ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚУМИТАСИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ФАРҒОНА ФИЛИАЛИ

Қўл ёзма хуқуқида

УДК 004.42

ТОЖИМАМАТОВ ИСРАИЛ НУРМАМАТОВИЧ

Ишлаб чиқариш учун дастурий таъминот яратишда ахборотларни ҳимоялаш муаммолари бўйича дастурлаш тилларида қўлланиладиган тасодифий рақамлар генераторлари сифатини тадқиқ этиш

5А 330201 – «Компьютер тизимлари
ва уларнинг дастурий таъминоти»

МАГИСТР академик даражасини олиш учун ёзилган ДИССЕРТАЦИЯ

Илмий раҳбар:
т.ф.н. доц. А.А. ХОЛМУРЗАЕВ

Фарғона – 2014

МУНДАРИЖА

КИРИШ.

Муҳтарам юртбошимиз Ислом Каримов «Фуқароларнинг ахборот соҳасидаги ҳуқуқ ва эркинликларини таъминлаш масаласи инсоннинг ахборот олиш, ахборотни ва ўз шахсий фикрини тарқатиш ҳуқуқи ва эркинлигини ўзида мужассам этган бўлиб, бу Ўзбекистонда демократик жамият асосларини барпо этишнинг муҳим шарти, таъбир жоиз бўлса, тамал тоши ҳисобланади» деб эътироф этганлар.[1]

Зеро, ахборот асри дея эътироф этилаётган бугунги кунида бутун дунё билан хамнафас тарзда мамлакатимизда ҳам компьютер ва ахборот технологиялари, телекоммуникация ва маълумот узатиш тармоқлари, интернет хизматларини ривожлантириш, уларни дунё стандартларига етказиш ва шу асосда ахборотлашган жамият сари жадал интилиш мақсадида кенг кўламли чора тадбирлар ва амалий ишлар олиб борилмоқда. Чунки бугунги кунда замонавий ахборот технологияларини интенсив тарзда ривожланиб бориши янги ахборотни қайта ишлаш воситалари, ахборот хавфсизлиги муаммолари, ахборотни ҳимоя қилиш тизимлари, жамиятимизнинг турли сохларида уларни қўллаш ва усулларини яратиш ушбу масалаларни долзарблигини вужудга келтирамоқда. [2]

Ахборот хавфсизлигига бўлган эхтиёжларнинг тобора ортиб бориши, янги ҳимоя қилиш тизимларини турлари ва усулларини яратиш ҳамда уларни тадқиқ этиш бўйича самарали ишларни олиб боришни талаб қилади. Бу эса доимий равишда ташкилот ва корхоналарни ҳимоялаш тизимларидан тўғри, самарали, муваффақиятли фойдаланишига боғликдир. Айни вақтда кўплаб ахборотни ҳимоя қилиш воситалари тасодифий рақамлар генераторлари (ТРГ) асосида қурилмоқда ва ташкил этилмоқда. Шу нуқтаи назардан хар бир ташкилот ва корхоналарни ўзига тегишли ахборот тизимлари ва технологияларидан тўғри, самарали, муваффақиятли фойдаланиши уларни қандай ва нима асосга қурилишига асосланади.

Диссертация мавзусининг асосланиши ва унинг долзарблиги. Ахборот-коммуникация тизимларида локал ва корпоратив компьютер

тармоқларининг кўпайиши ва бу тармоқларнинг глобал интернет тармоғига уланиши фойдаланувчилар ўртасида электрон маълумот алмашувининг кенг қўлланилишига олиб келди. Жамиятнинг ахборотга бўлган эхтиёжи ахборот-ресурс марказларининг ташкил этилиши ва очиқ интернет тармоғи орқали фаолият юритишига олиб келиши билан бир вақтда алмашинувчи маълумотларнинг узатилиши давомида кафолатли муҳофазасини таъминлаш масаласини келтириб чиқарди. Ахборот-коммуникация тизимларининг тўлиқ равишда рақамлилаштирилиши, маълумотни узатишда оптик толали воситалардан фойдаланилиши, вилоятлараро видеоконференция, IP-телефония, электорн рақамли имзо ва бошқа тутилишсиз узатилишни талаб қилувчи катта миқдордаги ахборот оқимларининг очиқ алоқа каналларида узатилиш давомида муҳофазасини таъминлаш масаласи ўз навбатида юқори тезликда тутилишсиз ишловчи криптографик воситаларни талаб қилади. Бундай криптографик воситалар асосини аппарат ва аппарат-дастурий воситаларда қулай ҳамда самарали амалга оширилувчи криптобардошли узлуксиз шифрлаш алгоритмлари ташкил этади. Ахборот-коммуникация тизимларидан фойдаланувчи корхона, ташкилот ҳамда муассасалар ўз фаолияти учун зарур бўлган маълумотларининг узатилиши ва қабул қилиниши давомида кафолатли муҳофазани таъминлаш учун четда ишлаб чиқарилган аппарат ва аппарат-дастурий криптографик воситаларини қўлламоқдалар. [3]

Ахборот-коммуникация тизимларида маълумотларни кафолатли муҳофазасини таъминловчи криптографик воситаларнинг маҳаллий шароитда яратилиши иқтисодий самарали бўлиши билан бир қаторда уларнинг доимий дастурий-техник кузатуви ҳамда такомиллаштирилиб бориши таъминланади. Самарали тасодифий рақамлар генераторлари, шифрлаш алгоритмлари шифрлашдан ташқари ахборот хавфсизлигини таъминлашнинг бошқа барча криптографик воситаларининг (блокли шифрлаш, асимметрик шифрлаш, электрон рақамли имзо, хэш-функция) таркибида сеанс калитларини ҳосил қилиш, дастлабки тасодифий қийматлар

ҳосил қилиш генератори сифатида қўлланилиши билан ахборот хавфсизлиги тизими криптобардошлигининг юқори бўлишини таъминлайди. Диссертация иши, криптографик акслантиришлари мавжуд ТРГ ларни акслантиришларидан фарқли, аппарат ва аппарат-дастурий қурилмалар яратишда қулай ва самарали амалга ошириш имкониятини берувчи, криптобардошлиги етарли даражада юқори, асосий акслантиришлари криптобардошликни янада оширилишига ҳамда аппарат воситаларини кам харж эвазига такомиллаштириш ва модернизациялаш қулайлигини таъминловчи тасодифий рақамлар генераторлари ишлаб чиқиш, шифрлаш алгоритмларини яратиш, уларнинг криптобардошлиги ва самарадорлигини баҳолаш масалалари ечимларига бағишланган.

Ахборот хавфсизлиги тизимининг воситаларида тасодифий кетма-кетлик генераторларидан ва тезкор ишловчи аппарат-дастурий воситалардан фойдаланиш учун псевдотасодифий сонлар кетма-кетлиги генераторларини кенг ўрганиш, узлуксиз шифрлаш алгоритмларининг криптобардошлик талаблари, гамма ишлаб чиқиш хусусиятлари ва самарадорлиги чуқур таҳлил қилиниши ва етарли даражада ўрганилиши керак. [4]

Ўзбекистон Республикаси Президенти фармонларида ва Хукуматининг қарор ҳамда буйруқларида мамлакатни компьютерлаштириш, ахборот-лаштириш, банк, савдо-сотиқ ва бошқа қатор соҳаларда электрон маълумотнинг муҳофазасини кафолатли таъминловчи тасодифий рақамлар генераторларини ахборотларни ҳимоя қилиш тизимларида қўллашнинг қонуний меъёрий хужжатлари асослари ишлаб чиқилиб, бу соҳадаги илмий тадқиқот ишларни жадаллаштиришни тақазо этади. Ушбу диссертация иши ҳам Ўзбекистон Республикаси Президенти И.А. Каримовнинг 2007 йил 3 апрелдаги ПҚ-614–сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» қарори, Ўзбекистон Республикасининг «Ахборотлаштириш тўғрисида»ги қонуни, Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонуни ушбу йўналишида олиб борилаётган

давлатимизнинг устивор тамойилларидан бири ҳисобланиб, илмий тадқиқот ишини мазмунини мақсадли эканлигини белгилаб беради. [5]

Тадқиқот объекти ва предметининг белгиланиши. Тадқиқотнинг объекти тасодифий рақамлар генераторларини ахборотларни ахборотларни ҳимоялаш воситаларда қўлланилувчи криптобардошли ТРГ алгоритмлари ва дастурларини ишлаб чиқариш жараёнларига қўллаш ҳисобланади.

ТРГ ларни яратиш ва таркибидаги акслантиришларнинг криптографик бардошлиги, самарадорлик мезонлари ва юқори тезликдаги квантли ТРГ даражаларини баҳолаш усуллари тадқиқотнинг предмети ҳисобланади.

Тадқиқот мақсади ва вазифалари. Ушбу магистрлик диссертациясида олиб борилган тадқиқотнинг мақсади ишлаб чиқариш учун дастурий таъминот яратишда ахборотларни ҳимоялаш муаммолари бўйича дастурлаш тилларида қўлланиладиган тасодифий рақамлар генераторлари сифатини тадқиқ этиш ва маълумотларнинг муҳофазасини таъминловчи аппарат-дастурий криптографик воситаларда қулай ҳамда самарали қўлланувчи криптобардошли ТРГ лар алгоритмларини яратиш, уларнинг самарадорлигини баҳолаш усулларини ва дастурий таъминотларини таклиф этишдир.

Тадқиқот мақсадини амалга ошириш учун диссертация ишини бажаришда қуйидаги вазифалар қўйилди:

- мавжуд ахборот хавфсизлиги муаммоларини ўрганиш ва яратиш йўналишларини туркумлаш;
- ахборот хавфсизлигини таъминлашнинг асосий йўллари ҳамда хуқуқий ва ташкилий таъминотини назарий жихатларини ўрганиш;
- ахборотни ҳимоялашнинг криптографик усуллари, криптографик воситаларида самарали қўлланувчи криптобардошли акслантиришлардан фойдаланиб ТРГ алгоритмларини яратиш ва жараён босқичларининг функционал схемасини тузиш;
- яратилган алгоритмларнинг самарадорлигини баҳолаш талабларини ва усулини ишлаб чиқиш;

– тасодифий рақамлар генераторлари ва уларнинг турларини ўрганиш ва шу асосида янги кўринишдаги криптобардошлик ва самарадорликни баҳолаш усулларининг дастурий таъминотларини ишлаб чиқиш;
– псевдотасодифий кетма-кет рақамли генереторларни тузилиши ва хусусиятларини ўрганиш ва янги характерли псевдотасодифий ТРГ лар таклиф қилиш;
– тасодифий рақамлар генераторлари сифатини бахолаш мезонларини ишлаб чиқиш асосида юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш услубларини яратиш;
– яратилган ТРГ криптографияда ва ахборотни ҳимоялаш тизимларида қўллаш алгоритмларнинг криптобардошлиги ва самарадорлиги кўрсаткичлари хақида аниқ натижаларга эришиш.

Тадқиқтонинг асосий масаллари ва фаразалари. Ахборот коммуникация тизимларидаги маълумотларнинг муҳофаза-сини таъминловчи аппарат ва аппарат-дастурий криптографик воситаларда қулай ҳамда самарали қўлланувчи криптобардошли тасодифий рақамлар генераторларини яратиш, криптобардошлик ва самарадорликни баҳолаш усулларини криптографик алгоритмларига қўллаш ва уларни ахборотларни хавфсизлиги муаммолари ҳамда ушбу масалаларини ечимларига эришиш.

Мавзу бўйича қисқача адабиётлар тахлили. Ахборотни ҳимоялаш ва ахборот хавфсизлигини тъминлаш бўйича ҳамда тасодифий рақамлар генераторлари, псевдотасодифий сонлар кетма-кетлиги генераторлари, криптография ва шифрлаш тизимларига доир манбалар мавжуд адабиётлар ҳамда C++, Borland Delphi, VB дастурлаш тиллари ва 1cX платформасидан фойдаланиш йўрқномалари диссертация мавзусини ёртишга хизмат қилади. Масалан. Б.Шнайернинг “Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С”, М.А.Ивановнинг “Криптографические методы защиты информации”, Н. А.Колесова, И. М.Ажмухамедовларнинг “Методика оценки качества последовательности случайных чисел” номли адабиётларини келтириш мумкин.

Тадқиқтода қўлланилган услубларнинг қисқача тавсифи. Ушбу диссертацияда ахборотни криптографик ҳимоялаш тизимлари назарияси, эҳтимоллар назарияси, сонлар назарияси, математик мантиқ ва комбинаторика методларидан ҳамда уларни ишлаб чиқариш жараёнларига қўллаш усулларидан фойдаланилган.

Шунингдек, тасодифий рақамлар генераторларини дастурлаш тилларида яратиш усуллари ва йўллари, турли дастурларда жумладан C++, Borland Delphi, VB дастурлаш тиллари ҳамда 1c8.2. платформасида қўллаш усуллари тадбиқ қлинган.

Тадқиқот натижаларининг илмий ва амалий аҳамияти. Мавжуд ва яратилган ТРГ ни ахборотлар хавфсизлиги муаммоларини хал этишдаги криптобардошлигини баҳолаш ва тизимли тадқиқлаш диссертациянинг илмий аҳамияти ҳисобланади.

Диссертация ишининг амалий аҳамияти - яратилган ТРГ ва дастурий таъминотларини Ўзбекистон шароитида ишлаб чиқиладиган ишончли ва тезкор ишловчи дастурий воситаларида, компьютердаги маълумотларнинг махфийлигини таъминлашда фойдаланиш мумкинлигидадир.

Диссертация доирасида яратилган дастурий таъминот, 1С8.2 дастурий платформаси мисолида Ўзбекистон Республикаси ишлаб чиқариш корхоналарида, жумладан “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ ларида бухгалтерия ҳисоби бўйича олинган маълумотларни ҳимоялашга тадбиқ этилди. Ундан ташқари Фарғона компьютер технологиялари касб-ҳунар коллежи, ФарДУ қошидаги академик лицейнинг ўқув жараёнида қўлланилди.

Ушбу магистрлик диссертацияси устида олиб борилган ишлар ва дастурий восита Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ ларида бухгалтерия ҳисоби бўйича олинган маълумотларини, ўрнатилган маълумотлар базасини ҳимоялашда ҳамда Фарғона компьютер технологиялари касб-ҳунар коллежи, ФарДУ қошидаги академик лицейнинг

ўқув жараёнида синовдан ўтказилди. Қўлланилганлиги ҳамда синовдан ўтказилганлиги ҳақидаги жорий этиш далолатномалари олинди.

Тадқиқотнинг илмий янгилиги. Мазкур дисертация ишининг илмий янгилиги қуйидагилардан иборат:

- мавжуд тасодифий сонлар кетма-кетлиги генераторларининг такомиллаштирилган туркуми ишлаб чиқилди;
- ТРГининг криптобардошлиги ва самарадорлигини баҳолаш усули ишлаб чиқилди;
- учта дастуралаш тили ва битта дастурий платформада ТРГ яратилди;
- ТРГ ларнинг криптобардошлик ва самарадорлик даражасини баҳолаш усулининг дастурий таъминотлари ишлаб чиқилди.

Диссертация таркибининг қисқача тавсифи. Диссертация кириш, тўртта бўлим ва хулосадан ташкил топган. 92 та номдаги фойдаланилган адабиётлар руйхати бўлиб, жумладан 68 та адабиёт ва ўқув қўллнмалар, 10 та илмий тадқиқот ишлари, 14 та интернет илова ва ресурсларидан ҳамда 6 та иловадан иборат. Диссертациянинг асосий хажми 99 бет матн, 15 та расмдан ташкил топган. Шунингдек, диссертация мавзуси бўйича 3 та илмий тезис ва мақола эълон қилинган.

I-БОБ. АДАБИЁТЛАР ШАРҲИ ВА ТАҲЛИЛИ.

Ахборот технологияларини интенсив ривожланишида ахборот хавфсизлиги муаммолари ва уларни ечишнинг сифати, ахборотни ҳимоя қилиш тизимларини янги турлари ва усулларини яратиш ушбу масалаларни долзарблигини вужудга келтирмоқда. Бу эса доимий равишда ташкилот ва корхоналарни ҳимоялаш тизимларидан тўғри, самарали, муваффақиятли фойдаланишига боғлиқдир. Айни вақтда кўплаб ахборотни ҳимоя қилиш воситалари тасодифий рақамлар генераторлари (ТРГ) асосида қурилмоқда ва ташкил этилмоқда. ТРГ ларини қуриш муаммолари ва уларни тадқиқ этишда А. Зубков, А. Щербаков, Д. Кнут, Б Шнайер, Д.Келси, А.Шамир, М. Наор, О. Рейнголд, Н. Фергюсон, Н. А.Колесова, А.В. Архангельская, И.М.Ажмухамедов каби жуда кўплаб олимлар илмий тадқиқотлар олиб боришган[*].

Хусусан Ўзбекистон Республикасининг бир қатор олимлари Д.Э.Акбаров, И.А.Мусаев, И.М.Каримов, С.К.Ғаниев, П.Ф.Хасанов, М.М.Арипов, Р.И.Исаев, Х.П.Хасанов, О.П.Ахмедова, О.Х.Расулов ва К.А.Ташиевлар томонидан олиб борилган тадқиқотлар келтирилиши мумкин. Улар томонидан олинган тадқиқотнинг назарий ва амалий натижаларни замонавий иқтисодиётнинг турли соҳаларида қўллаш, ахборот хавсизлигини таъминловчи аппарат ва аппарат-дастурий воситалар таркибида фойдаланиш катта аҳамиятга эга[**].

Тасодифий рақамлар генераторлари асосида аппарат ва аппарат-дастурий воситаларни яратиш устида дунёнинг кўплаб етакчи илмий тадқиқот институтлари ва компаниялари («Crypto AG» Швейцария, «Анкад» Россия, «Global Crypto» АҚШ, «RSA Data Security» АҚШ ва бошқа.) томонидан инженерлик-тадқиқот ишлари олиб борилмоқда. Олиб борилган тадқиқотлар криптографик тизимнинг криптобардошлиги унинг таркибига

[*] - Фойдаланилган адабиётлар рўйхатида берилган 3,5, 7, 9, 65 рақмли адабиётлар юқорида қўрсатилган олимлар томонидан ишлаб чиқилган.

[**] - Фойдаланилган адабиётлар рўйхатидаги 5, 33, 34, 35, 69, 70 рақмларидаги адабиётлар юқорида қўрсатилган олимлар томонидан ишлаб чиқилган.

кирувчи алгоритмнинг маҳфий сақланишига боғлиқ бўлмай, фақат махфий сақланувчи калитгагина боғлиқ қилиб яратиш кераклигини келтириб чиқарди ва исботлади. Нисбатан кичик узунликка эга бўлган, яъни кафолатланган криптобардошликни таъминловчи узунликка эга калит билан бир томонлама криптографик акслантиришлар асосида, етарли даражада катта узунликдаги псевдотасодифий сонлар кетма-кетлиги гаммасини ишлаб чиқарувчи генераторлар негизида тезкор узлуксиз шифрлаш алгоритмлари, бардошли калит ва бошқа тасодифий параметрлар ишлаб чиқиш алгоритмлари яратилди.[6]

Ушбу илмий-тадқиқот ишини ёритиш учун жами 92 та адабиётлар манбаидан фойдаланилган бўлиб, жумладан 68 та адабиёт ва ўқув қўллнмалар, 10 та илмий тадқиқот ишлари, 14 та интернет илова ва ресурсларидан, 10 та илмий тадқиқот ишларидан фойдаланилган.

Адабиётларнинг 14 таси президентимиз Ислом Абдуғаниевич Каримовнинг асарлари бўлиб, улардан Ўзбекистон Республикаси Президенти фармонларида ва Хукуматининг қарор ҳамда буйруқларида мамлакатни компьютерлаштириш, ахборотлаштириш, банк, савдо-сотиқ ва бошқа қатор соҳаларда электрон маълумотнинг муҳофазасини кафолатли шартларини муҳим жиҳатларини ва йўналишларини очиш жараёнида фойдаланилди. Шунингдек кириш ва хулосавий қисмда президентимизнинг аниқ ва устивор қилиб белгилаб берган фикр ва мулохазаларидан фойдаланилди.

Ўзбекистон Республикаси қонун ҳужжатларидан 5-тасидан фойдаланилган бўлиб, улардан ахборот хавфсизлигини таъминлашнинг асосий йўллари ҳамда хуқуқий ва ташкилий таъминоти ҳамда уларнинг меъёрий талабларини ёритишда асос сифатида фойдаланилди.

68 та адабиёт ва ўқув қўлланмалардан дисертацияининг асосий моҳиятини очиб беришда, яъни, ахборот хавфсизлигига тахдидлар ва уларни келиб чиқиш асослари, ахборотни ҳимоялашнинг криптографик усуллари, индентификация ва аутентификация, тасодифий рақамлар генераторлари ва уларнинг турлари, псевдотасодифий кетма-кет рақамли генереторларни

тузилиши ва хусусиятлари ва бошқа шу каби ишнинг асосий қисмларини ёртишда фойдаланилди.

10 илмий тадқиқот ишларидан қиёсий тахлил ва солиштириш натижалари олиниб, тасодифий рақамлар генераторлари сифатини бахолаш мезонлари, юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш, тасодифий рақамлар генераторларини ахборот тизим ва криптографик иловаларда қўллаш ишларини ёртишда асос сифатида қўлланилди.

14 интернет ресурсларидан ахборотларни ҳимоялаш муаммолари бўйича c++, Borland Delphi, Visual Basic дастурлаш тилларида ва 1С8.2 дастурий платформасида яратилган тасодифий рақамлар генераторини сифатини тадқиқ этиш ва яратиш жараёнида фойдаланилди.

