O’ZBEKISTON RESPUBLIKASI OLIY VA O’RTA MAXSUS TA’LIM VAZIRLIGI

BUXORO MUHANDISLIK TEXNOLOGIYA INSTITUTI

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta’limi («Informatika va axborot texnologiyalari») ta’lim yo’nalishi bo’yicha

«MS SQL Server 2005 muhitidagi xavfsizlik masalalarini namoyish qiluvchi elektron ko`rgazma yaratish» mavzusidagi

BITIRUV MALAKAVIY ISH

Bajardi: **14-09 MIIT guruhi talabasi**
Mamatova S.Y.

Rahbar: **Nurullayev M.M.**

Himoyaga ruxsat etildi

“____”_____2013y.

Kafedra mudiri: _____ dots. Razzoqov Sh.I.

BUXORO - 2013

BUXORO YUQORI TEXNOLOGIYALAR MUHANDISLIK TEXNIKA INSTITUTI

«TEXNOLOGIK JARAYONLARNI AVTOMATLASHTIRISH» fakulteti

«Informatika va axborot texnologiyalari» kafedrasi

5140900 – Kasb ta'limi («Informatika va axborot texnologiyalari») ta'lim yo'nalishi

14-09 MIIT guruhi

«Tasdiqlayman»_____

Kafedra mudiri dots.Razzoqov Sh.I.

«_____» _____ 2012 y.

BITIRUV MALAKAVIY ISHI BO'YICHA TOPSHIRIQ

Talaba: Mamatova Sadoqat Yunus qizi

1. Bitiruv malakaviy ish mavzusi: «MS SQL Server 2005 muhitidagi xavfsizlik masalalarini namoyish qiluvchi elektron ko`rgazma yaratish»

Kafedra majlisida 08.11.2012 yil tasdiqlangan.

2. Bitiruv malakaviy ishini topshirish muddati: «__05__» iyun 2013 yil

3. Bitiruv malakaviy ishni bajarish uchun kerakli ma'lumotlar:

Adabiyotlar, BMI mavzusi bo'yicha nazariy ma'lumotlar, Flash va Front Page dasturlash tizimi.

4. Hisoblash-tushuntirish yozuvlarining tarkibi (ishlab chiqilgan masalalar ro'yxati):

Kirish; Mavzu bo'yicha nazariy ma'lumotlar; Asosiy qism; Mavzu mazmunining qisqacha bayoni; BMI dasturiy mahsulotini yaratish tartibi va uni yaratishda qo'llaniladigan dastur tizimlari; Hayot faoliyati xavfsizligi; Xulosa; Foydalanilgan adabiyotlar ro'yxati; Ilova.

5. Chizma ishlab chiqarish ro'yxati (chizmalar nomi aniq ko'rsatiladi): *Yo'q*

6. Bitiruv ishi bo'yicha maslahatchilar:

№	Bo'lim mavzusi	Maslahatchi o'qituvchi	Imzo	
			Topshiriq berildi	Topshiriq bajarildi
1	Nazariy qism	Nurullayev M.M.		
2	Asosiy qism	Nurullayev M.M.		
3	Hayot faoliyati xavfsizligi	Beshimov Y.S.		

7. Bitiruv ishini bajarish rejasi:

№	Bitiuv ishi bosqichlari nomi	Bajarish muddati, sana	Tekshiruvdan o'tganlik belgisi
1	Mavzu bilan tanishish, adabiyotlar ustida ishlash	Noyabr-Dekabr	
2	Bitiruv malakaviy ishining I bobi ustida ishlash	Yanvar-Fevral	

3	Bitiruv malakaviy ishi mavzusining dasturi ustida ishlash	Mart-Aprel	
4	Bitiruv malakaviy ishining II bobi ustida ishlash	May	
5	«Hayot faoliyati xavfsizligi» bobi ustida ishlash	May	
6	Bitiruv malakaviy ishini rasmiylashtirish	Iyun	
7	Bitiruv malakaviy ishi himoyasiga tayyorlanish	__iyun __ iyun	
8	Bitiruv malakaviy ishini himoya qilish	_____iyun	

Bitiruv malakaviy ishi rahbari: _____ Nurullayev M.M.

Topshiriqni bajarishga oldim: _____ Mamatova S.Y.

Topshiriq berilgan sana:
«_____»_____2012 yil

MUNDARIJA

14-09 МІІТ гуруҳи талабаси Маматова Садоқатнинг “MS SQL Server 2005 муҳитидаги хавфсизлик масалаларини намойиш қилувчи электрон кўргазма яратиш” мавзусидаги битирув малакавий ишига

АННОТАЦИЯ

Ушбу битирув малакавий ишида MS SQL Server 2005 муҳитидаги хавфсизлик масалаларини намойиш қилувчи электрон кўргазма яратилган.

Битирув малакавий иши кириш, назарий қисм, асосий қисм, ҳаёт фаолияти хавфсизлиги қисми, хулоса ва фойдаланилган адабиётлар рўйхатларидан иборат.

Кириш қисмида асосан масаланинг долзарблиги ва актуаллиги, шу билан бирга масаланинг амалий аҳамиятлари келтирилган.

Назарий қисмида масалани ечиш учун зарур бўлган назарий маълумотлар ва электрон кўргазманинг ўқув жараёнида тутган ўрни ва уни яратиш технологиялари, ҳамда яратилаётган электрон кўргазманинг мавзуси бўйича назарий маълумотлар, ахборот хавфсизлиги бўйича, маълумотлар базалари тўғрисида батафсил маълумот келтирилган.

Асосий қисмда масаланинг қўйилиши ва уни ечиш усуллари келтирилган. SQL Server 2005 да авторизация ва аутентификация, унинг хизматларида ҳуқуқлар бошқаруви, минимал ҳуқуқлар билан кодни бажариш, маълумотлар ва трафикни шифрлаш каби масалалар батафсил ёритиб берилган.

Тайёрланган битирув малакавий иш Олий ва ўрта махсус ўқув юртларида таълим оладиган талабалар учун мўлжалланган. Электрон кўргазманинг яна бир афзаллиги шундаки, у ўзбек тилида тайёрланган. Бу электрон кўргазма нафақат ОЎЮнинг талабалари, балки ихтиёрий маълумотлар базаси фойдаланувчилари учун ҳам қизиқарли, ҳам фойдали бўлади.

КИРИШ

XXI аср илмий-техника инқилоби мислсиз суръатларда илгарилаётган давр. Бу даврда ахборот технологиялари соҳаси вужудга келди ва у жадал ривожланиб инсон фаолиятининг барча жабҳаларига кириб бормоқда. Ахборот ресурслари ҳажми хам кундан кунга ортиб бормоқда. Ахборот ресурсларини сақлаш, ишлов бериш ва узатиш учун мижоз компьютерлари, серверлар, компьютер тармоқлари ва дастурий воситалардан фойдаланилмоқда. Ўз навбатида бу маълумотларни, бу воситалардан ўғирлаш учун турли таҳдидлар ва ҳужумлар ҳам ошди. Шунинг учун, бу таҳдидларга қарши хавфсизлик чора-тадбирлари ишлаб чиқила бошланди.

Кундалик ҳаётимизда барчамиз маълумотлар базасидан фойдаланамиз ва улар турли хил шаклда сақланади. Ахборот технологияларининг ривожланиши, маълумотлар базаларини компьютер хотирасида сақлаш, уни шакллантириш ва ундан фойдаланиш имконини берди. Айниқса, компьютер тармоқларининг яратилиши маълумотлар базаларидан кўпчиликнинг тармоқ орқали фойдаланишига йўл очиб берди. Маълумотлар базалари билан ишлашни ташкил қилиш учун махсус дастурлар мажмуаси, яъни маълумотлар базасини бошқариш тизими (МББТ) ишлатилади. Ҳозирги кунда маълумотлар базаларининг кўпчилиги реляцион моделга асосланиб қурилмоқда. Ўз навбатида бу моделга асосланган MS Access, MS SQL Server, Oracle, PostgreSQL сингари МББТ лари энг кўп ишлатилади. Улар бир-биридан имкониятлари ва ҳимояланиш даражаси билан фарқ қилади.

Мавзунинг долзарблиги: Иш жараёнини ташкил қилиш учун ишлатилаётган маълумотлар базаларининг кўпчилиги SQL Server МББТ да яратилмоқда. Чунки, у жуда ҳам тез ишлайдиган реляцион МББТ ҳисобланади. Бундан ташқари маълумотлардан тармоқ орқали фойдаланиш амалга оширилаётганлиги сабабли хавфсизлик масалалари ҳозирги кунда энг долзарб муаммолардан бирига айланди. Шунинг учун, маълумотларни имкон даражада ҳимоялаш усулларининг энг мақбул усулларини излаб топиш ва уни қўллаш талаб қилинади. Шу сабабли, SQL Server да ҳимояланиш масалалари бўйича ўзбек тилида маълумотлар йўқлиги ҳамда ҳимояланиш масалаларига эътибор берилаётганлиги сабабли ушбу мавзу танлаб олинди.

Ишнинг мақсади. Мавзу доирасида SQL Server 2005 да қандай ҳимояланиш ташкил қилингани таҳлил қиламиз ва ушбу таҳлилга асосланган ҳолда энг асосий жиҳатларини баён қиламиз. Бунинг учун, шу соҳа бўйича жаҳонда амалга оширилган ишлар билан танишамиз, интернет тизимида мавжуд булган ахборотларни ўрганамиз. Санаб ўтилган ҳужжатлар улкан ахборот оқимини ҳосил қилади, унинг суръати йилдан–йилга ошиб бормоқда. Бундай улкан ахборот оқимида зарур ахборотни излаб топиш анча мураккаб жараён ҳисоблансада, керакли ахборотларни танлаб олган ҳолда мавзуни тавсифлашга ҳаракат киламиз.

Ишнинг вазифаси. SQL Server да маълумотлар базасининг хавфсизлигини таъминлаш мавзусини очиб бериш учун энг аввало: Маълумотлар базаси ва маълумотлар базасини бошқариш тизими, мижоз-сервер ва тақсимланган маълумотлар базаси технологияси, маълумотлар базасининг хавфсизлиги ва SQL Server маълумотлар базасини бошқариш тизими ва маълумотлар базаси билан ишлаш ҳақида асосий тушунчаларни қисқача тавсифлаймиз. Шундан сўнг бевосита SQL Server маълумотлар базасида ҳимоя усулларини кўриб чиқамиз.

Ишнинг амалий аҳамияти. Биз кундалик ҳаётимизда турли хил маълумотлар базаларини яратамиз. Бу маълумотлар базасидан турли хил фойдаланувчилар фойдаланишади. Бу маълумотларнинг кўпчилиги бевосита маълум бир фойдаланувчиларга мўлжалланган бўлади. Бу маълумотларни бегоналардан ҳимоялаш керак, чунки улар маълумотларни олиб турли хил хавфларни содир этиши мумкин. Маълумотларни ҳимоялаш учун компьютеримизга парол қўямиз, аммо паролни синдирувчи дастурлар ҳам анчагина. Компьютеримиз тармоққа уланган, бу эса ҳужум

