

муҳофазаланган фойдаланиш режими

en - protected usage mode

Режим защищенной обработки базы данных, в котором все прикладные программы, работающие параллельно с программой, открывшей области базы данных в этом режиме, могут читать записи, но не могут их обновлять до тех пор, пока программа не закроет эти области.

Ma'lumotlar bazasini muhofazalangan tarzda qayta ishlash rejimi, bu rejimda ma'lumotlar bazasi sohalarini ochgan dastur bilan parallel ishlaydigan barcha amaliy dasturlar yozuvlarni o'qishi mumkin, lekin dastur bu sohalarni yopmaguncha, ularni yangilay olmaydi.

Ma'lumotlar bazasini muhofazalangan tarzda qayta ishlash rejimi, bu rejimda ma'lumotlar bazasi sohalarini ochgan dastur bilan parallel ishlaydigan barcha amaliy dasturlar yozuvlarni o'qishi mumkin, lekin dastur bu sohalarni yopmaguncha, ularni yangilay olmaydi.

Режим обхода

uz - chetlab o'tish rejimi

четлаб ўтиш режими

en - by-pass mode

Режим работы оборудования шифрования данных, при котором открытый текст передается без искажения.

Ma'lumotlarni shifrlash uskunasining ishlash rejimi bo'lib, bunda ochiq matn buzilmasdan uzatiladi.

Ma'lumotlarni shifrlash uskunasining ishlash rejimi bo'lib, bunda ochiq matn buzilmasdan uzatiladi.

Р

Режим разграничения доступа

uz - erkin foydalanishni chegaralash rejimi

эркин фойдаланишни чегаралаш режими

en - access demarcation mode

Порядок доступа лиц к техническим средствам, программе при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами.

Shaxslarning, oldindan ishlab chiqilgan va tasdiqlangan qoidalarga muvofiq, hisoblash texnikasi vositalaridan, qayta ishlashda dasturdan foydalana olish tartibi.

Шахсларнинг, олдиндан ишлаб чиқилган ва тасдиқланган қоидаларга мувофиқ, ҳисоблаш техникаси воситаларидан, қайта ишлашда дастурдан фойдалана олиш тартиби.

Резидентный

uz - rezident

резидент

en - resident

Постоянно присутствующий в оперативной памяти.

Operativ хотирада doimo mavjud boʻladigan.

Оператив хотирада доимо мавжуд бўладиган.

Результаты деятельности

uz - faoliyat natijalari

фаолият натижалари

en - performance

Измеримый результат.

Примечание – Результаты деятельности могут быть выражены в количественных и качественных показателях.

Oʻlchangan natija.

Izoh – Faoliyat natijalari miqdor va sifat koʻrsatkichlarida ifodalanishi mumkin.

Ўлчанган натижа.

Izoh – Фаолият натижалари миқдор ва сифат кўрсаткичларида ифодаланиши мумкин.

Результаты измерения

uz - oʻlchash natijalari

ўлчаш натижалари

en - measurement results

Один или более индикаторов и ассоциированных с ними интерпретаций, соответствующие информационной потребности.

Axborotga boʻlgan ehtiyojga mos keladigan bitta yoki bir nechta indikatorlar va ular bilan assotsiat-siyalangan talqinlar.

Ахборотга бўлган эҳтиёжга мос келадиган битта ёки бир нечта индикаторлар ва улар билан ассоциацияланган талқинлар.

Реконструкция данных

uz - maʼlumotlarni tiklash

маълумотларни тиклаш

Метод реставрации данных путем анализа первоисточников.

Asl manbani tahlil qilish yoʻli bilan maʼlumotlarni

Р

en - data reconstruction

Реставрация данных

uz - ma'lumotlarni

restavratsiya qilish

маълумотларни

реставрация қилиш

en - data restoration

restavratsiya qilish metodi.

Асл манбани таҳлил қилиш йўли билан маълумотларни реставрация қилиш методи.

Восстановление потерянных или зараженных данных.

Примечание – Совокупность метода копирования архивных данных, метода реконструкции данных из исходных данных или метода воссоздания данных из альтернативных источников.

Ҳо‘қолган yoki zararlangan ma'lumotlarni tiklash. Izoh – Arxiv ma'lumotlaridan nusxa ko'chirish, ma'lumotlarni dastlabki ma'lumotlardan tiklash yoki ma'lumotlarni muqobil manbalardan hosil qilish metodlarining jami.

Йўқолган ёки зарарланган маълумотларни тиклаш.

Изоҳ – Архив маълумотларидан нусха кўчириш, маълумотларни дастлабки маълумотлардан тиклаш ёки маълумотларни муқобил манбалардан ҳосил қилиш методларининг жами.

Ресурс

uz - resurs

ресурс

en - resource

Любой из компонентов вычислительной системы и предоставляемые ею возможности.

Hisoblash tizimi komponentlaridan istalgani hamda bu tizim tomonidan taqdim etiladigan imkoniyatlar.

Ҳисоблаш тизими компонентларидан исталгани ҳамда бу тизим томонидан тақдим этиладиган имкониятлар.

Ресурс защищенный

uz - muhofazalangan resurs

муҳофазаланган ресурс

en - locked resource

Ресурс, для которого определен замок защиты (секретности), т.е. управление доступом специфицировано.

Muhofaza (maxfiylik) qulfi belgilangan, ya'ni erkin foydalanishni boshqarish spetsifikatsiyalangan (tasniflangan) resurs.

Муҳофаза (махфийлик) қулфи белгиланган, яъни эркин фойдаланишни бошқариш спецификацияланган (таснифланган) ресурс.

Ресурс объекта оценки

uz - baholash obykti resursi

баҳолаш объекти ресурси

en - TOE resource

Все, что может использоваться или потребоваться объектом оценки.

Baholash obykti foydalanadigan yoki unga zarur

Р

bo'ladigan barcha narsa.

Баҳолаш объекти фойдаланадиган ёки унга зарур бўладиган барча нарса.

Ресурсы информационные

uz - axborot resurslari

ахборот ресурслари

en - information resources

Отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Alohida hujjatlar va hujjatlarning alohida massivlari, axborot tizimlaridagi (kutubxona, arxiv, fond, ma'lumotlar banki, boshqa axborot tizimlari) hujjatlar va hujjatlarning massivlari.

Алоҳида ҳужжатлар ва ҳужжатларнинг алоҳида массивлари, ахборот тизимларидаги (кутубхона, архив, фонд, маълумотлар банки, бошқа ахборот тизимлари) ҳужжатлар ва ҳужжатларнинг массивлари.

Решение по защите

информации техническое

uz - axborotni muhofaza qilish

bo'yicha texnik yechim

ахборотни муҳофаза

қилиш бўйича техник ечим

en - technical solution on
information security

Техническое, планировочное, архитектурное или конструкторское решение по защите информации.

Axborotni muhofaza qilish bo'yicha texnik, loyiha, arxitektura yoki konstruktorlik yechimi.

Ахборотни муҳофаза қилиш бўйича техник, лойиҳа, архитектура ёки конструкторлик ечими.

Решетка Кардано

uz - Kardano panjarasi

Кардано панжараси

en - Cardano grid

Криптографическая система, реализующая шифр перестановок. Представляет собой квадратную таблицу (решетку), в которой четверть ячеек прорезана так, чтобы при четырех поворотах покрывать всю таблицу. Открытый текст вписывается в прорезанные ячейки решетки, которая поворачивается на 90° , открывая тем самым новые, незаполненные ячейки.

Almashtirib qo'yish shifrini amalga oshiruvchi kriptografik tizim. O'zida, yacheykalarining to'rtidan biri to'rt burilishda barcha jadvalni qamrab oladigan tarzda kesilgan kvadrat jadval (panjara)ni aks ettiradi. Ochiq matn 90° ga buriladigan panjaraning kesilgan yacheykalariga yoziladi, shu bilan yangi,

Р

to'ldirilmagan yacheykalar ochiladi.

Алмаштириб қўйиш шифрини амалга оширувчи криптографик тизим. Ўзида, ячейкаларнинг тўртдан бири тўрт бурилишда барча жадвални қамраб оладиган тарзда кесилган квадрат жадвал (панжара)ни акс эттиради. Очиқ матн 90° га буриладиган панжаранинг кесилган ячейкаларига ёзилади, шу билан янги, тўлдирилмаган ячейкалар очилади.

Решетка кодовая

uz - kodli panjara

кодли панжара

en - code grid

Направленный граф, в который превращается дерево сверхточного кода с конечной длиной ограничения.

Yo'naltirilgan graf bo'lib, unga oxirgi cheklash uzunligiga ega yuqori aniqlikdagi kod daraxti aylanadi.

Йўналтирилган граф бўлиб, унга охирги чеклаш узунлигига эга юқори аниқликдаги код дарахти айланади.

Риск

uz - risk

риск

en - risk

1 Возможность использования конкретной уязвимости системы обработки данных при реализации конкретной угрозы.

2 Следствие влияния неопределенности на достижение поставленных целей.

Примечания

1 Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

2 Неопределенность – это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей.

3 Риск часто характеризуют путем описания возможного события и его последствий или их сочетания.

4 Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности события.

5 В контексте систем управления информационной безопасностью риски информационной безопасности могут быть представлены в виде влияния неопределенности на цели информационной безопасности.

6 Риск информационной безопасности связан с вероятностью использования угрозами уязвимостей информационных активов или группы информационных активов, в результате чего будет нанесен ущерб организации.

1 Muayyan xavfni amalga oshirishda, ma'lumotlarni qayta ishlash tizimining muayyan zaifligidan foyda-

P

lanish imkoniyati.

2 Qo'yilgan maqsadlarga erishish uchun noaniqlikning ta'sir etish natijasi.

Izohlar

1 Noaniqlikning ta'sir etishi oqibati deganda – kutiladigan natija yoki voqea-hodisadan chetga chiqish (ijobiy va/yoki salbiy) tushunilishi zarur.

2 Noaniqlik – bu, voqea-hodisani, uning oqibatlarini va ularning ehtimolliklarini tushunish uchun zarur axborotning to'liq yoki qisman yetishmaslik holatidir.

3 Risk ko'pincha mumkin bo'lgan voqea-hodisa va uning oqibatlari yoki ularning birikmasini tavsiflash yo'li bilan tavsiflanadi.

4 Risk ko'pincha mumkin bo'lgan voqea-hodisaning oqibatlarini (shu jumladan, sharoitlar o'zgarishi) va hodisaning tegishli ehtimolliги ko'rinishida ifodalanadi.

5 Axborot xavfsizligini boshqarish tizimlarining kontekstida axborot xavfsizligining risklari noaniqlikning axborot xavfsizligi maqsadiga ta'siri ko'rinishida taqdim etilishi mumkin.

6 Axborot xavfsizligi riski axborot aktivlari yoki axborot aktivlari guruhi zaifliklarining tahdidlaridan foydalanish ehtimolliги bilan bog'liq, buning natijasida tashkilotga zarar yetkaziladi.

1 Муайян хавфни амалга оширишда, маълумотларни қайта ишлаш тизимининг муайян заифлигидан фойдаланиш имконияти.

2 Қўйилган мақсадларга эришиш учун ноаниқликнинг таъсир этиш натижаси.

Изоҳлар

1 Ноаниқликнинг таъсир этиши оқибати деганда – кутиладиган натижа ёки воқеа-ходисадан четга чиқиш (ижобий ва/ёки салбий) тушунилиши зарур.

2 Ноаниқлик – бу, воқеа-ходисани, унинг оқибатларини ва уларнинг эҳтимолликларини тушуниш учун зарур ахборотнинг тўлиқ ёки қисман етишмаслик ҳолатидир.

3 Риск кўпинча мумкин бўлган воқеа-ходиса ва унинг оқибатлари ёки уларнинг бирикмасини тавсифлаш йўли билан тавсифланади.

4 Риск кўпинча мумкин бўлган воқеа-ходисанинг оқибатлари (шу жумладан, шароитлар ўзгариши) ва ҳодисанинг тегишли эҳтимоллиги кўринишида ифодаланadi.

5 Ахборот хавфсизлигини бошқариш тизимларининг контекстида ахборот хавфсизлигининг riskлари ноаниқликнинг ахборот хавфсизлиги мақсадига таъсири кўринишида тақдим этилиши мумкин.

6 Ахборот хавфсизлиги riskи ахборот активлари ёки ахборот активлари гуруҳи заифликларининг таҳдидларидан фойдаланиш эҳтимоллиги билан боғлиқ, бунинг нати-

Р

жасида ташкилотга зарар етказилади.

Риск остаточный

uz - qoldiq risk

қолдик риск

en - residual risk

Риск , оставшийся после обработки риска.

Примечания

1 Остаточный риск может представлять собой неопределенный риск.

2 Остаточный риск иногда называют «сохраняемым риском».

Risk qayta ishlanganidan soʻng qoladigan risk.

Izohlar

1 Qoldiq risk noaniq riskdan iborat boʻlishi mumkin.

2 Qoldiq risk baʼzida «saqlanadigan risk» deb ataladi.

Риск қайта ишланганидан сўнг қоладиган риск.

Изохлар

1 Қолдик риск ноаниқ рискдан иборат бўлиши мумкин.

2 Қолдик риск баъзида «сақланадиган риск» деб аталади.

Роль

uz - rol

роль

en - role

Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и объектом оценки.

Baholash obyektini va foydalanuvchi oʻrtasida yoʻl qoʻyiladigan oʻzaro aloqani oʻrnatadigan qoidalar-ning oldindan belgilangan jami.

Баҳолаш объекти ва фойдаланувчи ўртасида йўл қўйиладиган ўзаро алоқани ўрнатадиган қоидаларнинг олдиндан белгиланган жами.

Руководство высшее

uz - oliy rahbariyat

олий раҳбарият

en - top management

Физическое лицо или группа лиц, осуществляющих руководство и управление организацией на высшем уровне.

Примечания

1 Высшее руководство имеет возможность делегировать полномочия и снабжать ресурсами в пределах организации.

2 Если область действия системы управления распространяется только на некоторые подразделения организации, тогда в состав высшего руководства входят только те лица, которые осуществляют руководство и управление этими подразделениями.

Tashkilotga yuqori darajada rahbarlik qiluvchi va uni boshqaruvchi jismoniy shaxs yoki shaxslar guruhi.

Izohlar

1 Oliy rahbariyat tashkilot doirasida vakolatlar berish va resurslar bilan taʼminlash imkoniyatiga ega.

2 Agar boshqarish tizimining amal qilish sohasi tashkilotning

Р

faqat ba'zi bir sohalariga taalluqli bo'lsa, unda oliy rahbariyat tarkibiga faqat ushbu bo'linmalarga rahbarlik qilish va ularni boshqarishni amalga oshiruvchi shaxslar kiradi.

Ташкилотга юқори даражада рахбарлик қилувчи ва уни бошқарувчи жисмоний шахс ёки шахслар гуруҳи.

Изоҳлар

1 Олий раҳбарият ташкилот доирасида ваколатлар бериш ва ресурслар билан таъминлаш имкониятига эга.

2 Агар бошқариш тизимининг амал қилиш соҳаси ташкилотнинг фақат баъзи бир соҳаларига тааллуқли бўлса, унда олий раҳбарият таркибига фақат ушбу бўлинмаларга рахбарлик қилиш ва уларни бошқаришни амалга оширувчи шахслар киради.

Ряд

uz - qator

қатор

en - family

Семейство ЭВМ, использующих единое программное обеспечение.

Yagona dasturiy ta'minotdan foydalanuvchi EHM turkumi.

Ягона дастурий таъминотдан фойдаланувчи ЭХМ туркуми.

С

Самокодирование

uz - o'zini o'zi kodlash

ўзини ўзи кодлаш

en - intrinsic coding

Кодирование информации с использованием самой информации в качестве ключа.

Axborotni, kalit sifatida axborotning o'zidan foydalanib, kodlash.

Ахборотни, калит сифатида ахборотнинг ўзидан фойдаланиб, кодлаш.

Сбор мусора

uz - axlat yig'ish

ахлат йиғиш

en - garbage collection

1 Атака, заключающаяся в поиске информации, остающейся в оперативной памяти или на накопителях информации после работы субъекта или объекта системы.

2 Выполнение несанкционированного поиска остаточных данных для получения чувствительной информации.

1 Subyekt yoki tizim obyektini ishidan so'ng, operativ

С

xotira yoki axborot to'plagichlarda qolgan axborotni izlashdan iborat hujum.

2 Ta'sirchan axborotni olish uchun qoldiq ma'lumotlarni qidirishni ruxsat etilmagan tarzda amalga oshirish.

1 Субъект ёки тизим объекти ишидан сўнг, оператив хотира ёки ахборот тўплагичларда қолган ахборотни излашдан иборат хужум.

2 Таъсирчан ахборотни олиш учун қолдиқ маълумотларни қидиришни рухсат этилмаган тарзда амалга ошириш.

Сведения особой важности

uz - alohida muhim
ma'lumotlar

алоҳида муҳим
маълумотлар

en - highly important
information

Наиболее охраняемые государством сведения из числа составляющих государственные секреты.

Davlat tomonidan qattiq muhofaza qilinadigan, davlat siri hisoblanadigan ma'lumotlar tarkibiga kiradigan ma'lumotlar.

Давлат томонидан қаттиқ муҳофаза қилинадиган, давлат сири ҳисобланадиган маълумотлар таркибига қирадиган маълумотлар.

Сведения секретные

uz - maxfiy ma'lumotlar

махфий маълумотлар

en - secret informations

Сведения, составляющие служебную тайну.

Xizmat siri hisoblanadigan ma'lumotlar.

Хизмат сири ҳисобланадиган маълумотлар.

Сведения совершенно секретные

uz - mutlaqo maxfiy

ma'lumotlar

мутлақо махфий
маълумотлар

en - top secret informations

Сведения, составляющие государственную тайну за исключением сведений особой важности.

Alohida muhim ma'lumotlardan tashqari davlat siri hisoblanadigan ma'lumotlar.

Алоҳида муҳим маълумотлардан ташқари давлат сири ҳисобланадиган маълумотлар.

Свидетельства аудита

uz - audit dalillari

аудит далиллари

en - audit evidence

Записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита и могут быть проверены.

Примечание – Свидетельства аудита могут быть качественными или количественными.

С

Audit kriteriyalariga aloqador va tekshirilishi mumkin bo'lgan, yozuvlar, faktlar bayoni yoki boshqa axborot.

Izoh – Audit dalillari sifat va miqdor jihatdan bo'lishi mumkin.

Аудит критерийларига алоқадор ва текширилиши мумкин бўлган, ёзувлар, фактлар баёни ёки бошқа ахборот.

Изоҳ – Аудит далиллари сифат ва миқдор жиҳатдан бўлиши мумкин.

Свидетельство управления конфигурацией

uz - konfiguratsiyani boshqarish dalili

конфигурацияни бошқариш далили

en - configuration management evidence

Все, что может быть использовано для укрепления доверия к правильному функционированию системы УК.

Примечание – Например, выходные данные УК, логические обоснования, предоставленные разработчиком, результаты измерений, эксперименты или интервью, проведенные оценщиком во время посещения им объекта.

КВ тизими то'g'ri ishlashiga bo'lgan ishonchni mustahkamlash uchun foydalaniladigan barcha narsa.

Izoh – Masalan, KB chiqish ma'lumotlari, ishlab chiquvchi tomonidan taqdim etilgan mantiqiy asoslar, o'lchashlar natijalari, baholovchi obyektga borganda o'tkazilgan eksperimentlar yoki intervyular.

КВ тизими тўғри ишлашига бўлган ишончни мустаҳкамлаш учун фойдаланиладиган барча нарса.

Изоҳ – Масалан, КВ чиқиш маълумотлари, ишлаб чиқувчи томонидан тақдим этилган мантиқий асослар, ўлчашлар натижалари, баҳоловчи объектга борганда ўтказилган экспериментлар ёки интервьюлар.

Связность

uz - bog'langanlik

боғланганлик

en - connectivity

Свойство объекта оценки, позволяющее ему взаимодействовать с логическими объектами информационной технологии, внешними по отношению к нему.

Примечание – Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

Baholash obyektining xususiyati, axborot texnologiyasining o'ziga nisbatan tashqi bo'lgan mantiqiy

С

obyektlari bilan o‘zaro hamkorlik qilish imkonini beradi.

Izoh – Bu o‘zaro hamkorlik simli yoki simsiz vositalar orqali, har qanday masofa, muhit yoxud har qanday konfiguratsiyada ma’lumotlar almashinuvini ichiga oladi.

Баҳолаш объектининг хусусияти, ахборот технологиясининг ўзига нисбатан ташқи бўлган мантикий объектлари билан ўзаро ҳамкорлик қилиш имконини беради.

Изоҳ – Бу ўзаро ҳамкорлик симли ёки симсиз воситалар орқали, ҳар қандай масофа, муҳит ёхуд ҳар қандай конфигурацияда маълумотлар алмашинувини ичига олади.

Связность временная

uz - vaqtinchalik bog‘langanlik

вақтинчалик

боғланганлик

en - temporal cohesion

Характеристики модуля, функции которого необходимо выполнять почти одновременно.

Примечание – Примерами модулей с временной связностью являются модули инициализации, модули восстановления и модули завершения работы.

Funksiyalari deyarli bir vaqtda bajarilishi zarur bo‘lgan modul xarakteristikalarini.

Izoh – Initsializatsiya moduli, qayta tiklanish moduli va ishni tugatish moduli vaqtinchalik bog‘langanlik modullariga misol bo‘ladi.

Функциялари деярли бир вақтда бажарилиши зарур бўлган модуль характеристикалари.

Изоҳ – Инициализация модули, қайта тикланиш модули ва ишни тугатиш модули вақтинчалик боғланганлик модулларига мисол бўлади.

Связность

коммуникативная

uz - kommunikativ

bog‘langanlik

коммуникатив

боғланганлик

en - communicational cohesion

Характеристика модуля, результаты функций которого выдаются другим функциям или функции которого используют результаты других функций.

Примечание – Примером модуля коммуникативной связности является модуль управления доступом, осуществляющий мандатное и дискреционное управление доступом, а также полномочное управление доступом.

Funksiyalarining natijalari boshqa funksiyalarga beriladigan yoki funksiyalari boshqa funksiyalar natijalaridan foydalanadigan modulning xarakteristikasi.

Izoh – Kommunikativ bog‘langan modulga misol bo‘lib, foydalana olishni boshqarish moduli, mandatli va diskret foydalana olishni boshqarish, shuningdek, foydalana olishning vakolatli boshqaruvi hisoblanadi.

С

Функцияларининг натижалари бошқа функцияларга бериладиган ёки функциялари бошқа функциялар натижаларидан фойдаланадиган модулнинг характеристикаси.

Изоҳ – Коммуникатив боғланган модулга мисол бўлиб, фойдалана олишни бошқариш модули, мандатли ва дискрет фойдалана олишни бошқариш, шунингдек, фойдалана олишнинг ваколатли бошқаруви ҳисобланади.

Связность логическая (процедурная)

uz - mantiqiy (protseduraviy) bog‘lanish

мантикий (процедурвий) боғланиш

en - logical (procedural) cohesion

Характеристики модуля, выполняющего одинаковые действия в разных структурах данных.

Примечание – Модуль имеет логическую связность, если его функции выполняют взаимосвязанные, но разные операции с разными входными данными.

Ma'lumotlarning turli strukturasiida bir xil harakatni bajaradigan modul xarakteristikasi.

Izoh – Modul uning funksiyalari o‘zaro bog‘liq, lekin turli kirish ma'lumotlari bilan turli operatsiyalarni bajarsa, mantiqiy bog‘lanishga ega bo‘ladi.

Маълумотларнинг турли структурасида бир хил ҳаракатни бажарадиган модуль характеристикаси.

Изоҳ – Модуль унинг функциялари ўзаро боғлиқ, лекин турли кириш маълумотлари билан турли операцияларни бажарса, мантикий боғланишга эга бўлади.

Связность (элементов модуля), прочность модульная

uz - bog‘langanlik (modul elementlarining bog‘langanligi), modulli chidamlilik

боғланганлик (модуль элементларининг боғланганлиги), модулли чидамлилиқ

en - cohesion, module strength

Способ и степень связи между собой задач, выполняемых одиночным программным модулем.

Примечание – Существуют различные виды связности элементов модуля: случайная, коммуникативная, функциональная, логическая, последовательная и временная.

Yakka dasturiy modul bajaradigan vazifalarning o‘zaro bir-biri bilan bog‘lanishining usul va darajasi.

Izoh – Modul elementlari bog‘lanishining turli ko‘rinishlari mavjud: tasodifiy, kommunikativ, funksional, mantiqiy, ketma-ket va vaqtinchalik.

Якка дастурий модуль бажарадиган вазифаларнинг ўзаро бир-бири билан боғланишининг усул ва даражаси.

Изоҳ – Модуль элементлари боғланишининг турли кўринишлари мавжуд: тасодифий, коммуникатив, функционал, мантикий, кетма-кет ва вақтинчалик.

Связность

Характеристика модуля, выходные данные каж-

С

последовательная

uz - ketma-ket bog‘langanlik

кетма-кет боғланганлик

en - sequential cohesion

дой функции которого являются входными данными для следующей функции этого модуля.

Примечание – Примером модуля с последовательной связностью является модуль, который выполняет функции ведения записей аудита и функции сохранения значений счетчика количества зарегистрированных нарушений определенного типа.

Nar bir funksiyasining chiqish ma’lumotlari shu modulning keyingi funksiyasi uchun kirish ma’lumotlari hisoblanadigan modulning xarakteristikasi.

Izoh – Audit yozuvlarini yuritish va ma’lum turdagi qayd etilgan buzilishlar sonini hisoblagich qiymatlarini saqlash funksiyalarini bajaradigan modul ketma-ket bog‘langanlikka ega modulga misol bo‘lib hisoblanadi.

Ҳар бир функциясининг чиқиш маълумотлари шу модулнинг кейинги функцияси учун кириш маълумотлари ҳисобланадиган модулнинг характеристикаси.

Изоҳ – Аудит ёзувларини юритиш ва маълум турдаги қайд этилган бузилишлар сонини ҳисоблагич қийматларини сақлаш функцияларини бажарадиган модуль кетма-кет боғланганликка эга модулга мисол бўлиб ҳисобланади.

Связность случайная

uz - tasodifiy bog‘langanlik

тасодифий боғланганлик

en - coincidental cohesion

Характеристика модуля, выполняющего несвязанные или слабо связанные действия.

Bog‘lanmagan yoki bo‘sh bog‘langan harakatlarni bajaradigan modul xarakteristikasi.

Боғланмаган ёки бўш боғланган ҳаракатларни бажарадиган модуль характеристикаси.

Связность функциональная

uz - funksional bog‘lanish

функционал боғланиш

en - functional cohesion

Функциональная характеристика модуля, который выполняет действия, связанные только с одной задачей.

Примечание – Функционально связный модуль преобразует один тип входных данных в один тип выходных данных; примерами таких модулей являются модуль управления стеком или модуль управления очередью.

Modulning faqat bitta vazifa bilan bog‘liq harakatni bajaradigan funksional xarakteristikasi.

Izoh – Funksional bog‘langan modul bir turdagi kiruvchi ma’lumotlarni bir turdagi chiquvchi ma’lumotlarga o‘zgartiradi; bunday modullarga stekni boshqaradigan modul yoki navbatni boshqaradigan modul misol bo‘lib hisoblanadi.

С

Модулнинг фақат битта вазифа билан боғлиқ ҳаракатни бажарадиган функционал характеристикаси.

Изоҳ – Функционал боғланган модуль бир турдаги кирувчи маълумотларни бир турдаги чиқувчи маълумотларга ўзгартиради; бундай модулларга стекни бошқарадиган модуль ёки навбатни бошқарадиган модуль мисол бўлиб ҳисобланади.

Секрет

uz - sir

сир

en - secret

Информация, которая должна быть известна только уполномоченным пользователям и/или функции безопасности объекта оценки для осуществления определенной политики функции безопасности.

Faqat vakolatli foydalanuvchiga ma'lum bo'lgan va/ yoki baholash obyektining xavfsizlik funksiyasi uchun belgilangan xavfsizlik funksiyasi siyosatini amalga oshiradigan axborot.

Фақат ваколатли фойдаланувчига маълум бўлган ва/ёки баҳолаш объектининг хавфсизлик функцияси учун белгиланган хавфсизлик функцияси сиёсатини амалга оширадиган ахборот.

Секретность информации

uz - axborotning maxfiyligi

ахборотнинг махфийлиги

en - information secrecy

Свойство информации, обеспечивающее при ее обработке техническими средствами предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Axborotning, uni texnik vositalar bilan qayta ishlashda axborotdan ruxsat etilmagan tarzda tanishishning yoki hujjatlashtirishning (nusxalar olishning) bartaraf etilishini ta'minlovchi xossasi.

Ахборотнинг, уни техник воситалар билан қайта ишлашда ахборотдан рухсат этилмаган тарзда танишишнинг ёки ҳужжатлаштиришнинг (нусхалар олишнинг) бартараф этилишини таъминловчи хоссаси.

Секретность совершенная

uz - mukammal maxfiylik

мукаммал махфийлик

Условие, заключающееся в том, что открытый текст и шифротекст статистически независимы и получение (перехват) шифротекста не дает крип-

С

en - unconditional secrecy

тоаналитику дополнительной информации об открытом тексте.

Ochiq matn va shifratn statistik jihatdan mustaqil va shifratnni olish (qo‘lga kiritish) kriptanalitikka ochiq matn to‘g‘risida qo‘shimcha axborot bermaydigan sharoit.

Очиқ матн ва шифрматн статистик жиҳатдан мустақил ва шифрматнни олиш (қўлга киритиш) криптоаналитикка очиқ матн тўғрисида қўшимча ахборот бермайдиган шароит.

Секреты государственные

uz - davlat sirlari

давлат сирлари

en - state secrets

Защищенные государством сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Республики Узбекистан. Государственные секреты делятся по степени секретности на сведения особой важности и совершенно секретные (государственная тайна).

Tarqatilishi O‘zbekiston Respublikasi manfaatlariga ziyon keltirishi mumkin bo‘lgan harbiy, tashqi siyosiy, iqtisodiy, ilmiy-texnikaviy, razvedka, kontrrazvedka bilan shug‘ullanuvchi va operativ-qidiruv faoliyati sohasidagi davlat tomonidan muhofaza qilindigan ma’lumotlar. Davlat sirlari maxfiylik darajasi-ga ko‘ra, alohida muhim ma’lumotlar va mutlaqo maxfiy (davlat siri) ma’lumotlarga bo‘linadi.

Тарқатилиши Ўзбекистон Республикаси манфатларига зиён келтириши мумкин бўлган ҳарбий, ташқи сиёсий, иқтисодий, илмий-техникавий, разведка, контрразведка билан шуғулланувчи ва оператив-қидирув фаолияти соҳасидаги давлат томонидан муҳофаза қилинадиган маълумотлар. Давлат сирлари махфийлик даражасига кўра, алоҳида муҳим маълумотлар ва мутлақо махфий (давлат сирини) маълумотларга бўлинади.

Сектор дополнительный

uz - qo‘shimcha sektor

Часть метода защиты от копирования, когда на дорожку сверх стандартного количества секто-

С

кўшимча сектор
en - extra sector

ров записывается еще один сектор.

Nusxa ko‘chirishdan muhofaza qilish metodining qismi, bunda yo‘lkaga sektorlarning standart miqdoridan ortiq yana bitta sektor yoziladi.

Нусха кўчиришдан муҳофаза қилиш методининг қисми, бунда йўлгага секторларнинг стандарт миқдоридан ортиқ яна битта сектор ёзилади.

Сектор ложный
uz - chalg‘ituvchi sektor
чалғитувчи сектор
en - false sector

Сектор, состоящий только из одного заголовка без данных, многократно записываемый на диск, чтобы его было невозможно скопировать с помощью программы несанкционированного копирования.

Ma‘lumotlarsiz, faqat sarlavhadan iborat bo‘lgan, uni ruxsat etilmagan tarzda nusxa ko‘chirish dasturi yordamida ko‘paytirish mumkin bo‘lmasligi uchun diskka ko‘p marotaba yozib olinadigan sektor.

Маълумотларсиз, фақат сарлавҳадан иборат бўлган, уни рухсат этилмаган тарзда нусха кўчириш дастури ёрдамида кўпайтириш мумкин бўлмаслиги учун дискка кўп маротаба ёзиб олинadиган сектор.

Семейство
uz - turkum
туркум
en - family

Набор компонентов, которые объединены одинаковыми целями, но могут отличаться акцентами или строгостью.

Bir xil maqsadlar bilan birlashtirilgan lekin, urg‘ulari yoki qat‘iyligi bilan farqlanuvchi komponentlar guruhi.

Бир хил мақсадлар билан бирлаштирилган лекин, урғулари ёки қатъийлиги билан фарқланувчи компонентлар гуруҳи.

Сервер-посредник
uz - vositachi server
воситачи сервер
en - proxy server

Межсетевой экран, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с межсетевым экраном, используется процесс, называемый трансляцией адресов.

Tarmoqlararo ekran, unda barcha mualliflashtirilgan mijozlarning IP-adreslarini tarmoqlararo ekran bilan

С

assotsiatsiyalangan *IP*-adreslarga o'zgartirish uchun adreslarni translyasiya qilish deb ataladigan jarayondan foydalaniladi.

Тармоқлараро экран, унда барча муаллифлаштирилган мижозларнинг *IP*-адресларини тармоқлараро экран билан ассоциацияланган *IP*-адресларга ўзгартириш учун адресларни трансляция қилиш деб аталадиган жараёндан фойдаланилади.

Сертификат

uz - sertifikat

сертификат

en - certificate

Набор относящихся к обеспечению безопасности данных, который выдан органом обеспечения безопасности или пользующейся доверием третьей стороной, в совокупности с информацией о безопасности, которая используется для предоставления услуг обеспечения целостности и аутентификации источника данных в отношении данных.

Xavfsizlikni ta'minlash organi yoki ishonch qozongan uchinchi tomon bergan, xavfsizlikni ta'minlashga taalluqli bo'lgan, ma'lumotlar manbaini autentifikatsiya qilishni ta'minlash xizmatlarini taqdim etish uchun foydalaniladigan, xavfsizlik to'g'risidagi axborot bilan birgalikdagi, ma'lumotlar to'plami.

Хавфсизликни таъминлаш органи ёки ишонч қозонган учинчи томон берган, хавфсизликни таъминлашга тааллуқли бўлган, маълумотлар манбаини аутентификация қилишни таъминлаш хизматларини тақдим этиш учун фойдаланиладиган, хавфсизлик тўғрисидаги ахборот билан биргаликдаги, маълумотлар тўплами.

Сертификат

аутентификации

uz - autentifikatsiya qilish
sertifikati

аутентификация қилиш
сертификати

en - authentication certificate

Сертификат безопасности, который гарантирован органом сертификации и который может быть использован для обеспечения идентификации объекта.

Sertifikatlash organi tomonidan kafolatlangan va obyektning identifikatsiya qilinishini ta'minlash uchun foydalanilishi mumkin bo'lgan xavfsizlik sertifikati.

Сертификатлаш органи томонидан кафолатланган ва объектнинг идентификация қилинишини

С

Сертификат авторизации
uz - mualliflashtirish sertifikatini
муаллифлаштириш
сертификати
en - authorization certificate

таъминлаш учун фойдаланилиши мумкин бўлган хавфсизлик сертификати.

Электронный документ, подтверждающий право доступа к информации, личность пользователя или иные его права и полномочия.

Axborotdan erkin foydalanish huquqini, foydalanuvchining shaxsini yoki uning boshqa huquqlari va vakolatlarini tasdiqlovchi elektron hujjat.

Ахборотдан эркин фойдаланиш ҳуқуқини, фойдаланувчининг шахсини ёки унинг бошқа ҳуқуқлари ва ваколатларини тасдиқловчи электрон ҳужжат.

Сертификат аннулирования
uz - bekor qilish sertifikatini
бекор қилиш сертификати
en - revocation certificate

Сертификат безопасности, выданный органом безопасности для указания, что конкретный сертификат безопасности был аннулирован.

Xavfsizlik organi tomonidan, muayyan xavfsizlik sertifikatini bekor qilinganligini ko'rsatish uchun beriladigan xavfsizlik sertifikatini.

Хавфсизлик органи томонидан, муайян хавфсизлик сертификати бекор қилинганлигини кўрсатиш учун бериладиган хавфсизлик сертификати.

Сертификат атрибута
uz - atribut sertifikatini
атрибут сертификати
en - attribute certificate

Структура данных, имеющая цифровую подпись органа по присвоению атрибутов, которая связывает некоторые значения атрибутов с идентификационной информацией о держателе этого атрибута.

Atributlarni berish organining raqamli imzosiga ega bo'lgan, atributlarning ba'zi qiymatlarini bu atributlarning egasi to'g'risidagi identifikatsion axborot bilan bog'laydigan ma'lumotlar strukturasi.

Атрибутларни бериш органининг рақамли имзосига эга бўлган, атрибутларнинг баъзи қийматларини бу атрибутларнинг эгаси тўғрисидаги идентификацион ахборот билан боғлайдиган маълумотлар структураси.

Сертификат безопасности
uz - xavfsizlik sertifikatini
хавфсизлик сертификати
en - security certificate

Набор связанных с безопасностью данных, выданных органом безопасности или пользующейся доверием третьей стороной, вместе с информацией безопасности, которая используется для обес-

С

печения услуг целостности и аутентификации источника данных.

Xavfsizlik organi yoki ishonch qozongan uchinchi tomon bergan xavfsizlik bilan bog'liq ma'lumotlarning, ma'lumotlar manbaini autentifikatsiya qilish va ma'lumotlarning yaxlitligini ta'minlash uchun foydalaniladigan xavfsizlik axboroti bilan birgalikdagi, to'plami.

Xavfsizlik organi ёки ишонч қозонган учинчи томон берган хавфсизлик билан боғлиқ маълумотларнинг, маълумотлар манбаини аутентификация қилиш ва маълумотларнинг яхлитлигини таъминлаш учун фойдаланиладиган хавфсизлик ахбороти билан биргаликдаги, тўплами.

Сертификат защиты

uz - muhofaza qilish sertifikati

муҳофаза қилиш

сертификати

en - protection certificate

1 Документ, удостоверяющий соответствие средств вычислительной техники или автоматизированной системы набору требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и/или распространение их как защищенных.

2 Надлежащим образом оформленный документ, выданный по правилам системы сертификации и подтверждающий соответствие средства защиты информации требованиям по безопасности информации.

1 Hisoblash texnikasi yoki avtomatlashtirilgan tizim vositalarining axborotdan ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish bo'yicha talablarga muvofiqligini tasdiqlovchi va ishlab chiquvchiga axborotdan muhofazalangan axborot sifatida foydalanish va/yoki tarqatish huquqini beradigan hujjat.

2 Tegishli ravishda rasmiylashtirilgan, sertifikatlash tizimi qoidalariga ko'ra berilgan va axborotni muhofaza qilish vositalarining axborot xavfsizligi bo'yicha talablarga muvofiq kelishini tasdiqlovchi hujjat.

1 Ҳисоблаш техникаси ёки автоматлаштирилган тизим воситаларининг ахборотдан рухсат этилмаган тарзда фойдалана олишдан муҳофаза қи-

С

лиш бўйича талабларга мувофиқлигини тасдиқловчи ва ишлаб чиқувчига ахборотдан муҳофазаланган ахборот сифатида фойдаланиш ва/ёки тарқатиш ҳуқуқини берадиган ҳужжат.

2 Тегишли равишда расмийлаштирилган, сертификатлаш тизими қоидаларига кўра берилган ва ахборотни муҳофаза қилиш воситаларининг ахборот хавфсизлиги бўйича талабларга мувофиқ келишини тасдиқловчи ҳужжат.

Сертификат ключа

uz - kalit sertifikati

калит сертификати

en - key certificate

Цифровое свидетельство, подтверждающее соответствие открытого ключа лицу, его выработавшему. В самой простой форме сертификаты содержат открытый ключ и имя автора ключа. Кроме этой информации, в сертификате также может содержаться дата окончания срока действия сертификата, название организации, выдавшей сертификат и некоторая другая информация.

Ochiq kalitning, uni ishlab chiquvchi shaxsga muvofiqligini tasdiqlovchi raqamli guvohnoma. Eng oddiy shaklda sertifikatlar ochiq kalit va kalit muallifining nomini o'z ichiga oladi. Bu axborotdan tashqari, sertifikatda sertifikatning amal qilish muddati tugagan sana, sertifikat bergan tashkilot nomi va ayrim boshqa axborot bo'lishi mumkin.

Очиқ калитнинг, уни ишлаб чиқувчи шахсга мувофиқлигини тасдиқловчи рақамли гувоҳнома. Энг оддий шаклда сертификатлар очиқ калит ва калит муаллифининг номини ўз ичига олади. Бу ахборотдан ташқари, сертификатда сертификатнинг амал қилиш муддати тугаган сана, сертификат берган ташкilot номи ва айрим бошқа ахборот бўлиши мумкин.

Сертификат органа

uz - organ sertifikati

орган сертификати

en - authority certificate

Сертификат, выданный органу (например, органу сертификации или органу по присвоению атрибутов).

Organga (masalan, sertifikatlash organiga yoki atributlarni berish bo'yicha organga) berilgan sertifikat.

Органга (масалан, сертификатлаш органига ёки атрибутларни бериш бўйича органга) берилган

С

сертификат.

Сертификат открытого ключа

uz - ochiq kalit sertifikati

очик калит сертификати

en - public key certificate

1 Открытый ключ пользователя и некоторая другая информация, не поддающаяся подделке благодаря шифрованию, вместе с личным ключом выдавшего его органа сертификации.

2 Значения, представляющие собой открытый ключ владельцев (и другую факультативную информацию), которые проверены и подписаны доверенным органом в формате, не поддающемся подделке.

1 Foydalanuvchining ochiq kaliti, uni bergan sertifikatlash organining shaxsiy kaliti bilan birga, shuningdek, shifrlash tufayli qalbakilashtirib bo'lmaydigan ba'zi bir boshqa axborot.

2 Qalbakilashtirib bo'lmaydigan formatda vakolatli organ tomonidan tekshirilgan va imzolangan, o'zida egalarining ochiq kalitini (boshqa ixtiyoriy axborotni) ifodalaydigan qiymatlar.

1 Фойдаланувчининг очик калити, уни берган сертификатлаш органининг шахсий калити билан бирга, шунингдек, шифрлаш туфайли қалбакилаштириб бўлмайдиган баъзи бир бошқа ахборот.
2 Қалбакилаштириб бўлмайдиган форматда ваколатли орган томонидан текширилган ва имзоланган, ўзида эгаларининг очик калитини (бошқа ихтиёрий ахборотни) ифодаляйдиган қийматлар.

Сертификат соответствия

uz - muvofiqlik sertifikati

мувофиқлик сертификати

en - conformance certificate

Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции и дающий право разработчику на эксплуатацию и/или распространение их как защищенных.

Hisoblash texnikasi vositalari yoki avtomat-lashtirilgan tizimning, davlat standartlari talablariga, sertifikatlash bo'yicha davlat organlari tomonidan, ularning vakolatlari doirasida tasdiqlangan axborotni

С

muhofaza qilish bo'yicha boshqa normativ hujjatlar talablariga muvofiqligini tasdiqlovchi va ishlab chiquvchiga ulardan muhofaza qilingan hujjat sifatida foydalanish va/yoki tarqatish huquqini beruvchi hujjat.

Хисоблаш техникаси воситалари ёки автоматлаштирилган тизимнинг, давлат стандартлари талабларига, сертификатлаш бўйича давлат органлари томонидан, уларнинг ваколатлари доирасида тасдиқланган ахборотни муҳофаза қилиш бўйича бошқа норматив ҳужжатлар талабларига мувофиқлигини тасдиқловчи ва ишлаб чиқувчига улардан муҳофаза қилинган ҳужжат сифатида фойдаланиш ва/ёки тарқатиш ҳуқуқини берувчи ҳужжат.

Сертификат списка аннулирования

uz - bekor qilish ro'yxatining sertifikati

бекор қилиш рўйхатининг сертификати

en - revocation list certificate

Сертификат безопасности, определяющий список сертификатов безопасности, которые были аннулированы.

Bekor qilingan xavfsizlik sertifikatlarining ro'yxatini belgilovchi xavfsizlik sertifikat.

Бекор қилинган хавфсизлик сертификатларининг рўйхатини белгиловчи хавфсизлик сертификати.

Сертификат цифровой

uz - raqamli sertifikat

рақамли сертификат

en - digital certificate

1 Электронный документ, которым доверенное третье лицо снабжает открытый ключ пользователя. Сертификат подтверждает, что срок действия ключа не истек и он действительно принадлежит пользователю.

2 Набор данных, который объединяет название организации или имя физического лица и его открытый ключ.

1 Ishonchli uchinchi shaxs foydalanuvchining ochiq kalitini ta'minlaydigan elektron hujjat. Sertifikat kalitning amal qilish muddati tugamaganligini va u haqiqatdan foydalanuvchiga tegishli ekanligini tasdiqlaydi.

2 Tashkilot nomini yoki jismoniy shaxs ismini hamda uning ochiq kalitini birlashtiradigan ma'lumotlar to'plami.

С

1 Ишончли учинчи шахс фойдаланувчининг очик калитини таъминлайдиган электрон хужжат. Сертификат калитнинг амал қилиш муддати тугамаганлигини ва у ҳақиқатдан фойдаланувчига тегишли эканлигини тасдиқлайди.

2 Ташкилот номини ёки жисмоний шахс исмини ҳамда унинг очик калитини бирлаштирадиган маълумотлар тўплами.

Сертификация

uz - sertifikatlash

сертификатлаш

en - certification

Процедура, посредством которой третья сторона гарантирует, что вся система обработки данных или ее часть соответствует требованиям безопасности.

Маълумотларни қайта ишлаш тизими yoki uning qismi xavfsizlik talablariga mos kelishini uchinchi tomon kafolatlaydigan protsedura.

Маълумотларни қайта ишлаш тизими ёки унинг қисми хавфсизлик талабларига мос келишини учинчи томон кафолатлайдиган процедура.

Сертификация системы защиты информации

uz - axborotni muhofaza qilish tizimini sertifikatlash

ахборотни муҳофаза

қилиш тизимини

сертификатлаш

en - information security system certification

Деятельность по подтверждению соответствия системы защиты информации требованиям государственных стандартов, иных нормативных документов по защите информации, утвержденных государственными органами по сертификации в пределах их компетенции.

Axborotni muhofaza qilish tizimining davlat standartlari talablariga, sertifikatlash bo'yicha davlat organlari tomonidan ularning vakolatlari doirasida tasdiqlangan axborotni muhofaza qilish bo'yicha boshqa normativ hujjatlarning talablariga muvofiqligini tasdiqlash bo'yicha faoliyat.

Ахборотни муҳофаза қилиш тизимининг давлат стандартлари талабларига, сертификатлаш бўйича давлат органлари томонидан уларнинг ваколатлари доирасида тасдиқланган ахборотни муҳофаза қилиш бўйича бошқа норматив хужжатларнинг талабларига мувофиқлигини тасдиқлаш бўйича фаолият.

Сертификация

Деятельность по подтверждению соответствия

С

соответствия в области защиты информации

uz - axborotni muhofaza qilish sohasida muvofiqlikni sertifikatlash

ахборотни муҳофаза қилиш соҳасида мувофиқликни сертификатлаш
en - conformance certificate in the information security field

Сеть телекоммуникаций общего пользования защищенная

uz - muhofazalangan umumiy foydalanishdagi telekommunikatsiyalar tarmogʻi

муҳофазаланган умумий фойдаланишдаги телекоммуникациялар тармоғи
en - protected public switched telecommunications network

средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации.

Axborotni muhofaza qilish vositalarining axborotni muhofaza qilish boʻyicha davlat standartlari yoki boshqa normativ hujjatlarning talablariga muvofiqligini tasdiqlash boʻyicha faoliyat.

Ахборотни муҳофаза қилиш воситаларининг ахборотни муҳофаза қилиш бўйича давлат стандартлари ёки бошқа норматив ҳужжатларнинг талабларига мувофиқлигини тасдиқлаш бўйича фаолият.

Сеть в которой любое воздействие нарушителя (из множества заданных при проектировании) либо не допускается с заданной вероятностью, либо обнаруживается средствами сети с заданной вероятностью, инициируя при этом реакцию сети, направленную на ликвидацию с заданной вероятностью последствий этого воздействия: информирование пользователей, локализацию места воздействия, восстановление работоспособности сети и создание условий, обеспечивающих передачу информации (данных) пользователей.

Muhofazalangan umumiy foydalanishdagi telekommunikatsiyalar tarmogʻi, bunda buzgʻunchining har qanday taʼsiriga (loyihalashda berilgan koʻplikdan), yo berilgan ehtimollik bilan yoʻl qoʻyilmaydi, yo tarmoq vositalari bilan berilgan ehtimollikda aniqlanadi, bunda tarmoqning ushbu taʼsirning oqibatlarini berilgan ehtimollikda bartaraf qilishga yoʻnaltirilgan javobi: foydalanuvchilarni xabardor qilish, taʼsir joyini kengayishiga yoʻl qoʻymasligini, tarmoqning ish qobiliyatini tiklash va foydalanuvchilarning axboroti (maʼlumotlari) uzatilishini taʼminlovchi sharoitlar yaratiladi.

Муҳофазаланган умумий фойдаланишдаги телекоммуникациялар тармоғи, бунда бузғунчининг ҳар қандай таъсирига (лойиҳалашда берилган

С

кўпликдан), ё берилган эҳтимоллик билан йўл кўйилмайди, ё тармоқ воситалари билан берилган эҳтимолликда аниқланади, бунда тармоқнинг ушбу таъсирнинг оқибатларини берилган эҳтимолликда бартараф қилишга йўналтирилган жавоби: фойдаланувчиларни хабардор қилиш, таъсир жойини кенгайтиришга йўл қўймаслигини, тармоқнинг иш қобилиятини тиклаш ва фойдаланувчиларнинг ахбороти (маълумотлари) узатилишини таъминловчи шароитлар яратилади.

Сеть Файстеля

uz - Faystel tarmog'i

Файстель тармоғи

en - Feistel network

Архитектура построения блочных шифров, доминирующая в настоящее время в традиционной криптографии, в которой весь процесс шифрования блока выполняется за серию шагов (раундов), на каждом из которых блок делится на изменяемую и постоянную части, с помощью функции шифрования из постоянной части и раундового ключа вырабатывается модифицирующий код, который используется для модификации изменяемой части посредством операции гаммирования.

Blokli shifrlar tuzish arxitekturasi. Bunda blokni shifrlashning butun jarayoni qadamlar (raundlar) ichida bajariladi. Ularning har birida blok o'zgaradigan va o'zgarmaydigan qismlarga ajratiladi. Shifrlash funksiyasi yordamida o'zgarmaydigan qism va raund kalitidan, gammalash operatsiyasi vositasida o'zgaradigan qismni modifikatsiyalashda foydalaniladigan modifikatsiyalovchi kod ishlab chiqiladi.

Блокли шифрлар тузиш архитектураси. Бунда блокни шифрлашнинг бутун жараёни қадамлар (раундлар) ичида бажарилади. Уларнинг ҳар бирида блок ўзгарадиган ва ўзгармайдиган қисмларга ажратилади. Шифрлаш функцияси ёрдамида ўзгармайдиган қисм ва раунд калитидан, гаммалаш операцияси воситасида ўзгарадиган қисмни модификациялашда фойдаланиладиган модификацияловчи код ишлаб чиқилади.

Сигнал информативный

uz - informativ signal

информатив сигнал

en - informative signal

Физический сигнал или химическая среда, содержащие информацию с ограниченным доступом.

Foydalanilishi cheklangan axborotni o'z ichiga oladi-

С

gan fizik signal yoki kimyoviy muhit.

Фойдаланилиши чекланган ахборотни ўз ичига оладиган физик сигнал ёки кимёвий муҳит.

Сигнатура
uz - signatura
 сигнатура
en - signature

1 Уникальная характеристика системы, которая может быть проверена программным способом. Примером сигнатуры может служить вторичный признак диска, используемый в качестве идентификационной метки диска-оригинала. Этот признак не должен копироваться программным способом.

2 Участок постоянного кода программы, по которому антивирусные программы обычно определяют принадлежность программ к программам-вирусам и другим нежелательным типам программ.

3 Характерные признаки вторжения (атаки), используемые для его (ее) обнаружения.

1 Tizimning dasturiy usulda tekshirish mumkin boʻlgan noyob xarakteristikasi. Original-diskning identifikatsion belgisi sifatida qoʻllaniladigan diskning ikkinchi belgisi signaturaga misol boʻladi. Bu belgidan dasturiy usulda nusxa koʻchirish mumkin emas.

2 Dastur doimiy kodining qismi, unga qarab, virusga qarshi dasturlar dasturlarning virus dasturlarga va dasturlarning boshqa nomaqbul turlariga mansubligini aniqlaydi.

3 Bostirib kirilish (hujum) ining, uni aniqlashda qoʻllaniladigan, xarakterli belgilari.

1 Tizimning dasturiy usulda tekshirish mumkin boʻlgan noyob xarakteristikasi. Original-diskning identifikatsion belgisi sifatida qoʻllaniladigan diskning ikkinchi belgisi signaturaga misol boʻladi. Bu belgidan dasturiy usulda nusxa koʻchirish mumkin emas.

2 Dastur doimiy kodining qismi, unga qarab, virusga qarshi dasturlar dasturlarning virus dasturlarga va dasturlarning boshqa nomaqbul turlariga mansubligini aniqlaydi.

3 Bostirib kirilish (hujum) ining, uni aniqlashda qoʻllaniladigan, xarakterli belgilari.

С

Сигнатура вируса

uz - virus signaturasi

вирус сигнатураси

en - virus signature

Уникальная последовательность битов, которая присуща каждой копии специфического вируса и которая может быть использована сканирующей программой для обнаружения его присутствия.

Bitlarning, spetsifik virusning har bir nusxasiga xos boʻlgan va uning mavjudligini aniqlash uchun skanlovchi dastur tomonidan foydalanilishi mumkin boʻlgan, yagona ketma-ketligi.

Битларнинг, специфик вируснинг ҳар бир нусхасига хос бўлган ва унинг мавжудлигини аниқлаш учун сканловчи дастур томонидан фойдаланилиши мумкин бўлган, ягона кетма-кетлиги.

Символ управляющий

uz - boshqaruvchi simvol

бошқарувчи символ

en - control character

Байт кода ASCII, который не выводится на печать, но управляет компьютером, принтером или другим устройством.

ASCII kodining bayti, u kompyuterdan chiqarilmaydi, lekin kompyuter, printer yoki boshqa qurilmani boshqaradi.

ASCII кодининг байти, у компьютердан чиқарилмайди, лекин компьютер, принтер ёки бошқа қурилмани бошқаради.

Система автоматизированная в защищённом исполнении

uz - muhofaza qilingan

avtomatlashtirilgan tizim

муҳофаза қилинган

автоматлаштирилган тизим

en - automatized system in

guarded construction

Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

Axborotni muhofaza qilish boʻyicha standartlar va/yoki normativ hujjatlarning talablariga muvofiq, belgilangan funksiyalar bajarilishining axborot texnologiyasini amalga oshiradigan avtomatlashtirilgan tizim.

Ахборотни муҳофаза қилиш бўйича стандартлар ва/ёки норматив ҳужжатларнинг талабларига мувофиқ, белгиланган функциялар бажарилишининг ахборот технологиясини амалга оширадиган

С

Система анализа защищенности

uz - muhofaza qilinganlikni
tahlil qilish tizimi

муҳофаза қилинганликни
таҳлил қилиш тизими

en - protection analysis system

автоматлаштирилган тизим.

Техническое или программное средство, предназначенное или используемое для анализа защищенности технических средств или автоматизированной системы.

Texnik vositalar yoki avtomatlashtirilgan tizimning muhofaza qilinganligini tahlil qilish uchun mo'ljallangan yoki ishlatiladigan texnik yoki dasturiy vosita.

Техник воситалар ёки автоматлаштирилган тизимнинг муҳофаза қилинганлигини таҳлил қилиш учун мўлжалланган ёки ишлатиладиган техник ёки дастурий восита.

Система восстановления

uz - tiklash tizimi

тиклаш тизими

en - recovery system

Комплекс программ и управляющих таблиц, предназначенных для поддержания целостности данных. Используется в банках данных и других автоматизированных системах.

Ма'lumotlarning yaxlitligini ta'minlashga qaratilgan dasturlar hamda boshqaruvchi jadvallar kompleksi. Ma'lumotlar bankida va boshqa avtomatlashtirilgan tizimlarda foydalaniladi.

Маълумотларнинг яхлитлигини таъминлашга қаратилган дастурлар ҳамда бошқарувчи жадваллар комплекси. Маълумотлар банкида ва бошқа автоматлаштирилган тизимларда фойдаланилади.

Система замков и ключей

uz - qulflar va kalitlar tizimi

қулфлар ва калитлар
tizimi

en - locks and keys (system)

Система защиты памяти, в которой сегментам памяти операционной системой присвоены идентификационные номера – замки, а зарегистрированным пользователям, числовые коды – ключи.

Xotirani muhofaza qilish tizimi. Unda хотира segmentlariga operatsion tizim tomonidan identifikatsion raqamlar – qulflar, ro'yxatga olingan foydalanuvchilarga esa, sonli kodlar – kalitlar beriladi.

Хотирани муҳофаза қилиш тизими. Унда хотира

С

сегментларига операцион тизим томонидан идентификацион рақамлар – қулфлар, рўйхатга олинган фойдаланувчиларга эса, сонли кодлар – калитлар бериледи.

Система защиты информации

uz - axborotni muhofaza qilish tizimi

ахборотни муҳофаза қилиш тизими

en - information security system

Совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Axborotni muhofaza qilish sohasiga tegishli huquqiy, tashkiliy-farmoyish beruvchi va normativ hujjatlar bilan belgilangan qoidalar bo'yicha tashkil qilingan hamda faoliyat ko'rsatadigan organlar va/yoki ijro etuvchilar, ular tomonidan foydalaniladigan axborotni muhofaza qilish texnikasining jami.

Ахборотни муҳофаза қилиш соҳасига тегишли ҳуқуқий, ташкилий-фармойиш берувчи ва норматив ҳужжатлар билан белгиланган қоидалар бўйича ташкил қилинган ҳамда фаолият кўрсатадиган органлар ва/ёки ижро этувчилар, улар томонидан фойдаланиладиган ахборотни муҳофаза қилиш техникасининг жами.

Система защиты информации (данных)

uz - axborot (ma'lumotlar)ni muhofaza qilish tizimi

ахборот (маълумотлар)ни муҳофаза қилиш тизими

en - information (data) protection system

1 Комплекс аппаратных, программных и криптографических средств, а также мероприятий, обеспечивающих защиту информации (данных) от случайного или преднамеренного разрушения, искажения или использования.

2 Совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности автоматизированной системы или циркулирующей в ней информации.

1 Apparat, dasturiy va kriptografik vositalar, shuningdek, axborot (ma'lumotlar)ning tasodifiy yoki

С

qasddan buzishdan, buzib ko'rsatilishdan yoki foydalanishdan muhofaza qilinishini ta'minlovchi tadbirlar kompleksi.

2 Huquqiy (qonuniy) va ma'muriy xarakterdagi maxsus chora-tadbirlar, tashkiliy tadbirlar, jismoniy va texnik (dasturiy va apparat) muhofaza vositalari, shuningdek, avtomatlashtirilgan tizim yoki unda aylanadigan axborotning xavfsizligini ta'minlash uchun mo'ljallangan maxsus personalning jami (kompleksi).

1 Аппарат, дастурий ва криптографик воситалар, шунингдек, ахборот (маълумотлар)нинг тасодифий ёки қасддан бузишдан, бузиб кўрсатилишдан ёки фойдаланишдан муҳофаза қилинишини таъминловчи тadbirlar kompleksi.

2 Ҳуқуқий (қонуний) ва маъмурий характердаги махсус чора-тадбирлар, ташкилий тадбирлар, жисмоний ва техник (дастурий ва аппарат) муҳофаза воситалари, шунингдек, автоматлаштирилган тизим ёки унда айланадиган ахборотнинг хавфсизлигини таъминлаш учун мўлжалланган махсус персоналнинг жами (комплекси).

Система защиты одноступенчатая

uz - bir pog'onali muhofaza tizimi

бир поғонали муҳофаза тизими

en - key to the door protection

Система защиты, в которой единственный ключ обеспечивает доступ к программному обеспечению.

Yagona kalit dasturiy ta'minotdan foydalanishni ta'minlaydigan muhofaza qilish tizimi.

Yagona kalit dasturiy ta'minotdan foydalaniшни таъминлайдиган муҳофаза қилиш тизими.

Система защиты информации от несанкционированного доступа

uz - axborotni ruxsatsiz foydalana olishdan muhofaza qilish tizimi

ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш тизими

en - unauthorized access data

Комплекс организационных мер и программно-технических (в том числе и криптографических) средств защиты информации от несанкционированного доступа к информации в автоматизированных системах.

Avtomatlashtirilgan tizimlarda axborotni ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish bo'yicha ko'riladigan tashkiliy chora-tadbirlar va dasturiy-texnik (shu jumladan, kriptografik) vosita-

С

protection system

lar kompleksi.

Автоматлаштирилган тизимларда ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш бўйича кўриладиган ташкилий чоратadbирлар ва дастурий-техник (шу жумладан, криптографик) воситалар комплекси.

Система защищенная

uz - muhofaza qilingan tizim

муҳофаза қилинган тизим

en - protected system

Система, вход в которую требует ввода пароля.

Kirish uchun parolning kiritilishi talab etiladigan tizim.

Кириш учун паролнинг киритилиши талаб этиладиган тизим.

Система идентификации

uz - identifikatsiyalash tizimi

идентификациялаш

тизими

en - identification system,

ID system

Криптографическая система, выполняющая функцию аутентификации сторон в процессе информационного взаимодействия.

Axborotga oid (informatsion) o'zaro hamkorlik jarayonida tomonlarni autentifikatsiya qilish funksiyasini bajaradigan kriptografik tizim.

Ахборотга оид (информацион) ўзаро ҳамкорлик жараёнида томонларни аутентификация қилиш функциясини бажарадиган криптографик тизим.

Система избыточная

uz - ortiqcha tizim

ортиқча тизим

en - redundant system

Система, обладающая избыточностью некоторого типа аппаратной, алгоритмической, информационной, обеспечивающей повышение надежности ее функционирования.

Tizimning ishonchli ishlash darajasi oshishini ta'minlovchi, qandaydir turdagi apparat, algoritm, axborot ortiqchaligiga ega tizim.

Тизимнинг ишончли ишлаш даражаси ошишини таъминловчи, қандайдир турдаги аппарат, алгоритм, ахборот ортиқчалигига эга тизим.

Система имитозащиты

uz - imitomuhofaza tizimi

имитомуҳофаза тизими

Криптографическая система, выполняющая функцию аутентификации содержания сообщения или документа и предназначенная для защи-

С

en - protection system from
fasified data

ты от несанкционированной модификации информации или навязывания ложной информации.

Xabar yoki hujjat mazmunini autentifikatsiya qilish funksiyasini bajaradigan va axborotni ruxsat etilmagan tarzda o'zgartirilishdan yoki soxta axborotning majburan kiritilishidan (qabul qilinishidan) muhofaza qilish uchun mo'ljallangan kriptografik tizim.

Хабар ёки ҳужжат мазмунини аутентификация қилиш функциясини бажарадиган ва ахборотни рухсат этилмаган тарзда ўзгартирилишдан ёки сохта ахборотнинг мажбуран киритилишидан (қабул қилинишидан) муҳофаза қилиш учун мўлжалланган криптографик тизим.

Система информационная
uz - axborot tizimi
ахборот тизими
en - information system

1 Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и телекоммуникаций, реализующих информационные процессы.

2 Приложения, сервисы, активы информационных технологий или любые другие компоненты обработки информации.

1 Hujjatlar (hujjatlar massivi) va axborot texnologiyalarining, shu jumladan, axborot jarayonlarini amalga oshiruvchi hisoblash texnikasi va telekommunikatsiyalar vositalaridan foydalanib, tashkiliy ravishda tartibga solingan to'plami.

2 Axborot texnologiyalarining ilovalari, servislari, aktivlari yoki axborotni qayta ishlashning har qanday boshqa komponentlari.

1 Ҳужжатлар (ҳужжатлар массиви) ва ахборот технологияларининг, шу жумладан, ахборот жараёнларини амалга оширувчи ҳисоблаш техникаси ва телекоммуникациялар воситаларидан фойдаланиб, ташкилий равишда тартибга солинган тўплами.

2 Ахборот технологияларининг иловалари, сервислари, активлари ёки ахборотни қайта ишлашнинг ҳар қандай бошқа компонентлари.

С

Система информационная автоматизированная

uz - avtomatlashtirilgan axborot tizimi

автоматлаштирилган ахборот тизими

en - automated information system

Совокупность программных и аппаратных средств, предназначенных для создания, передачи, обработки, распространения, хранения и/или управления данными и информацией и производства вычислений.

Axborot va ma'lumotlarni yaratish, uzatish, qayta ishlash, tarqatish, saqlash va/yoki boshqarish, shuningdek, hisoblashlarni amalga oshirish uchun mo'ljallangan dasturiy va apparat vositalarning jami.

Axborot va ma'lumotlarni yaratish, uzatish, qayta ishlash, tarqatish, saqlash va/yoki boshqarish, shuningdek, hisoblashlarni amalga oshirish uchun mo'ljallangan dasturiy va apparat vositalarning jami.

Система информационная защищенная

uz - muhofazalangan axborot tizimi

муҳофазаланган ахборот тизими

en - protected information system

Информационная система, в которой реализованы механизмы выполнения правил, удовлетворяющих установленному на основе анализа угроз перечню требований по защите информации и компонентов этой системы.

Tahdidlarni tahlil qilish asosida o'rnatilgan, axborotni hamda tizim komponentlarini muhofaza qilish bo'yicha talablar ro'yxatini qondiradigan qoidalarining bajarilish mexanizmi amalga oshirilgan axborot tizimi.

Tahdidlarni tahlil qilish asosida o'rnatilgan, axborotni hamda tizim komponentlarini muhofaza qilish bo'yicha talablar ro'yxatini qondiradigan qoidalarining bajarilish mexanizmi amalga oshirilgan axborot tizimi.

Система ключевая

uz - kalit tizimi

калит тизими

en - key system

1 Совокупность правил, определяющих порядок генерации, распределения, использования, хранения, смены, уничтожения и восстановления криптографических ключей.

2 Совокупность криптографических ключей и правил обращения с ними при обеспечении криптографической защиты информации.

1 Kriptografik kalitlarni generatsiya qilish, taqsim-

С

lash, ulardan foydalanish, saqlash, almashtirish, yo‘q qilish va tiklash tartibini belgilovchi qoidalar to‘plami.

2 Axborotning kriptografik muhofaza qilinishini ta‘minlashda, kriptografik kalitlar va ulardan foydalanish qoidalarining to‘plami.

1 Криптографик калитларни генерация қилиш, тақсимлаш, улардан фойдаланиш, сақлаш, алмасштириш, йўқ қилиш ва тиклаш тартибини белgilovchi қоидалар тўплами.

2 Ахборотнинг криптографик муҳофаза қилинишини таъминлашда, криптографик калитлар ва улардан фойдаланиш қоидаларининг тўплами.

Система кодирования

uz - kodlash tizimi

кодлаш тизими

en - coding system

Совокупность символов и правил кодирования; код.

Kodlash simvollari va qoidalarining yig‘indisi; kod.

Кодлаш символлари ва қоидаларининг йиғиндисиди; код.

Система компьютерная достоверная

uz - ishonchli kompyuter tizimi

ишончли компьютер

tizimi

en - trusted computer system

1 Система обработки данных, в которой предусмотрена достаточная компьютерная безопасность с учетом возможности одновременного доступа пользователей к данным с разными грифами секретности и категориями безопасности.

2 Система, обеспечивающая ведение безопасной обработки несортированного потока критичной информации за счет использования аппаратных и программных средств обеспечения безопасности.

1 Foydalanuvchilarning maxfiylik griflari va xavfsizlik kategoriyalari turlicha bo‘lgan ma‘lumotlardan bir vaqtda foydalana olish imkoniyati hisobga olingan holda, yetarlicha kompyuter xavfsizligi ko‘zda tutiladigan ma‘lumotlarni qayta ishlash tizimi.