Эълон қилинган ишлар рўйхати:

1. И.Тожимаматов, Д.Халилов, “Тасодифий рақамлар генераторлари сифатини бахолаш мезонлари” мавзусида илмий тезис, Республика миқиёсда ўтказилган «Ахборот технологиялари ва телекоммуникация тизимларини самарали ривожлантириш истиқболлари» илмий-техник конференциясида маъруза қилинган ва мутахасислар томонидан муҳокама қилинган (Тошкент, 13-14-март 2014й.)173**,** 174, 175 бет**.**

2. И.Тожимаматов, Д.Халилов, “Юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш” мавзусида илмий тезис, Фарғона Вилояти Ҳокимлиги Хотин-Қизлар Қўмитаси, Вилоят Худудий Инновацион Фаолияти ва Технологиялар Трансфери Маркази, Вилоят Маънавият Тарғиботи Маркази, Вилоят Олий Таълим Муассасалари томонидан ўтказилган «Иқтисодиётимизнинг ривожланишида янги инновацион технологияларнинг ўрни» мавзусидаги илмий-амалий конференциясида маъруза қилинган ва мухокамадан ўтган (Фарғона, 2014й.). 110-112 бет.
3. И.Тожимаматов, Д.Халилов, “Тасодифий рақамлар генераторларини ахборот тизими ва криптографик иловларда қўллаш” мавзусида илмий

тезис, Андижон машинасозлик институти да «Современные материалы техника и технологии ва машиностроении» мавзусидаги халыаро илмий-техник конференциясида маъруза қилинган ва мухокамадан ўтган (Андижон, 2014 йил) 148-151 бет.

I-боб бўйича хулоса.

Ушбу боб бўйича олиб борилган тахлил ва ўргнишлар натижасида жуда ҳам кўплаб тадқиқ қилинган ишларни кўриб чқилди. Натижда, ТРГ ларини қуриш муаммолари ва уларни тадқиқ этишда А. Зубков, А. Щербаков, Д. Кнут, Б Шнайер, Д.Келси, А.Шамир, М. Наор, О. Рейнголд, Н. Фергюсон, Н. А.Колесова, А.В. Архангельская, И.М.Ажмухамедов каби олимлар илмий тадқиқотларини ўрганишга муваффақ бўлинди.

Айниқса, Ўзбекистон Республикасида айни сохага тегишли долзарб муаммоларни ечимига қаратилган ишларни олиб борган олимларимизнинг, жумладан Д.Э.Акбаров, И.А.Мусаев, И.М.Каримов, С.К.Ғаниев, П.Ф.Хасанов, М.М.Арипов, Р.И.Исаев, Х.П.Хасанов, О.П.Ахмедова, О.Х.Расулов ва К.А.Ташиевларнинг илмий тадқиқотлар ҳамда ишлари муҳим ахамият касб этади.

Шунингдек фойдаланилган адабиётлар, интернет ресурслари ва илмий тадқиқот ишлари чукур ўрганилган.

Олиб борилган изланишлар натижасида “Тасодифий рақамлар генераторлари сифатини бахолаш мезонлари”, “Юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш” ҳамда “Тасодифий рақамлар генераторларини ахборот тизими ва криптографик иловларда қўллаш” мавзуларида илмий мақола ва тезислар элон қилинган.

Ушбу бобда олиб борилган ишлар диссертациянинг келгусидаги боблари ва бўлимларини чуқур ва етарли даражада ёритишга мезон бўлиб хизмат қилади.*

* - Фойдаланилган адабиётлар рўйхатида берилган барча адабиётлар ва эълон қилинган ишлар ҳамда олиб борилган тадқиқотлар бобнинг асосий манбалари ҳисобланди.

II-БОБ. АХБОРОТЛАРНИ ҲИМОЯЛАШ МУАММОЛАРИ ВА УЛАРНИ ТАШКИЛ ЭТИШ УСУЛЛАРИ

2.1. Ахборот хавфсизлигига тахдидлар ва уларни келиб чиқиш асослари.

Хавфсизлик – ҳар куни биз тўқнашадиган ҳаётимизнинг бир муҳим кўринишдир. Уйимизнинг эшигини қулф билан беркитиш, хамённи сақлаш ва бошқача шу каби турли хавсизлик чораларини кўрамиз. Бундай чораларни ҳам “рақамли дунёда”, яъни компьютерлар дунёсида кўрмаслик мумкин эмас.

Умуман олганда ахборотни муҳофаза қилишнинг мақсадини қуйидагича ифодалаш мумкин:

- ахборотни тарқаб кетиши, ўғирланиши, бузилиши, қалбакилаш-тирилишини олдини олиш;
- шахс, жамият, давлатнинг хавфсизлигига таҳдидни олдини олиш;
- ахборотни йўқ қилиш, модификациялаш, бузиш, нусха олиш, блокировка қилиш каби ноқонуний ҳаракатларнинг олдини олиш;
- ахборот ресурслари ва ахборот тизимларига ноқонуний таъсир қилишнинг бошқа шаклларини олдини олиш, ҳужжатлаштирилган ахборотга шахсий мулк объекти сифатида ҳуқуқий режимни таъминлаш;
- ахборот тизимида мавжуд бўлган шахсий маълумотларнинг махфийлигини ва конфеденциаллигини сақлаш орқали фуқароларнинг конституциявий ҳуқуқларини ҳимоялаш;
- давлат сирларини сақлаш, қонунчиликка асосан ҳужжатлаштирилган ахборотлар конфеденциаллигини таъминлаш;
- ахборот жараёнларида ҳамда ахборот тизимлари, технологиялари ва уларни таъминлаш воситаларини лойиҳалаш, ишлаб чиқиш ва қўллашда субъектларнинг ҳуқуқларини таъминлаш.

Ахборотни муҳофаза қилишнинг самарадорлиги унинг ўз вақтидалиги, фаоллиги, узлуксизлиги ва комплекслиги билан белгиланади. Ҳимоя тадбирларини комплекс тарзда ўтказиш ахборотни тарқаб кетиши мумкин

бўлган хавфли каналларни йўқ қилишни таъминлайди. Маълумки, биргина очиқ қолган ахборотни тарқаб кетиш канали бутун ҳимоя тизимининг самарадорлигини кескин камайтириб юборади.

Ахборотни муҳофаза қилиш соҳасидаги ишлар ҳолатининг таҳлили шуни кўрсатадики, муҳофаза қилишнинг тўлиқ шаклланган концепцияси ва тузилиши ҳосил қилинган, унинг асосини қуйидагилар ташкил этади:

- саноат асосида ишлаб чиқилган, ахборотни муҳофаза қилишнинг ўта такомиллашган техник воситалари;
- ахборотни муҳофаза қилиш масалаларини ҳал этишга ихтисослаштирилган ташкилотларнинг мавжудлиги;
- ушбу муаммога оид етарлича аниқ ифодаланган қарашлар тизими;
- етарлича амалий тажриба ва бошқалар.

Бироқ, хорижий матбуот хабарларига кўра маълумотларга нисбатан жиноий ҳаракатлар камайиб бораётгани йўқ, аксинча барқарор ўсиш тенденциясига эга бўлиб бормоқда.

Умумий йўналишга кўра ахборот хавфсизлигига таҳдидлар қуйидагиларга бўлинади:

- Ўзбекистоннинг маънавий равнақи соҳаларида, маънавий ҳаёт ва ахборот фаолиятида фуқароларнинг конституциявий ҳуқуқлари ва эркинликларига таҳдидлар;
- мамлакатнинг ахборотлаштириш, телекоммуникация ва алоқа воситалари индустриясини ривожланишига, ички бозор талабларини қондиришга, унинг маҳсулотларини жаҳон бозорига чиқишига, шунингдек маҳаллий ахборот ресурсларини йиғиш, сақлаш ва самарали фойдаланишни таъминлашга нисбатан таҳдидлар;
- Республика ҳудудида жорий этилган ҳамда яратилаётган ахборот ва телекоммуникация тизимларининг меъёрида ишлашига, ахборот ресурслари хавфсизлигига таҳдидлар.

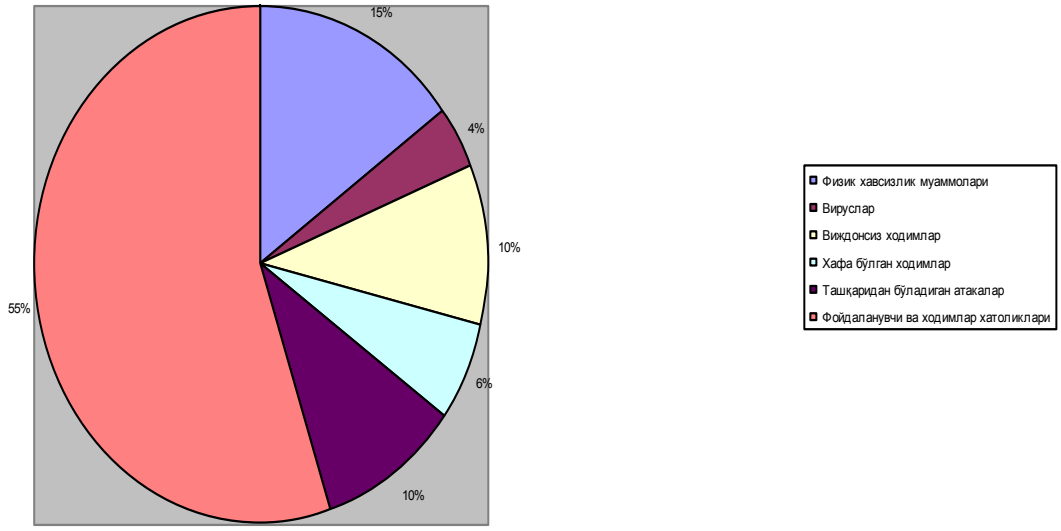
Умуман олганда компьютер мухити икки хил хавф-хатарга дучор бўлиши мумкин:

1. Маълумотларни йўқолиши ёки ўзгартирилиши.
2. Сервиснинг тўхталиши.

Бунда инсон хатоликлари хавфсизликки жиддий тахдид туғдиради ва хавфсизликни бузилиш манбаларини олдини олиш чораларини кўришни талаб қилади. Хавфсизликни бузилиш манбаларига қуйидагиларни киритиш мумкин (1-расмга қаранг) :

– Физик хавсизлик муаммолари;
– Вируслар;
– Виждонсиз ходимлар;
– Хафа бўлган ходимлар;
– Ташқаридан бўладиган атакалар;
– Фойдаланувчи ва ходимлар хатоликлари.

Статистик маълумотларга кўра бу холатни қуйидаги диаграммада тўлиқ тахлил қилиш мумкин:



1-расм. Хавфсизликни бузилиш манбалари.

Ахборот ҳисоблаш тизимларида ахборот хавфсизлигини таъминлаш нуқтаи назаридан ўзаро боғлиқ бўлган учта ташкил этувчини кўриб чиқиш мақсадга мувофиқ:

1. Ахборот;
2. Техник ва дастурий воситалар;

3. Хизмат кўрсатувчи персонал ва фойдаланувчилар.

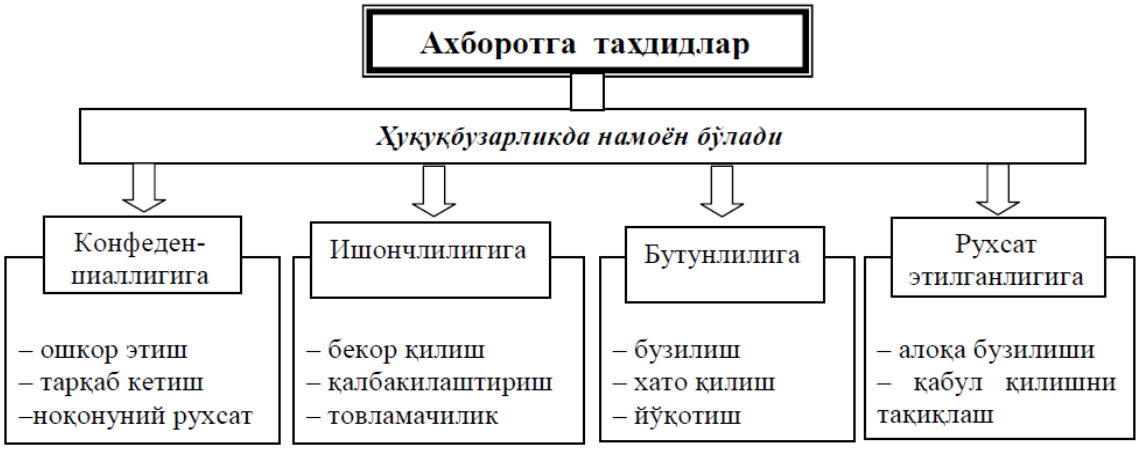
Таҳдиднинг учта кўриниши мавжуд.

1. Конфеденциалликнинг бузилишига таҳдид шуни англатадики, бунда ахборот унга рухсати бўлмаганларга маълум бўлади. Бу ҳолат конфеденциал ахборот сақланувчи тизимга ёки бир тизимдан иккинчисига узатилаётганда ноқонуний фойдалана олишликни қўлга киритиш орқали юзага келади.
2. Бутунликни бузишга таҳдид ҳисоблаш тизимида ёки бир тизимдан иккинчисига узатилаётганда ахборотни ҳар қандай қасддан ўзгартиришни ўзида мужассамлайди. (2-расмга қаранг) Жиноятчилар ахборотни қасддан ўзгартирганда, бу ахборот бутунлиги бузилганлигини билдиради. Шунингдек, дастур ва аппарат воситаларнинг тасодифий хатоси туфайли ахборотга ноқонуний ўзгаришлар киритилганда ҳам ахборот бутунлиги бузилган ҳисобланади. Ахборот бутунлиги ахборотнинг бузилмаган ҳолатда мавжудлигидир.
3. Хизматларнинг издан чиқиш таҳдиди ҳисоблаш тизими ресурсларида бошқа фойдаланувчилар ёки жиноятчилар томонидан атайлаб қилинган ҳаракатлар натижасида фойдалана олишлиликни блокировка бўлиб қолиши натижасида юзага келади. Ахборотдан фойдалана олишлилик – ахборот айланувчи, субъектларга уларни қизиқтирувчи ахборотларга ўз вақтида қаршиликларсиз киришини таъминлаб берувчи ҳамда ихтиёрий вақтда мурожаат этилганда субъектларнинг сўровларига жавоб берувчи автоматлаштирилган хизматларга тайёр бўлган тизимнинг хусусиятидир.[7]

Ахборот хавфсизлигига таҳдидларнинг тоифаланиши. Ахборот хавфсизлигига таҳдидлар даражасига кўра қуйидагича тоифаланиши мумкин:

а) шахс учун:

– ахборотларни қидириш, олиш, узатиш, ишлаб чиқиш ва тарқатиш бўйича фуқароларнинг конституциявий ҳуқуқлари ва эркинликларини бузилиши;

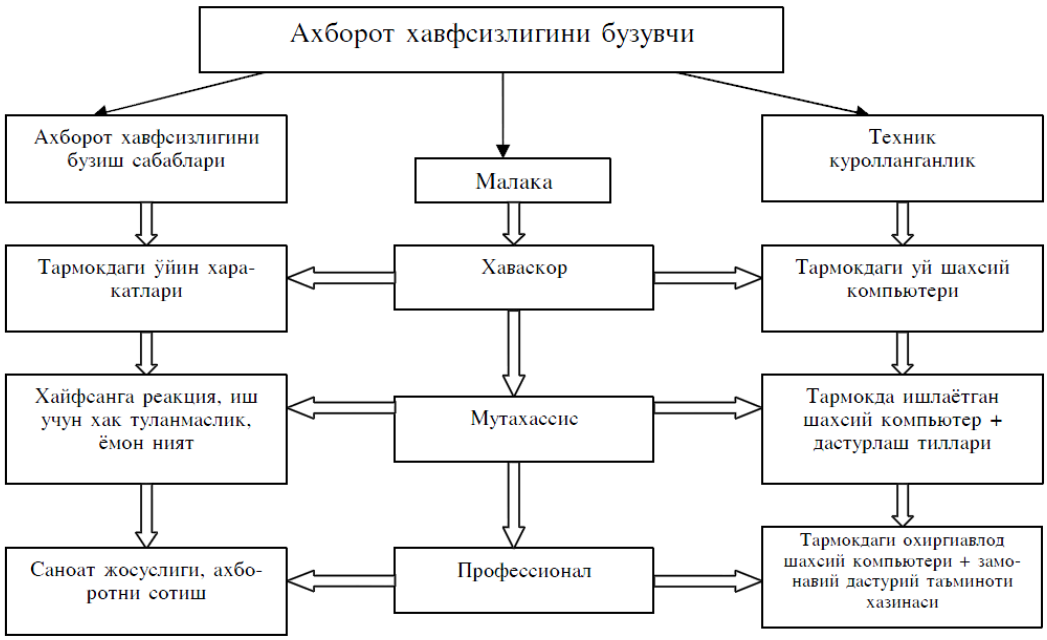


2-расм. Ахборотга таҳдидлар.

– фуқароларни шахсий ҳаёт дахлсизлиги ҳуқуқидан маҳрум қилиш;
– ғайриихтиёрий зарарли ахборотлардан фуқароларнинг ўз соғлиқларини ҳимоя қилиш ҳуқуқлари бузилиши;
– интеллектул мулк объектларига таҳдид.

б) жамият учун:

– ахборотлаштирилган жамиятни қуришга тўсиқлар;
– жамиятнинг маънавий янгиланиш, унинг маънавий бойликларини сақлаш, фидойилик ва холислик, мамлакатнинг кўп асрлик маънавий анъаналарини ривожлантириш, миллий, маданий меросни тарғиб қилиш, ахлоқ меъёрлари ҳуқуқларидан маҳрум қилиш;



3-расм. Ахборот хавсизлигини бузувчининг модел.

– замонавий телекоммуникация технологияларини тараққий этиши, мамлакат илмий ва ишлаб чиқариш потенциалини ривожлантириш ва сақлаб қолишга қаршилик қилувчи муҳитни яратиш.

Ахборот хавсизлигини бузувчининг модел мавжуд бўлиб, у қуйидаги кўринишда бўлиши мумкин. (3-расмга қаранг)

2.2. Ахборот хавфсизлигини таъминлашнинг асосий йўллари ҳамда ҳуқуқий ва ташкилий таъминоти.

Ахборотни муҳофаза қилиш тизимларидан фойдаланиш амалиёти шуни кўрсатмоқдаки, фақатгина комплекс ахборотни муҳофаза қилиш тизимлари самарали бўлиши мумкин. Унга қуйидаги чора-тадбирлар киради:

1. Қонунчилик. Ахборот ҳимояси соҳасида юридик ва жисмоний шахсларнинг, шунингдек давлатнинг ҳуқуқ ва мажбуриятларини қатъий белгиловчи қонуний актлардан фойдаланиш.
2. Маънавий-этик. Объектда қатъий белгиланган ўзини тутиш қоидаларининг бузилиши кўпчилик ходимлар томонидан кескин салбий баҳоланиши жорий этилган муҳитни ҳосил қилиш ва қўллаб қувватлаш.
3. Физик. Ҳимояланган ахборотга бегона шахсларнинг киришини тақиқловчи физик тўсиқлар яратиш.
4. Маъмурий. Тегишли махфийлик режими, кириш ва ички режимларни ташкил этиш.
5. Техник. Ахборотни муҳофаза қилиш учун электрон ва бошқа ускуналардан фойдаланиш.
6. Криптографик. Ишлов берилаётган ва узатилаётган ахборотларга ноқонуний киришни олдини олувчи шифрлаш ва кодлашни татбиқ этиш.
7. Дастурий. Фойдалана олишлиликни чегаралаш учун дастур воситаларини қўллаш.

Физик, аппаратли, дастурли ва ҳужжатли воситаларни ўз ичига олувчи барча ахборот ташувчиларга комплекс ҳолда *ҳимоя объекти* сифатида қаралади. Одатда, сўнгги вақтларда ахборотдан фойдаланиш, сақлаш, узатиш

ва қайта ишлашда турли кўринишдаги ахборот тизимларида амалга оширилмоқда.

Ахборот тизими – бу одатда матнли ёки график ахборотларни йиғиш, сақлаш, қидириш ва қайта ишлашга мўлжалланган амалий дастурий, баъзан эса аппарат-дастурий нимтизимдир.

Маълумотларнинг ахборот тизимида мавжуд бўлишининг моддий асоси бу электрон ва электрон-механик қурилмалар, шунингдек ахборот ташувчилардир. Ахборот ташувчилари сифатида қоғоз, магнит ва оптик ташувчилар, электрон схемалар фойдаланилиши мумкин. Демак, қурилма ва нимтизимларни ҳамда ахборот ташувчиларини ҳимоя қилиш зарур.

Ахборот хавфсизлигини таъминлашга йўналтирилган ҳимоя ҳаракатлари қатор катталиклар билан тавсифланиши мумкин: таҳдид характери, ҳаракат усуллари, унинг тарқалганлиги, ўраб олиш масштаби кабилар.

Таҳдид характерига кўра ҳимоя ҳаракатлари маълумотларни ошкор бўлиши, чиқиб кетиши ва ноқонуний киришдан ҳимоя қилишга йўналтирилади. Ҳаракат усулларига кўра уларни камомад ёки бошқа зарарларни: огоҳлантириш, аниқлаш, олдини олиш ва тиклаш кабиларга тақсимлаш мумкин. Ўраб олиш бўйича ҳимоя ҳаракатлари ҳудудга, бинога, иншоатга, қурилмаларга ёки уларнинг алоҳида элементларига йўналтирилган бўлиши мумкин. Ҳимоя тадбирларининг масштаби эса объект, гуруҳ ёки индивидуал ҳимоя бўйича тавсифланади.

Ахборот ҳимояси турлари икки асосий белгига кўра таснифланади:

- биринчидан, ахборот хусусийлиги, аниқроғи қўриқланадиган сирлар турига кўра;
- иккинчидан, ахборот ҳимояси учун қўлланилувчи кучлар, воситалар ва усуллар гуруҳлари бўйича.

Биринчи гуруҳга қуйидаги асосий йўналишлар киритилиши мумкин: давлат сирларини ҳимоя қилиш, давлатлараро махфий маълумотларни ҳимоя қилиш, тадбиркорлик сирларини ҳимоя қилиш, хизмат сирларини ҳимоя

қилиш, мутахассислик сирларини ҳимоя қилиш ва хусусий маълумотларни ҳимоя қилиш.

Иккинчи гуруҳга қуйидаги асосий йўналишлар киради: ахборотларни ҳуқуқий ҳимоялаш, ахборотларни ташкилий ҳимоялаш, ахборотларни муҳандислик-техник ҳимоялаш.

Ҳуқуқий ҳимоялаш – бу ҳуқуқий асосда ахборот ҳимоясини таъминловчи махсус қонунлар, бошқа меъёрий ҳужжатлар, қоидалар, жараёнлар ва тадбирлар.