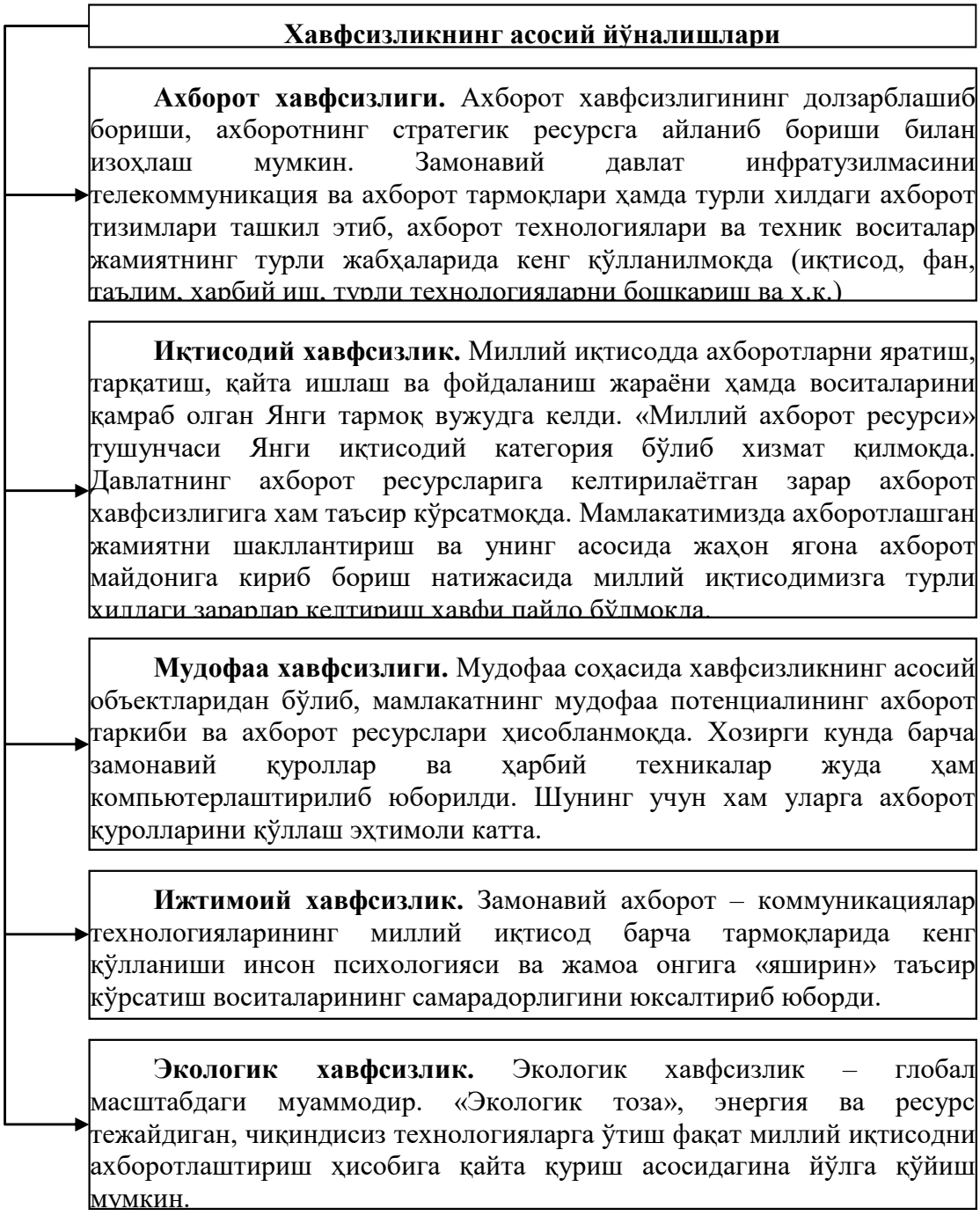
қилувчилар тармоқ орқали компьютеримизга кириб маълумотимизни олишига имкон яратади. Биз тармоққа боғланмасдан, ташқи дунёдан узилган ҳолда ишлай олмаймиз. Шунинг учун, мавзу доирасида SQL Server да маълумотлар базасини бегоналардан ҳимоялаш учун нималар қилиш кераклигини таҳлил қиламиз. Бу тавсиялар маълумотлар базасини яратувчи дастурчиларга ва маълумотлар базасини ишини ташкил қилувчи администраторлар учун қўлланма бўлади деган фикрдамиз. Бундан ташқари ушбу битирув малакавий ишини ахборот технологиялари соҳаси бўйича билим олаётган талабаларга қўлланма сифатида тавсия қиламиз.

Тадқиқот объекти ва предмети. Мавзумизда тадқиқот объекти маълумотлар базаси, МББТ, тармоқда маълумотлар базаларини ташкил қилиш технологиялари ва SQL Server 2005 МББТ дир. Тадкикот предмети эса SQL 2005 МББТ да маълумотлар хавфсизлигини таъминлаш масалаларини тавсифлаб беришдир.

1.1. Ахборот хавфсизлигига кириш

Мамлакатимиз миллий иқтисодининг ҳеч бир тармоғи самарали ва мўътадил ташкил қилинган ахборот инфратузилмасисиз фаолият кўрсатиши мумкин эмас. Ҳозирги кунда миллий ахборот ресурслари хар бир давлатнинг иқтисодий ва ҳарбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат килмокда. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот – коммуникациялар технологияларини қўллаш кенгаяди. Турли хилдаги ахборотлар худудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга Internet ҳалқаро компьютер тармоғи орқали кириб келди. Ахборотлашган жамият шу компьютер тармоғи орқали тезлик билан шаклланиб бормокда. Ахборотлар дунёсига саёҳат қилишда давлат чегаралари деган тушунча йўқолиб бормокда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмокда, яъни давлат ахборотларнинг тарқалиши механизмини бошқара олмай қолмокда. Шунинг учун ҳам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Буларнинг бари шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмокда. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборот ҳимояси эса давлатнинг бирламчи масалаларига айланмокда.

Ҳозирги кунда хавфсизликнинг бир қанча йўналишларини қайд этиш мумкин. (1- расм)


Хавфсизликнинг асосий йўналишлари
Ахборот хавфсизлиги. Ахборот хавфсизлигининг долзарблашиб бориши, ахборотнинг стратегик ресурсга айланиб бориши билан изоҳлаш мумкин. Замонавий давлат инфратузилмасини телекоммуникация ва ахборот тармоқлари ҳамда турли хилдаги ахборот тизимлари ташкил этиб, ахборот технологиялари ва техник воситалар жамиятнинг турли жабҳаларида кенг қўлланилмоқда (иқтисод, фан, таълим, харбий иш, турли технологияларни бошкариш ва х.к.)
Иқтисодий хавфсизлик. Миллий иқтисодда ахборотларни яратиш, тарқатиш, қайта ишлаш ва фойдаланиш жараёни ҳамда воситаларини қамраб олган Янги тармоқ вужудга келди. «Миллий ахборот ресурси» тушунчаси Янги иқтисодий категория бўлиб хизмат қилмоқда. Давлатнинг ахборот ресурсларига келтирилаётган зарар ахборот хавфсизлигига хам таъсир кўрсатмоқда. Мамлакатимизда ахборотлашган жамиятни шакллантириш ва унинг асосида жаҳон ягона ахборот майдонига кириб бориш натижасида миллий иқтисодимизга турли хилдаги зарарлар келтириш хавфи пайдо бўлмоқда.
Мудофаа хавфсизлиги. Мудофаа соҳасида хавфсизликнинг асосий объектларидан бўлиб, мамлакатнинг мудофаа потенциалининг ахборот таркиби ва ахборот ресурслари ҳисобланмоқда. Хозирги кунда барча замонавий қуроллар ва ҳарбий техникалар жуда ҳам компьютерлаштирилиб юборилди. Шунинг учун хам уларга ахборот қуролларини қўллаш эҳтимоли катта.
Ижтимоий хавфсизлик. Замонавий ахборот – коммуникациялар технологияларининг миллий иқтисод барча тармоқларида кенг қўлланиши инсон психологияси ва жамоа онгига «яширин» таъсир кўрсатиш воситаларининг самарадорлигини юксалтириб юборди.
Экологик хавфсизлик. Экологик хавфсизлик – глобал масштабдаги муаммодир. «Экологик тоза», энергия ва ресурс тежайдиган, чиқиндисиз технологияларга ўтиш фақат миллий иқтисодни ахборотлаштириш ҳисобига қайта қуриш асосидагина йўлга қўйиш мумкин.

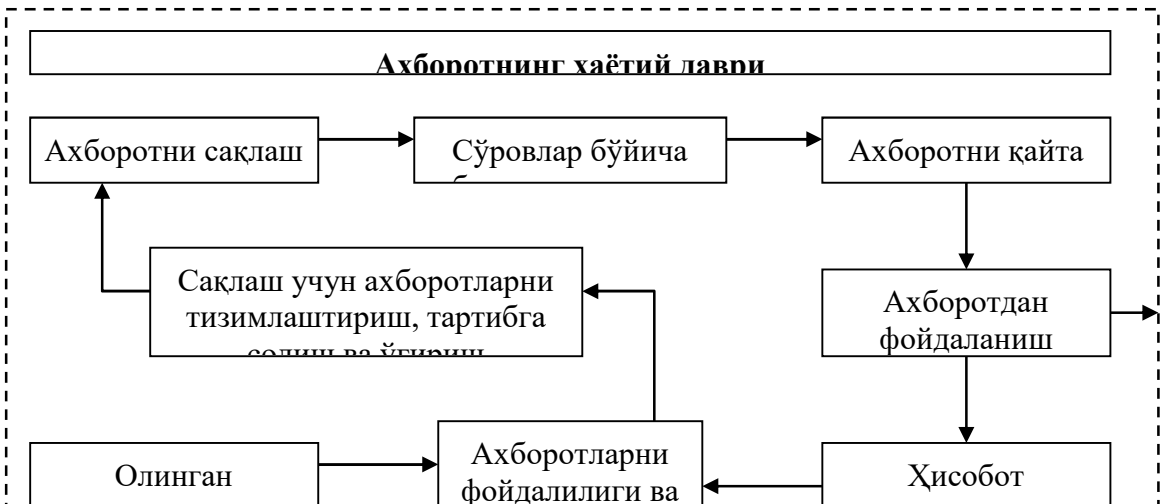
1 – расм.

Ахборотнинг муҳимлик даражаси қадим замонлардан маълум. Шунинг учун ҳам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири – сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат – сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденциялари ва разведка миссияларидан ташқарига чиқмаган. Фақат бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар, сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни ўғирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади. Ахборотни қайта ишлаш саноатининг пайдо бўлиши ахборотни ҳимоялаш саноатининг пайдо бўлишига олиб келади.

Автоматлаштирилтан ахборот тизимларида ахборотлар ўзининг ҳаётий даврига эга бўлади. Бу давр уни яратиш, ундан фойдаланиш ва керак бўлмаганда йўқотишдан иборатдир (2-расм).

Ахборотлар хаётий даврининг хар бир босқичида уларнинг ҳимояланганлик даражаси турлича баҳоланади.

Махфий ва қимматбаҳо ахборотларга рухсатсиз киришдан ҳимоялаш энг муҳим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулки ҳуқуқларини ҳимоялаш - бу ишлаб чиқарилаётган ахборотларни жиддий иқтисодий ва бошҳа моддий ҳамда номоддий зарарлар келтириши мумкин бўлган турли киришлар ва ўғирлашлардан ҳимоялашдир.



Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан ҳар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва ҳужжатларни ўғирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компьютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир. Булардан ташқари, бу харакатлардан моддий фойда олишга интилиш ҳам ривожланди.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Ахборотнинг эгасига, фойдаланувчисига ва бошқа шахсга зарар етказмокчи бўлган ноҳуқуқий муомаладан хар қандай ҳужжат**лаштирилган,** яъни идентификация қилиш имконини берувчи реквизитлари қўйилган ҳолда моддий жисмда қайд этилган **ахборот** ҳимояланиши керак.

Ахборот хавфсизлиги нуктаи назаридан ахборотни қуйидагича туркумлаш мумкин:

• **махфийлик** — аниқ бир ахборотга фақат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши қонуний ҳужжатларга мувофиқ чеклаб қўйилиб, ҳужжатлаштирилганлиги кафолати. Бу банднинг бузилиши **ўғирлик** ёки **ахборотни ошкор қилиш,** дейилади;

• **конфиденциаллик** — иншончлилиги, тарқатилиши мумкин эмаслиги, махфийлиги кафолати;

• **яхлитлик** — ахборот бошланғич кўринишда эканлиги, яъни уни сақлаш ва узатишда рухсат этилмаган ўзгаришлар қилинмаганлиги кафолати; бу банднинг бузилиши **ахборотни сохталаштириш** дейилади;

• **аутентификация** — ахборот захираси эгаси деб эълон қилинган шахс хақиқатан хам ахборотнинг эгаси эканлигига бериладиган кафолат; бу банднинг бузилиши **хабар муаллифини сохталаштириш** дейилади;

• **апелляция қилишлик** — етарлича мураккаб категория, лекин электрон бизнесда кенг қўлланилади. Керак бўлганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги кафолати.

Юкоридагидек, ахборот тизимига нисбатан қуйидагича таснифни келтириш мумкин:

• **ишончлилик** — тизим меьёрий ва ғайри табиий холларда режалаштирилганидек ўзини тутишлик кафолати;

• **аниқлилик** — хамма буйруқларни аниқ ва тўлиқ бажариш кафолати;

• **тизимга киришни назорат килиш —** турли шахс гурухлари ахборот манбаларига хар хил киришга эгалиги ва бундай киришга чеклашлар доим бажарилишлик кафолати;

• **назорат килиниши** — исталган пайтда дастур мажмуасининг хохлаган кисмини тулик текшириш мумкинлиги кафолати;

• **идентификациялашни назорат килиш** — ҳозир тизимга уланган мижоз аниқ ўзини ким деб атаган булса, аниқ ўша эканлигининг кафолати;

• **қасддан бузилишларга тўсқинлик** — олдиндан келишилган меъёрлар чегарасида қасддан хато киритилган маълумотларга нисбатан тизимнинг олдиндан келишилган ҳолда ўзини тутиши.

Ахборотни ҳимоялашнинг мақсадлари куйидагилардан иборат:

- ахборотнинг келишувсиз чиқиб кетиши, угирланиши, йукотилиши, ўзгартирилиши, сохталаштирилишларнинг олдини олиш;

- шахс, жамият, давлат хавфсизлилигига бўлган хавф – хатарнинг олдини олиш;

- ахборотни йук килиш, ўзгартириш, сохталаштириш, нусха кучириш, тусиклаш буйича рухсат этилмаган харакатларнинг олдини олиш;

- ҳужжатлаштирилган ахборотнинг микдори сифатида ҳуқуқий тартибини таъминловчи, ахборот заҳираси ва ахборот тизимига хар қандай ноконуний аралашувларнинг куринишларининг олдини олиш;

- ахборот тизимида мавжуд бўлган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сақловчи фуқароларнинг конституцион ҳуқуқларини ҳимоялаш;

- давлат сирини, қонунчиликка мос ҳужжатлаштирилган ахборотнинг конфиденциаллигини сақлаш;

- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чиқиш ва қўллашда субъектларнинг ҳуқуқларини таъминлаш.

Тармоқ хавфсизлигини назорат қилиш воситалари

Замонавий ахборот - коммуникациялар технологияларининг ютуқлари ҳимоя услубларининг бир қатор зарурий инструментал воситаларини яратиш имконини берди.