2 Xavfsizlikni ta‘minlashning apparat va dasturiy vositalaridan foydalanish hisobiga, saralanmagan kritik axborot oqimining qayta ishlanishi xavfsiz olib borilishini ta‘minlovchi tizim.

1 Фойдаланувчиларнинг махфийлик грифлари ва хавфсизлик категориялари турлича бўлган маъ-

С

лумотлардан бир вақтда фойдалана олиш имконияти ҳисобга олинган ҳолда, етарлича компьютер хавфсизлиги кўзда тутиладиган маълумотларни қайта ишлаш тизими.

2 Хавфсизликни таъминлашнинг аппарат ва дастурий воситаларидан фойдаланиш ҳисобига, сараланмаган критик ахборот оқимининг қайта ишланиши хавфсиз олиб борилишини таъминловчи тизим.

1 Семейство выбираемых с помощью ключа обратимых преобразований, которые преобразуют открытый текст в шифротекст и обратно.

2 Совокупность технических и/или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

1 Ochiq matnni shifratga va aksincha o'zgartiradigan qayta o'zgartirishlarning kalit yordamida tanlab olinadigan turkumi.

2 Axborotning kriptografik qayta o'zgartirilishini va kalitlarni taqsimlash jarayoni boshqarilishini ta'minlovchi texnik va/yoki dasturiy vositalar, tashkiliy metodlarning jami.

1 Ochiq matnni shifratga va aksincha ўзgartiradigan qayta ўзgartirishlarning kalit ёрдамида танлаб олинadigan туркуми.

2 Ахборотнинг криптографик қайта ўзgartирилишини ва калитларни тақсимлаш жараёни бошқарилишини таъминловчи техник ва/ёки дастурий воситалар, ташкилий методларнинг жами.

Система, осуществляющая криптографическое преобразование информации для обеспечения ее безопасности.

Axborotni, uning xavfsizligini ta'minlash maqsadida, kriptografik qayta o'zgartirilishini amalga oshiruvchi tizim.

Ахборотни, унинг хавфсизлигини таъминлаш

Система

криптографическая

uz - kriptografik tizim

криптографик тизим

en - cryptographic system, cryptosystem

Система криптографической защиты информации

uz - axborotni kriptografik muhofaza qilish tizimi

ахборотни криптографик муҳофаза қилиш тизими

en - data cryptoprotection system

С

Система обеспечения информационной безопасности

uz - axborot xavfsizligini ta'minlash tizimi

ахборот хавфсизлигини таъминлаш тизими

en - information security system

мақсадида, криптографик қайта ўзгартирилишини амалга оширувчи тизим.

1 Совокупность органов и/или исполнителей, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами.

2 Совокупность правовых, организационных и технических мероприятий, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба интересам собственника информации.

1 Organlar yoki bajaruvchilar jami, ular foydalanadigan axborotni muhofaza qilish vositalari, shuningdek, tegishli huquqiy, tashkiliy-farmoyish beruvchi va normativ hujjatlar bilan belgilangan qoidalar bo'yicha tashkil qilingan va ish yuritadigan muhofaza obyektleri.

2 Axborot egasi manfaatlariga ziyon keltirilishini bartaraf qilish yoki jiddiy qiyinlashtirishga yo'naltirilgan huquqiy, tashkiliy va texnik tadbirlar, vositalar va normalar jami.

1 Органлар ёки бажарувчилар жами, улар фойдаланадиган ахборотни муҳофаза қилиш воситалари, шунингдек, тегишли ҳуқуқий, ташкилий-фармойиш берувчи ва норматив ҳужжатлар билан белгиланган қоидалар бўйича ташкил қилинган ва иш юритадиган муҳофаза объектлари.

2 Ахборот эгаси манфаатларига зиён келтирилишини бартараф қилиш ёки жиддий қийинлаштиришга йўналтирилган ҳуқуқий, ташкилий ва техник тadbirlar, воситалар ва нормалар жами.

Система обеспечения информационной безопасности сети телекоммуникаций общего пользования

uz - umumiy foydalanishdagi telekommunikatsiyalar tarmog'i

Совокупность правовых, организационных и технических мероприятий, служб и механизмов информационной безопасности, норм, органов управления и исполнителей в определенной сети телекоммуникаций общего пользования, направленных на обеспечение ее информационной без-

С

axborot xavfsizligini ta'minlash tizimi

умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизими
en - public switched telecommunications network information security system

опасности.

Umumiy foydalanishdagi muayyan telekommunikatsiyalar tarmog'ida, bu tarmoqning axborot xavfsizligini ta'minlashga qaratilgan huquqiy, tashkiliy va texnik tadbirlar, axborot xavfsizligi xizmatlari va mexanizmlari, normalar, boshqaruv organlari va bajaruvchilar jami.

Умумий фойдаланишдаги муайян телекоммуникациялар тармоғидаги, бу тармоқнинг ахборот хавфсизлигини таъминлашга қаратилган ҳуқуқий, ташкилий ва техник тadbirlar, ахборот хавфсизлиги хизматлари ва механизмлари, нормалар, бошқарув органлари ва bajaruvchilar жами.

Система обнаружения атак
uz - hujumlarni aniqlash tizimi

хужумларни аниқлаш тизими
en - intrusion detection system

Техническое или программное средство, предназначенное или используемое для обнаружения атак на ресурсы системы.

Tizim resurslariga qilinadigan hujumni aniqlash uchun mo'ljallangan yoki ishlatiladigan texnik yoki dasturiy vosita.

Тизим ресурсларига қилинадиган хужумни аниқлаш учун мўлжалланган ёки ишлатиладиган техник ёки дастурий восита.

Система обнаружения вторжений

uz - bostirib kirishlarni aniqlash tizimi

бостириб киришларни аниқлаш тизими
en - intrusion detection system

Программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

Axborot tizimida axborotdan qasddan foydalanishga yo'naltirilgan harakatlarni avtomatlashtirilgan tarzda aniqlash (blokirovkalash) funksiyalarini amalga oshiradigan, dasturiy yoki dasturiy-texnik vosita, axborotni qo'lga kiritish, yo'q qilish, buzish va undan foydalanishni blokirovkalash maqsadida, axborotga (axborot tashuvchilariga) maxsus ta'sir ko'rsatish.

Ахборот тизимида ахборотдан қасддан фойдаланишга йўналтирилган ҳаракатларни автоматлаштирилган тарзда аниқлаш (блокировкалаш) функцияларини амалга оширадиган, дастурий ёки дастурий-техник восита, ахборотни қўлга киритиш, йўқ қилиш, бузиш ва ундан фойдаланишни блокировкалаш мақсадида, ахборотга (ахборот ташувчиларига) махсус таъсир кўрсатиш.

Система обработки информации автоматизированная
uz - avtomatlashtirilgan
 axborotni qayta ishlash
 tizimi

автоматлаштирилган ахборотни қайта ишлаш тизими
en - automated data processing
 system

Организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, общественных или коммерческих организаций (юридических лиц), отдельных граждан (физических лиц) и иных потребителей информации.

Quyidagi o‘zaro bog‘langan komponentlarning jamini o‘zida aks ettiruvchi tashkiliy-texnik tizim: ma’lumotlarni qayta ishlash va uzatish texnik vositalari (hisoblash texnikasi va aloqa vositalari), tegishli dasturiy ta’minot ko‘rinishidagi qayta ishlash metodlari va algoritmlari, turli tashuvchilardagi ma’lumot massivlari (to‘plamlari, bazalari), davlat organlari, jamoat yoki tijorat tashkilotlari (yuridik shaxslar), ayrim fuqarolar (jismoniy shaxslar) va axborot boshqa iste’molchilarining axborotga bo‘lgan ehtiyojlarini qondirish maqsadida, ma’lumotlarni avtomatlashtirilgan tarzda qayta ishlashni bajarish uchun tashkiliy-struktura, tematik, texnologik yoki boshqa belgilarga ko‘ra birlashtirilgan personal va foydalanuvchilar.

С

Қуйидаги ўзаро боғланган компонентларнинг жамини ўзида акс эттирувчи ташкилий-техник тизим: маълумотларни қайта ишлаш ва узатиш техник воситалари (ҳисоблаш техникаси ва алоқа воситалари), тегишли дастурий таъминот кўринишидаги қайта ишлаш методлари ва алгоритмлари, турли ташувчилардаги маълумот массивлари (тўпламлари, базалари), давлат органлари, жамонат ёки тижорат ташкилотлари (юридик шахслар), айрим фуқаролар (жисмоний шахслар) ва ахборот бошқа истеъмолчиларининг ахборотга бўлган эҳтиёжларини қондириш мақсадида, маълумотларни автоматлаштирилган тарзда қайта ишлашни бажариш учун ташкилий-структура, тематик, технологик ёки бошқа белгиларга кўра бирлаштирилган персонал ва фойдаланувчилар.

Система операционная

uz - operatsion tizim
операцион тизим
en - operating system

Главная часть программного обеспечения, которая координирует и управляет ресурсами ЭВМ.

Dasturiy ta'minotning, EHM resurslarini muvofiq-lashtiradigan va boshqaradigan asosiy qismi.

Дастурий таъминотнинг, ЭХМ ресурсларини мувофиқлаштирадиган ва бошқарадиган асосий қисми.

Система операционная безопасная

uz - xavfsiz operatsion tizim
хавфсиз операцион тизим
en - secure operating system

Операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Tizim tomonidan nazorat qilinadigan ma'lumotlar va resurslar mazmuniga mos keladigan muhofaza darajasini ta'minlash maqsadida, apparat va dasturiy vositalarni samarali boshqaradigan operatsion tizim.

Тизим томонидан назорат қилинадиган маълумотлар ва ресурслар мазмунига мос келадиган муҳофаза даражасини таъминлаш мақсадида, аппарат ва дастурий воситаларни самарали бошқарадиган операцион тизим.

Система оценки

Административно-правовая структура, в рамках

С

uz - baholash tizimi
баҳолаш тизими
en - evaluation scheme

которой в определенном сообществе органы оценки применяют соответствующие стандарты.

Baholash organlarining muayyan hamjamiyati doirasida muvofiq standartlarni qoʻllaydigan maʼmuriy-huquqiy tizim.

Баҳолаш органларининг муайян ҳамжамияти доирасида мувофиқ стандартларни қўллайдиган маъмурий-ҳуқуқий тизим.

Система разграничения доступа
uz - foydalana olishni belgilash tizimi
фойдалана олишни белгилаш тизими
en - security policy realization

Совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Hisoblash texnikasi vositalari yoki avtomatlashtirilgan tizimlarda foydalana olishni belgilashni amalga oshiradigan qoidalar jami.

Ҳисоблаш техникаси воситалари ёки автоматлаштирилган тизимларда фойдалана олишни белгилашни амалга оширадиган қоидалар жами.

Система сертификации в области защиты информации
uz - axborotni muhofaza qilish sohasida sertifikatlash tizimi
ахборотни муҳофаза қилиш соҳасида сертификатлаш тизими
en - certification system in the field of information security

Система, располагающая собственными правилами, процедурами и управлением для проведения сертификации соответствия в области защиты информации.

Axborotni muhofaza qilish sohasida muvofiqlik sertifikatlashini oʻtkazish uchun oʻz qoidalari, protseduralari va boshqaruviga ega boʻlgan tizim.

Ахборотни муҳофаза қилиш соҳасида мувофиқлик сертификациясини ўтказиш учун ўз қоидалари, процедуралари ва бошқарувига эга бўлган тизим.

Система управления
uz - boshqarish tizimi
бошқариш тизими
en - management system

Совокупность взаимосвязанных или взаимодействующих элементов организации, на основе которых разрабатываются политики, цели и процессы, необходимые для достижения целей организации.

Примечания

1 Система управления может контролировать одну или более сфер деятельности.

2 Элементы системы включают структуру организации, роли и ответственности, планирование, процессы и т.д.

3 Область действия системы управления может распро-

С

страняться на всю организацию, специальные и общие функции организации, специальные и общие подразделения организации, или на одну или более функций, выполняемых группой организаций.

Tashkilotning o‘zaro bog‘liq yoki o‘zaro ishlaydigan elementlari jami, ular asosida tashkilot maqsadlariga erishish uchun zarur siyosatlar, maqsadlar va jarayonlar ishlab chiqiladi.

Izohlar

1 Boshqarish tizimi faoliyatning bitta yoki undan ko‘p sohasini nazorat qilishi mumkin.

2 Tizim elementlari tashkilot strukturasi, vazifalari va javobgarligini, rejalashtirish, jarayonlar va h.k.ni o‘z ichiga oladi.

3 Boshqarish tizimining amal qilish sohasi butun tashkilotga, tashkilotning maxsus va umumiy funksiyalariga, tashkilotning maxsus va umumiy bo‘linmalariga, tashkilotlar guruhi bajaradigan bitta yoki undan ortiq vazifaga taalluqli bo‘lishi mumkin.

Ташкилотнинг ўзаро боғлиқ ёки ўзаро ишлайдиган элементлари жами, улар асосида ташкилот мақсадларига эришиш учун зарур сиёсатлар, мақсадлар ва жараёнлар ишлаб чиқилади.

Изоҳлар

1 Бошқариш тизими фаолиятнинг битта ёки undan кўп соҳасини назорат қилиши мумкин.

2 Тизим элементлари ташкилот структурасини, вазифалари ва жавобгарлигини, режалаштириш, жараёнлар ва х.к.ни ўз ичига олади.

3 Бошқариш тизимининг амал қилиш соҳаси бутун ташкилотга, ташкилотнинг махсус ва умумий функцияларига, ташкилотнинг махсус ва умумий бўлинмаларига, ташкилотлар гуруҳи бажарадиган битта ёки undan ортик вазифага тааллуқли бўлиши мумкин.

Система управления доступом

uz - foydalana olishni

boshqarish tizimi

фойдалана олишни

бошқариш тизими

en - controlled access system

Автоматизированные средства физического управления доступом.

Примечание – В СУД используются идентификационные карты с магнитной полосой, смарт-карты, считывающие биометрические устройства.

Foydalana olishni jismoniy boshqarishning avtomatlashtirilgan vositalari.

Izoh – FBTda magnit polosali identifikatsion kartalardan, o‘qiydigan biometrik qurilmalardan, smart-kartalardan foydalaniladi.

С

Фойдалана олишни жисмоний бошқаришнинг автоматлаштирилган воситалари.

Изоҳ – ФБТда магнит полосали идентификацион карталардан, ўқийдиган биометрик қурилмалардан, смарт-карталардан фойдаланилади.

Система управления информационной безопасностью

uz - axborot xavfsizligini
boshqarish tizimi

ахборот хавфсизлигини

бошқариш тизими

en - information security man-
agement system ISMS

Часть общей системы управления, основанная на использовании методов оценки бизнес-рисков, предназначенная для разработки, внедрения, функционирования, мониторинга, анализа, обслуживания и совершенствования информационной безопасности.

Примечание – Система управления включает организационную структуру, политики, планирование деятельности, распределение ответственности, правила, процедуры, процессы и ресурсы.

Umumiy boshqarish tizimining, axborot xavfsizligini ishlab chiqish, joriy qilish, uning ishlashi, monitoringi, tahlili, unga xizmat ko'rsatish va uni takomillashtirish uchun mo'ljallangan, biznes-risklarni baholash usullaridan foydalanishga asoslangan qismi.

Izoh – Boshqarish tizimi o'z ichiga tashkiliy strukturani, siyosatlarini, faoliyatni rejalashtirishni, javobgarlikni taqsimlashni, qoidalarni, protseduralarni, jarayonlar va resurslarni oladi.

Умумий бошқариш тизимининг, ахборот хавфсизлигини ишлаб чиқиш, жорий қилиш, унинг ишлаши, мониторинги, таҳлили, унга хизмат кўрсатиш ва уни такомиллаштириш учун мўлжалланган, бизнес-рикларни баҳолаш усулларидан фойдаланишга асосланган қисми.

Изоҳ – Бошқариш тизими ўз ичига ташкилий структура-ни, сиёсатларни, фаолиятни режалаштиришни, жавобгар-ликни тақсимлашни, қоидаларни, процедураларни, жара-ёнлар ва ресурсларни олади.

Система управления ключами

uz - kalitlarni boshqarish
tizimi

калитларни бошқариш

tizimi

en - key management system

Составная часть ключевой системы, определяющая порядок использования, смены, хранения и архивирования, резервного копирования и восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения старых ключей.

Kalit tizimining, putur yetkazilgan (obro'sizlantirilgan) kalitlardan foydalanish, ularni almashtirish, saq-

С

lash va arxivlash, rezerv nusxa ko‘chirish, tiklash, muomaladan chiqarib tashlash, shuningdek, eski katalitlarni yo‘q qilish tartibini belgilovchi tarkibiy qismi.

Калит тизимининг, путур етказилган (обрўсизлантирилган) калитлардан фойдаланиш, уларни алмаштириш, сақлаш ва архивлаш, резерв нусха кўчириш, тиклаш, муомаладан чиқариб ташлаш, шунингдек, эски калитларни йўқ қилиш тартибини белгиловчи таркибий қисми.

Система управления конфигурацией

uz - konfiguratsiyani boshqarish tizimi

конфигурацияни

бошқариш тизими

en - configuration management system

Совокупность процедур и инструментальных средств (в том числе их документация), используемая разработчиком при разработке и сопровождении конфигураций его продуктов в течение их жизненных циклов.

Примечание – Системы управления конфигурацией могут обладать различными степенями строгости и функциями. Системы управления конфигурацией более высокого уровня могут быть автоматизированы, иметь механизмы устранения дефектов, механизмы контроля изменений и другие соответствующие механизмы.

Ishlab chiquvchi tomonidan konfiguratsiyani ishlab chiqish va uning mahsulotlarini ularning hayot sikli mobaynida ta'minlashda foydalaniladigan protseduralar va instrumental vositalar (shu jumladan, ularning hujjatlari) jami.

Izoh – Konfiguratsiyani boshqarish tizimlari turli darajadagi qat'iy va funksiyalarga ega bo'lishi mumkin. Birmuncha yuqori darajadagi konfiguratsiyani boshqarish tizimlari avtomatlashtirilgan bo'lishi, kamchiliklarni bartaraf etish mexanizmiga, o'zgarishlarni nazorat qilish mexanizmiga va boshqa tegishli mexanizmlarga ega bo'lishi mumkin.

Ишлаб чиқувчи томонидан конфигурацияни ишлаб чиқиш ва унинг маҳсулотларини уларнинг ҳаёт цикли мобайнида таъминлашда фойдаланиладиган процедуралар ва инструментал воситалар (шу жумладан, уларнинг ҳужжатлари) жами.

Изоҳ – Конфигурацияни бошқариш тизимлари турли даражадаги қатъий ва функцияларга эга бўлиши мумкин. Бирмунча юқори даражадаги конфигурацияни бошқариш тизимлари автоматлаштирилган бўлиши, камчиликларни бартараф этиш механизмига, ўзгаришларни назорат қи-

С

лиш механизмига ва бошқа тегишли механизмларга эга бўлиши мумкин.

Система установки ключей

uz - kalitlarni oʻrnatish tizimi

калитларни ўрнатиш

тизими

en - key setting system

Составная часть ключевой системы, определяющая алгоритмы и процедуры генерации, распределения, передачи и проверки ключей.

Kalit tizimining, kalitlarni generatsiyalash, taqsimlash, berish va tekshirish algoritmlari hamda protseduralarini belgilovchi tarkibiy qismi.

Калит тизимининг, калитларни генерациялаш, тақсимлаш, бериш ва текшириш алгоритмлари ҳамда процедураларини белгиловчи таркибий қисми.

Система цифровой подписи

uz - raqamli imzo tizimi

рақамли имзо тизими

en - digital signature system

Процедура и средства, обеспечивающие получателю гарантию подлинности полученного набора данных и достоверность факта отправки данных именно тем отправителем, от имени которого направлено сообщение.

Oluvchiga, olingan maʼlumotlar toʻplamining haqiqiyligini va maʼlumotlarning, aynan, nomidan xabar yuborilgan joʻnatuvchi tomonidan yuborilganlik faktining ishonchligini taʼminlaydigan protsedura hamda vositalar.

Олувчига, олинган маълумотлар тўпламининг ҳақиқийлигини ва маълумотларнинг, айнан, номидан хабар юборилган жўнатувчи томонидан юборилганлик фактининг ишончилигини таъминлайдиган процедура ҳамда воситалар.

Система экспертная

uz - ekspert tizimi

эксперт тизими

en - expert system

Комплекс программных средств, в основу которого положена интерпретация правил, аккумулирующих знания экспертов по определенной специальности.

Dasturiy vositalar kompleksi, uning asosiga maʼlum mutaxassislik boʻyicha ekspertlar bilimini toʻplovchi qoidalar talqini kiritilgan.

С

Дастурий воситалар комплекси, унинг асосига маълум мутахассислик бўйича экспертлар билимини тўпловчи қодалар талқини киритилган.

Сканер безопасности

uz - xavfsizlik skaneri

хавфсизлик сканери

en - security scanner

Программное средство, предназначенное для автоматизированного контроля и анализа сетевой безопасности, выявления активных компонентов сетевого взаимодействия и анализа их уязвимостей.

Tarmoq xavfsizligini tahlil va avtomatlashtirilgan nazorat qilish, tarmoq birgalikda ishlash aktiv komponentlarini aniqlash va ularning zaif tomonlarini tahlil qilish uchun mo'ljallangan dasturiy vosita.

Тармоқ хавфсизлигини таҳлил ва автоматлаштирилган назорат қилиш, тармоқ биргаликда ишлаш актив компонентларини аниқлаш ва уларнинг заиф томонларини таҳлил қилиш учун мўлжалланган дастурий восита.

Сканер сетевой

uz - tarmoq skaneri

тармоқ сканери

en - network scanner

Программа, которая осуществляет сбор информации о сети для нахождения компьютеров и программ, потенциально уязвимых к атакам.

Hujumlardan potensial yaxshi muhofazalanmagan dasturlar va kompyuterlarni topish maqsadida, tarmoq to'g'risida axborot to'plovchi dastur.

Хужумлардан потенциал яхши муҳофазаланмаган дастурлар ва компьютерларни топиш мақсадида, тармоқ тўғрисида ахборот тўпловчи дастур.

Сканер уязвимости

программ

uz - dasturlarning yaxshi

muhofazalanmaganlik skaneri

дастурларнинг яхши

муҳофазаланмаганлик

сканери

en - program vulnerability scanner

Программа, которая осуществляет проверку больших групп компьютеров в сети Интернет в поисках машин, уязвимых к тому или иному конкретному виду атаки.

Hujumning u yoki boshqa bir aniq turidan yaxshi muhofazalanmagan mashinalarni izlab topish maqsadida, Internet tarmog'ida kompyuterlarning katta guruhi tekshirilishini amalga oshiradigan dastur.

Хужумнинг у ёки бошқа бир аниқ туридан яхши муҳофазаланмаган машиналарни излаб топиш мақсадида, Интернет тармоғида компьютерларнинг катта гуруҳи текширилишини амалга оширадиган дастур.

С

Сканирование портов

uz - portlarni skanerlash
портларни сканерлаш
en - scanning port

Скремблер

uz - skrembler
скремблер
en - scrambler

Скремблирование

uz - skremblerlash
скремблерлаш
en - scrambling

След

uz - iz
из
en - footprint

Слово кодовое

Определение открытых TCP- или UDP-портов.

Ochiq TCP- yoki UDP-portlarini aniqlash.

Очиқ TCP- ёки UDP-портларини аниқлаш.

1 Шифровальное средство, предназначенное для защиты информации только от непосредственного прослушивания, просмотра или прочтения.

2 Аналоговый речевой шифратор.

1 Axborotni faqat bevosita eshitish, ko‘rib chiqish yoki o‘qishdan muhofaza qilish uchun mo‘ljallangan shifrlash vositasi.

2 Analog nutq shifrotori.

1 Ахборотни фақат бевосита эшитиш, кўриб чиқиш ёки ўқишдан муҳофаза қилиш учун мўлжалланган шифрлаш воситаси.

2 Аналог нутқ шифратори.

Простейший способ шифрования, основанный на перемешивании входного потока данных (обычно используется для улучшения синхронизирующих свойств входных данных).

Oddiy shifrlash usuli, ma'lumotlarning kirish oqimini aralashtirishga asoslangan (odatda, kirish ma'lumotlarining sinxronlovchi xususiyatlarini yaxshilash uchun ishlatiladi).

Оддий шифрлаш усули, маълумотларнинг кириш оқимини аралаштиришга асосланган (одатда, кириш маълумотларининг синхронловчи хусусиятларини яхшилаш учун ишлатилади).

Часть избыточного кода, которую можно использовать для выявления случаев нарушения авторского права.

Ortiqcha kodning, mualliflik huquqi buzilgan hollarini aniqlashda foydalanish mumkin bo‘lgan qismi.

Ортиқча коднинг, муаллифлик ҳуқуқи бузилган ҳолларни аниқлашда фойдаланиш мумкин бўлган қисми.

Средство аутентификации, представляющее со-

С

дополнительное

uz - qo‘shimcha kodli so‘z

кўшимча кодли сўз

en - supplementary codeword

бой кодовое слово, которое запрашивается у пользователя дополнительно после предъявления пароля.

Autentifikatsiya qilish vositasi. Parol ko‘rsatilgandan keyin foydalanuvchidan qo‘shimcha ravishda so‘raladigan kodli so‘z.

Аутентификация қилиш воситаси. Пароль кўрсатилгандан кейин фойдаланувчидан кўшимча равишда сўраладиган кодли сўз.

Сложность

uz - murakkablik

мураккаблик

en - complexity

Мера трудности понимания, анализа, тестирования и сопровождения программного обеспечения.

Dasturiy ta‘minotni tushunishdagi, tahlil qilish, testlash va ta‘minlashdagi qiyinchiliklar o‘lchovi.

Дастурий таъминотни тушунишдаги, таҳлил қилиш, тестлаш ва таъминлашдаги қийинчиликлар ўлчови.

Служба аутентификации удаленных пользователей по коммутируемым линиям

uz - kommutatsiyalanadigan

liniyalar bo‘yicha olisdagi foydalanuvchilarni autentifikatsiya qilish xizmati

коммутацияланадиган

линиялар бўйича олисдаги

фойдаланувчиларни аутентификация қилиш хизмати

en - remote authentication

dial-in user service

Протокол, предназначенный для централизованной проверки регистрационных данных пользователей (паролей и т.п.) на сервере аутентификации.

Autentifikatsiya qilish serverida foydalanuvchilarning qayd qilingan ma‘lumotlarini (parollar va sh.k.) markazlashtirilgan tarzda tekshirish uchun mo‘ljallangan protokol.

Аутентификация қилиш серверида фойдаланувчиларнинг қайд қилинган маълумотларини (пароллар ва ш.к.) марказлаштирилган тарзда текшириш учун мўлжалланган протокол.

Служба безопасности

uz - xavfsizlik xizmati

хавфсизлик хизмати

en - security service

Служба, обеспечивающая защиту систем телекоммуникаций и передаваемых данных.

Telekommunikatsiyalar tizimlarining va uzatiladigan ma‘lumotlarning muhofaza qilinishini ta‘minlovchi xizmat.

Телекоммуникациялар тизимларининг ва узатиладиган маълумотларнинг муҳофаза қилинишини таъминловчи хизмат.

Служба информационной

Организационно-техническая структура сети теле-

С

безопасности сети телекоммуникаций общего пользования

uz - umumiy foydalanishdagi telekommunikatsiyalar tarmog'ining axborot xavfsizligi xizmati

умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги хизмати
en - public switched telecommunications network information security service

Служба обеспечения информационной безопасности

uz - axborot xavfsizligini ta'minlash xizmati

ахборот хавфсизлигини таъминлаш хизмати
en - information security service

Смарфинг

uz - smarfing
смарфинг
en - smurfing

коммуникаций общего пользования, реализующая на базе определенных механизмов информационной безопасности определенные процедуры защиты, направленные на обеспечение информационной безопасности сети телекоммуникаций общего пользования.

Umumiy foydalanishdagi telekommunikatsiyalar tarmog'i axborot xavfsizligini ta'minlashga yo'naltirilgan, axborot xavfsizligining belgilangan mexanizmlari asosida belgilangan muhofaza protseduralarini amalga oshiruvchi, umumiy foydalanishdagi telekommunikatsiyalar tarmog'ining tashkiliy-texnik strukturasi.

Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлашга йўналтирилган, ахборот хавфсизлигининг белгиланган механизмлари асосида белгиланган муҳофаза процедураларини амалга оширувчи, умумий фойдаланишдаги телекоммуникациялар тармоғининг ташкилий-техник структураси.

Структурное подразделение, занимающееся разработкой, реализацией и контролем выполнения организационно-технических, аппаратно-программных и режимных мер обеспечения информационной безопасности.

Axborot xavfsizligini ta'minlashning tashkiliy-texnik, apparat-dasturiy va rejimli chora-tadbirlarini ishlab chiqish, amalga oshirish va nazorat qilish bilan shug'ullanadigan strukturaviy bo'linma.

Ахборот хавфсизлигини таъминлашнинг ташкилий-техник, аппарат-дастурий ва режимли чоратadbirlarини ишлаб чиқиш, амалга ошириш ва назорат қилиш билан шуғулланадиган структуравий бўлинма.

Способ атаки хакеров на сервер провайдера, заключающийся в отправке множества ping-запросов с ложным обратным адресом.

Hakerlarning provayder serveriga qiladigan hujum

С

usuli. Teskari adresi soxta bo'lgan ko'plab *ping* so'rovlarni yuborishda ifodalanadi.

Хакерларнинг провайдер серверига қиладиган хужум усули. Тескари адреси сохта бўлган кўплаб *ping* сўровларни юборишда ифодаланadi.

Снижение риска

uz - riskning pasayishi

рискнинг пасайиши

en - risk reduction

Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском.

Risk bilan bog'liq bo'lgan ehtimollikni, salbiy oqibatlarini yoki har ikkisini birgalikda kamaytirish uchun amalga oshiriladigan ishlar.

Риск билан боғлиқ бўлган эҳтимолликни, салбий оқибатларни ёки ҳар иккисини биргаликда камай-тириш учун амалга ошириладиган ишлар.

Сниффинг

uz - sniffing

сниффинг

en - sniffing

Прослушивание трафика с целью сбора передаваемых паролей, ключей и другой идентификационной или аутентификационной информации.

Uzatiladigan parollar, kalitlar va boshqa identifikatsion yoki autentifikatsion axborotni to'plash maqsadida, trafikni eshitish.

Узатиладиган пароллар, калитлар ва бошқа идентификацион ёки аутентификацион ахборотни тўплаш мақсадида, трафикни эшитиш.

Собственник информации

uz - axborot egasi

ахборот эгаси

en - owner of information

1 Субъект, реализующий в полном объеме полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

2 Субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информаци-

С

онный ресурс по наследству.

1 Qonunchilik aktlariga muvofiq axborotga egalik qilish, foydalanish vakolatini to'liq hajmda amalga oshiruvchi subyekt.

2 Axborot munosabatlarining, axborot resursiga egalik qilish, tasarruf etish va foydalanish yuridik huquqiga ega bo'lgan subyekt. Bunday yuridik huquq bu axborot resursini meros bo'yicha olgan shaxsga tegishli bo'ladi.

1 Қонунчилик актларига мувофиқ ахборотга эгаллик қилиш, фойдаланиш ваколатини тўлиқ ҳажмда амалга оширувчи субъект.

2 Ахборот муносабатларининг, ахборот ресурсига эгаллик қилиш, тасарруф этиш ва фойдаланиш юридик ҳуқуқига эга бўлган субъект. Бундай юридик ҳуқуқ бу ахборот ресурсини мерос бўйича олган шахсга тегишли бўлади.

Событие

uz - voqea-hodisa

воқеа-ҳодиса

en - event

1 Появление значимого нормального или отличного от нормального условия.

2 Случай определенного стечения обстоятельств.

Примечания

1 Событие может быть единичным или многократным и может иметь несколько причин.

2 Событие может быть определенным или неопределенным.

3 Вместо термина «событие» также могут быть использованы термины «инцидент» или «несчастный случай».

1 Ahamiyatli normalning yoki normal sharoitdan farq qiluvchining paydo bo'lishi.

2 Voqealarning muqarrar bir-biriga to'g'ri kelib qolish holati.

Izohlar

1 Voqea-hodisa bir yoki bir necha marta yuzaga kelishi va bir qancha sababga ega bo'lishi mumkin.

2 Voqea-hodisa ma'lum yoki noma'lum bo'lishi mumkin.

3 «Voqea-hodisa» atamasi o'rniga «insident» yoki «baxtsiz hodisa» atamalaridan ham foydalanish mumkin.

1 Аҳамиятли нормалнинг ёки нормал шароитдан фарқ қилувчининг пайдо бўлиши.

С

2 Воқеаларнинг муқаррар бир-бирига тўғри келиб қолиш ҳолати.

Изоҳлар

1 Воқеа-ҳодиса бир ёки бир неча марта юзага келиши ва бир қанча сабабга эга бўлиши мумкин.

2 Воқеа-ҳодиса маълум ёки номаълум бўлиши мумкин.

3 «Воқеа-ҳодиса» атамаси ўрнига «инцидент» ёки «бахтсиз ҳодиса» атамаларидан ҳам фойдаланиш мумкин.

Событие информационной безопасности

uz - axborot xavfsizligi hodisasi

ахборот хавфсизлиги

ҳодисаси

en - information security event

Идентифицированный случай состояния системы, услуги или сети, указывающий на возможное нарушение политики безопасности или на отказ средств защиты, либо на ранее неизвестную ситуацию, которая может быть существенной для безопасности.

Tizim, xizmat yoki tarmoq holatining xavfsizlik siyosatining buzilishi mumkinligini yoki himoya vositalarining buzilishini, yohud avval ma'lum bo'lmagan, xavfsizlik uchun ahamiyatga ega bo'lgan holatni ko'rsatuvchi identifikatsiyalangan hodisa.

Тизим, хизмат ёки тармоқ ҳолатининг хавфсизлик сиёсатининг бузилиши мумкинлигини ёки ҳимоя воситаларининг бузилишини, ёхуд аввал маълум бўлмаган, хавфсизлик учун аҳамиятга эга бўлган ҳолатни кўрсатувчи идентификацияланган ҳодиса.

Совместимость (компонентов)

uz - moslik (komponentlarning)

мослик

(компонентларнинг)

en - compatible (components)

Свойство компонента, заключающееся в способности предоставлять необходимые другим компонентам сервисы через соответствующие интерфейсы каждого компонента в совместимых средах функционирования.

Faoliyatning mos keladigan sohasida, har bir komponentning muvofiq interfeyslar orqali boshqa komponentlarga zarur xizmatlar ko'rsatish layoqati hisoblanadigan komponent xossasi.

Фаолиятнинг мос келадиган соҳасида, ҳар бир компонентнинг мувофиқ интерфейслар орқали бошқа компонентларга зарур хизматлар кўрсатиш лаёқати ҳисобланадиган компонент хоссаси.

С

Соглашение об аутентификации и выборе ключей

uz - kalitlarni autentifikatsiya qilish va tanlash to'g'risida bitim

калитларни
аутентификация қилиш ва
танлаш тўғрисида битим
en - authentication and key
selction agreement

Процедура двусторонней аутентификации в 3G-сетях, при которой на передающей стороне формируется аутентификационный вектор и согласуется с приемной стороной. Если соглашение достигнуто, то осуществляется вычисление ключей шифрования и целостности, в противном случае запрос отклоняется.

3G tarmoqlarida ikki tomonlama autentifikasiya qilish protsedurasi, bunda uzatuvchi tomonda autentifikatsion vektor shakllanadi va qabul qiluvchi tomon bilan kelishiladi. Agar kelishuvga erishilsa, shifrlash kalitini hisoblash amalga oshiriladi, aks holda, so'rov bekor qilinadi.

3G tarmoqlarida ikki tomonlama autentifikatsiya qilish protsedurasi, bunda uzatuvchi tomonda autentifikatsion vektor shakllanadi va qabul qiluvchi tomon bilan kelishiladi. Agar kelishuvga erishilsa, shifrlash kalitini hisoblash amalga oshiriladi, aks holda, so'rov bekor qilinadi.

Соккрытие

uz - yashirish
яшириш

en - hiding, concealment

Способ технической защиты информации, состоящий в ухудшении условий обнаружения носителей информации и ее получения.

Axborotni texnik muhofaza qilish usuli bo'lib, axborot tashuvchilarni aniqlash va axborotni olish sharoitlarini yomonlashtirishdan iborat.

Axborotni texnik muhofaza qilish usuli bo'lib, axborot tashuvchilarni aniqlash va axborotni olish sharoitlarini yomonlashtirishdan iborat.

Сообщение

uz - xabar
xabar

en - message

1 Строка битов ограниченной длины.

2 Информация, выраженная в определенной форме и предназначенная для передачи от источника информации к ее получателю с помощью сигналов различной физической природы.

1 Cheklangan uzunlikdagi bitlar satri.

2 Ma'lum shaklda ifodalangan va turli fizik tabiatga ega bo'lgan signallar yordamida axborot manбайдan uni oluvchiga uzatish uchun mo'ljallangan axborot.

С

1 Чекланган узунликдаги битлар сатри.

2 Маълум шаклда ифодаланган ва турли физик табиатга эга бўлган сигналлар ёрдамида ахборот манбаидан уни олувчига узатиш учун мўлжалланган ахборот.

Сообщение криптостойкое

uz - kriptobardoshli xabar

криптобардошли хабар

en - crypto-proof message

Сообщение, которое не может быть дешифровано без знания криптографического ключа.

Kriptografik kalitni bilmasdan turib, deshifrovka qilish mumkin bo'lmagan xabar.

Криптографик калитни билмасдан туриб, дешифровка қилиш мумкин бўлмаган хабар.

Сообщение одноразовое

uz - bir martali xabar

бир мартали хабар

en - single-shot message

Идентификатор или номер, который используется только один раз, т.е. в каждом последующем сеансе связи его значение обновляется.

Faqat bir marta ishlatiladigan identifikator yoki raqam, ya'ni har bir keyingi aloqa seansida uning qiymati yangilanadi.

Фақат бир марта ишлатиладиган идентификатор ёки рақам, яъни ҳар бир кейинги алоқа сеансида унинг қиймати янгиланади.

Сообщение с цифровой подписью

uz - raqamli imzoli xabar

рақамли имзоли хабар

en - digital signature message

Сообщение, которое не зашифровано, но содержит цифровую подпись.

Shifrlanmagan, lekin raqamli imzoga ega bo'lgan xabar.

Шифрланмаган, лекин рақамли имзога эга бўлган хабар.

Сообщество по обмену информацией

uz - axborot almashinuvi

bo'yicha hamjamiyat

ахборот алмашинуви

бўйича ҳамжамият

en - information sharing

community

Группа организаций, заключивших соглашение об обмене информацией.

Примечание – Организацией может называться и индивидуальный предприниматель.

Axborot almashinuvi to'g'risida shartnoma tuzgan tashkilotlar guruhi.

Izoh – Yakka tartibdagi tadbirkor ham tashkilot deb atalishi mumkin.

Ахборот алмашинуви тўғрисида шартнома тузган ташкилотлар гуруҳи.

Изоҳ – Якка тартибдаги тадбиркор ҳам ташкилот деб ата-

С

Соответствие

uz - muvofiqlik
мувофиқлик
en - conformity

Соответствие очевидное

uz - oshkora muvofiqlik
ошкора мувофиқлик
en - demonstrable conformance

Соответствие строгое

uz - qat'iy muvofiqlik
қатъий мувофиқлик
en - strict conformance

лиши мумкин.

Выполнение требования.

Talabning bajarilishi.

Талабнинг бажарилиши.

Связь между ЗБ и ПЗ, при которой ЗБ обеспечивает решение общей задачи безопасности, определенной в ПЗ.

Примечание – В ПЗ и ЗБ могут быть включены совершенно разные утверждения, относящиеся к разным логическим объектам, а также использоваться разные понятия и т.п. Очевидное соответствие применимо для тех типов объектов оценки, для которых уже имеются несколько аналогичных ПЗ; оно позволяет разработчику ЗБ одновременно утверждать о соответствии этим ПЗ и уменьшить трудоемкость.

HP va XT orasidagi bog'lanish, bunda XT HP belgilangan, umumiy xavfsizlik vazifasi hal qilinishini ta'minlaydi.

Izoh – XT hamda HP turli mantiqiy obyektlarga tegishli mutlaqo har xil fikrlar kiritilgan bo'lishi, shuningdek, turli tushunchalar va sh.k.dan foydalanilishi mumkin. Oshkora muvofiqlik baholash obyektining bir nechta o'xshash HP ega bo'lgan turlari uchun qo'llaniladi; u XT ishlab chiquvchisiga bir vaqtda shu HP mos kelishlikni tasdiqlash va mehnat sig'imini kamaytirish imkonini beradi.

ХП ва ХТ орасидаги боғланиш, бунда ХТ ХП белгиланган, умумий хавфсизлик вазифаси ҳал қилинишини таъминлайди.

Изоҳ – ХТ ҳамда ХП турли мантиқий объектларга тегишли мутлақо ҳар хил фикрлар киритилган бўлиши, шунингдек, турли тушунчалар ва ш.к.дан фойдаланилиши мумкин. Ошкора мувофиқлик баҳолаш объектининг бир нечта ўхшаш ХП эга бўлган турлари учун қўлланилади; у ХТ ишлаб чиқувчисига бир вақтда шу ХП мос келишликни тасдиқлаш ва меҳнат сигимини камайтириш имконини беради.

Иерархическая связь между профилем защиты и заданием по безопасности, когда все требования профиля защиты также содержатся и в задании по безопасности.

Himoya profili hamda xavfsizlik bo'yicha top-

С

shiriqlarning o‘zaro iyerarxik bog‘lanishi, bunda barcha himoya profili talablari xavfsizlik bo‘yicha topshiriqlarda ham bo‘ladi.

Химоя профили ҳамда хавфсизлик бўйича топшириқларнинг ўзаро иерархик боғланиши, бунда барча химоя профили талаблари хавфсизлик бўйича топшириқларда ҳам бўлади.

Состояние безопасное

uz - xavfsiz holat

хавфсиз ҳолат

en - secure state

Состояние, при котором данные функции безопасности объекта оценки являются непротиворечивыми и функции безопасности объекта оценки продолжает корректно выполнять функциональные требования безопасности.

Baholash obyektining xavfsizlik funksiyasi ma'lumotlari ziddiyatsiz bo'lgan va baholash obyektining xavfsizlik funksiyasi, xavfsizlikning funksional talblarini samarali bajarishda davom etadigan holat.

Баҳолаш объектнинг хавфсизлик функцияси маълумотлари зиддиятсиз бўлган ва баҳолаш объектнинг хавфсизлик функцияси, хавфсизликнинг функционал талабларини самарали бажаришда давом этадиган ҳолат.

Состояние безопасности

uz - xavfsizlik holati

хавфсизлик ҳолати

en - security state

Информация о состоянии, которая хранится в открытой системе и требуется для предоставления услуг безопасности.

Ochiq tizimda saqlanadigan va xavfsizlik xizmatlarini taqdim etish uchun talab etiladigan, holat to'g'risidagi axborot.

Очиқ тизимда сақланадиган ва хавфсизлик хизматларини тақдим этиш учун талаб этиладиган, ҳолат тўғрисидаги ахборот.

Состояние санкционированное (разрешенное)

uz - ruxsat etilgan holat

рухсат этилган ҳолат

en - authorized (allowed) state

Состояние, при котором непривилегированная программа имеет доступ к ресурсам, недоступным в других условиях.

Imtiyozga ega bo'lmagan dastur boshqa sharoitlarda erkin foydalanish mumkin bo'lmagan resurslardan foydalana oladigan holat.

С

Сохранность данных

uz - ma'lumotlarning yaxshi saqlanganligi

маълумотларнинг яхши сақланганлиги

en - data integrity

Спаминг

uz - spaming

спаминг

en - spamming

Специфицировать, определять

uz - spetsifikatsiyalamoq, belgilamoq

спецификацияламок, белгиламок

en - specify

Имтиёзга эга бўлмаган дастур бошқа шароитларда эркин фойдаланиш мумкин бўлмаган ресурслардан фойдалана оладиган ҳолат.

Способность информационной системы обеспечивать в течение своего жизненного цикла хранение данных в неискаженном виде и исключать их случайное уничтожение.

Axborot tizimining, o'z hayotiy sikli mobaynida, ma'lumotlarning buzilmagan holda saqlanishini va ularning tasodifiy ravishda yo'q qilinmasligini ta'minlash xususiyati.

Ахборот тизимининг, ўз ҳаётий цикли мобайнида, маълумотларнинг бузилмаган ҳолда сақланишини ва уларнинг тасодифий равишда йўқ қилинмаслигини таъминлаш хусусияти.

Посылка большого числа одинаковых сообщений в различные группы USENET. Часто используется для организации дешевой рекламной компании, пирамид или просто для того, чтобы надоест людям.

USENET turli guruhlariga bir xil xabarlarini ko'plab yuborish. Odatda, arzon reklama kompaniyasi, piramidalar tashkil qilish yoki shunchaki odamlarning joniga tegish uchun qo'llaniladi.

USENET turli guruhlariga bir xil xabarlarini ko'plab yuborish. Odatda, arzon reklama kompaniyasi, piramidalar tashkil qilish yoki shunchaki odamlarning joniga tegish uchun qo'llaniladi.

Предоставлять специфические подробности по некоторому логическому объекту в строгой и точной форме.

Ayrim mantiqiy obyektlar bo'yicha qat'iy va aniq shaklda spetsifik tafsilotlarni taqdim etish.

Айрим мантикий объектлар бўйича қатъий ва аниқ шаклда специфик тафсилотларни тақдим этиш.

С

Список апробированной продукции

uz - ma'qullangan mahsulot ro'uxati

маъқулланган маҳсулот рўйхати

en - evaluated products list

Список оборудования, аппаратуры и программного обеспечения, которое было оценено и признано соответствующим определенному классу, согласно стандарту Trusted Computer System Evaluation Criteria.

Trusted Computer System Evaluation Criteria standartiga muvofiq, ma'lum klassga mos keladi deb baholangan va tan olingan uskuna, apparatura va dasturiy ta'minot ro'uxati.

Trusted Computer System Evaluation Criteria standartiga muvofiq, ma'lum klassga mos keladi deb baholangan va tan olingan uskuna, apparatura va dasturiy ta'minot ruyxati.

Список доступа

uz - erkin foydalanish ro'uxati

эркин фойдаланиш рўйхати

en - access list

Массив записей контроля доступа.

Примечание – Различают дискреционный список контроля доступа, управляющий доступом пользователей к объекту, и системный список контроля доступа, управляющий аудитом доступа к объекту.

Erkin foydalanishni nazorat qilish yozuvlarining massivi.

Izoh – Erkin foydalanishni nazorat qilishning diskretion ro'uxati, foydalanuvchilarning obyektдан erkin foydalanishini nazorat qilishning tizim ro'uxati, obyektдан erkin foydalanish auditini boshqaruvchi farqlanadi.

Эркин фойдаланишни назорат қилиш ёзувларининг массиви.

Изоҳ – Эркин фойдаланишни назорат қилишнинг дискрецион рўйхати, фойдаланувчиларнинг объектдан эркин фойдаланишини назорат қилишнинг тизим рўйхати, объектдан эркин фойдаланиш аудитини бошқарувчи фарқланади.

Список конфигурации

uz - konfiguratsiya ro'uxati

конфигурация рўйхати

en - configuration list

Документ, содержащий выходные данные системы управления конфигурации с перечислением всех элементов конфигурации для конкретного продукта вместе с точной версией каждого элемента управления конфигурацией, соответствующей конкретной версии готового продукта.

Konfiguratsiyaning barcha sanab o'tilgan elementlari bilan konfiguratsiyani boshqarish tizimining chiqish ma'lumotlarini ichiga oladigan, ma'lum bir mahsulot

С

uchun har qaysi konfiguratsiyani boshqarish elementini aniq versiyasi bilan birga, tayyor mahsulotning aniq versiyasiga muvofiq keladigan hujjat.

Конфигурациянинг барча санаб ўтилган элементлари билан конфигурацияни бошқариш тизимининг чиқиш маълумотларини ичига оладиган, маълум бир маҳсулот учун ҳар қайси конфигурацияни бошқариш элементини аниқ версияси билан бирга, тайёр маҳсулотнинг аниқ версиясига мувофиқ келадиган ҳужжат.

Список полномочий

uz - vakolatlar ro'yxati
ваколатлар рўйхати
en - capability list

Ассоциированный с субъектом список, в котором указаны все виды доступа этого субъекта ко всем объектам.

Примечание – Для процесса, включенного в список, должны быть определены все виды доступа ко всем файлам и другим защищенным ресурсам.

Subyekt bilan assotsiatsiyalangan, shu subyektning hamma obyektlardan foydalanishining barcha turlari ko'rsatilgan ro'yxat.

Izoh – Ro'yxatga kiritilgan jarayon uchun barcha fayllardan va boshqa himoyalangan resurslardan foydalanishning barcha turlari aniqlangan bo'lishi kerak.

Субъект билан ассоциацияланган, шу субъектнинг ҳамма объектлардан фойдаланишининг барча турлари кўрсатилган рўйхат.

Изоҳ – Рўйхатга киритилган жараён учун барча файллардан ва бошқа ҳимояланган ресурслардан фойдаланишнинг барча турлари аниқланган бўлиши керак.

Список управления доступом

uz - erkin foydalanishni boshqarish ro'yxati
эркин фойдаланишни бошқариш рўйхати
en - access control list

1 Список логических объектов, имеющих полномочия на получение доступа к ресурсу, вместе с перечнем их прав доступа.

2 Представление матрицы доступа по столбцам – каждому объекту соответствует список субъектов вместе с их правами.

1 Resursdan erkin foydalanish imkoniyatini olish vakolatiga ega bo'lgan mantiqiy obyektlarning ularning foydalana olish huquqlari bilan birgalikdagi ro'yxati.

2 Erkin foydalanish matritsalarini ustunlar bo'yicha taqdim etish – har bir obyektga subyektlarning ro'y-

С

xati, ularning huquqlari bilan birga, mos keladi.

1 Ресурсдан эркин фойдаланиш имкониятини олиш ваколатига эга бўлган мантикий объектларнинг уларнинг фойдалана олиш ҳуқуқлари билан биргаликдаги рўйхати.

2 Эркин фойдаланиш матрицаларини устунлар бўйича такдим этиш – ҳар бир объектга субъектларнинг рўйхати, уларнинг ҳуқуқлари билан бирга, мос келади.

Способ защиты информации

uz - axborotni muhofaza qilish usuli

ахборотни муҳофаза

қилиш усули

en - information safety methods

Порядок и правила применения определенных принципов и средств защиты информации.

Axborotni muhofaza qilishning muayyan prinsiplari hamda vositalarini qo'llash tartibi va qoidalari.

Ахборотни муҳофаза қилишнинг муайян принциплари ҳамда воситаларини қўллаш тартиби ва қоидалари.

Спуфинг

uz - spufing

спуфинг

en - spoofing

1 Подмена адреса отправителя, реализуемая, как правило, одним из двух способов: либо злоумышленник маскируется под узел внутренней сети, где все узлы – доверенные (то есть попытка соединения выглядит как запрос внутреннему узлу от другого внутреннего узла), либо под доверенный внешний узел, если не предусмотрено никаких специальных алгоритмов аутентификации.

2 Вид сетевой атаки, при которой злоумышленник пытается войти в защищенную сеть, используя ложный сетевой адрес.

3 Получение доступа путем обмана, т.е. ситуация, когда пользователь пытается соединиться с Интернет-сервером, проху-сервером или межсетевым экраном, используя ложный IP-адрес.

1 Qoidaga ko'ra, ikkita usuldan birida amalga oshiriladigan jo'natuvchining adresini almashtirish: barcha uzellar ishonchli bo'lganda (ya'ni ulanishga urinish ichki uzalga boshqa ichki uzeldan so'rov sifatida ko'rinadi) yo jinoyatkor ichki tarmoq uzeli ostida niqoblanadi, yoki agar autentifikatsiya qilishning hech qanday maxsus algoritmlari ko'zda tutilmagan bo'lsa,

С

ishonchli tashqi uzal ostida niqoblanadi.

2 Tarmoq hujumining bir turi, bunda jinoyatkor soxta tarmoq adresidan foydalanib, muhofazalangan tarmoqqa kirishga harakat qiladi.

3 Foydalanuvchi soxta IP-adresni ishga solgan holda, internet-server, proxy-server yoki tarmoqlararo ekran bilan bog'lanishga harakat qilganda yuzaga keladigan vaziyat.

1 Қоидага кўра, иккита усулдан бирида амалга ошириладиган жўнатувчининг адресини алмаштириш: барча узеллар ишончли бўлганда (яъни уланишга уриниш ички узелга бошқа ички узелдан сўров сифатида кўринади) ё жинояткор ички тармоқ узели остида ниқобланади, ёки агар аутентификация қилишнинг ҳеч қандай махсус алгоритмлари кўзда тутилмаган бўлса, ишончли ташқи узел остида ниқобланади.

2 Тармоқ хужумининг бир тури, бунда жинояткор сохта тармоқ адресидан фойдаланиб, муҳофазаланган тармоққа киришга ҳаракат қилади.

3 Фойдаланувчи сохта IP-адресни ишга солган ҳолда, интернет-сервер, проху-сервер ёки тармоқлараро экран билан боғланишга ҳаракат қилганда юзага келадиган вазият.

Среда безопасная замкнутая

uz - yoriq xavfsiz muhit
ёпиқ хавфсиз муҳит
en - closed-security environment

Среда, в которой особое внимание уделяется защите данных и ресурсов от случайных или злоумышленных действий (в виде авторизации, категорий допусков, управления конфигурацией и т.д).

Маълумотлар ва ресурсларни тасодифий ёки қасддан қилинадиган ҳаракатлардан (муаллифлик, рұхсат бериш категориялари, конфигурациyani бoшқариш ва ҳ.к. кўринишда) муҳофаза қилишга алоҳида ётибор бериладиган муҳит.

Маълумотлар ва ресурсларни тасодифий ёки қасддан қилинадиган ҳаракатлардан (муаллифлик, рұхсат бериш категориялари, конфигурациyani бoшқариш ва ҳ.к. кўринишда) муҳофаза қилишга алоҳида ётибор бериладиган муҳит.

Среда безопасная открытая Среда, в которой защита данных и ресурсов от

С

uz - ochiq xavfsiz muhit
очик хавфсиз мухит
en - open-security environment

случайных или злоумышленных действий достигается посредством нормальных операционных процедур.

Ma'lumotlar va resurslarni tasodifiy yoki qasddan qilinadigan harakatlardan muhofaza qilishga normal operatsion protseduralar vositasida erishiladigan muhit.

Маълумотлар ва ресурсларни тасодифий ёки қасддан қилинадиган ҳаракатлардан муҳофаза қилишга нормал операцион процедуралар воситасида эришиладиган мухит.

Среда личной безопасности
uz - shaxsiy xavfsizlik muhiti
шахсий хавфсизлик
муҳити
en - personal security
environment

Безопасное местное хранилище для личного ключа объекта, ключ органа сертификации, пользующегося непосредственным доверием и возможно другие данные.

Примечание – В зависимости от политики обеспечения безопасности объекта или требований к системе эта среда может быть, например, криптографически защищенным файлом или маркером аппаратных средств, защищённых от умышленных повреждений.

Obyektning shaxsiy kaliti saqlnadigan xavfsiz mahalliy joy, bevosita ishonch qozongan sertifikatlash organining kaliti va mumkin bo'lgan boshqa ma'lumotlar.

Izoh – Obyekt xavfsizligini ta'minlash siyosatiga yoki tizimga qo'yiladigan talablarga bog'liq ravishda, bu muhit, masalan, kriptografik muhofazalangan fayl yoki qasddan shikastlashlardan muhofazalangan apparat vositalar markeri bo'lishi mumkin.

Объектнинг шахсий калити сақлнадиган хавфсиз маҳаллий жой, бевосита ишонч қозонган сертификатлаш органининг калити ва мумкин бўлган бошқа маълумотлар.

Изоҳ – Объект хавфсизлигини таъминлаш сиёсатига ёки тизимга қўйиладиган талабларга боғлиқ равишда, бу мухит, масалан, криптографик муҳофазаланган файл ёки қасддан шикастлашлардан муҳофазаланган аппарат воситалар маркери бўлиши мумкин.

Среда разработки
uz - ishlab chiqish muhiti
ишлаб чиқиш муҳити
en - development environment

Среда, в которой разрабатывается объект оценки.

Baholash obyektini ishlab chiqiladigan muhit.

Баҳолаш объекти ишлаб чиқиладиган мухит.

С

Среда с защитой целостности

uz - yaxlitlik muhofaza qilingan muhit

яхлитлик муҳофаза қилинган муҳит

en - integrity-protected environment

Среда, в которой предотвращаются или обнаруживаются несанкционированные изменения данных (включая создание и удаление).

Ma'lumotlarning ruxsat etilmagan tarzda o'zgartirishi (jumladan, yaratilishi va chiqarib tashlanishi)ning oldi olinadigan yoki aniqlanadigan muhit.

Маълумотларнинг рұхсат этилмаган тарзда ўзгартирилиши (жумладан, яратилиши ва чиқариб ташланиши)нинг олди олинадиган ёки аниқланадиган муҳит.

Среда функционирования

uz - ishlash muhiti

ишлаш муҳити

en - operational environment

Среда, в которой функционирует объект оценки.

Baholash obyekti faoliyat yuritadigan muhit.

Баҳолаш объекти фаолият юритадиган муҳит.

Средства защиты информации

uz - axborotni muhofaza qilish vositalari

ахборотни муҳофаза қилиш воситалари

en - data protection facilities

Технические, криптографические, программные и другие средства, предназначенные для защиты информации, средств, в которых они реализованы, а также средства контроля эффективности защиты информации.

Axborotni muhofaza qilish uchun mo'ljallangan texnik, kriptografik, dasturiy va boshqa vositalar, ular amalga oshirilgan vositalar, shuningdek, axborotni muhofaza qilish samaradorligini nazorat qilish vositalari.

Ахборотни муҳофаза қилиш учун мўлжалланган техник, криптографик, дастурий ва бошқа воситалар, улар амалга оширилган воситалар, шунингдек, ахборотни муҳофаза қилиш самарадорлигини назорат қилиш воситалари.

Средства защиты информации морально-этические

uz - axborotni muhofaza qilishning ma'naviy-axloqiy vositalari

ахборотни муҳофаза қилишнинг маънавий-ахлоқий воситалари

en - moral and ethical protection means

Всевозможные нормы, сложившиеся традиционно в государстве и обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако, несоблюдение их ведет обычно к потере авторитета и престижа человека.

Davlat va jamiyatda an'anaviy tarzda yuzaga keladigan barcha mumkin bo'lgan normalar. Ushbu normalarning katta qismi qonuniy choralar sifatida majburiy hisoblanmaydi, lekin ularga rioya qilmaslik, odatda inson obro'yi va nufuzi yo'qolishiga olib keladi.

С

Давлат ва жамиятда анъанавий тарзда юзага келадиган барча мумкин бўлган нормалар. Ушбу нормаларнинг катта қисми қонуний чоралар сифатида мажбурий ҳисобланмайди, лекин уларга риоя қилмаслик, одатда инсон обрўи ва нуфузи йўқолишига олиб келади.

Средства защиты информации от несанкционированного доступа

uz - axborotni ruxsatsiz foydalana olishdan muhofaza qilish vositalari

ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш воситалари

en - protection facilities of information from unauthorized access

Средства защиты информации технические (аппаратно-программные)

uz - axborotni muhofaza qilish texnik (apparat-dasturiy) vositalari

ахборотни муҳофаза қилиш техник (аппарат-дастурий) воситалари

en - technical (hardware and software) data protection facilities

Аппаратные, программные, аппаратно-программные, криптографические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа, а также средства контроля эффективности защиты информации.

Ruxsat etilmagan tarzda foydalana olishning oldini olish yoki sezilarli darajada qiyinlashtirish uchun mo'ljallangan apparat, dasturiy, apparat-dasturiy, kriptografik vositalar, shuningdek, axborotni muhofaza qilish samaradorligini nazorat qilish vositalari.

Рухсат этилмаган тарзда фойдалана олишнинг олдини олиш ёки сезиларли даражада қийинлаштириш учун мўлжалланган аппарат, дастурий, аппарат-дастурий, криптографик воситалар, шунингдек, ахборотни муҳофаза қилиш самарадорлигини назорат қилиш воситалари.

Различные электронные устройства и специальные программы, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

Axborotni muhofaza qilish funksiyalarini (foydalanuvchilarni identifikatsiyalash va autentifikatsiya qilish, resurslardan erkin foydalanishni cheklash, voqealarni qayd qilish, axborotni kriptografik berkitish va b.q.) (mustaqil yoki boshqa vositalar bilan birgalikda) bajaradigan turli xil elektron qurilmalar va maxsus dasturlar.

Ахборотни муҳофаза қилиш функцияларини

С

(фойдаланувчиларни идентификациялаш ва аутентификация қилиш, ресурслардан эркин фойдаланишни чеклаш, воқеаларни қайд қилиш, ахборотни криптографик беркитиш ва б.қ.) (мустақил ёки бошқа воситалар билан биргаликда) бажарадиган турли хил электрон қурилмалар ва махсус дастурлар.

Средства защиты физические

uz - jismoniy muhofaza
qilish vositalari

жисмоний муҳофаза
қилиш воситалари

en - physical protection
facilities

Автономные устройства и системы, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа злоумышленника.

Примечание – Физическими средствами защиты могут быть замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Jinoyatkorning suqulib kirishi va foydalana olishi mumkin bo'lgan yo'llarda jismoniy to'siqlarni yaratish uchun maxsus mo'ljallangan avtonom qurilma va tizimlar.

Izoh – Apparatura joylashgan eshiklardagi qulflar, derazadagi panjaralar, qo'riqlash signalizatsiyasining elektron mexanik uskunasi jismoniy muhofaza qilish vositalari bo'lishi mumkin.

Жинояткорнинг суқулиб кириши ва фойдалана олиши мумкин бўлган йўлларда жисмоний тўсиқларни яратиш учун махсус мўлжалланган автоном қурилма ва тизимлар.

Изоҳ – Аппаратура жойлашган эшиклардаги қулфлар, деразадаги панжаралар, қўриқлаш сигнализациясининг электрон механик ускунаси жисмоний муҳофаза қилиш воситалари бўлиши мумкин.

Средства защиты информации законодательные

uz - axborotni muhofaza
qilishning qonunchilik
vositalari

ахборотни муҳофаза
қилишининг қонунчилик
воситалари

en - legislative data protection
facilities

Законодательные акты страны, которые регламентируют правила использования, обработки и передачи информации ограниченного доступа и устанавливают меры ответственности за нарушение этих правил.

Mamlakatning, erkin foydalanilishi cheklangan axborotdan foydalanish, ularni qayta ishlash va uzatish qoidalarini qat'iy tartibga soladigan va bu qoidalarning buzilganligi uchun javobgarlik choralarini belgilaydigan qonunchilik aktlari.

С

Мамлакатнинг, эркин фойдаланилиши чекланган ахборотдан фойдаланиш, уларни қайта ишлаш ва узатиш қоидаларини қатъий тартибга соладиган ва бу қоидаларнинг бузилганлиги учун жавобгарлик чораларини белгилайдиган қонунчилик актлари.

Средства защиты информации организационные

uz - axborotni muhofaza qilishning tashkiliy vositalari

ахборотни муҳофаза қилишнинг ташкилий воситалари

en - organizational protection means

Организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации сети телекоммуникаций для обеспечения защиты информации.

Примечание – Организационные мероприятия охватывают все структурные элементы сети на всех этапах их жизненного цикла (проектирование, испытание и эксплуатация).

Axborotning muhofaza qilinishini ta'minlash maqsadida, telekommunikatsiyalar tarmoqlarini yaratish va ulardan foydalanish jarayonida amalga oshiriladigan tashkiliy-texnik va tashkiliy-huquqiy tadbirlar.

Izoh – Tashkiliy tadbirlar ular hayot siklining barcha bosqichlarida (loyihalash, sinov va ekspluatatsiya qilish) tarmoqning barcha struktura elementlarini qamrab oladi.

Ахборотнинг муҳофаза қилинишини таъминлаш мақсадида, телекоммуникациялар тармоқларини яратиш ва улардан фойдаланиш жараёнида амалга ошириладиган ташкилий-техник ва ташкилий-ҳуқуқий тадбирлар.

Изоҳ – Ташкилий тадбирлар улар ҳаёт циклининг барча bosqichlarida (лойиҳалаш, синов ва эксплуатация қилиш) тармоқнинг барча структура элементларини қамраб олади.

Средства имитозащиты

uz - imitomuhofaza vositalari

имитомуҳофаза воситалари

en - imitoprotection means

Аппаратные, программные и аппаратно-программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Axborotni kriptografik almashtirish algoritmlarini amalga oshiruvchi va yolg'on axborotni majburan qabul qildirishdan muhofaza qilish uchun mo'ljallangan apparat, dasturiy va apparat-dasturiy vositalar.

С

Ахборотни криптографик алмаштириш алгоритмларини амалга оширувчи ва ёлгон ахборотни мажбуран қабул қилдиришдан муҳофаза қилиш учун мўлжалланган аппарат, дастурий ва аппарат-дастурий воситалар.

Средства кодирования

uz - kodlash vositalari

кодлаш воситалари

en - coding tools

Средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций.

Almashtirishning bir qismini qo‘l operatsiyalari yordamida bajargan holda axborotni kriptografik almashtirish algoritmlarini amalga oshiruvchi vositalar.

Алмаштиришнинг бир қисмини қўл операциялари ёрдамида бажарган ҳолда ахборотни криптографик алмаштириш алгоритмларини амалга оширувчи воситалар.

Средства

криптографические

uz - kriptografik vositalar

криптографик воситалар

en - cryptographic facilities

1 Методы и средства обеспечения безопасности информации, использующие криптографические преобразования информации.

2 Средства, реализованные в виде документов, механических, электромеханических, электронных, технических устройств или программ, предназначенных для выполнения функций криптографической системы.

1 Axborotni kriptografik o‘zgartirishlardan foydalaniladigan, axborot xavfsizligini ta’minlashning metod hamda vositalari.

2 Kriptografik tizim funksiyalarini bajarish uchun mo‘ljallangan hujjatlar, mexanik, elektromexanik, elektron texnik qurilmalar yoki dasturlar ko‘rinishidagi vositalar.

1 Ахборотни криптографик ўзгартиришлардан фойдаланиладиган, ахборот хавфсизлигини таъминлашнинг метод ҳамда воситалари.

2 Криптографик тизим функцияларини бажариш учун мўлжалланган ҳужжатлар, механик, электромеханик, электрон техник қурилмалар ёки дастурлар кўринишидаги воситалар.

С

Средства криптографической защиты информации

uz - axborotni kriptografik muhofaza qilish vositalari

axborotni kriptografik muhofaza qilish vositalari
en - cryptographic information protection facilities

Аппаратные, программные или аппаратно-программные средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности.

Примечание – К средствам криптографической защиты информации относятся также средства изготовления ключевых документов и сами ключевые документы (независимо от вида носителя ключевой информации).

Axborot xavfsizligini ta'minlash uchun axborotning kriptografik almashtirilishini amalga oshiradigan apparat, dasturiy yoki apparat-dasturiy vositalar.

Izoh – Axborotni kriptografik muhofaza qilish vositalariga, shuningdek, muhim hujjatlarni tayyorlash vositalari va muhim hujjatlarning o'zi ham (muhim axborotni tashuvchining turiga bog'liq bo'lmagan holda) kiradi.

Axborot xavfsizligini ta'minlash uchun axborotning kriptografik almashtirilishini amalga oshiradigan apparat, dasturiy yoki apparat-dasturiy vositalar.

Izoh – Axborotni kriptografik muhofaza qilish vositalariga, shuningdek, muhim hujjatlarini tayyorlash vositalari va muhim hujjatlarining o'zi ham (muhim axborotni tashuvchining turiga bog'liq bo'lmagan holda) kiradi.

Средства обработки информации

uz - axborotni qayta ishlash vositalari

axborotni qayta ishlash vositalari
en - information processing facilities

Любая система обработки информации, сервисы или инфраструктура, или места, где они физически расположены.

Axborotni qayta ishlashning istalgan tizimi, servislar yoki infratuzilma yoki ular fizik jihatdan joylashgan joylar.

Axborotni qayta ishlashning istalgan tizimi, servislar yoki infratuzilma yoki ular fizik jihatdan joylashgan joylar.