Ташкилий ҳимоя – бу бажарувчиларга етказилиши мумкин бўлган ихтиёрий зарарни бартараф этувчи ёки енгиллаштирувчи, бажарувчиларнинг меъёрий-ҳуқуқий асосдаги ўзаро муомаласи ва ишлаб чиқариш фаолиятини қатъий белгилаш.

Муҳандислик-техник ҳимоя – бу фаолиятга етказилувчи зарарларга қаршилик қилувчи турли техник воситалардан фойдаланишдир.

Ахборот ҳимояси воситаларини ва усулларини таснифлаш. Ахборотни муҳофаза қилишда фойдаланилувчи асосий усуллар қуйидагилар ҳисобланади: яшириш, ранжирлаш, нотўғри маълумот бериш, бўлаклаш, суғурта қилиш, ҳисобга олиш, кодлаш ва шифрлаш.

Яшириш – ахборотни муҳофаза қилиш усули сифатида амалиётда маълумотларни ҳимоялашнинг асосий ташкилий усулларидан бири ҳисобланади, махфий маълумотларга рухсат этилган шахслар сонини чегаралайди. Яшириш ахборотларни ҳимоя қилишда жуда кенг қўлланилувчи усуллардан бири ҳисобланади.

Ранжирлаш ахборот ҳимоя усули сифатида, биринчидан, махфий маълумотларни махфийлик даражаси бўйича тақсимлайди, ва иккинчидан ҳимояланган ахборотга рухсатни чегаралайди.

Нотўғри маълумот бериш – ахборот ҳимоя усулларидан бири бўлиб, бирор объект ҳақидаги ҳақиқий маълумот ўрнига атайин ёлғон маълумот тарқатишни англатади.

Ахборотни бўлаклаш усули ахборотни бўлакларга бўлиб, унинг бирор қисми орқали тўлиқ маълумот олиб бўлмасликни англатади. Бу усул ҳарбий техника ва қуролланиш воситаларини ишлаб чиқаришда, шунингдек янги маҳсулотларни ишлаб чиқаришда кенг қўлланилади.

Суғурта қилиш – ахборотни муҳофаза қилиш усули сифатида эндигина тан олинмоқда. Унинг маъноси ахборот эгаси ҳуқуқлари ва манфаатларини ёки ахборот воситаларини анъанавий таҳдидлар ва ахборот хавфсизлиги таҳдидларидан ҳимоя қилишни билдиради.

Ушбу усул тижорат сирларини сақлашда кўпроқ қўлланилиши эҳтимоли мавжуд. Ахборотни суғурта қилишда у дастлаб, аудиторлик текширувидан ўтиши ва хулосага эга бўлиши талаб этилади.

Ахборотларни маънавий-маърифий ҳимоялаш усули ахборотни муҳофаза қилишда жуда муҳим рол ўйнайди. Айнан инсон, у корхона ёки ташкилот ходими, махфий маълумотлардан воқиф бўлиб, ўз хотирасида кўплаб маълумотларни жамлайди ва баъзи ҳолларда ахборот чиқиб кетиши манбаига айланиши мумкин ҳамда унинг айби билан ўзгалар ушбу ахборотга ноқонуний эга бўладилар. Ахборотларни маънавий-маърифий ҳимоялаш усули қуйидагиларни назарда тутади:

– ходимни тарбиялаш, у билан маълум сифатларни, қарашларни шакллантиришга йўналтирилган махсус ишларни олиб бориш (ватанпарварлик, ахборотни муҳофаза қилиш унинг шахсан ўзи учун ҳам қандай аҳамият касб этишини тушунтириш);
– ходимни ахборотни муҳофаза қилиш қоидалари ва усулларига ўргатиш, конфеденциал ахборот ташувчилар билан амалий ишлаш кўникмаларини шакллантириш.

Ҳисобга олиш ахборотни муҳофаза қилишнинг муҳим усулларидан бири бўлиб, конфеденциал маълумотлар ташувчиларнинг ҳамда ундан фойдаланувчиларнинг ихтиёрий вақтда қаерда жойлашганлиги ҳақида маълумот олиш имконини беради. Ушбу усулсиз ҳимоя муаммосини ҳал этиш жуда қийин. Сир сақланувчи ахборотларни ҳисобга олиш тамойиллари:

– ҳимояланувчи ахборотларни ташувчиларнинг барчасини рўйхатга олиш мажбурийлиги;
– муайян ахборот ташувчини рўйхатга олиш бир марта бўлишлигини (такрорланмаслигини) таъминлаш;
– рўйхатда конфеденциал маълумот ташувчининг айни вақтда қайси манзилдалигини кўрсатиш;
– ҳар бир ҳимояланган ахборот ташувчининг сақланишига ягона жавобгарлик ва ҳисобда ушбу ахборотни ишлатган фойдаланувчи ҳақида маълумотни акс эттириш.

Кодлаш – ҳимояланувчи ахборотни рақибдан яшириш мақсадида, ахборотни канал орқали узатиш жараёнида ўзгалар томонидан тутиб олиниши хавфи мавжуд бўлганда, уни кодлаш усули ёрдамида очиқ матнни шартли ахборотга айлантириш усулидир. Кодлаш учун одатда белгилар тўплами (белгилар, рақамлар ва бошқалар), шунингдек ахборотни тушунарсиз белгилар тўплами кўринишига айлантириш имконини берувчи маълум қоидалар тизими фойдаланилади. Бу ахборотни ўқиш учун эса уни яна ўз холига келтириш, яъни кодни очиш (калит) керак бўлади. Ахборотни кодлаш техник воситалар ёрдамида ёки қўлда амалга оширилиши мумкин.

Шифрлаш – ахборотни муҳофаза қилиш усули бўлиб, кўпинча ахборотларни радиоқурилмалар воситасида узатишда, рақиб томонидан тутиб олиш хавфи бўлганда қўлланилади. Ахборотни шифрлаш, уни ўзгалар томонидан тутиб олинганда ҳам калитсиз маъносини тушуниб бўлмайдиган ҳолатга ўтказишни англатади.

Ахборотни муҳофаза қилиш воситалари – бу ахборотни муҳофаза қилиш масалаларини ҳал этиш учун фойдаланилувчи муҳандислик-техник, электр, электрон, оптик ва бошқа қурилма воситалар тўпламидир.

Ахборотни муҳофаза қилишнинг кадр ва ресурс таъминоти. Давлат сирларини ташкил этувчи ахборотни муҳофаза қилишни ташкил этувчи кадрлар тайёрлаш тизимига қуйидагилар киради:

1. Ташкилот ва бўлинма раҳбарлари.

2. Ахборотни муҳофаза қилиш бўйича махсус комиссиялар.
3. Ягона хавфсизлик хизмати таркибига кирувчи ихтисослашган бўлинмалар.

Меъёрий-ҳуқуқий ҳужжат тушунчаси. Маълумки, ҳуқуқ – бу ҳукумат томонидан турмушнинг маълум бир соҳаларига, давлат органлари, ташкилотлари ёки аҳолига нисбатан ўрнатилган ёки санкцияланган умуммажбурий қоидалар ва меъёрлар тўпламидир.

Ўзбекистон Республикасининг 2012 йил 24 декабрдаги «*Норматив-ҳуқуқий ҳужжатлар тўғрисида* (янги таҳрири)»ги қонунининг [31] 3-моддасига асосан «Норматив-ҳуқуқий ҳужжат ушбу Қонунга мувофиқ қабул қилинган, умуммажбурий давлат кўрсатмалари сифатида ҳуқуқий нормаларни белгилашга, ўзгартиришга ёки бекор қилишга қаратилган расмий ҳужжатдир».

Меъёрий ҳуқуқий ҳужжат – бу ҳуқуқ ижодкорлиги ҳужжати бўлиб, маълум бир тартибда, қатъий белгиланган субъектлар томонидан қабул қилинади ва ҳуқуқ меъёрига эга бўлади.

Меъёрий ҳуқуқий ҳужжат ҳуқуқнинг асосий манбаи ҳисобланади. Меъёрий ҳуқуқий ҳужжат (бошқа ҳуқуқ манбаларига нисбатан) кафолат доирасида фақат масъул давлат органлари томонидан қабул қилинади ҳамда маълум бир кўринишга, ҳужжат шаклига эга бўлади.

Меъёрий ҳуқуқий ҳужжатлар мамлакат бўйича амал қилади ва ягона тизимни ҳосил қилади.

Меъёрий ҳуқуқий ҳужжатлар белгилари:

– меъёрий характер
– ҳуқуқий акт
– ҳуқуқ ижодкорлиги натижаси ҳисобланади
– умуммажбурийлик
– расмий ҳужжат кўринишида тузилади
– ҳуқуқ меъёрларини гуруҳлашда маълум бир тартибга риоя қилинади.

Меъёрий ҳуқуқий ҳужжатлар турлари. Ўзбекистон Республикасининг 2012 йил 24 декабрдаги «*Норматив-ҳуқуқий ҳужжатлар тўғрисида*»ги қонунининг 5-моддаси меъёрий ҳуқуқий ҳужжатларнинг турларини аниқлайди.

Қуйидагилар меъёрий ҳуқуқий ҳужжат ҳисобланади:

– Ўзбекистон Республикаси Конституцияси;

– Ўзбекистон Республикаси қонунлари;

– Ўзбекистон Республикаси Олий Мажлиси палаталари қарорлари;

– Ўзбекистон Республикаси Президенти фармонлари;

– Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари;

– Вазирликлар, давлат комитетлари ва ташкилотлари ҳужжатлари;

– Давлат ҳокимиятининг жойлардаги органлари қарорлари.

Меъёрий ҳуқуқий ҳужжатлар қонунчилик ҳужжатлари ҳисобланади ва Ўзбекистон Республикаси қонунчилигини ташкил этади. [8]

Ўзбекистон Республикаси Конституцияси, Ўзбекистон Республикаси Қонунлари, Ўзбекистон Республикаси Олий Мажлиси палаталари қарорлари қонунчилик ҳужжатлари ҳисобланади. Ўзбекистон Республикаси Президенти Фармонлари, Ўзбекистон Республикаси Вазирлар Маҳкамаси қарорлари, Вазирликлар, давлат комитетлари ва ташкилотлари актлари, давлат ҳокимиятининг жойлардаги органлари қарорлари қонуности ҳужжатлари ҳисобланади (ушбу қонуннинг 6-моддаси).

Ахборот хавфсизлигини таъминлашда меъёрий-ҳуқуқий бошқарувнинг зарурлиги. Ҳуқуқий база ахборотга эгалик ҳуқуқига ва уни муҳофаза қилишга оид вазифаларни ечиш имконини бериши зарур.

Ҳимояланаётган ахборотга таҳдидни аниқлаши ва уни ҳимоялаш тартибини белгилаши керак. Ҳуқуқий давлатда барча ташкилот ва муассасалар, раҳбар шахслар ва фуқаролар фаолияти амалдаги қонунлар доирасида ташкил этилиши лозим.

Ахборотни муҳофаза қилиш соҳасига оид меъёрий-ҳуқуқий ҳужжатларда:

– ахборотни муҳофаза қилиш, унинг махфийлиги ва ҳимоя учун ўрнатилган қоидалар соҳасида турли субъектларнинг ҳуқуқлари ифодаланиши;

– ҳимояланаётган ахборотга ноқонуний таҳдид қилиш ёки унинг эгасига зарар етказувчи оқибатларни келтириб чиқариши мумкин бўлган ҳаракатлар учун жиноий, маъмурий, моддий ва маънавий жавобгарлик белгиланиши керак.

Ўзбекистон Республикасида ахборот хавфсизлиги ва маълумотларни ҳимоялаш бўйича меъёрий ҳуқуқий ҳужжатлар. Ахборотни ҳуқуқий ҳимоялаш захира сифатида давлат ва халқаро миқёсда танолинган ҳамда халқаро шартнома, конвенция ва декларацияларда аниқланади. Давлат миқёсида ахборотни ҳуқуқий ҳимоялаш давлат ва ташкилот ҳужжатлари орқали назорат қилинади. (4-расмга қаранг)

Бизнинг мамлакатимизда бундай меъёрий ҳужжатларга Конституция, Ўзбекистон Республикаси Қонунлари, Ҳукумат қарорлари, фуқаролик, маъмурий ва жиноят кодексларида келтирилган тегишли моддалар киради. Ташкилот меъёрий ҳужжатларига эса ушбу ташкилот доирасида амал қилинувчи буйруқ, йўриқнома, кўрсатма кабилар киради.

4-расм.Ахборотни ҳуқуқий ҳимоялаш модели.

Ахборот хавфсизлиги ва маълумотларни ҳимоялаш соҳасида меъёрий ҳуқуқий ҳужжатларни қабул қилиш ва амал қилишда тизимли кетма-кетлик хавфсизликни таъминлаш муаммоси комплекс характерга эга. Уни ҳал қилиш учун ҳуқуқий ҳамда ташкилий чоралар ва дастурий-техник таъминотни (идентификация ва аутентификация; рухсатни бошқариш; протоколлаштириш ва аудит; криптография) биргаликда кўриш талаб этилади (мисол учун, корхона бошқаруви миқёсида унинг компьютер ахборот тармоғида ахборот хавфсизлигини таъминлаш учун хавфсизлик сиёсатини ишлаб чиқиш ҳамда керакли ресурслар талаб этилади).[9]

2.3. Ахборотни ҳимоялашнинг криптографик усуллари.

Криптология атамаси грекча «махфий» ва «суз» бирикмасидан хосил булган. Минг йилликлар давомида криптография харбий ва дипломатия алокасини химоялашда фойдаланиб келинган. Аммо ахборот асрининг бошланиши билан криптология хусусий секторда хам фойдаланиш учун жуда зарур булиб колди. хозирги кунда пинхона ахборотнинг(масалан,юридик хужжатлар, молиявий, кредит ставкалари хакидаги ахборотлар, касаллик тарихи ва шунга ухшаш) талай кисми компьтерлар аро одатдаги алока линиялари оркали узатилмокда. Жамият учун бундай ахборотнинг пинхоналиги ва асл холда сакланиши заруратга айланган. Криптологияда кенг микёсда очик тадкикотлар бошланганига бор йуги 20 йилдан ошди. [10]

Криптология тарихини икки даврга ажратиш мумкин: илмий криптологиягача булган давр, илмий криптология даври. Илмий криптологиягача булган давр XX асрнинг биринчи ярмигача давом этган. Илмий криптология даври 1949 йилдан бошланган булиб, унда криптотизимлар кадимдаги каби факат симметрик(махфий калитли) тарзда мавжуд булган XX асрнинг учинчи чораги ва ундан кейинги-криптотизимлар симметрик ва носимметрик(ошкора хам махфий калитларга асосланган) тарзда мавжуд булган давр характерлидир. [11]

Илмий асослари шакллангунга кадар амалиётда кулланилиб келган криптология буйича Оврупа фани тарихида Плутарх, Аристотел(милоддан аввалги ИВ аср), Юлий Цезар(милоддан олдинги 100 - 44 йй.), Р.Бекон(1214-1294), Леон Баттиста Алберти (1404 - 1472 йй.), Ёганн Тритемий(1462-1516), Джиролано Кардоно, кардинал Ришеле, Джованни Батиста Порт, Блез де Вижинар, Франсуа Виет (1540 - 1603 йй.), Френсис Бекон(1562-1626), Карл Фридрих Гаусс (1777 - 1855 йй.), Огюст Керкхофф (1835 - 1903 йй.), Жилбер Вернам (Г.С. Вернам)ларга алохида урин берилган.

Бундан 4000 йил аввалги даврга тегишли энг кадимий шифрматн Месопатамия казилмаларида топилган. Унда лойдан ишланган тахтачада уймакор ёзувда тижорат сири - кулолчилик буюмларини глазурлаш рецепти ёзилган. Кадимий Мисрда шифрланган диний матнлар ва тиббий рецептлар хам мавжуд булган.

Эрамизгача булган IX аср уртасида Плутарх шифр курилмаси- скитал мавжуд булиб, у урин алмаштириш амали асосида матнларни шифрлаб берган. Сузлар скиталга -цилиндрга уралган тор лентага уни ташкил этувчиси буйлаб ёзилган. Шу лента ёйилгач унда харфлар урни алмашган шифрланган матн хосил булган. Номаълум параметр-калит сифатида цилиндр диаметри хисобланган. Бундай матнни шифрини бузиб очиш усули Аристотел томонидан таклиф этилган: лента конусга (бирор кундаланг кесимга устма-уст) уралгач, (урамлар конус уки буйлаб бироз силжитилгач) укиладиган тушунарли суз пайдо булган конус кундаланг кесимининг диаметри калит хисобланган. Шунга кура бизгача етиб келган маълумотларга кура криптотахлилнинг асосчиси -Аристотел деб хисобласак хато булмайди.

Криптотизимда ахборотни шифрлаш ва унинг шифрини очишда ишлатиладиган калитларнинг бир-бирига муносабатига кура улар бир калитли ва икки калитли тизимларга фаркланадилар. Одатда барча криптотизимларда шифрлаш алгоритми шифр очиш алгоритми билан айнан ё бироз фаркли булади. Криптотизимнинг таъбир жоиз булса "кулфнинг" бардошлилиги алгоритм маълум булган холда факат калитнинг химоя

хоссаларига, асосан калит ахборот микдори (битлар сони)нинг катталигига боглик деб кабул килинган.[12]

Шифрлаш калити шифр очиш калити билан айнан ё улардан бири асосида иккинчиси осон топилиши мумкин булган криптотизимлар симметрик(синонимлари: махфий калитли, бир калитли) криптотизим деб аталади.

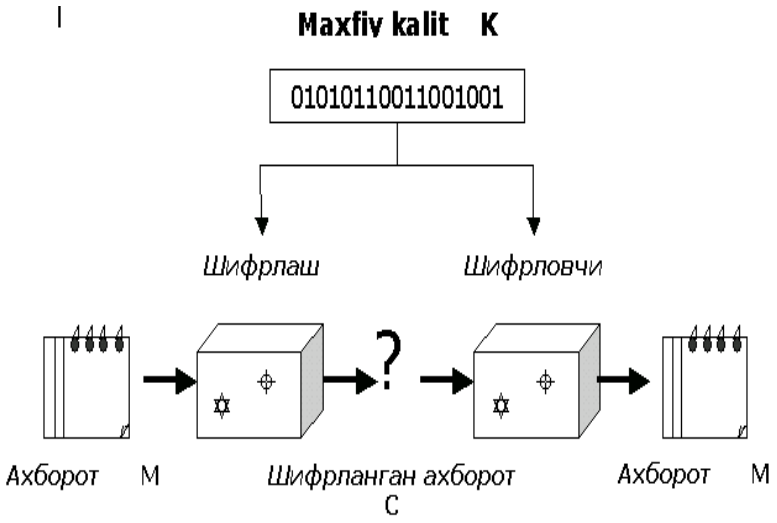
Бундай криптотизимда калит алоканинг иккала томони учун бир хил махфий ва икковларидан бошка хеч кимга ошкор булмаслиги шарт. Бундай тизимнинг хавфсизлиги асосан ягона махфий калитнинг химоя хоссаларига боглик.

Симметрик криптотизимлар узок утмишга эга булсада, улар асосида олинган алгоритмлар компьтерлардаги ахборотларни химоялаш зарурати туфайли баъзи давлатларда стандарт мАкомига кутарилдилар. Масалан, АКШда маълумотларни шифрлаш стандарти сифатида 56 битли калит билан ишлайдиган DES(Data Encryption Standart) алгоритми 1977 йилда кабул килинган. Россия (собик иттифок)да унга ухшаш стандарт (ГОСТ 28147-89) сифатида 128 битли калит билан ишлайдиган алгоритм 1989 йилда тасдикланган. Булар дастлабки ахборотни 64 битли блокларга булиб алохида ёки бир-бирига боглик холда шифрлашга асосланганлар. Алгоритмларнинг математикавий асосида ахборот битларини аралаштириш, урнига куйиш, урин алмаштириш ва модул буйича кушиш амаллари ётади. Унда кириш ва чикишдаги матнларнинг ахборот микдорлари деярли бир хил булади. [13]

Симметрик криптотизимни ишлашини бу кунги давримизнинг Зухра ва Тохирлари орасида электрон мактублар алмашиш мисолида куриб чикамиз. Пинхона алокага нисбатан тажовузкор шахсни Қора ботир деб атаймиз.

Фараз килайликки, Тохир Зухрага пинхона мактуб йулламокчи. Улар орасида алока бошлангунча узларининг ягона махфий калит нусхаларини бир-бирларига бериб, мактубни факат шифрланган шаклда юборишга келишиб куйган эдилар. Тохир Зухрага М мактубини ёзиб, уни К калити билан шифрлайди. Натижада М мактуби шифрланган матн С га айланади.

Сунгра Тохир шифрланган мактубни электрон почта оркали Зухрага жунатади. Зухра шифрланган мактуб С ни кабул килиб олгач уни узидаги махфий калит билан унинг шифрини очиб Тохир ёзган М мактубига айлантириб уни укийди. (5-расмга қаранг)



5-расм. Симметрик криптотизимни ишлаш схемаси.

Алока канали химояланмаган булгани учун бу мактуб Қора ботирнинг кулига тушиши хам мумкин. Лекин, Қора ботирда Зухра ва Тохирларнинг махфий калити булмагани учун у хатнинг мазмунини билаолмайди ва хатни узгартириб куяолмайди. Қора ботирнинг кулидан мактубни йук килиб юборишгина келади холос. Қора ботир мактуб мазмунини билмай туриб Тохир номидан шифрланмаган ёки бирор калит билан шифрланган мактуб жунаца хам, бунинг калбаки эканлиги Зухрага дархол ошкор булади. Чунки, хат шифрланмай келса, бу пинхона хат алмашиш хакидаги уларнинг келишувига зид булиб чикади. Агар хат Қора ботирдаги бошка калит билан шифрланиб келса, уни Зухра узидаги ва Тохирдаги махфий калит нусхаси билан оча олмайди ва бу билан хатнинг Тохирдан эмаслигини билиб олади.

Шифрлаш алгоритми одатда барча учун ошкора булади. Бундай тизимнинг

Хавфсизлиги асосан махфий калитнинг химоя хоссаларига боглик.