Ахборотларни ҳимояловчи инструментал воситалар деганда дастурлаш, дастурий - аппаратли ва аппаратли воситалар тушунилади.

Уларнинг функционал тўлдирилиши хавфсизлик хизматлари олдига қуйилган ахборотларни ҳимоялаш масалаларини ечишда самаралидир. Ҳозирги кунда тармоқ хавфсизлигини назорат килиш техник воситаларининг жуда кенг спектри ишлаб чиқарилган.

1.2. Ахборотларга ҳужумнинг асосий кўринишлари

Автоматлаштирилган ахборот тизимларида ҳимоялаш зарурияти

Ахборот - коммуникациялар технологияларининг оммавий равишда қоғозсиз автоматлаштирилган асосда бошқарилиши сабабли ахборот хавфсизлигини таъминлаш мураккаблашиб ва муҳимлашиб бормоқда. Шунинг учун хам автоматлаштирилган ахборот тизимларида ахборотни ҳимоялашнинг янги замонавий технологияси пайдо бўлмоқда. DataQuest компаниясининг маълумотига кура, 1996—2000 йилларда ахборот ҳимояси воситаларининг сотувдаги хажми 13 млрд. АКШ долларига тенг бўлган.

Ахборотни ҳимоялаш тизими

Ахборотнинг заиф томонларини камайтирувчи ахборотга рухсат этилмаган киришга, унинг чиқиб кетишига ва йўқотилишига тўсқинлик қилувчи ташкилий, техник, дастурий, технологик ва бошқа восита, усул ва чораларнинг комплекси — **ахборотни ҳимоялаш тизими** дейилади.

Ахборот эгалари ҳамда ваколатли давлат органлари шахсан ахборотнинг қимматлилиги, унинг йўқотилишидан келадиган зарар ва ҳимоялаш механизмининг нархидан келиб чиққан ҳолда ахборотни ҳимоялашнинг зарурий даражаси ҳамда тизимнинг турини, ҳимоялаш усуллар ва воситаларини аниқлашлари зарур. Ахборотнинг қимматлилиги ва талаб қилинадиган ҳимоянинг ишончлилиги бир-бири билан бевосита боғлиқ.

Ҳимоялаш тизими узлуксиз, режали, марказлаштирилган, мақсадли, аниқ, ишончли, комплексли, осон мукаммаллаштириладиган ва куриниши тез ўзгартириладиган бўлиши керак. У одатда барча экстремал шароитларда самарали бўлиши зарур.

Ташкилотлардаги ахборотларни ҳимоялаш

Ахборот хажми кичик бўлган ташкилотларда ахборотларни ҳимоялашда оддий усулларни қўллаш мақсадга мувофиқ ва самаралидир. Масалан, укиладиган кимматбохо когозларни ва электрон ҳужжатларни алохида гурухларга ажратиш ва никоблаш, ушбу ҳужжатлар билан ишлайдиган ходимни тайинлаш ва ургатиш, бинони куриклашни ташкил этиш, хизматчиларга кимматли ахборотларни таркатмаслик мажбуриятини юклаш, ташкаридан келувчилар устидан назорат килиш, компьютерни ҳимоялашнинг энг оддий усулларини қўллаш ва хоказо. Одатда, ҳимоялашнинг энг оддий усулларини қўллаш сезиларли самара беради.

Мураккаб таркибли, куп сонли автоматлаштирилган ахборот тизими ва ахборот хажми катга бўлган ташкилотларда ахборотни ҳимоялаш учун ҳимоялашнинг мажмуали тизими ташкил килинади. Лекин ушбу усул ҳамда ҳимоялашнинг оддий усуллари хизматчиларнинг ишига хаддан ташкари халакит бермаслиги керак.

Ҳимоялаш тизимининг комплекслилиги

Ҳимоя тизимининг комплекслилигига унда ҳуқуқий, ташкилий, муҳандис – техник ва дастурий – математик элементларнинг мавжудлиги билан эришилади. Элементлар нисбати ва уларнинг мазмуни ташкилотларнинг ахборотни ҳимоялаш тизимининг ўзига хослигини ва унинг такрорланмаслигини ҳамда бузиш қийинлигини таъминлайди.

Аниқ тизимни кўп турли элементлардан иборат, деб тасаввур қилиш мумкин. Тизим элементларининг мазмуни нафақат унинг узига хослигини, балки ахборотнинг қимматлилигини ва тизимнинг қийматини ҳисобга олган ҳолда белгиланган ҳимоя даражасини аниқлайди.

Ахборотни ҳуқуқий ҳимоялаш элементи ҳимоялаш чораларининг ҳақли эканлиги маъносида ташкилот ва давлатларнинг узаро муносабатларини юридик мустаҳкамлаш хамла персоналнинг ташкилот қимматли ахборотини ҳимоялаш тартибига риоя қилиши ва ушбу тартибни бузилишида жавобгарлиги тасаввур қилинади.

Ахборотларни ташкилий ҳимоялаш элементлари

Ҳимоялаш технологияси персонални ташкилотнинг қимматли ахборотларини ҳимоялаш қоидаларига риоя қилишга ундовчи бошқариш ва чеклаш характерига эга бўлган чора-тадбирларни ўз ичига олади.

Ташкилий ҳимоялаш элементи бошқа барча элементларни ягона тизимга боғловчи омил бўлиб ҳисобланади. Кўпчилик мутахассисларнинг фикрича, ахборотларни ҳимоялаш тизимлари таркибида ташкилий ҳимоялаш 50—60 % ни ташкил қилади. Бу ҳол кўп омилларга боғлиқ, жумладан, ахборотларни ташкилий ҳимоялашнинг асосий томони амалда ҳимоялашнинг принципи ва усулларини бажарувчи персонални танлаш, жойлаштириш ва ургатиш ҳисобланади.

Ахбортларни ҳимоялашнинг ташкилий чора – тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида уз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элементларининг ягана номи — ахборотни ташкилий - ҳуқуқий ҳимоялаш элементини ишлатадилар.

Ахборотларни муҳандис – техиик ҳимоялаш элементи — техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни қуриқлашни ташкил қилиш ҳамда техник текшириш воситаларига карши суст ва фаол

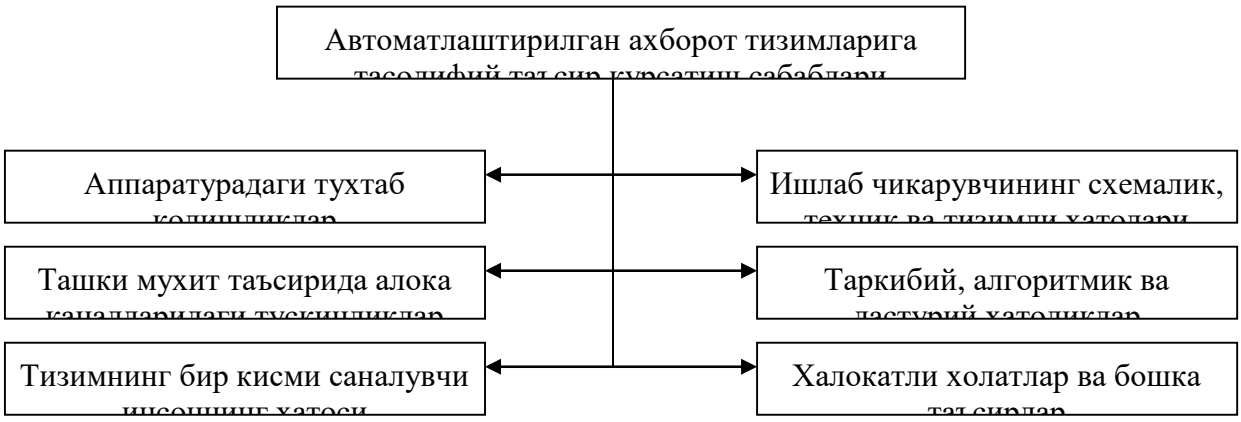
кураш учун мулжалланган. Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.

Ахборотни ҳимоялашнинг дастурий – математик элементи компьютер, локал тармоқ ва турли ахборот тизимларида қайта ишланадиган ва сақланадиган қимматли ахборотларни ҳимоялаш учун мўлжалланган.

Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

Компьютер тизими (тармоги)га зиён етказиши мумкин бўлган шароит, харакат ва жараёнлар **компьютер тизими (тармоги)** учун хавф - хатарлар, деб ҳисобланади.

Автоматлаштирилган ахборот тизимларига тасодифий таъсир курсатиш сабаблари таркибига куйидагилар киради.



Маълумки, компьютер тизим (тармоғ)ининг асосий компонентлари — техник воситалари, дастурий - математик таъминот ва маълумотлардир.

Назарий томондан бу компонентларга нисбатан тўрт турдаги хавфлар мавжуд, яъни **узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш:**

— узилиш — қандайдир ташқи ҳаракатлар (ишлар, жараёнлар)ни бажариш учун ҳозирги ишларни вақтинча марказий процессор қурилмаси ёрдамида тухтатишдир, уларни бажаргандан сўнг процессор олдинги ҳолатга қайтади ва тўхтатиб қуйилган ишни давом эттиради. Ҳар бир узилиш тартиб рақамига эга, унга асосан марказий процессор қурилмаси қайта ишлаш учун қисм – дастурни қидириб топади. Процессорлар икки турдаги узилишлар билан ишлашни вужудга келтириши мумкин: дастурий ва техник. Бирор қурилма фавқулодда хизмат кўрсатилишига муҳтож бўлса, унда техник узилишлар пайдо бўлади. Одатда бундай узилиш марказий процессор учун кутилмаган ҳодисадир. Дастурий узилишлар асосий дастурлар ичида процессорнинг махсус буйруқлари ёрдамида бажарилади. Дастурий узилишда дастур ўз – ўзини вактинча тўхтатиб, узилишга тааллуқли жараённи бажаради.

— тутиб олиш — жараёни оқибатида ғаразли шахслар дастурий воситалар ва ахборотларнинг турли магнитли ташувчиларига киришни қулга киритади. Дастур ва маълумотлардан ноқонуний нусха олиш, компьютер тармоқлари алоқа каналларидан номуаллифлик ўқишлар ва ҳоказо ҳаракатлар тутиб олиш жараёнларига мисол бўла олади.

— ўзгартириш — ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тупламлари, дастурлар, техник элементлари) киришни қулга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам килади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман копьютер тизими файлларини ўзгартириши, ёки

қандайдир қўшимча ноқонуний кайта ишлашни амалга ошириш мақсадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилали;

— сохталаштириш — хам жараён саналиб, унинг ёрдамида ғаразли шахслар тизимда ҳисобга олинмаган вазиятларни ўрганиб, ундаги камчиликларни аниқлаб, кейинчалик ўзига керакли ҳаракатларни бажариш мақсадида тизимга қандайдир сохта жараённи ёки тизим ва бошқа фойдаланувчиларга сохта ёзувларни юборади.

1.3. Ахборотларни криптографик ҳимоялаш усуллари

Криптография ҳақида асосий тушунчалар

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб қуймоқ» маъносини билдирган. Биринчи марта у ёзув пайдо бўлган даврлардаёк айтиб ўтилган. Ҳозирги вақтда криптография деганда ҳар қандай шаклдаги, яъни дискда сақланадиган сонлар кўринишида ёки ҳисоблаш тармоқларида узатиладиган хабарлар кўринишидаги ахборотни яшириш тушунилади. Криптографияни рақамлар билан кодланиши мумкин бўлган ҳар қандай ахборотга нисбатан қўллаш мумкин. Махфийликни таъминлашга қаратилган криптография кенгроқ қўлланилиш доирасига эга. Аниқроқ айтганда, криптографияда қўлланиладиган усулларнинг ўзи ахборотни ҳимоялаш билан боғлиқ бўлган кўп жараёнларда ишлатилиши мумккн.

Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди. Масалан, тулов варакларини электрон почта оркали узатишда унинг ўзгартирилиши ёки сохта ёзувларнинг қушилиши мумкин. Бундай ҳолларда ахборотнинг яхлитлигини таъминлаш зарурияти пайдо бўлади. Умуман олганда компьютер тармогига рухсатсиз киришнинг мутлақо олдини олиш мумкин эмас, лекин уларни аниқлаш мумкин. Ахборотнинг яхлитлигини текширишнинг бундай жараёни, кўп ҳолларда, ахборотнинг ҳақиқийлигини таъминлаш дейилади. Криптографияда қўл-

ланиладиган усуллар кўп бўлмаган ўзгартиришлар билан ахборотларнинг ҳақикийлигини таъминлаши мумкин.

Нафақат ахборотнинг компьютер тармогидан маъноси бузилмасдан келганлигини билиш, балки унинг муаллифдан келганлигига ишонч хосил қилиш жуда муҳим. Ахборотни узатувчи шахсларнинг ҳақиқийлигини тасдикловчи турли усуллар маълум. Энг универсал процедура пароллар билан алмашувдир, лекин бу жуда самарали бўлмаган процедура. Чунки паролни қулига киритган ҳар қандай шахс ахборотдан фойдаланиши мумкин бўлади. Агар эҳтиёткорлик чораларига риоя қилинса, у ҳолда парольларнинг самарадорлигини ошириш ва уларни криптографик усуллар билан ҳимоялаш мумкин, лекин криптография бундан кучлироқ паролни узлуксиз ўзгартириш имконини берадиган процедураларни ҳам таъминлайди.