Средства разработки инструментальные

uz - instrumental ishlab chiqish vositalari

инструментал ishlab chiqish vositalari

Инструментальные средства (в том числе, при необходимости, программное обеспечение тестирования), используемые при разработке и производстве ОО.

Примечание – Например, при разработке программного ОО обычно используются следующие инструментальные

С

en - development tools

средства: языки программирования, компиляторы, инструментальные средства компоновки и генерации.

BOни ishlab chiqarish hamda ishlab chiqishda (shuningdek, zarur bo'lganda, testlashni dasturiy ta'minlash) ishlatiladigan instrumental vositalar.

Izoh – Masalan, dasturiy BOни ishlab chiqishda odatda, quyidagi instrumental vositalardan foydalaniladi: dasturlash tillari, kompilyatorlar, komponovka va generatsiya instrumental vositalari.

BOни ишлаб чиқариш ҳамда ишлаб чиқишда (шунингдек, зарур бўлганда, тестлашни дастурий таъминлаш) ишлатиладиган инструментал воситалар.

Изоҳ – Масалан, дастурий BOни ишлаб чиқишда одатда, қуйидаги инструментал воситалардан фойдаланилади: дастурлаш тиллари, компиляторлар, компоновка ва генерация инструментал воситалари.

**Средства технические
вспомогательные**

uz - yordamchi texnik vositalar
ёрдамчи техник воситалар
en - support technology

Средства и системы формирования, передачи, приема, преобразования, отображения и хранения открытой информации, средства и системы жизнеобеспечения различного назначения, которые могут создавать технические каналы утечки информации.

Ochiq axborotni shakllantirish, uzatish, qabul qilish, o'zgartirish, aks ettirish va saqlash vositalari hamda tizimlari, axborot chiqib ketishi mumkin bo'lgan texnik kanallar yaratadigan, turli maqsadlardagi hayotni ta'minlash tizimlari va vositalari.

Очиқ ахборотни шакллантириш, узатиш, қабул қилиш, ўзгартириш, акс эттириш ва сақлаш воситалари ҳамда тизимлари, ахборот чиқиб кетиши мумкин бўлган техник каналлар яратадиган, турли мақсадлардаги ҳаётни таъминлаш тизимлари ва воситалари.

**Средства технические
основные**

uz - asosiy texnik vositalar
асосий техник воситалар
en - general technical facilities

Средства и системы формирования, передачи, приема, преобразования, отображения и хранения информации с ограниченным доступом.

Erkin foydalanilishi cheklangan axborotni shakllan-

С

tirish, uzatish, qabul qilish, o'zgartirish, aks ettirish va saqlash vositalari hamda tizimlari.

Эркин фойдаланилиши чекланган ахборотни шакллантириш, узатиш, қабул қилиш, ўзгартириш, акс эттириш ва сақлаш воситалари ҳамда тизимлари.

Средства технической защиты информации

uz - axborotni texnik muhofaza qilish vositalari

ахборотни техник муҳофаза қилиш воситалари

en - facilities of technical protection of information

Аппаратные, программные или аппаратно-программные средства, обеспечивающие техническую защиту информации на стадиях ее формирования, передачи, приема, преобразования, отображения и хранения.

Axborotni shakllantirish, uzatish, qabul qilish, o'zgartirish, aks ettirish va saqlash bosqichlarida texnik muhofaza qilinishini ta'minlaydigan apparat, dasturiy yoki apparat-dasturiy vositalar.

Ахборотни шакллантириш, узатиш, қабул қилиш, ўзгартириш, акс эттириш ва сақлаш босқичларида техник муҳофаза қилинишини таъминлайдиган аппарат, дастурий ёки аппарат-дастурий воситалар.

Средства управления

uz - boshqarish vositalari

бошқариш воситалари

en - controls

Мера, применяя которую, модифицируют риск.

Примечания

1 К средствам управления относятся любые процессы, политики, устройства, процедуры или иные действия, направленные на модификацию риска.

2 Средства управления не всегда могут выполнять предполагаемую или допускаемую модификацию.

Riskni modifikatsiya qilishda qo'llaniladigan o'lchov.

Izohlar

1 Boshqarish vositalariga har qanday jarayonlar, siyosatlar, qurilmalar, protseduralar yoki riskni modifikatsiya qilishga yo'naltirilgan boshqa ishlar kiradi.

2 Boshqarish vositalari taxmin qilinadigan yoki yo'l qo'yiladigan modifikatsiyani har doim ham bajara olmaydi.

Рискни модификация қилишда қўлланиладиган ўлчов.

Изоҳлар

1 Бошқариш воситаларига ҳар қандай жараёнлар, сиёсатлар, қурилмалар, процедуралар ёки рискни модифи-

С

Средства управления доступом uz - erkin foydalanishni boshqarish vositalari эркин фойдаланишни бошқариш воситалари en - access control facilities	кация қилишга йўналтирилган бошқа ишлар киради. 2 Бошқариш воситалари тахмин қилинадиган ёки йўл қўйиладиган модификацияни ҳар доим ҳам бажара олмайди. Средства, предотвращающие случайный или преднамеренный доступ к данным.
Средства управления конфигурацией инструментальные uz - instrumental konfiguratsiyani boshqarish vositalari инструментал конфигурацияни бошқариш воситалари en - configuration management tools	Ма'lumotlardan tasodifan yoki qasddan foydalana olishni bartaraf etuvchi vositalar. Маълумотлардан тасодифан ёки қасддан фойдалана олишни бартараф этувчи воситалар. Инструментальные средства с ручным управлением или автоматизированные инструментальные средства, реализующие или поддерживающие систему управления конфигурацией.
Средства шифрования uz - shifrlash vositalari шифрлаш воситалари en - facilities of cryptooperation	Qo'lda boshqariladigan instrumental vositalar yoki konfiguratsiyani boshqarish tizimini qo'llab-quvvatlaydigan yoki amalga oshiradigan, avtomatlashtirilgan instrumental vositalar. Қўлда бошқариладиган инструментал воситалар ёки конфигурацияни бошқариш тизимини қўллаб-қувватлайдиган ёки амалга оширадиган, автоматлаштирилган инструментал воситалар. Аппаратные, программные или аппаратно-программные средства, реализующие криптографические алгоритмы преобразования информации и предназначенные для защиты информации от несанкционированного доступа при ее обработке, хранении и передаче по каналам связи.
	Axborotni almashtirish kriptografik algoritmlarini amalga oshiruvchi va axborotni qayta ishlash, saqlash hamda aloqa kanallari bo'ylab uzatishda uni ruxsatsiz foydalana olishdan muhofaza qilish uchun mo'ljallangan apparat, dasturiy yoki apparat-dasturiy vositalar. Ахборотни алмаштириш криптографик алгоритмларини амалга оширувчи ва ахборотни қайта ишлаш, сақлаш ҳамда алоқа каналлари бўйлаб узатишда уни рухсатсиз фойдалана олишдан муҳо-

С

фаза қилиш учун мўлжалланган аппарат, дастурий ёки аппарат-дастурий воситалар.

Средства электронной цифровой подписи

uz - elektron raqamli imzo vositalari

электрон рақамли имзо воситалари

en - facilities of electronic digital signature

Совокупность технических и программных средств, обеспечивающих создание электронной цифровой подписи в электронном документе, подтверждение подлинности электронной цифровой подписи, создание открытых и закрытых ключей электронной цифровой подписи.

Elektron hujjatda elektron raqamli imzo yaratilishi, elektron raqamli imzo haqiqiylikining tasdiqlanishi, elektron raqamli imzo ochiq va yopiq kalitlarining yaratilishini ta'minlovchi texnik va dasturiy vositalar jami.

Электрон ҳужжатда электрон рақамли имзо яратилиши, электрон рақамли имзо ҳақиқийлигининг тасдиқланиши, электрон рақамли имзо очик ва ёпик калитларининг яратилишини таъминловчи техник ва дастурий воситалар жами.

Средство вычислительной техники

uz - hisoblash texnikasi vositasi

ҳисоблаш техникаси воситаси

en - computer facilities

1 Техническое средство обработки информации, в котором информация представлена в цифровом коде.

Примечание – К средствам вычислительной техники относятся процессоры, каналы селективные и мультиплексные, внешние запоминающие устройства, устройства ввода и вывода данных, устройства непосредственной связи оператора с ЭВМ, устройства систем телеобработки данных, устройства повышения достоверности и т.д.

2 Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

1 Axborot raqamli kodda taqdim etilgan, axborotni qayta ishlash texnik vositasi.

Izoh – Protsessorlar, selektiv hamda multipleks kanallar, tashqi xotirlovchi qurilmalar, ma'lumotlarni kiritish va

С

chiqarish qurilmalari, operatorning elektron hisoblash mashinasi bilan bevosita bog'lanish qurilmalari, ma'lumotlarni teleqayta ishlash tizimlarining qurilmalari, ishonchlikni oshirish qurilmalari va boshqa qurilmalar hisoblash texnikasi vositalariga tegishlidir.

2 Mustaqil ravishda yoki boshqa tizimlar tarkibida ishlay oladigan ma'lumotlarni qayta ishlash tizimlari dasturiy va texnik elementlarining jami.

1 Ахборот рақамли кодда тақдим этилган, ахборотни қайта ишлаш техник воситаси.

Изоҳ – Процессорлар, селектив ҳамда мультимплекс каналлар, ташқи хотирловчи қурилмалар, маълумотларни киритиш ва чиқариш қурилмалари, операторнинг электрон ҳисоблаш машинаси билан бевосита боғланиш қурилмалари, маълумотларни телеқайта ишлаш тизимларининг қурилмалари, ишонччиликни ошириш қурилмалари ва бошқа қурилмалар ҳисоблаш техникаси воситаларига тегишлидир.

2 Мустақил равишда ёки бошқа тизимлар таркибида ишлай оладиган маълумотларни қайта ишлаш тизимлари дастурий ва техник элементларининг жами.

Средство вычислительной техники защищенное

uz - muhofazalangan hisoblash texnikasi vositasi

муҳофазаланган
ҳисоблаш техникаси воситаси

en - protected computer facilities

Средство защиты

uz - muhofaza qilish vositasi

муҳофаза қилиш воситаси
en - protection facilities

Средство вычислительной техники, в котором реализован комплекс средств защиты.

Muhofaza qilish vositalarining kompleksi amalga oshirilgan hisoblash texnikasi vositasi.

Муҳофаза қилиш воситаларининг комплекси амалга оширилган ҳисоблаш техникаси воситаси.

Функциональный блок, используемый в качестве фильтра безопасности между двумя системами обработки данных, имеющими разные уровни безопасности, или между терминалом пользователя и базой данных, и предназначенный для отфильтровывания данных, для доступа к которым у пользователя отсутствуют полномочия.

Turli xavfsizlik darajasiga ega bo'lgan ikkita ma'lumotni qayta ishlash tizimi o'rtasida yoki foydala-

С

nuvchi terminali va ma'lumotlar bazasi o'rtasida himoya filtri sifatida foydalaniladigan hamda foydalanuvchida ulardan erkin foydalanish vakolati bo'lmagan ma'lumotlarni saralash uchun mo'ljallangan funksional blok.

Турли хавфсизлик даражасига эга бўлган иккита маълумотни қайта ишлаш тизими ўртасида ёки фойдаланувчи терминали ва маълумотлар базаси ўртасида ҳимоя филтри сифатида фойдаланиладиган ҳамда фойдаланувчида улардан эркин фойдаланиш ваколоти бўлмаган маълумотларни саралаш учун мўлжалланган функционал блок.

Средство защиты информации

uz - axborotni muhofaza qilish vositasi

ахборотни муҳофаза қилиш воситаси
en - information security products

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Axborotni muhofaza qilish samaradorligini nazorat qilish uchun mo'ljallangan yoki ishlatiladigan texnik, dasturiy vosita, buyum va/yoki material.

Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш учун мўлжалланган ёки ишлатиладиган техник, дастурий восита, буюм ва/ёки материал.

Средство защиты информации активное

uz - aktiv axborotni muhofaza qilish vositasi

актив ахборотни муҳофаза қилиш воситаси
en - active information security product

Средство, обеспечивающее создание активных помех, исключаящих или существенно снижающих возможность использования канала утечки информации.

Axborot chiqib ketishi mumkin bo'lgan kanaldan foydalanish imkoniyatini yo'qqa chiqaradigan yoki jiddiy ravishda kamaytiruvchi aktiv xalqlar vujudga keltirilishini ta'minlaydigan vosita.

Ахборот чиқиб кетиши мумкин бўлган каналдан фойдаланиш имкониятини йўққа чиқарадиган ёки жиддий равишда камайтирувчи актив халакитлар вужудга келтирилишини таъминлайдиган восита.

Средство защиты информации аппаратное

1 Механические, электромеханические, электронные, оптические, лазерные, радио, радиотехниче-

С

uz - axborotni muhofaza qilish apparat vositasi
ахборотни муҳофаза қилиш аппарат воситаси
en - information security hardware

ские, и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи, модификации или разрушения.

2 Специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

1 Axborotni ruxsat etilmagan tarzda foydalanish, nusxa ko‘chirish, o‘g‘irlash, o‘zgartirish yoki buzishdan muhofaza qilish uchun mo‘ljallangan, mexanik, elektromexanik, elektron, optik, lazer, radio, radio-texnik va boshqa qurilmalar, tizimlar va inshootlar.

2 Maxsus himoya qurilmasi yoki axborotni qayta ishlash texnik vositasining komplektiga kiruvchi moslama.

1 Ахборотни рухсат этилмаган тарзда фойдаланиш, нусха кўчириш, ўғирлаш, ўзгартириш ёки бузишдан муҳофаза қилиш учун мўлжалланган, механик, электромеханик, электрон, оптик, лазер, радио, радиотехник ва бошқа қурилмалар, тизимлар ва иншоотлар.

2 Махсус ҳимоя қурилмаси ёки ахборотни қайта ишлаш техник воситасининг комплектига кирувчи мослама.

Средство защиты информации программное

uz - axborotni muhofaza qilish dasturiy vositasi
ахборотни муҳофаза қилиш дастурий воситаси
en - information security software

Специальная программа, входящая в комплект программного обеспечения и предназначенная для защиты информации.

Dasturiy ta’minot komplektiga kiruvchi va axborotni muhofaza qilish uchun mo‘ljallangan maxsus dastur.

Дастурий таъминот комплектига кирувчи ва ахборотни муҳофаза қилиш учун мўлжалланган махсус дастур.

Средство защиты информации техническое

uz - axborotni muhofaza qilish texnik vositasi
ахборотни муҳофаза қилиш техник воситаси

1 Техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средствам доступа информации.

2 Специальные средства (устройства), предна-

С

en - technical information security equipment

значенные для предотвращения противоправных действий с информацией и/или обеспечения охраны (физической защиты) объекта защиты.

1 Obyektning demaskirovkalovchi alomatlarini bartaraf qilish yoki susaytirish, soxta (imitatsiyalovchi) alomatlarni, shuningdek, axborotdan erkin foydalanish texnik vositalariga xalaqitlar vujudga keltirish uchun mo'ljallangan texnik vosita.

2 Axborot bilan bog'liq bo'lgan qonunga xilof ishlarining oldini olish va/yoki muhofaza obyektining qo'riqlanishini (jismoniy himoya qilinishini) ta'minlash uchun mo'ljallangan maxsus vositalar (qurilmalar).

1 Объектнинг демаскировкаловчи аломатларини бартараф қилиш ёки сусайтириш, сохта (имитацияловчи) аломатларни, шунингдек, ахборотдан эркин фойдаланиш техник воситаларига халақитлар вужудга келтириш учун мўлжалланган техник восита.

2 Ахборот билан боғлиқ бўлган қонунга хилоф ишларнинг олдини олиш ва/ёки муҳофаза объектнинг қўриқланишини (жисмоний химоя қилинишини) таъминлаш учун мўлжалланган махсус воситалар (қурилмалар).

Средство контроля эффективности защиты информации

uz - axborotni muhofaza qilish samaradorligini nazorat qilish vositasi

ахборотни муҳофаза қилиш самарадорлигини назорат қилиш воситаси

en - information security efficiency control facility

Техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

Axborotni muhofaza qilish samaradorligini nazorat qilish uchun mo'ljallangan yoki foydalaniladigan texnik, dasturiy vosita, modda va/yoki material.

Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш учун мўлжалланган ёки фойдаланиладиган техник, дастурий восита, модда ва/ёки материал.

Средство криптографической защиты информации

Аппаратное, программное или аппаратно-программное средство, осуществляющее криптографическое преобразование информации для обес-

С

uz - axborotni kriptografik muhofaza qilish vositasi

ахборотни криптографик муҳофаза қилиш воситаси

en - cryptographic information protection facility

Средство обработки информации техническое
uz - axborotni qayta ishlash texnik vositasi

ахборотни қайта ишлаш техник воситаси

en - information processing hardware

печения ее безопасности.

Axborot xavfsizligini ta'minlash maqsadida, axborotning kriptografik o'zgartirilishini amalga oshiruvchi apparat, dasturiy yoki apparat-dasturiy vosita.

Ахборот хавфсизлигини таъминлаш мақсадида, ахборотнинг криптографик ўзгартирилишини амалга оширувчи аппарат, дастурий ёки аппарат-дастурий восита.

Техническое средство, предназначенное для приема, хранения, поиска, преобразования, отображения и/или передачи информации по каналам телекоммуникаций.

Примечание – К техническим средствам обработки информации относятся средства вычислительной техники, средства и системы телекоммуникаций, средства записи, усиления и воспроизведения звука, переговорные и телевизионные устройства, средства изготовления и размножения документов, кинопроекторная аппаратура и другие технические средства, связанные с приемом, накоплением, хранением, поиском, преобразованием, отображением и/или передачей информации по каналам телекоммуникаций.

Telekommunikatsiya kanallari orqali axborotni qabul qilish, saqlash, izlash, o'zgartirish, aks ettirish va/yoki uzatish uchun mo'ljallangan texnik vosita.

Izoh – Axborotni qayta ishlash texnik vositalariga hisoblash texnikasi vositalari, telekommunikatsiyalar tizimlari va vositalari, ovoz yozish, kuchaytirish va qayta eshittirish vositalari, so'zlashuv va televizion qurilmalar, hujjatlar tayyorlash va ko'paytirish vositalari, kinoprojektsion apparatura hamda telekommunikatsiyalar kanallari orqali axborot qabul qilish, to'plash, saqlash, izlash, o'zgartirish, aks ettirish va/yoki uzatish bilan bog'liq bo'lgan boshqa texnik vositalar kiradi.

Телекоммуникация каналлари орқали ахборотни қабул қилиш, сақлаш, излаш, ўзгартириш, акс эттириш ва/ёки узатиш учун мўлжалланган техник восита.

Изоҳ – Ахборотни қайта ишлаш техник воситаларига ҳисоблаш техникаси воситалари, телекоммуникациялар тизимлари ва воситалари, овоз ёзиш, кучайтириш ва қайта эшиттириш воситалари, сўзлашув ва телевизион

С

курулмалар, хужжатлар тайёрлаш ва кўпайтириш воситалари, кинопроектцион аппаратура ҳамда телекоммуникациялар каналлари орқали ахборот қабул қилиш, тўплаш, сақлаш, излаш, ўзгартириш, акс эттириш ва/ёки узатиш билан боғлиқ бўлган бошқа техник воситалар қиради.

Средство разграничения доступа

uz - erkin foydalanishni chegaralash vositasi

эркин фойдаланишни чегаралаш воситаси

en - access isolation facility

Программно-аппаратное средство, обеспечивающее разграничение доступа субъектов к информационным ресурсам в соответствии с принятой моделью.

Примечание – Средствами разграничения доступа являются матрица доступа и метка секретности (конфиденциальности).

Qabul qilingan modelga muvofiq, subyektlarning axborot resurslaridan erkin foydalanishi chegaralanishini ta'minlovchi dasturiy-apparat vosita.

Izoh – Foydalanish matritsasi va maxfiylik (konfidensiallik) belgisi erkin foydalanishni chegaralash vositalari hisoblanadi.

Қабул қилинган моделга мувофиқ, субъектларнинг ахборот ресурсларидан эркин фойдаланиши чегараланишини таъминловчи дастурий-аппарат восита.

Изоҳ – Фойдаланиш матрицаси ва махфийлик (конфиденциаллик) белгиси эркин фойдаланишни чегаралаш воситалари ҳисобланади.

Средство шифровальное

uz - shifrllovchi vosita

шифрловчи восита

en - encryption facility

1 Реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам телекоммуникаций, включая шифровальную технику.

2 Аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации.

3 Аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты

С

от навязывания ложной информации, включая средства имитозащиты и электронной подписи, реализующие криптографические алгоритмы преобразования информации.

1 Axborotni o'zgartirishning kriptografik algoritmlarini amalga oshiradigan apparat, dasturiy, apparat-dasturiy vositalar, texnik vositalarda aylanadigan axborotni, uni qayta ishlash, saqlash va telekommunikatsiyalar kanallari orqali uzatish paytida muhofaza qilish uchun mo'ljallangan tizim hamda komplekslar, jumladan, shifrlash texnikasi.

2 Kalitli axborotni tashuvchining turidan qat'i nazar, shifrlash vositalarida foydalaniladigan kalitli hujjatlarni tayyorlash va tarqatish uchun mo'ljallangan apparat, dasturiy, apparat-dasturiy vositalar, tizim va komplekslar.

3 Soxta axborotni majburan kiritilishidan (qabul qilinishidan) muhofaza qilishning apparat, dasturiy va apparat-dasturiy vositalari, tizimlari va komplekslari, jumladan axborotni o'zgartirishning kriptografik algoritmlarini amalga oshiruvchi, imitomuhofaza va elektron imzo vositalari.

1 Ахборотни ўзгартиришнинг криптографик алгоритмларини амалга оширадиган аппарат, дастурий, аппарат-дастурий воситалар, техник воситаларда айланадиган ахборотни, уни қайта ишлаш, сақлаш ва телекоммуникациялар каналлари орқали узатиш пайтида муҳофаза қилиш учун мўлжалланган тизим ҳамда комплекслар, жумладан, шифрлаш техникаси.

2 Калитли ахборотни ташувчининг туридан қатъи назар, шифрлаш воситаларида фойдаланиладиган калитли ҳужжатларни тайёрлаш ва тарқатиш учун мўлжалланган аппарат, дастурий, аппарат-дастурий воситалар, тизим ва комплекслар.

3 Сохта ахборотни мажбуран киритилишидан (қабул қилинишидан) муҳофаза қилишнинг аппарат, дастурий ва аппарат-дастурий воситалари, тизимлари ва комплекслари, жумладан ахборотни ўзгартиришнинг криптографик алгоритмларини амалга оширувчи, имитомуҳофаза ва электрон имзо воситалари.

С

Стандарт в области обеспечения безопасности

uz - xavfsizlikni ta'minlash sohasidagi standart
хавфсизликни таъминлаш соҳасидаги стандарт
en - security implementation standard

Стеганография

uz - steganografiya
стеганография
en - steganography

Стеганография компьютерная

uz - kompyuter steganografiyasi
компьютер стеганографияси
en - computer stenography

Стегоканал

uz - stegokanal
стегоканал
en - stegochannel

Стегоключ

uz - stegokalit
стегокалит
en - stegokey

Стегоконтейнер

uz - stegokonteyner
стегоконтейнер

Официально принятый документ, устанавливающий методы обеспечения безопасности.

Xavfsizlikni ta'minlash usullarini belgilab beradigan rasmiy qabul qilingan hujjat.

Хавфсизликни таъминлаш усуллари белгилаб берадиган расмий қабул қилинган ҳужжат.

Отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.

Ochiq axborot massivlarida konfidensial axborotni yashirishning matematik metodlarini o'rganuvchi fan sohasi.

Очиқ ахборот массивларида конфиденциал ахборотни яширишнинг математик методларини ўрганувчи фан соҳаси.

Сокрытие сообщения или файла в другом сообщении или файле.

Xabar yoki faylni boshqa xabar yoki faylda yashirish.

Хабар ёки файлни бошқа хабар ёки файлда яшириш.

Канал скрытой передачи информации.

Axborotni yashirin uzatish kanali.

Ахборотни яширин узатиш канали.

Секретный ключ, необходимый для сокрытия (шифрования) информации.

Axborotni yashirish (shiflash) uchun zarur bo'ladigan maxfiy kalit.

Ахборотни яшириш (шифрлаш) учун зарур бўладиган махфий калит.

Контейнер, содержащий встроенное сообщение.

Kiritilgan xabar bo'lgan konteyner.

С

en - stegocontainer

Стойкость

криптографическая

uz - kriptografik bardoshlilik

криптографик

бардошлилик

en - cryptoresistability

Кирилган хабар бўлган контейнер.

Способность криптосистемы противостоять попыткам криптоаналитика дешифровать шифротекст, раскрыть ключи шифра или нарушить целостность и/или подлинность информации.

Kriptotizimning, kriptoolitikning shifratni deshifrlash, shifr kalitini ochish yoki axborot yaxlitligini va/yoki haqiqiylikini buzishga boʻlgan urinishlariga qarshi tura olish qobiliyati.

Криптотизимнинг, криптоаналитикнинг шифратни дешифрлаш, шифр калитини очиш ёки ахборот яхлитлигини ва/ёки ҳақиқийлигини бузишга бўлган уринишларига қарши тура олиш қобилияти.

Сторона заинтересованная

uz - manfaatdor tomon

манфаатдор томон

en - interested party,

stakeholder

Физическое лицо или организация, которые могут воздействовать, подвергаться воздействию или осознавать, что на них влияет какое-либо решение или деятельность.

Taʼsir etishi, taʼsirga uchrashi mumkin boʻlgan yoki qandaydir qaror yoki faoliyat taʼsir etayotganini his etishi mumkin boʻlgan jismoniy shaxs yoki tashkilot.

Таъсир этиши, таъсирга учраши мумкин бўлган ёки қандайдир қарор ёки фаолият таъсир этаётганини ҳис этиши мумкин бўлган жисмоний шахс ёки ташкилот.

Стратегия защиты

uz - muhofaza qilish

strategiyasi

муҳофаза қилиш

стратегияси

en - protection strategy

Формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Tizimning maʼlum tahdidlardan muhofaza qilinishini taʼminlashda amal qilinishi kerak boʻlgan kriteriyalarni, ayniqsa, operativ kriteriyalarni rasmiy aniqlash.

Тизимнинг маълум таҳдидлардан муҳофаза қилинишини таъминлашда амал қилиниши керак бўлган критерийларни, айниқса, оператив критерийларни расмий аниқлаш.

Субключ

uz - subkalit

Ключ, который включается в состав главного ключа и который можно в любой момент аннулировать.

С

субкалит
en - subkey

вать без последствий для главного ключа.

Asosiy kalit tarkibiga kiritiladigan va istalgan vaqtda asosiy kalit uchun salbiy oqibatlarisiz bekor qilinishi mumkin bo'lgan kalit.

Асосий калит таркибига киритиладиган ва исталган вақтда асосий калит учун салбий оқибатларсиз бекор қилиниши мумкин бўлган калит.

Субъект
uz - subyekt
субъект
en - subject

1 Активный логический объект, имеющий доступ к объектам. Например, процесс, который запускает выполнение программы.

Примечание – Субъект может быть причиной потока информации между объектами или изменения состояния системы обработки данных.

2 Активный компонент системы, обычно представленный в виде пользователя, процесса или устройства, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы. Обычно субъект представляется парой процесс – домен.

1 Obyektlardan foydalana olish imkoniyati bo'lgan mantiqiy aktiv obyekt. Masalan, dastur bajari-lishini ishga tushiradigan jarayon.

Izoh – Subyekt obyektlar o'rtasidagi axborot oqimining yoki ma'lumotlarni qayta ishlash tizimi holati o'zgarishi-ning sababchisi bo'lishi mumkin.

2 Odatda, foydalanuvchi, jarayon yoki qurilma ko'rinishida taqdim etilgan tizimning aktiv komponenti, u obyektдан obyektga boradigan axborot oqimi yoki tizim holati o'zgarishining sababchisi bo'lishi mumkin. Odatda, subyekt jarayon – do- men jufti tarzida taqdim etiladi.

1 Объектлардан фойдалана олиш имконияти бўлган мантиқий актив объект. Масалан, дастур бажарилишини ишга туширадиган жараён.

Изоҳ – Субъект объектлар ўртасидаги ахборот оқими- нинг ёки маълумотларни қайта ишлаш тизими ҳолати ўзгаришининг сабабчиси бўлиши мумкин.

2 Одатда, фойдаланувчи, жараён ёки қурилма кўринишида тақдим этилган тизимнинг актив компоненти, у объектдан объектга борадиган ах- борот оқими ёки тизим ҳолати ўзгаришининг

С

Субъект безопасности

uz - xavfsizlik subyekti

хавфсизлик субъекти

en - security subject

Субъект доступа

uz - erkin foydalanish

subyekti

эркин фойдаланиш субъекти

en - access subject

Субъект доступа

авторизованный

uz - mualliflashtirilgan

erkin foydalanish subyekti

муаллифлаштирилган эркин фойдаланиш субъекти

en - authorized access subject

Субъекты информационных отношений

uz - axborot munosabatlarining

subyektlari

сабабчиси бўлиши мумкин. Одатда, субъект жараён – домен жуфти тарзида тақдим этилади.

Активная системная составляющая, к которой применяется политика безопасности.

Xavfsizlik siyosati tatbiq qilinadigan aktiv tizim tashkil etuvchisi.

Хавфсизлик сиёсати татбиқ қилинадиган актив тизим ташкил этувчиси.

1 Лицо или процесс, действия которых регламентируются правилами разграничения доступа.

2 Лицо или процесс, осуществляющие доступ к информационному ресурсу с использованием штатных технических средств.

1 Harakatlari foydalana olishni chegaralash qoidalarini bilan qat'iy tartibga solinadigan shaxs yoki jarayon.

2 Shtat texnik vositalar yordamida, axborot resursidan erkin foydalanishni amalga oshiruvchi shaxs yoki jarayon.

1 Ҳаракатлари фойдалана олишни чегаралаш қоидалари билан қатъий тартибга солинадиган шахс ёки жараён.

2 Штат техник воситалар ёрдамида, ахборот ресурсидан эркин фойдаланишни амалга оширувчи шахс ёки жараён.

Субъект, которому предоставлены соответствующие права доступа к объектам системы (полномочия).

Tizim obyektlaridan erkin foydalanish yuzasidan tegishli huquqlar (vakolatlar) taqdim etilgan subyekt.

Тизим объектларидан эркин фойдаланиш юзасидан тегишли ҳуқуқлар (ваколатлар) тақдим этилган субъект.

Государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические

С

ахборот муносабатлари-
нинг субъектлари
**en - parties of information
relationships**

лица) и иные субъекты, взаимодействующие с целью совместной обработки информации.

Примечание – По отношению к информации, обрабатываемой в информационной системе, различные субъекты – участники информационных отношений могут выступать (возможно, одновременно) в качестве:

- источников информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается и обрабатывается информация;
- владельцев информационной системы и участников процессов обработки и передачи информации и т.д.

Axborotni birgalikda qayta ishlash maqsadida o‘zaro hamkorlik qiluvchi davlat, davlat organlari, davlat, jamoat yoki tijorat tashkilotlari (birlashmalari) va korxonalar (yuridik shaxslar), ayrim fuqarolar (jismoniy shaxslar) va boshqa subyektlar.

Izoh – Axborot tizimida qayta ishlanadigan axborotga nisbatan, turli subyektlar – axborot munosabatlari ishtirokchilari sifatida chiqishlari (balki, bir vaqtda) mumkin:

- axborot manbalari;
- axborot foydalanuvchilari (iste’molchilari);
- axborot egalari;
- axborot to‘planadigan va qayta ishlanadigan jismoniy va yuridik shaxslar;
- axborot tizimi egalari va axborotni qayta ishlash va uzatish jarayonlarining ishtirokchilari va h.k.

Axborotni birgalikda qayta ishlash maqsadida o‘zaro hamkorlik qiluvchi davlat, davlat organlari, davlat, jamoat yoki tijorat tashkilotlari (birlashmalari) va korxonalar (yuridik shaxslar), ayrim fuqarolar (jismoniy shaxslar) va boshqa subyektlar.

Izoh – Axborot tizimida qayta ishlanadigan axborotga nisbatan, turli subyektlar – axborot munosabatlari ishtirokchilari sifatida chiqishlari (balki, bir vaqtda) mumkin:

- axborot manbalari;
- axborot foydalanuvchilari (iste’molchilari);
- axborot egalari;
- axborot to‘planadigan va qayta ishlanadigan jismoniy va yuridik shaxslar;
- axborot tizimi egalari va axborotni qayta ishlash va uzatish jarayonlarining ishtirokchilari va h.k.

С

Сумма контрольная

uz - nazorat summasi

назорат суммаси

en - checking sum

узатиш жараёнларининг иштирокчилари ва ҳ.к.

1 Информация, предназначенная для проверки правильности записи данных путем подсчета суммы байтов и добавления ее к записи. При считывании данных сумма байтов должна совпасть с контрольной суммой.

2 Некоторая функция, сопоставляемая блоку данных для целей проверки, обычно формируется в виде суммы соответствующих полей всех записей файла. Это число не имеет какого-то особого смысла, а служит только для проверки записей файла. Всякое изменение значения поля обнаруживается из-за несовпадения зарегистрированной ранее и вновь вычисленной контрольных сумм.

1 Baytlar summasini hisoblash va uni yozuvga qo‘shish yo‘li bilan ma‘lumotlar yozuvining to‘g‘riligini tekshirish uchun mo‘ljallangan axborot. Ma‘lumotlarni hisoblashda baytlar summasi nazorat summasi bilan mos kelishi kerak.

2 Ma‘lumotlar blokiga tekshirish maqsadlarida solishtiriladigan qandaydir funksiya, odatda faylning barcha yozuvlari maydonlariga mos keluvchi summa ko‘rinishida shakllanadi. Bu son biror-bir muhim ma‘noga ega emas, faqat fayl yozuvlarini tekshirish uchun xizmat qiladi. Maydon qiymatining har qanday o‘zgarishi oldindan qayd qilingan va qaytadan hisoblangan nazorat summalarining mos kelmasligidan aniqlanadi.

1 Байтлар суммасини ҳисоблаш ва уни ёзувга қўшиш йўли билан маълумотлар ёзувининг тўғрилигини текшириш учун мўлжалланган ахборот. Маълумотларни ҳисоблашда байтлар суммаси назорат суммаси билан мос келиши керак.

2 Маълумотлар блокига текшириш мақсадларида солиштириладиган қандайдир функция, одатда файлнинг барча ёзувлари майдонларига мос келувчи сумма кўринишида шаклланади. Бу сон бирор-бир муҳим маънога эга эмас, фақат файл ёзувларини текшириш учун хизмат қилади. Май-

С

дон қийматининг ҳар қандай ўзгариши олдиндан қайд қилинган ва қайтадан ҳисобланган назорат суммаларининг мос келмаслигидан аниқланади.

Суперсектор

uz - supersektor
суперсектор
en - supersector

Часть метода защиты от копирования, когда на диск записывается сектор с размерами больше обычного.

Nusxa ko'chirishdan muhofaza qilish metodining qismi. Diskka odatdagidan katta o'lchamlardagi sektor yozilganda qo'llaniladi.

Нусха кўчиришдан муҳофаза қилиш методининг қисми. Дискка одатдагидан катта ўлчамлардаги сектор ёзилганда қўлланилади.

Схема концептуальная

uz - konseptual sxema
концептуал схема
en - conceptual scheme

Описание возможных состояний связей в предметной области, включая классификации, правила, законы и т.п., действующие между объектами в пределах предметной области.

Predmet sohasi doirasida obyektlar o'rtasida amal qiluvchi klassifikatsiyalar, qonunlar va sh.k. o'z ichiga olgan holda, predmet sohasidagi aloqalar mumkin bo'lgan holatlarining tavsifi.

Предмет соҳаси доирасида объектлар ўртасида амал қилувчи классификациялар, қонунлар ва ш.к. ўз ичига олган ҳолда, предмет соҳасидаги алоқалар мумкин бўлган ҳолатларининг тавсифи.

Схема предварительного распределения ключей

uz - kalitlarni oldindan
taksimlash sxemasi
калитларни олдиндан
таксимлаш схемаси
en - preliminary key distribution
scheme

Совокупность алгоритма распределения исходной ключевой информации и алгоритма формирования ключей.

Boshlang'ich kalit axborotni taqsimlash va kalitlarni shakllantirish algoritmlarining jami.

Бошланғич калит ахборотни тақсимлаш ва калитларни шакллантириш алгоритмларининг жами.

Схема цифровой подписи

uz - raqamli imzo sxemasi
рақамли имзо схемаси
en - digital signature scheme

Совокупность алгоритма формирования цифровой подписи и алгоритма ее проверки.

Raqamli imzoni shakllantirish va uni tekshirish algoritmlarining jami.

С

Сцепление (модулей)

uz - bog‘lanish

(modullarning bog‘lanishi)

боғланиш

(модуларнинг боғланиши)

en - coupling

Рақамли имзони шакллантириш ва уни текшириш алгоритмларининг жами.

Способ и степень взаимозависимости программных модулей.

Примечание – Существуют различные виды сцепления модулей: по вызову, по общей области и по содержанию.

Dasturiy modullar o‘zaro bog‘liqligining usul va darajasi.

Izoh – Modullar bog‘lanishining turli xil ko‘rinishi mavjud: chaqiruv bo‘yicha, umumiy soha bo‘yicha va mazmun bo‘yicha.

Дастурий модулар ўзаро боғлиқлигининг усул ва даражаси.

Изоҳ – Модулар боғланишининг турли хил кўриниши мавжуд: чакирув бўйича, умумий соҳа бўйича ва мазмун бўйича.

Сцепление

криптографическое

uz - kriptografik ilashish

криптографик илашиш

en - cryptographic chaining

Режим использования криптографического алгоритма, при котором преобразование осуществляется алгоритмом, который зависит от значений предыдущих входных или выходных данных.

Kriptografik algoritmdan foydalanish rejimi, bunda o‘zgartirish oldingi kirish yoki chiqish ma’lumotlari qiymatlariga bog‘liq bo‘lgan algoritm tomonidan amalga oshiriladi.

Криптографик алгоритмдан фойдаланиш режими, бунда ўзгартириш олдинги кириш ёки чиқиш маълумотлари қийматларига боғлиқ бўлган алгоритм томонидан амалга оширилади.

Сцепление по вызову

uz - chaqiruv bo‘yicha

bog‘lanish

чакирув бўйича

боғланиш

en - call coupling

Взаимосвязь между двумя модулями, строго взаимодействующими через вызовы их документированных функций.

Примечание – Примерами сцепления по вызову являются сцепление по данным, сцепление по образцу и сцепление по управлению.

Hujjatlashtirilgan funksiyalarini chaqirish orqali qat’iy birgalikda ishlaydigan ikkita modul o‘rtasidagi o‘zaro bog‘lanish.

Izoh – Chaqiruv bo‘yicha bog‘lanishga ma’lumotlar bo‘yicha bog‘lanish, namunalar bo‘yicha bog‘lanish va boshqarish bo‘yicha bog‘lanishlar misol bo‘ladi.

Хужжатлаштирилган функцияларини чакириш

С

орқали қатъий биргаликда ишлайдиган иккита модуль ўртасидаги ўзаро боғланиш.

Изоҳ – Чақирув бўйича боғланишга маълумотлар бўйича боғланиш, намуналар бўйича боғланиш ва бошқариш бўйича боғланишлар мисол бўлади.

Сцепление по данным

uz - ma'lumotlar bo'yicha bog'lanish

маълумотлар бўйича боғланиш

en - call coupling data

Взаимосвязь между двумя модулями, строго взаимодействующими через вызовы параметров, которые представляют собой отдельные элементы данных.

Ma'lumotlarning ayrim elementlarini o'zida ifodalaydigan parametrlarni chaqirish orqali qat'iy birgalikda ishlaydigan ikkita modul o'rtasidagi o'zaro bog'lanish.

Маълумотларнинг айрим элементларини ўзида ифодаладиган параметрларни чақириш орқали қатъий биргаликда ишлайдиган иккита модуль ўртасидаги ўзаро боғланиш.

Сцепление по образцу

uz - namuna bo'yicha bog'lanish

намуна бўйича боғланиш

en - call coupling stamp

Взаимосвязь между двумя модулями, строго взаимодействующими через вызовы параметров, которые содержат составные поля или которые имеют значительную внутреннюю структуру.

Tarkibiy maydonlarga yoki zarur ichki strukturaga ega bo'lgan parametrlarni chaqirish orqali qat'iy birgalikda ishlaydigan ikkita modul o'rtasidagi o'zaro bog'lanish.

Таркибий майдонларга ёки зарур ички структурага эга бўлган параметрларни чақириш орқали қатъий биргаликда ишлайдиган иккита модуль ўртасидаги ўзаро боғланиш.

Сцепление по общей области

uz - umumiy soha bo'yicha bog'lanish

умумий соҳа бўйича боғланиш

en - common coupling

Взаимосвязь между двумя модулями, использующими общую область данных или другой общий ресурс системы.

Примечание – Наличие глобальных переменных указывает на то, что использовавшие их модули сцеплены по общей области. Сцепление по общей области посредством глобальных переменных, как правило, допускается, но только в ограниченной степени.

Ma'lumotlarning umumiy sohasidan yoki boshqa tizimning umumiy resursidan foydalanadigan ikkita modul o'rtasidagi o'zaro bog'lanish.

Izoh – Global o'zgaruvchilarning mavjudligi, ulardan foydalanган modullar umumiy soha bo'yicha bog'langanligini

С

ko'rsatadi. Global o'zgaruvchilar vositasida umumiy soha bo'yicha bog'lanishga qoidaga ko'ra, faqat cheklangan darajada ruxsat beriladi.

Маълумотларнинг умумий соҳасидан ёки бошқа тизимнинг умумий ресурсидан фойдаланадиган иккита модуль ўртасидаги ўзаро боғланиш.

Изоҳ – Глобал ўзгарувчиларнинг мавжудлиги, улардан фойдаланган модуллар умумий соҳа бўйича боғланганлигини кўрсатади. Глобал ўзгарувчилар воситасида умумий соҳа бўйича боғланишга қоидага кўра, фақат чекланган даражада рўхсат берилади.

Сцепление по содержанию

uz - mazmun bo'yicha bog'lanish

мазмун бўйича боғланиш

en - content coupling

Взаимосвязь между двумя модулями, когда один модуль непосредственно обращается к внутренним элементам другого модуля.

Примечание – Примерами сцепления по содержанию являются модификация текста или обращение к внутренним меткам другого модуля.

Bir modul boshqa modulning ichki elementlariga bevosita murojaat qiladigan ikkita modul o'rtasidagi o'zaro bog'lanish.

Izoh – Mazmun bo'yicha bog'lanishga matnni o'zgartirish yoki boshqa modulning ichki belgilariga murojaat misol bo'la oladi.

Бир модуль бошқа модулнинг ички элементларига бевосита мурожаат қиладиган иккита модуль ўртасидаги ўзаро боғланиш.

Изоҳ – Мазмун бўйича боғланишга матнни ўзгартириш ёки бошқа модулнинг ички белгиларига мурожаат мисол бўла олади.

Сцепление по управлению

uz - boshqarish bo'yicha bog'lanish

бошқариш бўйича боғланиш

en - call coupling control

Взаимосвязь между двумя модулями, когда один из них передает информацию, которая влияет на внутреннюю логику другого.

Bir modul uzatgan axborot bir modulning ichki mantiqiga ta'sir qiladigan, ikkita modul o'rtasidagi o'zaro bog'lanish.

Бир модуль узатган ахборот бир модулнинг ички мантиғига таъсир қиладиган, иккита модуль ўртасидаги ўзаро боғланиш.

Счетчик команд

uz - komandalarni

Внутренний регистр процессора, содержащий адрес следующей выбираемой команды либо сле-

С

hisoblagich
командаларни
хисоблагич
en - program counter
control counter

дующего байта (слова) программы.

Protsessorning navbatdagi tanlanadigan komanda adresini yoki dasturning navbatdagi bayti (soʻzi)ni ichiga oladigan ichki registri.

Процессорнинг навбатдаги танланадиган команда адресини ёки дастурнинг навбатдаги байти (сўзи) ни ичига оладиган ички регистри.

Т

Тайна коммерческая
uz - tijorat siri
тижорат сирини
en - commercial confidentiality

Сведения конфиденциального характера из любой сферы деятельности государственного или частного предприятия, разглашение которых может нанести материальный или моральный ущерб ее владельцам или пользователям (юридическим лицам). Охрана коммерческой тайны осуществляется ее владельцем.

Davlat yoki xususiy korxonada faoliyatining istalgan sohasidagi konfidensial xarakterdagi ma'lumotlar, ularning tarqatilishi egalari yoki foydalanuvchilariga (yuridik shaxslarga) moddiy yoki ma'naviy zarar yetkazishi mumkin. Tijorat sirini saqlash uning egasi tomonidan amalga oshiriladi.

Давлат ёки хусусий корхона фаолиятининг исталган соҳасидаги конфиденциал характердаги маълумотлар, уларнинг тарқатилиши эгалари ёки фойдаланувчиларига (юримдик шахсларга) моддий ёки маънавий зарар етказиши мумкин. Тижорат сирини сақлаш унинг эгаси томонидан амалга оширилади.

Текст зашифрованный
uz - shifrlangan matn
шифрланган матн
en - ciphertext

Текст или иной вид сообщений, структура которого преобразована с использованием криптографических алгоритмов.

Strukturasi kriptografik algoritmlardan foydalanib oʻzgartirilgan matn yoki xabarlarining boshqa turi.

Структураси криптографик алгоритмлардан фойдаланиб ўзгартирилган матн ёки хабарларнинг бошқа тури.

Текст открытый
uz - ochiq matn

1 Данные, семантическое содержимое которых доступно без использования криптографических

T

Очиқ матн
en - plaintext

методов.

2 Исходное защищаемое сообщение.

3 Сообщение, поступающее на вход устройства шифрования или считываемое с выхода приемника после дешифрования.

1 Semantik tarkibini kriptografik metodlardan foydalanmasdan bilish mumkin bo'lgan ma'lumotlar.

2 Dastlabki muhofaza qilinadigan xabar.

3 Shifrlash qurilmasining kirishiga kelib tushadigan yoki shifrlashdan so'ng qabul qilgichning chiqishida hisoblanadigan xabar.

1 Семантик таркибини криптографик методлардан фойдаланмасдан билиш мумкин бўлган маълумотлар.

2 Дастлабки муҳофаза қилинадиган хабар.

3 Шифрлаш қурилмасининг киришига келиб тushадиган ёки шифрлашдан сўнг қабул қилгичнинг чиқишида ҳисобланадиган хабар.

Тестирование на проникновение

uz - suqulib kirishga testlash

суқулиб киришга
тестлаш

en - penetration testing

Исследование функций системы обработки данных с целью поиска способов обхода компьютерной безопасности.

Компьютер хавфсизлигини четлаб о'тish usullarini izlab topish maqsadida, ma'lumotlarni qayta ishlash tizimi funksiyalarini tadqiq etish.

Компьютер хавфсизлигини четлаб ўтиш усуллари излаб топиш мақсадида, маълумотларни қайта ишлаш тизими функцияларини тадқиқ этиш.

Токен аппаратный

uz - apparat token

аппарат токен

en - hard token

Компактное устройство, используемое для идентификации его владельца, безопасного удаленного доступа к информационным ресурсам.

Примечание – К аппаратным токенам относятся смарт-карта, брелок.

Qurilma egasini identifikatsiya qilish, axborot resurslaridan xavfsiz uzoqdan foydalana olish uchun foydalaniladigan kompakt qurilma.

Izoh – Apparat tokenlarga smart-karta, brelok kiradi.

Қурилма эгасини идентификация қилиш, ахборот ресурсларидан хавфсиз узоқдан фойдалана олиш

Т

учун фойдаланиладиган компакт курилма.
Изоҳ – Аппарат токенларга смарт-карта, брелок киради.

Токен программный

uz - dasturiy token
дастурий токен
en - soft token

Ключ для доступа к сервисам, выдаваемый пользователю после успешной авторизации.

Muvaffaqiyatli mualliflashtirishdan keyin foydalanuvchiga servislardan foydalana olish uchun beriladigan kalit.

Муваффақиятли муаллифлаштиришдан кейин фойдаланувчига сервислардан фойдалана олиш учун бериладиган калит.

Точка доступа к сети

uz - tarmoqdan foydalana olish nuqtasi
тармоқдан фойдалана олиш нуқтаси
en - network access point

Точка, в которой оператор сети предоставляет услуги пользователю, то есть точка разделения ответственности оператора и ответственности пользователя в условиях эксплуатации.

Tarmoq operatori foydalanuvchiga xizmatlarni ko'rsatadigan nuqta, ya'ni ekspluatatsiya qilish sharoitlarida operator javobgarligi va foydalanuvchi javobgarligini ajratish nuqtasi.

Тармоқ оператори фойдаланувчига хизматларни кўрсатадиган нуқта, яъни эксплуатация қилиш шароитларида оператор жавобгарлиги ва фойдаланувчи жавобгарлигини ажратиш нуқтаси.

Трансляция

uz - translyatsiya
трансляция
en - translation

Описание процесса изложения требований безопасности на стандартизованном языке.

Standartlashtirilgan tilda xavfsizlik talablarining izohini tavsiflash jarayoni.

Стандартлаштирилган тилда хавфсизлик талабларининг изоҳини тавсифлаш жараёни.

Требование

uz - talab
талаб
en - requirement

Потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

Примечания

1 Выражение «обычно предполагается» означает, что это общепринятая практика организации и заинтересованных сторон, когда предполагаются рассматриваемые потребности или ожидания.

2 Установленным является такое требование, которое определено, например, в документированной информации.

Ehtiyoj yoki belgilangan kutiladigan natija, odatda

T

taxmin qilinadi yoki majburiy hisoblanadi.

Izohlar

1 «Odatda taxmin qilinadi» ifodasi bu ko‘rib chiqilayotgan ehtiyojlar va kutilgan natijalar taxmin qilinganda, tashkilot va manfaatdor tomonlarning umumiy qabul qilingan amaliyoti ekanligini bildiradi.

2 Hujjatlashtirilgan axborotda belgilab berilgan talab rasmiy hisoblanadi.

Эҳтиёж ёки белгиланган кутиладиган натижа, одатда тахмин қилинади ёки мажбурий ҳисобланади.

Изоҳлар

1 «Odatda taxmin qilinadi» ifodasi bu ko‘rib chiqilayotgan ehtiyojlar va kutilgan natijalar taxmin qilinganda, tashkilot va manfaatdor tomonlarning umumiy qabul qilingan amaliyoti ekanligini bildiradi.

2 Hujjatlashtirilgan axborotda belgilab berilgan talab rasmiy hisoblanadi.

Требование безопасности

uz - xavfsizlik talablari

хавфсизлик талаблари

en - security requirement

Требование, изложенное стандартизированным языком, предназначением которого является содействие в достижении целей безопасности объекта оценки.

Standartlashtirilgan tilda ifodalangan, baholash obyekting xavfsizlikka erishish maqsadida, ko‘maklashishga mo‘ljallangan talablar.

Стандартлаштирилган тилда ифодаланган, баҳолаш объектининг хавфсизликка эришиш мақсадида, кўмаклашишга мўлжалланган талаблар.

Троянская программа

uz - trojan dasturi

троян дастури

en - trojan programm

1 Вредоносная программа, выглядящая как функционально полезная, позволяющая производить несанкционированный сбор, фальсификацию или уничтожение данных.

2 Программа, выполняющая в дополнение к основным функциям, неописанные в документации действия.

Примечание – Данные действия могут использовать законные полномочия субъекта системы для осуществления несанкционированного доступа.

T

1 Ma'lumotlarni ruxsat etilmagan tarzda to'plash, qalbakilashtirish yoki yo'q qilishni amalga oshirish imkonini beruvchi, funksional foydali bo'lib ko'rindigan zararli dastur.

2 Asosiy funksiyalariga qo'shimcha ravishda hujjatlarda yozilmagan harakatlarni bajaruvchi dastur.

Izoh – Bunday harakatlar davomida tizim subyektining qonuniy vakolatlaridan ruxsat etilmagan tarzda erkin foydalanish mumkin.

1 Маълумотларни рухсат этилмаган тарзда тўplash, қалбакилаштириш ёки йўқ қилишни амалга ошириш имконини берувчи, функционал фойдали бўлиб кўринадиган зарарли дастур.

2 Асосий функцияларига қўшимча равишда ҳужжатларда ёзилмаган ҳаракатларни бажарувчи дастур.

Изоҳ – Бундай ҳаракатлар давомида тизим субъектининг қонуний ваколатларидан рухсат этилмаган тарзда эркин фойдаланиш мумкин.

У

Угроза

uz - tahdid

тахдид

en - threat

1 Потенциальная возможность нарушения компьютерной безопасности.

2 Любые обстоятельства или события, которые могут являться причиной нанесения ущерба системе в форме разрушения, раскрытия или модификации данных, и/или отказа в обслуживании.

3 Потенциальная причина нежелательного инцидента, который может причинить ущерб системе или организации.

1 Kompyuter xavfsizligi buzilishining potensial imkoniyati.

2 Ma'lumotlarni buzish, ochish yoki o'zgartirish va/yoki xizmat ko'rsatishni rad etish shaklida tizimga zarar yetkazish sababchisi hisoblanishi mumkin bo'lgan har qanday holat yoki voqea.

3 Tizim yoki tashkilotga zarar keltirishi mumkin bo'lgan nomaqbul insidentning potensial sababi.

1 Компьютер хавфсизлиги бузилишининг потенциал имконияти.

У

2 Маълумотларни бузиш, очиш ёки ўзгартириш ва/ёки хизмат кўрсатишни рад этиш шаклида тизимга зарар етказиш сабабчиси ҳисобланиши мумкин бўлган ҳар қандай ҳолат ёки воқеа.

3 Тизим ёки ташкилотга зарар келтириши мумкин бўлган номақбул инцидентнинг потенциал сабаби.

Угроза автоматизированной системы

uz - avtomatlashtirilgan tizimga tahdid

автоматлаштирилган тизимга таҳдид

en - automated system treat

Потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба (материального, морального или иного) ресурсам автоматизированной системы.

Avtomatlashtirilgan tizim resurslariga (moddiy, ma'naviy yoki boshqa) zarar keltirishi mumkin bo'lgan, potensial voqea, harakat, jarayon yoki hodisa.

Автоматлаштирилган тизим ресурсларига (моддий, маънавий ёки бошқа) зарар келтириши мумкин бўлган, потенциал воқеа, ҳаракат, жараён ёки ҳодиса.

Угроза активная

uz - aktiv tahdid

актив таҳдид

en - active threat

1 Любая угроза преднамеренного несанкционированного изменения состояния системы обработки данных.

Примечание – Примером активной угрозы является угроза, в результате реализации которой возможны модификация сообщений, вставка ложных сообщений, маскарад или отказ в обслуживании.

2 Угроза преднамеренного несанкционированного изменения состояния функционирования системы или сети телекоммуникаций.

1 Ma'lumotlarni qayta ishlash tizimi holatini qasddan ruxsat etilmagan tarzda o'zgartirishning har qanday tahdidi.

Izoh – Aktiv tahdidga, amalga oshirilishi natijasida xabarlarni modifikatsiyalash, yolg'on xabarlarni kiritish, aldamchilik yoki xizmat ko'rsatishni rad etish misol bo'lishi mumkin.

2 Telekommunikatsiyalar tizimlari yoki tarmoqning ishlash holatini qasddan ruxsat etilmagan tarzda o'zgartirishga bo'lgan tahdid.

1 Маълумотларни қайта ишлаш тизими ҳолатини қасддан рuxсат этилмаган тарзда ўзгартириш-

У

нинг ҳар қандай таҳдиди.

Изоҳ – Актив таҳдидга, амалга оширилиши натижасида хабарларни модификациялаш, ёлгон хабарларни кириштиш, алдамчилик ёки хизмат кўрсатишни рад этиш мисол бўлиши мумкин.

2 Телекоммуникациялар тизимлари ёки тармоқнинг ишлаш ҳолатини қасдан рухсат этилмаган тарзда ўзгартиришга бўлган таҳдид.

Угроза безопасности

uz - xavfsizlikka tahdid

хавфсизликка таҳдид

en - security threat

Возможная опасность (потенциальная или реально существующая) совершения какого-либо действия, направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.

Axborotning buzib ko'rsatilishi va yo'qolish xavfi bo'lishida ko'rinadigan, mulkdorga yoki foydalalanuvchiga zarar yetkazadigan, muhofaza obyektiga (axborot resurslariga) qarshi yo'naltirilgan qandaydir harakatni amalga oshirishning mumkin bo'lgan (potensial yoki real mavjud) xavfi.

Ахборотнинг бузиб кўрсатилиши ва йўқолиш хавфи бўлишида кўринадиган, мулкдорга ёки фойдаланувчига зарар етказадиган, муҳофаза объектига (ахборот ресурсларига) қарши йўналтирилган қандайдир ҳаракатни амалга оширишнинг мумкин бўлган (потенциал ёки реал мавжуд) хавфи.

Угроза безопасности

информации

uz - axborot xavfsizligiga tahdid

ахборот хавфсизлигига

таҳдид

en - data security treat

1 Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному ее тиражированию.

2 Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

У

1 Axborotning konfidensialligi, yaxlitligi, undan foydalana olishlik buzilishiga, shuningdek uning g'ayriqonuniy tarzda ko'paytirilishiga olib kelishi mumkin bo'lgan potensial voqea, harakat, jarayon yoki hodisa.

2 Axborotning tarqatilishi va/yoki unga ruxsat etilmagan tarzda va/yoki ko'zda tutilmagan ta'sirlar bilan bog'liq potensial yoki mavjud real xavfni vujudga keltiruvchi sharoitlar va omillar jami.

1 Ахборотнинг конфиденциаллиги, яхлитлиги, ундан фойдалана олишлик бузилишига, шунингдек, унинг ғайриқонуний тарзда кўпайтирилишига олиб келиши мумкин бўлган потенциал воқеа, ҳаракат, жараён ёки ҳодиса.

2 Ахборотнинг тарқатилиши ва/ёки унга рухсат этилмаган тарзда ва/ёки кўзда тутилмаган таъсирлар билан боғлиқ потенциал ёки мавжуд реал хавфни вужудга келтирувчи шароитлар ва омиллар жами.

Угроза интересам субъектов информационных отношений

uz - axborot munosabatlari subyektlarining manfaatlariga tahdid

ахборот муносабатлари субъектларининг манфаатларига таҳдид

en - treat towards the interests of information relapses subjects

Потенциально возможное событие, действие, процесс или явление, которое посредством воздействия на информацию и другие компоненты автоматизированной системы может привести к нанесению ущерба интересам данных субъектов.

Axborotga va avtomatlashtirilgan tizimning boshqa komponentlariga ta'sir etish orqali, berilgan subyektlarning manfaatlariga zarar keltirishi mumkin bo'lgan potensial voqea, harakat, jarayon yoki hodisa.

Ахборотга ва автоматлаштирилган тизимнинг бошқа компонентларига таъсир этиш орқали, берилган субъектларнинг манфаатларига зарар келтириши мумкин бўлган потенциал воқеа, ҳаракат, жараён ёки ҳодиса.

Угроза информационная

uz - axborot tahdidi

ахборот таҳдиди

en - information treat

Фактор или совокупность факторов, создающих опасность нарушения свойств информации.

Axborot xususiyatlarining buzilish xavfini vujudga keltiruvchi omil yoki omillar yig'indisi.

Ахборот хусусиятларининг бузилиш хавфини ву-

У

Угроза информационной безопасности инфокоммуникационной системы

uz - axborot-kommunikatsiya tizimi axborot xavfsizligiga tahdid

ахборот-коммуникация тизими ахборот

хавфсизлигига таҳдид

en - treat towards infocommunication system information security

Угроза информационной безопасности сети

телекоммуникаций

общего пользования

uz - umumiy foydalanishdagi telekommunikatsiyalar tarmog‘i axborot xavfsizligiga tahdid

умумий фойдаланишдаги телекоммуникациялар

тармоғи ахборот

хавфсизлигига таҳдид

en - public switched telecommunications network information security threat

Угроза пассивная

uz - passiv tahdid

пассив таҳдид

en - passive threat

жудга келтирувчи омил ёки омиллар йиғиндиси.

Действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию ресурсов сети.

Tarmoq resurslarini buzish, buzib ko‘rsatish yoki ulardan ruxsat etilmagan tarzda foydalanishga olib kelishi mumkin bo‘lgan harakat yoki voqea.

Тармоқ ресурсларини бузиш, бузиб кўрсатиш ёки улардан рухсат этилмаган тарзда фойдаланишга олиб келиши мумкин бўлган ҳаракат ёки воқеа.

Предполагаемое воздействие злоумышленника на сеть телекоммуникаций общего пользования, не предотвращение, не обнаружение и не ликвидация которого средствами сети может привести к снижению заданного уровня обеспечения информационной безопасности сети телекоммуникаций общего пользования.

Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘iga jinoyatkorning ko‘zda tutilgan ta’siri, uning tarmoq vositalari bilan bartaraf qilinmagani, aniqlanmagani va yo‘q qilinmagani umumiy foydalanishdagi telekommunikatsiyalar tarmog‘i axborot xavfsizligini ta’minlashning berilgan darajasi pasayishiga olib kelishi mumkin.

Умумий фойдаланишдаги телекоммуникациялар тармоғига жинояткорнинг кўзда тутилган таъсири, унинг тармоқ воситалари билан бартараф қилинмагани, аниқланмагани ва йўқ қилинмагани умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлашнинг берилган даражаси пасайишига олиб келиши мумкин.

1 Угроза несанкционированного раскрытия содержания информации без изменения состояния системы обработки данных.

Примечание – Примером пассивной угрозы является угроза, в результате реализации которой возможно восстановление чувствительной информации из перехвачен-

У

ных передаваемых данных.

2 Возможность несанкционированного доступа к информации без изменения режима функционирования системы.

1 Ma'lumotlarni qayta ishlash tizimi holatini o'zgartirmasdan, axborot mazmunini ruxsat etilmagan tarzda, ochishga bo'lgan tahdid.

Izoh – Amalga oshirilishi natijasida qo'lga kiritilib, uzatilgan ma'lumotlardan ta'sirchan axborotni tiklash imkoni bo'lgan tahdid passiv tahdidga misol bo'lib hisoblanadi.

2 Tizimning ishlash rejimini o'zgartirmasdan axborotdan ruxsat etilmagan tarzda foydalana olish imkoniyati.

1 Маълумотларни қайта ишлаш тизими ҳолатини ўзгартирмасдан, ахборот мазмунини рuxсат этилмаган тарзда, очишга бўлган таҳдид.

Изоҳ – Амалга оширилиши натижасида қўлга киритилиб, узатилган маълумотлардан таъсирчан ахборотни тиклаш имкони бўлган таҳдид пассив таҳдидга мисол бўлиб ҳисобланади.

2 Тизимнинг ишлаш режимини ўзгартирмасдан ахборотдан рuxсат этилмаган тарзда фойдалана олиш имконияти.

Угроза физическая

uz - fizik tahdid

физик таҳдид

en - physical threat

Угроза, последствием реализации которой является физический ущерб всей системе.

Shunday tahdidki, uning amalga oshirilishi oqibatida, butun tizimga fizik zarar yetkaziladi.

Шундай таҳдидки, унинг амалга оширилиши оқибатида, бутун тизимга физик зарар етказилади.

Угрозы преднамеренные

uz - qasddan qilinadigan

tahdidlar

қасддан қилинадиган

таҳдидлар

en - intentional threats

Угрозы от случайного просмотра с использованием легко доступных инструментов слежения до изоощренных попыток нарушения защиты с использованием специальных знаний о системе.

Foydalanish oson bo'lgan kuzatuv asboblaridan foydalanib tasodifiy ko'rib chiqishdan tortib tizim to'g'risida maxsus bilimlardan foydalanib muhofaza buzilishiga ustalik bilan urinishgacha bo'lgan tahdidlar.

Фойдаланиш осон бўлган кузатув асбобларидан фойдаланиб тасодифий кўриб чиқишдан тортиб

У

тизим тўғрисида махсус билимлардан фойдаланиб муҳофаза бузилишига усталик билан уришишгача бўлган таҳдидлар.

Угрозы случайные

uz - tasodifiy tahdidlar

тасодифий таҳдидлар

en - accidental threats

Угрозы, не связанные с умышленным намерением. Например, нарушения работы системы, грубые эксплуатационные ошибки и ошибки в программном обеспечении.

Qasddan qilingan niyat bilan bog'liq bo'lmagan tahdidlar. Masalan, tizim ishlashining buzilishi, qo'pol ekspluatatsion xatolar va dasturiy ta'minotdagi xatolar.

Қасддан қилинган ният билан боғлиқ бўлмаган таҳдидлар. Масалан, тизим ишлашининг бузилиши, кўпол эксплуатацион хатолар ва дастурий таъминотдаги хатолар.

Улучшение постоянное

uz - doimiy yaxshilanish

доимий яхшиланиш

en - continual improvement

Повторяющаяся деятельность по улучшению результатов деятельности.

Faoliyat natijalarini yaxshilash bo'yicha takrorlanadigan faoliyat.

Фаолият натижаларини яхшилаш бўйича такролландиган фаолият.

Уничтожение информации

uz - axborotni yo'q qilish

ахборотни йўқ қилиш

en - data destruction

Случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, в том числе хищение носителей и технических средств.

Texnik vositalar bilan qayta ishlashda tashuvchilardagi axborotni tasodifan yoki qasddan o'chirish, shu jumladan, tashuvchilar va texnik vositalarni o'g'irlash.

Техник воситалар билан қайта ишлашда ташувчилардаги ахборотни тасодифан ёки қасддан ўчириш, шу жумладан, ташувчилар ва техник воситаларни ўғирлаш.

Управление

uz - boshqarish

бошқариш

Процесс целенаправленного воздействия на объект, осуществляемый для организации его функционирования в соответствии с заданными тре-

у

en - controlling

бованиями.

Obyektga maqsadga yo'naltirilgan ta'sir etish jarayoni. Berilgan talablarga muvofiq, uning ishlashini tashkil qilish uchun amalga oshiriladi.

Объектга мақсадга йўналтирилган таъсир этиш жараёни. Берилган талабларга мувофиқ, унинг ишлашини ташкил қилиш учун амалга оширилади.

Управление безопасностью

uz - xavfsizlikni boshqarish

хавфсизликни бошқариш

en - security control

Служба управления и контроля доступа к ресурсам сети. Осуществляет запуск механизмов защиты от внешних атак и проверяет целостность данных при их хранении и передаче через сеть.

Tarmoq resurslaridan erkin foydalanishni boshqarish va nazorat qilish xizmati. Tashqi hujumlardan muhofaza mexanizmi ishga tushirilishini amalga oshiradi va ma'lumotlarni, ularni saqlash va tarmoq orqali uzatishda yaxlitligini tekshiradi.

Тармоқ ресурсларидан эркин фойдаланишни бошқариш ва назорат қилиш хизмати. Ташқи хужумлардан муҳофаза механизми ишга туширилишини амалга оширади ва маълумотларни, уларни сақлаш ва тармоқ орқали узатишда яхлитлигини текширади.

Управление доступом

uz - foydalana olishni

boshqarish

фойдалана олишни

бошқариш

en - access control

1 Методы, обеспечивающие возможность обращения к ресурсам системы обработки данных только уполномоченным логическим объектам и только разрешенным способом.

2 Метод защиты информации регулированием использования всех ресурсов системы (элементов баз данных, программных и технических средств).

3 Методы обеспечения санкционированного и ограниченного доступа к активам, основанные на требованиях бизнеса и безопасности.

4 Процесс ограничения доступа к ресурсам системы только разрешенным программам, процессам или другим системам (в сети).

1 Ma'lumotlarni qayta ishlash tizimi resurslariga fa-

у

qat vakolatga ega mantiqiy obyektlar va faqat ruxsat etilgan usul bilan murojaat qilish imkoniyatini ta'minlaydigan metodlar.

2 Tizimning barcha resurslaridan (ma'lumotlar bazalari elementlari, dasturiy va texnik vositalari) foydalanishni tartibga solish bilan, axborotni muhofaza qilish metodi.

3 Biznes va xavfsizlik talablariga asoslangan, aktivlardan ruxsat etilgan va cheklangan tarzda foydalana olishni ta'minlash usullari.

4 Faqat ruxsat etilgan dasturlar, jarayonlar yoki boshqa tizimlarga (tarmoqdagi) tizim resurslaridan erkin foydalanishni cheklash jarayoni.