Симметрик криптотизимдан фойдаланиб электрон ёзишмалар бошлаш учун аввало махфий калитни ёки паролни икки алока иштирокчисидан бири

иккинчисига махфий холда етказиши керак. Махфий калитни етказиш учун махфий алока канали(шахсан учрашиш, химояланган алока канали ва ш.у.) керак. Шундай килиб ёпик давра хосил булади: махфий калитни топшириш учун махфий канал керак, махфий канални хосил килиш учун махфий калит керак. Махфий калит тез-тез узгартириб турилса(аслида, харбир ёзишмага алохида махфий калит ишлатилганда энг юкори махфийликка эришилади) бу муаммо доимо кундаланг булаверади. [14]

Шифрлаш ва шифр очиш калитлари узаро функционал богланган булиб улардан бири асосида иккинчиси амалий жихатдан (мавжуд хисоблаш воситалари тараккиёти даражасида) хисоблаб топилиши мумкин булмаган ва улардан бири факат битта алока иштирокчисига маълум булиб бошкалардан махфий тутиладиган, иккинчиси эса алока иштирокчиларининг хаммасига ошкор булган криптотизим носимметрик(синонимлари: ошкора калитли, икки калитли) криптотизим деб аталади.

Носимметрик криптотизимлар асослари симметрик тизимларда ечилмай колган калит таркатиш ва ракамли имзо муаммоларининг ечимини излаш йулларида Массачусец технология институтида У.Диффи (W.Diffie) ва унинг илмий рахбари М.Хеллман (M.E.Hellman) томонидан 1975 йилда таклиф этилган. 1977 йили шу тамойил асосида уша институтда Р.Ривест, А.Шамир,Л.Адлман(R.Rivest,A.Shamir, L.Adleman) томонидан RSA алгоритми ишлаб чикилди. Кейинчалик эллиптик ва ш.у. бир томонлама осон хисобланадиган функциялар асосига курилган бошка алгоритмлар (El Gamal ва бошкалар алгоритмлари) яратилди.

Носимметрик криптотизимлар симметрик криптотизимларга нисбатан унлаб марта купрок ахборот микдорига эга (512, 1024,2048,4096 битли) калитлардан фойдаланади ва шунга кура юзлаб марта секинрок ишлайди. Носимметрик криптотизимларнинг математик асосида бир томонлама осон хисобланадиган функциялар (даражага ошириш, эллиптик функция, рекурсия ва ш.у.) ётади.

У.Диффи ва М.Хеллман таклиф этган химояланмаган очик алока канали оркали калит таркатиш усулининг мохиятини куйидаги мисолда курамиз.

Фараз килайликки Тохир ва Зухра симметрик криптотизимдан фойдаланиш учун узаро махфий калит белгилаб олмокчилар. Бунинг учун улардан бири бирор катта туб сон М ни ва 1 билан М-1 орасидан бутун сон г ни танлаб химояланмаган алока канали(масалан, телефон) оркали иккинчиларига билдириб келишиб оладилар. Сунгра икковлари хам 1 билан М-1 орасидан алохида ихтиёрий бутун сонларни танлаб уни узларининг шахсий калитлари деб белгилайдилар ва уни хеч кимсага(бир-бирларига хам) билдирмайдилар. Фараз килайликки, Тохирнинг шахсий махфий калити **о,** Зухранинг шахсий махфий калити эса **к** булсин. Бу шахсий махфий калитлар узаро махфий(икковларидан бошка хеч ким билмайдиган) калитни ва узларининг шахсий ошкора калитларини хосил килишда катнашадиган калитлардир. Тохир уз шахсий ошкора калити Эота ни, Зухра уз шахсий ошкора калити Экум ни хосил килиш учун г сонини М модули буйича уз шахсий махфий калитларига тенг булган даражага оширишлари кифоя. Улар уз шахсий ошкора калитларини бир-бирларига ва бошкаларга хам очик алока канали оркали маълум килганларидан сунг узаро махфий калитни хисоблаб топишлари мумкин булади.

Тохир билан Зухранинг узаро махфий калити к бирларининг ошкора калитини иккинчиларининг махфий калитига тенг даражага М модули буйича оширилганига тенг. Энди улар бирор симметрик криптотизимдан фойдал аниб мактуб алмашишда факат икковларигагина маълум булган калит **К** билан уз мактубларини шифрлайдилар ва шу калит билан шифрланган мактуб шифрини очиб укийдилар.

Шахсий ошкора калитлар, М модули ва г асос Қора ботирга хам маълум. Лекин, у шахсий махфий калитлардан бехабар булгани учун Тохир ва Зухраларнинг узаро махфий калитларини билаолмайди. Чунки, бунинг учун ё Тохирнинг ё Зухранинг шахсий махфий калитини билиши зарур. Уни билиш учун г асосда М модули буйича ошкора калитнинг дискрет логарифмини

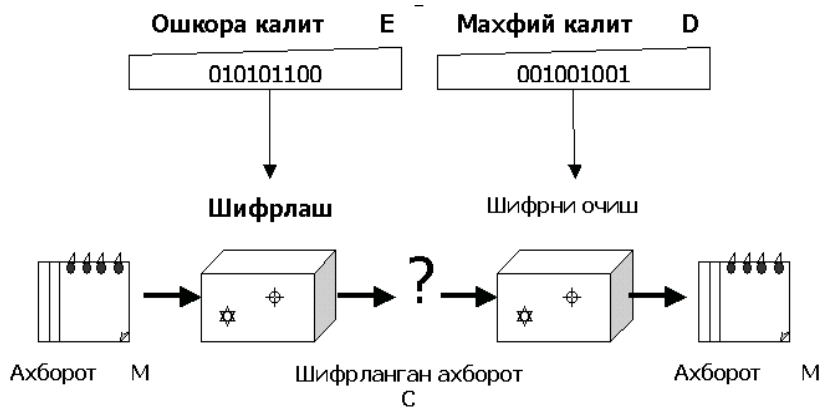
хисоблаб топиш зарур. М сони 2 нинг 512 чи даражасига тенг сонга якин сон булса ва у «яхши туб сон» (яъни, ундан битта кам сонни ярмиси хам туб сон) булса дискрет логарифмни хисоблашда ишлатиладиган купайтув амаллари нинг (М модули буйича) сони 2 нинг 256 чи даражасига якин булади. Бунча амалларни бажариш учун энг зур замонавий суперкомпьютер хам минглаб йиллар давомида тинимсиз ишлаши лозим булади.

Юкорида куриб утилган шахсий ошкора ва шахсий махфий калитлар бир томонлама хисобланадиган функция асосига курилган булиб, улар мактубларни бевосита шифрлаш ва шифрини очиш муаммосини эмас, балки мактуб(умуман, харкандай ахборот)ларни симметрик криптотизимларда шифрлашда ва шифр очишда фойдаланиладиган узаро махфий калитларни ошкора таксимлаш муаммосини ечиб беради.

Яширин йулли бир томонлама функциялардан фойдаланилганда алмашиладиган ахборотларни узатиш ва ракамли имзо асосида аутентификация муаммосини ечиш хам осон хал булади. Бундай кулай функция турини биринчи булиб RSA алгоритмининг муаллифлари таклиф этишган. (6-расмга қаранг) Унда ошкора модул М икки туб соннинг купайтмаси булиб, купайтувчилар сир тутилади. Купайтувчилардан битта кам сонлар купайтмаси иккинчи (махфий) модул булиб, у хам сир тутилади. Махфий модулга нисбатан узаро тескари икки сондан бири шахсий ошкора калит, иккинчиси шахсий махфий калит деб кабул килинади. Шу шахсга йулланиладиган ахборот блоклари унинг ошкора калитида шифрлаб (М модули буйича ошкора калитга тенг даражага ошириб) жунатилади. Кабул килиб олинган ахборот блоклари шифри шу шахснинг шахсий махфий калитида очилади(М модули буйича махфий калитга тенг даражага ошириб).

Фараз килайликки, Тохир Зухрага носимметрик криптотизимдан фойдаланиб пинхона мактуб йулламокчи. Улар орасида алока бошлангунча Зухра уз ошкора калити нусхасини Тохирка ва бошкаларга маълум килган. Улар бир-бирларига мактубни факат шифрланган шаклда юборишга келишиб куйганлар. Тохир Зухрага М мактубини ёзиб, уни Зухранинг ошкора калити

билан шифрлайди. Натижада М мактуби шифрланган матн С га айланади. Сунгра Тохир шифрланган мактубни электрон почта оркали Зухрага жунатади. Хат Зухранинг ошкора калити билан шифрланган булгани учун уни Зухра уз махфий калити билан очиб бемалол укий олади. Яъни, шифрланган матн С Зухранинг махфий калити билан дастлабки матн М га айлантирилади.



6-расм. Яширин йулли бир томонлама функцияли шифрлаш.

Алока канали химояланмаган булгани учун бу мактуб Хамиднинг кулига хам тушиши мумкин. Лекин Қора ботирда Зухранинг махфий калити булмагани учун у хатнинг мазмунини билаолмайди ва хатни узгартириб куя олмайди. Қора ботирнинг кулидан мактубни йук килиб юбориш ва, ёки Зухрага унинг ошкора калитидан фойдаланиб Тохир номидан шифрланган янги калбаки мактуб йуллаш келади. Қора ботир мактуб мазмунини билмай туриб Тохир номидан шифрланган мактуб жунатса, бунинг калбаки эканлиги Зухрага дархол ошкор булмаслиги мумкин. Чунки, хат Зухранинг ошкора калити билан шифрланган булгани учун уни Зухра уз махфий калити билан очиб укийди. Бу хатнинг чиндан хам Тохирдан эканига ишонч хосил килиш учун буерда аутентификация муаммосини(Тохирнинг ракамли имзосини текшириш оркали) хал килиш лозим булади. Бу муаммони ечишда ракамли имзо куйиш учун шахсий махфий калитдан, имзони текшириш учун шахснинг ошкора калитидан фойдаланилади. Бу сал кейинрок курилган.

Тарихан криптотизимлар юкорида келтирилган ахборот хавфсизлиги муаммоларидан асосан биттасини - пинхоналик муаммосини ечишга

каратилган эдилар. Колган муаммоларнинг кун тартибига куйилиши симметрик-калитли тизимлар билан бир каторда носимметрик-калитли криптотизимларнинг яратилишига сабаб булди.

Фойдаланувчилар сони кам булганда симметрик криптотизимдан фойдаланиш кулай. Лекин фойдаланувчилар сони куп булиб улар бутун дунё буйлаб таркалган булишса калит таксимлаш катта муаммога айланади. Хар бир киши бундай тармокда харбир бошка киши билан ахборот алмашиши учун алохида махфий калитга эга булиши керак. Масалан, 1000 фойдаланувчига эга булган тизим тахминан 500,000 калит булишини ва шунча алмашув жараёнини амалга оширишни ва шунча калитни махфий саклашни талаб этади.

Носимметрик-калитли криптотизимларда тармокдан фойдаланувчининг хар бири узининг ягона махфий калитига эга. Узининг ва бошкаларнинг ошкора калитларини сир саклашига хожат йук. Масалан, 1000 фойдаланувчиси булган тармокда харбир фойдаланувчи биттадан ошкора ва биттадан махфий калитга эга булиши кифоя. Яни бунда, симметрик калитли тизимдаги 500,000 калит урнига хаммаси булиб 2000 калит булиши етарли.[15]

Носимметрик криптотизимлар ахборот хавфсизлигининг барча муаммоларини ечиб беришга кодир. Куйида носимметрик криптотизимдан симметрик криптотизим калитини шифрлаб узатишда, симметрик криптотизимдан эса ахборотни шифрлаб алмашишда фойдаланиш амалиёти баён этилади. (7-расмга қаранг)

Хар бир алока томони бажарадиган амалларни бу кунги давримизнинг Зухра ва Тохирлари орасидаги электрон мактублар алмашиш ва уларга нисбатан тажовузкор шахс Қора ботир тимсолида намойиш киламиз. Тохирнинг махфий (шахсий) калитини Dтохир унинг ошкора калитини Етохир оркали белгилаймиз.

Фараз килайликки, Зухра Тохирка пинхона мактуб йулламокчи. Улар орасида алока бошлангунча Тохир узининг ошкора калитини Зухрага ва

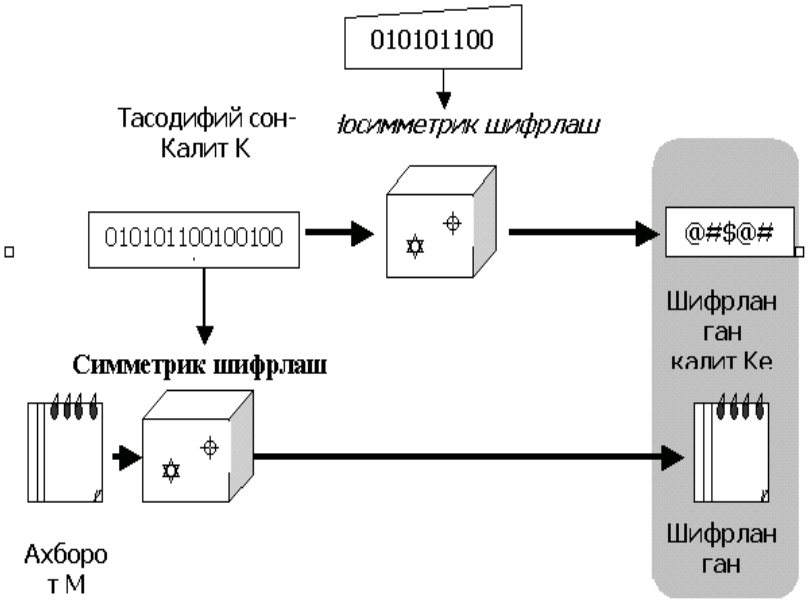
бошкаларга хам бериб куйган эди. Тохирка М мактубини шифрлаб жунатиш учун Зухра аввало тасодифий бирор сон танлаб, уни бир марта ишлатиладиган махфий сеанс калити К сифатида кабул килади ва у билан мактубни симметрик криптотизим асосида шифрлайди.

Сунгра Етохир ошкора калитни олиб у билан носимметрик криптотизим асосида махфий сеанс калити К ни шифрлайди ва натижада М мактуби шифрланган матн С га, махфий сеанс калити К эса шифрланган сеанс калити Ке га айланади. Бу жараён куйидагича функциявий богланиш тарзида ифодаланиши мумкин:

С к К(М)

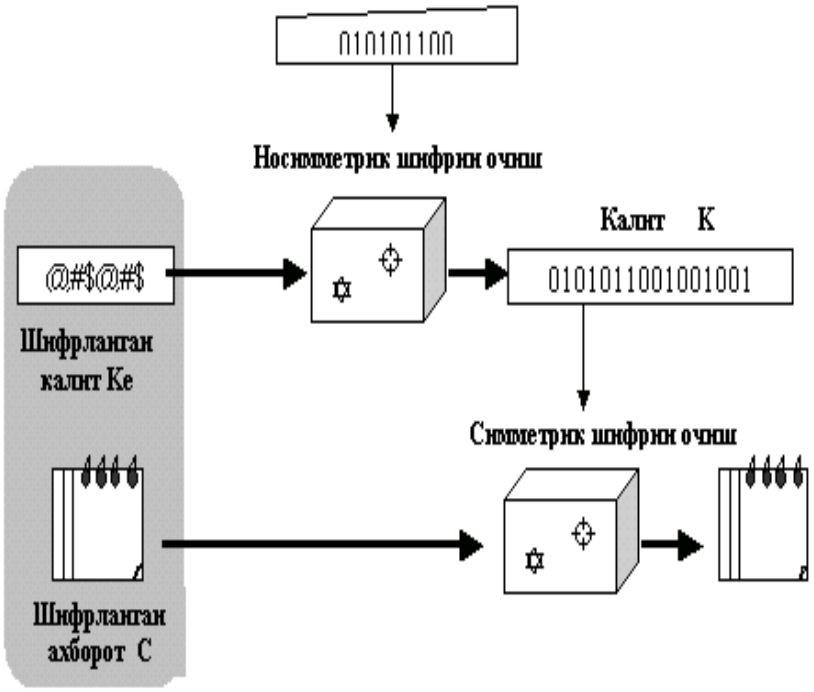
Ке к Етохир(К)

Сунгра Зухра С ва Ке дан таркиб топган жунатмани Тохирка йуллайди.



7-расм. Носимметрик криптотизимларда шифрлаш

Тохир С ва Ке дан таркиб топган жунатмани кабул килиб олгач, шифрланган сеанс калити Ке шифрини уз махфий калити Dтохир ёрдамида очиб махфий сеанс калити К ни топади, сунгра К калити билан шифрланган С хатни М мактубига айлантиради:



8-расм. Носимметрик ва симметрик шифрларни очиш схемаси.

Зухра ва Тохирнинг ишончи комилки, улардан бошка хеч ким М мактубини курмаган. Чунки, S мактуби ва Ке калити бегона (масалан, Қора ботир)нинг кулига тушиб колган такдирда хам у шифрланган хатнинг мазмунини мутлако тушунмаган булур эди, чунки S мактубини асл М мактубига айлантириш учун зарур булган махфий сеанс калити К ни Ке асосида топиш мумкин булган махфий калит Dтохир факат Тохирдагина бор. Бу мактубни хатто уни ёзган Зухра хам агар дастлабки М мактубини ёкиб юбориб ёдида саклаб колмаган булса кайтадан М мактубини тиклай ололмайди. (8-расмга қаранг).

Зухра Тохирка йуллаган мактубни Қора ботир кулга туширган такдирда уни англай олмасада Қора ботир Тохирка Зухра номидан калбаки хат жунатиши мумкин. Чунки Тохирнинг ошкора калити хаммага маълум килинган. Бундай холларнинг олдини олиш учун Зухра уз хатига ракамли имзо куйиши лозим булади. Бу холда аутентификация муаммосини хал килиш лозим булади. Куйида шу хакда гап боради.

Ракамли имзо анъанавий кулда куйиладиган имзонинг электрон эквивалентидир. Когозга кул куйишда шахсий имзони калбаки имзо билан

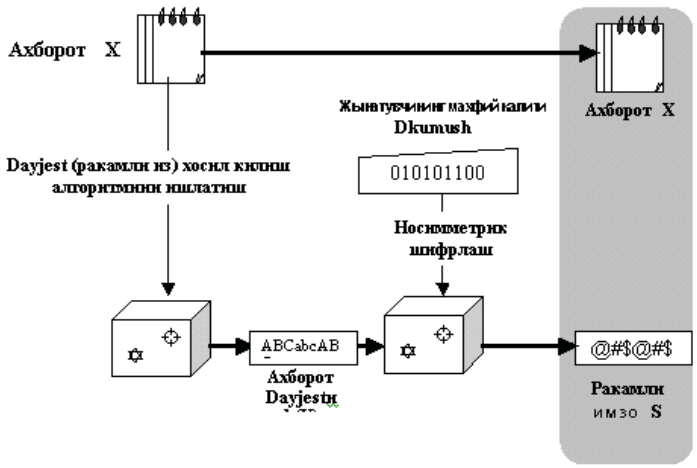
алмаштириш анча мушкул. Чунки хар ким узининг кайтариш кийин булган имзосига эга. Лекин ракамли имзо барча хужжат учун бир хил куйиладиган булса уни осон кучириб олиниб бошка хужжатга куйилиши мумкин. Бу ерда хар бир ракамли имзони факат битта хужжат билан боглаш муаммоси кундаланг булади. Бунинг учун очик калитли криптотизим жуда кул келади. Бунда аввалги мактуб жунатишдагидан фаркли уларок шифрлаш учун махфий калит, шифрни очиш учун эса ошкора калит ишлатилади.

Зухра Тохирка мактуб йулламокчи булса аввалдан уз ошкора калити ЕЗухрани эълон килиб куйган булиши лозим. Шунда жунатилаётган мактуб билан бирга уз махфий калити ва мактуб М асосида шакллантирилган Ракамли имзосини хам жунатади.

Шунда Тохир шифрланган S хатнинг Зухрадан келганига ишонч хосил килиш учун унинг Ракамли имзосини ЕЗухра калити ёрдамида синаб куриши кифоя килади. Гап шундаки ЕЗухра ошкора калит билан очиладиган шифрланган ахборотни факат Зухрага маълум булган унинг махфий калити DЗухра билангина шифрлаш мумкин. Қора ботир юборган мактуб эса бундай хусусиятга эга эмас, чунки у Зухранинг махфий калитини билмайди. Ракамли имзони хосил килиш ва уни синаб куриш жараёнларида ошкора хисобланган бир томонлама функцияларга кушимча тарзда факат бир томонлама хисобланадиган ва хаммага ошкора булган яна бошка бир функция (шифрланадиган матннинг бир томонлама хисоблана оладиган функцияси h(M), купинча хеш-функция) лардан хам фойдаланилади. Худди ана шу функция аввало, дастлабки М мактуби асосида хисобланиб (хисобланган h(M) message digest дейилади), сунгра махфий калит DЗухра билан шифрланиб Ракамли имзо сифатида жунатилади.

Ракамли имзо мохиятини очиб бериш учун куйида Зухра томонидан хосил килинган ракамли имзоланган очик хужжат Х жунатишни куриб чикиш билан чекланилган. Формал тарзда ракамли имзо S хосил килиш куйидагича ифодаланади:

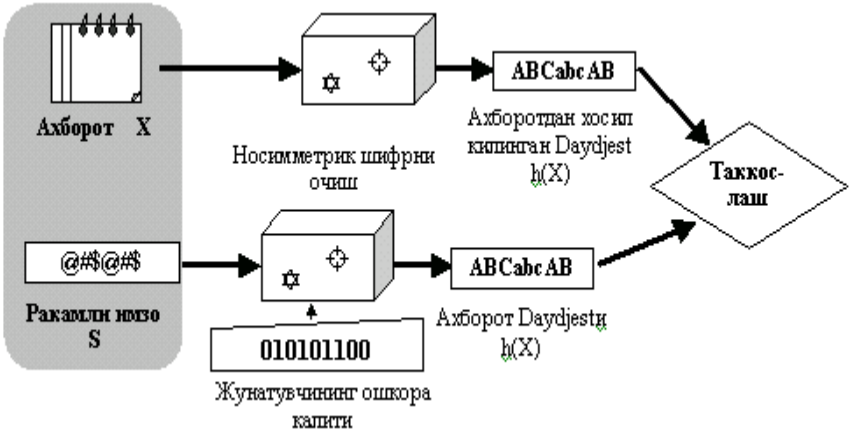
С к DЗухра (h(X))



9-расм. Шифрлашда рақамли имзони қўллаш.