Криптография соҳасидаги охирги ютуклардан бири — рақамли сигнатура — махсус хосса билан ахборотни тўлдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очиқ калит маълум бўлгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усулларан кўпроқ афзалликларга эга.

Криптография усулларини қўллашнинг баъзи бирларини кўриб чикамиз. Узаталадиган ахборотнинг маъносини яшириш учун икки хил ўзгартиришлар қўлланилади: **кодлаштириш** ва **шифрлаш**.

Кодлаштириш учун тез-тез ишлатиладиган иборалар тўпламини ўз ичига олувчи китоб ёки жадваллардан фойдаланилади. Бу иборалардан ҳар бирига, кўп ҳалларда, рақамлар тўплами билан бериладиган ихтиёрий танланган кодли суз тўғри келади. Ахборотни кодлаш учун худди шундай китоб ёки жадвал талаб қилинади. Кодлаштирувчи китоб ёки жадвал ихтиёрий криптографик ўзгартиришга мисол бўлади. Кодлаштиришнинг ахборот технологиясига мос талаблар — каторли маълумотларни сонли маълумотларга айлантириш ва аксинча ўзгартиришларни бажара билиш. Кодлаштириш китобини тезкор ҳамда ташқи хотира қурилмаларида амалга

ошириш мумкин, лекин бундай тез ва ишончли криптографик тизимни муваффакиятли деб булмайди. Агар бу китобдан бирор марта рухсатсиз фойдаланилса, кодларнинг янги китобини яратиш ва уни хамма фойдаланувчиларга таркатиш зарурияти пайдо бўлади.

Криптографик ўзгартиришнинг иккинчи тури **шифрлаш** ўз ичига — бошланғич матн белгиларини англаб олиш мумкин бўлмаган шаклга ўзгартириш алторитмларини камраб олади. Ўзгартиришларнинг бу тури ахборот-коммуникациялар технологияларига мос келади. Бу ерда алгоритмни ҳимоялаш муҳим аҳамият касб этади. Криптографик калитни қўллаб, шифрлаш алгоритмининг ўзида ҳимоялашга бўлган талабларни камайтариш мумкин. Энди ҳимоялаш объекти сифатада фақат калит хизмат қилади. Агар калитдан нусха олинган бўлса, уни алмаштириш мумкин ва бу кодлаштирувчи китоб ёки жадвални алмаштиришдан енгилдир. Шунинг учун ҳам кодлаштириш эмас, балки шифрлаш ахборот-коммуникациялар технологияларида кенг кўламда қулланилмоқда.

Сирли (махфий) алоқалар соҳаси **криптология** деб айтилади. Ушбу сўз юнонча «**kripto**» — сирли ва **«logus»** — хабар маъносини билдирувчи сўзлардан иборат. Криптология икки йўналиш, яъни **криптография** ва **криптотаҳлил**дан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ҳақиқийлигини таъминлашдан иборат.

Криптотаҳлилнинг вазифаси эса криптографлар томонидан ишлаб чиқилган ҳимоя тизимини очишдан иборат.

Ҳозирги кунда **криптотизим**ни икки синфга ажратиш мумкин:

• симметрияли бир калитлилик (махфий калитли);

• асимметрияли икки калитлилик (очиқ калитли).

Симметрияли тизимларда куйидаги иккита муаммо мавжуд:

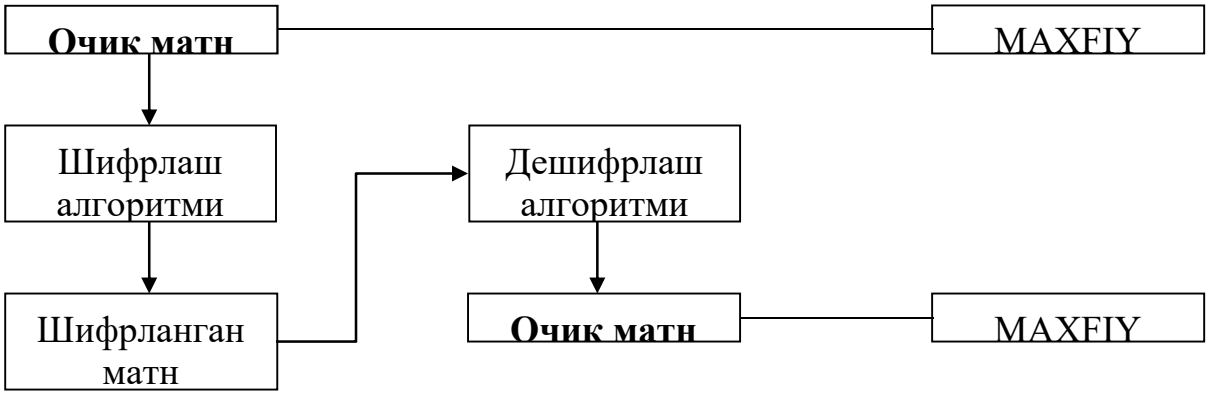
1) Ахборот алмашувида иштирок этувчилар қандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит қўлланилади. Биридан иккинчисини хисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул қилувчи томонидан ахборотни тиклашда қўлланилади ва у сир сақланиши лозим.



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қуллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо булади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

• фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниқлаш:

• тармоқ абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентнфикациялаш.

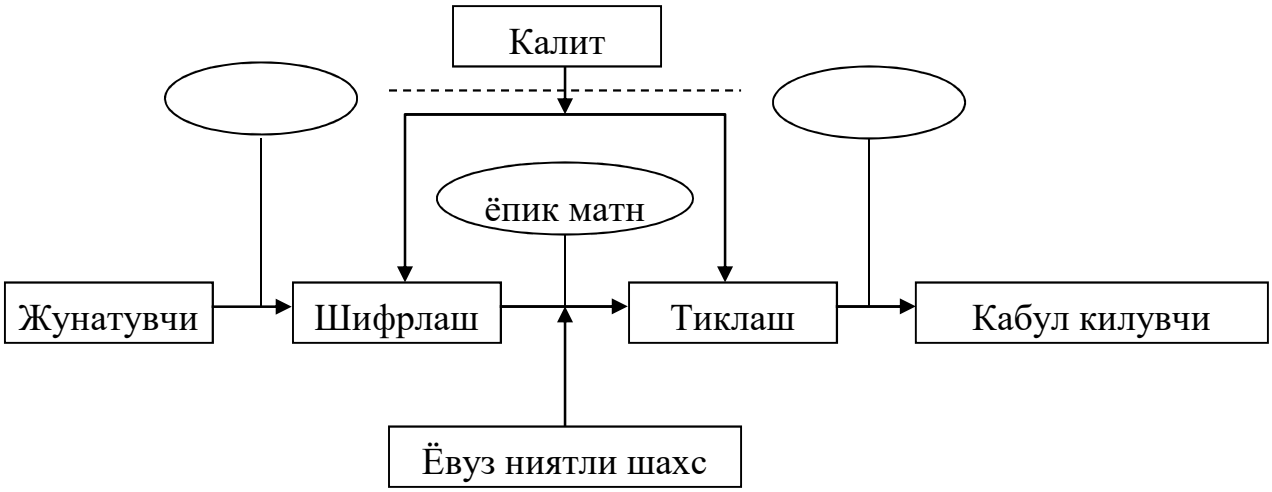
Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Internet ёрдамида амалга ошириладиган электрон савдолардир.

Ахборотларни криптографияли ҳимоялаш тамойиллари

Криптография — маълумотларни ўзгартириш усулларининг туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: **махфийлик; яхлитлилик.**

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:



Бу ерда калит қандайдир ҳимояланган канал оркали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуклидир.

Ассимметрияли икки калитлик криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:

Бу ҳолда ҳимояланган канал бўйича очиқ калит жўнатилиб, махфий калит жўнатилмайди.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптотахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим **криптомустаҳкам тизим де**б айтилади.

Криптотизимнинг мустахкамлиги унинг калити билан аниқланади ва бу криптотаҳлилнинг асосий қоидаларидан бири бўлиб хисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маьлум тизим ҳисобланиб, унинг ўзгартирилиши кўп вакт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни ҳимоялаш талаб қилинади.

2.1. **SQL Server 2005 да авторизация ва аутентификация**

Аутентификация — бу фойдаланувчининг бирор ресурсга ҳуқуқи бор-йўқлигини текшириш жараёни. Одатда аутентификация логин ва паролни киритиш орқали амалга оширилади.

SQL Server 2005 да 2 хил аутентификация режими мавжуд: Windows ёрдамида ва SQL Server ёрдамида. Биринчи режим фойдаланувчининг бир марталик рўйхатдан ўтиши ва битта парол орқали турли дастурлардан фойдаланиш имконини беради. Бундай режим фойдаланувчига бир нечта паролни эсда сақлаш мажбуриятидан халос этиб унинг ишини осонлаштиради. Бундан ташқари бу режим операцион тизим тақдим этадиган гуруқ ва домен хавфсизлик сиёсати, паролни шакллантириш ва ўзгартириш қоидаси, паролларни шифрлаш орқали аутентификациянинг ҳимояланган протоколлари каби хавфсизлик воситаларидан фойдаланиш имконини беради.

SQL Server ёрдамида аутентификация асосан Windows дан фарқли платформаларда ишлайдиган мижоз дастурлар учун мўлжалланган. Бу усул нисбатан хавсизлиги паст ҳисобланади, лекин SQL Server 2005 да мижоз ва сервер орасида алмашинадиган маълумотларни сервер томонидан генерация қилинадиган сертификат орқали шифрлаш имкони мавжуд. Шифрлаш яна бу усулнинг ишончлигини оширади.