1 Маълумотларни қайта ишлаш тизими ресурсларига фақат ваколатга эга мантиқий объектлар ва фақат рuxсат этилган усул билан муружаат қилиш имкониятини таъминлайдиган методлар.

2 Тизимнинг барча ресурсларидан (маълумотлар базалари элементлари, дастурий ва техник воситалари) фойдаланишни тартибга солиш билан, ахборотни муҳофаза қилиш методи.

3 Бизнес ва хавфсизлик талабларига асосланган, активлардан рuxсат этилган ва чекланган tarzda фойдалана олишни таъминлаш усуллари.

4 Фақат рuxсат этилган дастурлар, жараёнлар ёки бошқа тизимларга (тармоқдаги) тизим ресурсларидан эркин фойдаланишни чеклаш жараёни.

Управление доступом дискреционное

uz - diskretsion foydalana olishni boshqarish

дискрецион фойдалана олишни бошқариш

en - discretionary access control

1 Разграничение доступа между поименованными субъектами и поименованными объектами. Примечание – Субъект с определенным правом доступа может передать это право любому другому равноправному субъекту.

2 Управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

1 Nommanom ko'rsatilgan subyektlar va nommanom ko'rsatilgan obyektlar o'rtasidagi foydalanishni belgilash.

Izoh – Foydalanishning ma'lum huquqiga ega subyekt bu

У

huquqni istalgan boshqa teng huquqli subyektga berishi mumkin.

2 Foydalana olishni boshqarish ro'yxatlari yoki erkin foydalanish matritsasi asosida, subyektlarning obyektlardan foydalana olishini boshqarish.

1 Номманом кўрсатилган субъектлар ва номманом кўрсатилган объектлар ўртасидаги фойдаланишни белгилаш.

Изоҳ – Фойдаланишнинг маълум ҳуқуқига эга субъект бу ҳуқуқни исталган бошқа тенг ҳуқуқли субъектга бериши мумкин.

2 Фойдалана олишни бошқариш рўйхатлари ёки эркин фойдаланиш матрицаси асосида, субъектларнинг объектлардан фойдалана олишини бошқариш.

Управление доступом логическое

uz - foydalana olishni mantiqiy boshqarish

фойдалана олишни мантиқий бошқариш

en - logical access control

Использование механизмов, обеспечивающих управление доступом к данным или информации.

Примечание – Как правило, для логического управления доступом используется пароль.

Ma'lumotlar yoki axborotdan foydalana olish boshqarilishini ta'minlaydigan mexanizmlarning qo'llanilishi.

Izoh – Qoidaga ko'ra, foydalana olishni mantiqiy boshqarishda paroldan foydalaniladi.

Маълумотлар ёки ахборотдан фойдалана олиш бошқарилишини таъминлайдиган механизмларнинг қўлланилиши.

Изоҳ – Қоидага кўра, фойдалана олишни мантиқий бошқаришда паролдан фойдаланилади.

Управление доступом на основе ролей

uz - rollar asosida foydalana olishni boshqarish

роллар асосида фойдалана олишни бошқариш

en - role based access control

1 Модель системы разграничения прав доступа, в которой роли используются для выполнения различных задач, а разрешения на выполнение операций привязываются к ролям.

2 Общая модель обеспечения безопасности, которая упрощает администрирование путем назначения ролей пользователям и установки разрешений для этих ролей.

1 Foydalana olish huquqini belgilash tizimining modeli, bunda rollardan turli vazifalarni bajarish uchun foydalaniladi, operatsiyalarni bajarishga ruxsat esa,

у

rollarga bogʻlanadi.

2 Foydalanuvchilarga rollarni belgilash va bu rollar uchun ruxsat oʻrnatish orqali maʼmuriy boshqarishni soddalashtiradigan, xavfsizlikni taʼminlashning umumiy modeli.

1 Фойдалана олиш ҳуқуқини белгилаш тизимининг модели, бунда роллардан турли вазифаларни бажариш учун фойдаланилади, операцияларни бажаришга рухсат эса, ролларга боғланади.

2 Фойдаланувчиларга ролларни белгилаш ва бу роллар учун рухсат ўрнатиш орқали маъмурий бошқаришни соддалаштирадиган, хавфсизликни таъминлашнинг умумий модели.

Управление доступом полномочное (мандатное)

uz - foydalana olishni vakolatli
(mandatli) boshqarish

фойдалана олишни
ваколатли (мандатли)

бошқариш

en - mandatory access control

1 Способ управления доступом к объектам, основанный на степени секретности или критичности информации (представленной специальными метками), содержащейся в объекте и формальной проверке полномочий и прав субъекта при доступе к информации данного уровня критичности.

2 Разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

1 Obyektlardan erkin foydalanishni boshqarish usuli obyektida mavjud boʻlgan axborotning (maxsus belgilar bilan taqdim etilgan) maxfiylik yoki kritiklik darajasiga va berilgan kritiklik darajasidagi axborotdan erkin foydalanishda subyektning vakolatlari va huquqlarini rasman tekshirishga asoslangan.

2 Subyektlarning obyektlardan foydalana olishlarini obyektlarda boʻlgan axborot uchun konfidensiallik belgisini tayinlashga va subyektlarga shunday konfidensiallik darajasidagi axborotga murojaat qilishlari uchun rasmiy ruxsatlar berilishiga asoslangan belgilash.

1 Объектлардан эркин фойдаланишни бошқариш усули объектда mavjud бўлган ахборотнинг (maxsus белгилар билан тақдим этилган) махфийлик ёки критиклик даражасига ва берилган критиклик

У

даражасидаги ахборотдан эркин фойдаланишда субъектнинг ваколатлари ва ҳуқуқларини расман текширишга асосланган.

2 Субъектларнинг объектлардан фойдалана олишларини объектларда бўлган ахборот учун конфиденциаллик белгисини тайинлашга ва субъектларга шундай конфиденциаллик даражасидаги ахборотга мурожаат қилишлари учун расмий рухсатлар берилишига асосланган белгилаш.

Управление доступом физическое

uz - fizik foydalana olishni
boshqarish

физик фойдалана олишни

бошқариш

en - physical access control

Использование физических механизмов, обеспечивающих управление доступом.

Примечание – Примером физического управления доступом является хранение компьютера в запираемом на замок помещении.

Foydalana olishning boshqarilishini ta'minlaydigan fizik mexanizmlardan foydalanish.

Izoh – Kompyuterni qulflanadigan xonada saqlash foydalana olishni fizik boshqarishga misol bo'lib hisoblanadi.

Фойдалана олишнинг бошқарилишини таъминлайдиган физик механизмлардан фойдаланиш.

Изоҳ – Компьютерни қулфланадиган хонада сақлаш фойдалана олишни физик бошқаришга мисол бўлиб ҳисобланади.

Управление информационной безопасностью корпоративное

uz - korporativ axborot
xavfsizligini boshqarish

корпоратив ахборот

хавфсизлигини бошқариш

en - governance of information
security

Система, обеспечивающая руководство и контроль деятельности организаций в области информационной безопасности.

Axborot xavfsizligi sohasida tashkilot faoliyatiga rahbarlik qilish va nazorat qilishni ta'minlovchi tizim.

Ахборот хавфсизлиги соҳасида ташкилот фаолиятига раҳбарлик қилиш ва назорат қилишни таъминловчи тизим.

Управление информационным потокком

uz - axborot oqimini
boshqarish

ахборот оқимини

бошқариш

en - information flow control

1 Процедуры управления информационным потоком, удостоверяющие, что информация не может передаваться с верхних уровней безопасности на нижние (в соответствии с положениями модели Белла-Лападула).

2 Процедуры управления, удостоверяющие, что информация не может передаваться по скрытым каналам, то есть в обход политики безопасности.

у

1 Axborot xavfsizlikning yuqori darajasidan quyi darajasiga (Bella-Lapadula modeli qoidalariga muvofiq) uzatilishi mumkin emasligini tasdiqlovchi axborot oqimini boshqarish protseduralari.

2 Axborot yashirin kanallar bo‘ylab, ya’ni xavfsizlik siyosatini chetlab o‘tib, uzatilishi mumkin emasligini tasdiqlovchi boshqarish protseduralari.

1 Ахборот хавфсизликнинг юқори даражасидан қуйи даражасига (Белла-Лападула модели қоидаларига мувофиқ) узатилиши мумкин эмаслигини тасдиқловчи ахборот оқимини бошқариш процедуралари.

2 Ахборот яширин каналлар бўйлаб, яъни хавфсизлик сиёсатини четлаб ўтиб, узатилиши мумкин эмаслигини тасдиқловчи бошқариш процедуралари.

Управление инцидентами информационной безопасности

uz - axborot xavfsizligi insidentlarini boshqarish
ахборот хавфсизлиги инцидентларини бошқариш
en - information security incident management

Процессы обнаружения, учета, оценки, реагирования и изучения, относящиеся к инцидентам информационной безопасности.

Axborot xavfsizligi insidentlariga tegishli aniqlash, hisobga olish, baholash, munosabat bildirish va o‘rganish jarayonlari.

Ахборот хавфсизлиги инцидентларига тегишли аниқлаш, ҳисобга олиш, баҳолаш, муносабат билдириш ва ўрганиш жараёнлари.

Управление ключами

uz - kalitlarni boshqarish
калитларни бошқариш
en - key management

Генерация, хранение, распределение, удаление, учет и применение ключей в соответствии с политикой безопасности.

Xavfsizlik siyosatiga muvofiq, kalitlarni generatsiyalash, saqlash, taqsimlash, chiqarib tashlash, hisobga olish va qo‘llash.

Хавфсизлик сиёсатига мувофиқ, калитларни генерациялаш, сақлаш, тақсимлаш, чиқариб ташлаш, ҳисобга олиш ва қўллаш.

Управление конфигурацией

Дисциплина, использующая техническое и адми-

У

uz - konfiguratsiyani boshqarish
конфигурацияни бошқариш
en - configuration management

нистративное руководство и контроль за идентификацией и документированием функциональных и физических характеристик элемента конфигурации, контроль за изменениями этих характеристик, контроль регистрации внесенных изменений и предоставления отчетности по ним, а также хода выполнения и подтверждения соответствия соответствующим требованиям.

Texnik va ma'muriy qo'llanmalardan foydalanadigan fan konfiguratsiya elementining fizik va funksional xarakteristikalarini hujjatlashtirish, identifikatsiya qilish va bu xarakteristikalarning o'zgarishi ustidan nazorat, kiritilgan o'zgarishlar qayd etilishini va ular bo'yicha hisobot taqdim etilishini shuningdek, bajarilishining borishini va tegishli talablarga moslikning nazorat qilinishi.

Техник ва маъмурий қўлланмалардан фойдаланадиган фан конфигурация элементининг физик ва функционал характеристикаларини ҳужжатлаштириш, идентификация қилиш ва бу характеристикаларнинг ўзгариши устидан назорат, киритилган ўзгаришлар қайд этилишини ва улар бўйича ҳисобот тақдим этилишини шунингдек, бажарилишининг боришини ва тегишли талабларга мосликнинг назорат қилиниши.

Управление прикладное
uz - amaliy boshqarish
амалий бошқариш
en - application management

Набор функций, способствующих предоставлению пользователям возможности наблюдать и управлять выполнением операций распределенной обработки данных.

Foydalanuvchilarga ma'lumotlarni taqsimlangan qayta ishlash operatsiyalarining bajarilishini boshqarish va kuzatib borish imkoniyatini beruvchi funksiyalar to'plami.

Фойдаланувчиларга маълумотларни тақсимланган қайта ишлаш операцияларининг бажарилишини бошқариш ва кузатиб бориш имкониятини берувчи функциялар тўплами.

Управление рисками
uz - risklarni boshqarish
рисklarни бошқариш

1 Последовательность операций, выработанных практикой управления в области безопасности систем или сетей.

у

en - risk management

2 Процесс определения контрмер в соответствии с оценкой рисков.

3 Координированная деятельность по руководству и управлению организацией по отношению к риску.

Примечание – Управление рисками обычно включает определение рисков, обработку рисков, принятие рисков и сообщение о рисках.

1 Tizimlar yoki tarmoqlar xavfsizligi sohasida boshqarish amaliyoti davomida ishlab chiqilgan operatsiyalar ketma-ketligi.

2 Risklarni baholashga muvofiq, qarshi chora-tadbirlarni belgilash jarayoni.

3 Riskka nisbatan tashkilotga rahbarlik qilish va uni boshqarish bo'yicha muvofiqlashtirilgan faoliyat.

Izoh – Risklarni boshqarish, odatda, risklarni aniqlash, risklarni qayta ishlash, risklarni qabul qilish va risklar to'g'risida xabar berishni o'z ichiga oladi.

1 Tizimlar ёки тармоқлар хавфсизлиги соҳасида бошқариш амалиёти давомида ишлаб чиқилган операциялар кетма-кетлиги.

2 Risklarni baholashga muvofiq, qarshi chora-tadbirlarni belgilash jarayoni.

3 Riskka nisbatan tashkilotga rahbarlik qilish va uni boshqarish bo'yicha muvofiqlashtirilgan faoliyat.

Izoh – Risklarni boshqarish, odatda, risklarni aniqlash, risklarni qayta ishlash, risklarni qabul qilish va risklar to'g'risida xabar berishni o'z ichiga oladi.

Уровень безопасности

uz - xavfsizlik darajasi

хавфсизлик даражаси

en - security level

1 Совокупность иерархического грифа секретности и категории безопасности, которая указывает на чувствительность объекта к категории допуска лица.

2 Комбинация иерархической классификации (уровень доступа) и неиерархической категории, представляющих уровень критичности (чувствительности) информации.

1 Obyektning shaxs foydalanish huquqi kategoriyasiga sezgirligini ko'rsatadigan iyerarxik maxfiylik grifi va xavfsizlik kategoriyasi jami.

2 Axborotning kritiklik (sezgirlik) darajasini ko'rsa-

У

tuvchi, noiyerarxik kategoriya va iyerarxik klassifikatsiya (foydalana olish darajasi) birikmasi.

1 Objektning шахс фойдаланиш ҳуқуқи категориясига сезгирлигини кўрсатадиган иерархик махфийлик грифи ва хавфсизлик категорияси жами.

2 Ахборотнинг критиклик (сезгирлик) даражасини кўрсатувчи, ноиерархик категория ва иерархик классификация (фойдалана олиш даражаси) бирикмаси.

Уровень безопасности базовый

uz - bazaviy xavfsizlik darajasi

базавий хавфсизлик даражаси

en - baseline security

Обязательный минимальный уровень защищенности для информационных систем.

Muhofaza qilinganlikning, axborot tizimlari uchun qabul qilingan, majburiy bo'lgan eng past darajasi.

Муҳофаза қилинганликнинг, ахборот тизимлари учун қабул қилинган, мажбурий бўлган энг паст даражаси.

Уровень доверия оценочный

uz - baholi ishonch darajasi

баҳоли ишонч даражаси

en - evaluation assurance level

Набор требований доверия к безопасности, занимающий некоторое положение на заданной шкале доверия и составляющий пакет доверия.

Berilgan ishonch shkalasida ma'lum joyni band etib va ishonch paketini tashkil etadigan, xavfsizlikning ishonch talablari majmui.

Берилган ишонч шкаласида маълум жойни банд этиб ва ишонч пакетини ташкил этадиган, хавфсизликнинг ишонч талаблари мажмуи.

Уровень доступа

uz - foydalana olish darajasi

фойдалана олиш даражаси

en - access level

1 Уровень полномочий, необходимый логическому объекту для получения доступа к защищенному ресурсу.

Примечание – Уровнем доступа могут быть полномочия на доступ к данным или информации заданного уровня безопасности.

2 Иерархическая часть метки уровня безопасности, используемая для идентификации критичности данных или прозрачности субъектов. Уровень доступа вместе с неиерархическими категориями составляет уровень безопасности.

у

1 Mantiqiy obyektga muhofaza qilingan resursdan foydalanish imkoniyatini olish uchun zarur bo'lgan vakolatlar darajasi.

Izoh – Berilgan xavfsizlik darajasidagi axborotdan yoki ma'lumotlardan foydalana olishga vakolatlar foydalana olish darajasi bo'lishi mumkin.

2 Ma'lumotlarning kritikligini yoki subyektlarning ochiqqligini identifikatsiya qilish uchun qo'llaniladigan, xavfsizlik darajasi belgisining iyerarxik qismi. Erkin foydalanish darajasi noiyerarxik kategoriyalar bilan birga xavfsizlik darajasini tashkil etadi.

1 Мантиқий объектга муҳофаза қилинган ресурсдан фойдаланиш имкониятини олиш учун зарур бўлган ваколатлар даражаси.

Изоҳ – Берилган хавфсизлик даражасидаги ахборотдан ёки маълумотлардан фойдалана олишга ваколатлар фойдалана олиш даражаси бўлиши мумкин.

2 Маълумотларнинг критиклигини ёки субъектларнинг очиклигини идентификация қилиш учун қўлланиладиган, хавфсизлик даражаси белгисининг иерархик қисми. Эркин фойдаланиш даражаси ноиерархик категориялар билан бирга хавфсизлик даражасини ташкил этади.

Уровень полномочий субъекта

uz - subyekt vakolatlari darajasi

субъект ваколатлари даражаси

en - subject privilege

Совокупность прав доступа субъекта доступа.

Foydalana olish subyekting foydalana olish (kira olish) yuzasidan huquqlarining jami.

Фойдалана олиш субъектининг фойдалана олиш (кира олиш) юзасидан ҳуқуқларининг жами.

Уровень прозрачности

uz - ochiqlik darajasi

очиқлик даражаси
en - transparency level, clearance

Максимальный уровень безопасности, доступ к которому разрешен данному субъекту правилами модели Белла-Лападула. Текущий уровень субъекта (уровень, на котором он в данный момент выполняет операции) может варьироваться от минимального до уровня прозрачности.

Xavfsizlikning maksimal darajasi, subyektga undan foydalana olish uchun Bella-Lapadula modeli qoidalariga ko'ra ruxsat berilgan. Subyekting joriy darajasi (u shu vaqtda operatsiyalar bajarayotgan daraja) minimaldan ochiqlik darajasigacha o'zgartirilishi

У

mumkin.

Хавфсизликнинг максимал даражаси, субъектга ундан фойдалана олиш учун Белла-Лападула модели қоидаларига кўра рухсат берилган. Субъектнинг жорий даражаси (у шу вақтда операциялар бажараётган даража) минималдан очиклик даражасигача ўзгартирилиши мумкин.

Уровень риска

uz - risk darajasi

риск даражаси

en - level of risk

Величина риска, характеризующаяся сочетанием последствий и их вероятности.

Risk oqibatlari va ular ehtimolligi birikmasini ifodalaydigan risk kattaligi.

Риск оқибатлари ва улар эҳтимоллиги бирикмасини ифодалайдиган риск катталиги.

Усиление

uz - kuchaytirish

кучайтириш

en - augmentation

Добавление в пакет одного или нескольких требований.

Paketga bitta yoki bir nechta talabni qo'shish.

Пакетга битта ёки бир нечта талабни қўшиш.

Услуга аутентификации

uz - autentifikatsiya qilish

xizmati

аутентификация қилиш

хизмати

en - authentication service

Услуга, предоставляющая доказательство того, что идентификация объекта или субъекта на самом деле является идентификацией, которая заявлена им.

Примечание – В зависимости от действующего субъекта и целей идентификации могут потребоваться следующие виды аутентификации: аутентификация пользователя, аутентификация одноранговых объектов, аутентификация источника данных.

Obyekt yoki subyektni identifikatsiyalash, aslida ular tomonidan bayon qilingan identifikatsiya ekanligining dalilini ko'rsatuvchi xizmat.

Izoh – Amaldagi subyektga va identifikatsiya maqsadlariga bog'liq ravishda quyidagi autentifikatsiya turlari talab qilinishi mumkin: foydalanuvchini autentifikatsiya qilish, bitta rang obyektlarini autentifikatsiya qilish, ma'lumotlar manbai-ni autentifikatsiya qilish.

Объект ёки субъектни идентификациялаш, аслида улар томонидан баён қилинган идентификация эканлигининг далилини кўрсатувчи хизмат.

Изоҳ – Амалдаги субъектга ва идентификация мақсадларига боғлиқ равишда қуйидаги аутентификация турлари талаб қилиниши мумкин: фойдаланувчини аутентифика-

У

ция қилиш, битта ранг объектларини аутентификация қилиш, маълумотлар манбаини аутентификация қилиш.

Услуга безопасности

uz - xavfsizlik xizmati

хавфсизлик хизмати

en - security service

Услуга, предоставляемая каким-либо уровнем взаимосвязи открытых систем, которая гарантирует достаточную защиту систем или процессов передачи данных.

Ochiq tizimlar o‘zaro bog‘liqligining qandaydir darajasi taqdim etadigan xizmat. Ma’lumotlar uzatish tizimlari yoki jarayonlarining yetarlicha muhofaza qilinishini kafolatlaydi.

Очиқ тизимлар ўзаро боғлиқлигининг қандайдир даражаси тақдим этадиган хизмат. Маълумотлар узатиш тизимлари ёки жараёнларининг етарлича муҳофаза қилинишини кафолатлайди.

Услуга

конфиденциальности

uz - konfidensiallik xizmati

конфиденциаллик

хизмати

en - confidentiality service

Услуга конфиденциальности предоставляет защиту от неразрешенного раскрытия данных об-мена.

Примечание – Различают следующие виды услуг обеспечения конфиденциальности: конфиденциальность выбранного поля; конфиденциальность в режиме с установлением соединения; конфиденциальность в режиме без установления соединения; конфиденциальность трафика.

Almashinadigan ma’lumotlarning ruxsat etilmagan tarzda oshkor etilishdan muhofaza qilinishini ifodalaydigan konfidensiallik xizmati.

Izoh – Konfidensiallikni ta’minlash xizmatlarining quyidagi turlari ajratiladi: tanlangan maydon konfidensialligi; bog‘lanish o‘rnatilgan rejimdagi konfidensiallik; bog‘lanish o‘rnatilmagan rejimdagi konfidensiallik; trafikning konfidensialligi.

Алмашинадиган маълумотларнинг рухсат этилмаган тарзда ошкор этилишдан муҳофаза қилинишини ифодалайдиган конфиденциаллик хизмати.

Изоҳ – Конфиденциалликни таъминлаш хизматларининг қуйидаги турлари ажратилади: танланган майдон кон-фиденциаллиги; боғланиш ўрнатилган режимдаги кон-фиденциаллик; боғланиш ўрнатилмаган режимдаги кон-фиденциаллик; трафикнинг конфиденциаллиги.

Услуга отметки времени

uz - vaqtni belgilash xizmati

вақтни белгилаш хизмати

en - time stamping service

Услуга, которая подтверждает существование электронных данных в определенный момент времени.

Примечание – Услуги отметки времени полезны и, воз-

У

можно, совершенно необходимы для поддержки проверки цифровых подписей в течение длительного срока.

Ma'lum bir vaqt onida elektron ma'lumotlar mavjudligini tasdiqlaydigan xizmat.

Izoh – Vaqtni belgilash xizmatlari foydali, shuningdek, uzoq muddat mobaynida raqamli imzolar tekshiruvini olib borish uchun mutlaqo zarur.

Маълум бир вақт онида электрон маълумотлар мавжудлигини тасдиқлайдиган хизмат.

Изоҳ – Вақтни белгилаш хизматлари фойдали, шунингдек, узоқ муддат мобайнида рақамли имзолар текширувини олиб бориш учун мутлақо зарур.

Услуга рассылки ключей

uz - kalitlarni tarqatish xizmati

калитларни тарқатиш хизмати

en - key distribution service

Услуга безопасной рассылки ключей уполномоченным объектам, выполняемая центром рассылки ключей.

Kalitlarni vakolatli obyektarga xavfsiz tarqatish xizmati. Kalitlarni tarqatish markazi tomonidan bajariladi.

Калитларни ваколатли объектларга хавфсиз тарқатиш хизмати. Калитларни тарқатиш маркази томонидан бажарилади.

Услуга управления доступом

uz - foydalana olishni boshqarish xizmati

фойдалана олишни бошқариш хизмати

en - access control service

Способы, обеспечивающие доступ субъектов только разрешенным способом.

Subyektlarning faqat ruxsat etilgan yo'l bilan foydalana olishini ta'minlaydigan usullar.

Субъектларнинг фақат рухсат этилган йўл билан фойдалана олишини таъминлайдиган усуллар.

Услуга целостности

uz - yaxlitlik xizmati

яхлитлик хизмати

en - integrity service

Предоставление способов гарантирования правильности данных обмена, защиты от изменения, удаления, создания (вставки) и повторного использования данных обмена.

Almashinadigan ma'lumotlar to'g'riligini, almashinadigan ma'lumotlarning o'zgarishlardan, chiqarib tashlashlardan, yaratish (kiritish) va takror foydalanishdan muhofaza qilinishini kafolatlash usullarining taqdim etilishi.

Алмашинадиган маълумотлар тўғрилигини, алма-

У

шинадиган маълумотларнинг ўзгаришлардан, чиқариб ташлашлардан, яратиш (киритиш) ва такрор фойдаланишдан муҳофаза қилинишини кафолатлаш усуллари­нинг тақдим этилиши.

Установление подлинности криптографическое

uz - haqiqiylikni kriptografik aniqlash

ҳақиқийликни

криптографик аниқлаш

en - cryptographic authentication

Установление подлинности, основанное на криптографических преобразованиях, использующих симметричное шифрование или шифрование с открытым ключом.

Simmetrik shifrlash yoki ochiq kalit bilan shifrlashdan foydalaniladigan kriptografik o'zgartirishlarga asoslangan holda, haqiqiylikni aniqlash.

Симметрик шифрлаш ёки очик калит билан шифрлашдан фойдаланиладиган криптографик ўзгартиришларга асосланган ҳолда, ҳақиқийликни аниқлаш.

Установление последовательности сообщений

uz - xabarlarning ketma-ketligini aniqlash

хабарларнинг кетма-

кетлигини аниқлаш

en - message sequencing

Установление последовательности сообщений включает: повторное использование сообщений; изменение порядка следования сообщений; передачу сообщений ранее назначенного времени; задержку сообщений.

Xabarlarning ketma-ketligini aniqlash xabarlardan takror foydalanishni; xabarlar borish tartibi o'zgarishini; xabarlarning belgilangan vaqtdan oldin uzatilishini; xabarlarning kechikishini o'z ichiga oladi.

Хабарларнинг кетма-кетлигини аниқлаш хабарлардан такрор фойдаланишни; хабарлар бориш тартиби ўзгаришини; хабарларнинг белгиланган вақтдан олдин узатилишини; хабарларнинг кечикишини ўз ичига олади.

Устойчивость

uz - barqarorlik

барқарорлик

en - robustness

Способность сети сохранять работоспособное состояние во времени и в условиях, создаваемых воздействиями внешних и внутренних дестабилизирующих факторов. Устойчивость характеризуется свойствами надежности и живучести.

Tarmoqning, ichki va tashqi destabillashtiruvchi omillar ta'sirida vujudga keladigan sharoitlar hamda vaqtda ishanlik holatini saqlash qobiliyati. Barqarorlik ishonchlilik va yashovchanlik xususiyatlari bi-

У

lan tavsiflanadi.

Тармоқнинг, ички ва ташқи дестабиллаштирувчи омиллар таъсирида вужудга келадиган шароитлар ҳамда вақтда ишчанлик ҳолатини сақлаш қобилияти. Барқарорлик ишончилилик ва яшовчанлик хусусиятлари билан тавсифланади.

Устройство выдачи сигнала тревоги

uz - trevoga signalini berish qurilmasi

тревога сигналини бериш қурилмаси

en - alert signal transmitting device

Программно-аппаратное устройство, обеспечивающее выдачу звукового и/или светового сигнала на контрольный пост в случае попыток несанкционированного доступа.

Ruxsat etilmagan tarzda foydalanishga urinish boʻlganda, nazorat postiga tovush va/yoki yorugʻlik signali uzatilishini taʼminlovchi dasturiy-apparat qurilma.

Рухсат этилмаган тарзда фойдаланишга уриниш бўлганда, назорат постига товуш ва/ёки ёруғлик сигнали узатилишини таъминловчи дастурий-аппарат қурилма.

Устройство закладное электронное специальное

uz - maxsus oʻrnatiladigan elektron qurilma

махсус ўрнатиладиган электрон қурилма

en - special electronic inset device

Электронное устройство, несанкционированно и замаскировано установленное в техническом средстве обработки информации, чтобы в нужный момент времени обеспечить утечку информации, нарушение ее целостности или блокирование.

Zarur vaqt onida axborotning chiqib ketishini, uning yaxlitligi buzilishini yoki blokirovka qilinishini taʼminlash uchun, ruxsatsiz va yashirin holda texnik vositada oʻrnatilgan elektron qurilma.

Зарур вақт онида ахборотнинг чиқиб кетишини, унинг яхлитлиги бузилишини ёки блокировка қилинишини таъминлаш учун, рухсатсиз ва яширин ҳолда техник воситада ўрнатилган электрон қурилма.

Устройство закладочное

uz - oʻrnatilgan qurilma

ўрнатилган қурилма

en - bug device

Элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование,

У

предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Axborotni olish mumkin bo'lgan joyga (shu jumladan to'siqqa, konstruksiyaga, uskunaga, interyer predmetiga, transport vositalariga, shuningdek, axborotni qayta ishlash texnik vositalariga va tizimiga) yashirin joriy qilinadigan (qo'yiladigan yoki kiritiladigan) axborotni olish vositasining elementi.

Ахборотни олиш мумкин бўлган жойга (шу жумладан тўсиққа, конструкцияга, ускунага, интерьер предметига, транспорт воситаларига, шунингдек, ахборотни қайта ишлаш техник воситаларига ва тизимига) яширин жорий қилинадиган (қўйиладиган ёки киритиладиган) ахборотни олиш воситасининг элементи.

Устройство защиты техническое

uz - texnik muhofaza
qurilmasi

техник муҳофаза
қурилмаси

en - technical protection device

Устройство электронного или другого типа, предотвращающее возможность работы с программой лицам, не имеющим такого устройства.

Elektron yoki boshqa turdagi qurilma. Bunday qurilmaga ega bo'lmagan shaxslarga dastur bilan ishlash imkoniyatini bermaydi.

Электрон ёки бошқа турдаги қурилма. Бундай қурилмага эга бўлмаган шахсларга дастур билан ишлаш имкониятини бермайди.

Устройство защиты электронное

uz - elektron muhofaza
qurilmasi

электрон муҳофаза
қурилмаси

en - dongle

Электронное устройство в составе компьютера, выполняющее функции замка, ответчика и т.п. и предназначенное для защиты программы и данных от несанкционированного доступа.

Kompyuter tarkibidagi qulf, javob bergich va sh.k. funksiyalarni bajaruvchi va dasturni hamda ma'lumotlarni ruxsat etilmagan tarzda foydalanishdan muhofaza qilish uchun mo'ljallangan elektron qurilma.

Компьютер таркибидаги қулф, жавоб бергич ва ш.к. функцияларни бажарувчи ва дастурни ҳамда маълумотларни рухсат этилмаган тарзда фойдаланишдан муҳофаза қилиш учун мўлжалланган

У

Устройство защиты электронное активное

uz - aktiv elektron muhofaza
qurilmasi

актив электрон муҳофаза
қурилмаси

en - active dongle

электрон қурилма.

Электронное устройство защиты, выполненное на основе заказной микросхемы, имеющее электрически программируемую энергонезависимую память и присоединяемое к параллельному порту.

Buyurtma mikrosxema asosida yasalgan, elektr dasturlashtiriladigan energiyaga bog'liq bo'lmagan хотирага эга ва параллел портга уланадиган электрон муҳофаза қурилмаси.

Буюртма микросхема асосида ясалган, электр дастурлаштирилладиган энергияга боғлиқ бўлмаган хотирага эга ва параллел портга уланадиган электрон муҳофаза қурилмаси.

Устройство кодирующее

uz - kodlovchi qurilma

кодловчи қурилма

en - coder

1 Автоматическое или автоматизированное устройство для кодирования программ и данных на носителе информации с целью последующего их ввода в ЭВМ.

2 Устройство для преобразования вида представления информации, в котором каждому входному сигналу соответствует определенная комбинация выходных сигналов, являющихся кодом входного сигнала.

1 Dasturlar va ma'lumotlarni axborot tashuvchisidagi, ularni keyinchalik EHMga kiritish maqsadida kodlash uchun mo'ljallangan avtomatik yoki avtomatlashtirilgan qurilma.

2 Axborotni taqdim etish shaklini o'zgartiruvchi qurilma, bunda har bir kirish signaliga, kirish signalining kodi hisoblanadigan, chiqish signallarining ma'lum kombinatsiyasi mos keladi.

1 Дастурлар ва маълумотларни ахборот ташувчисидаги, уларни кейинчалик ЭҲМга киритиш мақсадида кодлаш учун мўлжалланган автоматик ёки автоматлаштирилган қурилма.

2 Ахборотни тақдим этиш шаклини ўзгартирувчи қурилма, бунда ҳар бир кириш сигналига, кириш сигналнинг коди ҳисобланадиган, чиқиш сигналларининг маълум комбинацияси мос келади.

У

Устройство многоуровневое Функциональный блок, который может одновременно обрабатывать данные двух или более уровней безопасности без риска нарушения компьютерной безопасности.

uz - ko'p darajali qurilma
кўп даражали қурилма

en - multilevel device

Kompyuter xavfsizligining buzilish riski bo'lmagan holda, ikki yoki undan ko'p xavfsizlik darajasidagi ma'lumotlarni bir vaqtning o'zida qayta ishlay olishi mumkin bo'lgan funksional blok.

Компьютер хавфсизлигининг бузилиш rischi бўлмаган ҳолда, икки ёки undan кўп хавфсизлик даражасидаги маълумотларни бир вақтнинг ўзида қайта ишлай олиши мумкин бўлган функционал блок.

Устройство одноуровневое Функциональный блок, который может обрабатывать в данное время данные только одного уровня безопасности.

uz - bir darajali qurilma
бир даражали қурилма

en - single-level device

Berilgan vaqtda bitta xavfsizlik darajasidagi ma'lumotlarni qayta ishlay olishi mumkin bo'lgan funksional blok.

Берилган вақтда битта хавфсизлик даражасидаги маълумотларни қайта ишлай олиши мумкин бўлган функционал блок.

Устройство повышения достоверности идентификации Программно-аппаратное устройство, обеспечивающее корректировку ошибок идентификации, переданных с удаленных терминалов по каналам телекоммуникаций.

uz - identifikatsiyalash
ishonchliligini oshirish
qurilmasi
идентификациялаш
ишончлилигини ошириш
қурилмаси

en - identification integrity
increase device

Примечание – Для корректировки ошибок используются различные способы: обратная посылка сообщений на передающий конец для сравнения его с оригиналом; посылка одновременно с сообщением контрольных разрядов; использование избыточных кодов (код Хемминга, циклические коды) и т.д.

Telekommunikatsiyalar kanallari orqali olisdagi terminallardan uzatilgan identifikatsiya xatolari tuzatilishini ta'minlaydigan dasturiy-apparat qurilma.

Izoh – Xatolarni tuzatish uchun turli usullar; xabarlarni uzatuvchi tomonga original bilan taqqoslash uchun qayta yuborish; xabar bilan bir vaqtda nazorat razryadlarini yuborish; ortiqcha kodlardan (Xemming kodi, siklik kodlar) foydalanish va h.k. qo'llaniladi.

Телекоммуникациялар каналлари орқали олисдаги терминаллардан узатилган идентификация хатолари тузатилишини таъминлайдиган дастурий-аппарат қурилма.

Изоҳ – Хатоларни тузатиш учун турли усуллар; хабарларни узатувчи томонга оригинал билан таққослаш учун қайта юбориш; хабар билан бир вақтда назорат разрядларини юбориш; ортикча кодлардан (Хемминг коди, циклик кодлар) фойдаланиш ва ҳ.к. қўлланилади.

Устройство прерывания программы пользователя

uz - foydalanuvchi dasturini to'xtatib qo'yish qurilmasi
 фойдаланувчи дастурини тўхтатиб қўйиш қурилмаси
en - user program interrupt device

Программно-аппаратное устройство, обеспечивающее прерывание (блокирование) программы пользователя в случае попыток несанкционированного доступа.

Ruxsat etilmagan tarzda foydalanishga urinish bo'lganda, foydalanuvchi dasturining to'xtatib qo'yilishini (blokirovka qilinishini) ta'minlaydigan dasturiy-apparat qurilma.

Рухсат этилмаган тарзда фойдаланишга уриниш бўлганда, фойдаланувчи дастурининг тўхтатиб қўйилишини (блокировка қилинишини) таъминлайдиган дастурий-аппарат қурилма.

Устройство регистрации доступа пользователей

uz - foydalanuvchilarning erkin foydalanishini qayd etish qurilmasi
 фойдаланувчиларнинг эркин фойдаланишини қайд этиш қурилмаси
en - users access registration device

Программно-аппаратное устройство, обеспечивающее регистрацию пользователей при всех их обращениях к системе с указанием номера терминала, даты и времени обращения.

Tizimga qilingan barcha murojaatlar paytida, terminal raqamini, murojaat sanasi hamda vaqtini ko'rsatgan holda, foydalanuvchilarning qayd etilishini ta'minlaydigan dasturiy-apparat qurilma.

Тизимга қилинган барча мурожаатлар пайтида, терминал рақамини, мурожаат санаси ҳамда вақтини кўрсатган ҳолда, фойдаланувчиларнинг қайд этилишини таъминлайдиган дастурий-аппарат қурилма.

Устройство стирания данных

uz - ma'lumotlarni o'chirish

Программно-аппаратное устройство, обеспечивающее стирание оставшихся после обработки данных в оперативном запоминающем устройстве.

У

qurilmasi
маълумотларни ўчириш
қурилмаси
en - data cancellation device

ве путем записи нулей во все ячейки соответствующего блока памяти.

Operativ-xotira qurilmasida qayta ishlashdan keyin qolgan ma'lumotlarning, tegishli xotira blokining barcha yacheykalariga nollar yozish yo'li bilan o'chirilishini ta'minlaydigan dasturiy-apparat qurilma.

Оператив-хотира қурилмасида қайта ишлашдан кейин қолган маълумотларнинг, тегишли хотира блокининг барча ячейкаларига ноллар ёзиш йўли билан ўчирилишини таъминлайдиган дастурий-аппарат қурилма.

Устройство электромагнитного зашумления
uz - elektromagnit shovqin qurilmasi
электромагнит шовқин
қурилмаси
en - electromagnetic noise masking

Широкополосный излучатель (генератор) электромагнитного шума, предназначенный для маскировки (подавления) информационного электромагнитного поля, создаваемого техническими средствами обработки информации, или наводок в токопроводящих коммуникациях, в заданной полосе частот.

Berilgan chastotalar polosasida, axborotni qayta ishlash texnik vositalari vujudga keltiradigan axborot elektromagnit maydonni niqoblash (bostirish) yoki tok o'tkazadigan kommunikatsiyalarda to'g'rilashlar uchun mo'ljallangan keng polosali elektromagnit shovqin nurlatgich (generatori).

Берилган частоталар полосасида, ахборотни қайта ишлаш техник воситалари вужудга келтирадиган ахборот электромагнит майдонни ниқоблаш (бостириш) ёки ток ўтказадиган коммуникацияларда тўғрилашлар учун мўлжалланган кенг полосали электромагнит шовқин нурлатгич (генератори).

Утечка информации
uz - axborotning chiqib ketishi (yo'qolishi)
ахборотнинг чиқиб кетиши (йўқолиши)
en - information loss

Утрата информацией при ее обработке техническими средствами свойства секретности (конфиденциальности) в результате несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

Axborotni texnik vositalar bilan qayta ishlashda, ruxsat etilmagan tarzda tanishish yoki hujjatlashti-

У

rish (nusxa olish) natijasida axborot maxfiylik (konfidensiallik) xususiyatining yo'qolishi.

Ахборотни техник воситалар билан қайта ишлашда, рухсат этилмаган тарзда танишиш ёки ҳужжатлаштириш (нусха олиш) натижасида ахборот махфийлик (конфиденциаллик) хусусиятининг йўқолиши.

Утечка секретной информации

uz - maxfiy axborotning chiqib ketishi (yo'qolishi)

махфий ахборотнинг чиқиб кетиши (йўқолиши)

en - secret information leaking

Неправомерное распространение сведений, составляющих государственную и служебную тайну, за пределы организации или круга лиц, которым эти сведения доверены (обладают).

Davlat va xizmat siri hisoblanadigan ma'lumotlarning, shu ma'lumotlar ishonib topshirilgan (bunday ma'lumotlar bo'lgan) tashkilot yoki shaxslar doirasidan tashqariga noqonuniy tarqatilishi.

Давлат ва хизмат сирини ҳисобланадиган маълумотларнинг, шу маълумотлар ишониб топширилган (бундай маълумотлар бўлган) ташкилот ёки шахслар доирасидан ташқарига ноқонуний тарқатилиши.

Утилиты скрытого администрирования

uz - yashirin boshqarish utilitalari

яширин бошқариш утилиталари

en - latent administration utilities

Программы для осуществления несанкционированного администрирования удаленных компьютеров: приема/отсылки файлов, их запуска или уничтожения, вывода сообщений, удаления информации, перезагрузки компьютера и т.д.

Olisdagi kompyuterlarning ruxsat etilmagan tarzda boshqarilishini amalga oshirish, ya'ni, fayllarni qabul qilish/jo'natish, ularni ishga tushirish yoki yo'q qilish, xabarlarini chiqarish, axborotni o'chirish, kompyuterni qayta yuklash va h.k. uchun mo'ljallangan dasturlar.

Олисдаги компьютерларнинг рухсат этилмаган тарзда бошқарилишини амалга ошириш, яъни, файлларни қабул қилиш/жўнатиш, уларни ишга тушириш ёки йўқ қилиш, хабарларни чиқариш, ахборотни ўчириш, компьютерни қайта юклаш ва ҳ.к. учун мўлжалланган дастурлар.

Уточнение

Добавление деталей в компонент.

у

uz - aniqlamoq
аниқламоқ
en - refinement

Утрата секретных документов или изделий

uz - maxfiy hujjatlar yoki buyumlarni yo'qotish
махфий ҳужжатлар ёки буюмларни йўқотиш
en - secret documents or articles loss

Учет индивидуальный

uz - individual hisobga olish
индивидуал ҳисобга олиш
en - individual accountability

Ущерб

Komponentga detallarni qo'shish.

Компонентга деталларни қўшиш.

Потеря (в том числе временная) документа или изделия лицом, ответственным за их сохранность, являющаяся результатом нарушения установленных правил обращения с ними, вследствие чего эти документы или изделия стали, либо могли стать достоянием посторонних лиц.

Hujjat yoki buyumning, ularning saqlanishi uchun javobgar shaxs tomonidan yo'qotilishi (shu jumladan, vaqtinchalik), bu ular bilan ishlashning belgilangan qoidalarining buzilish natijasi bo'lib, oqibatda bu hujjatlar yoki buyumlar begona shaxslarning mulkiga aylanadi yoki aylanishi mumkin.

Ҳужжат ёки буюмнинг, уларнинг сақланиши учун жавобгар шахс томонидан йўқотилиши (шу жумладан, вақтинчалик), бу улар билан ишлашнинг белгиланган қоидаларининг бузилиш натижаси бўлиб, оқибатда бу ҳужжатлар ёки буюмлар бегона шахсларнинг мулкига айланади ёки айланиши мумкин.

Комплекс мер, за счет которых идентификация пользователя может быть использована для определения возможности доступа пользователя к машинам, материалам и т.п.; правила предоставления пользователю времени, методов и режимов доступа.

Foydalanuvchini identifikatsiya qilishdan uning mashinalar, materiallar va sh.k.lardan foydalana olish imkoniyatini aniqlashda qo'llanilishi mumkin bo'lgan chora-tadbirlar kompleksi; foydalanuvchiga foydalana olish vaqti, metodlari va rejimlarini taqdim etish qoidalari.

Фойдаланувчини идентификация қилишдан унинг машиналар, материаллар ва ш.к.лардан фойдалана олиш имкониятини аниқлашда қўлланилиши мумкин бўлган чора-тадбирлар комплекси; фойдаланувчига фойдалана олиш вақти, методлари ва режимларини тақдим этиш қоидалари.

1 Количественная мера ущерба или убытка, по-

у

uz - zarar
зарар
en - loss

лученного в результате компрометации.
2 Явное повреждение какого-либо из компонентов системы или приведение компонентов системы в неработоспособное состояние, а также различного рода утечки информации и изменение некоторых физических и логических характеристик системы.

1 Obro'sizlantirish natijasida yuzaga kelgan zarar yoki ziyonning miqdor o'lchovi.

2 Tizim komponentlaridan birining ochiq shikastlanishi yoki tizim komponentlarining ishlash qobiliyati yo'qolgan holatga tushib qolishi, shuningdek, axborotning turli ko'rinishda chiqib ketishi hamda tizim ba'zi fizik va mantiqiy xarakteristikalarining o'zgarishi.

1 Обрўсизлантириш натижасида юзага келган зарар ёки зиённинг миқдор ўлчови.

2 Тизим компонентларидан бирининг очик шикастланиши ёки тизим компонентларининг ишлаш қобилияти йўқолган ҳолатга тушиб қолиши, шунингдек, ахборотнинг турли кўринишда чиқиб кетиши ҳамда тизим баъзи физик ва мантиқий хarakterистикаларининг ўзгариши.

Уязвимости потенциальные обнаруженные

uz - aniqlangan potensial
zaifliklar

аниқланган потенциал
заифликлар

en - encountered potential
vulnerabilities

Потенциально уязвимые места ОО, идентифицированные оценщиком при выполнении оценки, которые могут быть использованы для нарушения ФТБ.

BOning, baholash bajarilayotganda baholovchi tomonidan identifikatsiya qilingan, FXT buzilishi uchun ishlatiladigan potensial zaif joylari.

BOning, baholash bajarilayotganda baholovchi tomonidan identifikatsiya qilingan, FXT buzilishi uchun ishlatiladigan potensial zaif joylari.

Уязвимость

uz - yaxshi himoya
qilinmaganlik

яхши ҳимоя
қилинмаганлик

en - vulnerability

1 Недостаток в системе обработки данных, используя который, можно нарушить её целостность и вызвать неправильную работу.

Примечания

1 Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, воздействия вирусов

У

или других вредоносных программ и т.п.

2 Если при наличии уязвимости имеется соответствующая угроза, то существует и риск.

2 Слабость в системных средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для нарушения политики безопасности системы.

3 Ошибка при назначении полномочий или упущение при разработке, реализации или управлении средствами защиты системы, которые могут привести к преодолению защиты.

4 Слабость активов или средств управления, которая может быть использована одной или более угроз.

5 Свойство системы, которое может привести к нарушению ее защиты при наличии угрозы. Уязвимость может возникать случайно из-за неадекватного проектирования или неполной отладки, или может быть результатом злого умысла.

1 Ma'lumotlarni qayta ishlash tizimidagi kamchilik, undan foydalanish tizim yaxlitligi buzilishiga va noto'g'ri ishlashiga olib kelishi mumkin.

Izohlar

1 Yaxshi himoya qilinmaganlik dasturlash xatolari, tizimni loyihalashda yo'l qo'yilgan kamchiliklar, ishonchli bo'lmagan parollar, viruslar yoki boshqa zararli dasturlar ta'sirlari va sh.k. natijasi bo'lishi mumkin.

2 Agar yaxshi himoya qilinmaganlik mavjud bo'lganda tegishli tahdid bo'lsa, unda risk ham mavjud bo'ladi.

2 Tizim xavfsizlik siyosatini buzish uchun qo'llanilishi mumkin bo'lgan, protseduralar, loyihadagi, amalga oshirishdagi, tizimni ichki nazorat qilishdagi xatolar yoki kamchiliklar keltirib chiqargan, tizim muhofaza vositalaridagi kamchilik.

3 Muhofazani yengib o'tishga olib kelishi mumkin bo'lgan, tizimning muhofaza vositalarini ishlab chiqish, amalga oshirish yoki boshqarishdagi yo'qotishlar yoki vakolatlarni tayinlashdagi xato.

4 Aktivlar yoki boshqarish vositalarining bir yoki undan ko'p tahdid foydalanishi mumkin bo'lgan zaifligi.

5 Tizimning tahdid yuzaga kelganda, muhofaza qi-

у

linishi buzilishiga olib keladigan xususiyati. Zaiflik mos darajada loyihalanganlik yoki to'la sozlanmaslik tufayli tasodifan yuzaga kelishi yoki yomon niyat natijasi bo'lishi mumkin.

1 Маълумотларни қайта ишлаш тизимидаги камчилик, ундан фойдаланиш тизим яхлитлиги бузилишига ва нотўғри ишлашига олиб келиши мумкин.

Изоҳлар

1 Яхши ҳимоя қилинмаганлик дастурлаш хатолари, тизимни лойиҳалашда йўл қўйилган камчиликлар, ишончли бўлмаган пароллар, вируслар ёки бошқа зарарли дастурлар таъсирлари ва ш.к. натижаси бўлиши мумкин.

2 Агар яхши ҳимоя қилинмаганлик мавжуд бўлганда тегишли таҳдид бўлса, унда риск ҳам мавжуд бўлади.

2 Тизим хавфсизлик сиёсатини бузиш учун қўлланилиши мумкин бўлган, процедуралар, лойиҳадаги, амалга оширишдаги, тизимни ички назорат қилишдаги хатолар ёки камчиликлар келтириб чиқарган, тизим муҳофаза воситаларидаги камчилик.

3 Муҳофазани енгиб ўтишга олиб келиши мумкин бўлган, тизимнинг муҳофаза воситаларини ишлаб чиқиш, амалга ошириш ёки бошқаришдаги йўқотишлар ёки ваколатларни тайинлашдаги хато.

4 Активлар ёки бошқариш воситаларининг бир ёки ундан кўп таҳдид фойдаланиши мумкин бўлган заифлиги.

5 Тизимнинг таҳдид юзага келганда, муҳофаза қилиниши бузилишига олиб келадиган хусусияти. Заифлик мос даражада лойиҳаланмаслик ёки тўла созланмаслик тўғрисида тасодифан юзага келиши ёки ёмон ният натижаси бўлиши мумкин.

Уязвимость автоматизированной системы

uz - avtomatlashtirilgan tizimning zaifligi

автоматлаштирилган тизимнинг заифлиги

Любая характеристика автоматизированной системы, использование которой нарушителем может привести к реализации угрозы.

Avtomatlashtirilgan tizimning, buzg'unchining undan foydalanishi tahdidni amalga oshirishga olib

у

en - automated system vulnerability

kelishi mumkin bo'lgan har qanday xarakteristikasi.

Автоматлаштирилган тизимнинг, бузғунчининг ундан фойдаланиши тахдидни амалга оширишга олиб келиши мумкин бўлган ҳар қандай хarakteristikasi.

Уязвимость доступная

uz - foydalana olinadigan zaiflik

фойдалана олинадиган заифлик

en - exploitable vulnerability

Уязвимое место ОО, которое может быть использовано для нарушения ФТБ в среде функционирования ОО.

ВОning ishlash muhitida FXT buzilishi uchun ishlatiladigan, ВОning zaif joyi.

БОнинг ишлаш мухитида ФХТ бузилиши учун ишлатиладиган, БОнинг заиф жойи.

Уязвимость информации

uz - axborotning zaifligi

ахборотнинг заифлиги

en - information vulnerability

Подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению ее конфиденциальности, целостности, доступности или неправомерному ее тиражированию.

Axborotning, uning konfidensialligi, yaxlitligi, undan erkin foydalanish mumkinligi buzilishiga va noqonuniy tarzda ko'paytirilishiga olib kelishi mumkin bo'lgan turli destabillashtiruvchi omillar ta'siriga moyilligi.

Ахборотнинг, унинг конфиденциаллиги, яхлитлиги, ундан эркин фойдаланиш мумкинлиги бузилишига ва ноқонуний тарзда кўпайтирилишига олиб келиши мумкин бўлган турли дестабилаштирувчи омиллар таъсирига мойиллиги.

Уязвимость нулевого дня

uz - nolinchí kun zaifligi

нолинчи кун заифлиги

en - zero day exploit

Вредоносная программа или уязвимость, против которой еще не разработаны защитные механизмы.

Himoya mexanizmlari hali ishlab chiqilmagan zararli dastur yoki zaiflik.

у

	<p>Ҳимоя механизмлари ҳали ишлаб чиқилмаган зарарли дастур ёки заифлик.</p>
<p>Уязвимость остаточная uz - qoldiq zaiflik қолдиқ заифлик en - residual vulnerability</p>	<p>Непригодное для использования уязвимое место в среде функционирования ОО, но которое может быть использовано для нарушения ФТБ нарушителем с более высоким потенциалом атаки, чем который предполагается для predetermined среды функционирования ОО.</p>
	<p>BO ishlash sohasidagi foydalanish uchun yaroqsiz boʻlgan, biroq buzgʻunchi tomonidan BO ishlashining oldindan belgilangan muhiti uchun moʻljallanganiga qaraganda, yuqori hujum potentsiali bilan FXT buzilishi uchun ishlatilishi mumkin boʻlgan zaif joy.</p>
	<p>BO ishlash sohasidagi foydalanish uchun yaroqsiz boʻlgan, biroq buzgʻunchi tomonidan BO ishlashining oldindan belgilangan muhiti uchun moʻljallanganiga qaraganda, yuqori hujum potentsiali bilan FXT buzilishi uchun ishlatilishi mumkin boʻlgan zaif joy.</p>
<p>Уязвимость потенциальная uz - potensial zaiflik потенциал заифлик en - potential vulnerability</p>	<p>Предполагаемое, но не подтвержденное уязвимое место. Примечание – Предположение основывается на предполагаемой возможности атаки с целью изменения ФТБ.</p>
	<p>Taxmin qilinayotgan lekin tasdiqlanmagan zaif joy. Izoh – FXTni oʻzgartirish maqsadida, hujumlarning boʻlish ehtimoli taxminiga asoslanadi.</p>
	<p>Taxmin qilinayotgan lekin tasdiqlanmagan zaif joy. Izoh – FXTni oʻzgartirish maqsadida, hujumlarning boʻlish ehtimoli taxminiga asoslanadi.</p>
<p>Уязвимость сетевой службы uz - tarmoq xizmatining zaifligi тармоқ хизматининг заифлиги en - vulnerability of network service</p>	<p>Дефект соответствующего программного обеспечения, за счёт использования которого потенциально могут быть реализованы: переполнение буфера, уязвимость к DoS-атакам, ошибочная конфигурация службы, слабая парольная защита, возможность повышения привилегий пользовате-</p>

У

ля, SQL-инъекция, инъекция кода, межсайтовое выполнение скриптов.

Tegishli dasturiy ta'minot nuqsoni, undan foydalanish hisobiga quyidagilarni amalga oshirish mumkin: buferning to'lib ketishi, DoS-hujumlardan bo'sh himoyalanganlik, xizmatning xato konfiguratsiyasi, kuchsiz parolli himoya, foydalanuvchining imtiyozlarini oshirish imkoniyati, SQL-in'eksiya, kod in'eksiyasi, skriptlarni saytlararo bajarish.

Тегишли дастурий таъминот нуқсони, ундан фойдаланиш ҳисобига қуйидагиларни амалга ошириш мумкин: буфернинг тўлиб кетиши, DoS-хужумлардан бўш ҳимояланганлик, хизматнинг хато конфигурацияси, кучсиз паролли ҳимоя, фойдаланувчининг имтиёзларини ошириш имконияти, SQL-инъекция, код инъекцияси, скриптарни сайтлараро бажариш.

Уязвимость субъекта информационных отношений

uz - axborot munosabatlari subyektining zaifligi

ахборот муносабатлари субъектининг заифлиги

en - vulnerability of information relapse

Потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, ее носители и процессы ее обработки.

Subyektning, uning uchun kritik bo'lgan axborotga, uni tashuvchilarga va qayta ishlash jarayonlariga ta'sir etish vositasida, hayotiy muhim manfaatlariga zarar yetkazilishiga potensial yo'liqishi.

Субъектнинг, унинг учун критик бўлган ахборотга, уни ташувчиларга ва қайта ишлаш жараёнларига таъсир этиш воситасида, ҳаётий муҳим манфаатларига зарар етказилишига потенциал йўлиқиши.

Ф

Файл архивный

uz - arxivga oid fayl

архивга оид файл

en - archive file

Файл, сохраняемый для более позднего изучения или верификации, для безопасности или любой другой цели.

Keyinroq o'rganish yoki verifikatsiya (asl nusxa)

Ф

uchun, xavfsizlik yoki istalgan boshqa maqsad uchun saqlanadigan fayl.

Кейинроқ ўрганиш ёки верификация (асл нусха) учун, хавфсизлик ёки исталган бошқа мақсад учун сақланадиган файл.

Файл заархивированный

uz - arxivlashtirilgan fayl

архивлаштирилган файл

en - archived file

Файл, для которого существует архивный файл.

Arxivlangan fayli mavjud boʻlgan fayl.

Архивланган файли мавжуд бўлган файл.

Файл защищенный

uz - muhofaza qilingan fayl

муҳофаза қилинган файл

en - protected file

Файл, для доступа к записям которого необходимо ввести пароль.

Yozuvlaridan foydalana olish uchun parol kiritilishi zarur boʻlgan fayl.

Ёзувларидан фойдалана олиш учун пароль киритилиши зарур бўлган файл.

Файл контрольной проверки

uz - nazorat tekshiruv fayli

назорат текширув файли

en - checking file

Файл, созданный оператором с целью подготовки данных для проверки.

Operator tomonidan ma'lumotlarni tekshirish uchun tayyorlash maqsadida yaratilgan fayl.

Оператор томонидан маълумотларни текшириш учун тайёрлаш мақсадида яратилган файл.

Файл неотображаемый

uz - aks ettirilmaydigan

fayl

акс эттирилмайдиган

файл

en - invisible file

Дисковый файл, который не указывается в справочнике диска на экране дисплея.

Displey ekranidagi disk spravochnigida ko'rsatilmaydigan disk fayli.

Дисплей экранидаги диск справочнигида кўрсатилмайдиган диск файли.

Файл резервный

uz - rezerv fayl

резерв файл

en - backup file

Файл, создаваемый для возможно более поздней реставрации данных. Например, копия файла, сохраняемая в резервном пункте обработки данных.

Ф

Ma'lumotlarni mumkin qadar keyinroq tiklash uchun yaratilgan fayl. Masalan, ma'lumotlarni qayta ishlash rezerv punktida saqlanadigan fayl nusxasi.

Маълумотларни мумкин қадар кейинроқ тиклаш учун яратилган файл. Масалан, маълумотларни қайта ишлаш резерв пунктида сақланадиган файл нусхаси.

Фактор воздействующий внешний

uz - ta'sir etuvchi tashqi omil

таъсир этувчи ташқи омил

en - external influencing factor

Внешнее воздействие на информацию или ее носитель, приводящее к искажению, уничтожению или блокированию защищаемой информации.

Muhofaza qilinadigan axborotning buzib ko'rsatilishiga, yo'q qilinishiga yoki blokirovkalanishiga olib keluvchi, axborotga yoki uni tashuvchiga ko'rsatiladigan tashqi ta'sir.

Муҳофаза қилинадиган ахборотнинг бузиб кўрсатилишига, йўқ қилинишига ёки блокировканишига олиб келувчи, ахборотга ёки уни ташувчига кўрсатиладиган ташқи таъсир.

Фактор, воздействующий на защищаемую информацию

uz - muhofaza qilinadigan axborotga ta'sir ko'rsatuvchi omil

муҳофаза қилинадиган

ахборотга таъсир кўрсатувчи омил

en - factor, acting upon protectable information

Явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Muhofaza qilinadigan axborot chiqib ketishi, buzib ko'rsatilishi, yo'q qilinishi, undan foydalana olish blokirovkalanishi mumkin bo'lgan hodisa, harakat yoki jarayon.

Муҳофаза қилинадиган ахборот чиқиб кетиши, бузиб кўрсатилиши, йўқ қилиниши, ундан фойдалана олиш блокировканиши мумкин бўлган ҳодиса, ҳаракат ёки жараён.

Фактор дестабилизирующий

uz - destabillashtiruvchi omil

дестабиллаштирувчи

1 Явление или событие, нарушившее конфиденциальность, целостность и/или доступность информационных ресурсов, нарушение работоспособности сети или ее элементов. Например, угроза информационной безопасности.

Ф

омил

en - destabilizing factor

2 Воздействие на сеть телекоммуникаций, источником которого является физический или технологический процесс внутреннего или внешнего по отношению к сети телекоммуникаций характера, приводящее к выходу из строя элементов сети.

1 Yuz berishi oqibatida axborot resurslarining konfidensialligi, yaxlitligi va/yoki ulardan erkin foydalanish, tarmoq yoki tarmoq elementlari ish qobiliyatlari buzilishi mumkin bo'lgan voqea yoki hodisa. Masalan, axborot xavfsizligiga tahdid.

2 Manbai telekommunikatsiyalar tarmog'iga nisbatan ichki yoki tashqi xarakterdagi fizik yoki texnologik jarayon bo'lgan, tarmoq elementlarining ishdan chiqishiga olib keladigan ta'sir.

1 Юз бериши оқибатида ахборот ресурсларининг конфиденциаллиги, яхлитлиги ва/ёки улардан эркин фойдаланиш, тармоқ ёки тармоқ элементлари иш қобилиятлари бузилиши мумкин бўлган воқеа ёки ҳодиса. Масалан, ахборот хавфсизлигига таҳ-дид.

2 Манбаи телекоммуникациялар тармоғига нисбатан ички ёки ташқи характердаги физик ёки технологик жараён бўлган, тармоқ элементларининг ишдан чиқишига олиб келадиган таъсир.

**Фактор дестабилизи-
рующий внешний**

uz - tashqi destabillashtiruvchi
omil

ташқи дестабиллаш-
тирувчи омил

en - external destabilizing factor

Дестабилизирующий фактор, источник которого расположен вне сети телекоммуникаций.

Manbai telekommunikatsiyalar tarmog'idan tashqari-
da joylashgan destabillashtiruvchi omil.

Манбаи телекоммуникациялар тармоғидан таш-
қарида жойлашган дестабиллаштирувчи омил.

**Фактор дестабилизи-
рующий внутренний**

uz - ichki destabillashtiruvchi
omil

Дестабилизирующий фактор, источник которого расположен внутри сети телекоммуникаций или ее элементов.

Ф

ички дестабиллаштирувчи
омил
en - internal destabilizing factor

Manbai telekommunikatsiyalar tarmog'ining yoki uning elementlarining ichida joylashgan detsillashtiruvchi omil.

Манбаи телекоммуникациялар тармоғининг ёки унинг элементларининг ичида жойлашган дестабиллаштирувчи омил.

Фактор опасности

uz - xavf omili
хавф омили
en - treat factor

Причина, обуславливающая появление угроз для безопасности информации при ее обработке техническими средствами.

Примечание – Основными факторами опасности для информации, обрабатываемой техническими средствами, являются: побочные электромагнитные излучения и наводки; несанкционированный доступ к информации штатными техническими средствами; специальные электронные закладные устройства (аппаратные закладки); внешние воздействия на информационный ресурс.

Axborotni texnik vositalar bilan qayta ishlashda, uning xavfsizligi uchun tahdidlar paydo bo'lishini shartlovchi sabab.

Izoh – Yondosh elektromagnit nurlanishlar va to'g'rilashlar, axborotdan shtat texnik vositalari bilan ruxsat etilmagan tarzda foydalanish, maxsus elektron o'rnatuvchi qurilmalar; axborot resursiga bo'ladigan tashqi ta'sirlar texnik vositalar bilan qayta ishlanadigan axborot uchun asosiy xavf omillari hisoblanadi.

Axborotni texnik vositalar bilan qayta ishlashda, uning xavfsizligi uchun tahdidlar paydo bo'lishini shartlovchi sabab.

Izoh – Yondosh elektromagnit nurlanishlar va to'g'rilashlar, axborotdan shtat texnik vositalari bilan ruxsat etilmagan tarzda foydalanish, maxsus elektron o'rnatuvchi qurilmalar; axborot resursiga bo'ladigan tashqi ta'sirlar texnik vositalar bilan qayta ishlanadigan axborot uchun asosiy xavf omillari hisoblanadi.

Фальсификация

uz - soxtalashtirish
soxtalashtirish
en - falsification

Использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, используя ее IP-адрес.

Ф

Boshqa tizim ostida niqoblanish yordamida, uning IP-adresidan foydalanib, IP-adreslar asosida erkin foydalanishni boshqarish tizimlarini chetlab o'tish uchun turli texnologiyalardan foydalanish.

Бошқа тизим остида ниқобланиш ёрдамида, унинг IP-адресидан фойдаланиб, IP-адреслар асосида эркин фойдаланишни бошқариш тизимларини четлаб ўтиш учун турли технологиялардан фойдаланиш.

Фиксация авторства

uz - mualliflikni qayd etish

муаллифликни қайд этиш

en - non-repudiation

1 Способность предотвратить последующее непризнание отправителем факта отправки сообщения или выполнения действия.

2 Защита от отказа признания одним из участвующих в сеансе связи объектов участия во всем или в части сеанса связи.

3 Процесс, обеспечивающий невозможность непризнания отправителем сообщения (например, запроса на услугу «разовая плата за просмотр программы») факта его направления.

1 Jo'natuvchining xabarni jo'natish yoki harakatni bajarish faktini keyinchalik tan olmasligini bartaraf qilish qobiliyati.

2 Obyektlarning aloqa seansida ishtirok etuvchilardan biri tomonidan, aloqa seansining barchasida yoki bir qismida ishtirok etganlikni tan olishni rad etishdan muhofaza qilish.

3 Jo'natuvchi tomonidan xabarni, (masalan, «dasturni ko'rish uchun bir martalik to'lov» xizmatiga so'rov) uning jo'natish faktini tan olmaslik mumkin emasligini ta'minlash jarayoni.

1 Жўнатувчининг хабарни жўнатиш ёки ҳаракатни бажариш фактини кейинчалик тан олмаслигини бартараф қилиш қобилияти.

2 Объектларнинг алоқа сеансида иштирок этувчилардан бири томонидан, алоқа сеансининг барчасида ёки бир қисмида иштирок этганликни тан олишни рад этишдан муҳофаза қилиш.

3 Жўнатувчи томонидан хабарни, (масалан,

Ф

«дастурни кўриш учун бир марталик тўлов» хизматига сўров) унинг жўнатиш фактини тан олмаслик мумкин эмаслигини таъминлаш жараёни.

Фиксация контроля средств защиты

uz - muhofaza vositalari nazorat qilinishini qayd etish

муҳофаза воситалари назорат қилинишини қайд этиш

en - security audit trail

Совокупность сведений о состоянии средств защиты, накапливаемых во времени и предназначенных для упрощения управления средствами защиты.

Vaqt bo'yicha to'planadigan va muhofaza vositalarini boshqarishni soddallashtirish uchun mo'ljallangan, muhofaza vositalarining holati to'g'risidagi ma'lumotlar jami.

Вақт бўйича тўпланадиган ва муҳофаза воситаларини бошқаришни соддалаштириш учун мўлжалланган, муҳофаза воситаларининг ҳолати тўғрисидаги маълумотлар жами.

Философия защиты

uz - muhofaza falsafasi

муҳофаза фалсафаси

en - protection philosophy

Общая схема системы в целом, позволяющая видеть использование механизмов защиты (формальными и неформальными методами).

Muhofaza mexanizmlaridan foydalanishni (rasmiy yoki norasmiy metodlar bilan) ko'rishga imkon beruvchi, tizimning to'la umumiy sxemasi.

Муҳофаза механизмларидан фойдаланишни (расмий ёки норасмий методлар билан) кўришга имкон берувчи, тизимнинг тўла умумий схемаси.

Фильтр безопасности

uz - xavfsizlik filtri

хавфсизлик фильтри

en - security filter

Доверенная компьютерная система, которая реализует политику безопасности для данных, циркулирующих в системе.

Tizimda aylanuvchi ma'lumotlarning xavfsizlik siyosatini amalga oshiradigan ishonchli kompyuter tizimi.

Тизимда айланувчи маълумотларнинг хавфсизлик сиёсатини амалга оширадиган ишончли компьютер тизими.