Имзонинг хакикийлигини синаш кабул килиб олинган хужжатнинг хисоблаб топилган хеш-функцияси (hash function) у билан бирга кабул килиб олинган ракамли имзо шифрининг очилган холати (message digest) айнанлиги асосида хулоса чикаришдир.(9-расмга қаранг)

Тохир X ва S ни кабул килиб олгач Зухранинг ошкора калитидан фойдаланиб S асосида h(X) (message digest) ни хосил килади сунгра X асосида маълум алгоритмдан фойдаланиб Хнинг дайджести h(X) ни хисоблайди ва уларни таккослаш натижасига кура хужжат X нинг Зухра томонидан имзолангани ё имзоланмагани хакида хукм чикаради (10-расмга қаранг):



10-расм. Шифрлашда DayDjest ҳосил қилиши алгоритимини ишлатиш.

Жунатиладиган хужжатнинг пинхоналигини хам таъминлаш зарурати булса хужжат юкорида курилган усулда шифрланиб жунатилади. Шундай килиб, ахборот пинхоналиги ва уни жунатувчининг конуний кимса эканлигини билиш (аутентификация) муаммоларини ечишда носимметрик ва аралаш (симметрикКносимметрик) криптотизимларда икки жуфт калитлардан фойдаланилади.

RSA

RSA алгоритми 1977 йилда АКШнинг Массачусетс технология институтида ишлаб чикилган булиб, 4405829 ракамли АКШ патенти билан химояланган. Алгоритмнинг номи унинг муаллифлари фамилияларининг бош харфлари (Ривест, Шамир, Адлеман)дан тузилган. Алгоритмнинг криптобардошлилиги катта сонни туб купайтувчиларга ажратиш муаммоси математикада амалий хисоблаш нуктаи-назаридан хануз ечилмаганлигига асосланади.

ElGamal

ElGamal алгоритми 1985 йилда ишлаб чикилган. Алгоритмнинг номи унинг муаллифи фамилиясида аталган. DSS (Digital Signature Standard) АКШ стандартида ишлатилади. Алгоритмнинг криптобардошлилиги чекли майдонларда бутун сонларни логарифмлаш муаммоси математикада амалий хисоблаш нуктаи-назаридан хануз ечилмаганлигига асосланади**.**

PGP

PGP дастури PHilip TSimmermann томонидан 1991 йилда ишлаб чикилган. Pretty Good Privacy -бинойидек махфийлик деб номланган. PGP криптотизимининг ишлаш тамойили симметрик ва носимметрик криптотизимларни бирга ишлашига асосланган. PGP RSA га алтернатива булиб унинг криптобардошлилиги PGP каби катта сонни туб купайтувчиларга ажратиш муаммоси математикада амалий хисоблаш нуктаи-назаридан хануз ечилмаганлигига асосланади.

PGP датурини Интернет оркали куйидаги манзиллардан олиш мумкин:

- Норвегиядаги http:ГГwww.ifi.uio.noГpgpГ бош сайтдан 2.6.3и русум(и харфи интернатионал , яъни АКШдан ташкарида яшовчилар учун эркин таркатиладиган русумни белгилайди).
- Россиядан (323К) ftp:ГГftp.kiae.suГpubГwindowsГcryptoГpgpГpgp263i-win32.zip.
- Европасайтларидан ftp:ГГftp.ox.ac.ukГpubГcryptoГpgpГpcГwindows95ГPGP50trial.exe 3.5 MB хажмли Windows 95 амал тизими учун мулжалланган PGP дастурининг 5.0 версиясини ёзиб олиш мумкин.
- АКШ да истикомат килувчилар ё бепул 2.6.2 русумни MIT сайтидан http:ГГbs.mit.edu:8001Гpgp-form.html манзили буйича, ёки сунгги турли платформалар (Windows 95 ва Makintosh) учун ёзилган PGP 5.0 русумини http:ГГwww.pgp.com манзилидан олишлари мумкин

PGP дастурининг аввалги 2-русумларидан Windows мухитида ишлатиш учун куйидаги манзиллардаги кобик- дастурлардан фойдаланиш мумкин:

- Aegis Shell (2.43M)
- MailPGP 1.3 (80K)

Иккала дастур хам шифрлаш-шифр очиш амалларини файллар клавиатурадан ё дискдан киритилганда кунгилдагидек бажарадилар. Лекин бу дастурлардан фойдаланиш учун pgp263i-win32.zip, файлининг узи хам керак булади.

RPK алгоритми АКШ ва Янги Зеландия фукароси математик, хисоблаш техникаси буйича мутахассис доктор Виллиам М.Раике (Uilyam M.Reyk) томонидан New Zealand компанияси (Янги Зеландия, Окиянда ташкил этилган) да яратилган. Дастур "RPK Sate Cracker Challenge" деб номланган булиб, унинг муаллифи фамилиясининг бош харфидан бошланади. Дастур муаллифи узи ишлаб чиккан алгоритмни энг тез ишлайдиган ва хавфсизлиги буйича RSA алгоритми билан тенг янги носимметрик криптотизим алгоритми эканини эълон килди. Унинг криптобардошлилиги чекли катта

майдонларда дискрет логарифмни хисоблаш амалий нуктаи-назардан ечилмаганлигига ва кориштириш генераторининг комплекс хисоблашларига асосланган.

RPK хакида икки огиз суз.

Reyknинг RPK тизими содда компонентларни бирлаштириб "кориштирувчи генератор " (михтуре генератор) деб номланган янги криптографик тизим ядросини яратишга асосланган.

Бу алгоритм билан WWW оркали ёзиб олиб, уни текшириб куриш мумкин. Бу компания химоя ва шифрлаш буйича саноат даражасидаги умумий стандартни яратишни максад килиб куйган. Технологияни тестдан утказишда катнашишни истовчиларни рагбатлантириш мАксадида "RPK Sate Cracker Challenge" дастурнинг бепул русумини httpГГcrypto.swdev.co.nz манзилдан юклаб олиниши мумкинлиги билдирилган. Унинг Web-сахифаси "Ошкора калитли криптография" деб номланиб, алгоритмни бахолаш учун унда кенг материал (махсулотнинг дастлабки матни, алгоритмлар ва техникавий хужжат) берилган. Унда Windows 95 ёки Windows NT фойдаланувчилари учун унинг янги усули аслида янгиллигини курсатиш учун бепул компьтер дастури хам келтирилган.

Технология ихтирочиси кимда-ким RPK нинг виртуал сейфига кира олса ва бу билан унинг лойихаси заиф эканини исбот эца унга 3000 доллар мукофот ваъда килган.

Reyk якинда Security Dinamics Technologies, Inc. RSA Data Security. Inc ни 300 млн. долларга сотиб олганини, RSA алгоритмини очик калитли саноат криптографик тизим деб тан олиб, уз технологиясини анча тез ва жахон микёсида жуда кенг кулланилиши мумкин деб хисоблайди

Бу АКШ хукумати томонидан Америкада ишлаб чикарилган криптотизимларнинг экспортига чекловлар куйилгани (RSA га, PGPга) хисобга олинса анча фойдали маълумотдир.

PGP хакида икки огиз суз.

Электрон почталарни бегона кузлардан химоялаш дастурлари ичида энг оммавийлашиб бораётганларидан бири - бепул таркатиладиган PGP-дастуридир. Хозирги кунда унинг электрон ёзишмалар учун жахон стандарти даражасига кутарилиб бораётганининг сабаби бу криптотизимни кулфини бузиш учун хозирги энг кучли компьютерлар учун хам асрлар давомида хисоблашлар бажаришга тугри келади.

PGP дастури икки калитли - махфий ва ошкора калитли криптотизимнинг асосини ташкил этади. Бунда хар бир хат олувчи уз ошкора калитини барча учун(масалан уз Web сахифасида) эълон килиб куяди ёки хат ёзиши кутилаётган кимсага уз ошкора калитини электрон кути оркали жунатади. Кимда-ким унга электрон хат юборадиган булса PGP дастуридан фойдаланиб шу ошкора калит ёрдамида уз хатини шифрлаб хат олувчига жунатади. Бу хатнинг шифрини шу хат олувчидан узга кимса очаолмайди, чунки бу хатни оча оладиган махфий калит факат ошкора калитнинг эгасидагина бор.

Filip Zimmermann 1991 йилда инсонпарварлик максадларини кузлаб Интернетда уз дастурини бепул нашр этгач, криптография воситаларининг экспорти коидаларини бузганликда гумон килиниб, АКШ хукукий органлари томонидан терговга тортилган. 1996 йилда тергов тухтатилгач у уз компаниясини очган. PGP дастурининг янги 5,0 русуми Windows ва Apple Macintosh амал тизимларида ишлашга мулжалланган. 1997 йилда Диффи ва Хеллманларнинг хамда Хеллман ва Мерклининг патентлари муддати тугагани ошкора калитли янги алгоритмлар яратишга (патент учун чегирувлардан холи)кенг йул очилиб, ошкора калитли тизимларга булган монополия тугаган.

Янги русумдан хар бир фойдаланувчига икки жуфт калит берилади. Битта жуфти Диффи-Хеллман алгоритмидаги каби шифрлаш ва шифрни очиш учун ишлатилади, иккинчи жуфти NIST томонидан таклиф этилган сертификатли имзо куйиш(DSS) учун ишлатилади. Бу русумда хам симметрик криптотизимнинг IDEA шифридан фойдаланишда давом этилган, уч карра

DES ёки CASTни танлаш имконияти хам сакланган. Ракамли имзодан фойдаланиш учун SHA-1 хеш алгоритмидан фойдаланилган. Бу эса RSA да ишлатилган MD5 хеш-алгоритмидан мукаммалдир. PGP ни очик калитлар серверлари билан ишлай олиши унинг кучли томони хисобланади. Фойдаланувчи янги ошкора калитни хосил килганда PGP уни олисдаги (масалан MIT даги) серверга урнатишни таклиф килади. Бу PGPдан фойдаланувчиларни глобал маконга бирлаштиради. Бундай имконият хозирча бошка ошкора калитли тизимларда мавжуд эмас.[16]

Криптография – криптография амаллари асосида ахборот хавфсизлигини таъминлаш фани булиб, асосан турт хил хавфсизлик муаммоси ечимларини топиш билан шугулланади. [17]

Булар:

Пинхонийлик(Confidentiality).

Ахборот бутунлиги(Data Integrity).

Аутентификация:

Ахборот эгасини аутентификацияси(User Authentication)-ахборот юборган шахс асл шахслигини текшириш.

Ахборот асл нусхасини аутентификацияси(Data Origin Authentication)-олинган ахборот уз аслига айнанлигини текшириш.

Алока катнашчилари назорати:

Инкор этаолмаслик(Non-repudiation) - ахборот йуллаганликни ё уни (умуман ё уз вактида) кабул килиб олганликни буйнига олмасликни олдини олиш.

Криптография амалларининг энг асосийлари шифрлаш ва шифрни очишдир. Шифрлаш (инглизча- enciphering)- шифрлаш калити иштирокида берилган (дастлабки) ахборотни бегона олиб тушунмайдиган шаклга, яъни шифрланган ахборотга айлантиришдир. Шифрни очиш (инглизча-deciphering) - шифрланган ахборотни уни очиш калити ёрдамида дастлабки ахборотга айлантиришдир. Шифрни бузиб очиш - шифрланган ахборотни

шифрни очиш калитини билмаган холда дастлабки ахборотга айлантиришдир.

Шифрлаш пинхонийликни таъминлаб ахборотни бегоналардан махфий саклаш имконини беради. Шифрланадиган ахборот, умуман олганда матн, овоз ёзуви ва тасвир шаклида ё булмаса аралаш шаклда берилиши мумкин. Амалиётда шифрланадиган ахборот асосан матн (инглизча- plaintext) шаклида берилади ва шифрланган матн (инглизча- ciphertext)га айлантирилади.

Криптография усуллари алока тизимининг хавфсизлигини таъминлаш учун кулланилганда у алока мазмунинигина, яъни узатилаётган ахборотнинг узинигина химоялайди, алока мавжудлигини, шу жумладан алоканинг кимлар орасида ва кандай интенсивликда содир булаётганини эса химоялаёлмайди. Алока мавжудлигини стеганография усуллари химоялаш имконини беради. Бунда айрим холларда каналдаги трафикнинг доимий(масалан, бирхил шовкин тарзида) булишига, яъни трафикнинг узатилаётган ахборотга боглик булмаслигига эришиш кифоя килади.

Ахборот узатиш ва саклаш жараёнларининг ракамлаштирилиши узлукли (нутк) ва узлуксиз (матн, факс, телекс, тасвир, анимация) ахборотларни химоялаш учун ягона алгоритмлардан фойдаланиш имконини беради. Бундан буён шифрланадиган ахборот матн шаклида берилиши назарда тутилади.

Шифрлаш алгоритмларига куйидаги талаблар куйилади:

- шифрланган ахборотни узгартириб куйиш ё уни шифрини бузиб очишга йул колдирмаслик;
- ахборот химояси факат калитнинг маълумлигига боглик булиб, алгоритмнинг маълум ё номаълумлигига боглик эмас (Kerkgoff коидаси);
- дастлабки (шифрланадиган) ахборотни ёки калитни бироз узгартириш шифрланган матннинг бутунлай узгартириб юбориши лозим ("упирилиш" ходисаси);

– калитнинг кийматлар сохаси шундай катта булиши керакки, ундан калит кийматларини бир бошдан куриб-чикиш асосида шифрни бузиб очиш имкони булмаслиги лозим;
– алгоритм иктисодий жихатдан тежамли ва етарли тезкорликка эга булиши лозим;
– шифр матнини бузиб очишга кетадиган сарф-харажатлар ахборот бахосидан юкори булиши лозим.

Барча носимметрик криптотизимларни криптотахлил килиш асосан калитларни бир бошдан куриб чикиш асосида амалга оширилади. Шунинг учун уларнинг симметрик криптотизимларга тенг бардошлилигини таъминлаш максадида анча узун (битлар сони буйича) калитлардан фойдаланилади. Брюс Шнэер узининг "Амалий криптография: Си да протоколлар, алгоритмлар и дастлабки матн " китобида калитларнинг эквивалент узунликлари учун куйидаги ракамларни келтиради.[18]

Симметрик калит узунлиги, бит 56 64 80 112 128

Носимметрик калит узунлиги, бит 384 512 768 1792 2304

Симметрик криптотизимлар

Симметрик криптотизимларда ахборот алмашиш уч боскичда юз беради:

1. ахборот жунатувчи уни олувчига узаро махфий калитни, яъни икковларидан узга хечкимга маълум булмаган калитни топширади;
2. жунатувчи узаро махфий калит билан ахборотни шифрлаб уни олувчига жунатади;
3. кабул килиб олувчи ахборотни олиб унинг шифрини узаро махфий калит билан очади. [19]

Умуман олганда иккала томон бу калитдан бир неча бор кайта фойдаланишлари мумкин. Шу калитдан алока учун кайта фойдаланилганда ёки калит ахборот эгасининг узи ишлатадиган матнни шифрлаш учун тузилган булса, албатта.

Шифрланадиган ахборот микдори билан тенг калитдан фойдаланиш хар доим хам кулай булавермайди. Биринчи боскичга хожат булмайди. Агар

хар куни ва хар бир алока сеанси учун янги ноёб калит ишлатилса, криптотизимнинг хавфсизлиги юкорирок булади. [20]

2.4. Индентификация ва аутентификация.

Идентификация ва аутентификация (Ид ва А) - фойдаланувчи ва жараёнлар тўғрисидаги маълумотларнинг ҳақиқийлигини (асллигини) текшириш ва аниқлаш жараёнидир. Улар фойдаланувчига система ресурсларидан фойдаланишининг мумкин ёки мумкин эмаслиги ҳақида қарор қабул қилишда ишлатилади. У ёки бу маълумотдан кимлар фойдалана олиши мумкинлигини аниқлаш маълумотлар синфланиши жараёнининг таркибий қисми бўлиши лозим.[21]

Аутентификациянинг учта асосий кўриниши мавжуд бўлиб, улар - статик, барқарор ва ўзгармас. Статик аутентификация пароллардан ва бошқа технологиялардан фойдаланади. Бу парол ва технологияларни такрорлаш йўли билан йўққа чиқариш мумкин. Одатда, бу пароллар такрор фойдаланиладиган деб номланади. Барқарор аутентификация бир марта ишлатиладиган паролларни яратиш учун криптографиядан фойдаланади. Бу усул тармоққа уланиш жойига атака қилувчи хабарларни қўйиш билан йўққа чиқарилади. Ўзгармас аутентификация тармоққа уланиш жойига атака қилувчи информацияни қўйишдан сақлайди. [22]

Статик аутентификация

Статик аутентификация аутентификацияловчи ва аутентификация-ланувчи томонлар ўртасида узатилаётган информацияни ёт ҳужум қилувчи томон кўра олмайдиган, ўзгартира олмайдиган, кўя олмайдиган пайтдагина ҳимояни таъминлайди. Бундай ҳолатда бузғунчи фақат аутентификация жараёнини бошлаш (буни фақат қонуний фойдаланувчи амалга ошира олади) ва бир қатор уринишларни амалга ошириш ёрдамидагина маълумотларни аниқлашга уриниши мумкин. Пароллардан фойдаланишнинг анъанавий схемалари ҳимоянинг мана шу туридан фойдаланади. Лекин аутентификация мустаҳкамлиги асосан паролларни топишнинг мураккаблиги ҳамда бу

паролларнинг қанчалик даражада яхши ҳимояланганлигига боғлиқ бўлади. [23]

Барқарор аутентификация

Аутентификациянинг бу синфи ҳар бир аутентификация сеансларида алмашиниб турадиган динамик аутентификация маълумотларидан фойдаланади. Аутентификацияловчи ва аутентификацияланувчи орасида узатиладиган информацияни тутиб қолиши мумкин бўлган атака қилувчи янги аутентификация сеансини аутентификацияланувчи билан биргаликда бошлашга ва қонуний фойдаланувчи назорати остида ниқоблаш умидида маълумотларни такрорлашга ҳаракат қилади. 1-даражали кучайтирилган аутентификация шундай атакалардан ҳимоя қиладики, бу атака натижасида олдинги сеансда ёзилган аутентификация маълумотларидан кейинги сеансларда фойдаланиш мумкин бўлмай қолади.[24]

Шунга қарамасдан, барқарор аутентификация маълумотларни фаол атакалардан ҳимоя қила олмайди. Бундай атакалар аутентификация жараёни тугагандан сўнг фойдаланувчи томонидан серверга жўнатиладиган команда ва маълумотлар атака қилувчи томонидан ўзгартирилиши натижасида амалга оширилади. Сервер берилган аутентификацияланаётган фойдаланувчи ва мантиқий уланиш ўртасидаги алоқани таъминлайди, у ўзини ушбу уланишга таъллуқли барча командаларнинг манбаи деб ҳисоблайди.

Анъанавий пароллар барқарор аутентификацияни таъминлай олмайди. Фойдаланувчи пароллари кейинчалик фойдаланилиши ёки тутиб қолиниши мумкин. Лекин бир марталик пароллар ва электрон имзолар ушбу ҳимоя даражасини таъминлай олади.

Ўзгармас аутентификация

Аутентификациянинг бу тури аутентификацияланувчи ва аутентификацияловчи орасида узатиладиган маълумотлар оқими орасига информация қўшиши, ўзгартириши ва тутиб қолиши мумкин бўлган атака қилувчидан ҳаттоки, аутентификация жараёни тугагандан сўнг ҳам ҳимояни таъминлайди. Бундай атакалар фаол атака деб юритилиб, атака қилувчи,

асосан, сервер ва фойдаланувчи орасидаги боғланишга фаол таъсир кўрсатади. Ҳимоянинг бу турини амалга оширишнинг усулларидан бири фойдаланувчидан серверга жўнатилаётган ҳар бир маълумотлар битига ишлов беришни электрон имзоларни инерция қилиш алгоритми ёрдамида амалга оширишдан иборат. Криптография асосидаги бошқа комбинациялар ҳам мавжудки, булар ёрдамида аутентификацияни амалга ошириш мумкин. Лекин, мавжуд стратегияларда ҳар бир маълумот битини ишлаш учун шифрлашдан фойдаланилади. Акс ҳолда маълумотлар оқимининг ҳимоя қилинмаган қисми шубҳали ҳолда қолиши мумкин. [25]

Тармоққа киришда ва фойдаланувчи номини киритишда идентификация, парол киритишда аутентификация амалга оширилади. Агарда фойдаланувчи ушбу парол ва ном билан системада қайд қилинган бўлса, унга аниқ объект ва ресурслардан фойдаланишга рухсат этилади. Бироқ системага киришда, бу функцияларнинг бажарилиш жараёнида баъзи фарқлар мавжуд. Бу фарқлар иш жараёнида система ким ишлаётгани, унинг қандай ҳуқуқлари борлиги ва ҳоказолар ҳақида информацияга эга эканлигига асосланади ва шунинг учун мос ҳолда субъект саволларига жавоб қайтаради. Системага киришда буларнинг ҳаммасини олдиндан аниқлаш керак бўлади. Ушбу ҳолатда аслликни таъминлаш мақсадида фойдаланувчидан хавфсизлик ядроси томон боришда идентификацияловчи информациянинг узатилиш йўли - “ишончли маршрут”ни ташкил этиш зарурияти туғилади. Амалиёт шуни кўрсатадики, фойдаланувчининг системага кириши - ҳимоянинг анчагина нозик жойларидан биридир: кўпчилик ҳолларда паролларни синдириш, паролсиз кириш, паролларни тутиб қолиш ва ҳоказо ҳолатлар рўй беради. Шунинг учун фойдаланувчи ҳам, система ҳам ўзаро бевосита ишлаётгани, улар орасида бошқа программа ёки узатилувчи информациялар йўқлиги ҳақида ишонч ҳосил қилиши керак. [26]

Фойдаланувчи идентификаторлари ва уларнинг пароллари ҳар бир фойдаланувчи учун ягона бўлиши керак.

Пароллар 6 та символдан кам бўлмаслиги ва машҳур номлар ёки иборалардан тузилмаслиги лозим. Ўйлаб топиладиган паролларнинг пайдо бўлишини доимий равишда махсус программалар ёрдамида текшириб туриш зарур. Бундай программаларда ўйлаб топиладиган пароллар генерацияси бўйича қоидалар тўплами бўлиши лозим.