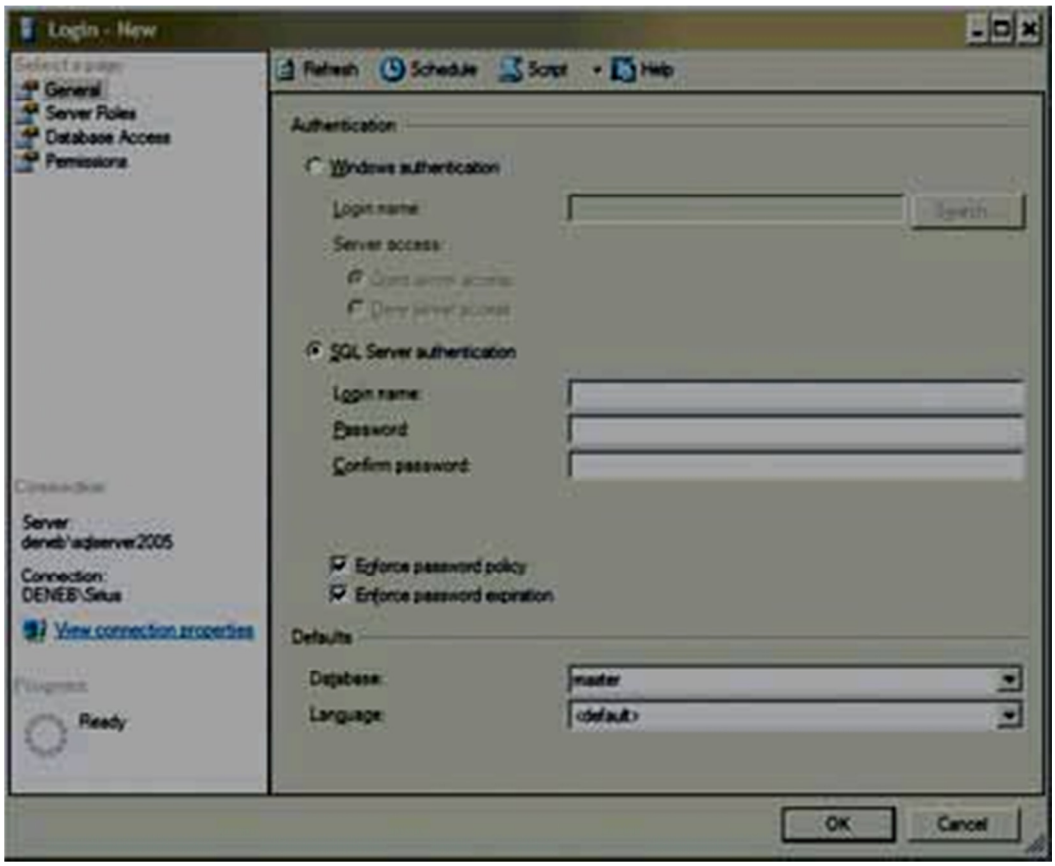


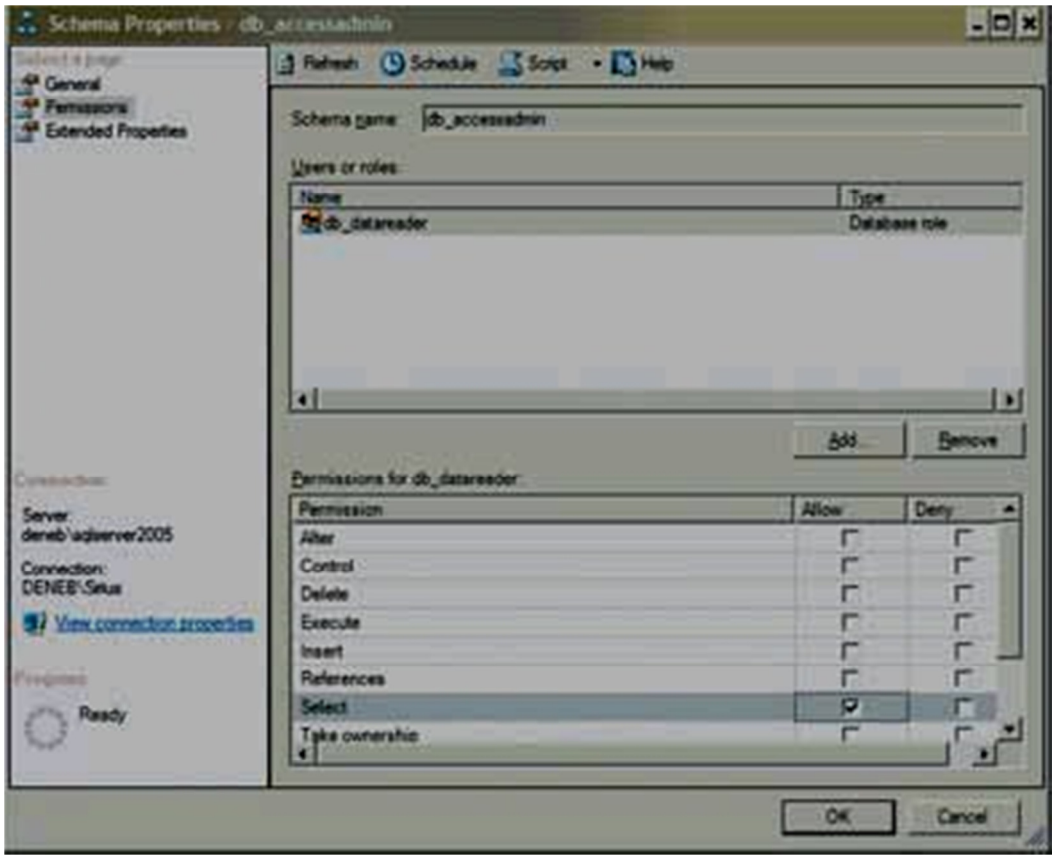
Рис. 1. *Установка правил для пароля пользователя*

Фойдаланувчига алоқаси бўлмаган схемалар

10 йиллардан бери кўпгина МББТларида база объектлардан фойдаланишга рухсат бериш ҳар бир база объекти эгасининг мавжудлигига асосланган. База объекти эгаси бошқа фойдаланувчиларга шу объектдан фойдаланиш ҳуқуқини бериши мумкин. Бунда битта фойдаланувчига тегишли объектлар тўплами схема дейилади. Объектларни бошқаришнинг бундай усули маълумотлар базасига эга бўлган дастурларни қўлаб-қувватлашда муаммолар келтириб чиқарарди. Масалан бир нечта фойдаланувчи томонидан фойдаланилаётган объект эгаси ишдан бўшатилганда, яъни базадан ўчирилганда сервер кодида ўзгаришлар қилинишига тўғри келарди. Бундай муаммоларнинг келиб чиқиши фойдаланувчи ҳақидаги маълумотни оддий жадвалларда сақлашга олиб

келди. Бу эса маълумотлардан ва дастурлардан рухсатсиз фойдаланиш хавфини оширди.

SQL Server 2005да роллар концепцияси кенгайтирилган: МББТ фойдаланувчини базанинг объекти ва схемаларидан ажратади. Энди маълумотлар базаси объекти бирор фойдаланувчига тегишли эмас, балки фойдаланувчига алоқаси бўлмаган схемаларга тегишли ҳисобланади. Шундай қилиб, схема фойдаланувчига объектдан фойдаланиш ҳуқуқини беришни осонлаштирадиган объектларни гуруҳлаш механизми ҳисобланади.



2-расм. *База схемасига ҳуқуқларни ўрнатиш*

Роллар

Ҳуқуқлар беришни бошқаришни осонлаштириш учун кўпгина сервер МББТ ларда роллар механизми қўлланилади. Рол бу бир нечта

фойдаланувчига бириктириш мумкин бўлган, маълумотлар базаси объектидан фойдаланиш ҳуқуқлари тўплами ҳисобланади. Бир хил функцияни бажарувчи ва бир хил дастурни ишлатувчи фойдаланувчиларга ҳуқуқларни беришни анча осонлаштиради. Рол яратилиб, унга бир марта ҳуқуқлар бириктирилади. Кейинчалик бу рол фойдаланувчиларга бириктирилади. SQL Server 2005 ичма-ич жойлашган ролларни яратиш имконини беради, яъни битта рол иккинчи ролга бириктирилиши мумкин.

SQL Server 2005 яна дастурлар учун ролларни(*application roles*) ҳам қўллаб қувватлайди. Бу роллар аниқ бир дастур орқали фойдаланувчилар ишлаётганда, база объектларига ҳуқуқни чегаралаш мумкин. Бу роллар оддий ролдан фарқли фойдаланувчига бириктирилмайди. Бу роллар барча фойдаланувчилар учун хавфсизлик талаби бир бўлганда қўллаш қулай. Бунда базада аниқ бир фойдаланувчининг ҳаракатларини аудит қилиш шарт эмас.

Схема ва ролларни қўллаш. Умумий принциплар

Лойиҳалаштиришнинг муҳим этапларидан бири база объектларидан фойдаланиш ҳуқуқларини батафсил аниқлашдир. Бу этапда қандай схемалар ишлатилади, қандай роллар яратиш керак, бўлиши мумкин бўлган фойдаланувчилар гуруҳини аниқлаш керак. Бундан ташқари бу этапда кўринишлар ва процедуралар хавфсизликни таъминлаш мақсадида қандай ишлатилади(масалан тўғридан тўғри жадвалларга мурожаатни чеклаш учун).

Охирги вақтларда ролларни ҳар қандай ҳолатда ҳам ишлатиш тавсия қилинади. Чунки у ҳуқуқларни бошқариш жараёнини анча осонлаштиради. Қисман бир хил ҳуқуқлар тўпламига эга бўлган ролларни яратишда ичма-ич жойлашган роллардан фойдаланиш тавсия этилади.

Мижоз дастурларнинг ҳуқуқларга талабини таҳлил вилиш керак ва бу талабларни схемалар ва ролларни лойиҳалаштириш жараёнида инобатга

олиш керак. Ҳуқуқларни бошқаришда SQL Server нинг турли хизматларида ҳуқуқлар бошқарувига ҳам эътибор қаратиш керак.

2.2. SQL Server 2005 нинг хизматларида ҳуқуқлар бошқаруви

Ҳисоботлар хизматида ҳуқуқлар бошқаруви

Ҳисоботлар хизматини(*Reporting Services*) қўллаганда ушбу хизматга мурожаат қиладигна дастурлар билан ишлайдиган фойдаланувчиларнинг база объектларига ҳуқуқлари ҳақида алоҳида эътибор бериш керак. Бундай категориядаги фойдаланувчилар учун ҳисоботнинг тавсифи ва шу ҳисоботни шакллантириш учун керак бўладиган база объектларидан фойдаланиш ҳуқуқи бўлиши керак. Шу учун бундай ҳолда алоҳида фақат ушбу ҳуқуқлар тўпламига эга бўлган рол яратиш керак. Шуни айтиб ўтиш керакки, аввалambор ҳисоботлар хизмати Internet Information Services (*IIS*) ва ҳисоботлар серверида фойдаланувчини аутентификация қилиш учун Windows хавфсизлик воситаларидан фойдаланади. Бу режим нисбатан хавфсиз ҳисобланади, чунки бу режим IIS бошқарувида бажарилаётган web-дасстур учун аноним киришни чеклаши мумкин.

Таъкидлаб ўтиш керакки, ҳисоботлар хизмати Integrated Security режимида ҳам ишлаши мумкин. Лекин бунда бир қатор компонентлар коди ҳисоботни генерация қилган фойдаланувчи ҳуқуқи билан бажариди. Бу эса фойдаланувчига юқори ҳуқуқлар бериши мумкин. Шу учун бу режим ҳисоботлар хизмати билан бирга фойдаланиш тавсия этилмайди.

Билдириш хизматида ҳуқуқлар бошқаруви

Билдириш хизмати(*Notification Services*) билдиришномани етказиш ҳуқуқига эга бўлган ва иложи борича кам ҳуқуқларга(ҳеч бўлмаганда

администратор гуруҳига кирмаслиги керак) эга бўлган ҳисоб ёзуви(учетная запись) бажаради.

Шуни айтиш керакки, билдириш хизмати учун махсус роллар — NSEventProvider, NSGenerator, NSDistributor мавжуд бўлиб, булар провайдер, тарқатиш механизми ва генераторига жавоб берадиган ҳисоб ёзуви(учетная запись) га бириктирилади. Яна NSRunService роли бўлиб, у юқоридаги 3 та ролни ўз ичига олади. Бу рол билдириш хизмати битта маълумотлар базаси ядросида бажарилаётганда ишлатилади.

Интеграллаштирилган хизматларда ҳуқуқлар бошқаруви

Интеграллаштирилган хизматларда ҳуқуқлар бошқаруви учун SQL Server 2005 янги роллар қўшилган: db_dt sadmin, db_dt sltuser ва db_dtsoperator. Улар msdb базасида жойлашган интеграллаштирилган хизматлар пакетларидан фойдаланишни назорат қилади.

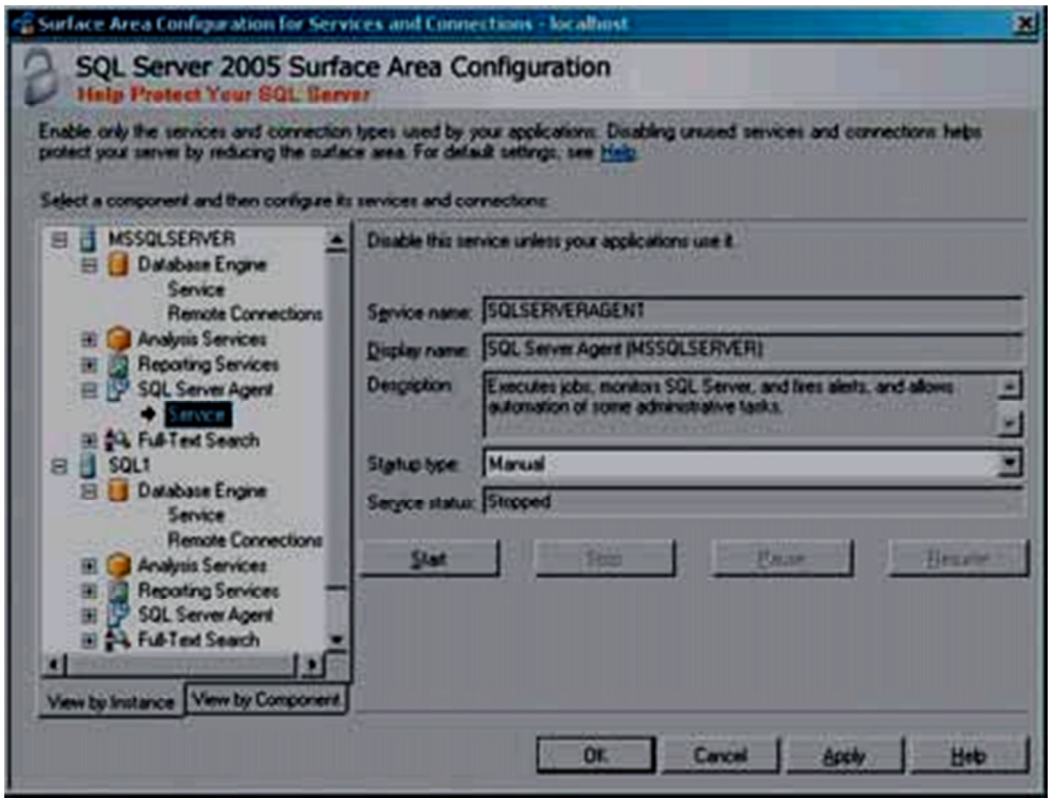
Репликация хизматларда ҳуқуқлар бошқаруви

SQL Server 2005 репликация хизматида ҳуқуқлар бошқаруви учун репликация агенти(*Replication Agent*) ҳисоб ёзувларини(учетная запись) осон бошқариш имконини берадиган янги модел яратилган. Энди ҳар бир агент ўзининг ҳисоб ёзуви(учетная запись) остида ишлаши мумкин. Бу эса агентнинг функциясига қараб, керакли ҳуқуқларни бириктириш имконини яратади. Агар репликация жараёнида қатнашадиган серверлар битта доменда жойлашган бўлса, ҳисоб ёзуви(учетная запись) учун Windows аутентификация усулини қўллаш тавсия этилади.

SQL Server Agent учун ҳуқуқлар бошқаруви

SQL Server Agent агенти `sysadmin ролига эга бўлган, лекин` Administrators гуруҳига кирмаган ва жараён учун хотира квотини ошириш ҳуқуқига эга бўлган Windows ҳисоб ёзуви(учетная запись) томонидан бажарилади. SQL Server Agent операцион тизим хизмати сифатида бажарилиши лозим.