Фильтрация входящего трафика

uz - kiruvchi trafikni

Сортировка входящего трафика маршрутизатора с отбрасыванием пакетов, адреса отправителей которых не используются в общем сетевом ад-

Ф

filtrlash

кирувчи трафикни

фильтраш

en - ingress filtering

Фильтрация исходящего трафика

uz - chiquvchi trafikni

filtrlash

чикувчи трафикни

фильтраш

en - egress filtering

Фишинг

uz - fishing

фишинг

en - phishing

ресном пространстве.

Joʻnatuvchilarning adreslaridan umumiy tarmoq adres maydonida foydalanilmaydigan paketlarni tashlab yuborish bilan, marshrutizatorning kiruvchi trafigini saralash.

Жўнатувчиларнинг адресларидан умумий тармоқ адрес майдонида фойдаланилмайдиган пакетларни ташлаб юбориш билан, маршрутизаторнинг кирувчи трафигини саралаш.

Сортировка исходящего трафика маршрутизатора с отбрасыванием пакетов, адреса отправителей которых не включены в диапазон адресов, используемых во внутренней сети.

Joʻnatuvchilarning adreslari ichki tarmoqda foydalaniladigan adreslar diapazoniga kiritilmagan paketlarni tashlab yuborish bilan, marshrutizatorning chiquvchi trafigini saralash.

Жўнатувчиларнинг адреслари ички тармоқда фойдаланиладиган адреслар диапазонида киритилмаган пакетларни ташлаб юбориш билан, маршрутизаторнинг чикувчи трафигини саралаш.

1 Вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Примечание – Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей.

2 Одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

1 Maqsadi foydalanuvchilarning konfidensial maʼlumotlari – loginlari va parollariga kirish hisoblanadigan Internet-firibgarlik turi.

Izoh – Bunga mashhur brendlar nomidan elektron xatlarni ommaviy yuborish orqali, shuningdek, turli servislarning ichi-

Ф

da shaxsiy xabarlar orqali erishiladi, masalan, bank nomidan yoki sotsial tarmoq ichida.

2 Sotsial injeneriyaning turli ko‘rinishlaridan biri, foydalanuvchilarning tarmoq xavfsizligi asoslarini bilmasligiga asoslangan: xususan, ko‘pchilik oddiy faktni bilmaydi: servislar o‘zining hisob ma’lumotlari, parol yoki boshqa xabarlarni berish haqidagi xatlarni jo‘natmaydi.

1 Мақсади фойдаланувчиларнинг конфиденциал маълумотлари – логинлари ва паролларига кириш ҳисобланадиган интернет-фирибгарлик тури.

Изоҳ – Бунга машхур брендлар номидан электрон хатларни оммавий юбориш орқали, шунингдек, турли сервисларнинг ичида шахсий хабарлар орқали эришилади, масалан, банк номидан ёки социал тармоқ ичида.

2 Социал инженериянинг турли кўринишларидан бири, фойдаланувчиларнинг тармоқ хавфсизлиги асосларини билмаслигига асосланган: хусусан, кўпчилик оддий фактни билмайди: сервислар ўзининг ҳисоб маълумотлари, парол ёки бошқа хабарларни бериш ҳақидаги хатларни жўнатмайди.

Флаг

uz - bayroq
байроқ

en - flag

Часть формата элемента данных из одного или нескольких битов, которые определяют статус этого элемента.

Bir yoki bir nechta bitdan iborat ma’lumotlar elementi formatining bir qismi. Bitlar bu elementning statusini belgilaydi.

Бир ёки бир нечта битдан иборат маълумотлар элементи форматининг бир қисми. Битлар бу элементнинг статусини белгилайди.

Формальный

uz - rasmiy
расмий

en - formal

Выраженный на языке с ограниченным синтаксисом и определенный семантикой, основанной на установившихся математических понятиях.

Belgilangan matematik tushunchalarga asoslanib, cheklangan sintaksis va aniqlangan semantika tilida ifodalangan.

Белгиланган математик тушунчаларга асосланиб, чекланган синтаксис ва аниқланган семантика тилида ифодаланган.

Ф

Формат диска

uz - disk formati

диск формати

en - disk format

Способ размещения информации на гибком диске, обеспечивающий идентификацию, контроль и верификацию данных.

Axborotni egiluvchan diskda joylashtirish usuli. Ma'lumotlarning identifikatsiya, nazorat va verifikatsiya qilinishini ta'minlaydi.

Ахборотни эгилувчан дискда жойлаштириш усули. Маълумотларнинг идентификация, назорат ва верификация қилинишини таъминлайди.

Фрод внутренний

uz - ichki frod

ички фрод

en - internal fraud

Вид криминальной деятельности, когда служащие используют свое служебное положение для получения выгоды лично или через третьих лиц путем передачи им сведений конфиденциального характера.

Jinoiy faoliyat turi bo'lib, xizmatchilar o'zlarining xizmat mavqelaridan shaxsan yoki uchinchi shaxslar orqali, ularga konfidensial xarakterdagi ma'lumotlarni berish yo'li bilan manfaat ko'rishda foydalanadilar.

Жиноий фаолият тури бўлиб, хизматчилар ўзларининг хизмат мавқеларидан шахсан ёки учинчи шахслар орқали, уларга конфиденциал характердаги маълумотларни бериш йўли билан манфаат кўришда фойдаланадилар.

Фрод хакерский

uz - hakerlik frodi

хакерлик фроди

en - hacking fraud

Вид мошенничества, связанный со взломом защиты сети и получением несанкционированного доступа к сетевым ресурсам.

Tarmoq muhofazasini buzish va tarmoq resurslaridan ruxsat etilmagan tarzda foydalanish bilan bog'liq firibgarlik turi.

Тармоқ муҳофазасини бузиш ва тармоқ ресурсларидан рухсат этилмаган тарзда фойдаланиш билан боғлиқ фирибгарлик тури.

Фрод, основанный на услуге переадресации вызова

uz - chaqiruvni qayta yo'llash

Метод получения якобы «легального» дохода, основанный на переадресации дорогостоящих вызовов на собственные каналы, как правило, развер-

Ф

xizmatiga asoslangan frod
чақирувни қайта йўллаш
хизматига асосланган фрод
en - premium rate service fraud,
PRS fraud

Фродастер
uz - frodaster
фродастер
en - fraudster

**Функции безопасности
объекта оценки**
uz - baholash obyektining
xavfsizlik funksiyalari
баҳолаш объектининг
хавфсизлик функциялари
en - security functions of
object evaluation

Функционирование
uz - ishlamoq
ишламоқ
en - operation

нутые в других странах.

Go'yoki, «qonuniy» daromad olish metodi bo'lib, odatda, boshqa mamlakatlarda tashkil etilgan o'z kanallariga qimmat chaqiruvlarni qayta yo'llashga asoslangan.

Гўёки, «қонуний» даромад олиш методи бўлиб, одатда, бошқа мамлакатларда ташкил этилган ўз каналларига қиммат чақирувларни қайта йўллашга асосланган.

Лицо, пользующееся услугами мобильной связи без их оплаты или получающее какие-либо иные выгоды.

Mobil aloqa xizmatlaridan, ularning haqini to'lamasdan foydalanuvchi yoki qandaydir boshqacha foyda oladigan shaxs.

Мобил алоқа хизматларидан, уларнинг ҳақини тўламасдан фойдаланувчи ёки қандайдир бошқача фойда оладиган шахс.

Совокупность всех функций безопасности объекта оценки, направленных на осуществление политики безопасности объекта оценки.

Baholash obyektining xavfsizlik siyosatini amalga oshirishga yo'naltirilgan, baholash obyektining barcha xavfsizlik funksiyalari yig'indisi.

Баҳолаш объектининг хавфсизлик сиёсатини амалга оширишга йўналтирилган, баҳолаш объектининг барча хавфсизлик функциялари йиғиндиси.

Стадия использования ОО, включающая его «обычное использование», администрирование и эксплуатацию после поставки и подготовки.

BOdan foydalanish bosqichi yetkazib berish va tayyorlashdan keyin «odatdagi foydalanish», boshqarish va ishlatishni ichiga oladi.

BOdan фойдаланиш босқичи етказиб бериш ва тайёрлашдан кейин «одатдаги фойдаланиш», бошқариш ва ишлатишни ичига олади.

Ф

Функция измерения

uz - o'lchash funksiyasi

ўлчаш функцияси

en - measurement function

Алгоритм или формула, посредством которых производится объединение двух или более основных мер.

Algoritm yoki formula, uning yordamida ikkita yoki undan ko'p asosiy o'lchovning birlashtirilishi amalga oshiriladi.

Алгоритм ёки формула, унинг ёрдамида иккита ёки ундан кўп асосий ўлчовнинг бирлаштирилиши амалга оширилади.

Функция односторонняя

uz - bir tomonlama funksiya

бир томонлама функция

en - one-sided function

Функция, для которой по заданному аргументу x легко вычислить значение функции $f(x)$, тогда как определение x из $f(x)$ трудно вычислимо. До сих пор строго не доказано, что односторонние функции существуют. Для шифрования информации односторонние функции не применимы, т.к. расшифровать текст, зашифрованный с их помощью, не сможет даже законный владелец. В криптографии используются однонаправленные функции с секретом.

Berilgan x argument bo'yicha $f(x)$ funksiya qiymati oson hisoblab chiqariladigan funksiya. $f(x)$ ni x dan hisoblab chiqarish anchagina murakkab. Hozirgacha bir tomonlama funksiyalarning mavjudligi qat'iy isbotlanmagan. Axborotni shifrlash uchun bir tomonlama funksiyalarni qo'llab bo'lmaydi, chunki ular yordamida shifrlangan matnni, hatto uning qonuniy egasi ham rasshifrovka qila olmaydi. Kriptografiyada siri bo'lgan bir tomonlama funksiyadan foydalaniladi.

Берилган x аргумент бўйича $f(x)$ функция қиймати осон ҳисоблаб чиқариладиган функция. $f(x)$ ни x дан ҳисоблаб чиқариш анчагина мураккаб. Ҳозиргача бир томонлама функцияларнинг мавжудлиги қатъий исботланмаган. Ахборотни шифрлаш учун бир томонлама функцияларни қўллаб бўлмайди, чунки улар ёрдамида шифрланган матнни, ҳатто унинг қонуний эгаси ҳам расшифровка қила

Ф

олмайди. Криптографияда сирин бўлган бир томонлама функциядан фойдаланилади.

Функция односторонняя с секретом

uz - siri bo'lgan bir tomonlama funksiya

сирин бўлган бир томонлама функция

en - one-sided secret function

Функция $f_k(x)$, зависящая от параметра k , такая что, при известном k можно найти полиномиальные алгоритмы E_k и D_k , позволяющие легко вычислить $f_k(x)$ для всех x и $f_k^{-1}(y)$ для всех y , а нахождение $f_k^{-1}(y)$ без знания k трудно вычислимо (полиномиального алгоритма не существует) даже при известном алгоритме E_k . На основе понятия односторонней функции с секретом был предложен принцип открытого распределения ключей и, как следствие, криптосистемы с открытым ключом.

k parametrğa bog'liq bo'lgan $f(x)$ funksiya, bu shunday funksiya, k ma'lum bo'lganda, barcha x lar uchun $f_k(x)$ ni, barcha y lar uchun $f_k^{-1}(y)$ ni oson hisoblab chiqarish imkonini beradigan E_k va D_k polinomial algoritmlarni topish mumkin. k ni bilmasdan turib, $f_k^{-1}(y)$ ni topish, hatto E_k algoritmi ma'lum bo'lganda ham, hisoblab chiqarish murakkab bo'lgan vazifa (polinomial algoritmi mavjud emas). Siri bo'lgan bir tomonlama funksiya tushunchasi asosida, kalitlarni ochiq taqsimlash, uning natijasida ochiq kalitli kriptotizim prinsipi taklif qilingan.

k parametrğa boғliq бўлган $f(x)$ функция, бу шундай функция, k маълум бўлганда, барча x лар учун $f_k(x)$ ни, барча y лар учун $f_k^{-1}(y)$ ни оson ҳисоблаб чиқариш имконини берадиган E_k ва D_k полиномиал алгоритмларни топиш мумкин. k ни билмасдан туриб, $f_k^{-1}(y)$ ни топиш, ҳатто E_k алгоритми маълум бўлганда ҳам, ҳисоблаб чиқариш мураккаб бўлган вазифа (полиномиал алгоритми мавжуд эмас). Сирин бўлган бир томонлама функция тушунчаси асосида, калитларни очик тақсимлаш, унинг натижасида очик калитли кriptotizim принципи таклиф қилинган.

Функция шифрования

uz - shifrlash funksiyasi

шифрлаш функцияси

Функция, используемая в шифре для преобразования данных с применением ключа.

Ф

en - encryption function

Shifrdada ma'lumotlarni kalit qo'llanilgan holda o'zgartirish uchun foydalaniladigan funktsiya.

Шифрда маълумотларни калит қўлланилган ҳолда ўзгартириш учун фойдаланиладиган функция.

Х

Хост-бастион

uz - xost-bastion

хост-бастион

en - bastion host

Компьютер-шлюз, на котором работает программное обеспечение межсетевого экрана и который устанавливается между внутренней и внешней сетями. К хост-бастионам можно отнести шлюзы сеансового и прикладного уровней, а также межсетевые экраны, использующие технологию Stateful inspection.

Tarmoqlararo ekranning dasturiy ta'minoti ishlaydigan va ichki hamda tashqi tarmoqlar o'rtasida o'rnatiladigan kompyuter-shlyuz. Xost-bastionlarga seans va amaliy darajadagi shlyuzlarni, shuningdek, *Stateful inspection* texnologiyasidan foydalanuvchi tarmoqlararo ekranlarni kiritish mumkin.

Tarmoqlararo ekranning dasturiy ta'minoti ishlaydigan va ichki hamda tashqi tarmoqlar o'rtasida o'rnatiladigan kompyuter-shlyuz. Xost-bastionlarga seans va amaliy darajadagi shlyuzlarni, shuningdek, *Stateful inspection* texnologiyasidan foydalanuvchi tarmoqlararo ekranlarni kiritish mumkin.

Хэш

uz - xesh

хэш

en - hash

Блок данных фиксированного размера, полученный в результате хэширования массива данных.

Ma'lumotlar massivini xeshlash natijasida olingan, qat'iy o'lchamdagi ma'lumotlar bloki.

Ma'lumotlar massivini xeshlash natijasida olingan, qat'iy o'lchamdagi ma'lumotlar bloki.

Хэш-алгоритм защищенный

uz - muhofazalangan

xesh-algoritm

Хэш-алгоритм, позволяющий генерировать электронные подписи.

Elektron imzolarni generatsiyalash imkonini beradi-

Х

муҳофазаланган
хэш-алгоритм
en - secure hash algorithm

Хэширование

uz - xeshlash
хэшлаш
en - hashing

gan xesh-algorithm.

Электрон имзоларни генерациялаш имконини берадиган хэш-алгоритм.

1 Процесс вычисления значения хэш-функции.
2 Преобразования массива данных произвольного размера в блок данных фиксированного размера, служащий заменителем исходного массива в некоторых контекстах.

1 Xesh-funksiya qiymatlarini hisoblash jarayoni.
2 Ba'zi bir matn bo'laklarida dastlabki massivning o'rni bosishga xizmat qiluvchi ixtiyoriy o'lchamdagi ma'lumotlar massivini belgilangan o'lchamdagi ma'lumotlar blokiga almashtirish.

1 Хэш-функция қийматларини ҳисоблаш жараёни.
2 Баъзи бир матн бўлақларида дастлабки массивнинг ўрнини босишга хизмат қилувчи ихтиёрий ўлчамдаги маълумотлар массивини белгиланган ўлчамдаги маълумотлар блокига алмаштириш.

Хэш-функция (функция хэширования)

uz - xesh-funksiya (xeshlash funksiyasi)
хэш-функция (хэшлаш функцияси)
en - hash-function

1 Функция, отображающая строку бит в строку бит фиксированной длины.
2 Математическое преобразование массива данных произвольного размера и вычисление для него фиксированной уникальной последовательности небольшой длины.

1 Bitlar satrini belgilangan uzunlikdagi bitlar satriga aylantirish funksiyasi.
2 Ixtiyoriy o'lchamdagi ma'lumotlar massivini matematik almashtirish va uning uchun uncha uzun bo'lmagan belgilangan yagona ketma-ketlikni hisoblash.

1 Битлар сатрини белгиланган узунликдаги битлар сатрига айлантириш функцияси.
2 Ихтиёрий ўлчамдаги маълумотлар массивини математик алмаштириш ва унинг учун унча узун бўлмаган белгиланган ягона кетма-кетликни ҳисоблаш.

Ц

Ц

Центр аутентификации

uz - autentifikatsiya qilish markazi

аутентификация қилиш маркази

en - authentication center

Сетевое оборудование, отвечающее за конфиденциальный обмен информацией в сети мобильной связи и обеспечивающее защиту от несанкционированного доступа.

Mobil aloqa tarmog'ida konfidensial axborot almashinish yuzasidan javobgar bo'lgan va ruxsat etilmagan tarzda foydalanishdan muhofaza qilinishni ta'minlaydigan tarmoq uskunası.

Мобил алоқа тармоғида конфиденциал ахборот алмашиниш юзасидан жавобгар бўлган ва рухсат этилмаган тарзда фойдаланишдан муҳофаза қилишни таъминлайдиган тармоқ ускунаси.

Целостность

uz - yaxlitlik

яхлитлик

en - integrity

1 Свойство сохранения правильности и полноты.
2 Состояние информации и ее носителя, при котором обеспечиваются неделимость и предотвращение несанкционированного или преднамеренного уничтожения, искажения, утечки, хищения, подделки, подмены в целом и ее отдельных составных частей.

1 To'g'rilik va to'liqlikni saqlab qolish xususiyati.
2 Axborot va uning tashuvchisining holati bo'lib, bunda umuman va uning alohida tarkibiy qismlarining bo'linmasligi va ruxsat etilmagan tarzda yoki qasddan yo'q qilinishi, buzilishi, chiqib ketishi, o'g'irlanishi, qalbakilashtirilishining oldini olish ta'minlanadi.

1 Tўғрилиқ ва тўлиқликни сақлаб қолиш хусусияти.

2 Ахборот ва унинг ташувчисининг ҳолати бўлиб, бунда умуман ва унинг алоҳида таркибий қисмларининг бўлинмаслиги ва рухсат этилмаган тарзда ёки қасддан йўқ қилиниши, бузилиши, чиқиб кетиши, ўғирланиши, қалбакилаштирилишининг олдини олиш таъминланади.

Целостность данных

1 Способность данных сохранять точность и не-

Ц

uz - ma'lumotlarning
yaxlitligi

маълумотларнинг
яхлитлиги

en - data integrity

противоречивость независимо от выполняемых изменений.

2 Свойство, гарантирующее невозможность изменения, подмены или уничтожения данных не санкционированным способом.

Примечание – Целостность данных включает устойчивость системы к отказам и автоматическое восстановление.

1 Amalga oshiriladigan o'zgartirishlardan qat'i nazar, ma'lumotlarning aniqlikni va zid kelmaslikni saqlash qobiliyati.

2 Ma'lumotlarni ruxsat etilmagan usulda o'zgartirib, o'rnini almashtirib yoki yo'q qilish mumkin bo'lmasligini kafolatlaydigan xususiyat.

Izoh – Ma'lumotlarning yaxlitligi tizimning buzilishlarga chidamliligini va avtomatik tiklanishini ichiga oladi.

1 Амалга ошириладиган ўзгартиришлардан қатъи назар, маълумотларнинг аниқликни ва зид келмасликни сақлаш қобилияти.

2 Маълумотларни рухсат этилмаган усулда ўзгартириб, ўрнини алмаштириб ёки йўқ қилиш мумкин бўлмаслигини кафолатлайдиган хусусият.

Изоҳ – Маълумотларнинг яхлитлиги тизимнинг бузилишларга чидамлилигини ва автоматик тикланишини ичига олади.

Целостность информации

uz - axborotning yaxlitligi

ахборотнинг яхлитлиги

en - information integrity

Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Hisoblash texnikasi vositalari va avtomatlashtirilgan tizimning, tasodifiy va/yoki qasddan buzib ko'rsatish (buzish) sharoitida axborotning o'zgarماسligini ta'minlash xususiyati.

Ҳисоблаш техникаси воситалари ва автоматлаштирилган тизимнинг, тасодифий ва/ёки қасдан бузиб кўрсатиш (бузиш) шароитида ахборотнинг ўзгармаслигини таъминлаш хусусияти.

Целостность системы

Свойство системы обработки данных одновре-

Ц

uz - tizimning yaxlitligi
тизимнинг яхлитлиги
en - system integrity

менно с выполнением своего оперативного предназначения предотвращать использование или модификацию ресурсов незарегистрированными пользователями, а также предотвращать использование или модификацию зарегистрированными пользователями не принадлежащих им ресурсов.

Ma'lumotlarni qayta ishlash tizimining, o'zining operativ vazifasini bajarish bilan bir vaqtda, ro'yxatga olinmagan foydalanuvchilar tomonidan resurslardan foydalanishning yoki o'zgartirilishining oldini olish, shuningdek, ro'yxatga olingan foydalanuvchilar tomonidan ularga tegishli bo'lmagan resurslardan foydalanishning yoki o'zgartirilishining oldini olish xususiyati.

Маълумотларни қайта ишлаш тизимининг, ўзининг оператив вазифасини бажариш билан бир вақтда, рўйхатга олинмаган фойдаланувчилар томонидан ресурслардан фойдаланишнинг ёки ўзгартирилишининг олдини олиш, шунингдек, рўйхатга олинган фойдаланувчилар томонидан уларга тегишли бўлмаган ресурслардан фойдаланишнинг ёки ўзгартирилишининг олдини олиш хусусияти.

Цель
uz - maqsad
мақсад
en - objective

Результат, который предполагается достичь.

Примечания

1 Цель может быть стратегической, тактической или оперативной.

2 Цели могут устанавливаться для разных сфер деятельности (например, для финансовой сферы, здравоохранения и безопасности, а также для показателей качества окружающей среды) и для разных уровней (например, стратегические цели организации, проекта, продукта и процесса).

3 Цель может быть выражена и другими способами, например, как запланированный результат, намерение, действующий критерий, как цель информационной безопасности или с помощью других слов-синонимов (например, замысел, показатель или задача).

4 В контексте систем управления информационной безопасности для достижения конкретных результатов устанавливаются цели информационной безопасности, соответствующие политике информационной безопасности организации.

Erishilishi taxmin qilinadigan natija.

Ц

Izohlar

1 Maqsad strategik, taktik yoki operativ bo'lishi mumkin.

2 Maqsadlar faoliyatning turli sohalari (masalan, moliya sohasi, sog'liqni saqlash va xavfsizlik sohasi uchun, shuningdek, atrof muhit sifat ko'rsatkichlari) uchun va turli darajalar (masalan, tashkilot, loyiha, mahsulot va jarayonning strategik maqsadlari) uchun belgilanishi mumkin.

3 Maqsad boshqa usullar bilan ham ifodalanishi mumkin, masalan, rejalashtirilgan natija, maqsad, amaldagi mezon, axborot xavfsizligining maqsadi kabi yoki boshqa so'zlar-sinonimlar (masalan, o'ylangan ish, ko'rsatkich yoki vazifa) yordamida.

4 Axborot xavfsizligini boshqarish tizimlarining kontekstida aniq natijalarga erishish uchun tashkilot axborot xavfsizligining siyosatiga mos keladigan axborot xavfsizligi maqsadlari belgilanadi.

Эришилиши тахмин қилинадиган натижа.

Изоҳлар

1 Мақсад стратегик, тактик ёки оператив бўлиши мумкин.

2 Мақсадлар фаолиятнинг турли соҳалари (масалан, молия соҳаси, соғлиқни сақлаш ва хавфсизлик соҳаси учун, шунингдек, атроф муҳит сифат кўрсаткичлари) учун ва турли даражалар (масалан, ташкilot, лойиҳа, маҳсулот ва жараённинг стратегик мақсадлари) учун белгиланиши мумкин.

3 Мақсад бошқа усуллар билан ҳам ифодаланиши мумкин, масалан, режалаштирилган натижа, мақсад, амалдаги меzon, ахборот хавфсизлигининг мақсади каби ёки бошқа сўзлар-синонимлар (масалан, ўйланган иш, кўрсаткич ёки вазифа) ёрдамида.

4 Ахборот хавфсизлигини бошқариш тизимларининг контекстида аниқ натижаларга эришиш учун ташкilot ахборот хавфсизлигининг сиёсатига мос келадиган ахборот хавфсизлиги мақсадлари белгиланади.

Цель анализа

uz - tahlil maqsadi

таҳлил мақсади

en - review objective

Записанное изложение полученных результатов анализа.

Olingan tahlil natijalarining yozilgan bayoni.

Олинган таҳлил натижаларининг ёзилган баёни.

Цель безопасности

uz - xavfsizlik maqsadi

хавфсизлик мақсади

en - security objective

Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

Belgilangan tahdidlarga qarshi tura olish va/yoki

Ц

tashkilotning belgilangan xavfsizlik siyosatini va/ yoki taxminlarni qanoatlantirishning ifodalangan maqsadi.

Belgilangan taхdidlarга қарши тура олиш ва/ёки ташкilotнинг белгиланган хавфсизлик сиёсати- ни ва/ёки тахминларни қаноатлантиришнинг ифодаланган мақсади.

Цель защиты информации

uz - axborotni muhofaza qilish maqsadi

ахборотни муҳофаза қилиш мақсади

en - Information security target

Заранее намеченный уровень защищенности информации, получаемый в результате реализации системы защиты на объекте.

Примечание – Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Obyektda muhofaza qilish tizimini amalga oshirish natijasida olinadigan, axborot muhofaza qilinganligining oldindan belgilangan darajasi.

Izoh – Axborotni muhofaza qilishdan maqsad, axborotning ehtimol tutilgan tarqalib ketishi va/ yoki axborotga ruxsat etilmagan, ko‘zda tutilmagan ta’sir natijasida axborot mulkdoriga, egasiga, foydalanuvchisiga yetkaziladigan zararining oldini olish bo‘lishi mumkin.

Объектда муҳофаза қилиш тизимини амалга ошириш натижасида олинадиган, ахборот муҳофаза қилинганлигининг олдиндан белгиланган даражаси.

Изоҳ – Ахборотни муҳофаза қилишдан мақсад, ахборотнинг эҳтимол тutilган тарқалиб кетиши ва/ ёки ахборотга рuxсат этилмаган, кўзда тutilмаган таъсир натижасида ахборот мулкдoriga, эгасига, фойдаланувчисига етказиладиган зарарнинг олдини олиш бўлиши мумкин.

Цель управления

uz - boshqarish maqsadi

бошқариш мақсади

en - control objective

Описанное состояние, которое должно быть достигнуто в результате внедрения средств управления.

Boshqarish vositalarini joriy etish natijasida erishilishi kerak bo‘lgan tavsiflangan holati.

Бошқариш воситаларини жорий этиш натижасида эришилиши керак бўлган тавсифланган ҳолати.

Ц

Центр обмена информацией доверенный

uz - ishonchli axborot
almashinuv markazi

ишончли ахборот
алмашинув маркази

en - trusted information
communication entity

Автономная организация, обеспечивающая обмен информацией в пределах сообщества по обмену информацией.

Axborot almashinuvi bo'yicha hamjamiyat doirasida axborot almashinuvini ta'minlaydigan avtonom tashkilot.

Ахборот алмашинуви бўйича ҳамжамият доирасида ахборот алмашинувини таъминлайдиган автоном ташкилот.

Центр распределения ключей

uz - kalitlarni taqsimlash
markazi

калитларни тақсимлаш
маркази

en - key distribution center

Механизм, позволяющий распределять секретные ключи в симметричных криптосистемах.

Simmetrik kriptotizimlarda maxfiy kalitlarni taqsimlash imkonini beradigan mexanizm.

Симметрик криптотизимларда махфий калитларни тақсимлаш имконини берадиган механизм.

Центр сертификации ключей

uz - kalitlarni sertifikatlash
markazi

калитларни
сертификатлаш маркази

en - key certification center

Механизм, который не требует при каждом запросе на установление защищенного соединения, обращаться за ключом абонента-респондента.

Muhofazalangan bog'lanishga bo'lgan har bir so'rovda abonent-respondent kalitiga murojaat qilinishini talab etmaydigan mexanizm.

Муҳофазаланган боғланишга бўлган ҳар бир сўровда абонент-респондент калитига мурожаат қилинишини талаб этмайдиган механизм.

Цикл жизненный

uz - hayotiy sikl
haётий цикл

en - life-cycle

Последовательность стадий существования объекта (например, продукта или системы) во времени.

Vaqtida obyekt (masalan, mahsulot yoki tizim) mavjudligi bosqichlarining ketma-ketligi.

Вақтда объект (масалан, маҳсулот ёки тизим) мавжудлиги босқичларининг кетма-кетлиги.

Ц

Цикл ключей жизненный

uz - kalitlarning hayotiy sikli
калитларнинг ҳаётий

цикли

en - key lifecycle

Последовательность стадий, которые проходят ключи от момента генерации до момента уничтожения.

Kalitlar generatsiya vaqtidan yo‘q qilish vaqtigacha o‘tadigan bosqichlar ketma-ketligi.

Калитлар генерация вақтидан йўқ қилиш вақтигача ўтадиган босқичлар кетма-кетлиги.

Цикл проверки

uz - tekshiruv sikli

текширув цикли

en - loop check

Проверка, выполняемая для определения правильности передачи данных, при которой полученные данные возвращаются к источнику для сравнения с первоначально переданными данными.

Ma'lumotlar uzatilishining to'g'riligini aniqlash maqsadida bajariladigan tekshiruv. Bunda olingan ma'lumotlar, dastlab uzatilgan ma'lumotlar bilan taqqoslash uchun manbaga qaytariladi.

Маълумотлар узатилишининг тўғрилигини аниқлаш мақсадида бажариладиган текширув. Бунда олинган маълумотлар, дастлаб узатилган маълумотлар билан таққослаш учун манбага қайтарилади.

Цифра контрольная

uz - nazorat raqami

назорат рақами

en - check digit

Ключ проверки, состоящий из одиночной цифры (символа).

Bitta raqam (simvol)dan iborat bo'lgan tekshiruv kaliti.

Битта рақам (символ)дан иборат бўлган текширув калити.

Ч

Человек-пользователь

uz - foydalanuvchi-odam

фойдаланувчи-одам

en - man-to-user

Любое физическое лицо, взаимодействующее с объектом оценки.

Baholash obyektini bilan birgalikda ishlaydigan har qanday jismoniy shaxs.

Баҳолаш объекти билан биргаликда ишлайдиган ҳар қандай жисмоний шахс.

Ч

«Черви» файловые

uz - fayl «qurtlari»

файл «куртлари»

en - file worms

Эти вирусы создают собственные копии с привлекательными для пользователя названиями (например, *Game.exe*, *install.exe* и др.) в надежде на то, что пользователь их запустит.

Foydalanuvchi ishga tushirib yuboradi degan umidda, uning e'tiborini tortadigan nomlar ostida (masalan, *Game.exe*, *install.exe* va b.lar) o'zining nusxalarini yaratadigan viruslar.

Фойдаланувчи ишга тушириб юборади деган умидда, унинг эътиборини тортадиган номлар остида (масалан, *Game.exe*, *install.exe* ва б.лар) ўзининг нусхаларини яратадиган вируслар.

Червь

uz - qurt

курт

en - worm

1 Независимая программа, способная самостоятельно распространяться в системах обработки данных или компьютерных сетях.

Примечание – Черви часто разрабатываются, чтобы использовать доступные ресурсы, например, объем памяти или время обработки.

2 Программа, распространяющаяся по сети и использующая уязвимости сетевых протоколов или сетевых программ для распространения своих копий по узлам сети, где она может быть активизирована.

3 Вредоносная программа, распространяющаяся по сети, не оставляя своей копии на магнитном носителе, вычисляющая адреса сетевых компьютеров и записывающая по этим адресам свои копии.

Примечание – Обычно «червь» прерывает ход обработки информации в системе, оставаясь не обнаруженным, а затем самоуничтожается.

1 Ma'lumotlarni qayta ishlash tizimlarida yoki kompyuter tarmoqlarida o'z-o'zidan tarqalish qobiliyatiga ega bo'lgan mustaqil dastur.

Izoh – Qurtlar, ko'pincha mumkin bo'lgan, resurslardan, masalan, xotira hajmi yoki qayta ishlash vaqtidan foydalanish uchun ishlab chiqiladi.

2 Tarmoq bo'ylab tarqaladigan, o'zining nusxalarini tarmoq uzellari orqali tarqatish uchun tarmoq protokollari yoki dasturlarining zaif tomonlaridan foydalanadigan dastur.

Ч

3 O‘zining nusxalarini magnit tashuvchida qoldirmagan holda, tarmoq bo‘ylab tarqaladigan, tarmoq kompyuterlarining adreslarini hisoblab chiqadigan va bu adreslar bo‘yicha o‘z nusxalarini yozadigan zararli dastur.

Izoh – Odatda, «qurt» topib bo‘lmaydigan holatda qolib, tizimda axborotni qayta ishlash jarayonini to‘xtatib qo‘yadi, so‘ng o‘zini o‘zi yo‘q qiladi.

1 Маълумотларни қайта ишлаш тизимларида ёки компьютер тармоқларида ўз-ўзидан тарқалиш қобилиятига эга бўлган мустақил дастур.

Изоҳ – Қуртлар, кўпинча мумкин бўлган, ресурслардан, масалан, хотира ҳажми ёки қайта ишлаш вақтидан фойдаланиш учун ишлаб чиқилади.

2 Тармоқ бўйлаб тарқаладиган, ўзининг нусхаларини тармоқ узеллари орқали тарқатиш учун тармоқ протоколлари ёки дастурларининг заиф томонларидан фойдаланадиган дастур.

3 Ўзининг нусхаларини магнит ташувчида қолдирмаган ҳолда, тармоқ бўйлаб тарқаладиган, тармоқ компьютерларининг адресларини ҳисоблаб чиқадиган ва бу адреслар бўйича ўз нусхаларини ёзадиган зарарли дастур.

Изоҳ – Одатда, «қурт» топиб бўлмайдиган ҳолатда қолиб, тизимда ахборотни қайта ишлаш жараёнини тўхтатиб қўяди, сўнг ўзини ўзи йўқ қилади.

Червь почтовый

uz - pochta qurti

почта қурти

en - email-worm

Программа, которая способна рассылаться самостоятельно по электронной почте всем адресатам каждого списка доставки.

Elektron pochta orqali har bir yetkazib berish ro‘yxatidagi adresatlarga mustaqil tarzda tarqalish qobiliyatiga ega bo‘lgan dastur.

Электрон почта орқали ҳар бир етказиб бериш рўйхатидаги адресатларга мустақил тарзда тарқалиш қобилиятига эга бўлган дастур.

Число начальное

uz - boshlang‘ich son

бошланғич сон

en - seed

Случайная числовая последовательность, используемая для генерации другой, обычно более длинной псевдослучайной последовательности.

Boshqa bir, yanada uzunroq bo‘lgan psevdotasodifiy ketma-ketlikni generatsiyalash uchun foydalaniladigan tasodifiy sonli ketma-ketlik.

Ч

Бошқа бир, янада узунроқ бўлган псевдотасодифий кетма-кетликни генерациялаш учун фойдаланиладиган тасодифий сонли кетма-кетлик.

Число случайное

uz - tasodifiy son

тасодифий сон

en - random challenge

Код, формируемый с помощью генератора псевдослучайных чисел и используемый при аутентификации, шифровании и проверки целостности.

Pseudotasodifiy sonlar generatori yordamida shakllanadigan va autentifikatsiya qilishda, shifrlashda, yaxlitlikni tekshirishda foydalaniladigan kod.

Псевдотасодифий сонлар генератори ёрдамида шаклланидиган ва аутентификация қилишда, шифрлашда, яхлитликни текширишда фойдаланиладиган код.

Чтение с линии

телекоммуникаций

активное

uz - telekommunikatsiyalar

liniyasidan aktiv o'qish

телекоммуникациялар

линиясидан актив ўқиш

en - active line-tap

Нежелательное взаимодействие с системой телекоммуникаций, при котором сигналы, данные или сообщения, передаваемые по линиям телекоммуникаций, могут быть задержаны или удалены из системы.

Telekommunikatsiyalar tizimi bilan nomaqbul o'zaro hamkorlik, bunda telekommunikatsiyalar liniyalari orqali uzatiladigan signallar, ma'lumotlar yoki xabarlar ushlanib qolishi yoki tizimdan chiqarib yuborilishi mumkin.

Телекоммуникациялар тизими билан номақбул ўзаро ҳамкорлик, бунда телекоммуникациялар линиялари орқали узатиладиган сигналлар, маълумотлар ёки хабарлар ушланиб қолиши ёки тизимдан чиқариб юборилиши мумкин.

Чтение с линии телекоммуникаций пассивное

uz - telekommunikatsiyalar

liniyasidan passiv o'qish

телекоммуникациялар

линиясидан пассив ўқиш

en - passive line-tap

Несанкционированное чтение сигналов, данных или сообщений из системы телекоммуникаций без изменения ее сигналов.

Telekommunikatsiyalar tizimidan chiqadigan signallar, ma'lumotlar yoki xabarlarni, tizim signallarini o'zgartirmasdan, ruxsat etilmagan tarzda o'qish.

Телекоммуникациялар тизимидан чиқадиган сигналлар, маълумотлар ёки хабарларни, тизим сигналларини ўзгартирмасдан, рухсат этилмаган тарзда ўқиш.

Ч

**Чувствительность,
критичность**
uz - ta'sirchanlik, kritiklik
таъсирчанлик,
критиклик
en - sensitivity

1 Степень важности информации, определяемая ее владельцем и указывающая на необходимость ее защиты.
2 Характеристика ресурса сети, определяющая его степень важности и, возможно, включающая уязвимость.

1 Axborotning, uning egasi tomonidan belgilanadigan va axborot muhofaza qilinishi zarurligini ko'rsatadigan muhimlik darajasi.

2 Tarmoq resursining xarakteristikasi bo'lib, uning muhimlik darajasini belgilaydi. Tarmoqning zaif tomonlarini ham ichiga olishi mumkin.

1 Ахборотнинг, унинг эгаси томонидан белгиладиган ва ахборот муҳофаза қилиниши зарурлигини кўрсатадиган муҳимлик даражаси.

2 Тармоқ ресурсининг хarakteristikasi бўлиб, унинг муҳимлик даражасини белгилайди. Тармоқнинг заиф томонларини ҳам ичига олиши мумкин.

Ш

Шарада Меркля
uz - Merkl sharadasi
Меркл шарадаси
en - Merkle charade

Алгоритм, распределения ключей, который применяется для передачи используемого для шифрования секретного ключа, скрывая его в большом наборе шарад (головоломок).

Kalitlarni taqsimlash algoritmi. Shifrlash uchun foydalaniladigan maxfiy kalitni, sharadalarining katta to'plamida uni yashirgan holda, uzatishda qo'llaniladi.

Калитларни тақсимлаш алгоритми. Шифрлаш учун фойдаланиладиган махфий калитни, шарадаларнинг катта тўпламида уни яширган ҳолда, узатишда қўлланилади.

Шифр
uz - shifr
шифр
en - cipher, cypher

Совокупность обратимых преобразований множества возможных открытых (исходных) данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Ш

Kalitlardan foydalangan holda alohida qoidalar bo'yicha amalga oshiriladigan, mumkin bo'lgan ochiq (dastlabki) ma'lumotlar to'plamini mumkin bo'lgan shifrlangan ma'lumotlar to'plamiga qayta o'zgartirishlar jami.

Калитлардан фойдаланган ҳолда алоҳида қоидалар бўйича амалга ошириладиган, мумкин бўлган очик (дастлабки) маълумотлар тўпламини мумкин бўлган шифрланган маълумотлар тўпламига қайта ўзгартиришлар жами.

Шифр абсолютно стойкий

uz - absolyut barqaror shifr

абсолют барқарор шифр

en - unbreakable cipher

Шифр, в котором знание шифротекста не позволяет улучшить оценку соответствующего открытого текста.

Shifratni bilish, tegishli ochiq matn baholanishini yaxshilash imkonini bermaydigan shifr.

Шифрматни билиш, тегишли очик матн баҳоланишини яхшилаш имконини бермайдиган шифр.

Шифр аддитивный

uz - additiv shifr

аддитив шифр

en - additive cipher

Шифр гаммирования, в котором для наложения гаммы на данные используется бинарная операция аддитивного типа.

Gammani ma'lumotlarga qo'yish uchun additiv turdagi binar operatsiyadan foydalaniladigan gammalash shifri.

Гаммани маълумотларга қўйиш учун аддитив турдаги бинар операциядан фойдаланиладиган гаммалаш шифри.

Шифр асимметричный

uz - asimmetrik shifr

асимметрик шифр

en - asymmetric cipher

Шифр, в котором ключ шифрования не совпадает с ключом дешифрования.

Shifrlash kaliti deshifrlash kaliti bilan mos tushmaydigan shifr.

Шифрлаш калити дешифрлаш калити билан мос тушмайдиган шифр.

Ш

Шифр блочный

uz - blokli shifr

блочки шифр

en - block cipher

1 Алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над n -битными блоками исходного или зашифрованного текста.

2 Шифр, входными текстами для которого являются блоки фиксированного размера.

1 Dastlabki yoki shifrlangan matnning n -bitli bloklari ustida kriptografik amallarni bajarish yo‘li bilan, dastlabki axborotning kriptografik almashtirilishini amalga oshiruvchi shifrlash algoritmi.

2 Kirish matnlari belgilangan o‘lchamdagi bloklardan iborat bo‘lgan shifr.

1 Дастлабки ёки шифрланган матнинг n -битли блоклари устида криптографик амалларни bajarish yo‘li bilan, дастлабки ахборотнинг кriptografik almashtirilishini amalga oshiruvchi shifrlash algoritmi.

2 Кириш матлари белгиланган ўлчамдаги блоклардан иборат бўлган шифр.

Шифр гаммирования

uz - gammalash shifri

гаммалаш шифри

en - additive stream cipher

Потоковый шифр, в котором для зашифрования данных используется гаммирование.

Ma'lumotlarni shifrlash uchun gammalashdan foydalaniladigan oqimli shifr.

Ma'lumotlarni shifrlash uchun gammalashdan foydalaniладиган оқимли шифр.

Шифр потоковый

uz - oqimli shifr

оқимли шифр

en - stream cipher, general stream cipher

Шифр, преобразующий последовательно отдельные биты или знаки открытого текста и ориентированный на реализацию в виде программы.

Ochiq matnning ketma-ket ayrim bitlarini yoki belgilarini o‘zgartiruvchi va dastur ko‘rinishida amalga oshirish uchun mo‘ljallangan shifr.

Очиқ матнинг кетма-кет айрим битларини ёки белгиларини ўзгартирувчи ва дастур кўринишида амалга ошириш учун мўлжалланган шифр.

Ш

Шифр симметричный

uz - simmetrik shifr

симметрик шифр

en - symmetric cipher

Шифр, являющийся, симметричной криптографической системой, то есть использующий для зашифрования и расшифрования один и тот же ключ или такие различные ключи, что по одному из них легко может быть получен другой.

Simmetrik kriptografik tizim bo'lgan, ya'ni shifrlash va rasshifrovka qilish uchun aynan bir kalitdan yoki biri orqali boshqasi oson olinadigan turli kalitlardan foydalaniladigan shifr.

Симметрик криптографик тизим бўлган, яъни шифрлаш ва расшифровка қилиш учун айнан бир калитдан ёки бири орқали бошқаси осон олинадиган турли калитлардан фойдаланиладиган шифр.

Шифр составной

uz - tarkibli shifr

таркибли шифр

en - product cipher

Шифр, составленный из нескольких более простых шифров, которые используются в определенной последовательности при зашифровании и расшифровании данных.

Ma'lumotlarni shifrlash va rasshifrovka qilishda ma'lum bir ketma-ketlikda foydalaniladigan bir nechta oddiyroq bo'lgan shifrdan tuzilgan shifr.

Маълумотларни шифрлаш ва расшифровка қилишда маълум бир кетма-кетликда фойдаланиладиган бир нечта оддийроқ бўлган шифрдан тузилган шифр.

Шифр Файстеля

uz - Faystel shifri

Файстел шифри

en - Facetel cipher

Специальный класс повторяющегося блочного шифра, в котором шифротекст вычисляется из открытого текста повторением применения функции обхода.

Takrorlanadigan blokli shifrnin maxsus klassi, unda shifr matn chetlab o'tish funksiyasi qo'llanishini takrorlash bilan ochiq matndan hisoblab chiqiladi.

Такрорланадиган блокли шифрнинг махсус классси, унда шифр матн четлаб ўтиш функцияси қўлланишини такрорлаш билан очик матндан ҳисоблаб чиқилади.

Ш

Шифратор

uz - shifrlagich

шифрлагич

en - encoder, encipher

Электронное устройство или программа, реализующая алгоритмы шифрования.

Shifrlash algoritmlarini amalga oshiradigan elektron qurilma yoki dastur.

Шифрлаш алгоритмларини амалга оширадиган электрон қурилма ёки дастур.

Шифрование

uz - shifrlash

шифрлаш

en - encryption

Способ обработки данных с использованием специальных алгоритмов, обеспечивающих их скрытую передачу. Преобразование информации осуществляется на уровне битов или их последовательностей в отличие от криптографических методов, где единицами кодирования обычно являются смысловые слова или фразы.

Ma'lumotlarni, ularning yashirin uzatilishini ta'minlovchi maxsus algoritmlardan foydalanib, qayta ishlash usuli. Axborotning o'zgartirilishi kodlash birliklari, odatda, mazmunli so'z yoki jumlar bo'lgan kriptografik metodlardan farqli o'laroq, bitlar yoki ularning ketma-ketligi darajasida amalga oshiriladi.

Ma'lumotlarni, ularning yashirin uzatilib ta'minlovchi maxsus algoritmlardan foydalanib, qayta ishlash usuli. Axborotning o'zgartirilishi kodlash birliklari, odatda, mazmunli so'z yoki jumlar bo'lgan kriptografik metodlardan farqli o'laroq, bitlar yoki ularning ketma-ketligi darajasida amalga oshiriladi.

Шифрование абонентское

uz - abonent shifrlash

абонент шифрлаш

en - end-to-end encryption

1 Криптографическая защита информации, передаваемой между двумя субъектами автоматизированной системы.

2 Защита информации, передаваемой средствами телекоммуникаций криптографическими методами, непосредственно между отправителем и получателем.

1 Avtomatlashtirilgan tizimning ikki subyekti orasida uzatiladigan axborotning kriptografik muhofaza qilinishi.

2 Jo'natuvchi va oluvchi o'rtasida telekommunikatsiyalar vositalari yordamida bevosita uzatiladigan axborotning kriptografik metodlar bilan muhofaza qilinishi.

Ш

1 Автоматлаштирилган тизимнинг икки субъекти орасида узатиладиган ахборотнинг криптографик муҳофаза қилиниши.

2 Жўнатувчи ва олувчи ўртасида телекоммуникациялар воситалари ёрдамида бевосита узатиладиган ахборотнинг криптографик методлар билан муҳофаза қилиниши.

Метод засекречивания, при котором для шифрования применяются разные ключи.

Shifrlash uchun turli kalitlardan foydalaniladigan maxfiylashtirish metodi

Шифрлаш учун турли калитлардан фойдаланиладиган махфийлаштириш методи.

Шифрование

асимметричное

uz - asimmetrik shifrlash

асимметрик шифрлаш

en - asymmetric encryption

Шифрование вероятностное

uz - ehtimoliy shifrlash

эҳтимолий шифрлаш

en - probability encryption

1 Схема шифрования, в которой одному открытому тексту может соответствовать множество шифртекстов.

2 Процесс шифрования с использованием случайных параметров.

1 Bitta ochiq matnga shifratnlar to'plami to'g'ri kelishi mumkin bo'lgan shifrlash sxemasi.

2 Tasodifiy parametrlardan foydalangan holda shifrlash jarayoni.

1 Битта очик матнга шифрматнлар тўплами тўғри келиши мумкин бўлган шифрлаш схемаси.

2 Тасодифий параметрлардан фойдаланган ҳолда шифрлаш жараёни.

Шифрование методом Ривестра-Шамира-Адлемана

uz - Rivestr-Shamir-Adleman metodi bilan shifrlash

Ривестр-Шамир-Адлеман методи билан шифрлаш

en - RSA encryption

Метод шифрования с открытым ключом, при котором ключ, используемый для шифрования, не совпадает с ключом для дешифрования (последний должен быть известен получателю).

Ochiq kalit bilan shifrlash metodi bo'lib, shifrlash uchun foydalaniladigan kalit deshifrlash uchun mo'ljallangan kalit bilan mos tushmaydi (deshifrlash kaliti oluvchiga ma'lum bo'lishi kerak).

Очиқ калит билан шифрлаш методи бўлиб, шифрлаш учун фойдаланиладиган калит дешифрлаш учун мўлжалланган калит билан мос тушмайди (дешифрлаш калити олувчига маълум бўлиши

Ш

керак).

Шифрование одностороннее
uz - bir tomonlama shifrlash
бир томонлама шифрлаш
en - one-way encryption

Шифрование, результатом которого является шифротекст, исходные данные которого не могут быть восстановлены.

Примечание – Одностороннее шифрование используется для аутентификации. Например, полученный в результате шифрования пароля методом одностороннего шифрования шифротекст сохраняется. Пароль, представленный позже, будет зашифрован таким же образом. Затем оба полученных шифротекста сравниваются, и если они идентичны, то предъявлен верный пароль.

Shifrlash, dastlabki ma'lumotlari tiklanishi mumkin bo'lmagan shifrlangan matn uning natijasi hisoblanadi.

Izoh – Bir tomonlama shifrlash autentifikatsiya qilishda ishlatiladi. Masalan, bir tomonlama shifrlash metodi bilan parolni shifrlash natijasida olingan shifrlangan matn saqlanib qoladi. Kechroq taqdim etilgan parol xuddi shu tarzda shifrlanadi. Keyin olingan ikkala shifrlangan matn solishtiriladi, agar ular bir xil bo'lsa, unda to'g'ri parol taqdim etilgan.

Шифрлаш, дастлабки маълумотлари тикланиши мумкин бўлмаган шифрланган матн унинг натижаси ҳисобланади.

Изоҳ – Бир томонлама шифрлаш аутентификация қилишда ишлатилади. Масалан, бир томонлама шифрлаш методи билан паролни шифрлаш натижасида олинган шифрланган матн сақланиб қолади. Кечроқ тақдим этилган пароль худди шу tarzda шифрланади. Кейин олинган иккала шифрланган матн солиштирилади, агар улар бир хил бўлса, унда тўғри парол тақдим этилган.

Шифрование сквозное
uz - ochiq shifrlash
очиқ шифрлаш
en - end-to-end encryption,
end-to-end encipherment

1 Метод засекречивания информации, при котором зашифрованный поток передается через сеть в прозрачном режиме, т.е. без перешифрования трафика в промежуточных узлах телекоммуникаций.

2 Шифрование данных в пределах системы или на стороне источника с соответствующим дешифрованием, которое осуществляется только в пределах системы или на стороне назначения.

1 Axborotni maxfiylashtirish metodi bo'lib, shifrlangan oqim tarmoq orqali ochiq rejimda, ya'ni trafikni oraliq telekommunikatsiyalar uzellarida qayta shifrlamasdan, uzatiladi.

Ш

2 Ma'lumotlarni tizim doirasida yoki tegishlicha deshifrlash bilan manba tomonda shifrlash. Faqat tizim doirasida yoki mo'ljallangan tomonda amalga oshiriladi.

1 Ахборотни махфийлаштириш методи бўлиб, шифрланган оқим тармоқ орқали очик режимда, яъни трафикни оралик телекоммуникациялар узелларида қайта шифрламасдан, узатилади.

2 Маълумотларни тизим доирасида ёки тегишлича дешифрлаш билан манба томонда шифрлаш. Фақат тизим доирасида ёки мўлжалланган томонда амалга оширилади.

Шифрование с открытым ключом

uz - ochiq kalit bilan shifrlash

очик калит билан шифрлаш

en - public key cryptography

Криптографический метод, в котором используется открытый ключ для формирования шифротекста и закрытый ключ для преобразования шифротекст в исходный текст.

Kriptografik metod bo'lib, shifratni tuzish uchun ochiq kalitdan, shifratni dastlabki matnga o'zgartirish uchun esa, yopiq kalitdan foydalaniladi.

Криптографический метод бўлиб, шифрматни тузиш учун очик калитдан, шифрматни дастлабки матнга ўзгартириш учун эса, ёпиқ калитдан фойдаланилади.

Шифросистема

uz - shifrtizim

шифртизим

en - cryptosystem

Криптографическая система, обеспечивающая конфиденциальность информации путем ее шифрования.

Shifrlash yo'li bilan axborotning konfidentsialligini ta'minlaydigan kriptografik tizim.

Шифрлаш йўли билан ахборотнинг конфиденциаллигини таъминлайдиган криптографик тизим.

Шифротекст

uz - shifratn

шифратн

en - ciphertext

Результат зашифрования исходного открытого текста, осуществляемого с целью сокрытия его смысла.

Dastlabki ochiq matni uning ma'nosini yashirish maqsadida amalga oshiriladigan, shifratga o'g'irish natijasi.

Дастлабки очик матни унинг маъносини яшириш мақсадида амалга оширилдиган, шифр-

Ш

Шкала
uz - shkala
шкала
en - scale

матнга ўгириш натижаси.

Непрерывное или дискретное упорядоченное множество значений или множество категорий, на которых отображается атрибут.

Примечание – Вид шкалы зависит от характера взаимосвязи между ее значениями. Обычно различают четыре основных вида шкал:

- шкала наименований (номинационная или номинальная): значения измерений – категории;
- шкала порядковая (ординальная или ранговая): значения измерений – ранги;
- шкала интервалов (интервальная): деления шкалы расположены равномерно и соответствуют одинаковым значениям атрибута;
- шкала отношений (относительная): деления шкалы расположены равномерно и соответствуют одинаковым значениям атрибута. Шкала отношений имеет фиксированный ноль, который соответствует полному отсутствию атрибута.

Atribut aks ettiriladigan uzluksiz yoki diskret tartibga solingan qiymatlar to'plami yoki kategoriyalar to'plami.

Izoh – Shkala turi uning qiymatlari o'rtasidagi o'zaro bog'liqlik xarakteriga bog'liq. Odatda, shkalaning to'rtta asosiy turi ajratiladi:

- nomlar shkalasi (nominatsion yoki nominal): o'lchashlar qiymatlari – kategoriyalar;
- tartib shkalasi (ordinal yoki darajaga oid): o'lchashlar qiymatlari – darajalar;
- intervallar shkalasi (intervalga oid): shkalaning bo'laklarga ajratilishi bir me'yorda joylashgan va atributning bir xil qiymatlariga to'g'ri keladi;
- nisbatlar shkalasi (nisbiy): shkala bo'linmalari bir xil joylashgan va atributning bir xil qiymatlariga to'g'ri keladi. Nisbatlar shkalasi atributning umuman yo'qligiga mos keladigan qayd qilingan nolga ega.

Атрибут акс этириладиган узлуксиз ёки дискрет тартибга солинган қийматлар тўплами ёки категориялар тўплами.

Изоҳ – Шкала тури унинг қийматлари ўртасидаги ўзаро боғлиқлик хактерига боғлиқ. Одатда, шкаланинг тўртта асосий тури ажратилади:

- номлар шкаласи (номинацион ёки номинал): ўлчашлар қийматлари – категориялар;
- тартиб шкаласи (ординал ёки даражага оид): ўлчашлар

Ш

қийматлари – даражалар;

- интерваллар шкаласи (интервалга оид): шкаланинг бўлакларга ажратилиши бир меъёрда жойлашган ва атрибутнинг бир хил қийматларига тўғри келади;

- нисбатлар шкаласи (нисбий): шкала бўлинмалари бир хил жойлашган ва атрибутнинг бир хил қийматларига тўғри келади. Нисбатлар шкаласи атрибутнинг умуман йўқлигига мос келадиган қайд қилинган нолга эга.

Шлюз двухпортовый

uz - ikki portli shlyuz

икки портли шлюз

en - dual-homed gateway

Компьютер, на котором работает программное обеспечение межсетевого экрана и который имеет две сетевых карты: одна подключена к внутренней сети, а вторая – к внешней. Шлюз передает информацию из одной сети в другую, исключая прямое взаимодействие между ними.

Tarmoqlararo ekran dasturiy ta'minoti ishlaydigan va ikkita – biri ichki tarmoqqa, ikkinchisi tashqi tarmoqqa ulangan tarmoq kartalariga ega bo'lgan kompyuter. Shlyuz axborotni bir tarmoqdan ikkinchisiga, ular o'rtasida bevosita o'zaro ta'sirni istisno qilgan holda, uzatadi.

Тармоқлараро экран дастурий таъминоти ишлайдиган ва иккита – бири ички тармоққа, иккинчиси ташқи тармоққа уланган тармоқ карталарига эга бўлган компьютер. Шлюз ахборотни бир тармоқдан иккинчисига, улар ўртасида бевосита ўзаро таъсирни истисно қилган ҳолда, узатади.

Шлюз прикладного уровня

uz - amaliy darajadagi shlyuz

амалий даражадаги шлюз

en - application-level gateway

Один из вариантов реализации межсетевого экрана, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Фильтрация всех входящих и исходящих пакетов осуществляется на прикладном уровне эталонной модели ВОС. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Tarmoqlararo ekranni amalga oshirish variantlaridan biri. Mualliflashtirilgan mijoz bilan tashqi xost o'rtasida bevosita o'zaro ta'sirni istisno qiladi. Barcha kiradigan va chiqadigan paketlar filtratsiyasi VOS etalon modelining amaliy darajasida amalga oshiriladi. Ilovalar bilan bog'langan vositachi dastur-

Ш

lar shlyuz orqali *TCP/IP* muayyan servislari generatsiyalaydigan axborotni qayta yoʻllaydi.

Тармоқлараро экранни амалга ошириш вариантларидан бири. Муаллифлаштирилган мижоз билан ташқи хост ўртасида бевосита ўзаро таъсирни истисно қилади. Барча кирадиган ва чиқадиган пакетлар филтрацияси ВОС эталон моделининг амалий даражасида амалга оширилади. Иловалар билан боғланган воситачи дастурлар шлюз орқали *TCP/IP* муайян сервислари генерациялайдиган ахборотни қайта йўллайди.

Шлюз сеансового уровня

uz - seans darajasidagi shlyuz

сеанс даражасидаги шлюз

en - circuit-level gateway

Один из вариантов реализации межсетевого экрана, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Принимает запрос доверенного клиента на определенные услуги и, после проверки прав доступа на запрошенный сеанс, устанавливает соединение с внешним хостом. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Tarmoqlararo ekranni amalga oshirish variantlaridan biri. Mualliflashtirilgan mijoz bilan tashqi xost oʻrtasida bevosita oʻzaro hamkorlikni istisno qiladi. Vakolatli mijozning muayyan xizmatlarga boʻlgan soʻrovini qabul qiladi, soʻralgan seansga kira olish huquqi tekshirilgandan soʻng, tashqi xost bilan bogʻlanishni amalga oshiradi. Bundan keyin shlyuz paketlar filtratsiyasini bajarmasdan, ikkala yoʻnalishda bu paketlardan nusxa oladi.

Тармоқлараро экранни амалга ошириш вариантларидан бири. Муаллифлаштирилган мижоз билан ташқи хост ўртасида бевосита ўзаро ҳамкорликни истисно қилади. Ваколатли мижознинг муайян хизматларга бўлган сўровини қабул қилади, сўралган сеансга кира олиш ҳуқуқи текширилгандан сўнг, ташқи хост билан боғланишни амалга оширади. Бундан кейин шлюз пакетлар филтрациясини бажармасдан, иккала йўналишда бу пакетлардан нусха олади.

Э

Экранирование

uz - ekranlash

экранлаш

en - screening

1 Функция межсетевого экрана, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

2 Разграничение межсетевого доступа путем фильтрации передаваемых данных.

1 Tarmoqlararo ekranning, tashqi sohadan bo'ladigan ruxsat etilmagan so'rovlarni rad qilgan holda, ichki soha obyektlarining xavfsizligini ta'minlaydigan funksiyasi.

2 Uzatiladigan ma'lumotlarni filtrlash yo'li bilan tarmoqlararo erkin foydalanish (kirish) chegaralarini belgilash.

1 Tarmoqlararo ekranning, tashqi sohadan bo'ladigan ruxsat etilmagan so'rovlarini rad qilgan holda, ichki soha obyektlarining xavfsizligini ta'minlaydigan funksiyasi.

2 Uzatiladigan ma'lumotlarni filtrlash yo'li bilan tarmoqlararo erkin foydalanish (kirish) chegaralarini belgilash.

Экран межсетевой

uz - tarmoqlararo ekran

тармоқлараро экран

en - firewall

Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в систему и/или выходящей из системы.

Примечания

1 Межсетевой экран обеспечивает защиту системы посредством фильтрации информации, т.е. анализа по совокупности критериев и принятия решения о ее распространении в (из) систему(ы) на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной системы к объектам другой системы.

2 Средство защиты, устанавливаемое на стыке двух сетей, защищающее одну сеть от трафика, циркулирующего в другой сети, и служащее для предотвращения атак извне.

Tizimga kelib tushadigan va/yoki tizimdan chiqib ketadigan axborotning nazorat qilinishini amalga oshiradigan lokal (bir komponentli) yoki funksional taqsimlangan dasturiy (dasturiy-apparat) vosita (kompleks).

Izohlar

Э

1 Tarmoqlararo ekran axborotni filtrlash, ya'ni mezonlar majmui bo'yicha tahlil qilish va uni berilgan qoidalar asosida tizimga (tizimdan) tarqatish to'g'risidagi qarorni qabul qilish yordamida tizim muhofaza qilinishini ta'minlaydi, shu yo'l bilan subyektning bir tizimdan turib boshqa tizim obyektidan foydalana olishini cheklash amalga oshiriladi.

2 Trafikdan bitta tarmoqni muhofaza qiladigan ikkita tarmoqning tutashishida o'rnatiladigan, boshqa tarmoqda aylanadigan va tashqaridan hujumlarning oldini olish uchun xizmat qiladigan muhofaza qilish vositasi.

Тизимга келиб тушадиган ва/ёки тизимдан чиқиб кетадиган ахборотнинг назорат қилинишини амалга оширадиган локал (бир компонентли) ёки функционал тақсимланган дастурий (дастурий-аппарат) восита (комплекс).

Изоҳлар

1 Тармоқлараро экран ахборотни филтрлаш, яъни меzonлар мажмуи бўйича таҳлил қилиш ва уни берилган қоидалар асосида тизимга (tizimdan) тарқатиш тўғрисидаги қарорни қабул қилиш ёрдамида тизим муҳофаза қилинишини таъминлайди, шу йўл билан субъектнинг бир тизимдан туриб бошқа тизим объектидан фойдалана олишини чеклаш амалга оширилади.

2 Трафикдан битта тармоқни муҳофаза қиладиган иккита тармоқнинг туташишида ўрнатиладиган, бошқа тармоқда айланадиган ва ташқаридан ҳужумларнинг олдини олиш учун хизмат қиладиган муҳофаза қилиш воситаси.

**Экран межсетевой с
филтрацией пакетов
uz - paketlar filtrlanadigan
tarmoqlararo ekran**

пакетлар филтрлана-
диган тармоқлараро экран
en - packet-filtering firewall

1 Межсетевой экран, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом путем фильтрации входящих и исходящих пакетов.

Примечание – Фильтрация осуществляется на основе информации, содержащейся в заголовке пакета (адреса отправителя и получателя, номера портов и т.п.).

2 Маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты.

1 Mualliflashtirilgan mijoz bilan tashqi xost o'rtasida kiruvchi va chiquvchi paketlarni filtrlash orqali bevosita o'zaro ta'sirni istisno qiladigan tarmoqlararo ekran.

Izoh – Filtrlash paket sarlavhasidagi axborot asosida (jo'natuvchi va oluvchi adreslari, port nomerlari va sh.k.) amalga

Э

o'shiriladi.

2 Marshrutizatorlar yoki serverda ishlaydigan, kiruvchi va chiquvchi paketlar filtrlanadigan qilib konfiguratsiyalangan dasturlar.

1 Mualliflashirilgan mijoz bilan tashqi host ўrtasida kiruvchi va chiquvchi paketlarni filtrlash orqali bevosita ўzaro ta'sirni istisno qiladigan tarmoqlararo ekran.

Изоҳ – Филтрлаш пакет сарлавҳасидаги ахборот асосида (жўнатувчи ва олувчи адреслари, порт номерлари ва ш.к.) амалга оширилади.

2 Маршрутизаторлар ёки серверда ишлайдиган, кирувчи ва чiqувчи пакетлар филтрланадиган қилиб конфигурацияланган дастурлар.

Специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов. При этом проверяется содержимое принимаемых пакетов на трех уровнях модели ВОС: сетевом, сеансовом и прикладном.

Paketlarni filtrlashning maxsus algoritmlari. Ular yordamida har bir paket mualliflashtirilgan paketlarning ma'lum namunasi bilan taqqoslanadi. Qabul qilinadigan paketlarning ichidagi VOS modelining uchta: tarmoq, seans va amaliy darajalarida tekshiriladi.

Пакетларни филтрлашнинг махсус алгоритмлари. Улар ёрдамида ҳар бир пакет муаллифлаштирилган пакетларнинг маълум намунаси билан таққосланади. Қабул қилинадиган пакетларнинг ичидаги ВОС моделининг учта: тarmoқ, сеанс ва амалий даражаларида текширилади.

Пользователь ОО, прошедший профессиональную подготовку и обладающий квалификацией, достаточной для корректного использования ОО.

Professional tayyorgarlikdan o'tgan va BOdan to'g'ri foydalanish uchun yetarli malakaga ega BO foydalanuvchisi.

Профессионал тайёргарликдан ўтган ва БОдан тўғри фойдаланиш учун етарли малакага эга БО фойдаланувчиси.

Экран межсетевой экспертного уровня

uz - ekspert darajadagi

эксперт даражадаги

en - stateful inspection firewall

Эксперт

uz - ekspert

эксперт

en - expert

Э

Эксплойт

uz - eksployt
эксплойт
en - exploit

Вредоносный код, эксплуатирующий уязвимости программных компонентов компьютера.

Kompyuter dasturiy komponentlarining zaif tomonlaridan foydalanadigan zararli kod.

Компьютер дастурий компонентларининг заиф томонларидан фойдаланадиган зарарли код.

Экспозиция

uz - ekpozitsiya
экпозиция
en - exposition

Форма возможной потери или ущерба для системы. Например, экспозициями считаются неавторизованный доступ к данным или противодействие авторизованному использованию системы.

Tizim uchun mumkin bo'lgan yo'qotishlar yoki zarar shakli. Masalan, ma'lumotlardan mualliflashtirilgan tarzda erkin foydalanish yoki tizimdan mualliflashtirilgan tarzda foydalanishga qarshi turish ekpozitsiya hisoblanadi.

Тизим учун мумкин бўлган йўқотишлар ёки зарар шакли. Масалан, маълумотлардан муаллифлаштирилмаган тарзда эркин фойдаланиш ёки тизимдан муаллифлаштирилган тарзда фойдаланишга қарши туриш экпозиция ҳисобланади.

Элемент

uz - element
элемент
en - element

Неделимое изложение какой-либо потребности в безопасности.

Xavfsizlik biror-bir talabining bo'linmas ifodasi.

Хавфсизлик бирор-бир талабининг бўлинмас ифодаси.

Элемент конфигурации

uz - konfiguratsiya elementi
конфигурация элемента
en - configuration item

Объект, управляемый системой УК в процессе разработки ОО.

Примечание – Элементами конфигурации могут быть либо части ОО, либо объекты, имеющие отношение к разработке ОО, например, документы оценки или инструментальные средства разработки.

BOni ishlab chiqish jarayonida KB tizimi boshqaradigan obyekt.

Izoh – BO qismlari yoki BOni ishlab chiqishga aloqasi bo'lgan obyektlar, masalan, baholash hujjatlari yoki ishlab chiqishning instrumental vositalari konfiguratsiya elementi bo'lishi mumkin.

BOni ishlab chiqish jarayonida KB tizimi boshqaradigan obyekt.

Э

Изоҳ – БО қисмлари ёки БОни ишлаб чиқишга алоқаси бўлган объектлар, масалан, баҳолаш ҳужжатлари ёки ишлаб чиқишнинг инструментал воситалари конфигурация элементи бўлиши мумкин.