Пароллар махфий ҳолда сақланиши, яъни бошқа одамларга айтилмаслиги, программа матнида ва ҳар хил қоғозларда ёзилмаслиги ҳамда ҳар 90 кунда алмаштирилиши лозим. Кўпчилик системалар маълум вақт ўтгач паролни мажбурий алмаштириши ва аввал фойдаланилаётган паролни йўққа чиқариши мумкин.[27]

Фойдаланувчилар бюджети системага киришда 3 та муваффақиятсиз уринишдан сўнг “қотиб қолиши” ҳамда нотўғри киритилган пароллар номи система журналига киритиб қўйилиши керак.

Фойдаланувчи ва сервер орасида бўладиган иш сеанси 15 минут давомидаги фаолиятсизликдан сўнг блокировка қилиниши лозим. Сеанс ишини қайта тиклаш учун яна парол киритиш талаб қилиниши керак.

Системага муваффақиятли кирилганда, ундан охирги марта фойдаланилган сана ва вақт акс эттирилиши лозим. .[28]

Фойдаланувчилар бюджети маълум вақт фойдаланилмагандан сўнг блокировка қилиниши шарт.

Юқори таваккалли системалар учун: бир қанча берухсат кириш учун уриниб кўришлардан сўнг система огоҳлантириш сигналини бериши ва бу уринишларни амалга ошираётган фойдаланувчи учун сервернинг ёлғон хабарларини бериши лозим. [29]

Чунки у системага қўшилган ҳолда турган вақтда хавфсизлик администратори унинг жойлашган ўрнини аниқлашга ҳаракат қилади.

II-боб бўйича хулоса.

Ушбу бобда асосан ахборотларни ҳимоялаш муаммолари ва уларни ечимлари, ахборот хавфсизлигига тахдидлар ва уларни келиб чиқиш асослари, ахборот хавфсизлигини таъминлашнинг асосий йўллари ҳамда хуқуқий ва ташкилий таъминоти, ахборотни ҳимоялашнинг криптографик усуллари ҳамда индентификация ва аутентификация масалалари устида назарий ва амалий тарзда изланишлар натижалари кўрсатилган.

Шунингдек, келтирилган аниқ мисол орқали криптографияда шифрлаш усуллари ва рақамли имзони олиш ғоялари ўрганилган.

Ахборотни муҳофаза қилиш соҳасидаги ишлар ҳолатининг таҳлили, муҳофаза қилишнинг тўлиқ шаклланган концепцияси ва тузилиши ҳақида фактли мисоллар келтирилган.

Ўзбекистоннинг маънавий равнақи соҳаларида, маънавий ҳаёт ва ахборот фаолиятида фуқароларнинг конституциявий ҳуқуқлари ва эркинликларига таҳдидларни интерент тармоғи ҳамда ахборотни қайта ишлаш воситаларидаги ахамиятини республика ҳудудида жорий этилган ҳамда яратилаётган ахборот ва телекоммуникация тизимларининг меъёрида ишлашига, ахборот ресурслари хавфсизлигини таъминлашга боғлиқлиги хусусида фикрлар берилган.

Ахборотни муҳофаза қилиш тизимларидан фойдаланишда комплекс ахборотни муҳофаза қилиш тизимларидан бошқа самарали чора-тадбирлари тўғрисида ҳам кенг тўхталиб ўтилган.

Идентификация ва аутентификациянинг моҳиятини очишга кенг тўҳталиб, аутентификациянинг асосий кўринишлари ҳамда фойдаланувчи ва жараёнлар тўғрисидаги маълумотларнинг ҳақиқийлигини (асллигини) текшириш ва аниқлаш жараёнларини ўрганилган.

Ушбу бобда ўрганилган ва олиб борилган тадқиқотлар 3-4 бобларни моҳиятини очиб беришга йўналтирилган.[*]

[*] Бобни ёртишда адабиётлар рўйхатидаги 30, 31, 32, 33 рақамли адабиётлардан қўшимча манба сифатида фойдаланилди.

III-БОБ. ТАСОДИФИЙ РАҚАМЛАР ГЕНЕРАТОРЛАРИ ВА УЛАРНИ СИФАТИНИ ТАДҚИҚ ЭТИШ.

3.1. Тасодифий рақамлар генераторлари ва уларнинг турлари.

Ахборот хавфсизлигига бўлган эхтиёжларнинг тобора ортиб бориши, янги ҳимоя қилиш тизимларини турлари ва усулларини яратиш ҳамда уларни тадқиқ этиш бўйича самарали ишларни олиб боришни талаб қилади. Бу эса доимий равишда ташкилот ва корхоналарни ҳимоялаш тизимларидан тўғри, самарали, муваффақиятли фойдаланишига боғликдир. Айни вақтда кўплаб ахборотни ҳимоя қилиш воситалари тасодифий рақамлар генераторлари (ТРГ) асосида қурилмоқда ва ташкил этилмоқда. Шу нуқтаи назардан хар бир ташкилот ва корхоналарни ўзига тегишли ахборот тизимлари ва технологияларидан тўғри, самарали, муваффақиятли фойдаланиши уларни қандай ва нима асосга қурилишига асосланади.

Хозирги кунда қўлланилаётган кўплаб ахборотларни қайта ишлаш воситалари тасодифий рақамлар генераторлари (ТРГ) асосида қурилмоқда. Масалан тест ўтказиш ва ўқитишнинг компьютерли дастурларида тасодифий герациялаш, электрон рақамли имзо (ЭРИ) олишда калит хабарларини генерациялаш, ахборотни ҳимоялашда генерация, компьютер графикасида ранглар генерацияси, криптографияда киптоалгаритмларни тузиш ва шу каби бошқа мисолларни келтириш мумкин. [34]

Тасодифий рақамлар генераторларига (ТРГ) қисқача тўхталиб ўтсак. ТРГ (рус. Генератор случайных чисел ГСЧ, англ. Random number generator, RNG) – бу кетма-кет рақамларни яратувчи алгоритм бўлиб, деярли бир биридан мустақил бўлган ва берилган тарқалишга боғланувчи (одатда тенг ўлчовда) элементлар берувчи дастурий таъминотдир. [35]

Замаонавий информатикада тасодифий рақамлар кенг кўламда ва турли иловаларда фойдаланилади. Буни Монте-Карло усулида, имитацион моделлаштиришда ва киптографияда кўриш мумкин. Фойдаланилаётган ТРГни сифати тўғридан-тўғри улардан олинаётган натижаларга боғлиқ

бўлади. Буни математика афоризмда таниқли Роберт Кавью шундай изоҳлайди: (англ.) ўзбекча: “тасодифий рақамлар генерацияси жуда ҳам муҳим, қачонки унга тасодифлар эркинлиги берилган бўлса”.

Яна шуниси муҳимки, ТРГ ларни натижалари уларнинг манбаларига боғлиқ бўлади. Аслида хақиқий тасодифий рақам манбасини ифодалаш қийин. Бироқ физик нуқтаи назардан уларни кўрсатиш мумкин. Масалан, товушлар, радиацияни ионловчи детекторлар, резистр ёки космик нурланишдан келган бўлинаётган товушлар ТРГ лар олишнинг хақиқий манбалари бўлиши мумкин.

Криптографик иловаларда ТРГ лар генерациялашда махсус алгоритмлардан фойдаланади. Бу алгоритмлар олдиндан аниқланган ва кетма-кет генерацияланувчи кетма-кет рақамни генрерациялаб беради, яъни назарий жиҳатдан бўлиши мумкин бўлмаган статик тасодифийликни яратиб беради. Бир вақтнинг ўзида, агар яхши алгоритм танланган бўлса, олинаётган кетма-кет рақамлар тасодифийлик тестларини кўпидан муваффақиятли ўтади. Бундай рақамлар тасодифий кетма-кет рақамлар деб номланади. [35]

Бироқ фанда бунинг алтернатив ечими ҳам мавжуд. Яъни катта миқдордаги тасодифий рақамлар тўпламидан луғат сифатида фойдаланиш орқали “бир марталик блакнот” тузиш мумкин. Бундай тўпламлар иловаларни ишлатишда талаб қилинаётган тасодифий рақамлар олиш манбасини жуда ҳам чегаралаб қўйиши мумкин. Масалан тармоқ хавфсизлигини таъминлашда бундай тўпламлар хақиқатда статик тасодифийликни берсада, хавфсизликни таъминлашда етарли ҳисобланмайди. Чунки туплам луғатини насхасини олиш хафи юқори.

ТРГ ларни аппарат қурилмалари яратилган бўлиб, улар физик жараёнларни лойихаловчи параметрлар ўлчамлари асосида тасодифий рақамни генерация қилади. Бундай қурилмаларни ишлаши кўпинча ишончли энтропия манбаларига асосланади, масалан иссиқлик товушлари, фотоэлектрик эффектлар, квантли ходиса ва шу кабилардир. [36]

ТРГ компьютер графикасида қўлланилиб, компьютер алгоритмларини текшириш эффективлигини оширишни яхши манбаси ҳисобланади.

ТРГ криптографияда муҳиб ахамиятга эга бўлиб, уни калит кетма-кетлиги сифатида қўллаш мумкин. Киптоалгаритмларни асимметрик тўғирлашда ҳар бир очиқ матн бўлаклари тасодифий байтни қўшишни талаб қилади. Шунингдек тасодифий сон бўлаклаб шифрлаш ва кешлашда ҳам фойдаланилади.

Шуни айтиб ўтиш керакки, аниқ рақамни, яъни мос келувчи аниқ қийматни олиш жуда мураккаб бўлиб, барча алгоритм ва технологияларни олинаётган натижасига қараб, олдиндан башоратлаш асосига қурилади. Хозирда етарли миқдорда турли дастурлаш тилларида ТРГ ишлаб чиқарилган. Умумий қилиб айтилганда улар қуйидаги асосий таълабларга жавоб бериши лозим:

- эффективлик;
- ишлаб чиқилган ТРГ ни такрорлаш генерациясини йўқлиги;
- мультиплатформалилиги;
- дастурлаш жараёнини одийлиги.

Бироқ амалиёт шуни кўрсатадики, ТРГ ни ишлаб чиқаришда юқорида айтиб ўтилган барча талаблар ва киритерияларни қаноатлантириш етарли даражада мураккаб ҳисобланади.

Айни вақтда жуда хам кенг миқёда тарқалган дастурий генереторлар, ёлғон тасодифий рақамларни ишлаб чиқувчи кетма-кетлик генерациясига асосланган бўлиб, детерминантларни рекуррент формулалари ёрдамида генерациялашга бўйсунади. Ёлғон тасодифий кетма-кетлик деб номланишга сабаб, барча мустақил ва тенг ўлчовли текширувларга қарамасдан, генерация тўлиқ детерминантликни сақлаб қолади. [37]

Бундай ТРГ генераторлари бир нечата қўшимча талабларни қаноатлантириши лозим:

- генерацияланган кетма-кет рақамлар тенг ўлчамли тарқалувчи ва мустақил бўлиши;

- кетма-кетлик даври катта узунликдаги имкониятни бериши лозим.

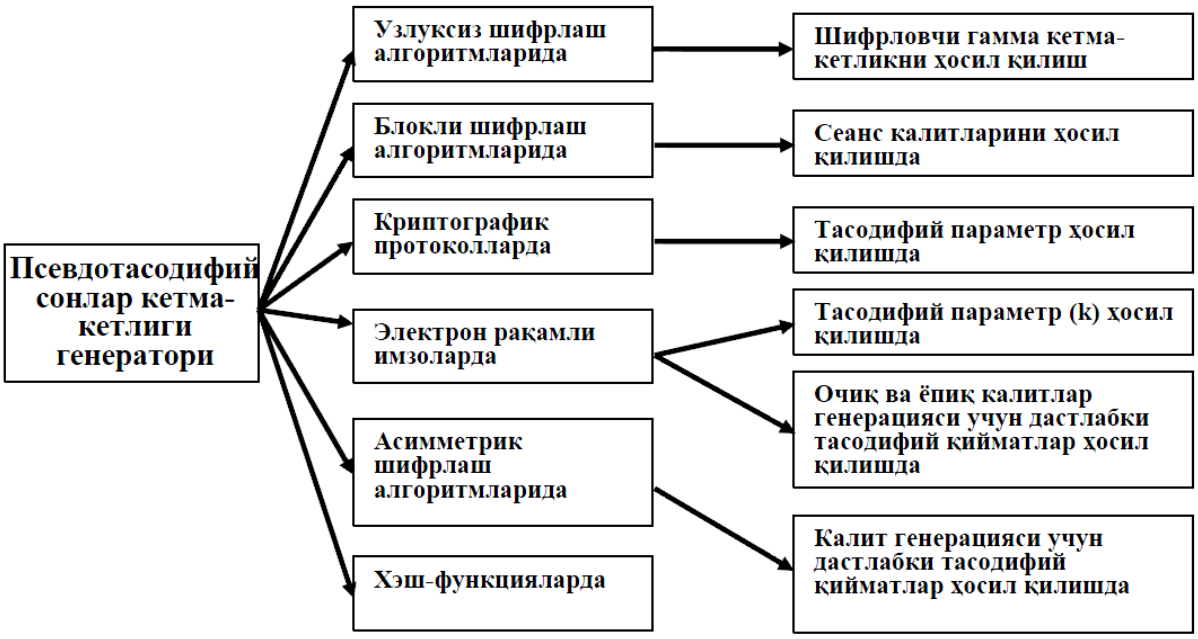
Генераторга қўйилаган талаблар даражаси кўпинча қўйилаётган вазифа ёрдамида уни ечиш синфларига боғлиқ бўлади. Шунинг учун криптографияда фойдаланилаётган ТРГ га “қаттиқ” талаблар қўйилиб, криптоустунлик шифрлари ва ишончли ҳимояга бўйсиниши лозим. Ўз навбатида бундай кетма-кетлик ва генераторлар сифатини аниқлаш учун эффектив алгоритмларни аниқлаш мақсадга мувофиқдир. [38]

Тасодифий рақам генератори “яхши” деб ҳисобланиши учун, ишлаб чиқарилаётган ТРГ ни катта қисми аниқланган миқдорда хар бир текширувлар гурухидан қониқарили ва етарли натижалар билан чиқариш керак. Бу эса ТРГ ни аниқ текширувлар натижасига асосан ечилаётган маслани қўйтлган “қаттиқ” талаби ва сифатини берилган шартларга кўра бажаришга олиб келади. Шнингдек криптография топшириқлари бўича генератор ишлаб чиқарган кетма-кетликни хаммаси тасодифий бўлиши талаб қилинади.

3.2. Псевдотасодифий кетма-кет рақамли генереторларни тузилиши ва хусусиятлари.

Узлуксиз шифрлаш алгоритмлари, псевдотасодифий кетма-кетлик генераторлари таҳлил қилиниб, улар асосида аппарат-дастурий воситаларда самарали қўлланувчи акслантиришлар ҳамда алгоритмларининг яратилиш ва қўлланилишининг криптографик заруриятлари мавжуд. Узлуксиз шифрлаш алгоритмларини тизимли-назарий ёндашув, мураккабликка асосланган ёндашув ва комбинациялашга асосланган ёндашув йўналишида яратиш мумкин. Тизимли-назарий ёндашувда математик усуллардан фойдаланган ҳолда ечиш мураккаб бўлган математик муаммо алгоритмга асосий акслантириш қилиб олинади ва бу қийинчиликни амалий ечимлари изланади. Турли ҳил криптографик таҳлил усулларига бардошли бўлган алгоритм янги алгоритм сифатида таклиф қилинади. Мураккабликка асосланган ёндашувда мураккаб деб тан олинган катта сонларни туб кўпайтувчиларга ажратиш, дискрет логарифмлаш ва бошқа шу каби акслантиришлар асосида алгоритм

яратилади. Бундай алгоритмларнинг криптобардошлиги даражаси юқорида келтирилган акслантиришларнинг мураккаблиги даражаси билан тенглаштирилади. Комбинациялаш йўналишида мавжуд бардошли алгоритмларнинг бир нечтасини биргаликда қўллаш асосида криптобардошлик оширилишига ҳаракат қилинади. Узлуксиз шифрлаш алгоритмлари асосини псевдотасодифий кетма-кетликлар хосил қилувчи генераторлар ташкил қилади. Псевдотасодифий сонлар кетма-кетлиги генераторлари узлуксиз шифрлаш алгоритмларидан ташқари ахборот хавфсизлигининг бошқа воситаларида ҳам кенг фойдаланилади (11-расмга қаранг).



11-расм. Псевдотасодифий сонлар кетма-кетлиги генераторини қўлланиш сохалари.

Яратилган псевдотасодифий сонлар кетма-кетлиги генераторларининг хаммасини ҳам самарали ҳамда криптобардошли деб бўлмайди. Ушбу бўлимда уларни баҳолаш учун қуйидаги талаблардан иборат махсус криптобардошлик ва самарадорликни баҳолаш усули ишлаб чиқилди:

- алгоритм акслантиришларининг соддалиги уларнинг криптографик таҳлилининг осон бўлишини таъминлаши керак;

- генератор асосидаги акслантиришларнинг умумий чизиқсизлик даражаси юқори бўлиши зарур;

-кириш параметридаги кичик ўзгаришнинг, ҳосил қилинган псевдотасодифий сонлар кетма-кетлиги элементларининг кескин ўзгаришига олиб келиши қатъий кўчки самарадорлиги мезони юқори бўлиши керак;

-акслантиришлар умумий бир томонламалик хусусиятига эга бўлиши керак;

-ишлаб чиқилган псевдотасодифий кетма-кетлик блоклари текис статистик тақсимот кўрсаткичига эга бўлиши, яъни тасодифийлик даражаси юқори бўлиши керак;

-алгоритм таркибидаги псевдотасодифий кетма-кетлик ишлаб чиқарувчи генераторнинг акслантиришлари етарли даражадаги такрорланмас узун даврга эга бўлган кетма-кетлик ишлаб чиқишини таъминлаши зарур;

-алгоритмнинг псевдотасодифий кетма-кетлик ишлаб чиқариш ва шифрлаш тезлиги юқори бўлиши зарур;

-махфий калитни аниқлашда мумкин бўлган барча калитларни танлаб чиқиш имконияти йўқлиги;

-ҳосил қилинган кетма-кетлик ёки унинг бирор қисми бўйича калитни тиклаш имкони йўқлиги;

-ҳосил қилинган кетма-кетликнинг маълум қисмини билган ҳолда унинг қолган қисмини тиклаш имкони йўқлиги;

-дифференциал криптотаҳлил усулига бардошлиги;

-чизиқли криптотаҳлил усулига бардошлиги.

Бу ерда алгоритм қатъий кўчки самарадорлиги мезони кўрсаткичи деб бир битга k`1 фарқ қилувчи ўхшаш кириш калитлари К1[k1, k2, …, kn] ва К2[k`1, k2, …, kn] орқали ҳосил қилинган G1[] ва G2[] псевдотасодифий кетма- кетликларнинг бир-биридан фарқ қилувчи мос тартибдаги битларининг миқдорига айтилади. Алгоритмнинг псевдотасодифий сонлар кетма-кетлиги ишлаб чиқиш тезлиги деб вақт бирлиги ичида ишлаб чиқилган псевдотасодифий битлар миқдорига айтилади. [39]

3.3. Тасодифий рақамлар генераторлари сифатини бахолаш мезонлари.

Хозирги вактда тасодифий кетма-кет рақам (ТРГ) деб номланувчи, яъни тасодифий тарзда танланувчи рақамларни дастурлаш тизимларида қўллаш кўплаб самарали натижаларга олиб келмоқда. Уни моделлаштиришнинг турли кўринишларида моделни адекватлигини ошириш мақсадида қўлланилади. Шунингдек, фойдаланилаётган ТРГ да махсус услуб ишлаб чиқилган бўлиб, мураккаб рақамлар тахлили масаласини ечиш учун ҳам қўлланилади. [40]

ТРГ компьютер графикасида қўлланилиб, компьютер алгоритмларини текшириш эффективлигини оширишни яхши манбаси ҳисобланади.

ТРГ криптографияда муҳим ахамиятга эга бўлиб, уни калит кетма-кетлиги сифатида қўллаш мумкин. Киптоалгаритмларни асимметрик тўғирлашда ҳар бир очиқ матн бўлаклари тасодифий байтни қўшишни талаб қилади. Шунингдек тасодифий сон бўлаклаб шифрлаш ва кешлашда ҳам фойдаланилади.

Шуни айтиб ўтиш керакки, аниқ рақамни, яъни мос келувчи аниқ рақамни олиш мураккаб бўлиб, барча алгоритм ва технологиялар олинаётган натижа олдиндан башоратлаш асосига қурилади. Хозирги кунда етарли кўп миқдорда турли ТРГ генераторлари ишлаб чиқарилган. Бироқ амалиёт шуни кўрсатадики, ТРГ генераторларини ишлаб чиқаришда юқорида айтиб ўтилган барча талаблар ва киритерияларни қаноатлантириш етарли даражада мураккаб ҳисобланади.

Айни вақтда жуда хам кенг миқёсда тарқалган дастурий генереторлар, ёлғон тасодифий рақамларни ишлаб чиқувчи кетма-кетлик генерациясига асосланган бўлиб, детерминантларни рекуррент формулалари ёрдамида генерациялайди. Ёлғон тасодифий кетма-кетлик деб номланишга сабаб, барча мустақил ва тенг ўлчовли текширувларга қарамасдан, генерация тўлиқ детерминантликни сақлаб қолади. [41]

Генераторга мансуб талаблар даражаси кўпинча қўйилаётган вазифа ёрдамида уни ечиш синфларига боғликдир. Шунинг учун криптографияда

фойдаланилаётган ТРГ га “қаттиқ” талаблар қўйилиб, криптоустунлик шифрлари ва ишончли ҳимояга бўйсиниши лозим. Ўз навбатида бундай кетма-кетлик ва генераторлар сифатини аниқлаш учун эффектив алгоритмларни аниқлаш мақсадга мувофиқдир. [42]

ТРГ генераторларини фойдаланилаётган дастурлаш тилларида рақамлар кетма-кетлик сифатини таққослаш ёрдамида тахлил қилиш кенг тарқалган. [43 Масалан C++ ва C# дастурлаш тилларида олинган кетма кетликни DES шифрли алгоритми ёрдамида чиқариш жуда кўп қўлланилади. [44] Масалан, шу усулда 60 та кетма-кет тасодифий рақамлар турли узунликлар ва даврларда текширилганда, C++ тилида (яъни Builder 2006 дастурий доирада) ёки C# тилида (Visual Studio 2008 дастурий доирада) random() функцияси қўлланилди. Шунигдек олинган маълумотларни шифрлашда DES шифрли алгоритмидан фойдаланилди. Ушбу тест натижасига кўра барча 60 та тест турлича деб ҳисобланди. Яъни, тасодифий (нотасодифий) ва қониқарли (қониқарсиз) натижаларга кўра кетма-кетлик 75% га тенг ўлчовли, 80% га мустақиллик ҳамда 75% га ишончли деб топилди. [45]

Тасодифий рақам генератори “яхши” деб ҳисобланиши учун, ишлаб чиқарилаётган ТРГ ни катта қисми аниқланган миқдорда хар бир текширувлар гурухидан қониқарили ва етарли натижалар билан чиқариш керак. Бу эса ТРГ ни аниқ текширувлар натижасига асосан ечилаётган маслани қўйтлган “қаттиқ” талаби ва сифатини берилган шартларга кўра бажаришга олиб келади. Шнингдек криптография топшириқлари бўича генератор ишлаб чиқарган кетма-кетликни хаммаси тасодифий бўлиши талаб қилинади. [46]

Бунда ўтказилаётган тадқиқотлар натижаларига асосан айтиш мумкинки, тасодифий рақамлар генреторлари ёрдами ишлаб чиқилган дастурий воситлар ахборотларни химоялаш ва хавфсизлиги муаммоларини камайтиришда ўз ўрнига эгалигини кўрсатиб турибди.