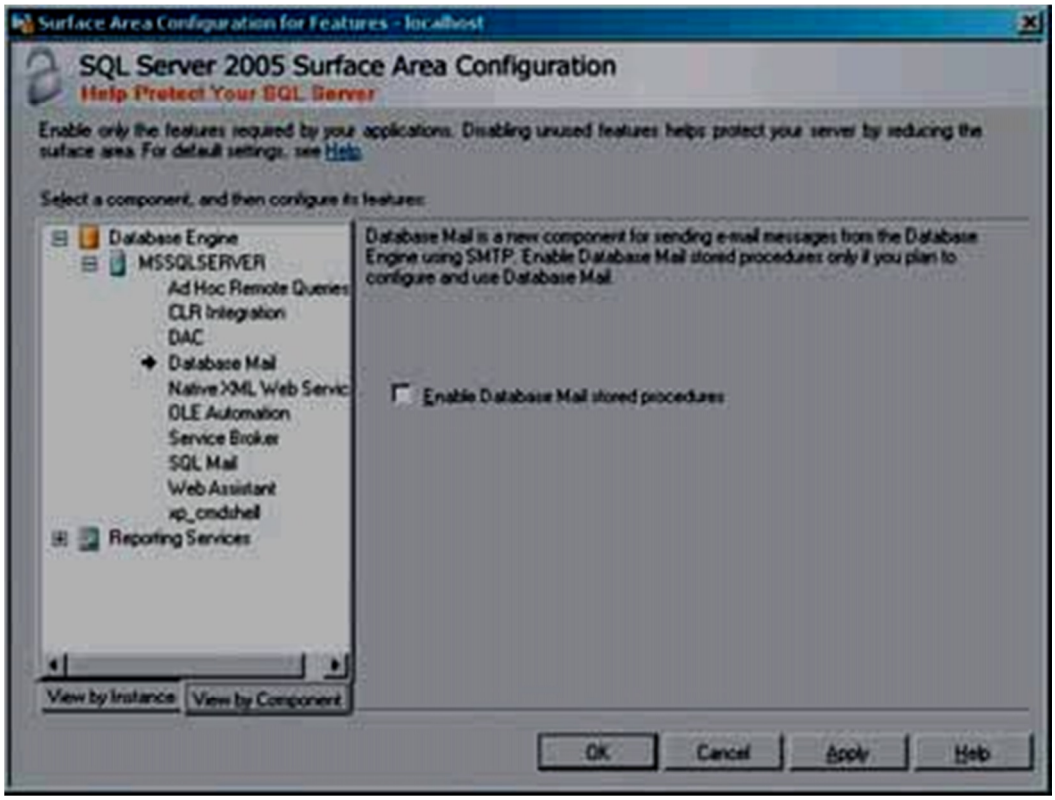
SQL Server Agent хизмати билан ишлаш учун Surface Area Configuration (3-расм) дастуридан фойдаланиш мумкин.



3-расм. SQL Server Agent хизмати билан ишлаш

Database Mail да ҳуқуқлар бошқаруви

Database Mail — бу SMTP (*Simple Mail Transport Protocol*) протоколини қўллаб қувватлаш учун SQL Server 2005 янги компоненти. Унда ҳуқуқларни бошқариш учун профил ташкил этиш тавсия қилинади. Database Mail хизмати билан ишлаш учун Surface Area Configuration (4-расм) дастуридан фойдаланиш мумкин.



4-расм. *Database Mail хизмати билан ишлаш*

HTTP протоколи орқали базада ҳуқуқлар бошқаруви

HTTP-мурожаат дастурга ташқаридан ҳужум қилишнинг энг кўп тарқалган усулларидан бири. Шунинг учун фақат зарур бўлган фойдаланувчиларга HTTP протокол орқали мурожаатга рухсат бериш керак. Яна сервер томонида Windows Guest ҳисоб ёзуви(учетная запись)ни ўчириш керак, чунки у комьютерга паролсиз кириш имконини беради. SQL Server га интернетдан мурожаат фақат брандмауэр орқали рухсат берилиши зарур.

2.3. Минимал ҳуқуқлар билан кодни бажариш

Стандарт ҳолда ўрнатиш

Хавфсиз дастурлар яратиш принципларидан бири қўйилган масалани минимал ҳуқуқлар билан бажариш. SQL Server 2005 да одатда МББТ ядросида Microsoft .NET Framework ни қўллаш, SQL Service Broker Network Connectivity функцияси, HTTP протоколи орқали аналитик хизматларга мурожаатлар каби функциялар актив бўлмайди. SQL Server Agent, Data Transformation Services ва тўлиқ матнли қидирув хизматлари сервер ўрнатилгандан кейин қўлда ёқилади.

Код бажарилишини контекст орқали бошқариш

SQL Server 2005 модул программаси операторлари бажариладиган хавфсизлик контекстини кўрсатиш имконини беради.

SQL Server 2005 устунликларидан бири минимал ҳуқуқлар принципи ҳисобланиб, фойдаланувчи томонидан эълон қилинган процедура ва функцияни бошқа фойдаланувчи ҳуқуқи билан бажаришдир. Бу учун `EXECUTE AS оператори мавжуд`. У бажарилаётган кодни ҳуқуқларини осон бошқариш имконини бериб, фойдаланувчининг ҳуқуқлари билан боғламайди. Бу функционаллик фойдаланувчилар ҳуқуқини хавфсиз бошқариш учун қўллаш мумкин. Бу жадвалга тўғридан-тўғри ҳуқуқ

бермасдан балки процедура орқали мурожаат қилинадиган масалаларда учраб туради. EXECUTE AS конструкциясида фойдаланувчи ҳисоб ёзуви(учетная запись) кўрсатилади. Бу ҳисоб ёзуви(учетная запись) процедура ва функцияда ишлатилган база объектига керакли ҳуқуқи бўлиши керак. Бунда код фойдаланувчи худди бошқа ҳисоб ёзуви(учетная запись) билан киргандадагидек бажарилади. EXECUTE AS конструкцияси SELECT, INSERT, UPDATE, DELETE ва EXECUTE амаларини бажаришда қайта-қайта ҳуқуқларни текширишни бекор қилади.

Бажарилаётган коднинг хавфсизлик даражалари

.NET-коднинг МББТ ядросида бажарилиши хавфсизликнинг заифлигига олиб келади. Шу учун бу код бажарилишдан олдин қуйидаги хавфсизлик даражаларидан бири кўрсатилиши сўралади: SAFE (ташқи ресурсларга рухсат этилмайди), EXTERNAL_ACCESS(файлга, тармоқ ресурсига,реестрга рухсат этилади),UNSAFE (барча ресурсларга рухсат этилади). Агар код бажарилилиши жараёнида кўрсатилган хавфсизлик параметрлари чегарасидан чиқса, унда Common Language Runtime хатоликни генерация қилиб, код бажарилиши тўхтатилади.

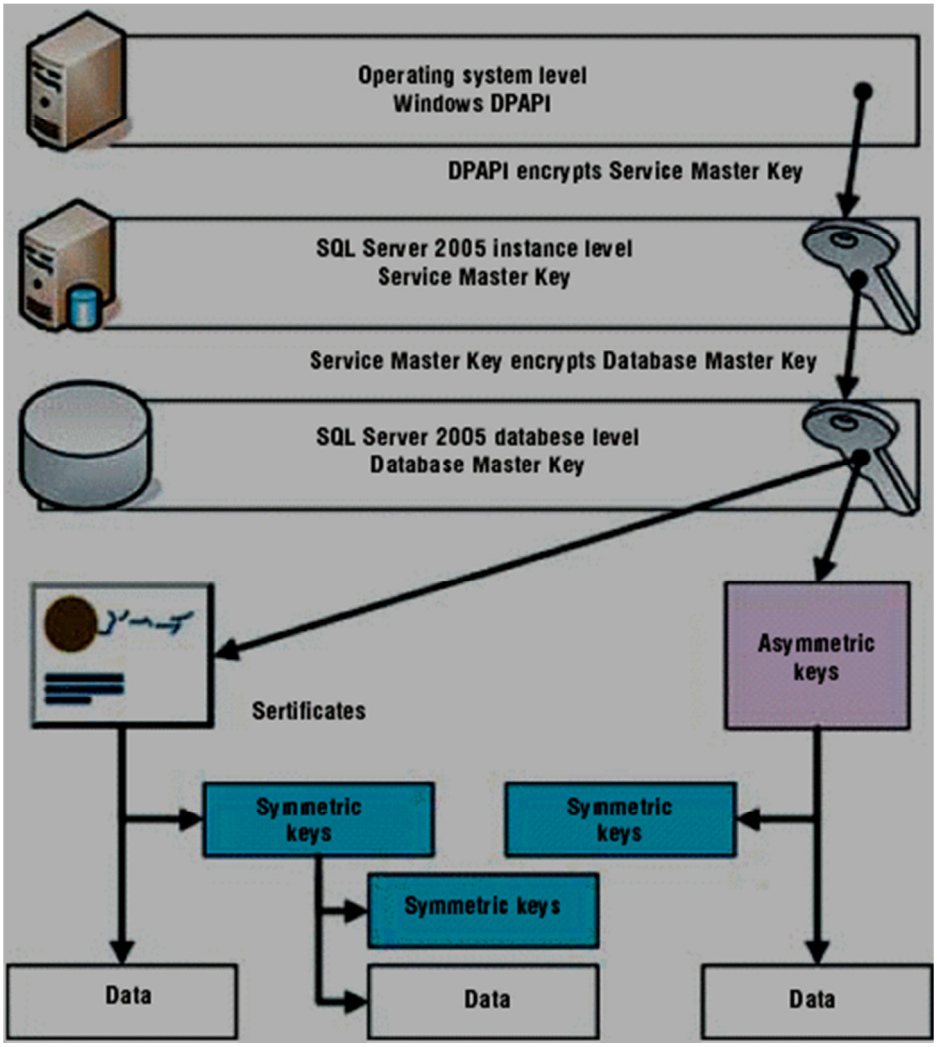
2.4. Маълумотлар ва трафикни шифрлаш

SQL Server 2005 да шифрлаш воситалари ва қўллаб қувватлайдиган алгоритмлари

SQL Server 2005 шифрлаш воситаларига эга бўлиб, рақамли имзо ва маълумотларни текшириш учун симметрик калитлар(RC4, RC2, DES, AES шифрлаш алгоритмлари) ва асимметрик калитлар(RSA алгоритми) дан

фойдаланади. Сервер ва мижоз орасидаги барча трафик IP Security (*IP SEC*) ва Secure Sockets Layer (*SSL*) протоколлари орқали шифрланади. SQL Server 2005 мижжоз ва сервер орасида ширфланмаган трафикни узатишни чеклаш хавфсизлик сиёсатини белгилаш мумкин. Бу эса трафик тутиб олинганида маълумотларни чиқиб кетишини олдини олади.

SSL протоколи Internet Information Services (*IIS*) хизмати билан интеграция қилинганда ёки X. 509v3 стандарти қўллаб қувватлайдиган сертификатлар сервери ёрдамида қўлланилади. Генерация қилинган сертификатлар фақат SSL-уланишларда эмас, балки SQL Service Broker да ҳам ишлатилади.



Устунлар даражасида маълумотларни шифрлаш

SQL Server 2005 устунлар ичидаги ахборотни шифрлаш эвазига устунлар даражасида маълумотлар хавфсизлигини таъминлаш имконини беради. У яна калитларни бошқариш инфраструктураси билан интеграллашган ҳолда маълумотларни шифрлашни қўллаб қувватлайди. Бу учун EncryptByCert, DecryptByCert, EncryptByKey, DecryptByKey, EncryptByAssym, DecryptByAssym каби функциялар мавжуд. Бу функциялар Transact-SQL кодида сертификатлар, симметрик ва асимметрик калитлар орқали шифрлаш имкони беради. Шуни инобатга олиш керакки, маълумотларни шифрлаш унумдорликни пасайтириши мумкин. Шунинг учун фақат конфиденциал маълумотларни шифрлаш мақсадга мувофиқ.

Устунлар даражасида шифрлашда маълумотларни филтрлаш, тартиблаш, индекслаш имкони бўлмайди. Шифрланмаган маълумот қандай типда бўлишидан қатъий назар шифрланган маълумот VARBINARY() каби сақланади.