Энтропия

uz - entropiya

энтропия

en - entropy

В теории информации – мера неопределенности состояния объекта или некоторой ситуации (случайной величины) с конечным числом исходов. Понятие энтропии введено Шенноном и используется для определения количества информации в сообщении.

Axborot nazariyasida – obyekt holatining yoki qandaydir vaziyatning (tasodifiy kattalikning) noaniqlik o‘lchovi. Entropiya tushunchasi Shennon tomonidan kiritilgan va undan xabardagi axborotning miqdorini aniqlash uchun foydalaniladi.

Axborot nazariyasida – obyekt holatining ёки қандайдир вазиятнинг (тасодифий катталиқнинг) ноаниқлик ўлчови. Энтропия тушунчаси Шеннон томонидан киритилган ва ундан хабардаги ахборотнинг миқдорини аниқлаш учун фойдаланилади.

Этикетка авторская

uz - mualliflik yorlig‘i

муаллифлик ёрлиғи

en - copyright notice

Уведомление об авторском праве на программный продукт, обычно включается в начало программного листинга и обязательно отображается на дисплее компьютера.

Dasturiy mahsulotga bo‘lgan mualliflik huquqi to‘g‘risidagi bildirishnoma. Odatda, dasturiy listing boshlanishida kiritiladi va kompyuter displeyida aks ettiriladi.

Дастурий маҳсулотга бўлган муаллифлик ҳуқуқи тўғрисидаги билдиришнома. Одатда, дастурий листинг бошланишида киритилади ва компьютер дисплейида акс эттирилади.

Эффективность защиты информации

uz - axborotni muhofaza

qilish samaradorligi

ахборотни муҳофаза

қилиш самарадорлиги

en - information technical

protection efficiency

1 Степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты.

2 Показатель, характеризующий уровень технической защиты информации.

1 Axborotni muhofaza qilish bo‘yicha erishilgan ish natijalarining qo‘yilgan maqsadga muvofiq kelish darajasi.

Э

2 Axborotni texnik muhofaza qilish darajasini tavsiflovchi ko'rsatkich.

1 Axborotni muhofaza qiliش b'uyicha eriшилган иш натижаларининг қўйилган мақсадга мувофик келиш даражаси.

2 Axborotni texnik muhofaza qiliش dаражасини тавсифловчи кўрсаткич.

**Эффективность,
результативность**

uz - samaradorlik,
natijaviylik

самарадорлик,
натижавийлик

en - effectiveness

Степень реализации запланированной деятельности и достижения запланированных результатов.

Rejalashtirilgan faoliyatni amalga oshirish va rejalashtirilgan natijalarga erishish darajasi.

Режалаштирилган фаолиятни амалга ошириш ва режалаштирилган натижаларга эришиш даражаси.

Я

Ядро безопасности

uz - xavfsizlik yadrosi

хавфсизлик ядроси

en - security kernel

Программные и аппаратные элементы достоверной вычислительной базы, реализующие концепцию монитора ссылок. Они должны разделять все попытки доступа субъектов к объектам, быть защищенными от модификации и проверены на корректное выполнение своих функций.

Ishonchli hisoblash bazasining, havolalar monitori konsepsiyasini amalga oshiradigan dasturiy va apparat elementlari. Ular subyektlarning obyektlardan erkin foydalanishga bo'lgan barcha urinishlarini ajratishi, o'zgartirishlardan muhofaza-langani bo'lishi va o'z funksiyalarini to'laqonli bajarish yuzasidan tekshirilishi kerak.

Ишончли ҳисоблаш базасининг, ҳаволалар монитори концепциясини амалга оширадиган дастурий ва аппарат элементлари. Улар субъектларнинг объектлардан эркин фойдаланишга бўлган барча уринишларини ажратиши, ўзгартиришлардан муҳофазаланган бўлиши ва ўз функцияларини тўлақонли бажариш юзасидан текширилиши керак.

Я

Ядро защиты

uz - muhofaza yadrosi

муҳофаза ядроси

en - security kernel

Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Muhofaza qilish vositalari kompleksining, erkin foydalanish (kirish) dispetcheri konsepsiyasini amalga oshiradigan texnik, dasturiy va mikroplasturiy elementlari.

Муҳофаза қилиш воситалари комплексининг, эркин фойдаланиш (кириш) диспетчери концепциясини амалга оширадиган техник, дастурий ва микродастурий элементлари.

Язык администрирования базы данных

uz - ma'lumotlar bazasini

boshqarish tili

маълумотлар базасини

бошқариш тили

en - database administration

language

Искусственный язык для описания действий, связанных с администрированием базы данных.

Ma'lumotlar bazasini boshqarish bilan bog'liq bo'lgan ishlarni tavsiflash uchun mo'ljallangan sun'iy til.

Маълумотлар базасини бошқариш билан боғлиқ бўлган ишларни тавсифлаш учун мўлжалланган сунъий тил.

Язык базы данных

uz - ma'lumotlar bazasi tili

маълумотлар базаси тили

en - database language

Искусственный язык для описания процессов создания, ведения и использования баз данных.

Ma'lumotlar bazasini yaratish, olib borish va undan foydalanish jarayonlarini tavsiflash uchun mo'ljallangan sun'iy til.

Маълумотлар базасини яратиш, олиб бориш ва ундан фойдаланиш жараёнларини тавсифлаш учун мўлжалланган сунъий тил.

Язык гипертекстовой разметки документов

uz - hujjatlarni gipermatnli

belgilash tili

хужжатларни

гиперматнли белгилаш тили

en - hypertext markup language

1 Язык, используемый для создания веб-страниц.

2 Способ описания документов в WWW. Язык HTML использует набор тегов, вводимых в текстовые документы, которые указывают браузеру или другой программе, каким образом информация должна выводиться на экран.

1 Veb-sahifalarni yaratish uchun foydalaniladigan til.

2 Hujjatlarni WWW da tavsiflash usuli. HTML tili matnli hujjatlarga kiritiladigan, brauzer yoki boshqa

Я

dasturga axborot ekranga qay tarzda chiqarilishini ko'rsatadigan teglar to'plamidan foydalanadi.

1 Веб-саҳифаларни яратиш учун фойдаланиладиган тил.

2 Ҳужжатларни WWW да тавсифлаш усули. HTML тили матнли ҳужжатларга киритиладиган, браузер ёки бошқа дастурга ахборот экранга қай тарзда чиқарилишини кўрсатадиган теглар тўпламидан фойдаланади.

Язык запросов

uz - so'rovlar tili

сўровлар тили

en - query language

Искусственный язык для описания запросов, поиска данных в базах данных и действий над запросами.

So'rovlarni tavsiflash, ma'lumotlar bazasida ma'lumotlarni izlab topish, so'rovlar ustida amallar bajarish uchun mo'ljallangan sun'iy til.

Сўровларни тавсифлаш, маълумотлар базасида маълумотларни излаб топиш, сўровлар устида амаллар бажариш учун мўлжалланган сунъий тил.

Язык Java

uz - Java tili

Java тили

en - Java language

Новый язык программирования, разработанный Sun Microsystems, Inc. Язык Java может использоваться как обычный язык программирования для разработки сетевых приложений, а также для написания небольших приложений, называемых апплетами.

Sun Microsystems, Inc tomonidan ishlab chiqilgan yangi dasturlash tili. *Java* tilidan tarmoq ilovalarini (dasturlarini) ishlab chiqish uchun oddiy dasturlash tili sifatida, shuningdek, appletlar deb ataladigan uncha katta bo'lmagan ilovalarni yozishda foydalaniladi.

Sun Microsystems, Inc tomonidan ishlab chiqilgan yangi dasturlash tili. Java tilidan tarmoq ilovalarini (dasturlarini) ishlab chiqish uchun oddiy dasturlash tili sifatida, shuningdek, appletlar deb ataladigan uncha katta bo'lmagan ilovalarni yozishda foydalaniladi.

Алфавитный указатель терминов на русском языке

Atamalarning rus tilidagi alifbo ko'rsatkichi

Атамаларнинг рус тилидаги алифбо кўрсаткичи

Аварийный	1
Автоконтроль целостности	1
Автокорреляция	1
Авторизация	2
Авторизация данных	3
Авторизация программы	3
Агент (источник) угроз	3
Агрегирование	3
Администрация	4
Администратор	4
Администратор базы данных	5
Администратор безопасности (защиты)	6
Администратор доступа	7
Администратор межсетевоего экрана	7
Администратор системный	7
Администратор службы безопасности	7
Администрация банка данных	8
Администрация системы защиты	8
Администрирование базы данных	8
Администрирование средств безопасности	8
Аккредитация	9
Аккредитация в области защиты информации	10
Активы	10
Активы информационные	10
Алгоритм	10
Алгоритм DES трёхкратный	11
Алгоритм дешифрования	11
Алгоритм Диффи-Хеллмана	11
Алгоритм имитозащищающего кодирования информации	11
Алгоритм криптографический	12
Алгоритм криптографический асимметричный	12
Алгоритм криптографический симметричный	12
Алгоритм проверки цифровой подписи	13
Алгоритм СМЕА	13
Алгоритм Сторнетта-Хабера	13
Алгоритм формирования цифровой подписи	13
Алгоритм хэширования односторонний	14
Алгоритм шифрования	14
Алгоритм шифрования данных	14
Алгоритм Эль-Гамала	15

Амортизация отказов	15
Анализ	15
Анализ затрат (выгоды)	16
Анализ защищенности	16
Анализ криптографический	17
Анализ прерывания	17
Анализ программы санкционированный	18
Анализ риска	18
Анализ риска полный	19
Анализ рисков базовый	20
Анализ трафика	20
Анализ угроз	20
Анализ уязвимостей	20
Анализатор	21
Анализатор аварийного состояния	21
Анализатор прерываний	21
Анализаторы сетевые	22
Антивирус	22
Аппаратура засекречивания	22
Архивирование	23
Архивировать	23
Атака	23
Атака активная	25
Атака аналитическая, атака криптоаналитическая	25
Атака внутренняя	25
Атака косвенная	26
Атака непосредственная	26
Атака пассивная	26
Атаки пассивные	27
Атака перебором открытого текста	27
Атака переполнения	28
Атака по известному открытому тексту	28
Атака полным перебором, атака лобовая	28
Атака с известным открытым сообщением	29
Атака с частой сменой пароля	29
Атака типа «отказ в обслуживании»	29
Атака только по шифротексту	30
Атрибут	30
Атрибут безопасности	30
Атрибут доступа	31
Аттестат объекта защиты	31
Аттестация	32
Аттестация в области защиты информации	33
Аттестация испытательных лабораторий	33
Аттестация объектов информатизации	33

Аудит	34
Аудит безопасности	35
Аудит внешний	36
Аудит внутренний	36
Аудит комплексный	36
Аудит компьютерной системы	37
Аудит совместный	37
Аудитор безопасности	37
Аутентификатор	37
Аутентификация	38
Аутентификация взаимная	39
Аутентификация данных	39
Аутентификация источника данных	39
Аутентификация личности, подтверждение подлинности личности	39
Аутентификация многофакторная	40
Аутентификация неявная	40
Аутентификация односторонняя	41
Аутентификация сильная	41
Аутентификация слабая	41
Аутентификация сообщения	41
Аутентификация явная	42
Аутентичность, подлинность	42
Аутсорсинг	42
База вычислительная достоверная	43
База данных распределенная	43
База информационная	44
Барьер информационный	44
Барьер коммуникационный	44
Безопасность	45
Безопасность автоматизированной информационной системы	45
Безопасность автоматизированной системы	45
Безопасность административная	46
Безопасность данных	46
Безопасность информации	47
Безопасность информации (данных)	48
Безопасность информационная	49
Безопасность информационной системы	50
Безопасность информационной технологии	51
Безопасность коммуникационная	51
Безопасность компьютерная	51
Безопасность многоуровневая	52
Безопасность операционная	52
Безопасность программного обеспечения	52
Безопасность процедурная	53
Безопасность реальной открытой системы	53

Безопасность ресурса автоматизированной системы	53
Безопасность сети	55
Безопасность сети телекоммуникаций информационная	55
Безопасность сети телекоммуникаций общего пользования информационная	56
Безопасность сети телекоммуникаций технологическая	56
Безопасность субъектов информационных отношений	57
Безопасность физическая	57
Биометрия	58
Бит достоверности	58
Бит защиты	58
Бит контроля по четности	58
Бит маски	59
Блок	59
Блокирование	59
Блокирование доступа (к информации)	60
Блокирование информации	60
Блокирование логическое	61
Блокирование передачи информации (данных)	61
Блокирование физическое	62
Блокировка	62
Блокировка данных	62
Блокировка доступа к памяти	62
Блокировка записи в память	63
Блокировка клавиатуры	63
Блокировка локальная	63
Блокировка учетной записи	64
Блокнот одноразовый	64
Бомба временная	64
Бомба логическая	65
Бомба почтовая	65
Бомба программная	66
Бот	66
Бот-сеть (ботнет)	67
Брешь, лазейка	67
Вакцинирование	67
Валидация (утверждение)	68
Ведение контроля	68
Вектор аутентификационный	69
Вектор инициализации	69
Величина контрольная криптографическая	69
Верификатор	69
Верификатор автоматический	70
Верификатор байт-кода	70
Верификатор условий	70

Верификация (проверка)	71
Верифицировать	71
Верификация и утверждение	72
Вероятность	72
Взаимодействие	73
Взлом	73
Взлом, вскрытие криптосистемы	73
Взлом компьютерный	74
Взломщик	74
Взрыв	74
Взрыв комбинированный	74
Вид активной атаки	75
Вид доступа	75
Вирус загрузочный	75
Вирус (компьютерный)	76
Вирус программный, вирус	77
Вирусы неопасные	77
Вирусы опасные	78
Вирусы очень опасные	78
Вирусы паразитические	78
Вирусы перезаписывающие	79
Вирусы полиморфные	79
Вирусы простейшие	79
Вирусы резидентные	80
Вирусы файловые	80
Вирусы, поражающие исходный код программ	81
Вирусы-звенья	81
Вирусы-компаньоны	82
Вирусы-мутанты	82
Вирусы-невидимки	83
Владелец информации	83
Владелец полномочия	84
Владелец риска	84
Владелец сертификата подписи	84
Внутренне непротиворечивый	85
Воздействие дестабилизирующее	85
Воздействие злонамеренное	85
Воздействие на информационный ресурс внешнее	86
Воздействие на информацию непреднамеренное	87
Воздействие на информацию несанкционированное	87
Воздействие с ретрансляцией злонамеренное	88
Воздействия негативные	88
Возможности недеklarированные	88
Возможности ОО функциональные	89
Воссоздание данных	89

Восстановление базы данных	89
Восстановление данных	90
Восстановление обратное	91
Восстановление после отказа	91
Восстановление при исчезновении питающего напряжения	91
Восстановление при ошибках	92
Восстановление прямое	92
Восстановление сети	93
Восстановление файла	93
Время безопасное	93
Время восстановления	93
Время доступа (обращения)	94
Время жизни	94
Время ремонта	94
Вскрывать пароль	94
Вторжение	95
Вход (в систему)	95
Вход между строк	95
Выбор	96
Выводы аудита	96
Вызов обратный	96
Вызов-ответ	97
Вызов санкционированный	97
Выравнивание сектора	97
Гамма криптостойкая	98
Гамма шифра	98
Гаммирование	99
Гарантированность механизмов защиты информации	99
Гарантия	99
Генератор ключевого потока	99
Генератор случайных паролей	100
Генерация ключей	101
Граница кодирования	101
Гриф секретности	101
Дайджест	103
Данные	103
Данные аутентификационные	104
Данные биометрические	104
Данные верительные	104
Данные закрытые (защищенные)	104
Данные зашифрованные	105
Данные персональные	105
Данные пользователя	105
Данные проверки безопасности	105
Данные с защитой целостности	106

Данные секретные	106
Данные теста	106
Данные управления конфигурацией выходные	106
Данные функции безопасности объекта оценки	107
Дата и время изменения файла	107
Действие корректирующее	108
Действие несанкционированное	108
Действия пользователя «явные»	108
Действия пользователя «скрытые»	108
Делать заключение	108
Делегирование	109
Демон	109
Демонстрировать	109
Депонирование ключей	110
Дерево вызовов	110
«Дерево» Меркля	110
Дескриптор	111
Дескриптор безопасности	111
Дешифратор	112
Дешифратор адреса	112
Дешифрование	112
Деятельность в сфере программного обеспечения незаконная	113
Директория	113
Диск основной	113
Диспетчер доступа, ядро защиты	113
Дифейсмент	114
Доверие	115
Доверие к информации	115
Доверенная компьютерная система	115
Доказательство	115
Доказывать	116
Документация по управлению конфигурацией	116
Документация УК	117
Документы руководящие	117
Домен	118
Домен безопасности	118
Допуск	119
Дорожка дополнительная	119
Дорожка смещённая	119
Дорожка спиральная	119
Дорожка широкая	120
Доска сообщений	120
Достоверность	120
Достоверность информации	121
Достоверность обработки информации	121

Достоверность передачи информации	121
Достоверность функциональная	122
Доступ	122
Доступ алгоритмический	122
Доступ групповой (коллективный)	123
Доступ дискреционный (избирательный)	123
Доступ к информации	124
Доступ к информации несанкционированный	124
Доступ к информации санкционированный	125
Доступ к информационному ресурсу	125
Доступ к сведениям, составляющим государственные секреты	125
Доступ к секретной информации несанкционированный	125
Доступ к файлу	126
Доступ мандатный	126
Доступ мошеннический	127
Доступ на запись	127
Доступ на чтение	128
Доступ неавторизованный	128
Доступ несанкционированный	128
Доступ при отказе	129
Доступность	129
Доступность информации	130
Доступность системы	130
Драйвер устройства	131
Дыра	131
Единица измерения	131
Жетон идентификатора личности	132
Живучесть	132
Журнал	132
Журнал аудита	133
Журнал восстановления	134
Журнал ошибок	134
Журнализация	134
Завершение аварийное	135
Зависание программы	135
Зависание системы	135
Зависимость	136
Загрузка по линиям телекоммуникаций	136
Загрязнение	136
Задание по безопасности	137
Задача безопасности	137
Задача контрольная	138
Задача перехвата	138
Закладка программная	138
Замещение	139

Замок защиты (секретности)	139
Замок памяти	140
Замысел защиты информации	140
Записи системы управления конфигурацией	140
Запись контрольная	141
Запись учетная	141
Заполнение страницы	142
Заполнение трафика	142
Запрос/ответ	142
Засекречивание сведений и их носителей	143
Захватчики паролей	143
Зацикливание	143
Зашифрование	144
Защита	144
Защита аппаратная	144
Защита вычислительной сети	144
Защита данных	145
Защита информации (данных)	146
Защита информации организационная	146
Защита информации организационно-техническая	147
Защита информации от несанкционированного воздействия	148
Защита информации от несанкционированного доступа	148
Защита информации от разглашения	149
Защита информации от утечки	149
Защита информации при ее обработке техническими средствами ...	149
Защита информации техническая	150
Защита криптографическая	150
Защита личной тайны	150
Защита многоуровневая	151
Защита накоплением	151
Защита непосредственная	151
Защита объектов	152
Защита от записи	152
Защита от копирования	152
Защита от несанкционированного доступа	153
Защита от ошибок	153
Защита от чтения	154
Защита памяти	154
Защита паролем	155
Защита поля избирательная	155
Защита прав пользователей	155
Защита предупредительная	156
Защита программы	156
Защита системы	156
Защита файла	157

Защита ФБО собственная	157
Защита физическая	157
Защита эшелонированная	158
Защищенное техническое средство информатизации	158
Защищенность	158
Заявитель	159
Заявление о применимости	159
Злоумышленник	159
Злоупотребление компьютерное	160
Знак защитный специальный	160
Знак соответствия в области защиты информации	161
Значение атрибута	162
Значение контрольное криптографическое	162
Значение начальной установки	162
Значение секретное коллективное	162
Зона	163
Зона безопасности	163
Зона контролируемая	164
Зона опасная 1	164
Зона опасная 2	164
Идентификатор	165
Идентификатор безопасности	166
Идентификатор безопасности общеизвестный	167
Идентификатор диагностического сообщения	167
Идентификатор доступа	167
Идентификатор задачи	167
Идентификатор относительный	167
Идентификатор пользователя	168
Идентификатор пользователя сети	169
Идентификация	169
Идентификация аутентифицированная	170
Идентификация риска	170
Идентификация сервисов	171
Идентификация терминала	171
Избыточность	171
Избыточность кода	171
Излучение побочное	172
Изменение формата	172
Измерение	173
Имитация	173
Имитация экрана	173
Имитовставка	174
Имитозащита	174
Имитостойкость	175
Имя уникальное	175

Индикатор	175
Инженерия программная	176
Инженерия социальная	176
Инсталлятор	176
Инсталляция	177
Интерпретация	177
Интерпретация программная	177
Интерфейс	178
Интерфейс (в системах обработки данных)	178
Интерфейс функции безопасности объекта оценки	178
Интерфейс функциональный	178
Информация	179
Информация (для процесса обработки данных)	180
Информация аутентификации	180
Информация безопасности	181
Информация документированная	181
Информация защищаемая	181
Информация конфиденциальная	182
Информация некритичная (несекретная)	183
Информация ограниченного доступа	183
Информация остаточная	184
Информация персональная	184
Информация чувствительная (критичная)	184
Инфраструктура открытых ключей	185
Инфраструктура управления привилегиями	185
Инцидент	185
Инцидент информационной безопасности	186
Искажение данных	186
Искажение информации	186
Использование вычислительной системы злоумышленное	187
Использование ловушек	187
Использование объекта повторное	187
Исправление	188
Испытание	188
Испытание на проникновение	188
Исследования специальные	189
Источник	190
Источник информации комбинаторный	190
Источники коррелированные	190
Источники угроз	190
Исчерпывающий	191
Итерация	191
Канал	191
Канал временный скрытый	191
Канал доверенный	192

Канал защищенный	192
Канал связи внутренний	193
Канал с защитой целостности	193
Канал скрытый	193
Канал с памятью скрытый	194
Канал утечки информации	194
Канал утечки информации технический	195
Кардер	195
Карта идентификационная (кодовая)	195
Карта интеллектуальная	196
Карта копирования	196
Карта с микропроцессором	196
Категория безопасности	197
Категория безопасности информации	197
Категория допуска, допуск	197
Категория доступа	198
Категория защиты информации	198
Категория конфиденциальности	198
Категория управления доступом	198
Качество	199
Качество данных	199
Качество документации	199
Квадрат Бофорта	200
Квадрат Виженера	200
Квадрат Полибия	201
Квинтет	202
Кейлоггер	202
Кибербезопасность	202
Киберпреступление	203
Кибертерроризм	203
Класс	204
Класс защищенности средств вычислительной техники (автоматизи- рованной системы)	204
Класс идентификатора	204
Классификация	204
Класс рисков	205
Клонирование	205
Ключ анонимности	205
Ключ аутентификации	206
Ключ базы данных	206
Ключ вторичный	207
Ключ закрытый	207
Ключ защиты памяти	208
Ключ (криптографический)	208
Ключ личный	209

Ключ общий	209
Ключ открытый	209
Ключ разблокирования PIN-кода	210
Ключ раундовый	210
Ключ сеансовый	211
Ключ секретный	211
Ключ системный	212
Ключ скрытый	212
Ключ стойкий	213
Ключ управления доступом	213
Ключ целостности	213
Ключ шифрования	213
Книга кодировочная	214
Код	214
Код аутентификации	215
Код аутентификации сообщений	215
Код изменяющийся во времени	216
Кодирование	216
Кодирование источника	217
Кодирование канальное	217
Кодирование с использованием флага	218
Кодирование с критерием верности	218
Код каскадный	218
Код контрольный	219
Код контрольный (проверочный)	219
Код обнаружения манипуляции	219
Код операции	220
Код с контролем на четность	220
Код с минимальной избыточностью	220
Код с минимальным расстоянием	221
Код с переменной скоростью	221
Код установления подлинности сообщения	221
Код Хаффмана	222
Код Хемминга	222
Коды Боуза-Чоудхури-Хокенгема	222
Коды Голея	223
Коды Гоппы	223
Коды, исправляющие ошибки	223
Коды Рида-Мюллера	224
Коды Рида-Соломона	224
Коды с повторением	224
Коллизия	225
Команда перехода в режим шифрования	225
Компетентность	225
Компилятор	225

Комплекс средств защиты	225
Комплексность защиты	226
Компонент	226
Компонент базовый	226
Компонент зависимый	227
Компонент объекта оценки	227
Компоновка, обобщение	227
Компрометация	227
Компрометация информации	228
Конверт цифровой	228
Контейнер	229
Контрмера	229
Контроллер безопасности сети с централизованным управлением	230
Контроллер дисковый	230
Контроллер домена	230
Контроль	231
Контроль битов	231
Контроль данных	231
Контроль доступа	232
Контроль дублированием	232
Контроль избыточным циклическим кодом	232
Контроль избыточным кодом продольный	233
Контроль качества	233
Контроль нажатия клавиш	234
Контроль по избыточности	234
Контроль по избыточности циклический	234
Контроль по остатку, контроль по модулю n	234
Контроль по четности продольный	235
Контроль по четности поперечный	236
Контроль правильности	236
Контроль продольный (циклический)	236
Контроль работы с данными	237
Контроль средств защиты	237
Контроль четности	237
Контроль эффективности защиты информации	238
Конфиденциальность	238
Конфиденциальность информации	239
Конфиденциальность трафика	240
Концепция диспетчера доступа	240
Концепция доступа	240
Концепция защиты информации	241
Концепция монитора ссылок	241
Концепция обеспечения информационной безопасности	241
Копировщик побитовый	242
Корреляция взвешенная	242

Коэффициент сжатия в источнике сообщений	242
Коэффициент экранирования технического средства обработки информации	243
Кракер	244
Крекинг	244
Криптоалгоритм	244
Криптоанализ	245
Криптоанализ дифференциальный	245
Криптоанализ линейный	246
Криптографическая стойкость	246
Криптография	247
Криптография многоуровневая	248
Криптография квантовая	249
Криптография на эллиптических кривых	249
Криптография с открытым ключом	250
Криптография симметричная	250
Криптология	251
Криптосистема	251
Криптосистема Габидулина	252
Криптосистема Крука	252
Криптосистема Мак Эллиса	252
Криптосистема Нидеррайтера	252
Криптосистема потоковая самосинхронизирующаяся	253
Криптосистема потоковая синхронизирующаяся	253
Криптосистема с эллиптическими кривыми	254
Криптосистема с временным раскрытием	254
Криптосистема с открытым ключом	255
Криптосистема с секретным ключом	256
Критерии аудита	256
Критерии приемки	256
Критерии принятия решений	257
Критерии риска	257
Критичность	258
Кэширование паролей	258
«Лечение» вируса	258
Лицензиар в области защиты информации	259
Лицензиат в области защиты информации	259
Лицензирование	259
Лицензирование в области защиты информации	259
Лицензирование обязательное	260
Лицензия	260
Лицензия свободная	261
Лицензия упакованная	261
Лицензия установочная	261
Ловушка	261

Ловушка сброса	262
Люк	262
Люк эксплуатационный	263
Макровирус	263
Мандат	263
Маркер	265
Маркер безопасности	265
Маркер доступа	266
Маркировка по времени	266
Маршрут доверенный	267
Маршрут достоверный	267
Маска доступа	267
Маскарад	268
Маскиратор	268
Маскировка	269
Матрица доступа	269
Матрица полномочий	271
Мера	271
Мера основная (базовая)	271
Мера производная	272
Мероприятие по защите информации	272
Меры защиты информации организационные	272
Меры защиты информации правовые	273
Меры защиты информации технические	273
Меры защиты информации физические	274
Метка безопасности	274
Метка грифа	275
Метка идентификационная	275
Метка конфиденциальности	275
Метод аутентификации асимметричный	275
Метод аутентификации симметричный	276
Метод записи с частичным разрушением памяти	276
Метод защиты информации криптографический	276
Метод измерения	276
Метод Казиски	277
Метод счетчиковый	278
Методы внешних вторжений	278
Механизм информационной безопасности сети телекоммуникаций общего пользования	279
Механизм контроля доступа	280
Микроб	280
Минимум привилегий	281
Модель аналитическая	281
Модель Белла-Лападула	282
Модель данных иерархическая	283

Модель жизненного цикла	283
Модель защиты	283
Модель информационных угроз (техническими средствами)	284
Модель концептуальная	284
Модель нарушителя правил разграничения доступа	284
Модель политики безопасности формальная	284
Модель угроз	285
Модификация	285
Модификация информации	286
Модуль защиты интеллектуальный	286
Модуль идентификации абонента (SIM-карта)	286
Модуль идентификационный сменный	287
Модуль услуг пользователя идентификационный	287
Монитор (программа)	287
Монитор ссылок	288
Мониторинг	288
Мошенничество	288
Мошенничество внутреннее	289
Мошенничество компьютерное	289
Мошенничество процедурное	290
Мошенничество с карточками предоплаты	290
Мошенничество с контрактами	290
Мошенничество с украденным телефоном	290
Мошенничество, основанное на умении общения	291
Наблюдатель	291
Наблюдение	292
Надежность информационная	292
Надежность сети	292
Назначение	293
Нападение	293
Нарушение защиты	293
Нарушение целостности	293
Нарушитель	294
Нарушитель правил разграничения доступа	294
Невозможность обхода (ФБО)	295
Недоверие взаимное	295
Незащищенность	296
Неотказуемость	296
Непрерывность информационной безопасности	296
Непризнание участия	297
Непротиворечивый	297
Несоответствие	298
Нестойкость	298
Неформальный	298
Нечувствительность к отказам	298

Номер идентификационный персональный	298
Номер порядковый	299
Норма безопасности	299
Нормы эффективности защиты информации	300
Носители информации	300
Носители сведений, являющиеся государственными секретами	300
Нотаризация	301
Область предметная	301
Область применения внешняя	301
Область применения внутренняя	302
Обеспечение программное безопасное	304
Обеспечение программное достоверное	304
Обеспечивать	304
Область блокирования	304
Обман	305
Обмен аутентификацией	305
Обмен данными	305
Обмен данными безопасности	305
Обмен информацией и консультации относительно риска	306
Обмен ключами	307
Обмен при установлении подлинности	307
Обнаружение атак	308
Обнаружение манипуляции	308
Обновление ключей быстрое	308
Оборудование криптографическое	308
Обоснование строгое	309
Обработка информации в автоматизированной системе	309
Обработка риска	309
Обработка рисков	311
Образ	311
Объект	311
Объект анализа	312
Объект безопасности	312
Объект вычислительной техники	313
Объект доступа	313
Объект защиты информации	314
Объект информатизации	314
Объект информатизации защищенный	314
Объект информационного обмена	315
Объект информационной безопасности сети телекоммуникаций обще- го пользования	315
Объект конечный	315
Объект логический внешний	316
Объект оценки	316
Объект оценки составной	317

Объекты информатики	317
Объекты режимные	317
Объём аудита	318
Объяснять	318
Один звонок	318
Операция (над компонентом)	319
Операция (над объектом)	319
Описывать	319
Определение риска	319
Определение рисков	319
Определение жизненного цикла	320
Определитель события	320
Орган	320
Орган безопасности	320
Орган оценки	321
Орган по присвоению атрибутов	321
Орган по сертификации в области защиты информации	322
Орган регистрации	322
Орган режимно-секретный (РСО)	322
Орган руководящий	323
Орган сертификации	323
Организация	324
Ответ ожидаемый	324
Отказ в обслуживании	325
Отказ в обслуживании распределенный	326
Отказ от авторства	326
Отклик ожидаемый	326
Отладчик	326
Отношение	326
Отношения доверительные	327
«Отпечаток» цифровой	327
Оценка	327
Оценка безопасности	328
Оценка качества программного изделия	328
Оценка риска	328
Очистка	329
Ошибка (преднамеренная) умышленная	330
Ошибка данных	330
Ошибка кратковременная	330
Ошибка невозстанавливаемая	331
Ошибка некорректируемая	331
Ошибка неповторяющаяся (нерегулярная, перемежающаяся, случайная)	331
Ошибка семантическая	331
Ошибка фатальная	332

Ошибка четности	332
Пакет	332
Пакет доверия составной	333
Пакеты-убийцы	333
Память с защитой	333
Память только для записи	333
Паролирование	334
Пароль	334
Пароль главный	335
Пароль одноразовый	335
Пассивное скрывание	336
Перебор номеров циклический	336
Перебор полный	336
Передача в пределах объекта оценки	337
Передача за пределы объекта оценки	337
Передача между функциями безопасности объекта оценки	337
Передача права	337
Перемешивание	338
Переполнение	338
Переполнение-SYN	338
Перестановка	339
Перехват информации	339
Перехват информации активный	339
Перехват информации пассивный	340
Перехват сообщений	340
Перечень сведений, подлежащих засекречиванию	340
Период действия ключа	340
Период доступа	341
Печать	341
Пиггибекинг физический	341
Пиггибекинг электронный	341
Пират телефонный (взломщик телефонных сетей)	342
Пиратство программное	342
План обеспечения непрерывной работы и восстановления функциони- рования	342
План управления конфигурацией	343
Плата копирования	343
Повтор	343
Подглядывание из-за плеча	344
Подготовка	344
Подделка	344
Подделка информации	344
Подотчетность	345
Подпись бесспорная	346
Подпись групповая	346

Подпись кода	347
Подпись самопроверяющаяся	347
Подпись слепая	348
Подпись цифровая	348
Подпись цифровая одноразовая	349
Подпись цифровая электронная	349
Подслушивание	349
Подстановка	350
Подстановка (заполнение) трафика	351
Подсчет побитовый	351
Подтверждать	351
Подтверждение подлинности	352
Показатели защищенности средств вычислительной техники (автоматизированной системы)	352
Показатель эффективности защиты информации	353
Поле (диска) адресное	353
Поле данных	353
Поле управления аутентификацией	353
Политика	353
Политика безопасности	354
Политика безопасности идентификационная	355
Политика безопасности инструкционная	355
Политика безопасности организации	356
Политика информационной безопасности сети телекоммуникаций общего пользования	356
Политика управления доступом	357
Политика функции безопасности	357
Полномочие	357
Полный	358
Полубайт	358
Полуформальный	358
Пользователь	359
Пользователь авторизованный	359
Пользователь зарегистрированный	359
Пользователь (потребитель) информации	359
Пользователь легальный	360
Пользователь уполномоченный	360
Понятный	361
Попытка доступа к информации неавторизованная	361
Попытка нарушения защиты прямая	361
Портал обеспечения безопасности кабельный	362
Последовательность команд	362
Последовательность сверхдлинная	362
Последствие	362
Посредник	363

Поставка	364
Потенциал атаки	365
Потеря или искажение информации	365
Поток ключевой	365
Потоки информационные	366
Потребность информационная	366
Права пользователя	366
Правила доступа	366
Правила политики безопасности	367
Правила разграничения доступа	367
Право авторское	367
Право доступа	368
Право доступа к записи	368
Право доступа к чтению	368
Право на доступ	368
Предоставление права на доступ	369
Представление реализации	369
Предъявление пароля	369
Преобразование информации криптографическое	369
Преобразования криптографические	370
Препятствие	370
Прерывание	370
Прерывание соединения	371
Преступление компьютерное	371
Приватность	372
Привилегии	372
Пригодный/непригодный	372
Признак объекта демаскирующий косвенный	373
Принуждение	373
Принцип «положено знать»	374
Принцип Кирхгофа	374
Принятие риска	375
Проверка безопасности	375
Проверка достоверности данных	376
Проверка криптографическая	376
Проверка ограничения	376
Проверка подлинности	377
Проверка подлинности сквозная	377
Проверка правильности (данных) на входе	377
Проверка системы	377
Программа	378
Программа антивирусная	378
Программа вредоносная	378
Программа диагностическая	379
Программа самозагрузки	379

Программа-вакцина	379
Программа TEMPEST	379
Программы бесплатные	380
Программы доктора-ревизоры	380
Программы общедоступные	380
Программы-детекторы	381
Программы-ревизоры	381
Программы-фильтры	381
Продажа вызовов	382
Продукт ИТ доверенный	382
Проект системы управления информационной безопасностью	383
Производство	383
Проникновение	384
Прослеживать, сопоставлять	384
Прослушивание	384
Просмотр	385
Противодействие сетевым угрозам	385
Противостоять	385
Протокол безопасной передачи данных	385
Протокол криптографический	386
Протокол отрицания	386
Протокол распределения ключей	387
Протокол с арбитром	387
Протокол с третейским судьей	388
Протокол, самообеспечивающий законность	388
Протоколы	389
Профиль защиты	389
Профиль полномочий	390
Профиль пользователя	390
Проход через систему защиты, обходной путь	391
Процедура резервирования	391
Процедуры восстановительные	391
Процедуры приемки	392
Процесс	392
Процесс управления риском	393
Процессы информационные	394
Прошивка сети	394
Пункт обработки данных запасной	394
Пункт обработки данных резервный	394
Путь доступа	395
Путь обхода системы защиты	395
Путь проникновения	396
Путь сертификата	396
«Пятна родимые»	396
Работа секретная	397

Работоспособность сети	397
Радиокиллер	397
Радиус (опасной) зоны	398
Разбиение на модули	398
Развертывание ключа	398
Разглашение информации	398
Разграничение доступа	399
Разграничение обязанностей	400
Разделение	400
Разделение доменов	401
Разделение на уровни	401
Разделение привилегий	402
Разделение риска	402
Разделение секретов	403
Разметка дорожек спиральная	403
Разметка ложная	404
Разработка	404
Разработчик	404
Разрешение	404
Разрешение на доступ	405
Разрушение информации	405
Разрушение секретной информации	405
Разрыв линии	406
Разряд защиты	406
Рандомизация	406
Раскрытие	407
Раскрытие информации	407
Распределение ключей	407
Распределение ключей открытое	408
Рассеивание	409
Рассекречивание сведений и их носителей	409
Рассылка спама	410
Расширение	410
Расшифрование	410
Раунд	411
Регистрация	411
Регистрация деятельности	411
Регистрация открытого ключа	411
Регистрация пользователя	412
Регистр постоянный запоминающий	412
Регламентация	412
Режим использования защищенный	413
Режим обхода	413
Режим разграничения доступа	413
Резидентный	414

Результаты деятельности	414
Результаты измерения	414
Реконструкция данных	414
Реставрация данных	414
Ресурс	415
Ресурс защищенный	415
Ресурс объекта оценки	415
Ресурсы информационные	415
Решение по защите информации техническое	416
Решетка Кардано	416
Решетка кодовая	416
Риск	417
Риск остаточный	418
Роль	419
Руководство высшее	419
Ряд	420
Самокодирование	420
Сбор мусора	420
Сведения особой важности	421
Сведения секретные	421
Сведения совершенно секретные	421
Свидетельства аудита	421
Свидетельство управления конфигурацией	422
Связность	422
Связность временная	423
Связность коммуникативная	423
Связность логическая (процедурная)	423
Связность (элементов модуля), прочность модульная	424
Связность последовательная	424
Связность случайная	425
Связность функциональная	425
Секрет	425
Секретность информации	426
Секретность совершенная	426
Секреты государственные	427
Сектор дополнительный	427
Сектор ложный	427
Семейство	428
Сервер-посредник	428
Сертификат	428
Сертификат аутентификации	429
Сертификат авторизации	429
Сертификат аннулирования	430
Сертификат атрибута	430
Сертификат безопасности	430

Сертификат защиты	431
Сертификат ключа	431
Сертификат органа	432
Сертификат открытого ключа	432
Сертификат соответствия	433
Сертификат списка аннулирования	434
Сертификат цифровой	434
Сертификация	434
Сертификация системы защиты информации	435
Сертификация соответствия в области защиты информации	435
Сеть телекоммуникаций общего пользования защищенная	436
Сеть Файстеля	436
Сигнал информативный	437
Сигнатура	437
Сигнатура вируса	438
Символ управляющий	439
Система автоматизированная в защищённом исполнении	439
Система анализа защищенности	439
Система восстановления	440
Система замков и ключей	440
Система защиты информации	440
Система защиты информации (данных)	441
Система защиты одноступенчатая	442
Система защиты информации от несанкционированного доступа	442
Система защищенная	442
Система идентификации	443
Система избыточная	443
Система имитозащиты	443
Система информационная	444
Система информационная автоматизированная	444
Система информационная защищенная	445
Система ключевая	445
Система кодирования	446
Система компьютерная достоверная	446
Система криптографическая	446
Система криптографической защиты информации	447
Система обеспечения информационной безопасности	447
Система обеспечения информационной безопасности сети телекоммуникаций общего пользования	448
Система обнаружения атак	449
Система обнаружения вторжений	449
Система обработки информации автоматизированная	449
Система операционная	451
Система операционная безопасная	451
Система оценки	451

Система разграничения	451
Система сертификации в области защиты информации	452
Система управления	452
Система управления доступом	453
Система управления информационной безопасностью	453
Система управления ключами	454
Система управления конфигурацией	454
Система установки ключей	455
Система цифровой подписи	456
Система экспертная	456
Сканер безопасности	456
Сканер сетевой	457
Сканер уязвимости программ	457
Сканирование портов	457
Скремблер	457
Скремблирование	458
След	458
Слово кодовое дополнительное	458
Сложность	458
Служба аутентификации удаленных пользователей по коммутируемым линиям	459
Служба безопасности	459
Служба информационной безопасности сети телекоммуникаций общего пользования	459
Служба обеспечения информационной безопасности	460
Смарфинг	460
Снижение риска	460
Сниффинг	461
Собственник информации	461
Событие	462
Событие информационной безопасности	462
Совместимость (компонентов)	463
Соглашение об аутентификации и выборе ключей	463
Соккрытие	464
Сообщение	464
Сообщение криптостойкое	464
Сообщение одноразовое	464
Сообщение с цифровой подписью	465
Сообщество по обмену информацией	465
Соответствие	465
Соответствие очевидное	465
Соответствие строгое	466
Состояние безопасное	466
Состояние безопасности	467
Состояние санкционированное (разрешенное)	467

Сохранность данных	467
Спаминг	467
Специфицировать, определять	468
Список апробированной продукции	468
Список доступа	468
Список конфигурации	469
Список полномочий	469
Список управления доступом	470
Способ защиты информации	470
Спуфинг	470
Среда безопасная замкнутая	472
Среда безопасная открытая	472
Среда личной безопасности	472
Среда разработки	473
Среда с защитой целостности	473
Среда функционирования	473
Средства защиты информации	473
Средства защиты информации морально-этические	474
Средства защиты информации от несанкционированного доступа	474
Средства защиты информации технические (аппаратно-программные)	475
Средства защиты физические	475
Средства защиты информации законодательные	476
Средства защиты информации организационные	476
Средства имитозащиты	477
Средства кодирования	477
Средства криптографические	477
Средства криптографической защиты информации	478
Средства обработки информации	479
Средства разработки инструментальные	479
Средства технические вспомогательные	479
Средства технические основные	480
Средства технической защиты информации	480
Средства управления	481
Средства управления доступом	481
Средства управления конфигурацией инструментальные	481
Средства шифрования	482
Средства электронной цифровой подписи	482
Средство вычислительной техники	483
Средство вычислительной техники защищенное	484
Средство защиты	484
Средство защиты информации	484
Средство защиты информации активное	485
Средство защиты информации аппаратное	485
Средство защиты информации программное	486
Средство защиты информации техническое	486

Средство контроля эффективности защиты информации	487
Средство криптографической защиты информации	487
Средство обработки информации техническое	487
Средство разграничения доступа	488
Средство шифровальное	489
Стандарт в области обеспечения безопасности	490
Стеганография	490
Стеганография компьютерная	490
Стегоканал	491
Стегоключ	491
Стегоконтейнер	491
Стойкость криптографическая	491
Сторона заинтересованная	491
Стратегия защиты	492
Субключ	492
Субъект	492
Субъект безопасности	493
Субъект доступа	493
Субъект доступа авторизованный	494
Субъекты информационных отношений	494
Сумма контрольная	495
Суперсектор	496
Схема концептуальная	496
Схема предварительного распределения ключей	497
Схема цифровой подписи	497
Сцепление (модулей)	497
Сцепление криптографическое	497
Сцепление по вызову	498
Сцепление по данным	498
Сцепление по образцу	498
Сцепление по общей области	499
Сцепление по содержанию	499
Сцепление по управлению	500
Счетчик команд	500
Тайна коммерческая	500
Текст зашифрованный	501
Текст открытый	501
Тестирование на проникновение	501
Токен аппаратный	502
Токен программный	502
Точка доступа к сети	502
Трансляция	502
Требование	503
Требование безопасности	503
Троянская программа	504

Угроза	504
Угроза автоматизированной системы	505
Угроза активная	505
Угроза безопасности	506
Угроза безопасности информации	507
Угроза интересам субъектов информационных отношений	507
Угроза информационная	508
Угроза информационной безопасности инфокоммуникационной системы	508
Угроза информационной безопасности сети телекоммуникаций общего пользования	508
Угроза пассивная	509
Угроза физическая	509
Угрозы преднамеренные	510
Угрозы случайные	510
Улучшение постоянное	510
Уничтожение информации	510
Управление	511
Управление безопасностью	511
Управление доступом	511
Управление доступом дискреционное	513
Управление доступом логическое	513
Управление доступом на основе ролей	514
Управление доступом полномочное (мандатное)	514
Управление доступом физическое	515
Управление информационной безопасностью корпоративное	515
Управление информационным потоком	516
Управление инцидентами информационной безопасности	516
Управление ключами	517
Управление конфигурацией	517
Управление прикладное	517
Управление рисками	518
Уровень безопасности	519
Уровень безопасности базовый	519
Уровень доверия оценочный	519
Уровень доступа	520
Уровень полномочий субъекта	520
Уровень прозрачности	521
Уровень риска	521
Усиление	521
Услуга аутентификации	521
Услуга безопасности	522
Услуга конфиденциальности	522
Услуга отметки времени	523
Услуга рассылки ключей	523

Услуга управления доступом	523
Услуга целостности	524
Установление подлинности криптографическое	524
Установление последовательности сообщений	524
Устойчивость	525
Устройство выдачи сигнала тревоги	525
Устройство закладное электронное специальное	525
Устройство закладочное	526
Устройство защиты техническое	526
Устройство защиты электронное	526
Устройство защиты электронное активное	527
Устройство кодирующее	527
Устройство многоуровневое	528
Устройство одноуровневое	528
Устройство повышения достоверности идентификации	528
Устройство прерывания программы пользователя	529
Устройство регистрации доступа пользователей	529
Устройство стирания данных	530
Устройство электромагнитного зашумления	530
Утечка информации	531
Утечка секретной информации	531
Утилиты скрытого администрирования	531
Уточнение	532
Утрата секретных документов или изделий	532
Учет индивидуальный	532
Ущерб	533
Уязвимости потенциальные обнаруженные	533
Уязвимость	534
Уязвимость автоматизированной системы	536
Уязвимость доступная	536
Уязвимость информации	536
Уязвимость нулевого дня	537
Уязвимость остаточная	537
Уязвимость потенциальная	537
Уязвимость сетевой службы	538
Уязвимость субъекта информационных отношений	538
Файл архивный	539
Файл заархивированный	539
Файл защищенный	539
Файл контрольной проверки	539
Файл неотображаемый	539
Файл резервный	540
Фактор воздействующий внешний	540
Фактор, воздействующий на защищаемую информацию.	540
Фактор дестабилизирующий	541

Фактор дестабилизирующий внешний	541
Фактор дестабилизирующий внутренний	542
Фактор опасности	542
Фальсификация	543
Фиксация авторства	543
Фиксация контроля средств защиты	544
Философия защиты	544
Фильтр безопасности	544
Фильтрация входящего трафика	545
Фильтрация исходящего трафика	545
Фишинг	545
Флаг	546
Формальный	546
Формат диска	547
Фрод внутренний	547
Фрод хакерский	547
Фрод, основанный на услуге переадресации вызова	548
Фродастер	548
Функции безопасности объекта оценки	548
Функционирование	548
Функция измерения	549
Функция односторонняя	549
Функция односторонняя с секретом	550
Функция шифрования	551
Хост-бастион	551
Хэш	551
Хэш-алгоритм защищенный	552
Хэширование	552
Хэш-функция (функция хэширования)	552
Центр аутентификации	553
Целостность	553
Целостность данных	554
Целостность информации	554
Целостность системы	555
Цель	555
Цель анализа	556
Цель безопасности	556
Цель защиты информации	557
Цель управления	557
Центр обмена информацией доверенный	558
Центр распределения ключей	558
Центр сертификации ключей	558
Цикл жизненный	558
Цикл ключей жизненный	559
Цикл проверки	559

Цифра контрольная	559
Человек-пользователь	559
«Черви» файловые	560
Червь	560
Червь почтовый	561
Число начальное	561
Число случайное	562
Чтение с линии телекоммуникаций активное	562
Чтение с линии телекоммуникаций пассивное	562
Чувствительность, критичность	563
Шарада Меркля	563
Шифр	563
Шифр абсолютно стойкий	564
Шифр аддитивный	564
Шифр асимметричный	564
Шифр блочный	565
Шифр гаммирования	565
Шифр потоковый	565
Шифр симметричный	566
Шифр составной	566
Шифр Файстеля	566
Шифратор	567
Шифрование	567
Шифрование абонентское	567
Шифрование асимметричное	568
Шифрование вероятностное	568
Шифрование методом Ри-вестра-Шамира-Адлемана	568
Шифрование одностороннее	569
Шифрование сквозное	569
Шифрование с открытым ключом	570
Шифросистема	570
Шифротекст	570
Шкала	571
Шлюз двухпортовый	572
Шлюз прикладного уровня	572
Шлюз сеансового уровня	573
Экранирование	574
Экран межсетевой	574
Экран межсетевой с фильтрацией пакетов	575
Экран межсетевой экспертного уровня	576
Эксперт	576
Эксплойт	577
Экспозиция	577
Элемент	577
Элемент конфигурации	577

Энтропия	578
Этикетка авторская	578
Эффективность защиты информации	578
Эффективность, результативность	579
Ядро безопасности	579
Ядро защиты	580
Язык администрирования базы данных	580
Язык базы данных	580
Язык гипертекстовой разметки документов	580
Язык запросов	581
Язык Java	581

**Алфавитный указатель терминов на узбекском языке
(на латинской графике)**

Atamalarning o‘zbek tili (lotin grafikasi) dagi alifbo ko‘rsatkichi

Атамаларнинг ўзбек тили (лотин графикаси) даги алифбо кўрсаткичи

Abonent shifrlash	567
Abonentni identifikatsiyalash moduli (<i>SIM</i> -karta)	286
Absolyut barqaror shifr	564
Additiv shifr	564
Adres deshifratori	112
Adresli (disk) maydoni	353
Agregirlash (birlashtirish)	3
Ajratish	400
Akkreditlash	9
Aks ettirilmaydigan fayl	539
Aktiv axborotni muhofaza qilish vositasi	485
Aktiv elektron muhofaza qurilmasi	527
Aktiv hujum turi	75
Aktiv tahdid	505
Aktivlar	10
Aldov	305
Algoritm	10
Algoritmik foydalana olish	122
Al-Jamol algoritmi	15
Alohida muhim ma'lumotlar	421
Amalga oshirishning taqdim etilishi	369
Amaliy boshqarish	517
Amaliy darajadagi shlyuz	572
Analitik hujum, kriptanalitik hujum	25
Analizator	21
Aniq autentifikatsiya	42
Aniq imzo	346
Aniqlamoq	532
Aniqlangan potensial zaifliklar	533
Anonimlik kaliti	205
Antivirus	22
Apparat token	502
Apparat vositasida muhofaza qilish	144
Aralashtirib yuborish	338
Arbitrli protokol	387
Arxivga oid fayl	539
Arxivlamoq	23
Arxivlash	23
Arxivlashtirilgan fayl	539

Asimmetrik autentifikatsiya qilish metodi	275
Asimmetrik kriptografik algoritm	12
Asimmetrik shifr	564
Asimmetrik shifrlash	568
Asosiy (bazaviy) o'lchov	271
Asosiy disk	113
Asosiy parol	335
Asosiy texnik vositalar	480
Ataylab (qasddan) qilingan xato	330
Atribut	30
Atribut qiymati	162
Atribut sertifikatini	430
Atributlar beruvchi organ	321
Attestatlash	32
Audit	34
Audit dalillari	421
Audit hajmi	318
Audit jurnali	133
Audit kriteriyalari	256
Audit xulosalari	96
Autentifikator	37
Autentifikatsion ma'lumotlar	104
Autentifikatsiya almashinish	305
Autentifikatsiya axboroti	180
Autentifikatsiya qilingan identifikatsiya	170
Autentifikatsiya qilish	38
Autentifikatsiya qilish kaliti	206
Autentifikatsiya qilish kodi	215
Autentifikatsiya qilish markazi	553
Autentifikatsiya qilish sertifikatini	429
Autentifikatsiya qilish xizmati	521
Autentifikatsiyani boshqarish maydoni	353
Autsorsing	42
Avarya holati analizatori	21
Avarya(viy)	1
Avaryaviy tugallanish	135
Avtokorrelyatsiya	1
Avtomatik verifikator	70
Avtomatlashtirilgan axborot tizimi	444
Avtomatlashtirilgan axborot tizimining xavfsizligi	45
Avtomatlashtirilgan axborotni qayta ishlash tizimi	449
Avtomatlashtirilgan tizim resursining xavfsizligi	53
Avtomatlashtirilgan tizimda axborotni qayta ishlash	309
Avtomatlashtirilgan tizimga tahdid	505
Avtomatlashtirilgan tizimning xavfsizligi	45

Avtomatlashtirilgan tizimning zaifligi	536
Axborot	179
Axborot aktivlari	10
Axborot almashinish obyekti	315
Axborot almashinuvi bo'yicha hamjamiyat	465
Axborot bazasi	44
Axborot chiqib ketadigan kanal	194
Axborot chiqib ketadigan texnik kanal	195
Axborot egasi	83
Axborot egasi	461
Axborot jarayonlari	394
Axborot (ma'lumotlar) uzatilishini blokirovkalash	61
Axborot (ma'lumotlar) xavfsizligi	48
Axborot (ma'lumotlar)ni muhofaza qilish tizimi	441
Axborot (ma'lumotlarni qayta ishlash jarayoni uchun)	180
Axborot munosabatlari subyekting zaifligi	538
Axborot munosabatlari subyektlarining manfaatlariga tahdid	507
Axborot munosabatlari subyektlarining xavfsizligi	57
Axborot munosabatlarining subyektlari	494
Axborot oqimini boshqarish	516
Axborot oqimlari	366
Axborot resursidan foydalana olish	125
Axborot resursiga ko'rsatiladigan tashqi ta'sir	86
Axborot resurslari	415
Axborot tahdidi	508
Axborot tahdidlari (texnik vositalar bilan amalga oshiriladigan) modeli ...	284
Axborot tashuvchilar	300
Axborot texnologiyasi xavfsizligi	51
Axborot tizimi	444
Axborot tizimi xavfsizligi	50
Axborot to'siq	44
Axborot xavfsizligi	47
Axborot xavfsizligi	49
Axborot xavfsizligi hodisasi	462
Axborot xavfsizligi insidenti	186
Axborot xavfsizligi insidentlarini boshqarish	516
Axborot xavfsizligi kategoriyasi	197
Axborot xavfsizligiga tahdid	507
Axborot xavfsizligini boshqarish tizimi	453
Axborot xavfsizligini boshqarish tizimining loyihasi	383
Axborot xavfsizligini ta'minlash konsepsiyasi	241
Axborot xavfsizligini ta'minlash tizimi	447
Axborot xavfsizligini ta'minlash xizmati	460
Axborot xavfsizligining uzluksizligi	296
Axborotdan foydalana olish	124

Axborotdan foydalana olishlik	130
Axborotdan foydalanuvchi (axborot iste'molchisi)	359
Axborotdan mualliflashtirilmagan tarzda foydalanishga urinish	361
Axborotdan ruxsat etilgan tarzda foydalana olish	125
Axborotdan ruxsatsiz foydalana olish	124
Axborotga bo'lgan ehtiyoj	366
Axborotga bo'lgan ishonch	115
Axborotga putur yetkazish (axborotni obro'sizlantirish)	228
Axborotga qasddan bo'lmagan ta'sir	87
Axborotga ruxsat etilmagan ta'sir	87
Axborot-kommunikatsiya tizimi axborot xavfsizligiga tahdid	508
Axborotlashtirish obyekti	314
Axborotlashtirish obyektlarini attestatsiya qilish	33
Axborotni (ma'lumotlarni) muhofaza qilish	146
Axborotni aktiv tutib qolish	339
Axborotni blokirovkalash	60
Axborotni imitomuhofazalovchi kodlash algoritmi	11
Axborotni kriptografik muhofaza qilish tizimi	447
Axborotni kriptografik muhofaza qilish vositalari	478
Axborotni kriptografik muhofaza qilish vositasi	487
Axborotni kriptografik o'zgartirish	369
Axborotni muhofaza qilish apparat vositasi	485
Axborotni muhofaza qilish bo'yicha tadbir	272
Axborotni muhofaza qilish bo'yicha texnik yechim	416
Axborotni muhofaza qilish dasturiy vositasi	486
Axborotni muhofaza qilish kategoriyasi	198
Axborotni muhofaza qilish konsepsiyasi	241
Axborotni muhofaza qilish maqsadi	557
Axborotni muhofaza qilish mexanizmlarining kafolatlanganligi	99
Axborotni muhofaza qilish obyekti	314
Axborotni muhofaza qilish samaradorligi	578
Axborotni muhofaza qilish samaradorligini nazorat qilish	238
Axborotni muhofaza qilish samaradorligini nazorat qilish vositasi	487
Axborotni muhofaza qilish samaradorligining normalari	300
Axborotni muhofaza qilish sohasida akkreditlash	10
Axborotni muhofaza qilish sohasida attestatlash	33
Axborotni muhofaza qilish sohasida litsenziyalash	259
Axborotni muhofaza qilish sohasida muvofiqlikni sertifikatlash	435
Axborotni muhofaza qilish sohasida sertifikatlash organi	322
Axborotni muhofaza qilish sohasida sertifikatlash tizimi	452
Axborotni muhofaza qilish sohasidagi litsenziar	259
Axborotni muhofaza qilish sohasidagi litsenziat	259
Axborotni muhofaza qilish sohasidagi muvofiqlik belgisi	161
Axborotni muhofaza qilish texnik (apparat-dasturiy) vositalari	475
Axborotni muhofaza qilish texnik vositasi	486

Axborotni muhofaza qilish tizimi	440
Axborotni muhofaza qilish tizimini sertifikatlash	435
Axborotni muhofaza qilish usuli	470
Axborotni muhofaza qilish vositalari	473
Axborotni muhofaza qilish vositasi	484
Axborotni muhofaza qilish g'oyasi	140
Axborotni muhofaza qilishning huquqiy chora-tadbirlari	273
Axborotni muhofaza qilishning jismoniy chora-tadbirlari	274
Axborotni muhofaza qilishning kriptografik usuli	276
Axborotni muhofaza qilishning ma'naviy-axloqiy vositalari	474
Axborotni muhofaza qilishning qonunchilik vositalari	476
Axborotni muhofaza qilishning samaradorlik ko'rsatkichi	353
Axborotni muhofaza qilishning tashkiliy vositalari	476
Axborotni muhofaza qilishning tashkiliy chora-tadbirlari	272
Axborotni muhofaza qilishning texnik chora-tadbirlari	273
Axborotni oshkor etilishdan muhofaza qilish	149
Axborotni passiv tutib qolish	340
Axborotni qayta ishlash ishonchliligi	121
Axborotni qayta ishlash texnik vositasi	487
Axborotni qayta ishlash texnik vositasini ekranlash koeffitsiyenti	243
Axborotni qayta ishlash vositalari	479
Axborotni qo'lga kiritish	339
Axborotni ruxsat etilmagan tarzda foydalana olishdan muhofaza qilish	148
Axborotni ruxsat etilmagan ta'sirdan muhofaza qilish	148
Axborotni ruxsatsiz foydalana olishdan muhofaza qilish tizimi	442
Axborotni ruxsatsiz foydalana olishdan muhofaza qilish vositalari	474
Axborotni soxtalashtirish	344
Axborotni tashkiliy jihatdan muhofaza qilish	146
Axborotni tashkiliy-texnik jihatdan muhofaza qilish	147
Axborotni texnik muhofaza qilish	150
Axborotni texnik muhofaza qilish vositalari	480
Axborotni texnik vositalar bilan qayta ishlashda muhofaza qilish	149
Axborotni uzatishning ishonchliligi	121
Axborotni yo'q qilish	510
Axborotni o'zgartirish	286
Axborotni chiqib ketishdan muhofaza qilish	149
Axborotning buzilishi	186
Axborotning buzilishi	405
Axborotning fosh etilishi	407
Axborotning ishonchliligi	121
Axborotning ishonchliligi	292
Axborotning konfidensialligi	239
Axborotning maxfiyligi	426
Axborotning oshkor bo'lishi	398
Axborotning yaxlitligi	554

Axborotning yo‘qotilishi yoki buzib ko‘rsatilishi	365
Axborotning zaifligi	536
Axborotning chiqib ketishi (yo‘qolishi)	531
Axborotlar almashinish va risk yuzasidan maslahatlashuvlar	306
Axlat yig‘ish	420
Aytentifikatsion vektor	69
Baho	327
Baholangan korrelyatsiya	242
Baholash obyekti	316
Baholash obyekti doirasida uzatish	337
Baholash obyekti doirasidan tashqariga uzatish	337
Baholash obyekti resursi	415
Baholash obyekti xavfsizlik funksiyalarining ma’lumotlari	107
Baholash obyekti xavfsizlik funksiyasining interfeysi	178
Baholash obyektini xavfsizlik funksiyalari orasida uzatish	337
Baholash obyektining komponenti	227
Baholash obyektining xavfsizlik funksiyalari	548
Baholash organi	321
Baholash tizimi	451
Baholi ishonch darajasi	519
Bardoshsizlik	298
Barqaror kalit	213
Barqarorlik	525
Bayroq	546
Bayroqdan foydalanib kodlash	218
Bayt-kod verifikatori	70
Bazaviy komponent	226
Bazaviy xavfsizlik darajasi	519
Bekor qilish ro‘yxatining sertifikati	434
Bekor qilish sertifikati	430
Bella-Lapadula modeli	282
Bepul dasturlar	380
Bevosita hujum	26
Bevosita muhofaza qilish	151
Bevosita tiklash	92
«Bilish zarur» prinsipi	374
Bilvosita hujum	26
Biometrik ma’lumotlar	104
Biometriya	58
Bir darajali qurilma	528
Bir martali bloknot	64
Bir martali parol	335
Bir martali raqamli imzo	349
Bir martali xabar	464
Bir pog‘onali muhofaza tizimi	442

Bir tomonlama autentifikatsiya qilish	41
Bir tomonlama funksiya	549
Bir tomonlama xeshlash algoritmi	14
Bir tomonlama shifrlash	569
Birgalikda ishlash	73
Birin-ketin joylashtirib muhofaza qilish	158
Bitlarni nazorat qilish	231
Bitma-bit hisoblash	351
Bitma-bit nusxa ko'chiruvchi	242
Bitta qo'ng'iroq	318
Blok	59
Blokirovka	62
Blokirovkalash	59
Blokirovkalash sohasi	304
Blokli shifr	565
Bofort kvadrati	200
BOning funksional imkoniyatlari	89
Bostirib kirish	95
Bostirib kirishlarni aniqlash tizimi	449
Bog'langanlik	422
Bog'langanlik (modul elementlarining bog'langanligi), modulli chidamlilik	424
Bog'lanish (modullarning bog'lanishi)	497
Bog'lanishning uzilishi	371
Bog'liq bo'lgan komponent	227
Bog'liqlik	136
Boshlang'ich o'rnatish qiymati	162
Boshlang'ich son	561
Boshqarish	511
Boshqarish bo'yicha bog'lanish	500
Boshqarish maqsadi	557
Boshqarish tizimi	452
Boshqarish vositalari	481
Boshqaruvchi simvol	439
Buzish	73
Buzuvchi	74
Buzg'unchi	294
Bo'ylama (siklik) nazorat	236
Dalil	115
Darajalarga bo'lish	401
Dastur	378
Dasturiy bomba	66
Dasturiy injeneriya	176
Dasturiy interpretatsiya	177
Dasturiy mahsulot sifatini baholash	328
Dasturiy qaroqchilik	342

Dasturiy ta'minot sohasidagi noqonuniy faoliyat	113
Dasturiy ta'minot xavfsizligi	52
Dasturiy token	502
Dasturiy virus, virus	77
Dasturiy o'rnatma	138
Dasturlarning boshlang'ich kodini zararlaydigan viruslar	81
Dasturlarning yaxshi muhofazalanmaganlik skaneri	457
Dasturni mualliflashtirish	3
Dasturni muhofaza qilish	156
Dasturni ruxsat etilgan tarzda tahlil qilish	18
Dasturning osilib qolishi	135
Davlat siri bo'lgan ma'lumotlardan foydalana olish	125
Davlat siri hisoblanadigan ma'lumotlarni tashuvchilar	300
Davlat sirlari	427
Dayjest	103
Deklaratsiya (e'lon) qilinmagan imkoniyatlar	88
Demon	109
Deshifратор	112
Deshifrlash	112
Deshifrlash algoritmi	11
Deskriptor	111
Destabillashtiruvchi omil	541
Destabillashtiruvchi ta'sir	85
Detektor dasturlar	381
Diagnostik dastur	379
Diagnostik xabar identifikatori	167
Difeysment	114
Differensial kriptotahlil	245
Diffi-Xellman algoritmi	11
Direktoriya	113
Disk formati	547
Disk kontrolleri	230
Diskretsion (tanlab) foydalana olish	123
Diskretsion foydalana olishni boshqarish	513
Doimiy xotirlovchi registr	412
Doimiy yaxshilanish	510
Doktor-revizor dasturlar	380
Domen	118
Domen kontrolleri	230
Domenlarga bo'lish	401
Ehtimoliy shifrlash	568
Ehtimollik	72
Ekpozitsiya	577
Ekran imitatsiyasi	173
Ekranlash	574

Ekspert	576
Ekspert darajadagi	576
Ekspert tizimi	456
Eksployt	577
Ekspluatatsion lyuk	263
Elektromagnit shovqin qurilmasi	530
Elektron muhofaza qurilmasi	526
Elektron piggibeking	341
Elektron raqamli imzo	349
Elektron raqamli imzo vositalari	482
Element	577
Elliptik egri chiziq asosidagi kriptografiya	249
Elliptik egri chizikli kriptotizim	254
Entropiya	578
Erkin foydalanish dispetcheri konsepsiyasi	240
Erkin foydalanish kategoriyasi	198
Erkin foydalanish konsepsiyasi	240
Erkin foydalanish ro'yxati	468
Erkin foydalanish subyekti	493
Erkin foydalanishga ruxsat	405
Erkin foydalanishni boshqarish kategoriyasi	198
Erkin foydalanishni boshqarish ro'yxati	470
Erkin foydalanishni boshqarish vositalari	481
Erkin foydalanishni chegaralash	399
Erkin foydalanishni chegaralash rejimi	413
Erkin foydalanishni chegaralash vositasi	488
Erkin litsenziya	261
Eshitish	384
Faol hujum	25
Faoliyat natijalari	414
Faoliyatni qayd qilish	411
Faqat shifmatn bo'yicha qilinadigan hujum	30
Faqat yozish uchun xotira	333
Fatal xato	332
Fayl «qurtlari»	560
Fayl viruslari	80
Fayl o'zgartirilgan sana va vaqt	107
Faylga kira olish	126
Faylni muhofaza qilish	157
Faylni tiklash	93
Faystel shifri	566
Faystel tarmog'i	436
Filtr dasturlar	381
Firibgarlik	288
Firibgarlik orqali foydalana olish	127