3.4. Юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш.

Шифрлаш тизимларини тасодифий рақамлар генерациясида, фақат абонент калити генерацияланмасдан, балки чиқиш идентификацияси учун бир марталик калит хабари ҳам юборилади. Бунда фойдаланаётган ХЕШ-функция баённомалари чиқиш идентификацияси баённомалари сертификатларида талаб қилинаётган етарли ҳажмдаги тасодифий маълумотларни "савол-жавоб" тарзида қабул қилади. Бу эса, тасодифий рақамни қабул қилиш учун қарши хужмни такрорий узатишга олиб келади. Бу алгоритмни хозирги кунда электрон рақамли имзо (ЭРИ) калитида кенг фойдаланиб келаётганлигини кўришимиз мумкин. Яъни, махфий калит ёрдамида имзолашда берилган қийматларни фойдаланилаётган бир марталик махфий калит ёрдамида тасодифий генерациялаш талаб қилинади. Бироқ кўпинча қўлланилаётган ахборотларни ҳимоя қилиш воситалари, хақиқий тасодифий қийматни доимо беришнинг ишончли манбаи ҳисобланмайди. [47]

Қайта ишланаётган ва узатилаётган ахборотлар хажмини доимий тарзда ортиб бориши ҳамда турли тизимлардан фойдаланувчилар сонини кўпайиб бориши ахборот хавфсизлиги муаммоларини ечишга қуйидаги талабларни қаноатлантириши зарур:

1. Ахборотларга рухсатни чегаралаш;
2. Тасодифий рақамлар генерациясини тезлигини ортириш.

Ушбу талабалар бажарилиши ўз ўрнида бош калитни калит жадвалида берилган энтропия бўлимли калитлар билан таққослаганда калит манбаларини етишмаслигини олдини олади. Шунингдек ТРГ ни тезлигини ошириш натижасида юқори тезликдаги каналларда маълумот узатиш тезлигини олишга, айниқса оптик толали алоқа линяларида мухим ахамият касб этади. [48]

Ишлаб чиқарилаётган ТРГ тезлиги фойдаланилаётган физик холатларга нисбатан олинганда анчагина чегараланган ҳисобланади. Одатда бу 100 Кбит/с дан ошмайди. Буни сабабини таниқли ТРГ лар тузилишига кўра

бинарли хусусиятли ходисалардан фойдаланишидадир. Яна бир томони кўпинча аналог ходисалар аососига қурилган ТРГ лар маълумотларни иккилик қийматга квантлаш услуби билан ўтаказиши натижасида хам тезлик камайиши мумкин. Масалан, товушларни сезиш электрон қурилмаларида аниқланган маълумот дискрет ходисаларни квантлаш ёрдамида поляризатор орқали ўтаётганда аниқланади. Катта тезликка эриши учун нобинарлик хусусияли кетма-кетликдаги квантлаш жараёнини ифодалайдиган ТРГ ларни яратиш лозимдир. [49]

Юқорида тўхталиб ўтилган фикрлардан келиб чиқиб, ТРГ ларни ишлаб чиқиш ва тахлил қилиш тасодифий ходисалар манбаси (ТХМ) асосида кўрилаётган квантли жараённи интенсив ўлчаш, нобинарлик хусусиятини ифодаловчи қийматлар ва уларни тахлил қилишнинг янги усулларини излаб топиш лозим. Бундай ТРГ лар ахборотлар хавфсизлиги ва уларни ҳимоя қилиш механизмларини мустахкамлиги ва уларни қўллашни имкониятларини жуда ҳам сезиларли даражада кўтаришга олиб келади. Масалан ЭРИ олишда ва уни қўллашда, нурланиш ёки иссиқлини кучсиз сигналларни сезувчи қурилмаларни ишлатишда, ишлаб чиқариш ташкилотлари маълумотлар базасини ҳимоялаш каби кўплаб ҳимоялаш воситаларини санаб ўтиш мумкин.

Хулоса қилиб шуни айтишимиз мумкинки, ишлаб чиқариш учун дастурий таъминот яратишда ахборотларни ҳимоялаш муаммолари бўйича дастурлаш тилларида қўлланиладиган ТРГ лар сифатини тадқиқ этиш натижасида келжакда юқори ишончлилик даражасини берувчи ҳамда юқори тезликда ишловчи ахборотни ҳимоялаш воситаларини яратиш кутилган самарали натижаларни беради деб ишонамиз.

3.5. Тасодифий рақамлар генераторларини ахборот тизим ва криптографик иловаларда қўллаш

Замонавий информатикада тасодифий рақамлар кенг кўламда ва турли иловаларда фойдаланилади. Буни Монте-Карло усулида, имитацион моделлаштиришда ва киптографияда кўриш мумкин. Фойдаланилаётган

ТРГни сифати тўғридан-тўғри улардан олинаётган натижаларга боғлиқ бўлади. Буни математика афоризмда таниқли Роберт Кавью шундай изоҳлайди: (англ.) ўзбекча: “тасодифий рақамлар генерацияси жуда ҳам муҳим, қачонки унга тасодифлар эркинлиги берилган бўлса”.

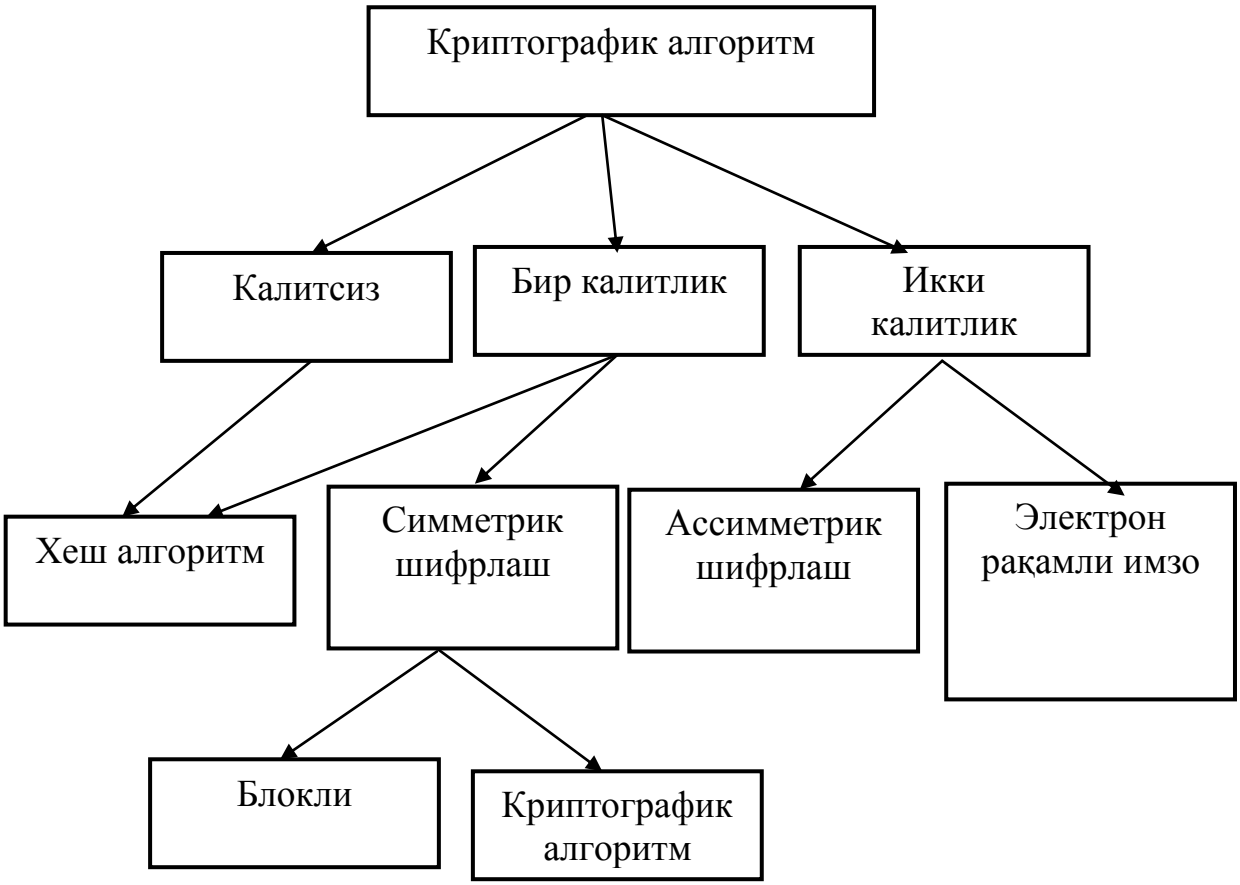
Яна шуниси муҳимки, ТРГ ларни натижалари уларнинг манбаларига боғлиқ бўлади. Аслида хақиқий тасодифий рақам манбасини ифодалаш қийин. Бироқ физик нуқтаи назардан уларни кўрсатиш мумкин. Масалан, товушлар, радиацияни ионловчи детекторлар, резистр ёки космик нурланишдан келган бўлинаётган товушлар ТРГ лар олишнинг хақиқий манбалари бўлиши мумкин.

Шунингдек, ТРГ лар криптографияда жуда ҳам кенг доирада қўлланилади. Шу ўринда криптография хақида бир оз тўхталиб ўтсак: криптография – сўзи қадимги грекча сўздан олинган бўлиб, “кўринмас” ва “ёзяпман” деган маноларни ангалатади. Фанда у ахборотни бегона шахслар томонидан ўқиш имкониятини чегаралаш (ишончлилик) ва ахборотга авторлик ҳуқуқини тўлиқлилиги ва ҳақиқийлигини ҳамда авторликдан воз кечмаслик имконини яратиш ҳисобланади. [50]

Криптографик ТРГ лар криптографик иловалар қўлланиладиган тасоодифий рақамларни ишлаб чиқаради, масалан калитни генерация қилиш. Криптографик ТРГ лари одатда “seed-қийматдан” фойдаланади, яъни ўз таркибида тасодифий қийматлар сақловчи ахборотлардан.

Криптографик иловаларда ТРГ лар генерациялашда махсус алгоритмлардан фойдаланади. (12-расмга қаранг) Бу алгоритмлар олдиндан аниқланган ва кетма-кет генерацияланувчи кетма-кет рақамни генрерациялаб беради, яъни назарий жиҳатдан бўлиши мумкин бўлмаган статик тасодифийликни яратиб беради. Бир вақтнинг ўзида, агар яхши алгоритм танланган бўлса, олинаётган кетма-кет рақамлар тасодифийлик тестларини кўпидан муваффақиятли ўтади. Бундай рақамлар тасодифий кетма-кет рақамлар деб номланади. [51]

Қуйида классик криптографик алгоритмни кўрамиз:



12-расм. Классик криптографик алгоритм.

Китографик ТРГ ларни қўллашнинг алтернатив ечими ҳам мавжуд. Яъни катта миқдордаги тасодифий рақамлар тўпламидан луғат сифатида фойдаланиш орқали “бир марталик блакнот” тузиш мумкин. Бундай тўпламлар иловаларни ишлатишда талаб қилинаётган тасодифий рақамлар олиш манбасини жуда ҳам чегаралаб қўйиши мумкин. Масалан тармоқ хавфсизлигини таъминлашда бундай тўпламлар хақиқатда статик тасодифийликни берсада, хавфсизликни таъминлашда етарли ҳисобланмайди. Чунки тўплам луғатини насхасини олиш хафи юқори.

ТРГ ларни аппарат қурилмалари яратилган бўлиб, улар физик жараёнларни лойихаловчи параметрлар ўлчамлари асосида тасодифий рақамни генерация қилади. Бундай қурилмаларни ишлаши кўпинча ишончли энропия манбаларига асосланади, масалан иссиқлик товушлари, фотоэлектрик эффектлар, квантли ходиса ва шу кабилардир. [52]

III-боб бўйича хулоса.

Келтирилган фикрлар, мулохаза ва мисоллардан келиб чиқиб, ТРГ ларни ишлаб чиқиш, тахлил қилиш ва уларни турли сохларга қўллаш амалий жихатдан ўз ўрнига эга эканлигини кўришимиз мумкин.

Таълим тизимида қўллашнинг муҳим жихати шундаки, ўсиб келаётган ёш авлод яъни бўлғуси мутахассисларни тайёрлаш жараёнида компьютерли дастурий воситалар, автоматлаштирилган ўқув тизимлари, масофадан ўқитиш ва тест синовларини ўтказиш каби жараёнларда ТРГ ларни қўлланилаётганини кузатиш мумкин. Кўпчилик холатларда ТРГлардан фойдаланиш ва қўллаш усулларини фақатгина дастурчиларни, компьютер мутахассисларини тайёрлашда ўргатиш керак деган изохларни, юқорида кўриб ўтган биргина мисол яъни рақамли ҳимоялаш воситаларини қуриш мисоли бекор қилиши мумкин.

Чунки ТРГ ларни қўллаш ёрдамида келажакда турли сохаларда яратилаётган дастурий воситаларни ишлаб чиқаришда, ахборотларни ҳимоялашда кутилган самарали натижаларни беради.

Мазкур бобда кўриб чиқилган ва илгари сурилган масаллар 4-бобни ҳамда диссертация ишиниг асосий мазмунини изохлашда ва очишда ўзининг салмоқли ўрнига эгадир.[*]

[*] Бобни ёртишда адабиётлар рўйхатидаги 53, 54, 55, 56, 57, 58, 59 рақамли адабиётлардан қўшимча манба сифатида фойдаланилди

IV-БОБ. ТУРЛИ ДАСТУРЛАШ ТИЛЛАРИДА ҚЎЛЛАНИЛАДИГАН ТАСОДИФИЙ РАҚАМЛАР ГЕНЕРАТОРЛАРИ СИФАТИНИ ТАХЛИЛ ҚИЛИШ.

4.1. Ахборотларни ҳимоялаш муаммолари бўйича c++ дастурлаш тилида яратилган тасодифий рақамлар генераторини сифатини тадқиқ этиш.

ТРГларини дастурлаш тилларида рақамларнинг кетма-кетлик сифатини таққослаш ёрдамида тахлил қилиш кенг тарқалган. Масалан C++ ва C# дастурлаш тилларида олинган кетма кетликни DES шифрли алгоритми ёрдамида чиқариш жуда кўп қўлланилади. Масалан, шу усулда 60 та кетма-кет тасодифий рақамлар турли узунликлар ва даврларда текширилганда, C++ тилида (яъни Builder 2006 дастурий доирада) ёки C# тилида (Visual Studio 2008 дастурий доирада) random() функцияси қўлланилди. Шунигдек олинган маълумотларни шифрлашда юқорида кўрибўтганимиздек DES шифрли алгоритмидан фойдаланилди. Ушбу тест натижасига кўра барча 60 та тест турлича деб ҳисобланди. Яъни, тасодифий (нотасодифий) ва қониқарли (қониқарсиз) натижаларга кўра кетма-кетлик 75% га тенг ўлчовли, 80% га мустақиллик ҳамда 75% га ишончли деб топилган эди. Ушбу натижаларга асосланиб қўйида тасодифий (нотасодифий) ва аниқланмаган тасодифй кетма-кетлик учун мисолларни келтириб ўтамиз:

C++ 81,7 16,6 1,7

C# 78,3 15 6,7

DES 96,7 3,3 0

ТРГ генераторини тенг ўлчовлик, мустақиллик ва ишончлиликга текшириш натижалари:

СЛ, % АН, % НТ, % ТС, %АН, % НТ, % ТС,% АН, % НТ, %

C++ 86,6 11,7 1,7 75 25 0 70 30 0

C# 81,7 11,6 6,7 71,7 28,3 0 73,3 26,7 0

DES 91,7 8,3 0 93,3 6,7 0 100 0 0

Изох: АН – аниқланмаган, НТ – нотасодифий, ТС – тасодифий кетма-кетликлар;

Қуйида С++ дастарлаш тилида яратилган ТРГ ни матнини келтирамиз:

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#define NUM_TESTS 100000000
int randomNumber(int hi)  // Қийматлар соҳаси учун тўғри ТРГ [0,hi]
{
// Қийматлар соҳасини олиш [0,1)
const float scale = rand()/(float)RAND_MAX;
// Қиймтни қийматлар соҳасига қайтариш [0,hi]
return (int)(scale*hi + 0.5); // сони каср қисмини олиб ташлаш ва
аниқланмаган типга ўтказиш
}
int main(void){
   int counters[2][10] = { 0 }, i;
   srand(time(NULL));
   for ( i = 0; i < NUM_TESTS; ++i ){
      ++counters[0][rand() % 10];
      ++counters[1][randomNumber(9)];
}
printf("Distribution of %d numbers from 0 to 9:\n", NUM_TESTS);
printf("#       Use %%          Use function\n");
for ( i = 0; i < 10; ++i )
printf("%d%15d%15d\n", i, counters[0][i], counters[1][i]);
return 0;
} [60]
```

Кўрсатиб ўтилган фикрлар, мулохаза ва мисоллардан келиб чиқиб, ТРГ ларни ишлаб чиқиш, тахлил қилиш ва уларни ахборот хавфсизлиги ва уларни ҳимоялаш сохасига қўллаш амалий жихатдан ўз ўрнига эга эканлигини кўришимиз мумкин.

4.2. Ахборотларни ҳимоялаш муаммолари бўйича Borland Delphi дастурлаш тилида яратилган тасодифий рақамлар генераторини сифатини тадқиқ этиш.

Ушбу бўлимда тасодифий рақамлар генераторлари сифатини тахлил қилиш усулларини Delphi дастурлаш тилида қандай амалга оширилиши тўғрисида маълумотлар бериб ўтамиз.

Delphi дастурлаш тилида тасодифий рақамлар генераторлари Randomize процедураси орқали амалга оширилади. Бу процедура ТРГ ишлаб чиқаришни таъминлаш процедураси бўлиб, RandSeed ўзгарувчиси билан бирга ишлайди.

Delphi дастурлаш тилида ушбу процедура ва узгарувчи функциялари асосида тасодифий рақамларни ишлаб чиқариш доимий равишда ижобий натижа бериши учун уларни тўғри ишлатиш мақсадга муофиқдир.

Тасодифий рақамни олиш:

Тасодифий рақамни олиш учун Random функциясидан фойдаланиш лозим. Унинг сарлавхаси қуйидагича:

function Random [(Range: Integer)];

Агар функцияга параметрларсиз мурожат қилинса, у Real типидаги курсатиган диапозондаги қийматларни қабул қилади:

0 <= X < 1

Агар параметрида бутун сон k кўрсатилса, функция бутун қийматларни қуйидаги диапазонда қабул қилади:

0 <= X < k,

ёки, қуйидагича ёзиш мумкин:

0 <= X <= k-1

Шуни таъкидлаб ўтиш керакки, Random функциясини ишлатиш компилятр версиясига боғоиқ равишда ўзгаришим мумкин. Шунинг учун бу функциядан шфрлашда фойдаланиш тавсия этилмайди.

Random функциясидан фойдаланишга мисол.

Биз катта бўлмаган тирни йиғишимиз мумкин, яъни Image тасвирида таймер ва ТРГ дан фойдаланилади.

Формага Timer1 ни ва Image1 тасвирни қўямиз ҳамда ходисаларни қайта ишлаш учун OnTimer ни ёзамиз.

```
procedure TForm1.Timer1Timer(Sender: TObject);
begin
Randomize; //ТРГ ни ишга туширамиз.
Image1.left:=Random(Form1.width);
Image1.top:=Random(Form1.height);
end;
```

Биз шунчаки хар сафар тасвирни кординаталарини тасодифий тарзда алмаштирамиз, қайсики форма бўйлаб тартибсиз харакатдаги тасвирни.

Энди тасвирга тегиш реакциясини ишлаб чиқамиз. Тасвир учун OnClick ходисасини ишга туширамиз:

```
procedure TForm1.Image1Click(Sender: TObject);
begin
Timer1.Enabled:=false; //остановим таймер
Showmessage('Попадание в цель!'); Timer1.Enabled:=true; //запустим его обратно end;
```

Бу ерга очколарни, тасвирни харакатланиш вақтини ва бошка шу каби ўйин шартларини ўрнатиш мумкин. Ўйин тезлигини ортириш учун таймер Interval ни камайтириш етарли.

Шу тартибда оддий ўйин яратилиши мумкин.

Массивни Random ёрдамида тўлдириш.