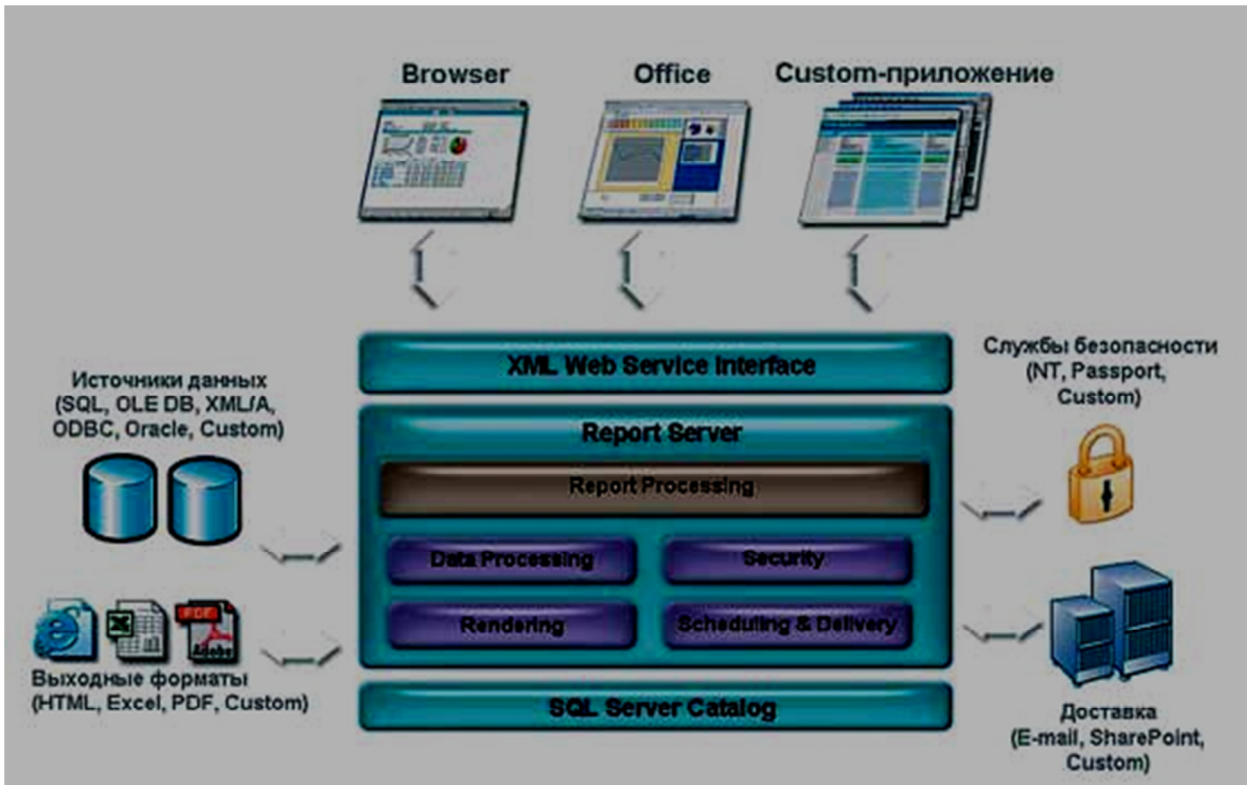
Интеграллашган хизматларда маълумотларни шифрлаш

SQL Server 2005 да мавжуд интеграллашган хизматларда маълумотлар пакетини шифрлаш билан боғлиқ бир қатор янги имкониятлар пайдо бўлди. Энди SQL Server Integration Services пакетларида рақамли имзонинг пайдо бўлгани пакетдаги ўзгаришларни аниқлаб, уларни юклашни тўхтатиши мумкин. Яна тўлиқ пакетни парол билан шифрлаш имкони мавжуд.

Пакет ичидаги барча объектларни ҳимоялаш учун уни тўлиқ шифрлаш керак.

Ҳисоботлар хизматида маълумотларни шифрлаш

Ҳисоботни генерация қилишда ҳисоботлар хизмати маълумотлар манбасига сўров бажаради. Бу учун улар маълумотлар манбасига рухсат олиш учун ҳисоб ёзуви(учетная запись)дан фойдаланади.



6-расм. *Ҳисоботлар хизмати ишлаш принципи*

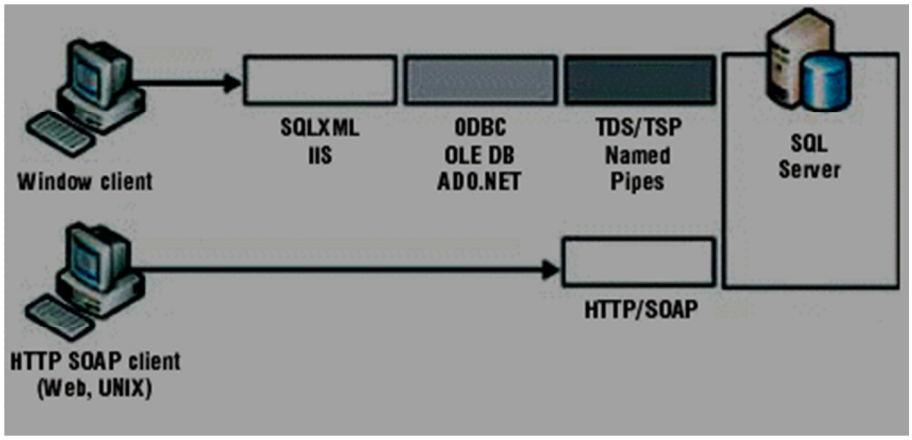
Маълумотларни ҳимоялаш учун SSL механизмини қўллаш тавсия этилади. Айниқса ностандарт аутентификация(*custom authentication*) қўлланилаётганда ёки ҳисоботни генерация қилишда қўшимча аутентификация талаб қиладиган ташқи маълумотлар манбасига мурожаат қилинганда фойдаланиш мақсадга мувофиқ.

Шифр калитининг қўшимча нусхасини қилиш тавсия этилади, чунки бу калитлар ҳисоботлар сервери ўрнатилганда ёки конфигурация қилинганда яратилиб, авария ҳолатидан қайта тикланганда шифрланган маълумотлар мурожаат қилишда керак бўлади. Ҳисоботлар хизматига мурожаат қиладиган мижоз дастурлар ҳам керак бўлганда маълумотларни шифрлашни

таъминлаши зарур. Бунда Data Protection Application Programming Interface (*DPAPI*) механизмидан фойдаланиш мумкин. Бундай дастурлар ишлаши учун минимал даражадаги ҳуқуқлардан фойдаланиш тавсия қилинади.

HTTP протоколи орқали рухсат этилган маълумотларни шифрлаш

Маълумотлар базаси ядросига HTTP-мурожаат учун рухсат бериш SQL Server 2005 янги имкониятларидан бири (7-расм).



7-расм. *Маълумотлар базаси ядросига HTTP-мурожаатни таъминлаш*

Лекин бу янгилик ҳимоянинг заифлигига олиб келади, чунки ҳозирги кунда HTTP орқали ҳужум қилиш энг кўп тарқалган. Шунинг учун сервер ва маълумотларни ҳимоялаш учун SQL Server 2005 воситалари орқали web – хизматлар ташкил қилинганда, web дастурлар ва web-хизматларда хавфсизликнинг умумий принциплари қўлланилади. Агар SQL Server ва мижоз ўртасида конфиденциал маълумот алмашишда web-хизмат ишлатиш режалаштирилган бўлса, унда керакли хавфсизликни таъминлаш учун SSL механизмини қўллаш керак.

SQL Server 2005 да SQL Server 2005 воситалари ёрдамида яратилган web-хизматларга мурожаат қилиш учун қуйидаги аутентификация механизмлари мавжуд: Basic, Digest, NTLM, Kerberos ва Integrated (NTLM и Kerberos). Kerberos аутентификация механизми анча ҳимояланган

ҳисобланади, чунки унда бошқаларига нисбатан кучли шифрлаш алгоритмлари қўлланилган.

Процедура ва кўринишлар кодини шифрлаш

Керакли ҳолда процедура кодини шифрлаш учун `CREATE PROCEDURE` ва `ALTER PROCEDURE конструкциясидан кейин WITH ENCRYPTION калит сўзини ёзиш керак`. Кўриниш кодини ҳам шифрлаш имкони мавжуд, бу учун `CREATE VIEW` ёки `ALTER VIEW конструкциясидан кейин WITH ENCRYPTION калит сўзини ёзиш керак`. Бу усул кўриниш ва процедура кодига рухсатсиз ўзгартириш киритишдан ҳимоялаш учун қўлланилади. Бунда кўриниш ва процедура кодини кейинчалик ўзгартириш учун SQL Server лойиҳасида сақлаш керак.

Маълумотлар ва мета маълумотларни аудит қилиш

Аудит — нотўғри ёки авторизациядан ўтмаган фойдаланувчилар ҳаракатини аниқлаш ва бунга қарши чора кўриш. SQL Server 2005 аудитнинг бир неча турини қўллаб қувватлайди. У Windows Security EventLog (объектларга мурожаатларни назорат қилиш механизми, ҳуқуқлардан фойдаланиш, аутентификацияга уринишлар), SQL Profiler (база объектларига мурожаатларни батафсил аудит қилиш) дан фойдаланиши мумкин.

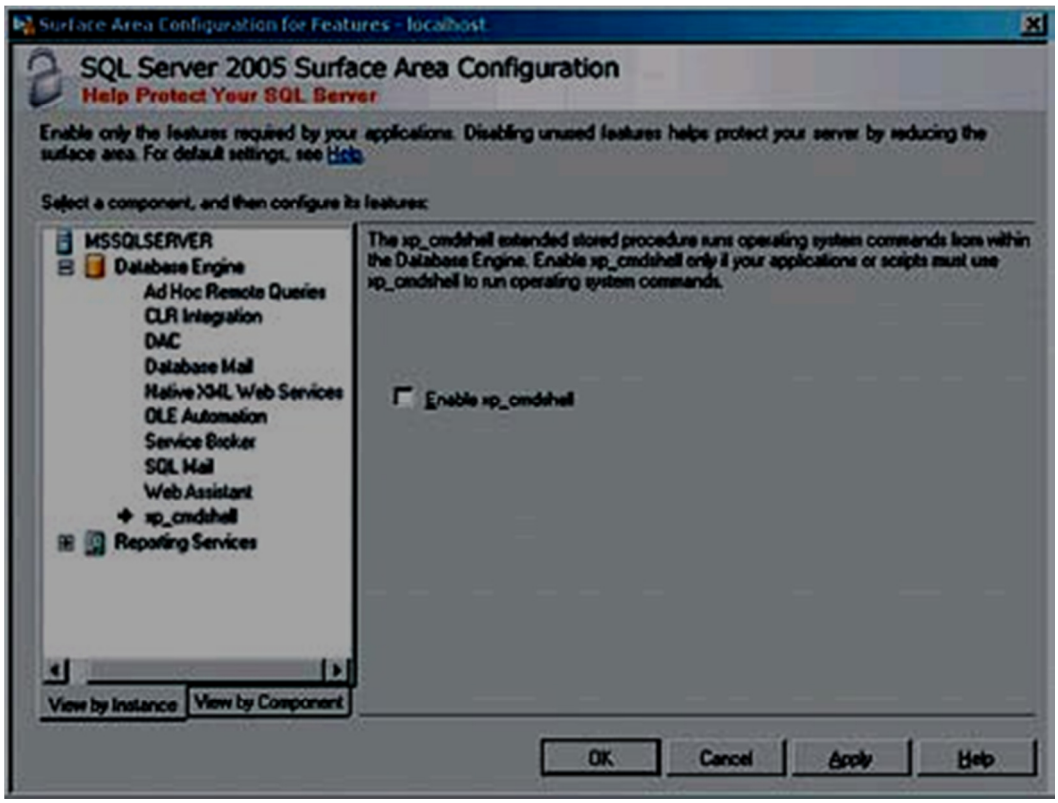
Аудитни амалга ошириш учун яна бир фойдали механизм SQL Server 2005 да пайдо бўлган, мета маълумотлар ўзгаришига реакция берадиган триггер(DDL-триггерлар) ҳисобланади. Бундай триггерларнинг яратилиши фойдаланувчи томонидан мета маълумотларни ўзгаришини кузатиш ва уни маън этиш имконини беради.

Яширин мета маълумотлар

В SQL Server 2005 да система объектлари `mssqlsystemresource` яширин базасида жойлашади, фойдаланувчилар учун унинг `Catalog Views` кўринишларига рухсат этилган. Кўринишдаги маълумотлар фойдаланувчи ҳуқуқига қараб филтрланади.

Кераксиз хизматларни ўчириб қўйиш

SQL Server нинг кўпгина хизматлари одатда ўчириб қўйилган бўлади. Агар бу хизматлар ишлатилмаса, уларни ўчирилган ҳолда қолдириш тавсия этилади. Microsoft.NET Framework ни МББТ ядросида бажариш ҳам керак бўлганда ёқиш керак. Шарт бўлмаган ҳолда қуйидаги амалларни бажариш тавсия этилмайди: Database Mail и SQL Mail, AdHoc Remote Queries, Web Assistant, Remote DAC (*Dedicated Administrator Connection*) хизматларни ёқиш, `xp_cmdshell` процедурасини бажаришга рухсат бериш, COM-кенгайтмали серверниng функционаллигини қўллаш, HTTP протокол орқали мурожаат нуқтасини яратиш (9-расм).