Fishing	545
Fizik blokirovkalash	62
Fizik foydalana olishni boshqarish	515
Fizik tahdid	509
Formal xavfsizlik siyosati modeli	284
Formatni o'zgartirish	172
Foydalana olinadigan zaiflik	536
Foydalana olinishi cheklangan axborot	183
Foydalana olish	122
Foydalana olish atributi	31
Foydalana olish darajasi	520
Foydalana olish dispetcheri, muhofaza qilish yadrosi	113
Foydalana olish huquqi	368
Foydalana olish huquqi	368
Foydalana olish huquqlarini taqdim etish	369
Foydalana olish identifikatori	167
Foydalana olish markeri	266
Foydalana olish matritsasi	269
Foydalana olish ma'muri	7
Foydalana olish (murojaat qilish) vaqti	94
Foydalana olish niqobi	267
Foydalana olish obyeksi	313
Foydalana olish qoidalari	366
Foydalana olishlik	129
Foydalana olishni belgilash qoidalari	367
Foydalana olishni belgilash qoidalarini buzuvchi	294
Foydalana olishni belgilash qoidalarini buzuvchining modeli	284
Foydalana olishni belgilash tizimi	451
Foydalana olishni blokirovkalash (axborotdan)	60
Foydalana olishni boshqarish	511
Foydalana olishni boshqarish kaliti	213
Foydalana olishni boshqarish siyosati	357
Foydalana olishni boshqarish tizimi	453
Foydalana olishni boshqarish xizmati	523
Foydalana olishni mantiqiy boshqarish	513
Foydalana olishni nazorat qilish	232
Foydalana olishni nazorat qilish mexanizmi	280
Foydalana olishni vakolatli (mandatli) boshqarish	514
Foydalanish davri	341
Foydalanish turi	75
Foydalanuvchi	359
Foydalanuvchi dasturini to'xtatib qo'yish qurilmasi	529
Foydalanuvchilar huquqlarini muhofaza qilish	155
Foydalanuvchilarning erkin foydalanishini qayd etish qurilmasi	529
Foydalanuvchini ro'yxatga olish	412

Foydalanuvchining «ochiq» harakatlari	108
Foydalanuvchining «yashirin» harakatlari	108
Foydalanuvchining huquqlari	366
Foydalanuvchining identifikatori	168
Foydalanuvchining ma'lumotlari	105
Foydalanuvchining profili	390
Foydalanuvchi-odam	559
Frodaster	548
Funksional bog'lanish	425
Funksional interfeys	178
Funksional ishonchlilik	122
Gabidulin kriptotizimi	252
Gammalash	99
Gammalash shifri	565
Goley kodlari	223
Gopp kodlari	223
Grif belgisi	275
Guruh (jamo) bo'lib foydalana olish	123
Guruhiy imzo	346
Hammaga ma'lum xavfsizlik identifikatori	167
Haqiqiylik, asllik	42
Haqiqiylikni aniqlashdagi almashish	307
Haqiqiylikni kriptografik aniqlash	524
Haqiqiylikni tasdiqlash	352
Haqiqiylikni tekshirish	377
Havolalar monitori	288
Havolalar monitori konsepsiyasi	241
Hayotiy sikl	558
Hayotiy sikl modeli	283
Hayotiy siklni aniqlash	320
Himoya profili	389
Himoyaga ega xotira	333
Himoyalangan axborotlashtirish texnik vositasi	158
Hisob berishlik	345
Hisobga oid yozuvni blokirovkalash	64
Hisobga olish yozuvi	141
Hisoblagich metodi	278
Hisoblash tarmog'ini muhofaza qilish	144
Hisoblash texnikasi obykti	313
Hisoblash texnikasi vositalarining (avtomatlashtirilgan tizimning) muhofaza qilinganlik klassi	204
Hisoblash texnikasi vositalarining (avtomatlashtirilgan tizimning) muhofaza qilinganlik ko'rsatkichlari	352
Hisoblash texnikasi vositasi	483
Hisoblash tizimidan qasddan foydalanish	187

Hodisani aniqlagich	320
Hosila o‘lchov	272
Hujjatlar sifati	199
Hujjatlarni gipermatnli belgilash tili	580
Hujjatlashtirilgan axborot	181
Hujum	23
Hujum	293
Hujum potentsiali	365
Hujumlarni aniqlash	308
Hujumlarni aniqlash tizimi	449
Huquqni berish	337
Identifikator	165
Identifikator klassi	204
Identifikatsion almashtiriladigan modul	287
Identifikatsion belgi	275
Identifikatsion foydalanuvchi xizmatlari moduli	287
Identifikatsion (kodli) karta	195
Identifikatsion xavfsizlik siyosati	355
Identifikatsiya qilish	169
Identifikatsiyalash ishonchliligini oshirish qurilmasi	528
Identifikatsiyalash tizimi	443
Ifloslanish	136
Ijtimoiy injeneriya	176
Ikki portli shlyuz	572
Ikkilamchi kalit	207
Imitatsiya	173
Imitobardoshlilik	175
Imitomuhofaza	174
Imitomuhofaza tizimi	443
Imitomuhofaza vositalari	477
Imitoqo‘shimcha	174
Imtiyozlar	372
Imtiyozlar minimumi	281
Imtiyozlarni boshqarish strukturasi	185
Imtiyozlarning taqsimlanishi	402
Imzo sertifikatining egasi	84
Indikator	175
Individual hisobga olish	532
Informatika obyektlari	317
Informativ signal	437
Initsializatsiya vektori	69
Inkor qilish protokoli	386
Insident	185
Installyator	176
Installyatsiya	177

Instrukcion xavfsizlik siyosati	355
Instrumental ishlab chiqish vositalari	479
Instrumental konfiguratsiyani boshqarish vositalari	481
Intellektual karta	196
Intellektual muhofaza qilish moduli	286
Interfeys	178
Interfeys (ma'lumotlarni qayta ishlash tizimlarida)	178
Interpretatsiya (talqin)	177
Isbot qilmoq	116
Iteratsiya	191
Iyerarxik ma'lumotlar modeli	283
Iz	458
Izohlamoq	318
Ishlab chiqarish	383
Ishlab chiqish	404
Ishlab chiqish muhiti	473
Ishlab chiquvchi	404
Ishlamay qolishda foydalana olish	129
Ishlamay qolishdan so'ng tiklash	91
Ishlamay qolishlar amortizatsiyasi	15
Ishlamay qolishlarga ta'sirchan bo'lmaslik	298
Ishlamoq	548
Ishlash muhiti	473
Ishonch	115
Ishonch ma'lumotlari	104
Ishonchli AT mahsuloti	382
Ishonchli axborot almashinuv markazi	558
Ishonchli dasturiy ta'minot	304
Ishonchli hisoblash bazasi	43
Ishonchli kanal	192
Ishonchli kompyuter tizimi	115
Ishonchli kompyuter tizimi	446
Ishonchli marshrut	267
Ishonchli munosabatlar	327
Ishonchli yo'nalish	267
Ishonchlilik	120
Ishonchlilik biti	58
Ishonchlilik kriteriysi bilan kodlash	218
Ishonchlilikni yalpi tekshirish	377
Ishtirokni tan olmaslik	297
Ichki aloqa kanali	193
Ichki audit	36
Ichki destabillashtiruvchi omil	542
Ichki firibgarlik	289
Ichki frod	547

Ichki hujum	25
Ichki qarama-qarshiliksiz	85
Ichki qo‘llanish sohasi	302
Jamoaviy maxfiy qiymat	162
Jarayon	392
Java tili	581
Jinoyatkor	159
Jismoniy muhofaza	157
Jismoniy muhofaza qilish vositalari	475
Jismoniy piggibeking	341
Jismoniy xavfsizlik	57
Joylangan litsenziya	261
Juda xavfli viruslar	78
Juftlik bo‘yicha bo‘ylama nazorat	235
Juftlik bo‘yicha ko‘ndalang nazorat	236
Juftlik bo‘yicha nazorat biti	58
Juftlik xatosi	332
Juftlikni nazorat qilish	237
Juftlikni nazorat qilish kodi	220
Jurnal	132
Jurnallashtirish	134
Kabelli xavfsizlikni ta’minlash portali	362
Kafolat	99
Kalit (kriptografik)	208
Kalit oqimi	365
Kalit oqimi generatori	99
Kalit sertifikatini	431
Kalit tizimi	445
Kalitlar almashinuvi	307
Kalitlar generatsiyasi	101
Kalitlarni autentifikatsiya qilish va tanlash to‘g‘risida bitim	463
Kalitlarni boshqarish	517
Kalitlarni boshqarish tizimi	454
Kalitlarni ochiq taqsimlash	408
Kalitlarni oldindan taksimlash sxemasi	497
Kalitlarni saqlash uchun topshirish	110
Kalitlarni sertifikatlash markazi	558
Kalitlarni taqsimlash	407
Kalitlarni taqsimlash markazi	558
Kalitlarni taqsimlash protokoli	387
Kalitlarni tarqatish xizmati	523
Kalitlarni tez yangilash	308
Kalitlarni o‘rnatish tizimi	455
Kalitlarning hayotiy sikli	559
Kalitni ochib ko‘rsatish	398

Kalitning amal qilish davri	340
Kanal	191
Kanal bo'yicha kodlash	217
Kardano panjarasi	416
Karder	195
Kaskadli kod	218
Kaziski metodi	277
KB hujjat	117
Keng yo'lka	120
Kengaytirish	410
Ketma-ket bog'langanlik	424
Keylogger	202
Kiberjinoyat	203
Kiberterrorizm	203
Kiberxavfsizlik	202
Kira olish (foydalana olish) yo'li	395
Kirish (tizimga kirish)	95
Kirishda (ma'lumotlarning) to'g'riligini tekshirish	377
Kiruvchi trafikni filtrlash	545
Kirxgof prinsipi	374
Klass	204
Klassifikatsiyalash (tasniflash)	204
Klaviaturani blokirovkalash	63
Klavishlar bosilishini nazorat qilish	234
Klonlash	205
Kod	214
Kod kitobi	214
Kod yozuvi	347
Kodlash	216
Kodlash tizimi	446
Kodlash vositalari	477
Kodlash chegarasi	101
Kodli panjara	416
Kodlovchi qurilma	527
Kodning ortiqchaligi	171
Kolliziya	225
Komandalar ketma-ketligi	362
Komandalarni hisoblagich	500
Kombinator axborot manbai	190
Kombinatsiyalangan portlash	74
Kommunikativ bog'langanlik	423
Kommunikatsion to'siq	44
Kommunikatsion xavfsizlik	51
Kommutatsiyalanadigan liniyalar bo'yicha olisdagi foydalanuvchilarni autentifikatsiya qilish xizmati	459

Kompanion viruslar	82
Kompetentlik	225
Kompilyator	225
Kompleks audit	36
Komponent	226
Komponovka qilish, umumlashtirish	227
Komprometatsiya (obro'sizlantirish)	227
Kompyuter firibgarligi	289
Kompyuter jinoyati	371
Kompyuter steganografiyasi	490
Kompyuter suiiste'molligi	160
Kompyuter tizimining auditi	37
Kompyuter vositasida buzish	74
Kompyuter xavfsizligi	51
Konfidensial axborot	182
Konfidensiallik	238
Konfidensiallik belgisi	275
Konfidensiallik kategoriyasi	198
Konfidensiallik xizmati	522
Konfiguratsiya elementi	577
Konfiguratsiya ro'yxati	469
Konfiguratsiyani boshqarish	517
Konfiguratsiyani boshqarish bo'yicha hujjatlar	116
Konfiguratsiyani boshqarish dalili	422
Konfiguratsiyani boshqarish rejasi	343
Konfiguratsiyani boshqarish tizimi	454
Konfiguratsiyani boshqarish tizimi yozuvlari	140
Konfiguratsiyani boshqarishning chiqish ma'lumotlari	106
Konseptual model	284
Konseptual sxema	496
Konteyner	229
Kontraktlar bilan bog'liq firibgarlik	290
Korporativ axborot xavfsizligini boshqarish	515
Kraker	244
Kreking	244
Kriptoalgoritm	244
Kriptobardoshli gamma	98
Kriptobardoshli xabar	464
Kriptografik algoritm	12
Kriptografik bardoshlilik	246
Kriptografik bardoshlilik	491
Kriptografik ilashish	497
Kriptografik muhofaza qilish	150
Kriptografik nazorat kattaligi	69
Kriptografik nazorat qiymati	162

Kriptografik protokol	386
Kriptografik tahlil qilish	17
Kriptografik tekshiruv	376
Kriptografik tizim	446
Kriptografik uskuna	308
Kriptografik vositalar	477
Kriptografik o'zgartirishlar	370
Kriptografiya	247
Kriptologiya	251
Kriptotahlil	245
Kriptotizim	251
Kriptotizimni buzish, ochish	73
Kritik (maxfiy) bo'lmagan axborot	183
Kritiklik	258
Kruk kriptotizimi	252
Kuchaytirish	521
Kuchli autentifikatsiya	41
Kuchsiz autentifikatsiya	41
Kutilgan javob	324
Kutilgan javob	326
Kuzatish	292
Kuzatmoq, taqqoslamoq	384
Kuzatuvchi	291
Kvant kriptografiyasi	249
Kvintet	202
Ko'p darajali kriptografiya	248
Ko'p darajali qurilma	528
Ko'p darajali xavfsizlik	52
Ko'p faktorli autentifikatsiya	40
Ko'p pog'onali himoya	151
Ko'rib chiqish	385
Ko'rinmas viruslar	83
Ko'r-ko'rona imzo	348
Liniyaning uzilishi	406
Litsenziya	260
Litsenziyalash	259
Lokal blokirovkalash	63
Lyuk	262
Majburiy litsenziyalash	260
Majburiyatlarning aniq belgilab olinishi	400
Majburlash	373
Mak Ellis kriptotizimi	252
Makrovirus	263
Manba	190
Manbani kodlash	217

Mandat	263
Mandatli foydalana olish	126
Manfaatdor bo‘lmagan hakam protokoli	388
Manfaatdor tomon	491
Manipulyatsiyani aniqlash	308
Manipulyatsiyani aniqlash kodi	219
Mantiqiy (protseduraviy) bog‘lanish	423
Mantiqiy blokirovkalash	61
Mantiqiy bomba	65
Maqsad	555
Markazlashtirilgan tarzda boshqariladigan tarmoq xavfsizlik kontrolleri	230
Marker	265
Maskarad	268
Maskirator	268
Maxfiy axborotdan ruxsat etilmagan tarzda foydalana olish	125
Maxfiy axborotning buzilishi	405
Maxfiy axborotning chiqib ketishi (yo‘qolishi)	531
Maxfiy hujjatlar yoki buyumlarni yo‘qotish	532
Maxfiy ish	397
Maxfiy kalit	211
Maxfiy kalitli kriptotizim	256
Maxfiy ma’lumotlar	106
Maxfiy ma’lumotlar	421
Maxfiylashtirilishi zarur bo‘lgan ma’lumotlar ro‘yxati	340
Maxfiylashtirish apparaturasi	22
Maxfiylik grifi	101
Maxfiy-rejimli organ (MRO)	322
Maxsus muhofaza belgisi	160
Maxsus tadqiqotlar	189
Maxsus o‘rnatiladigan elektron qurilma	525
Mazmun bo‘yicha bog‘lanish	499
Ma’lum ochiq matn bo‘yicha hujum	28
Ma’lum ochiq xabar bilan qilinadigan hujum	29
Ma’lumotlar	103
Ma’lumotlar almashinuvi	305
Ma’lumotlar banki ma’muriyati	8
Ma’lumotlar bazasi kaliti	206
Ma’lumotlar bazasi ma’muri	5
Ma’lumotlar bazasi tili	580
Ma’lumotlar bazasini boshqarish	8
Ma’lumotlar bazasini boshqarish tili	580
Ma’lumotlar bazasini tiklash	89
Ma’lumotlar bilan ishlashni nazorat qilish	237
Ma’lumotlar bo‘yicha bog‘lanish	498
Ma’lumotlar manbaini autentifikatsiya qilish	39

Ma'lumotlar maydoni	353
Ma'lumotlarni autentifikatsiya qilish	39
Ma'lumotlarni blokirovkalash	62
Ma'lumotlarni mualliflashtirish	3
Ma'lumotlarni muhofaza qilish	145
Ma'lumotlarni nazorat qilish	231
Ma'lumotlarni qayta ishlash rezerv punkti	394
Ma'lumotlarni qayta ishlash zaxira punkti	394
Ma'lumotlarni restavratsiya qilish	414
Ma'lumotlarni tiklash	90
Ma'lumotlarni tiklash	414
Ma'lumotlarni va ularni tashuvchilarni oshkor qilish	409
Ma'lumotlarni xavfsiz uzatish protokoli	385
Ma'lumotlarni yangitdan yaratish	89
Ma'lumotlarni o'chirish qurilmasi	530
Ma'lumotlarni shifrlash algoritmi	14
Ma'lumotlarning buzilishi	186
Ma'lumotlarning ishonchligini tekshirish	376
Ma'lumotlarning sifati	199
Ma'lumotlarning xatoligi	330
Ma'lumotlarning xavfsizligi	46
Ma'lumotlarning yaxlitligi	554
Ma'lumotlarning yaxshi saqlanganligi	467
Ma'lumotlat va ularning tashuvchilarini maxfiylashtirish	143
Ma'mur	4
Ma'muriy xavfsizlik	46
Ma'muriyat	4
Ma'qullangan mahsulot ro'yxati	468
Merkl «daraxti»	110
Merkl sharadasi	563
Mikrob	280
Mikroprotessorli karta	196
Minimal oraliqli kod	221
Minimal ortiqchalikka ega kod	220
Modullarga bo'lish	398
Monitor (dastur)	287
Monitoring	288
Moslik (komponentlarning)	463
Mualliflashtirilgan erkin foydalanish subyekti	494
Mualliflashtirilgan foydalanuvchi	359
Mualliflashtirilmagan foydalana olish	128
Mualliflashtirish	2
Mualliflashtirish sertifikatini	429
Mualliflik huquqi	367
Mualliflik yorlig'i	578

Mualliflikni qayd etish	543
Mualliflikni rad etish	326
Muhofaza (maxfiylik) qulfi	139
Muhofaza biti	58
Muhofaza falsafasi	544
Muhofaza qilinadigan axborot	181
Muhofaza qilinadigan axborotga ta'sir ko'rsatuvchi omil	540
Muhofaza qilinadigan obyekt attestati	31
Muhofaza qilingan avtomatlashtirilgan tizim	439
Muhofaza qilingan fayl	539
Muhofaza qilingan tizim	442
Muhofaza qilinganlik	158
Muhofaza qilinganlikni tahlil qilish	16
Muhofaza qilinganlikni tahlil qilish tizimi	439
Muhofaza qilinmaganlik	296
Muhofaza qilish	144
Muhofaza qilish modeli	283
Muhofaza qilish sertifikatini	431
Muhofaza qilish strategiyasi	492
Muhofaza qilish tizimini chetlab o'tish yo'li	395
Muhofaza qilish vositalari kompleksi	225
Muhofaza qilish vositasi	484
Muhofaza qilishning buzilishi	293
Muhofaza razryadi	406
Muhofaza tizimi ma'muriyati	8
Muhofaza tizimi orqali o'tish, aylanma yo'l	391
Muhofaza vositalari nazorat qilinishini qayd etish	544
Muhofaza vositalarini nazorat qilish	237
Muhofaza yadrosi	580
Muhofazalangan axborot tizimi	445
Muhofazalangan axbotor obyekti	314
Muhofazalangan foydalanish rejimi	413
Muhofazalangan hisoblash texnikasi vositasi	484
Muhofazalangan kanal	192
Muhofazalangan resurs	415
Muhofazalangan umumiy foydalanishdagi telekommunikatsiyalar tarmog'i	436
Muhofazalangan xesh-algoritm	552
Muhofazani bevosita buzishga urinish	361
Muhofazaning kompleksliligi	226
Muhr	341
Mukammal	191
Mukammal maxfiylik	426
Muloqot qila olishga asoslangan firibgarlik	291
Munosabat	326
Murakkablik	458

Mutant viruslar	82
Mutlaqo maxfiy ma'lumotlar	421
Muvofiqlik	465
Muvofiqlik sertifikatini	433
Namoyish etmoq	109
Namuna bo'yicha bog'lanish	498
Nazorat	231
Nazorat kodi	219
Nazorat olib borish	68
Nazorat qilinadigan zona	164
Nazorat raqami	559
Nazorat summasi	495
Nazorat (tekshirish) kodi	219
Nazorat tekshiruv fayli	539
Nazorat topshirig'i	138
Nazorat yozuvi	141
Niderrayter kriptotizimi	252
Niqob biti	59
Niqoblash	269
Nisbiy identifikator	167
Noaniq autentifikatsiya	40
Nolinchi kun zaifligi	537
Nomuvofiqlik	298
Norasmiy	298
Notariallashtirish	301
Noyob nom	175
Nusxa ko'chirilishidan muhofaza qilish	152
Nusxa ko'chirish kartasi	196
Nusxa ko'chirish platasi	343
Obraz	311
Obyekt	311
Obyektdan takror foydalanish	187
Obyektlarni muhofaza qilish	152
Obyektning demaskirovkalovchi bilvosita belgisi	373
Oddiy viruslar	79
Ogohlantiruvchi muhofaza qilish	156
Oldindan to'lov kartochkalari bilan bog'liq firibgarlik	290
Oliy rahbariyat	419
Operatsion tizim	451
Operatsion xavfsizlik	52
Operatsiya (komponent ustida)	319
Operatsiya (obyekt ustida)	319
Operatsiya kodi	220
Oqibat	362
Oqimli shifr	565

Organ	320
Organ sertifikatı	432
Ortiqcha kod bilan bo‘ylama nazorat qilish	233
Ortiqcha siklik kod bilan nazorat qilish	232
Ortiqcha tizim	443
Ortiqchalik	171
Ortiqchalik bo‘yicha nazorat qilish	234
Ortiqchalik bo‘yicha siklik nazorat	234
OXF shaxsiy himoyasi	157
Oxirgi obyekt	315
Oshkora muvofiqlik	465
Ochilish (fosh etilish)	407
Ochiq kalit	209
Ochiq kalit bilan shifrlash	570
Ochiq kalit sertifikatı	432
Ochiq kalitlar infrastrukturası	185
Ochiq kalitli kriptografiya	250
Ochiq kalitli kriptotizim	255
Ochiq kalitni ro‘yxatga olish	411
Ochiq matn	501
Ochiq matnni tanlash asosidagi hujum	27
Ochiq shifrlash	569
Ochiq xavfsiz muhit	472
Ochiqlik darajasi	521
Paket	332
Paketlar filtrlanadigan tarmoqlararo ekran	575
Parazit viruslar	78
Parol	334
Parol bilan muhofaza qilish	155
Parollarnı egallab oluvchilar	143
Parollarnı keshlash	258
Parollarnı ochuvchi	94
Parollashtirish	334
Parolni ko‘rsatish	369
Parolni tez-tez o‘zgartirish bilan qilinadigan hujum	29
Passiv hujum	26
Passiv hujumlar	27
Passiv tahdid	509
Passiv yashirish	336
Pochta bombasi	65
Pochta qurti	561
Polibiy kvadrati	201
Polimorf viruslar	79
Portlarnı skanerlash	457
Portlash	74

Potensial zaiflik	537
Predmet soha	301
Privatlik, xususiylik	372
Protokollar	389
Protsedura firibgarligi	290
Protseduralar bo'yicha xavfsizlik	53
Qabul qilib olish kriteriyalari	256
Qabul qilib olish protseduralari	392
Qarama-qarshi turmoq (qarshi turmoq)	385
Qarorlar qabul qilish kriteriyalari	257
Qarshi chora	229
Qasddan qilinadigan tahdidlar	510
Qator	420
Qat'iy asos	309
Qat'iy belgilash	412
Qat'iy muvofiqlik	466
Qayd qilish	411
Qayta yozadigan viruslar	79
Qayta chaqiruv	96
Qisqa muddatli xato	330
Qoldiq axborot	184
Qoldiq bo'yicha nazorat, n moduli bo'yicha nazorat	234
Qoldiq risk	418
Qoldiq zaiflik	537
Qonuniy foydalanuvchi	360
Qonuniylikni o'zi ta'minlaydigan protokol	388
Qotil paketlar	333
Qulflar va kalitlar tizimi	440
Qurilma drayveri	131
Qurt	560
Qo'lga kiritish masalasi	138
Qo'llanishlik to'g'risidagi bayonot	159
Qo'shimcha kodli so'z	458
Qo'shimcha sektor	427
Qo'shimcha yo'lka	119
Qo'shma audit	37
Rad etib bo'lmaslik	296
Radiokiller	397
Rahbariy hujjatlar	117
Rahbarlik qiluvchi organ	323
Randomizatsiya(lash)	406
Raqamlarni siklik saralash	336
Raqamli imzo	348
Raqamli imzo sxemasi	497
Raqamli imzo tizimi	456

Raqamli imzoli xabar	465
Raqamli imzoni shakllantirish algoritmi	13
Raqamli imzoni tekshirish algoritmi	13
Raqamli «iz»	327
Raqamli konvert	228
Raqamli sertifikat	434
Rasmiy	546
Rasshifrovkalash	410
Raund	411
Raund kaliti	210
Real ochiq tizim xavfsizligi	53
Rejimli obyektlar	317
Resurs	415
Retranslyatsiya qilish bilan yomon niyatda qilinadigan ta'sir	88
Revizor dasturlar	381
Rezerv fayl	540
Rezervlash protsedurasi	391
Rezident	414
Rezident viruslar	80
Rid-Myuller kodlari	224
Rid-Solomon kodlari	224
Risk	417
Risk darajasi	521
Risk egasi	84
Risk kriteriylari	257
Risk taqsimoti	402
Risklar klassi	205
Risklarni aniqlash	319
Risklarni boshqarish	518
Risklarni qayta ishlash	311
Risklarning asosiy tahlili	20
Riskni aniqlash	319
Riskni baholash	328
Riskni boshqarish jarayoni	393
Riskni identifikatsiya qilish	170
Riskni qabul qilish	375
Riskni qayta ishlash	309
Riskni tahlil qilish	18
Riskni to'liq tahlil qilish	19
Riskning pasayishi	460
Rivestr-Shamir-Adleman metodi bilan shifrlash	568
Rol	419
Rollar asosida foydalana olishni boshqarish	514
Ruxsat	404
Ruxsat berish	119

Ruxsat berish kategoriyasi, ruxsat berish	197
Ruxsat etilgan chaqiruv	97
Ruxsat etilgan holat	467
Ruxsat etilmagan tarzda foydalana olish	128
Ruxsatsiz faoliyat	108
Ruxsatsiz foydalana olishdan muhofaza qilish	153
Ro'yxatga olingan foydalanuvchi	359
Ro'yxatga olish organi	322
Sahifani to'ldirish	142
Salbiy ta'sir etish	88
Samaradorlik, natijaviylik	579
Satrlar orasiga kirish	95
Seans darajasidagi shlyuz	573
Seans kaliti	211
Sektorni to'g'rilash	97
Semantik xato	331
Sertifikat	428
Sertifikat yo'li	396
Sertifikatlash	434
Sertifikatlash organi	323
Servislarni identifikatsiya qilish	171
Sifat	199
Sifatni nazorat qilish	233
Signatura	437
Sikllash	143
Siljigan yo'lka	119
Simmetrik autentifikatsiya qilish metodi	276
Simmetrik kriptografik algoritm	12
Simmetrik kriptografiya	250
Simmetrik shifr	566
Sinov	188
Sinov laboratoriyalarini attestatlash	33
Sinxronlanuvchi oqimli kriptotizim	253
Sir	425
Siri bo'lgan bir tomonlama funksiya	550
Sirlarning taqsimlanishi	403
Siyosat	353
Skrembler	457
Skremblerlash	458
Smarfing	460
Sniffing	461
Soxtalashtirish	344
Soxtalashtirish	543
Sozlovchi	326
Spaming	467

Spamni yuborish	410
Spetsifikatsiyalamoq, belgilamoq	468
Spiral yo'lka	119
Spufing	470
Steganografiya	490
Stegokalit	491
Stegokanal	491
Stegokonteyner	491
Stornett-Xaber algoritmi	13
Subkalit	492
Subyekt	492
Subyekt vakolatlari darajasi	520
Supersektor	496
Suqulib kirish	384
Suqulib kirish yo'li	396
Suqulib kirishga sinash	188
Suqulib kirishga testlash	501
So'rov/javob	142
So'rovlar tili	581
Tahdid	504
Tahdidlar agenti (manbai)	3
Tahdidlar manbalari	190
Tahdidlar modeli	285
Tahdidlarning tahlili	20
Tahlil	15
Tahlil maqsadi	556
Tahlil obyekti	312
Tahliliy model	281
Takror(lash)	343
Takrorlanmaydigan (muntazam bo'lmagan, vaqt-vaqti bilan uchraydigan, tasodifiy) xato	331
Takrorlanuvchi kodlar	224
Takrorlash orqali nazorat qilish	232
Talab	503
Talabgor	159
Tanlamoq	96
Tanlangan maydon muhofazasi	155
Taqsimlangan ma'lumotlar bazasi	43
Tarkibiy baholash obyekti	317
Tarkibiy ishonch paketi	333
Tarkibli shifr	566
Tarmoq analizatorlari	22
Tarmoq skaneri	457
Tarmoq tahdidlariga qarshi turish	385
Tarmoq xavfsizligi	55

Tarmoq xizmatining zaifligi	538
Tarmoqdan foydalana olish nuqtasi	502
Tarmoqdan foydalanuvchi identifikatori	169
Tarmoqdan kirib olish	394
Tarmoqlararo ekran	574
Tarmoqlararo ekran ma'muri	7
Tarmoqni tiklash	93
Tarmoqning ish qobiliyati	397
Tarmoqning ishonchliligi	292
Tarqalish	409
Tartib raqami	299
Tasdiqlamoq	351
Tasodifiy bog'langanlik	425
Tasodifiy parollar generatori	100
Tasodifiy son	5621
Tasodifiy tahdidlar	510
Tavsiflamoq	319
Tayinlamoq	293
Tayyorgarlik	344
Tashkilot	324
Tashkilotning xavfsizlik siyosati	356
Tashqi audit	36
Tashqi bostirib kirishlar yo'llari	278
Tashqi destabillashtiruvchi omil	541
Tashqi mantiqiy obyekt	316
Tashqi qo'llanish sohasi	301
Ta'minlamoq	304
Ta'minot kuchlanishi yo'qolganda tiklash	91
Ta'mirlash vaqti	94
Ta'sir etuvchi tashqi omil	540
Ta'sirchan (kritik) axborot	184
Ta'sirchanlik, kritiklik	563
Tekshiruv sikli	559
Telefon qaroqchisi (telefon tarmoqlarini buzuvchi)	342
Telekommunikatsiyalar liniyalari bo'ylab yuklash	136
Telekommunikatsiyalar liniyasidan aktiv o'qish	562
Telekommunikatsiyalar liniyasidan passiv o'qish	562
Telekommunikatsiyalar tarmog'ining axborot xavfsizligi	55
Telekommunikatsiyalar tarmog'ining texnologik xavfsizligi	56
Terminalni identifikatsiya qilish	171
Teshik	131
Teshik, tuynuk	67
Teskari tiklash	91
Test ma'lumotlari	106
Texnik muhofaza qurilmasi	526

Tijorat siri	500
Tiklab bo‘lmaydigan xato	331
Tiklash jurnali	134
Tiklash tizimi	440
Tiklash vaqti	93
Tiklovchi protseduralar	391
Tizim kaliti	212
Tizim ma‘muri	7
Tizimdan foydalana olishlik	130
Tizimni muhofaza qilish	156
Tizimni tekshirish	377
Tizimning osilib qolishi	135
Tizimning yaxlitligi	555
Tozalash	329
Trafikni tahlil qilish	20
Trafikni to‘ldirish	142
Trafikni o‘rniga qo‘yish (to‘ldirish)	351
Trafikning konfidensialligi	240
Translyatsiya	502
Trevoga signalini berish qurilmasi	525
Troyan dasturi	504
Turkum	428
Tushunarli	361
Tuzatib bo‘lmaydigan xato	331
Tuzatish	188
Tuzoq	261
Tuzoqlardan foydalanish	187
To‘la	358
To‘ldirib yuborish hujumi	28
To‘lib ketish	338
To‘liq ajratib bajariladigan hujum, ro‘paradan qilingan hujum	28
To‘liq saralash	336
To‘plash bilan muhofaza qilish	151
To‘siq	370
To‘g‘rilikni nazorat qilish	236
To‘g‘rilovchi harakat	108
Umum foydalanishdagi telekommunikatsiyalar tarmog‘ining axborot xavfsizligi mexanizmi	279
Umumfoydalanish dasturlari	380
Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘i axborot xavfsizligini ta‘minlash tizimi	448
Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘i axborot xavfsizligi obyekti	315
Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘i axborot xavfsizligiga tahdid	508

Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘ining axborot xavfsizligi	56
Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘ining axborot xavfsizligi siyosati	356
Umumiy foydalanishdagi telekommunikatsiyalar tarmog‘ining axborot xavfsizligi xizmati	459
Umumiy kalit	209
Umumiy soha bo‘yicha bog‘lanish	499
Uzilish	370
Uzilishlar analizatori	21
Uzilishni tahlil qilish	17
Uzluksiz ishlashni ta‘minlash va tiklash rejasi	342
Uch martali <i>DES</i> algoritmi	11
Vakil qilish	109
Vakolat	357
Vakolat egasi	84
Vakolatlar matritsasi	271
Vakolatlar profili	390
Vakolatlar ro‘yxati	469
Vakolatli foydalanuvchi	360
Vaksina-dastur	379
Vaksinalash	67
Validatlash (tasdiqlash)	68
Vaqt bombasi	64
Vaqt bo‘yicha belgi qo‘yish	266
Vaqtida o‘zgaruvchi kod	216
Vaqtga bog‘liq bo‘lgan kanal	191
Vaqtga qarab ochiladigan kriptotizim	254
Vaqtinchalik bog‘langanlik	423
Vaqtning belgilash xizmati	523
Vazifa identifikatori	167
Verifikatlash (tekshirish)	71
Verifikator	69
Verifikatsiya va tasdiqlash	72
Verifikatsiyalamoq	71
Vijener kvadrati	200
Virus	76
Virus signaturasi	438
Virusga qarshi dastur	378
Virusni «davolash»	258
Voqea-hodisa	462
Vositachi	363
Vositachi server	428
Xabar	464
Xabarlar manbaidagi zichlash koeffitsiyenti	242

Xabarlar taxtasi	120
Xabarlarni autentifikatsiya qilish kodi	215
Xabarlarni tutib qolish	340
Xabarlarning ketma-ketligini aniqlash	524
Xabarni autentifikatsiya qilish	41
Xabarning haqiqiylikini o'rnatish kodi	221
Xaffman kodi	222
Xakerlik frodi	547
Xarajatlar (foйда)ni tahlil qilish	16
Xatolar bo'lganda tiklash	92
Xatolar jurnali	134
Xatolardan muhofaza qilish	153
Xatolarni tuzatuvchi kodlar	223
Xavf omili	542
Xavfli bo'lmagan viruslar	77
Xavfli viruslar	78
(Xavfli) zona radiusi	398
Xavfsiz dasturiy ta'minot	304
Xavfsiz holat	466
Xavfsiz operatsion tizim	451
Xavfsiz vaqt	93
Xavfsizlik	45
Xavfsizlik atributi	30
Xavfsizlik auditi	35
Xavfsizlik auditori	37
Xavfsizlik axboroti	181
Xavfsizlik belgisi	274
Xavfsizlik bo'yicha topshiriq	137
Xavfsizlik darajasi	519
Xavfsizlik deskriptori	111
Xavfsizlik domeni	118
Xavfsizlik filtri	544
Xavfsizlik funksiyasi siyosati	357
Xavfsizlik holati	467
Xavfsizlik identifikatori	166
Xavfsizlik kategoriyasi	197
Xavfsizlik maqsadi	556
Xavfsizlik markeri	265
Xavfsizlik ma'lumotlari almashinuvi	305
Xavfsizlik (muhofaza qilish) ma'muri	6
Xavfsizlik normasi	299
Xavfsizlik obyekti	312
Xavfsizlik organi	320
Xavfsizlik sertifikat	430
Xavfsizlik siyosati	354

Xavfsizlik siyosati qoidalari	367
Xavfsizlik skaneri	456
Xavfsizlik subyekti	493
Xavfsizlik talablari	503
Xavfsizlik vazifasi	137
Xavfsizlik vositalarini boshqarish	8
Xavfsizlik xizmati	459
Xavfsizlik xizmati	522
Xavfsizlik xizmati ma'muri	7
Xavfsizlik yadrosi	579
Xavfsizlik zonasi	163
Xavfsizlikka tahdid	506
Xavfsizlikni baholash	328
Xavfsizlikni boshqarish	511
Xavfsizlikni ta'minlash sohasidagi standart	490
Xavfsizlikni tekshirish	375
Xavfsizlikni tekshirish ma'lumotlari	105
Xemming kodi	222
Xesh	551
Xesh-funksiya (xeshlash funksiyasi)	552
Xeshlash	552
Xizmat ko'rsatishni rad etish	325
«Xizmat ko'rsatishni rad etish» turidagi hujum	29
Xizmat ko'rsatishni taqsimlangan rad etish	326
«Xol»	396
Xost-bastion	551
Xotira qulfi	140
Xotiraga ega yashirin kanal	194
Xotiraga kira olishni blokirovkalash	62
Xotiraga yozishni blokirovkalash	63
Xotirani muhofaza qilish	154
Xotirani muhofaza qilish kaliti	208
Xotirani qisman buzib yozish metodi	276
Xulosa qilmoq	108
Yarim bayt	358
Yarimformal	358
Yaroqli/yaroqsiz	372
Yaxlitligi muhofazalangan ma'lumotlar	106
Yaxlitlik	553
Yaxlitlik kaliti	213
Yaxlitlik muhofaza qilingan muhit	473
Yaxlitlik muhofazalangan kanal	193
Yaxlitlik xizmati	524
Yaxlitlikni avtonazorat qilish	1
Yaxlitlikning buzilishi	293

Yaxshi himoya qilinmaganlik	534
Yashash vaqti	94
Yashirin boshqarish utilitalari	531
Yashirin eshitish	349
Yashirin kalit	212
Yashirin kanal	193
Yashirish	464
Yashovchanlik	132
Yelka osha yashirincha qarash	344
Yetkazib berish	364
Yomon niyatda qilinadigan ta'sir	85
Yondosh nurlanish	172
Yopiq (muhofazalangan) ma'lumotlar	104
Yopiq kalit	207
Yopiq xavfsiz muhit	472
Yordamchi texnik vositalar	479
Yozib olishdan muhofaza qilish	152
Yozib olishga ruxsat	127
Yozuvdan foydalana olish huquqi	368
Yuklash virusi	75
Yo'lkalarni spiral bo'yicha belgilab chiqish	403
Yo'l-yo'riq ko'rsatuvchi litsenziya	261
Zaifliklar tahlili	20
Zarar	533
Zararli dastur	378
Ziddiyatsizlik	297
Zona	163
Zveno viruslar	81
O'lchash	173
O'lchash funksiyasi	549
O'lchash natijalari	414
O'lchash usuli	276
O'lchov	271
O'lchov birligi	131
O'qish imkoniyatini olish huquqi	368
O'qish uchun ruxsat	128
O'qishdan muhofaza qilish	154
O'rnatilgan qurilma	526
O'rniga qo'yish	350
O'rnini (tartibini) almashtirish	339
O'rnini bosish	139
O'ta uzun ketma-ketlik	362
O'zaro autentifikatsiya qilish	39
O'zaro bog'langan manbalar	190
O'zaro ishonchsizlik	295

O'zgartirish	285
O'zgaruvchan tezlikli kod	221
O'zini o'zi kodlash	420
O'z-o'zidan sinxronlanuvchi oqimli kriptotizim	253
O'z-o'zidan yuklash dasturi	379
O'z-o'zini tekshirish imzosi	347
O'g'irlangan telefon bilan bog'liq firibgarlik	290
Shartlar verifikatori	70
Shaxs identifikatori jetoni	132
Shaxsiy axborot	184
Shaxsiy identifikatsiya raqami	298
Shaxsiy kalit	209
Shaxsiy ma'lumotlar	105
Shaxsiy sirni muhofaza qilish	150
Shaxsiy xavfsizlik muhiti	472
Shaxsni autentifikatsiya qilish, shaxsning haqiqiylikini tasdiqlash	39
Shifr	563
Shifr gammasi	98
Shifrlagich	567
Shifrlangan matn	501
Shifrlangan ma'lumotlar	105
Shifrlash	144
Shifrlash	567
Shifrlash algoritmi	14
Shifrlash funksiyasi	551
Shifrlash kaliti	213
Shifrlash rejimiga o'tish komandasi	225
Shifrlash vositalari	482
Shifrlovchi vosita	489
Shifrmatn	570
Shifrtizim	570
Shkala	571
Chalg'ituvchi belgi	404
Chalg'ituvchi sektor	427
Chaqiruv bo'yicha bog'lanish	498
Chaqiruv-javob	97
Chaqiruvlar daraxti	110
Chaqiruvlarni sotish	382
Chaqiruvni qayta yo'llash xizmatiga asoslangan frod	548
Cheklashni tekshirish	376
Chetlab o'tish rejimi	413
Chetlab o'tishni iloji yo'qligi (OXF)	295
Chiqarib tashlash tuzog'i	262
Chiquvchi trafikni filtrlash	545
Chiziqli kriptotahlil	246

1-xavfli zona	164
2-xavfli zona	164
Bot	66
Bot-tarmoq (botnet)	67
Bouz-Choudxuri-Xokengem kodlari	222
<i>CMEA</i> algoritmi	13
PIN-kodni blokirovkadan chiqarish kaliti	210
SYN to‘lib ketish	338
TEMPEST dasturi	379

Алфавитный указатель терминов на узбекском языке

Atamalarning o‘zbek tili (kirill alifbosi) dagi alifbo ko‘rsatkichi

Атамаларнинг ўзбек тили (кирилл алифбоси) даги алифбо кўрсаткичи

Абонент шифрлаш	567
Абонентни идентификациялаш модули (SIM-карта)	286
Абсолют барқарор шифр	564
Авария ҳолати анализатори	21
Авария(вий)	1
Авариявий тугалланиш	135
Автокорреляция	1
Автоматик верификатор	70
Автоматлаштирилган ахборот тизими	444
Автоматлаштирилган ахборот тизимининг хавфсизлиги	45
Автоматлаштирилган ахборотни қайта ишлаш тизими	449
Автоматлаштирилган тизим ресурсининг хавфсизлиги	53
Автоматлаштирилган тизимга таҳдид	505
Автоматлаштирилган тизимда ахборотни қайта ишлаш	309
Автоматлаштирилган тизимнинг заифлиги	536
Автоматлаштирилган тизимнинг хавфсизлиги	45
Агрегирлаш (бирлаштириш)	3
Аддитив шифр	564
Адрес дешифратори	112
Адресли (диск) майдони	353
Ажратиш	400
Аккредитлаш	9
Акс эттирилмайдиган файл	539
Актив ахборотни муҳофаза қилиш воситаси	485
Актив таҳдид	505
Актив электрон муҳофаза қурилмаси	527
Актив ҳужум тури	75
Активлар	10
Алгоритм	10
Алгоритмик фойдалана олиш	122
Алдов	305
Ал-Жамол алгоритми	15
Алоҳида муҳим маълумотлар	421
Амалга оширишнинг тақдим этилиши	369
Амалий бошқариш	517
Амалий даражадаги шлюз	572
Анализатор	21
Аналитик ҳужум, криптоаналитик ҳужум	25
Аниқ аутентификация	42
Аниқ имзо	346

Аникламок	532
Аникланган потенциал заифликлар	533
Анонимлик калити	205
Антивирус	22
Аппарат воситасида муҳофаза қилиш	144
Аппарат токен	502
Аралаштириб юбориш	338
Арбитрли протокол	387
Архивга оид файл	539
Архивламок	23
Архивлаш	23
Архивлаштирилган файл	539
Асимметрик аутентификация қилиш методи	275
Асимметрик криптографик алгоритм	12
Асимметрик шифр	564
Асимметрик шифрлаш	568
Асосий (базавий) ўлчов	271
Асосий диск	113
Асосий пароль	335
Асосий техник воситалар	480
Атайлаб (қасддан) қилинган хато	330
Атрибут	30
Атрибут сертификати	430
Атрибут қиймати	162
Атрибутлар берувчи орган	321
Аттестатлаш	32
Аудит	34
Аудит далиллари	421
Аудит журнали	133
Аудит критерийлари	256
Аудит хулосалари	96
Аудит ҳажми	318
Аутентификатор	37
Аутентификацион вектор	69
Аутентификацион маълумотлар	104
Аутентификация алмашиниш	305
Аутентификация ахбороти	180
Аутентификация қилинган идентификация	170
Аутентификация қилиш	38
Аутентификация қилиш калити	206
Аутентификация қилиш коди	215
Аутентификация қилиш маркази	553
Аутентификация қилиш сертификати	429
Аутентификация қилиш хизмати	521
Аутентификацияни бошқариш майдони	353

Аутсорсинг	42
Ахборот	179
Ахборот активлари	10
Ахборот алмашилиш объекти	315
Ахборот алмашинуви бўйича ҳамжамият	465
Ахборот базаси	44
Ахборот жараёнлари	394
Ахборот (маълумотлар) узатилишини блокировкалаш	61
Ахборот (маълумотлар) хавфсизлиги	48
Ахборот (маълумотлар)ни муҳофаза қилиш тизими	441
Ахборот (маълумотларни қайта ишлаш жараёни учун)	180
Ахборот муносабатлари субъектининг заифлиги	538
Ахборот муносабатлари субъектларининг манфаатларига таҳдид	507
Ахборот муносабатлари субъектларининг хавфсизлиги	57
Ахборот муносабатларининг субъектлари	494
Ахборот оқимини бошқариш	516
Ахборот оқимлари	366
Ахборот ресурсига кўрсатиладиган ташқи таъсир	86
Ахборот ресурсидан фойдалана олиш	125
Ахборот ресурслари	415
Ахборот таҳдиди	508
Ахборот таҳдидлари (техник воситалар билан амалга ошириладиган) модели	284
Ахборот ташувчилар	300
Ахборот технологияси хавфсизлиги	51
Ахборот тизими	444
Ахборот тизими хавфсизлиги	50
Ахборот тўсиқ	44
Ахборот хавфсизлиги	47
Ахборот хавфсизлиги	49
Ахборот хавфсизлиги инциденти	186
Ахборот хавфсизлиги инцидентларини бошқариш	516
Ахборот хавфсизлиги категорияси	197
Ахборот хавфсизлиги ҳодисаси	462
Ахборот хавфсизлигига таҳдид	507
Ахборот хавфсизлигини бошқариш тизими	453
Ахборот хавфсизлигини бошқариш тизимининг лойиҳаси	383
Ахборот хавфсизлигини таъминлаш концепцияси	241
Ахборот хавфсизлигини таъминлаш тизими	447
Ахборот хавфсизлигини таъминлаш хизмати	460
Ахборот хавфсизлигининг узлуксизлиги	296
Ахборот чиқиб кетадиган канал	194
Ахборот чиқиб кетадиган техник канал	195
Ахборот эгаси	83
Ахборот эгаси	461

Ахборотга бўлган ишонч	115
Ахборотга бўлган эҳтиёж	366
Ахборотга путур етказиш (ахборотни обрўсизлантириш)	228
Ахборотга рухсат этилмаган таъсир	87
Ахборотга қасддан бўлмаган таъсир	87
Ахборотдан муаллифлаштирилмаган тарзда фойдаланишга уриниш	361
Ахборотдан рухсат этилган тарзда фойдалана олиш	125
Ахборотдан рухсатсиз фойдалана олиш	124
Ахборотдан фойдалана олиш	124
Ахборотдан фойдалана олишлик	130
Ахборотдан фойдаланувчи (ахборот истеъмолчиси)	359
Ахборот-коммуникация тизими ахборот хавфсизлигига таҳдид	508
Ахборотлар алмашилиши ва риск юзасидан маслаҳатлашувлар	306
Ахборотлаштириш объекти	314
Ахборотлаштириш объектларини аттестация қилиш	33
Ахборотни актив тутиб қолиш	339
Ахборотни блокировкалаш	60
Ахборотни имитомуҳофазаловчи кодлаш алгоритми	11
Ахборотни йўқ қилиш	510
Ахборотни криптографик муҳофаза қилиш воситалари	478
Ахборотни криптографик муҳофаза қилиш воситаси	487
Ахборотни криптографик муҳофаза қилиш тизими	447
Ахборотни криптографик ўзгартириш	369
Ахборотни (маълумотларни) муҳофаза қилиш	146
Ахборотни муҳофаза қилиш аппарат воситаси	485
Ахборотни муҳофаза қилиш бўйича тадбир	272
Ахборотни муҳофаза қилиш бўйича техник ечим	416
Ахборотни муҳофаза қилиш воситалари	473
Ахборотни муҳофаза қилиш воситаси	484
Ахборотни муҳофаза қилиш ғояси	140
Ахборотни муҳофаза қилиш дастурий воситаси	486
Ахборотни муҳофаза қилиш категорияси	198
Ахборотни муҳофаза қилиш концепцияси	241
Ахборотни муҳофаза қилиш мақсади	557
Ахборотни муҳофаза қилиш механизмларининг кафолатланганлиги	99
Ахборотни муҳофаза қилиш объекти	314
Ахборотни муҳофаза қилиш самарадорлиги	578
Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш	238
Ахборотни муҳофаза қилиш самарадорлигини назорат қилиш воситаси	487
Ахборотни муҳофаза қилиш самарадорлигининг нормалари	300
Ахборотни муҳофаза қилиш соҳасида аккредитлаш	10
Ахборотни муҳофаза қилиш соҳасида аттестатлаш	33
Ахборотни муҳофаза қилиш соҳасида лицензиялаш	259
Ахборотни муҳофаза қилиш соҳасида мувофиқликни сертификатлаш	435

Ахборотни муҳофаза қилиш соҳасида сертификатлаш органи	322
Ахборотни муҳофаза қилиш соҳасида сертификатлаш тизими	452
Ахборотни муҳофаза қилиш соҳасидаги лицензиар	259
Ахборотни муҳофаза қилиш соҳасидаги лицензиат	259
Ахборотни муҳофаза қилиш соҳасидаги мувофиқлик белгиси	161
Ахборотни муҳофаза қилиш техник (аппарат-дастурий) воситалари . .	475
Ахборотни муҳофаза қилиш техник воситаси	486
Ахборотни муҳофаза қилиш тизими	440
Ахборотни муҳофаза қилиш тизимини сертификатлаш	435
Ахборотни муҳофаза қилиш усули	470
Ахборотни муҳофаза қилишнинг жисмоний чора-тадбирлари	274
Ахборотни муҳофаза қилишнинг криптографик усули	276
Ахборотни муҳофаза қилишнинг маънавий-ахлоқий воситалари	474
Ахборотни муҳофаза қилишнинг самарадорлик кўрсаткичи	353
Ахборотни муҳофаза қилишнинг ташкилий воситалари	476
Ахборотни муҳофаза қилишнинг ташкилий чора-тадбирлари	272
Ахборотни муҳофаза қилишнинг техник чора-тадбирлари	273
Ахборотни муҳофаза қилишнинг ҳуқуқий чора-тадбирлари	273
Ахборотни муҳофаза қилишнинг қонунчилик воситалари	476
Ахборотни ошкор этилишдан муҳофаза қилиш	149
Ахборотни пассив тутиб қолиш	340
Ахборотни рухсат этилмаган тарзда фойдалана олишдан муҳофаза қилиш	148
Ахборотни рухсат этилмаган таъсирдан муҳофаза қилиш	148
Ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш воситалари	474
Ахборотни рухсатсиз фойдалана олишдан муҳофаза қилиш тизими . .	442
Ахборотни сохталаштириш	344
Ахборотни ташкилий жиҳатдан муҳофаза қилиш	146
Ахборотни ташкилий-техник жиҳатдан муҳофаза қилиш	147
Ахборотни техник воситалар билан қайта ишлашда муҳофаза қилиш . .	149
Ахборотни техник муҳофаза қилиш	150
Ахборотни техник муҳофаза қилиш воситалари	480
Ахборотни узатишнинг ишончлилиги	121
Ахборотни чиқиб кетишдан муҳофаза қилиш	149
Ахборотни ўзгартириш	286
Ахборотни қайта ишлаш воситалари	479
Ахборотни қайта ишлаш ишончлилиги	121
Ахборотни қайта ишлаш техник воситаси	487
Ахборотни қайта ишлаш техник воситасини экранлаш коэффициенти	243
Ахборотни қўлга киритиш	339
Ахборотнинг бузилиши	405
Ахборотнинг бузилиши	186
Ахборотнинг заифлиги	536
Ахборотнинг ишончлилиги	121

Ахборотнинг ишончилиги	292
Ахборотнинг йўқотилиши ёки бузиб кўрсатилиши	365
Ахборотнинг конфиденциаллиги	239
Ахборотнинг махфийлиги	426
Ахборотнинг ошкор бўлиши	398
Ахборотнинг фoш этилиши	407
Ахборотнинг чиқиб кетиши (йўқолиши)	531
Ахборотнинг яхлитлиги	554
Ахлат йиғиш	420
Базавий компонент	226
Базавий хавфсизлик даражаси	519
Байрок	546
Байроқдан фойдаланиб кодлаш	218
Байт-код верификатори	70
Бардошсизлик	298
Барқарор калит	213
Барқарорлик	525
Баҳо	327
Баҳоланган корреляция	242
Баҳолаш объекти	316
Баҳолаш объекти хавфсизлик функциясининг интерфейси	178
Баҳолаш объекти доирасида узатиш	337
Баҳолаш объекти доирасидан ташқарига узатиш	337
Баҳолаш объекти ресурси	415
Баҳолаш объекти хавфсизлик функцияларининг маълумотлари	107
Баҳолаш объектини хавфсизлик функциялари орасида узатиш	337
Баҳолаш объектининг компоненти	227
Баҳолаш объектининг хавфсизлик функциялари	548
Баҳолаш органи	321
Баҳолаш тизими	451
Баҳоли ишонч даражаси	519
Бевосита муҳофаза қилиш	151
Бевосита тиклаш	92
Бевосита ҳужум	26
Бекор қилиш рўйхатининг сертификати	434
Бекор қилиш сертификати	430
Белла-Лападула модели	282
Бепул дастурлар	380
Билвосита ҳужум	26
«Билиш зарур» принципи	374
Биометрик маълумотлар	104
Биометрия	58
Бир даражали қурилма	528
Бир мартали блокнот	64
Бир мартали пароль	335

Бир мартали рақамли имзо	349
Бир мартали хабар	464
Бир поғонали муҳофаза тизими	442
Бир томонлама аутентификация қилиш	41
Бир томонлама функция	549
Бир томонлама хэшлаш алгоритми	14
Бир томонлама шифрлаш	569
Биргаликда ишлаш	73
Бирин-кетин жойлаштириб муҳофаза қилиш	158
Битларни назорат қилиш	231
Битма-бит нусха кўчирувчи	242
Битма-бит ҳисоблаш	351
Битта кўнғироқ	318
Блок	59
Блокировка	62
Блокировкалаш	59
Блокировкалаш соҳаси	304
Блокли шифр	565
Боғланганлик	422
Боғланганлик (модуль элементларининг боғланганлиги), модулли чидамлилиқ	424
Боғланиш (модуларнинг боғланиши)	497
Боғланишнинг узилиши	371
Боғлиқ бўлган компонент	227
Боғлиқлик	136
Бонинг функционал имкониятлари	89
Бостириб кириш	95
Бостириб киришларни аниқлаш тизими	449
Бот	66
Бот-тармоқ (ботнет)	67
Боуз-Чоудхури-Хокенгем кодлари	222
Бофорт квадрати	200
Бошқариш	511
Бошқариш бўйича боғланиш	500
Бошқариш воситалари	481
Бошқариш мақсади	557
Бошқариш тизими	452
Бошқарувчи символ	439
Бошланғич сон	561
Бошланғич ўрнатиш қиймати	162
Бузиш	73
Бузувчи	74
Бузғунчи	294
Бўйлама (циклик) назорат	236
Вазифа идентификатори	167

Вакил қилиш	109
Ваколат	357
Ваколат эгаси	84
Ваколатлар матрицаси	271
Ваколатлар профили	390
Ваколатлар рўйхати	469
Ваколатли фойдаланувчи	360
Вакцина-дастур	379
Вакциналаш	67
Валидатлаш (тасдиқлаш)	68
Вақт бомбаси	64
Вақт бўйича белги қўйиш	266
Вақтга боғлиқ бўлган канал	191
Вақтга қараб очиладиган криптотизим	254
Вақтда ўзгарувчи код	216
Вақтинчалик боғланганлик	423
Вақтни белгилаш хизмати	523
Верификатлаш (текшириш)	71
Верификатор	69
Верификация ва тасдиқлаш	72
Верификацияламок	71
Виженер квадрати	200
Вирус	76
Вирус сигнатураси	438
Вирусга қарши дастур	378
Вирусни «даволаш»	258
Воситачи	363
Воситачи сервер	428
Воқеа-ходиса	462
Габидулин криптотизими	252
Гаммалаш	99
Гаммалаш шифри	565
Голей кодлари	223
Гопп кодлари	223
Гриф белгиси	275
Гуруҳ (жамоа) бўлиб фойдалана олиш	123
Гуруҳий имзо	346
Давлат сири бўлган маълумотлардан фойдалана олиш	125
Давлат сири ҳисобланадиган маълумотларни ташувчилар	300
Давлат сирлари	427
Дайжест	103
Далил	115
Даражаларга бўлиш	401
Дастур	378
Дастурий бомба	66

Дастурий вирус, вирус	77
Дастурий инженерия	176
Дастурий интерпретация	177
Дастурий махсулот сифатини баҳолаш	328
Дастурий таъминот соҳасидаги ноқонуний фаолият	113
Дастурий таъминот хавфсизлиги	52
Дастурий токен	502
Дастурий ўрнатма	138
Дастурий қароқчилик	342
Дастурларнинг бошланғич кодини зарарлайдиган вируслар	81
Дастурларнинг яхши муҳофазаланмаганлик сканери	457
Дастурни рухсат этилган тарзда таҳлил қилиш	18
Дастурни муаллифлаштириш	3
Дастурни муҳофаза қилиш	156
Дастурнинг осилиб қолиши	135
Декларация (эълон) қилинмаган имкониятлар	88
Демон	109
Дескриптор	111
Дестабиллаштирувчи омил	541
Дестабиллаштирувчи таъсир	85
Детектор дастурлар	381
Дешифратор	112
Дешифрлаш	112
Дешифрлаш алгоритми	11
Диагностик дастур	379
Диагностик хабар идентификатори	167
Директория	113
Диск контроллери	230
Диск формати	547
Дискрецион (танлаб) фойдалана олиш	123
Дискрецион фойдалана олишни бошқариш	513
Дифейсмент	114
Дифференциал криптотахлил	245
Диффи-Хеллман алгоритми	11
Доимий хотирловчи регистр	412
Доимий яхшиланиш	510
Доктор-ревизор дастурлар	380
Домен	118
Домен контроллери	230
Доменларга бўлиш	401
Елка оша яширинча қараш	344
Етказиб бериш	364
Ёзиб олишга рухсат	127
Ёзиб олишдан муҳофаза қилиш	152
Ёзувдан фойдалана олиш ҳукуқи	368

Ёмон ниятда қилинадиган таъсир	85
Ёндош нурланиш	172
Ёпиқ (муҳофазаланган) маълумотлар	104
Ёпиқ калит	207
Ёпиқ хавфсиз муҳит	472
Ёрдамчи техник воситалар	479
Жамоавий махфий қиймат	162
Жараён	392
Жинояткор	159
Жисмоний муҳофаза	157
Жисмоний муҳофаза қилиш воситалари	475
Жисмоний пиггибекинг	341
Жисмоний хавфсизлик	57
Жойланган лицензия	261
Жуда хавфли вируслар	78
Журнал	132
Журналлаштириш	134
Жуфтлик бўйича назорат бити	58
Жуфтлик бўйича бўйлама назорат	235
Жуфтлик бўйича кўндаланг назорат	236
Жуфтлик хатоси	332
Жуфтликни назорат қилиш	237
Жуфтликни назорат қилиш коди	220
Заифликлар таҳлили	20
Зарар	533
Зарарли дастур	378
Звено вируслар	81
Зиддиятсизлик	297
Зона	163
Идентификатор	165
Идентификатор класси	204
Идентификацион (кодли) карта	195
Идентификацион алмаштириладиган модуль	287
Идентификацион белги	275
Идентификацион фойдаланувчи хизматлари модули	287
Идентификацион хавфсизлик сиёсати	355
Идентификация қилиш	169
Идентификациялаш ишончилигини ошириш қурилмаси	529
Идентификациялаш тизими	443
Иерархик маълумотлар модели	283
Ижтимоий инженерия	176
Из	458
Изоҳламоқ	318
Икки портли шлюз	572
Иккиламчи калит	207

Имзо сертификатининг эгаси	84
Имитация	173
Имитобардошлилик	175
Имитомуҳофаза	174
Имитомуҳофаза воситалари	477
Имитомуҳофаза тизими	443
Имитокўшимча	174
Имтиёзлар	372
Имтиёзлар минимуми	281
Имтиёзларни бошқариш структураси	185
Имтиёзларнинг тақсимланиши	402
Индивидуал ҳисобга олиш	532
Индикатор	175
Инициализация вектори	69
Инкор қилиш протоколи	386
Инсталлятор	176
Инсталляция	177
Инструкцион хавфсизлик сиёсати	355
Инструментал ишлаб чиқиш воситалари	479
Инструментал конфигурацияни бошқариш воситалари	481
Интеллектуал карта	196
Интеллектуал муҳофаза қилиш модули	286
Интерпретация (талқин)	177
Интерфейс	178
Интерфейс (маълумотларни қайта ишлаш тизимларида)	178
Информатив сигнал	437
Информатика объектлари	317
Инцидент	185
Исбот қилмоқ	116
Итерация	191
Ифлосланиш	136
Ички алоқа канали	193
Ички аудит	36
Ички дестабиллаштирувчи омил	542
Ички қўлланиш соҳаси	302
Ички фирибгарлик	289
Ички фрод	547
Ички ҳужум	25
Ички қарама-қаршиликсиз	
Ишлаб чиқариш	383
Ишлаб чиқиш	404
Ишлаб чиқиш муҳити	473
Ишлаб чиқувчи	404
Ишламай қолишда фойдалана олиш	129
Ишламай қолишдан сўнг тиклаш	91

Ишламай қолишлар амортизацияси	15
Ишламай қолишларга таъсирчан бўлмаслик	298
Ишламоқ	548
Ишлаш муҳити	473
Ишонч	115
Ишонч маълумотлари	104
Ишончли АТ маҳсулоти	382
Ишончли ахборот алмашинув маркази	558
Ишончли дастурий таъминот	304
Ишончли йўналиш	267
Ишончли канал	192
Ишончли компьютер тизими	446
Ишончли компьютер тизими	115
Ишончли маршрут	267
Ишончли муносабатлар	327
Ишончли ҳисоблаш базаси	43
Ишончилилик	120
Ишончилилик бити	58
Ишончилилик критерийси билан кодлаш	218
Ишончилиликни ялпи текшириш	377
Иштирокни тан олмаслик	297
Йўл-йўриқ кўрсатувчи лицензия	261
Йўлкаларни спираль бўйича белгилаб чиқиш	403
Кабелли хавфсизликни таъминлаш портали	362
Казиски методи	277
Калит (криптографик)	208
Калит оқими	365
Калит оқими генератори	99
Калит сертификати	431
Калит тизими	445
Калитлар алмашинуви	307
Калитлар генерацияси	101
Калитларни аутентификация қилиш ва танлаш тўғрисида битим	463
Калитларни бошқариш	517
Калитларни бошқариш тизими	454
Калитларни олдиндан тақсимлаш схемаси	497
Калитларни очиқ тақсимлаш	408
Калитларни сақлаш учун топшириш	110
Калитларни сертификатлаш маркази	558
Калитларни тақсимлаш	407
Калитларни тақсимлаш маркази	558
Калитларни тақсимлаш протоколи	387
Калитларни тарқатиш хизмати	523
Калитларни тез янгилаш	308
Калитларни ўрнатиш тизими	455

Калитларнинг ҳаётий цикли	559
Калитни очиб кўрсатиш	398
Калитнинг амал қилиш даври	340
Канал	191
Канал бўйича кодлаш	217
Кардано панжараси	416
Кардер	195
Каскадли код	218
Кафолат	99
КБ ҳужжат	117
Квант криптографияси	249
Квинтет	202
Кейлоггер	202
Кенг йўлка	120
Кенгайтириш	410
Кетма-кет боғланганлик	424
Кибержиноят	203
Кибертерроризм	203
Киберхавфсизлик	202
Кира олиш (фойдалана олиш) йўли	395
Кириш (тизимга кириш)	95
Киришда (маълумотларнинг) тўғрилигини текшириш	377
Кирувчи трафикни филтрлаш	545
Кирхгоф принципи	374
Қисқа муддатли хато	330
Клавиатурани блокировкалаш	63
Клавишлар босилишини назорат қилиш	234
Класс	204
Классификациялаш (таснифлаш)	204
Клонлаш	205
Код	214
Код ёзуви	347
Код китоби	214
Кодлаш	216
Кодлаш воситалари	477
Кодлаш тизими	446
Кодлаш чегараси	101
Кодли панжара	416
Кодловчи қурилма	527
Коднинг ортиқчалиги	171
Коллизия	225
Командалар кетма-кетлиги	362
Командаларни ҳисоблагич	500
Комбинатор ахборот манбаи	190
Комбинацияланган портлаш	74

Коммуникатив боғланганлик	423
Коммуникацион тўсиқ	44
Коммуникацион хавфсизлик	51
Коммутацияланадиган линиялар бўйича олисдаги фойдаланувчиларни аутентификация қилиш хизмати	459
Компаньон вируслар	82
Компетентлик	225
Компилятор	225
Комплекс аудит	36
Компонент	226
Компоновка қилиш, умумлаштириш	227
Компрометация (обрўсизлантириш)	227
Компьютер воситасида бузиш	74
Компьютер жинояти	371
Компьютер стеганографияси	490
Компьютер суиистеъмоллиги	160
Компьютер тизимининг аудити	37
Компьютер фирибгарлиги	289
Компьютер хавфсизлиги	51
Контейнер	229
Контрактлар билан боғлиқ фирибгарлик	290
Конфигурация рўйхати	469
Конфигурация элементи	577
Конфигурацияни бошқариш	517
Конфигурацияни бошқариш бўйича хужжатлар	116
Конфигурацияни бошқариш далили	422
Конфигурацияни бошқариш режаси	343
Конфигурацияни бошқариш тизими	454
Конфигурацияни бошқариш тизими ёзувлари	140
Конфигурацияни бошқаришнинг чиқиш маълумотлари	106
Конфиденциал ахборот	182
Конфиденциаллик	238
Конфиденциаллик белгиси	275
Конфиденциаллик категорияси	198
Конфиденциаллик хизмати	522
Концептуал модель	284
Концептуал схема	496
Корпоратив ахборот хавфсизлигини бошқариш	515
Кракер	244
Крекинг	244
Криптоалгоритм	244
Криптобардошли гамма	98
Криптобардошли хабар	464
Криптографик алгоритм	12
Криптографик бардошлилик	246

Криптографик бардошлилик	491
Криптографик воситалар	477
Криптографик илашиш	497
Криптографик муҳофаза қилиш	150
Криптографик назорат катталиги	69
Криптографик назорат қиймати	162
Криптографик протокол	386
Криптографик таҳлил қилиш	17
Криптографик текширув	376
Криптографик тизим	446
Криптографик ускуна	308
Криптографик ўзгартиришлар	370
Криптография	247
Криптология	251
Криптотаҳлил	245
Криптотизим	251
Криптотизимни бузиш, очиш	73
Критик (махфий) бўлмаган ахборот	183
Критиклик	258
Крук криптотизими	252
Кузатиш	292
Кузатмоқ, таққосламоқ	384
Кузатувчи	291
Кутилган жавоб	324
Кутилган жавоб	326
Кучайтириш	521
Кучли аутентификация	41
Кучсиз аутентификация	41
Кўп даражали криптография	248
Кўп даражали қурилма	528
Кўп даражали хавфсизлик	52
Кўп поғонали ҳимоя	151
Кўп факторли аутентификация	40
Кўриб чиқиш	385
Кўринмас вируслар	83
Кўр-кўрона имзо	348
Линиянинг узилиши	406
Лицензия	260
Лицензиялаш	259
Локал блокировкалаш	63
Люк	262
Мажбурий лицензиялаш	260
Мажбуриятларнинг аниқ белгилаб олинishi	400
Мажбурлаш	373
Мазмун бўйича боғланиш	499

Мак Эллис криптолизими	252
Макровирус	263
Манба	190
Манбани кодлаш	217
Мандат	263
Мандатли фойдалана олиш	126
Манипуляцияни аниқлаш	308
Манипуляцияни аниқлаш коди	219
Мантикий (процедуравий) боғланиш	423
Мантикий блокировкалаш	61
Мантикий бомба	65
Манфаатдор бўлмаган ҳакам протоколи	388
Манфаатдор томон	491
Марказлаштирилган тарзда бошқариладиган тармоқ хавфсизлик контроллери	230
Маркер	265
Маскарад	268
Маскиратор	268
Махсус муҳофаза белгиси	160
Махсус тадқиқотлар	189
Махсус ўрнатиладиган электрон қурилма	525
Махфий ахборотдан рухсат этилмаган тарзда фойдалана олиш	125
Махфий ахборотнинг бузилиши	405
Махфий ахборотнинг чиқиб кетиши (йўқолиши)	531
Махфий иш	397
Махфий калит	211
Махфий калитли криптолизим	256
Махфий маълумотлар	106
Махфий маълумотлар	421
Махфий ҳужжатлар ёки буюмларни йўқотиш	532
Махфийлаштирилиши зарур бўлган маълумотлар рўйхати	340
Махфийлаштириш аппаратураси	22
Махфийлик грифи	101
Махфий-режимли орган (МРО)	322
Маъқулланган маҳсулот рўйхати	468
Маълум очик матн бўйича ҳужум	28
Маълум очик хабар билан қилинадиган ҳужум	29
Маълумотлар	103
Маълумотлар алмашинуви	305
Маълумотлар базаси калити	206
Маълумотлар базаси маъмури	5
Маълумотлар базаси тили	580
Маълумотлар базасини бошқариш	8
Маълумотлар базасини бошқариш тили	580
Маълумотлар базасини тиклаш	89

Маълумотлар банки маъмурияти	8
Маълумотлар билан ишлашни назорат қилиш	237
Маълумотлар бўйича боғланиш	498
Маълумотлар ва уларнинг ташувчиларини махфийлаштириш	143
Маълумотлар майдони	353
Маълумотлар манбаини аутентификация қилиш	39
Маълумотларни блокировкалаш	62
Маълумотларни аутентификация қилиш	39
Маълумотларни ва уларни ташувчиларни ошкор қилиш	409
Маълумотларни муаллифлаштириш	3
Маълумотларни муҳофаза қилиш	145
Маълумотларни назорат қилиш	231
Маълумотларни реставрация қилиш	414
Маълумотларни тиклаш	90
Маълумотларни тиклаш	414
Маълумотларни хавфсиз узатиш протоколи	385
Маълумотларни шифрлаш алгоритми	14
Маълумотларни янгитдан яратиш	89
Маълумотларни ўчириш қурилмаси	530
Маълумотларни қайта ишлаш захира пункти	394
Маълумотларни қайта ишлаш резерв пункти	394
Маълумотларнинг бузилиши	186
Маълумотларнинг ишончлилигини текшириш	376
Маълумотларнинг сифати	199
Маълумотларнинг хавфсизлиги	46
Маълумотларнинг хатолиги	330
Маълумотларнинг яхлитлиги	554
Маълумотларнинг яхши сақланганлиги	467
Маъмур	4
Маъмурий хавфсизлик	46
Мақсад	555
Маъмурият	4
Меркл «дарахти»	110
Меркл шарадаси	563
Микроб	280
Микропроцессорли карта	196
Минимал оралиқли код	221
Минимал ортиқчаликка эга код	220
Модуларга бўлиш	398
Монитор (дастур)	287
Мониторинг	288
Мослик (компонентларнинг)	463
Муаллифлаштирилган фойдаланувчи	359
Муаллифлаштирилган эркин фойдаланиш субъекти	494
Муаллифлаштирилмаган фойдалана олиш	128

Муаллифлаштириш	2
Муаллифлаштириш сертификати	429
Муаллифлик ёрлиғи	578
Муаллифлик ҳуқуқи	367
Муаллифликни қайд этиш	543
Муаллифликни рад этиш	326
Мувофиқлик	465
Мувофиқлик сертификати	433
Мукамал	191
Мукамал махфийлик	426
Мулоқот қила олишга асосланган фирибгарлик	291
Муносабат	326
Мураккаблик	458
Мутант вируслар	82
Мутлақо махфий маълумотлар	421
Муҳофаза (махфийлик) қулфи	139
Муҳофаза бити	58
Муҳофаза воситалари назорат қилинишини қайд этиш	544
Муҳофаза воситаларини назорат қилиш	237
Муҳофаза разряди	406
Муҳофаза тизими маъмурияти	8
Муҳофаза тизими орқали ўтиш, айланма йўл	391
Муҳофаза фалсафаси	544
Муҳофаза ядроси	580
Муҳофаза қилинадиган ахборот	181
Муҳофаза қилинадиган ахборотга таъсир кўрсатувчи омил	540
Муҳофаза қилинадиган объект аттестати	31
Муҳофаза қилинган автоматлаштирилган тизим	439
Муҳофаза қилинган тизим	442
Муҳофаза қилинган файл	539
Муҳофаза қилинганлик	158
Муҳофаза қилинганликни таҳлил қилиш	16
Муҳофаза қилинганликни таҳлил қилиш тизими	439
Муҳофаза қилинмаганлик	296
Муҳофаза қилиш	144
Муҳофаза қилиш воситалари комплекси	225
Муҳофаза қилиш воситаси	484
Муҳофаза қилиш модели	283
Муҳофаза қилиш сертификати	431
Муҳофаза қилиш стратегияси	492
Муҳофаза қилиш тизимини четлаб ўтиш йўли	395
Муҳофаза қилишнинг бузилиши	293
Муҳофазаланган ахборот объекти	314
Муҳофазаланган ахборот тизими	445
Муҳофазаланган канал	192

Муҳофазаланган ресурс	415
Муҳофазаланган умумий фойдаланишдаги телекоммуникациялар тармоғи	436
Муҳофазаланган фойдаланиш режими	413
Муҳофазаланган ҳисоблаш техникаси воситаси	484
Муҳофазаланган хэш-алгоритм	552
Муҳофазани бевосита бузишга уриниш	361
Муҳофазанинг комплекслиги	226
Мухр	341
Назорат	231
Назорат (текшириш) коди	219
Назорат ёзуви	141
Назорат коди	219
Назорат олиб бориш	68
Назорат рақами	559
Назорат суммаси	495
Назорат текширув файли	539
Назорат топшириғи	138
Назорат қилинадиган зона	164
Намойиш этмоқ	109
Намуна бўйича боғланиш	498
Нидеррайтер криптолизими	252
Ниқоб бити	59
Ниқоблаш	269
Нисбий идентификатор	167
Ноаниқ аутентификация	40
Ноёб ном	175
Нолинчи кун заифлиги	537
Номувофиклик	298
Норасмий	298
Нотариаллаштириш	301
Нусха кўчирилишидан муҳофаза қилиш	152
Нусха кўчириш картаси	196
Нусха кўчириш платаси	343
Образ	311
Объект	311
Объектдан такрор фойдаланиш	187
Объектларни муҳофаза қилиш	152
Объектнинг демаскировкаловчи билвосита белгиси	373
Огоҳлантирувчи муҳофаза қилиш	156
Оддий вируслар	79
Оқибат	362
Оқимли шифр	565
Олдиндан тўлов карточкалари билан боғлиқ фирибгарлик	290
Олий раҳбарият	420

Операцион тизим	451
Операцион хавфсизлик	52
Операция (компонент устида)	319
Операция (объект устида)	319
Операция коди	220
Орган	320
Орган сертификати	432
Ортиқча код билан бўйлама назорат қилиш	233
Ортиқча тизим	443
Ортиқча циклик код билан назорат қилиш	232
Ортиқчалик	171
Ортиқчалик бўйича назорат қилиш	234
Ортиқчалик бўйича циклик назорат	234
Охирги объект	315
ОХФ шахсий ҳимояси	157
Очилиш (фош этилиш)	407
Очиқ калит	209
Очиқ калит билан шифрлаш	570
Очиқ калит сертификати	432
Очиқ калитлар инфраструктураси	185
Очиқ калитли криптография	250
Очиқ калитли криптитизим	255
Очиқ калитни рўйхатга олиш	411
Очиқ матн	501
Очиқ матнни танлаш асосидаги ҳужум	27
Очиқ хавфсиз муҳит	472
Очиқ шифрлаш	569
Очиқлик даражаси	521
Ошкора мувофиқлик	465
Пакет	332
Пакетлар филтрланадиган тармоқлараро экран	575
Паразит вируслар	78
Паролларни кэшлаш	258
Паролларни очувчи	94
Паролларни эгаллаб олувчилар	143
Пароллаштириш	334
Паролни кўрсатиш	369
Паролни тез-тез ўзгартириш билан қилинадиган ҳужум	29
Пароль	334
Пароль билан муҳофаза қилиш	155
Пассив таҳдид	509
Пассив яшириш	336
Пассив ҳужум	26
Пассив ҳужумлар	27
Полибий квадрати	201

Полиморф вируслар	79
Портларни сканерлаш	457
Портлаш	74
Потенциал заифлик	537
Почта бомбаси	65
Почта курти	561
Предмет соҳа	301
Приватлик, хусусийлик	372
Протоколлар	389
Процедура фирибгарлиги	290
Процедуралар бўйича хавфсизлик	53
Рад этиб бўлмаслик	296
Радиокиллер	397
Рандомизация(лаш)	406
Расмий	546
Расшифровкалаш	410
Раунд	411
Раунд калити	210
Рақамларни циклик саралаш	336
Рақамли «из»	327
Рақамли имзо	348
Рақамли имзо схемаси	497
Рақамли имзо тизими	456
Рақамли имзоли хабар	465
Рақамли имзони текшириш алгоритми	13
Рақамли имзони шакллантириш алгоритми	13
Рақамли конверт	228
Рақамли сертификат	434
Раҳбарий ҳужжатлар	117
Раҳбарлик қилувчи орган	323
Реал очик тизим хавфсизлиги	53
Ревизор дастурлар	381
Режимли объектлар	317
Резерв файл	540
Резервлаш процедураси	391
Резидент	414
Резидент вируслар	80
Ресурс	415
Ретрансляция қилиш билан ёмон ниятда қилинадиган таъсир	88
Ривестр-Шамир-Адлеман методи билан шифрлаш	568
Рид-Мюллер кодлари	224
Рид-Соломон кодлари	224
Риск	417
Риск даражаси	521
Риск критерийлари	257

Риск тақсимооти	402
Риск эгаси	84
Рисклар классификацияси	205
Рискларни аниқлаш	319
Рискларни бошқариш	518
Рискларни қайта ишлаш	311
Рискларнинг асосий таҳлили	20
Рискни аниқлаш	319
Рискни баҳолаш	328
Рискни бошқариш жараёни	393
Рискни идентификация қилиш	170
Рискни таҳлил қилиш	18
Рискни тўлиқ таҳлил қилиш	19
Рискни қабул қилиш	375
Рискни қайта ишлаш	309
Рискнинг пасайиши	460
Роллар асосида фойдалана олишни бошқариш	514
Роль	419
Рухсатсиз фойдалана олишдан муҳофаза қилиш	153
Рухсат	404
Рухсат бериш	119
Рухсат бериш категорияси, рухсат бериш	197
Рухсат этилган ҳолат	467
Рухсат этилган чакирув	97
Рухсат этилмаган тарзда фойдалана олиш	128
Рухсатсиз фаолият	108
Рўйхатга олинган фойдаланувчи	359
Рўйхатга олиш органи	322
Салбий таъсир этиш	88
Самарадорлик, натижавийлик	579
Сатрлар орасига кириш	95
Саҳифани тўлдириш	142
Сеанс даражасидаги шлюз	573
Сеанс калити	211
Секторни тўғрилаш	97
Семантик хато	331
Сервисларни идентификация қилиш	171
Сертификат	428
Сертификат йўли	396
Сертификатлаш	434
Сертификатлаш органи	323
Сигнатура	437
Сиёсат	353
Силжиган йўлка	119
Симметрик аутентификация қилиш методи	276

Симметрик криптографик алгоритм	12
Симметрик криптография	250
Симметрик шифр	566
Синов	188
Синов лабораторияларини аттестатлаш	33
Синхронланувчи оқимли криптотизим	253
Сир	425
Сири бўлган бир томонлама функция	550
Сирларнинг тақсимланиши	403
Сифат	199
Сифатни назорат қилиш	233
Скремблер	457
Скремблерлаш	458
Смарфинг	460
Сниффинг	461
Созловчи	326
Сохталаштириш	344
Сохталаштириш	543
Спаминг	467
Спамни юбориш	410
Спецификацияламоқ, белгиламоқ	468
Спираль йўлка	119
Спуфинг	470
Стеганография	490
Стегокалит	491
Стегоканал	491
Стегоконтейнер	491
Сторнетт-Хабер алгоритми	13
Субкалит	492
Субъект	492
Субъект ваколатлари даражаси	520
Суперсектор	496
Суқулиб кириш	384
Суқулиб кириш йўли	396
Суқулиб киришга синаш	188
Суқулиб киришга тестлаш	501
Сўров/жавоб	142
Сўровлар тили	581
Тайёргарлик	344
Тайинламоқ	293
Такрор(лаш)	343
Такрорланмайдиган (мунтазам бўлмаган, вақт-вақти билан учрайдиган, тасодифий) хато	331
Такрорланувчи кодлар	224
Такрорлаш орқали назорат қилиш	232

Талаб	503
Талабгор	159
Танламоқ	96
Танланган майдон муҳофазаси	155
Тарқалиш	409
Таркибий баҳолаш объекти	317
Таркибий ишонч пакети	333
Таркибли шифр	566
Тармоқ анализаторлари	22
Тармоқ сканери	457
Тармоқ таҳдидларига қарши туриш	385
Тармоқ хавфсизлиги	55
Тармоқ хизматининг заифлиги	538
Тармоқдан кириб олиш	394
Тармоқдан фойдалана олиш нуқтаси	502
Тармоқдан фойдаланувчи идентификатори	169
Тармоқлараро экран	574
Тармоқлараро экран маъмури	7
Тармоқни тиклаш	93
Тармоқнинг иш қобилияти	397
Тармоқнинг ишончлилиги	292
Тартиб рақами	299
Тасдиқламоқ	351
Тасодифий боғланганлик	425
Тасодифий пароллар генератори	100
Тасодифий сон	562
Тасодифий таҳдидлар	510
Ташкилот	324
Ташкилотнинг хавфсизлик сиёсати	356
Ташқи аудит	36
Ташқи бостириб киришлар йўллари	278
Ташқи дестабиллаштирувчи омил	541
Ташқи қўлланиш соҳаси	301
Ташқи мантиқий объект	316
Таъминламоқ	304
Таъминот кучланиши йўқолганда тиклаш	91
Таъмирлаш вақти	94
Таъсир этувчи ташқи омил	540
Таъсирчан (критик) ахборот	184
Таъсирчанлик, критиклик	563
Тақсимланган маълумотлар базаси	43
Таҳдид	504
Таҳдидлар агенти (манбаи)	3
Таҳдидлар манбалари	190
Таҳдидлар модели	285

Таҳдидларнинг таҳлили	20
Таҳлил	15
Таҳлил мақсади	556
Таҳлил объекти	312
Таҳлилий модель	281
Текширув цикли	559
Телекоммуникациялар линиялари бўйлаб юклаш	136
Телекоммуникациялар линиясидан актив ўқиш	562
Телекоммуникациялар линиясидан пассив ўқиш	562
Телекоммуникациялар тармоғининг ахборот хавфсизлиги	55
Телекоммуникациялар тармоғининг технологик хавфсизлиги	56
Телефон қароқчиси (телефон тармоқларини бузувчи)	342
Терминални идентификация қилиш	171
Тескари тиклаш	91
Тест маълумотлари	106
Техник муҳофаза қурилмаси	526
Тешик	131
Тешик, туйнук	67
Тижорат сири	500
Тизим калити	212
Тизим маъмури	7
Тизимдан фойдалана олишлик	130
Тизимни муҳофаза қилиш	156
Тизимни текшириш	377
Тизимнинг осилиб қолиши	135
Тизимнинг яхлитлиги	555
Тиклаб бўлмайдиган хато	331
Тиклаш вақти	93
Тиклаш журнали	134
Тиклаш тизими	440
Тикловчи процедуралар	391
Тозалаш	329
Трансляция	502
Трафикни таҳлил қилиш	20
Трафикни тўлдириш	142
Трафикни ўрнига қўйиш (тўлдириш)	351
Трафикнинг конфиденциаллиги	240
Тревога сигналини бериш қурилмаси	525
Троян дастури	504
Тузатиб бўлмайдиган хато	331
Тузатиш	188
Тузок	261
Тузоклардан фойдаланиш	187
Туркум	428
Тушунарли	361

Тўла	358
Тўлдириб юбориш ҳужуми	28
Тўлиб кетиш	338
Тўлиқ ажратиб бажариладиган ҳужум, рўпарадан қилинган ҳужум ...	28
Тўлиқ саралаш	336
Тўплаш билан муҳофаза қилиш	151
Тўсик	370
Тўғрилиқни назорат қилиш	236
Тўғриловчи ҳаракат	108
Узилиш	370
Узилишлар анализатори	21
Узилишни таҳлил қилиш	17
Узлуксиз ишлашни таъминлаш ва тиклаш режаси	342
Умум фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги механизми	279
Умумий қалит	209
Умумий соҳа бўйича боғланиш	499
Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлиги объекти	315
Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигини таъминлаш тизими	448
Умумий фойдаланишдаги телекоммуникациялар тармоғи ахборот хавфсизлигига таҳдид	508
Умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги	56
Умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги сиёсати	356
Умумий фойдаланишдаги телекоммуникациялар тармоғининг ахборот хавфсизлиги хизмати	459
Умумфойдаланиш дастурлари	380
Уч мартали DES алгоритми	11
Файл вируслари	80
Файл ўзгартирилган сана ва вақт	107
Файл «қуртлари»	560
Файлга кира олиш	126
Файлни муҳофаза қилиш	157
Файлни тиклаш	93
Файстель шифри	566
Файстель тармоғи	436
Фаол ҳужум	25
Фаолият натижалари	414
Фаолиятни қайд қилиш	411
Фатал хато	332
Фақат ёзиш учун хотира	333
Фақат шифрматн бўйича қилинадиган ҳужум	30

Физик блокировкаш	62
Физик таҳдид	509
Физик фойдалана олишни бошқариш	515
Фильтр дастурлар	381
Фирибгарлик	288
Фирибгарлик орқали фойдалана олиш	127
Фишинг	545
Фойдалана олинадиган заифлик	536
Фойдалана олиниши чекланган ахборот	183
Фойдалана олиш	122
Фойдалана олиш (мурожаат қилиш) вақти	94
Фойдалана олиш атрибути	31
Фойдалана олиш даражаси	520
Фойдалана олиш диспетчери, муҳофаза қилиш ядроси	113
Фойдалана олиш идентификатори	167
Фойдалана олиш маркери	266
Фойдалана олиш матрицаси	269
Фойдалана олиш маъмури	7
Фойдалана олиш никоби	267
Фойдалана олиш объекти	313
Фойдалана олиш қоидалари	366
Фойдалана олиш ҳуқуқи	368
Фойдалана олиш ҳуқуқи	368
Фойдалана олиш ҳуқуқларини тақдим этиш	369
Фойдалана олишлик	129
Фойдалана олишни бошқариш тизими	453
Фойдалана олишни белгилаш қоидалари	367
Фойдалана олишни белгилаш қоидаларини бузувчи	294
Фойдалана олишни белгилаш қоидаларини бузувчининг модели	284
Фойдалана олишни белгилаш тизими	451
Фойдалана олишни блокировкаш (ахборотдан)	60
Фойдалана олишни бошқариш	511
Фойдалана олишни бошқариш калити	213
Фойдалана олишни бошқариш сиёсати	357
Фойдалана олишни бошқариш хизмати	523
Фойдалана олишни ваколатли (мандатли) бошқариш	514
Фойдалана олишни мантиқий бошқариш	513
Фойдалана олишни назорат қилиш	232
Фойдалана олишни назорат қилиш механизми	280
Фойдаланиш даври	341
Фойдаланиш тури	75
Фойдаланувчи	359
Фойдаланувчи дастурини тўхтатиб қўйиш қурилмаси	529
Фойдаланувчилар ҳуқуқларини муҳофаза қилиш	155
Фойдаланувчиларнинг эркин фойдаланишини қайд этиш қурилмаси	529

Фойдаланувчини рўйхатга олиш	412
Фойдаланувчининг «очик» ҳаракатлари	108
Фойдаланувчининг «яширин» ҳаракатлари	108
Фойдаланувчининг идентификатори	168
Фойдаланувчининг маълумотлари	105
Фойдаланувчининг профили	390
Фойдаланувчининг ҳуқуқлари	366
Фойдаланувчи-одам	559
Формал хавфсизлик сиёсати модели	284
Форматни ўзгартириш	172
Фродастер	548
Функционал боғланиш	425
Функционал интерфейс	178
Функционал ишончлилик	122
Хабар	464
Хабарлар манбаидаги зичлаш коэффициенти	242
Хабарлар тахтаси	120
Хабарларни аутентификация қилиш коди	215
Хабарларни тутиб қолиш	340
Хабарларнинг кетма-кетлигини аниқлаш	524
Хабарни аутентификация қилиш	41
Хабарнинг ҳақиқийлигини ўрнатиш коди	221
Хавф омили	542
Хавфли бўлмаган вируслар	77
Хавфли вируслар	78
(Хавфли) зона радиуси	398
Хавфсиз вақт	93
Хавфсиз дастурий таъминот	304
Хавфсиз операцион тизим	451
Хавфсиз ҳолат	466
Хавфсизлик	45
Хавфсизлик (муҳофаза қилиш) маъмури	6
Хавфсизлик атрибути	30
Хавфсизлик аудити	35
Хавфсизлик аудитори	37
Хавфсизлик ахбороти	181
Хавфсизлик белгиси	274
Хавфсизлик бўйича топшириқ	137
Хавфсизлик вазифаси	137
Хавфсизлик воситаларини бошқариш	8
Хавфсизлик даражаси	519
Хавфсизлик дескриптори	111
Хавфсизлик домени	118
Хавфсизлик зонаси	163
Хавфсизлик идентификатори	166

Хавфсизлик категорияси	197
Хавфсизлик мақсади	556
Хавфсизлик маркери	265
Хавфсизлик маълумотлари алмашинуви	305
Хавфсизлик нормаси	299
Хавфсизлик объекти	312
Хавфсизлик органи	320
Хавфсизлик сертификати	430
Хавфсизлик сиёсати	354
Хавфсизлик сиёсати қоидалари	367
Хавфсизлик сканери	456
Хавфсизлик субъекти	493
Хавфсизлик талаблари	503
Хавфсизлик фильтри	544
Хавфсизлик функцияси сиёсати	357
Хавфсизлик хизмати	459
Хавфсизлик хизмати	522
Хавфсизлик хизмати маъмури	7
Хавфсизлик ядроси	579
Хавфсизлик ҳолати	467
Хавфсизликка таҳдид	506
Хавфсизликни баҳолаш	328
Хавфсизликни бошқариш	511
Хавфсизликни таъминлаш соҳасидаги стандарт	490
Хавфсизликни текшириш	375
Хавфсизликни текшириш маълумотлари	105
Хакерлик фроди	547
Харажатлар (фойда)ни таҳлил қилиш	16
Хатолар бўлганда тиклаш	92
Хатолар журнали	134
Хатолардан муҳофаза қилиш	153
Хатоларни тузатувчи кодлар	223
Хаффман коди	222
Хемминг коди	222
Хизмат кўрсатишни рад этиш	325
«Хизмат кўрсатишни рад этиш» туридаги ҳужум	29
Хизмат кўрсатишни тақсимланган рад этиш	326
«Хол»	396
Хост-бастион	551
Хотира қулфи	140
Хотирага ёзишни блокировкалаш	63
Хотирага кира олишни блокировкалаш	62
Хотирага эга яширин канал	194
Хотирани қисман бузиб ёзиш методи	276
Хотирани муҳофаза қилиш	154

Хотирани муҳофаза қилиш калити	208
Хулоса қилмоқ	108
Хэш	551
Хэшлаш	552
Хэш-функция (хэшлаш функцияси)	552
Цикллаш	143
Чалғитувчи белги	404
Чалғитувчи сектор	427
Чақирув бўйича боғланиш	498
Чақирув-жавоб	97
Чақирувлар дарахти	110
Чақирувларни сотиш	382
Чақирувни қайта йўллаш хизматига асосланган фрод	548
Чеклашни текшириш	376
Четлаб ўтиш режими	413
Четлаб ўтишни иложи йўқлиги (ОХФ)	295
Чизиқли криптотахлил	246
Чиқариб ташлаш тузоғи	262
Чиқувчи трафикни филтрлаш	545
Шартлар верификатори	70
Шахс идентификатори жетони	132
Шахсий ахборот	184
Шахсий идентификация рақами	298
Шахсий калит	209
Шахсий маълумотлар	105
Шахсий сирни муҳофаза қилиш	150
Шахсий хавфсизлик муҳити	472
Шахсни аутентификация қилиш, шахсинг ҳақиқийлигини тасдиқлаш	39
Шифр	563
Шифр гаммаси	98
Шифрлагич	567
Шифрланган матн	501
Шифрланган маълумотлар	105
Шифрлаш	144
Шифрлаш	567
Шифрлаш алгоритми	14
Шифрлаш воситалари	482
Шифрлаш калити	213
Шифрлаш режимиға ўтиш командаси	225
Шифрлаш функцияси	551
Шифрловчи восита	489
Шифрматн	570
Шифртизим	570
Шкала	571
Экпозиция	577

Экран имитацияси	173
Экранлаш	574
Эксперт	576
Эксперт даражадаги	576
Эксперт тизими	456
Эксплойт	577
Эксплуатацион люк	263
Электромагнит шовқин қурилмаси	530
Электрон муҳофаза қурилмаси	527
Электрон пиггибекинг	341
Электрон рақамли имзо	349
Электрон рақамли имзо воситалари	482
Элемент	577
Эллиптик эгри чизиқ асосидаги криптография	249
Эллиптик эгри чизиқли криптитизим	254
Энтропия	578
Эркин лицензия	261
Эркин фойдаланиш диспетчери концепцияси	240
Эркин фойдаланиш категорияси	198
Эркин фойдаланиш концепцияси	240
Эркин фойдаланиш рўйхати	468
Эркин фойдаланиш субъекти	493
Эркин фойдаланишга рухсат	405
Эркин фойдаланишни бошқариш воситалари	481
Эркин фойдаланишни бошқариш категорияси	198
Эркин фойдаланишни бошқариш рўйхати	470
Эркин фойдаланишни чегаралаш	399
Эркин фойдаланишни чегаралаш воситаси	488
Эркин фойдаланишни чегаралаш режими	413
Эшитиш	384
Эҳтимолий шифрлаш	568
Эҳтимоллик	72
Юклаш вируси	75
Ярим байт	358
Яримформал	358
Яроқли/яроқсиз	372
Яхлитлиги муҳофазаланган маълумотлар	106
Яхлитлик	553
Яхлитлик калити	213
Яхлитлик муҳофаза қилинган муҳит	473
Яхлитлик муҳофазаланган канал	193
Яхлитлик хизмати	524
Яхлитликни автоназорат қилиш	1
Яхлитликнинг бузилиши	293
Яхши ҳимоя қилинмаганлик	534

Яшаш вақти	94
Яширин бошқариш утилиталари	531
Яширин калит	212
Яширин канал	193
Яширин эшитиш	349
Яшириш	464
Яшовчанлик	132
Ўзаро аутентификация қилиш	39
Ўзаро боғланган манбалар	190
Ўзаро ишончсизлик	295
Ўзгартириш	285
Ўзгарувчан тезликли код	221
Ўзини ўзи кодлаш	420
Ўз-ўзидан синхронланувчи оқимли криптолизим	253
Ўз-ўзидан юклаш дастури	379
Ўз-ўзини текшириш имзоси	347
Ўлчаш	173
Ўлчаш натижалари	414
Ўлчаш усули	276
Ўлчаш функцияси	549
Ўлчов	271
Ўлчов бирлиги	131
Ўрнатилган қурилма	526
Ўрнига қўйиш	350
Ўрнини (тартибини) алмаштириш	339
Ўрнини босиш	139
Ўта узун кетма-кетлик	362
Ўқиш имкониятини олиш ҳуқуқи	368
Ўқиш учун рухсат	128
Ўқишдан муҳофаза қилиш	154
Ўғирланган телефон билан боғлиқ фирибгарлик	290
Қабул қилиб олиш критерийлари	256
Қабул қилиб олиш процедуралари	392
Қайд қилиш	411
Қайта ёзадиган вируслар	79
Қайта чақирув	96
Қарама-қарши турмоқ (қарши турмоқ)	385
Қарорлар қабул қилиш критерийлари	257
Қарши чора	229
Қасддан қилинадиган таҳдидлар	510
Қатор	420
Қатъий асос	309
Қатъий белгилаш	412
Қатъий мувофиқлик	466
Қолдиқ ахборот	184

Қолдиқ бўйича назорат, <i>n</i> модули бўйича назорат	234
Қолдиқ заифлик	537
Қолдиқ риск	418
Қонуний фойдаланувчи	360
Қонунийликни ўзи таъминлайдиган протокол	388
Қотил пакетлар	333
Қулфлар ва калитлар тизими	440
Қурилма драйвери	131
Қурт	560
Қўлга киритиш масаласи	138
Қўлланишлик тўғрисидаги баёнот	159
Қўшимча йўлка	119
Қўшимча кодли сўз	458
Қўшимча сектор	427
Қўшма аудит	37
Ҳаволалар монитори	288
Ҳаволалар монитори концепцияси	241
Ҳаётлий цикл	558
Ҳаётлий цикл модели	283
Ҳаётлий циклни аниқлаш	320
Ҳақиқийлик, аслик	42
Ҳақиқийликни аниқлашдаги алмашиш	307
Ҳақиқийликни криптографик аниқлаш	524
Ҳақиқийликни тасдиқлаш	352
Ҳақиқийликни текшириш	377
Ҳаммага маълум хавфсизлик идентификатори	167
Ҳимоя профили	389
Ҳимояга эга хотира	333
Ҳимояланган ахборотлаштириш техник воситаси	158
Ҳисоб беришлик	345
Ҳисобга оид ёзувни блокировкалаш	64
Ҳисобга олиш ёзуви	141
Ҳисоблагич методи	278
Ҳисоблаш тармоғини муҳофаза қилиш	144
Ҳисоблаш техникаси воситаларининг (автоматлаштирилган тизим-нинг) муҳофаза қилинганлик классификацияси	204
Ҳисоблаш техникаси воситаларининг (автоматлаштирилган тизимнинг) муҳофаза қилинганлик кўрсаткичлари	352
Ҳисоблаш техникаси воситаси	483
Ҳисоблаш техникаси объекти	313
Ҳисоблаш тизимидан қасддан фойдаланиш	187
Ҳодисани аниқлагич	320
Ҳосила ўлчов	272
Ҳужжатлар сифати	199
Ҳужжатларни гиперматнли белгилаш тили	580

Ҳужжатлаштирилган ахборот	181
Ҳужум	23
Ҳужум	293
Ҳужум потенциали	365
Ҳужумларни аниқлаш	308
Ҳужумларни аниқлаш тизими	449
Ҳуқуқни бериш	337
1-хавfli зона	164
2-хавfli зона	164
СМЕА алгоритми	13
Java тили	581
PIN-кодни блокировкадан чиқариш калити	210
SYN тўлиб кетиш	338
TEMPEST дастури	379

Алфавитный указатель терминов на английском языке

Atamalarning ingliz tilidagi alifbo ko'rsatkichi

Атамаларнинг инглиз тилидаги алифбо кўрсаткичи

Abnormal end, abend	135
Aborted connection	371
Acceptance criteria	256
Acceptance procedures	392
Access	122
Access administrator	7
Access attribute	31
Access category	198
Access concept	240
Access control	512
Access control	232
Access control category	198
Access control facilities	481
Access control key	213
Access control list	470
Access control mechanism	280
Access control service	523
Access demarcation mode	413
Access demarcation rules	367
Access identifier	167
Access isolation	399
Access isolation facilito	488
Access level	520
Access list	468
Access mask	267
Access matrix	269
Access object	313
Access path	395
Access period	341
Access permission	405
Access right	368
Access right	368
Access rule	366
Access subject	493
Access time	94
Access to information	124
Access to information resource	125
Access to state secret information	125
Access token	266
Access type	75

Accidental threats	510
Account	141
Account lockout	64
Accountability	345
Accreditation	9
Accreditation in the field of information security	10
Active attack	25
Active attack type	75
Active dongle	527
Active information security product	485
Active line-tap	562
Active threat	505
Active wiretapping	339
Activity registration	411
Additive cipher	564
Additive stream cipher	565
Address decoder	112
Address field (disk)	353
Administrative security	46
Administrator	4
Adverse actions	88
Aggregation	3
Ale Hamale algorithm	15
Alert signal transmitting device	525
Algorithm	10
Algorithmic access	122
Analysis vulnerability	20
Analytical attack, cryptanalytical attack	25
Analytical model	281
Analyzer	21
Anonymity key	205
Antivirus	22
Anti-virus program	378
Application management	517
Application-level gateway	572
Archive file	539
Archived file	539
Archiving	23
Assertion checker	70
Assets	10
Assignment	293
Assignment of right	337
Assurance	99
Assurance	115
Assurance to information	115

Asymmetric authentication method	275
Asymmetric cipher	564
Asymmetric cryptographic algorithm	12
Asymmetric encryption	568
Attack	85
Attack	23
Attack detection	308
Attack potential	365
Attestation	32
Attestation in the field of information security	33
Attribute	30
Attribute authority	321
Attribute certificate	430
Attribute value	162
Audit	34
Audit criteria	256
Audit findings	96
Audit scope	318
Audit trail	133
Audit evidence	421
Auditing	68
Augmentation	521
Authenticated identity	170
Authentication	38
Authentication	352
Authentication	377
Authentication and key selection agreement	463
Authentication center	553
Authentication certificate	429
Authentication code	215
Authentication data	104
Authentication exchange	307
Authentication exchange	305
Authentication information	180
Authentication management field	353
Authentication service	521
Authentication vector	69
Authenticity	42
Authenticity, reliability, validity, adequacy	120
Authenticator	37
Authorised user	360
Authority	320
Authority	357
Authority certificate	432
Authority holder	84

Authorization	2
Authorization	369
Authorization certificate	429
Authorized (allowed) state	467
Authorized access subject	494
Authorized access to information	125
Authorized call	97
Authorized profile	390
Authorized program analysis	18
Authorized user	359
Autocorrelation	1
Automated data processing system	450
Automated information system	444
Automated information system security	45
Automated system security	45
Automated system treat	505
Automated system vulnerability	536
Automatized system in guarded construction	439
Automatized system source security	53
Availability	129
Backup file	540
Backup procedure	391
Backward recovery	91
Bad tracking	404
Base component	226
Base measure	271
Baseline risk analysis	20
Baseline security	519
Bastion host	551
Bearers of state secrets	300
Beaufirt square	200
Bella-Lapadula model	282
Between-the-lines entry	95
Biometric	58
Biometric data	104
Birthmarks	396
Bit copier	242
Bit counting	231
Bit counting	351
Blind signature	348
Block	59
Block access (to information)	60
Block cipher	565
Blocking	59
Blowup	74

Bootstrap	379
Bose-Chaudhuri-Hocquenghem codes	222
Bot-net	67
BoT	66
Browsing	385
Bug device	526
Bulletin board	120
By-pass mode	413
Byte code verifier	70
Cable security portal	362
Call coupling	498
Call coupling control	500
Call coupling data	498
Call coupling stamp	498
Call selling	382
Call tree	110
Call-back	96
Capability list	469
Cardano grid	416
Carder	195
Cascade code	218
Casual action on information	87
Cellular Message Encryption Algorithm (CMEA)	13
Centralized security controller	230
Certificate	428
Certification	434
Certification authority	323
Certification authority in field of information security	322
Certification path	396
Certification system in the field of information security	452
Challenge/response	142
Challenge-response	97
Channel	191
Channel coding	217
Check code	219
Check digit	559
Check problem	138
Checking code	219
Checking file	539
Checking sum	495
Chip card	196
Chosen-plaintext attack	27
Ciphering mode command	225
Cipher data	105
Cipher text-only attack	30

Cipher, cypher	563
Ciphertext	501
Ciphertext	570
Ciphony equipment	22
Circuit-level gateway	573
Claimant	159
Class	204
Classification	204
Classification of information and its bearers as secret	143
Clearance	119
Clearing	329
Cloning	205
Closed-security environment	472
CM documentation	117
Code	214
Code book	214
Code grid	416
Code redundancy	171
Code signature	347
Coder	527
Coding	144
Coding	216
Coding bound	101
Coding system	446
Coding tools	477
Coding with fidelity criterion	218
Coherent	361
Cohesion, module strength	424
Coincidental cohesion	425
Cold site	394
Collision	225
Combinatorial source	190
Combined blowup	74
Command sequence	362
Commercial confidentiality	500
Common access software	380
Common coupling	499
Communication barrier	44
Communicational cohesion	423
Communications security	51
Companion viruses	82
Compatible (components)	463
Compiler	225
Complete	358
Completeness	225

Complex audit	36
Complexity	458
Compliance mark in the field of information security	161
Component	226
Component target of evaluation	227
Composed assurance package	333
Composed target of evaluation	317
Compromise	227
Compromising emanation	172
Compulsory licence	260
Computer abuse	160
Computer crime	371
Computer facilities	483
Computer fraud	289
Computer fraud	187
Computer security	51
Computer stenography	490
Computer technology object	313
Computer-system audit	37
Conceptual model	284
Conceptual scheme	496
Confidential data	106
Confidential information	182
Confidentiality	238
Confidentiality mark	275
Confidentiality service	522
Configuration item	577
Configuration list	469
Configuration management	517
Configuration management evidence	422
Configuration management output	106
Configuration management plan	343
Configuration management system	454
Configuration management system records	140
Configuration management tools	481
Configuration management usage documentation	116
Confirm	351
Conformance certificate	433
Conformance certificate in the information security field	435
Conformity	465
Confusion	338
Connectivity	422
Consequence	362
Consistent	297
Container	229

Contamination	136
Content coupling	499
Contingency plan (backup plan, recovery plan)	342
Continual improvement	510
Control	231
Control character	439
Control objective	557
Control record	141
Controlled access system	453
Controlling	511
Controls	481
«Convert» user action	108
Copy card	196
Copy card	343
Copy protection	152
Copyright	367
Copyright notice	578
Correction	188
Corrective action	108
Correlated sources	190
Corruptable store method	276
Costbenefit analysis	16
Counter	385
Counter method	278
Countermeasure	229
Coupling	497
Covert channel	193
Covert channel	194
Covert storage channel	194
Covert timing channel	191
Cracking	74
Cracking	244
Craker	244
Credentials	104
Criticality,criticalness	258
Crook's cryptosystem	252
Cryptanalysis	245
Cryptoalgorithm	244
Cryptoanalysis	17
Cryptographic algorithm	12
Cryptographic authentication	524
Cryptographic chaining	497
Cryptographic check value	69
Cryptographic checkvalue	162
Cryptographic equipment	308

Cryptographic facilities	477
Cryptographic information protection facilities	478
Cryptographic information protection facility	487
Cryptographic key	208
Cryptographic method of information protection	276
Cryptographic protocol	386
Cryptographic system, cryptosystem	446
Cryptographic transformation	370
Cryptographic transformation of information	369
Cryptographic verification	376
Cryptography	247
Cryptology	251
Crypto-proof message	464
Cryptoresistability	491
Cryptosecurity, cryptographically security	150
Cryptostrength	246
Cryptosystem	251
Cryptosystem	570
Cryptosystem discrimination, hacking	73
Cryptosystem with elliptic curve	254
Cryptosystem with temporary disclosure	254
Cybercrime	203
Cybersecurity	202
Cyberterrorism	203
Cyclic redundancy control	232
Cyclic redundancy control	234
Cycling	143
Dangerous area radius	398
Data	103
Data and time stamp	107
Data authentication	39
Data authorization	3
Data cancellation device	530
Data carrier	300
Data communication	305
Data control	231
Data corruption	186
Data corruption	344
Data cryptoprotection system	447
Data destruction	510
Data encryption algorithm	14
Data error	330
Data field	353
Data integrity	554
Data integrity	467

Data interlock	62
Data origin authentication	39
Data processing validity	121
Data protection	145
Data protection facilities	473
Data quality	199
Data reconstitution	89
Data reconstruction	414
Data recovery (reconstruction)	90
Data restoration	414
Data security	46
Data security treat	507
Data transmission blocking	61
Data transmission validity	121
Data validation	376
Databank administration	8
Database administration	8
Database administration language	580
Database administrator	5
Database key	206
Database language	580
Database recovery	89
Data-flow selfsynchronizing cryptosystem	253
Data-flow synchronizing cryptosystem	253
Debugger	326
Deciphering	410
Decision criteria	257
Declassification of information and its carriers	409
Decoder	112
Decryption algorithm	11
Decryption, decipherment	112
Defacement	114
Defence-in-depth	158
Delegation	109
Delivery	364
Demon	109
Demonstrable conformance	465
Demonstrate	109
Denial of service	325
Denial of service attack	29
Denial protocol	386
Dependency	136
Dependent component	227
Derived measure	272
Describe	319

Descriptor	111
Destabilizing impact	85
Destabilizing factor	541
Detector software	381
Determination of password	334
Determine	108
Developer	404
Development	404
Development environment	473
Development tools	479
Device driver	131
Diagnostic message identifier	167
Diagnostic routine	379
Differential cryptanalysis	245
Diffie-Hellman algorithm	11
Diffusion	409
Digest	103
Digital certificate	434
Digital envelope	228
Digital fingerprint	327
Digital signature	348
Digital signature	349
Digital signature checking algorithm	13
Digital signature formation algorithm	13
Digital signature message	465
Digital signature scheme	497
Digital signature system	456
Direct attack	26
Direct attack	361
Directory	113
Disclosure of information	407
Disclosure, reveal	407
Discretionary (selective) access	123
Discretionary access control	513
Disincentive protection	156
Disk controller	230
Disk format	547
Distinguished name	175
Distributed database	43
Distributed denial of service	326
Division	400
Doctor-inspector proram	380
Documentation quality	199
Documented information	181
Domain	118

Domain controller	230
Domain separation	401
Dongle	527
Download	136
Dual-homed gateway	572
Duplication control	232
Eavesdropping	384
Eavesdropping	349
Effectiveness	579
Efficiency factor of information security	353
Egress filtering	545
Electromagnetic noise masking	530
Electronic piggyback	341
Element	577
Elliptic-curve cryptography	249
Email-worm	561
Emergency	1
Emergency (disaster situation) analyzer	21
Encoder, encipher	567
Encountered potential vulnerabilities	533
Encryption	567
Encryption algorithm	14
Encryption facility	489
Encryption function	551
Encryption key	213
End-to-end encryption	567
End-to-end encryption, end-to-end encipherment	569
Enforcement	373
Enhanced correlation	242
Ensure	304
Entrapment	187
Entropy	578
Error log	134
Error protection	153
Error recovery	92
Error-correction code	223
Evaluated products list	468
Evaluation	327
Evaluation assurance level	519
Evaluation authority	321
Evaluation scheme	451
Event	462
Event discriminator	320
Evidence	115
Executive management	4

Exhaustive	191
Exhaustive attack, brute-force attack	28
Exhaustive search	336
Expected response, XRES	324
Expert	576
Expert system	456
Explain	318
Explicit authentication	42
«Explicit» user action	108
Exploit	577
Exploitable vulnerability	536
Exposition	577
Exposure on information resources	86
Extension	410
External audit	36
External context	301
External destabilizing factor	541
External entity	316
External influencing factor	540
External intrusions techniques	278
Extra sector	427
Extra track	119
Faceted cipher	566
Facilities of cryptooperation	482
Facilities of electronic digital signature	482
Facilities of technical protection of information	480
Factor, acting upon protectable information	540
Fail soft	15
Failure access	129
Failure recovery	91
False sector	427
Falsification	543
Family	420
Family	428
Fatal error	332
Fault tolerance	298
Feistel network	436
File access	126
File protection	157
File recovery	93
File viruses	80
File worms	560
Filter programs	381
Firewall	574
Firewall administrator	7

Flag	546
Flag coding	218
Flaw, loophole	67
Flooding attack (overflow)	28
Footprint	458
Formal	546
Formal security policy model	284
Format alteration	172
Forward recovery	92
Fraud	288
Fraud access	127
Fraud based on communication ability	291
Fraudster	548
Free license	261
Freeware	380
Full risk analysis	19
Functional cohesion	425
Functional interface	178
Functional reliability	122
Gabidulin's cryptosystem	252
Gamming	99
Garbage collection	420
General technical facilities	480
Golay codes	223
Goppa codes	223
Governance of information security	516
Governing body	323
Group signature	346
Guidance documentation	117
Hacker	74
Hacking	73
Hacking	361
Hacking fraud	547
Hamming code	222
Hard token	502
Hardware security	144
Harmfull viruses	78
Harmless viruses	77
Hash	551
Hash-function	552
Hashing	552
Herceluan viruses	78
Hiding, concealment	464
Hierarchical data model	283
Highly important information	421

Hijacking	293
Honeypot, penetration entrapment	261
Hot site	394
Huffman code	222
Hypertext markup language	580
ID card (code)	195
Identification	169
Identification integrity increase device	529
Identification mark	275
Identification system, ID system	443
Identifying services	171
Identity	165
Identity authentication, identity validation	39
Identity-based security policy	355
Illegal access	128
Image	311
Imitation	173
Imitation (simulation) of protection	174
Imitoinserter	174
Imitoprotection means	477
Implementation representation	369
Implicit authentication	40
Incident	185
Indicator	175
Indirect attack	26
Indirect unmask object characteristics	373
Indisputable signature	346
Individual accountability	532
Informal	298
Information	179
Information integrity	554
Information (data) protection system	441
Information (data) security	146
Information (in data processing)	180
Information actuality, information integrity	121
Information asset	10
Information availability	130
Information barrier	44
Information base	44
Information blocking	60
Information compromise	228
Information confidentiality	239
Information defence mechanism security	99
Information destruction	405
Information disclosure	398

Information distortion	186
Information encoding igitoprotecting algorithm	11
Information exchange object	315
Information flow	366
Information flow control	516
Information loss	531
Information modification	286
Information need	366
Information owner	83
Information processing facilities	479
Information processing hardware	487
Information processing hardware screening factor	243
Information processing in the automated system	309
Information protection category	198
Information protective measures	272
Information relation subjects security	57
Information reliability	292
Information resources	415
Information safety methods	470
Information science objects	317
Information secrecy	426
Information security	47
Information security	49
Information security category	197
Information security concept	241
Information security continuity	296
Information security efficiency control facility	487
Information security efficiency rates	300
Information security event	462
Information security from disclosure	149
Information security from illegal impact	148
Information security from leak flow	149
Information security from unauthorized access	148
Information security hardware	485
Information security incident	186
Information security incident management	516
Information security management system ISMS	453
Information security management system project	383
Information security object	314
Information security of telecommunications network	55
Information security performance management	238
Information security plan	140
Information security products	484
Information security provision concept	241
Information security service	460

Information security software	486
Information security system	440
Information security system	447
Information security system certification	435
Information security target	557
Information security while processing it with technical facilities	149
Information sharing community	465
Information system	444
Information system security	50
Information technical protection efficiency	578
Information technology security	51
Information treat	508
Information treats model (by technical facilities)	284
Information user	359
Information vulnerability	536
Informational process	394
Informative signal	437
Ingress filtering	545
Initialization value	162
Initialization vector	69
Inoculate	67
Input (data) validation	377
Inroad, intrusion	95
Insecurity	296
Insider attack	25
Inspector programs	381
Installation	177
Installer	176
Integrity	553
Integrity authocontrol	1
Integrity key	213
Integrity-protected channel	193
Integrity service	524
Integrity violation	293
Integrity-protected data	106
Integrity-protected environment	473
Intelligent token	132
Intentional error	330
Intentional threats	510
Inter target security functions of evaluation transfers	337
Interaction	73
Interception problem	138
Interested party, stakeholder	491
Interface	178
Interface (in data processing systems)	178

Interference	370
Internal audit	36
Internal communication channel	193
Internal context	302
Internal destabilizing factor	542
Internal fraud	289
Internal fraud	547
Internal target of evaluation transfer	337
Internally consistent	85
Interpretation	177
Interrupt	370
Interrupt analysis	17
Interrupt analyzer	21
Intrinsic coding	420
Intruder	294
Intruder, malicious user	159
Intrusion detection system	449
Intrusion detection system	449
Invisible file	539
Iteration	191
Java language	581
Joint audit	37
Journal, log	132
Journalizing	134
Justification	309
Kazisky's method	277
Keeking behind shoulder	344
Key certificate	431
Key certification center	558
Key disk	113
Key distribution center	558
Key distribution protocol	387
Key distribution service	523
Key distribution, key management	407
Key escrow	110
Key exchange	307
Key freshness	308
Key generation	101
Key lifecycle	559
Key management	517
Key management system	454
Key scheduling	398
Key setting system	455
Key stream, gamma of the cipher	98
Key system	445

Key to the door protection	442
Key stream generator	99
Keyboard lockout	63
Keylogger	202
Keystream	365
Keystroke verification	234
Kirchhoff principal	374
Knapsack	362
Known-plaintext attack	28
Known-plaintext attack	29
Latent administration utilities	531
Layering	401
Leapfrog attack	29
Least privilege	281
Legal information protective measures	273
Legal user	360
Legislative data protection facilities	476
Level of risk	521
License	260
Licensee in the information protection field	259
Licensing	259
Licensing in the information protection field	259
Licensor in the information protection field	259
Life cycle	340
Life time	94
Life-cycle	558
Life-cycle definition	320
Life-cycle model	283
Likelihood	72
Limit check	376
Limited access information	183
Line disconnect	406
Linear cryptanalysis	246
Linkage, fusion	227
List of information to be classified as secret	340
Loading virus	75
Local lock	63
Lock, locking	62
Locked resource	415
Locking unit	304
Locks and keys (system)	440
Logic bomb	65
Logical (procedural) cohesion	424
Logical access control	513
Logical blocking	61

Logon	95
Log-on	411
Longitudinal parity check	235
Longitudinal redundancy control	233
Longitudinal repundancy check	236
Loop check	559
Loophole	131
Loss	533
Loss or corruption of information	365
Lurker	291
Lurking	292
Mac Alice cryptosystem	252
Macro-virus	263
Mail bomb	65
Main password	335
Maintenance hatch	263
Malicious logic	378
Management system	452
Mandatory access	126
Mandatory access control	514
Manipulation detection	308
Manipulation detection	237
Manipulation detection code	219
Man-to-user	559
Mask bit	59
Masking	269
Maskirator	268
Masquerade	268
Measure	271
Measurement	173
Measurement function	549
Measurement method	276
Measurement results	414
Mechanical verifier	70
Memory lock	140
Memory lockout	62
Memory protection, storage protection	154
Memory write lockout	63
Merkle charade	563
Merkle's tree	110
Message	464
Message authentication	41
Message authentication code	215
Message authentication code	221
Message sequencing	524

Message wiretapping	340
Microbe	280
Mimic resistance	175
Minimum distance code	221
Minimum redundancy code	220
Modification	285
Modular decomposition	398
Monitor (software)	287
Monitoring	288
Monitoring attacks	27
Moral and ethical protection means	474
Multi-factor authentication	40
Multilevel cryptography	248
Multilevel device	528
Multilevel protection	151
Multilevel security	52
Mutant viruses	82
Mutual authentication	39
Mutual distrust	295
Naming class	204
Need-to-know	374
Network access point	502
Network analyzers	22
Network capability	397
Network recovery	93
Network reliability	292
Network scanner	457
Network security	55
Network security	144
Network threat counteraction	385
Network user identifier	169
Network weaving	394
Nibble	358
Nidderrighter's cryptosystem	252
Non-bypassability of the TSF	295
Nonconformity	298
Nonpersistence	298
Non-repudiation	296
Non-repudiation	543
Notarization	301
Object	311
Object of informatization	314
Object protection	152
Object reuse	187
Objective	555

Offset track	119
One-shot digital signature	349
One-sided function	549
One-sided secret function	550
One-way encryption	569
Open-security environment	472
Operating system	451
Operation	319
Operation	319
Operation	548
Operation code	220
Operational data security	52
Operational environment	473
Organization	324
Organizational and technical security of information	147
Organizational information protective measures	272
Organizational protection means	476
Organizational security of information	146
Organizational security policy	356
Outsource	42
Overflow	338
Owner of information	461
Package	332
Packet-filtering firewall	575
Packets - killer	333
Page padding	142
Parasitic viruses	78
Parity check	237
Parity check bit, parity bit	58
Parity check code	220
Parity error	332
Parties of information relationships	494
Passive attack	26
Passive hiding	336
Passive line-tap	562
Passive threat	509
Passive wiretapping	340
Password	334
Password caching	258
Password discriminator	94
Password hook	143
Password protection	155
Penetration	384
Penetration route	396
Penetration test	188

Penetration testing	501
Performance	414
Permanent memory register	412
Permission	404
Permutation	339
Personal data	105
Personal identification number	298
Personal security environment	472
Phishing	545
Phreaker	342
Physical access control	515
Physical blocking	62
Physical information protective measures	274
Physical protection	157
Physical protection facilities	475
Physical security	57
Physical security	151
Physical threat	509
PIN unblocking key, PUK	210
Plaintext	501
Policy	353
Polybius checkerboard	201
Polymorphic viruses	79
Poor authentication	41
Potential vulnerability	537
Power fail recovery	91
Preliminary key distribution scheme	497
Prepaid fraud	290
Preparation	344
Privacy	372
Privacy lock, protection lock	139
Privacy protection	150
Private data	104
Private information	184
Private key	207
Private key	209
Private key cryptosystem	256
Privilege management infrastructure	185
Privilege matrix	271
Privilege sharing	402
Privileges	372
Probability encryption	568
Procedural fraud	290
Procedural security	53
Process	392

Product cipher	566
Production	383
Program authorization	3
Program bomb	66
Program counter control counter	500
Program hang-up	135
Program quality estimation	328
Program vulnerability scanner	457
Program, programme	378
Protected area	163
Protected computer facilities	484
Protected file	539
Protected informatics object	314
Protected information system	445
Protected public switched telecommunications network	436
Protected storage	333
Protected system	442
Protected technical facility of informatization	158
Protected usage mode	413
Protection analysis	16
Protection analysis system	439
Protection bit	406
Protection certificate	431
Protection criterions of facilities of computing machinery (computer-based system)	352
Protection facilities	484
Protection facilities of information from unauthorized access	474
Protection from unauthorized access	153
Protection key	208
Protection model	283
Protection object certificate	31
Protection philosophy	544
Protection profile	389
Protection strategy	492
Protection system from falsified data	443
Protocol with arbiter	387
Protocol with arbitrator	388
Protocols	389
Prove	116
Proxy	363
Proxy server	428
Public key	209
Public key	209
Public key certificate	432
Public key cryptography	570

Public key cryptosystem	256
Public key distribution	408
Public key infrastructure	185
Public key registry	411
Public switched telecommunications network information security	56
Public switched telecommunications network information security mechanism	279
Public switched telecommunications network information security object ..	315
Public switched telecommunications network information security policy ..	356
Public switched telecommunications network information security system	448
Public switched telecommunications network information security service	459
Public switched telecommunications network information security threat ..	508
Public-key cryptography	250
Quality	199
Quality control	233
Quantum cryptography	249
Query language	581
Quintet	202
Radio killer	397
Random challenge	562
Randomisation	406
Randompassword generator	100
Read access	128
Read access control	368
Read protection	154
Real open system security	53
Recovery log	134
Recovery procedures	391
Recovery system	440
Recovery time	93
Redundancy	171
Redundancy control	234
Redundant system	443
Reed-Muller codes, RM codes	224
Reed-Solomon codes, RS codes	224
Reference monitor concept	240
Reference monitor concept	241
Reference monitor concept	288
Reference monitor	114
Refinement	532
Refusal of authorship	326
Regime and secret authority (RSA)	322
Registered user	359
Registration authority	322
Regulation	412

Relationship	326
Relative identifier	167
Relay attack	88
Remote authentication dial-in user service	459
Removable user identity module, R-UIM	287
Repair time	94
Repetition codes	224
Replay	343
Replay (attack)	139
Repudiation	297
Requirement	503
Reset trapping	262
Resident	414
Resident viruses	80
Residual information	184
Residual risk	418
Residual vulnerability	537
Residue check, modulo- <i>n</i> - check	234
Resource	415
Review	15
Review object	312
Review objective	556
Revocation certificate	430
Revocation list certificate	434
Rewriting viruses	79
Risk	417
Risk acceptance	375
Risk analysis	18
Risk assessment	319
Risk category	205
Risk communication and consultation	306
Risk criteria	257
Risk evaluation	328
Risk identification	170
Risk management	518
Risk management process	393
Risk owner	84
Risk reduction	460
Risk sharing	402
Risk treatment	309
Risk treatment	311
Risks assessment	319
Robustness	525
Role	419
Role based access control	514

Round	411
Round key	210
RSA encryption	568
Rule-based security policy	355
Safety standard	299
Scale	571
Scanning port	457
Scrambler	457
Scrambling	458
Screen mimic	173
Screening	574
Seal	341
Sealed key	212
Secondary key	207
Secret	425
Secret documents or articles loss	532
Secret entities	317
Secret information destruction	405
Secret information leaking	531
Secret informations	421
Secret key	211
Secret sharing scheme	403
Secret work	397
Sector alignment	97
Secure channel	192
Secure hash algorithm	552
Secure operating system	451
Secure sockets layer	385
Secure state	466
Secured information	181
Security	158
Security	45
Security	144
Security (safety) administrator	6
Security attribute	30
Security audit	35
Security audit	237
Security audit trail	105
Security audit trail	544
Security auditor	37
Security authority	320
Security bit	58
Security breach	293
Security by generation	151
Security category	197

Security certificate	430
Security class of facilities of computing machinery (computer-based system)	204
Security classification	101
Security clearance, clearance	197
Security complexity	226
Security control	511
Security descriptor	111
Security domain	118
Security evaluation	328
Security exchange	305
Security facilities administration	8
Security filter	544
Security function policy	357
Security functions of object evaluation	548
Security identifier	166
Security implementation standard	490
Security information	181
Security inspection	375
Security kernel	579
Security kernel	580
Security label	275
Security level	519
Security mark	274
Security object	312
Security objective	556
Security of information (data)	48
Security policy	354
Security policy realization	451
Security policy rules	367
Security policy violator	294
Security policy violator model	284
Security problem	137
Security requirement	503
Security scanner	456
Security service	522
Security service	459
Security service administrator	7
Security software	304
Security state	467
Security subject	493
Security system administration	8
Security target	137
Security threat	506
Security time	93

Security token	265
Security trapdoor, bypass path	391
Security zone	163
Seed	561
Selection	96
Selective field protection	155
Self maintain law protocol	388
Self-verifying signature	347
Semantic error	331
Semiformal	358
Sensitive information	184
Sensitivity	198
Sensitivity	563
Separation of duties	400
Sequence number	299
Sequential cohesion	424
Session key	211
Shared access	123
Shared secret	162
Shrink-wrap license	261
Signature	437
Signature certificate owner	84
Signer response	326
Sign-on	369
Simple viruses	79
Single sided hashing algorithm	14
Single-level device	528
Single-shot message	464
Single-side authentication	41
Single-use pad	64
Single-use password	335
Site license	261
Smart card	196
Smart protection card	286
Smurfing	460
Sniffing	461
Social engineering	176
Soft error	330
Soft token	502
Software bug	138
Software engineering	176
Software interpretation	177
Software lock (software protection)	156
Software piracy	113
Software piracy	342

Software security	52
Source	190
Source coding	217
Source compressing factor	242
Spamming	467
Spamming	410
Special electronic inset device	525
Special security mark	160
Special study	189
Specify	468
Spiral track	119
Spiral tracking	403
Spoof	305
Spoofing	470
State secrets	427
Stateful inspection firewall	576
Statement of applicability	159
Stealth viruses	83
Steganography	490
Stegochannel	491
Stegocontainer	491
Stegokey	491
Stolen phone fraud	290
Stornett Khaber algorithm	13
Stream cipher, general stream cipher	565
Strict conformance	466
Strong authentication	41
Strong gamma	98
Strong key	213
Stun/unstun	372
Subject	492
Subject privilege	520
Subkey	492
Subscriber identification module, SIM	286
Subscription fraud	290
Substitution	350
Supersector	496
Supplementary codeword	458
Support technology	479
Symmetric authentication method	276
Symmetric cipher	566
Symmetric cryptographic algorithm	12
Symmetric cryptography	250
SYN overflow	338
System administrator	7

System availability	130
System checkout	377
System integrity	555
System key	212
System protection (sistem security)	156
System quiescing	135
Tampering	344
Target of evaluation	316
Target security functions of evaluation data	107
Target security functions of evaluation interface	178
Task identifier	167
Technical (hardware and software) data protection facilities	475
Technical convert channel	195
Technical information protective measures	273
Technical information security equipment	486
Technical protection device	526
Technical protection of information	150
Technical solution on information security	416
Technological security of telecommunications network	56
TEMPEST program	380
Temporal cohesion	423
Temporary (intermittent, soft, transient) error	331
Terminal identification	171
Terminal object	315
Test data	106
Test, testing	188
Testing laboratories attestation	33
Threat	504
Threat agent	3
Threat analysis	20
Threat model	285
Threat source	190
Throughout authentication	377
Ticket, capability	263
Time bomb	64
Time stamping	266
Time stamping service	523
Time variant code	216
To archive	23
To tailgate	341
TOE resource	415
TOE security functionality	89
Token	265
Top management	419
Top secret informations	421

Trace	384
Traffic analysis	20
Traffic confidentiality	240
Traffic padding	142
Traffic padding	351
Transfers outside of the target of evaluation	337
Translation	502
Transparency level, clearance	521
Transverse parity check	236
Trapdoor	262
Trapdoor	395
Treat factor	542
Treat towards infocommunication system information security	508
Treat towards the interests of information relapses subjects	507
Trojan programm	504
Trust relationships	327
Trusted channel	192
Trusted computer system	115
Trusted computer system	446
Trusted computing base	43
Trusted computing base	225
Trusted information communication entity	558
Trusted IT product	382
Trusted path	267
Trusted path	267
Trusted software	304
TSF self-protection	157
Tumbling	336
Unauthorized access	128
Unauthorized access data protection system	442
Unauthorized access to information	124
Unauthorized access to secret information	125
Unauthorized action	108
Unauthorized action on information	87
Unbreakable cipher	564
Unclassified information	183
Unconditional secrecy	426
Uncorrectable error	331
Undeclared capabilities	88
Under control zone	164
Unit of measurement	131
Unit viruses	81
Universe of discourse	301
Unrecoverable error	331
User	359

User data	105
User identifier, user ID	168
User profile	390
User program interrupt device	529
User registration	412
User rights protection	155
User services identity module	287
Users access registration device	529
Usr rights	366
Vaccine program	379
Validation (statement)	68
Validation of objects of informatization	33
Validity bit	58
Validity check	236
Variablerate code	221
Verification (check)	71
Verification and validation, V&V	72
Verifier	69
Verify	71
Viability	132
Vigenera square	200
Virus	76
Virus signature	438
Virus treatment	258
Viruses, attaching program initial code	81
Vulnerability	534
Vulnerability of information relapse	538
Vulnerability of network service	538
Wan-giri	318
Well-known security identifier	167
Wide track	120
Wiretapping	339
Worm	560
Write - only memory	333
Write access	127
Write access control	368
Write protect	152
Zero day exploit	537
Authentication key, A-KEY	206
Access control policy	357
Premium rate service fraud, PRS fraud	548
Program virus, virus	77
1 danger area	164
2 danger area	164
3DES (Triple DES)	11

Список использованных источников

Foydalanilgan manbalar ro'yxati

Фойдаланилган манбалар рўйхати

1. Англо-русский словарь: Мультимедиа-системы. Телекоммуникационные компьютерные сети. Безопасность компьютерных систем и сетей. / Мячев А.А., Алексеев Е.С., Веселов В.Н. и др. – М.: Радио и связь, 1995. – 192 с.
2. Безопасность в электросвязи и информационных технологиях. – Международный союз электросвязи, 2006.
3. Глоссарий криптографических терминов. – <http://www.enlight.ru/crypto/glossary/glossary.htm>.
4. Гринберг А.С., Горбачев Н.Н., Теплаков А.А. Защита информационных ресурсов государственного управления. Учебное пособие. – М.: ЮНИТИ-ДАНА, 2003.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты - <http://www.winblog.ru/2006/12/27/27120601.html>.
6. Концепция создания банковской инфраструктуры открытых ключей. // Управление защитой информации, 2007.
7. Лукацкий А.В. Краткий словарь по информационной безопасности. Версия 1.0 - http://software-testing.ru/lib/reviews/terminology/sec_dic.pdf.
8. Люцарев В.С., Ермаков К.В. и др. Безопасность компьютерных сетей на основе Windows NT. – М.: Издательский отдел «Русская редакция ТОО «Channel Nrading Ltd», 1998. – 304 с.
9. Невдяев Л.М. Глоссарий. Мобильная безопасность: от А до Z. // Информ-КурьерСвязь, № 3, 2004.
10. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие. – М.: ФОРУМ:Инфра-М, 2002.
11. Приходько А.Я. Словарь-справочник по информационной безопасности. – М.: СИНТЕГ, 2001. – 124 с.
- Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие – С.Пб.: БХВ-Перебург, Армет, 2002.
12. Терминология в области защиты информации. Справочник. – М.: ВНИИ-стандарт, 1993.
13. Словарь-справочник терминов и определений в области защиты информации и обеспечения информационной безопасности – http://www.zastava.ru/infostore_glossary.shtml.
14. Tst 45.010:2002 Отраслевой стандарт. Информационная безопасность в сфере связи и информатизации. Термины и определения. – Ташкент: Узбекское агентство связи и информатизации, 2002.
15. O'z DSt ISO/IEC 2382-8:2007 Государственный стандарт Узбекистана. Информационные технологии. Информационная безопасность. Термины и определения. – Ташкент: Узбекское агентство стандартизации, метрологии и сертификации (агентство «Узстандарт»).
16. O'z DSt 1109:2006 Государственный стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Термины и определения. – Ташкент: Узбекское агентство стандартизации, метрологии и сертификации (агентство «Узстандарт»).

17. Бизнес–Безопасность–Телекоммуникации. Терминологический словарь. – М.: Радио и связь, 2002.

18. O'z DSt ISO/IEC 15408-1:2008 Государственный стандарт Узбекистана. Информационная технология. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий. Введение и общая модель. – Ташкент: Узбекское агентство стандартизации, метрологии и сертификации (агентство «Узстандарт»).

19. O'z DSt 2927:2015 Государственный стандарт Узбекистана. Информационная технология. Информационная безопасность. Термины и определения. – Ташкент: Узбекское агентство стандартизации, метрологии и сертификации (агентство «Узстандарт»).

20. O'z DSt ISO/IEC 27000:2014 Государственный стандарт Узбекистана. Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь. – Ташкент: Узбекское агентство стандартизации, метрологии и сертификации (агентство «Узстандарт»).

«UNICON.UZ» Давлат унитар корхонаси
директорининг ўринбосари

_____ М. Джалалов

Ўзбекистон Радиотехника, электроника ва
алоқа илмий-техника жамияти раисининг
ўринбосари, т.ф.д., профессор

_____ М. Мухитдинов

Атамашунослик ва луғатлар
хизмати бошлиғи

_____ Ё. Аҳмедова

Таржимон

_____ Ш. Тўлаганов

Норма назорати

_____ Л. Шаймарданова

КЕЛИШИЛДИ

Ўзбекистон Республикаси Ахборот
технологиялари ва коммуникацияларини
ривожлантириш вазирлигининг

2018 йил «__» _____даги
_____ -сон хати

«UNICON.UZ» Давлат унитар корхонаси
директорининг ўринбосари

_____ А. Кадилов

«Ахборот хавфсизлиги ва криптология»
илмий-тадқиқот департаменти
«Криптография» илмий тадқиқот бўлими _____ С. Абрамова
етакчи муҳандиси

Атамашунослик ва луғатлар
хизмати бошлиғи _____ Ё. Аҳмедова

Таржимон _____ Ш. Тўлаганов

Норма назорати _____ Л. Шаймарданова

КЕЛИШИЛДИ

Ўзбекистон Республикаси ахборот
технологиялари ва коммуникацияларини
ривожлантириш Вазирлиги

Ахборот хавфсизлиги бўлимининг

2016 йил « 19 » майдаги

14-8/2870 -сон хати