9-расм. *SQL Server 2005хизматларидан фойдаланишга рухсат бериш*

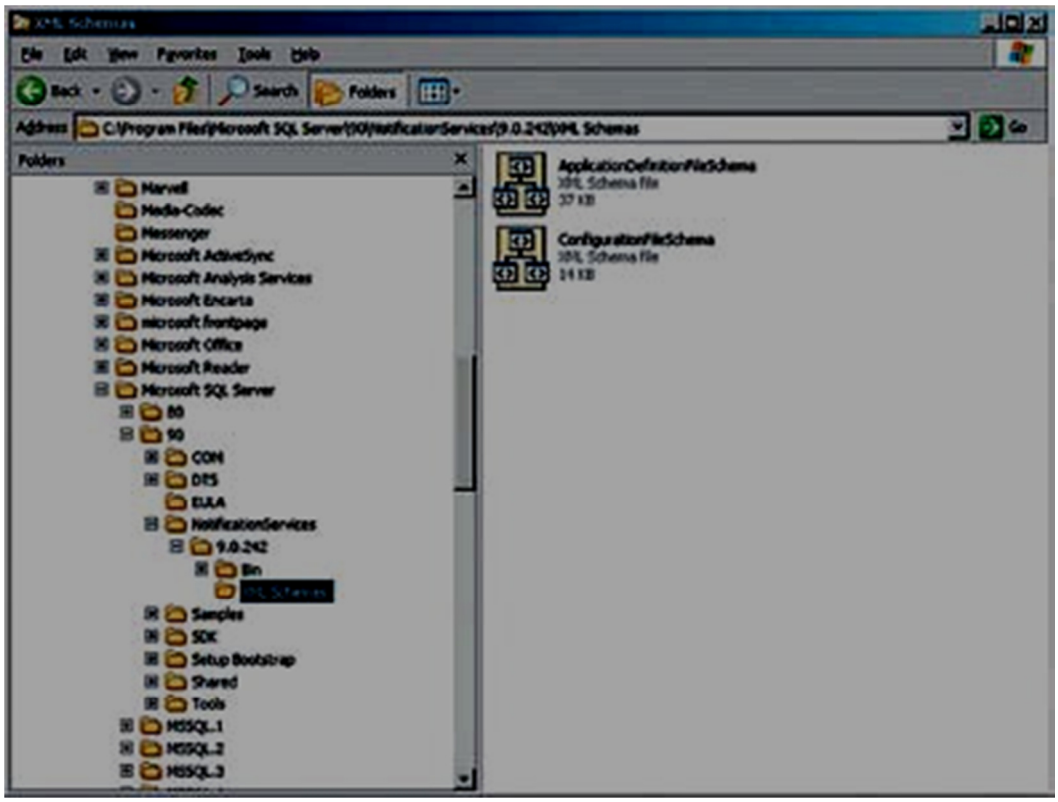
Серверда HTTP-мурожаат бўлганда брандмауэрдан фойдаланиш

Ҳозирги вақтда интернетдан HTTP протоколи орқали серверга ҳужумлар кўп тарқалганини инобатга олиб, SQL Server га HTTP протоколи орқали мурожаатга фақат зарур бўлганда рухсат бериш керак. Ва албатта бундай мурожаат брандмауэр орвали ташкил этилиши керак.

Файллар ва папкаларни хавфсизлигини таъминлаш

SQL Server нинг баъзи хизматлари(масалан, билдиришлар хизмати) конфигурация маълумотлари ва дастур маълумотларини сақлаш учун бир қатор файллар ва папкалардан фойдаланади. Билдиришлар хизмати ядроси

ушбу файлларга ҳуқуқи бўлиши керак,лекин фойдаланувчиларнинг бу файлларда сақланган маълумотларга ўзгартириш киритишга ҳуқуқи бўлмаслиги керак. Билдиришлар хизмати ишлатадиган файл ва папкаларни ҳимоялаш учун NTFS имкониятларидан фойдаланиш ёки файл ва папкаларни шифрлаш учун Encrypted File System (*EFS*) механизмидан фойдаланиш мумкин (10-расм).



10-расм. SQL Server 2005 хизматларини бошқариш

Интернет орқали репликация қилинадиган маълумотларни ҳимоялаш

SQL Server 2005 да маълумотларни интернет орқали репликация қилишда 2 хил ҳимояни қўллаш мумкин.

Биринчи репликация қилинадиган серверлар орасида (VPN-канал) ҳосил қилиш.

Иккинчи web-синхронизациядан фойдаланиш. Бу усул (*Merge Replication*) репликация турида яхши, чунки бунда HTTPS протоколи орқали SSL-шифрлаш қўлланилади.

Хавфсизлик воситаларини янгилаб туриш

Замонавий МББТ ларни яратишда бошқа дастурий маҳсулотлар каби дастурнинг янги камчиликлари аниқлаганда, ушбу камчиликларни бартараф этиш учун янгилаб туришни таклиф этади. SQL Server ни янгилаб туриш унча қийин эмас, фақат керакли опцияси танланиб қўйилса, янгилашлар автоматик тарзда ишлаб чиқарувчининг сайтидан юкланиб ўрнатилади.

Кўринишлардан фойдаланиш

Кўринишлар база объектларига хавфсиз мурожаат механизмини таъминлаш учун ишлатилади. Кўринишлар фақат шу фойдаланувчига рухсат этилган маълумотларни филтрлаб беради, жадваллар, ёзувлар, мета маълумотларга тўғридан-тўғри мурожаатни чеклаш имконини беради. Бундан ташқари кўринишлар фойдаланувчи амалларини чеклайди, чунки кўринишлар фақат `SELECT` конструкциясини қўллаб-қувватлайди, шунинг учун фойдаланувчи маълумотларни ўзгартира олмайди.

Кўринишлар яна бир неча жадвалларда йиғма маълумот олиш учун ишлатилади. Кўринишларни яратишда бошқа кўринишларда фойдаланиш тавсия этилмайди, чунки бундай лойиҳалаш кўпгина вақтинчалик жадваллар яратиш эвазига база ишлашини секинлашишига олиб келиши мумкин.

Процедуралардан фойдаланиш

Катта ҳажмдаги амалларни бажариш учун процедура ёки дастурда динамик яратилган сўровлардан фойдаланиш мумкин. Хавфсизлик нуқтаи назаридан динамик яратилган сўровлар бир қатор камчиликларга эга. Чунки улар SQL Injection каби ҳужумларни амалга ошириш имконини беради.

Хавфсизлик нуқтаи назаридан дастурлар `SELECT`, `INSERT`, `UPDATE` ва `DELETE` конструкциясини ишлатмаслиги керак. Бунинг ўрнига худи шу вазифани бажарувчи процедурага мурожаат қилиш керак. Бундан ташқари уларнинг қўлланиши фойдаланувчиларнинг жадвал ва кўринишга тўғридан-тўғри мурожаат қилишини олдини олади. Яна шуни таъкидлаш керакки, процедураларни қўллаш мижоз дастурни база схемасидан мустақил қилади, яъни схемага ўзгартириш киритиш дастурга ўзгартириш киритишга олиб келмайди.

Процедураларни қўллаш бир қатор ҳолда мижоз дастурига конфиденциал маълумотларга рухсат бермасдан сервернинг ўзида бу маълумотлар устида амаллар бажариши мумкин. Бу эса яна трафикни ҳам камайтиришга олиб келади.

Фойдаланувчининг киритган маълумотларини текшириш

Серверни мижоз дастурлар ҳужумидан қандай ҳимоя қилиш керак? Бу учун юқорида келтирилган кўрсатмаларга амал қилиш керак. Юқоридаги келтирилган кўрсатмалар қаторига фойдаланувчининг киритган маълумотини текширишни ҳам қўшиш мумкин. Бунда фойдаланувчининг киритган маълумоти серверга юборилмасдан типини текшириш ва бошқа филтрлардан ўтказиш керак.

Шуни таъкидлаб ўтмоқчимизки, билдиришлар хизматидан фойдаланганда, Subscriber, Subscriber Device ва Subscription Information

протокол майдонларида киритилган маълумотларни текшириш керак, чунки бу хизматда текшириш механизми мавжуд эмас.

ХУЛОСА

Охирги пайтларда ахборотларни ҳимоя қилиш ўта долзарблашмоқда. Чунки, жаҳонда компьютерлаштириш кўлами кенгайиб бормоқда. Бу жараён қанчалик кучайса, рухсат этилмаган ахборотларга киришга, зарур ахборотларни у ёки бу йўл билан йўқ қилишга интилувчи ёвуз ниятли кимсалар ёки «компьютер безорилари» шунчалик кўпаяверади. Шунинг учун ҳозир вақтда келиб, ахборотларни хавфсизлигини ошириш талаб этилади. Ҳозирги кунда дунёда ахборот коммуникация технологиялари, маълумотларни узатиш тармоқларининг ривожланиши, шу билан бирга, ахборот тизимларининг глобаллашуви ва ахборот интеграциялашуви жараёни юқори сурьатларда ривожланмоқда. Ушбу жараёнларнинг ривожланиши ахборот хавфсизлигини юқори даражада таьминлашни талаб қилади.

Турли хилдаги ахборотлар худудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга Internet ҳалқаро компьютер тармоғи орқали кириб келди. Шунинг учун хам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Айниқса, корпоратив МББТ(Маълумотлар базасини бошқариш тизими)ларда сақланаётган маълумотлар хавфсизлигини таъминлашга катта эътибор берилмоқда. МББТ ларда хавфсизлик воситалари мавжуд, лекин бу воситалардан тўғри фойдаланган ҳолдагина хавфсизликни таъминлаш мумкин. МББТ да асосан хавфсизлик объекти жадвал, кўриниш, процедура ва функциялар ҳисобланади. SQL Server 2005 да ҳар бир объектга турли фойдаланувчига турли даражадаги ҳуқуқлар бериш, фойдаланувчи ҳуқуқларини роллар орқали бошқариш, маълумотларни шифрлаш имкони мавжуд. Кўп ҳолларда фойдаланувчи даражасига қараб, маълум жадвал қаторларига(яъни бир қисмига) рухсат бериш керак бўлади. Бундай ҳолатда дастурчи масаланинг қўйилишига қараб ўзи ҳал қилади.

SQL Server 2005 да хавфсизликни таъминлаш учун бир қанча воситаларга эга бўлиб улар қуйидагиларни ташкил этади:

- Роллар орқали фойдаланувчилар ҳуқуқларни бошқариш
- SQL Server 2005 нинг хизматларида ҳуқуқлар бошқариш
- Маълумотлар ва трафикни шифрлаш
- Минимал ҳуқуқлар билан кодни бажариш
- Процедура ва кўринишлар кодини шифрлаш

SQL Server 2005 да хавфсизликни таъминлаш учун қуйидаги амалларни бажариш тавсия этилади:

- Фойдаланувчининг киритган маълумотларини текшириш
- Амаллар бажаришда процедуралардан фойдаланиш
- Фойдаланувчига рухсат этилган маълумотларни филтрлаш учун кўринишлардан фойдаланиш
- Хавфсизлик воситаларини янгилаб туриш
- Интернет орқали репликация қилинадиган маълумотларни ҳимоялаш
- Файллар ва папкаларни хавфсизлигини таъминлаш
- Маълумотлар ва мета маълумотларни, фойдаланувчи ҳаракатини аудит қилиш

Ушбу битирув малакавий ишимизда SQL Server 2005 да ахборот хавфсизлигини таҳлил қилган ҳолда уларни намойиш қилувчи электрон кўргазма яратилди. Ҳозирги кунда мамлакатимизда ахборот хавфсизлиги масалаларига катта эътибор берилмоқда. Ушбу мавзу доирасидаги ишимиз айнан шу муаммога қаратилгандир. Айниқса, яратилган электрон дастурий махсулот ушбу муаммони муайян даражада еча олади деб ҳисоблаймиз. Уни олий ўқув юртлари, ҳамда академик лицей ва касб ҳунар коллежларида ўқув жараёнида қўллаш мумкин. Шу билан бирга маълумотлар базаси барча фойдаланувчилари учун ҳам қизиқарли ва фойдали деб ҳисоблаймиз.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Каримов И.А. Юксак маънавият – енгилмас куч. – Тошкент: “Маънавият”, 2008
2. Брюс Шнайер. Секреты и ложь. Безопасность данных в цифровом мире. Триумф-2002.
3. Канноли Т. Брегк К. Базы данных, проектирование, реализация и сопровождение, теория и практика. Университет Пейсли, Шотландия, изд. М.- СПБ. –Киев, 2003.
4. Григорьев Ю.А., Ревунков Г.И. Банки данных. М.: Изд. МГТУ им Баумана, 2002.
5. Ғуломов С.С., Шермухамедов А.Т., Бегалов Б.А. Иқтисодий информатика. Дарслик/Академик С.С. Ғуломовнинг умумий таҳрири остида -Т.: Ўзбекистон, 1999. 528 б.
6. Ғуломов С.С., ва бошқалар. Ахборот тизимлари ва технологиялари: Олий ўқув юрти талабалари учун дарслик. Академик С.С. Ғуломовнинг умумий таҳрири остида -Т.: «Шарқ», 2000. 529 б.
7. Скляров. Искусство, защиты и взлома информации. Санкт-Петербург. "БХВ-Петербург. 2004.
8. Роберт Чёрчхаус. Коды и шифры. Москва 2006.
9. В. Громов, Г.А. Васильев Энциклопедия компьютерной безопасности. Москва 2007.
10. Ғаниев С.К.,Каримов М.М. Ҳисоблаш тизимлари ва тармоқларида информация ҳимояси: Олий ўқув юрт. талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.
11. Microsoft SQL Server 2005. Справочник администратора. Уильям Р. Станек. 2008
12. Программирование баз данных Microsoft SQL Server 2005 для профессионалов. Роберт Виейра. 2008
13. MS SQL Server 2005 для администраторов. Ростислав Михеев. 2007
14. SQL Server 2005. Библия пользователя. Пол Нильсен. 2008
15. SQL Server 2005. Новые возможности для разработчиков. С. Байдачный, Д. Маленко, Ю. Лозинский. 2006
16. www.ziyonet.uz
17. ftp://ftp.kiae.su/msdos/crypto/pgp
18. http://drago.centerline.com:8080/franl/pgp/…