```
Randomize;
// массивни тўлдириш
for i:= 1 to 10 do a[i]:=Random(10);
//Массив учун форма киритамиз
for i:= 1 to 10 do Canvas.TextOut(10+10*i,10,IntToStr(a[i]));
```

Массив таркибида хамма вақт ноижобий элементлар бўлиши мумкин, шунинг учун массивни ноижобий элементларни ҳисобга олиб тўлдириш учун қуйидагича ёзиш мумкин:

```
for i:= 1 to 10 do a[i]:=Random(20)-10;
```

шу йўл билан массив қийматлари (-10 .. 9) диапазонни қабул қилади.

Тасодифий рақамни RandSeed ёрдамида олиш:

ТРГ ларни ишга тушириш ва тасодифий рақамни олишни Randomize процедурсини қўлламасдан ҳам олиш мумкин. Бу RandSeed ўзгарувчиси ёрдамида амалга оширилиши мумкин. масалан:

```
procedure TForm1.Button1Click(Sender: TObject);
var RandSeed: LongInt;
begin
RandSeed:=random(10);
ShowMessage(IntToStr(RandSeed));
end; [62]
```

4.3. Ахборотларни ҳимоялаш муаммолари бўйича Visual Basic дастурлаш тилида яратилган тасодифий рақамлар генераторини сифатини тадқиқ этиш.

Visual Basic дастурлаш тилида тасодифий рақамлар генераторлари Randomize процедураси орқали амалга оширилади. Бу процедура ТРГ ишлаб чиқаришни таъминлаш процедураси бўлиб, Rnd ёрдамида ҳам амалга оширилиши мумкин.

Visual Basic дастурлаш тилида ушбу процедура ёрдамида тасодифий рақамни олиш ва ТРГ ларни қуришга бир неча мисолларни кўриб чиқамиз:

Таймер учун ТРГ

```
Option Explicit
Dim tr As Boolean
Dim i
Dim m(35)
 Private Sub Command1_Click()
Timer1.Interval = 1000
Timer1.Enabled = Not (Timer1.Enabled)
tr = Timer1.Enabled
End Sub
 Private Sub Command2_Click()
Randomize
tr = False
Timer1.Interval = 1
Timer1.Enabled = True
End Sub
 Private Sub Form_Load()
Timer1.Enabled = False
'Timer1.Interval = 1000
For i = 65 To 90
m(i - 64) = Chr(i)
Next i
For i = 0 To 9
m(i + 26) = i
Next i
End Sub
Private Sub Timer1_Timer()
Dim a, b, c
a = "": b = "": c = ""
For i = 1 To 4
```

```
a = a & m(Int(Rnd * 35) + 1)
b = b & m(Int(Rnd * 35) + 1)
c = c & m(Int(Rnd * 35) + 1)
Next i
Label1 = a & "  " & b & "  " & c
Timer1.Enabled = tr
End Sub
```

Рақамларни XXX-XXX-XXX-XXX типида генерациялаш:

```
Public Class Form1
    Dim i, l, m, o, p, r, s, t, w, e, g, h, k As Integer
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button1.Click
        i = (Int(Rnd() * 9))
        l = (Int(Rnd() * 9))
        m = (Int(Rnd() * 9))
        o = (Int(Rnd() * 9))
        p = (Int(Rnd() * 9))
        r = (Int(Rnd() * 9))
        s = (Int(Rnd() * 9))
        t = (Int(Rnd() * 9))
        w = (Int(Rnd() * 9))
        g = (Int(Rnd() * 9))
        h = (Int(Rnd() * 9))
        k = (Int(Rnd() * 9))
        TextBox1.Text = i & l & m & -o & p & r & -s & t & w & -g & h & k
    End Sub

    Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
```

```
    Randomize()
  End Sub
End Class [63]
```

4.4. 1c 8.2. бухгалтерия платформасида тасодифий рақамлар генераторини қўлланилиши.

1c 8.2. бухгалтерия платформасида турли мақсадларда ТРГ лардан фойдаланиш мумкин. Масалан, фойдаланувчиларга кириш паролларини ташкил қилишда, хужжатларни тасодифий танланишини амлага оширишда ва бошқа шу каби ишларни ташкил қилишда тадбиқ қилиш мумкин. Қуйида мисолларни кўришимиз мумкин:

1. Парол олишда:

```
СтрокаСимволов =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456
789+/";
ДлинаПароля = 8;
СтрокаНовогоПароля = "";
Для зы = 1 по ДлинаПароля Цикл
 СтрокаНовогоПароля  = СтрокаНовогоПароля +
ред(СтрокаСимволов,СлучайноеЧисло(64),1);
КонецЦикла;
Вовзрат СтрокаНовогоПароля ;
```

2. ТРГ ни ташкил қилиш:

```
А) вариант
ГСЧ = Новый ГенераторСлучайныхЧисел();
СлучайноеЧисло = ГСЧ.СлучайноеЧисло(0, 1000);
```

3. Уникал идентификацион рақам олиш:

```
Функция Рандом() Экспорт
```

```
UID=Новый УникальныйИдентификатор();
UID = СтрЗаменить(UID,"-","");
Значение = "";
Для Н=1 По СтрДлина(UID) Цикл
Симв = Сред(UID,Н,1);
Значение = Значение+Прав(КодСимвола(Симв),1);
КонецЦикла;
Возврат Число("0."+Значение);
КонецФункции
```

В) вариант

```
Функция Ранд(Парам=0)
   Если Парам<>0 Тогда
      Случай=Парам;
   КонецЕсли;
   Если Число(Случай)=0 Тогда
      Случай=Число(СтрЗаменить(""+ТекущееВремя(),":",""));
      Случай=(16807*Случай)%2147483647;
   КонецЕсли;
   Случай=(16807*Случай)%2147483647;
   Случай=макс(Случай,-Случай);
   Возврат(Случай/2147483647);
КонецФункции   [64]
```

4.5. “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ лари учун 1с 8.2. бухгалтерия платформасида қайта ишланган бухгалтерия дастури мисолида тасодифий рақамлар генераторини қўллаш.

Хавфсизлик муаммоси, аслида, янги муаммо эмас, чунки хавфсизлигини таъминлаш хар қандай система учун, унинг мураккаблиги, табиатидан қатъий назар, бирламчи вазифа ҳисобланади. Аммо, ҳимояланувчи объект информацион система бўлса, ёки агрессив таъсир воситалари информацион шаклда бўлганда, ҳимоянинг мутлоқ янги технологияларини ва методларини яратишга тўғри келади. Айниқса кўпчилик фойдаланадиган вақти бўлинувчи системаларда ҳамда алоқанинг оддий телефон линияси ёки очиқ компьютер тармоқлари орқали фойдаланувчи системаларда ҳимоя воситаларига бўлган талаб янада юқорироқ бўлади. Маълумотларни ҳимояловчи методлар хамда хакерларга қарши харакат воситалар мажмуасини белгилаш мақсадида *компьютер хавфсизлиги* атамаси ишлатила бошланди.

Маълумотларни ишловчи тақсимлан-ган системаларнинг пайдо бўлиши хавфсизлик масаласига янгича ёндашишнинг шаклланишига олиб келди. Маълумки, бундай системаларда тармоқлар ва коммуникацион ускуналар фойдаланувчиларнинг терминаллари билан марказий компьютерлар ўртасида маълумотлар алмашишга хизмат қилади. Шу сабабли маълумотлар узатилувчи тармоқларни химоялаш зарурияти туғилди ва шунинг билан бирга *тармоқ хавфсизлиги* атамаси пайдо бўлди. Бунда алохида олинган локаль тармоқ эмас, балки маълумотларни ишловчи бирлашган тармоқ билан боғланган корхона, хукумат идоралари ва ўқув юртлари тармоқларининг мажмуаси кўзда тутилади. Таъкидлаш лозимки, компьютер ва тармоқ хавфсизлиги ўртасида аниқ чегара қўйиб бўлмайди. Масалан, компьютер системасининг вирус билан заҳарланишидан сўнг, вирусни аниқлаш ва йўқотишда компьютер хавфсизлигининг локал воситаларидан фойдаланишга тўғри келади.

Бирлашган тармоқларда ишлаш хавфсизлигининг мураккаблигига қуйидаги мисоллар орқали ишонч ҳосил қилиш мумкин.

1. Информацияни узатишда хавфсизликни таъминлашга қўйиладиган талабларни бевосита қуйидаги атамалардан аниқлаш мумкин: конфиденциалик, аутентификация, яхлитликни сақлаш, ёлғоннинг мумкин эмаслиги, фойдаланувчанлик, фойдаланувчанликни бошқариш.

2. Кўп ҳолларда яратувчи эътиборидан четда қолган ҳимоя системасининг камчиликларини аниқлаш мақсадида муаммога қарши томоннинг нуқтаи назаридан қараш лозим. Бошқача айтганда, ҳимоянинг у ёки бу механизми ёки алгоритмини яратишда мумкин бўлган қарши чораларни ҳам кўриш лозим.

3. Ҳимоя воситаларидан барча қарши чоралар мажмуасини ҳисобга олган ҳолда

фойдаланиш лозим.

4. Хавфсизликни таъминлаш чоралари системаси яратилганидан сўнг бу чораларни қачон ва қаерда қўллаш масаласини ечиш лозим. Бу физикавий жой (маълум ҳимоя воситасини қўллаш учун тармоқ нуқтасини танлаш) ёки хавфсизликни таъминловчи мантиқий занжирдаги жой (масалан, информация узатувчи протокол сатхи ёки сатхларини танлаш) бўлиши мумкин.

5. Ҳимоя воситалари, одатда, маълум алгоритм ва протоколдан фарқланади. Уларга биноан барча ҳимоядан манфаатдор информациясининг қандайдир қисми махфий бўлиб қолиши шарт(масалан, шифр калити кўринишида). Бу эса ўз навбатида бундай махфий информацияни яратиш, тақсимлаш ва ҳимоялаш методларини ишлаб чиқиш заруриятини туғдиради.

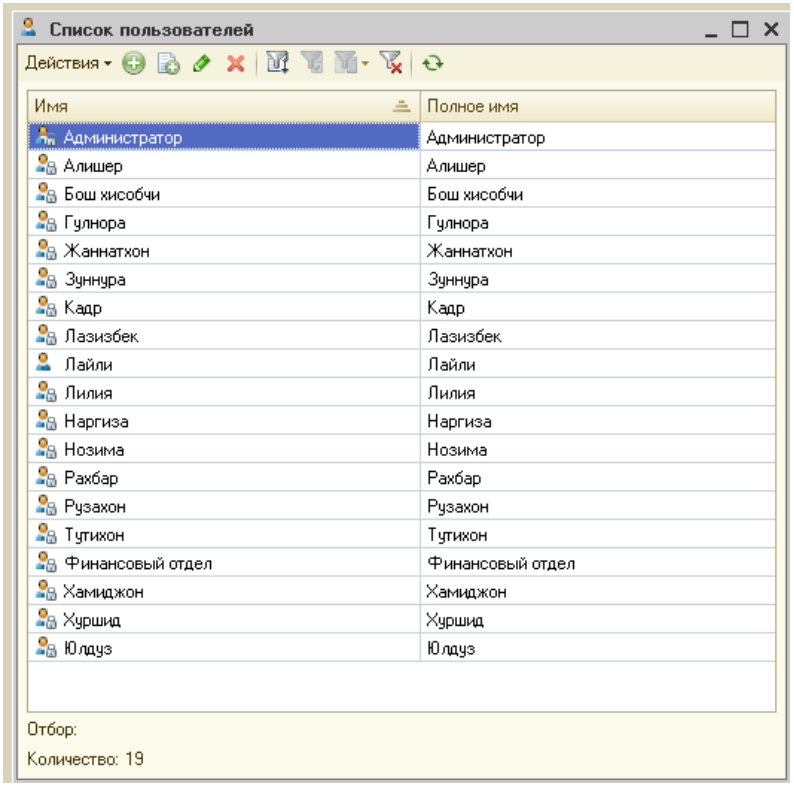
Бўндай махфий информацияни яратиш, тақсимлаш ва ҳимоялаш методларини ишлаб чиқиш зарурияти турли ташкилотларнинг турли соҳалари учун қўлланилаётган дастурий воситаларни тузилиши ва характерларига боғлиқ бўлади. Масалан, ишлаб чиқариш ташкилотларида ишлаб чиқариш дастгох ва роботларини бошқариш дастурлари, турникет ва

ходимлар назорати дастурлари, тарози ва сигнализация дастурлари ҳамда бухгалтерия ҳисобини юритиш дастурлари бўлиши мумкин.

1с8.2.Бухгалтерия платформасида “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ лари учун бухгалтерия учун қайта ишланган бухгалтерия дастурига тасодифий рақам генераторини (ГСЧ) ни қўллаб, Рандом функцияси ёрдамида яратилган фойдаланувчилар учун химоялаш генерациялари яратилди.

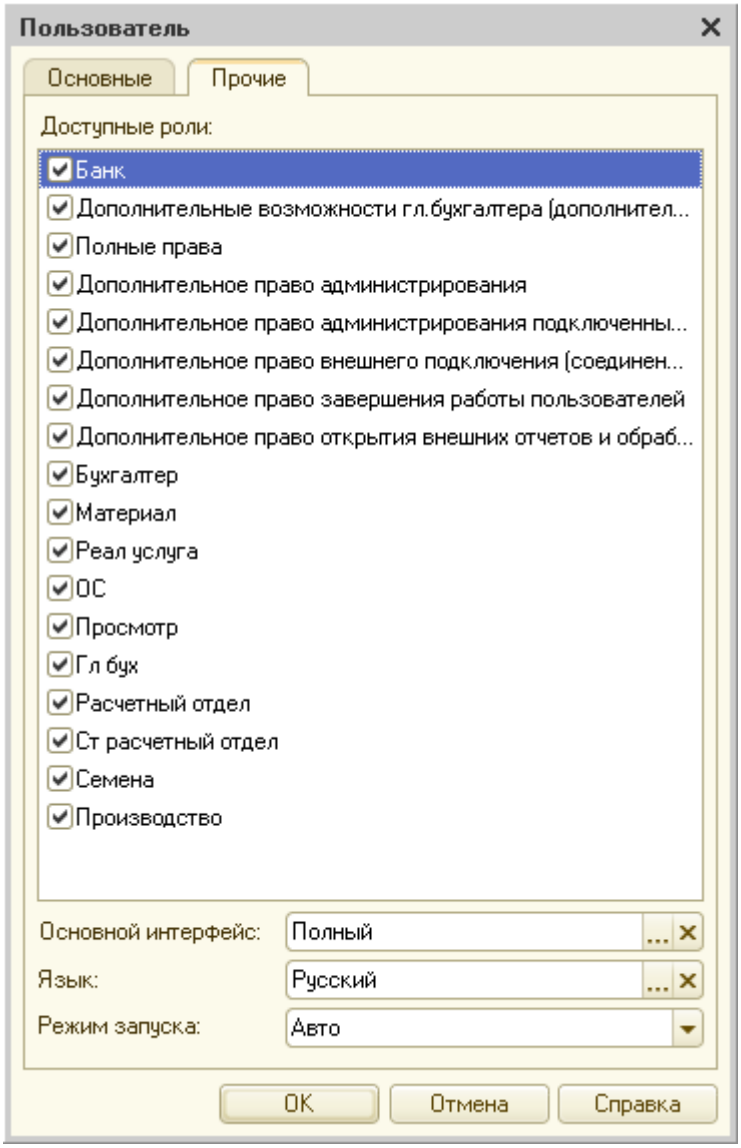
Генерация асосида олинган тасодифий рақамлар ёрдамида фойдаланувчиларнинг идентификацион рақамлари белгиланади ва ўзларини калит (парол) билан солиштириш натижасида фойдаланувчини маълумотлар базасига кириш рухсатини амалга оширади.

Ҳар бир ташкилотнинг ўз фойдаланувчилар сони бўлиб, уларни дастурда бажарадиган ишлари ва роллари аниқ қилиб белгилаб қўйилган бўлади. (13 ва 14-расмларга қаранг) Масалан, “Фарғонаёғмой” МЧЖ бухгалтерия дастурида фойдаланувчилар сони:



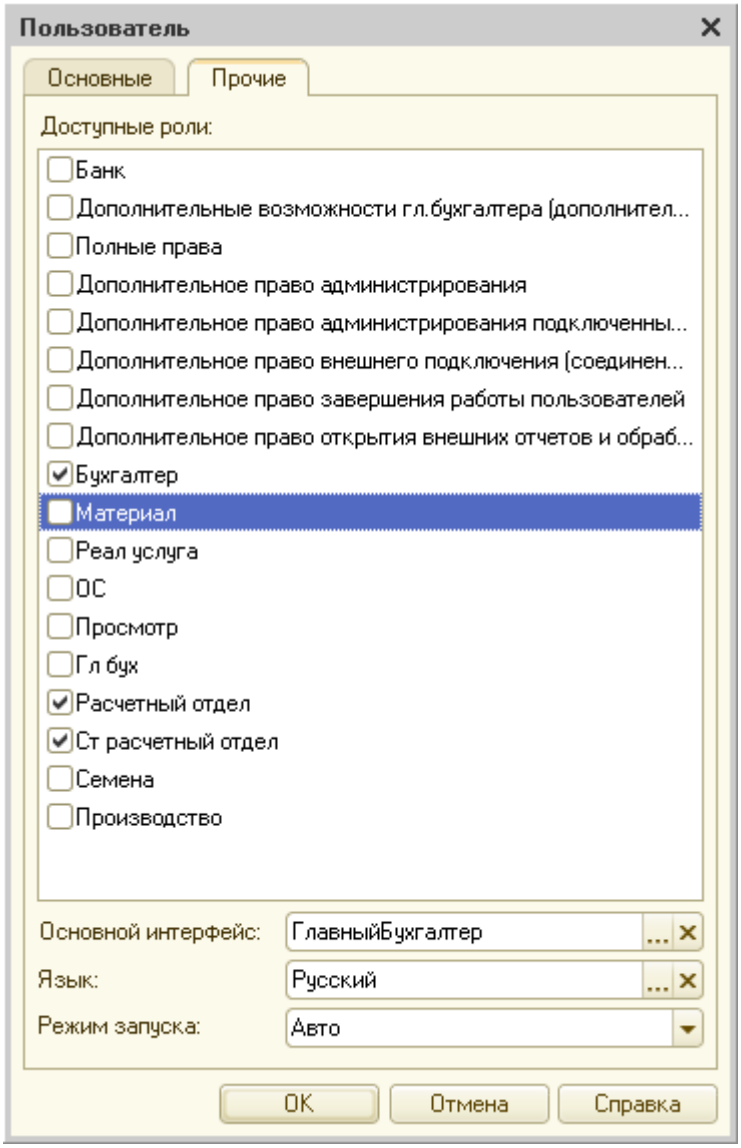
13-расм. “Фарғонаёғмой” МЧЖ бухгалтерия дастуридан фойдаланувчилари.

Уларнинг роллари:



14-расм.Фойдаланувчиларга бериладиган роллар.

Белгиланган роллар кўрсатилган тартибда тўлиқ қўйилган бўлса, шу фойдаланувчи тўлиқ имкониятли рухсат доирасига эга бўлади. Бундай ролни дастур администратори, масъул шахс ёки махсус ходимларга бериш тавсия қилинади. Сабаби, фойдаланувчи ўзига берилган рухсатлар доирасида конифигурацияни бошқариш ҳуқуқига эга бўлиб, ишлаб чиқарилган дастурий ГСЧ ни қўллаш натижасида олинган рақамларни қайта олиш ёки чеклаш имкониятини эга бўлиши мумкин. Шунинг учун, хар бир фойдаланувчини бажарадиган иши ва ўрнига боғлиқ равишда рухсатлар доираси белгиланиши лозим. Мисол, иш хақи бўлими ҳисобчиларига ўрнатилган ролларни кўрамиз:



15-расм. Ролларни ўрнатилиши.

1с8.2.Бухгалтерия платформасида “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ лари учун бухгалтерия учун қайта ишланган бухгалтерия дастурига тасодифий рақам генераторини (ГСЧ) ни қўллаб, Рандом функцияси ёрдамида яратилган фойдаланувчилар учун химоялаш воситалари ушбу жойларда амалиётда синовдан ўтказилди.

1с8.2.Бухгалтерия платформасида “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ лари учун яратилган бухгалтерия дастури маълумотлар базасини химоялашда тасодифий рақамлар генераторини қўллаш учун идентификацион рақам сифтида қаддиқ дискни ишлаб чиқарган завод томонидан қўйилаган серия рақами асос қилиб олинди.

Ушбу илова базага дастур ўрнатилгандан сўнг юкланади. Агар фойдаланувчилар бирон сабаб билан базани ёки дастурни бошқа компьютерга кўчиришга ҳамда ўзгартириш ишларини рухсатсиз бажаришга харакат қилганда жорий база берикитилади (блокировка қилинади). Ушбу холатда ёзилган генератор ёрдамчи дастури орқали қаттиқ дискни серия рақами аниқлаштирилиб, шу серия номери учун алохида активлаштириш рақами генерация қилиниши талаб қилинади. Агар идентификацион рақам, яъни бизда қаттиқ дискни серия рақами аниқлаштирилмаса унди аутидентификацион рақам, яъни бизда генерация рақами берилмайди. Бошқача айтганда генерация ишламайди ҳамда дастурни активлаштириш жараёни тўхтатилади.

Генераторни интерфейси ва дастур матни 1-ИЛОВА, 2-ИЛОВА, 3-ИЛОВАларда кўлиқ кўрсатиб ўтилган.

IV-боб бўйича хулоса.

Кўриб ўтилган айни бобда Ахборотларни ҳимоялаш муаммолари бўйича с++ дастурлаш тилида яратилган тасодифий рақамлар генераторини сифатини тадқиқ этиш, ТРГларини дастурлаш тилларида рақамларнинг кетма-кетлик сифатини таққослаш ёрдамида тахлил қилиш, С++ тилида (яъни Builder 2006 дастурий доирада) ёки С# тилида (Visual Studio 2008 дастурий доирада) қўллаш ишлари кўрсатилган.

Ушбу бўлимда тасодифий рақамлар генераторлари сифатини тахлил қилиш усулларини Delphi дастурлаш тилида қандай амалга оширилиши ва ТРГ процедураларини қўллаш ёртилган.

Шунингдек Visual Basic дастурлаш тилида тасодифий рақамлар генераторлари Randomize процедураси орқали амалга оширилиши изохланиб, уни қўллашни амалий жихатдан очиб беришга эришлиган.

ТРГ ларни 8.2. бухгалтерия платформасида турли мақсадларда қўллаш мумкинлигини кўрсатилиб, “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ лари учун 1с 8.2. бухгалтерия платформасида қайта ишланган бухгалтерия дастури мисолида тасодифий рақамлар генераторини қўллаш ёртилган.

ХУЛОСА

XXI асрни хақиқатдан “ахборот” асри деб тан олиниши бежиз эмас. Чунки бугунги кунда замонавий ахборот технологияларини интенсив тарзда ривожланиб бориши янги ахборотни қайта ишлаш воситалари, ахборот хавфсизлиги муаммолари, ахборотни ҳимоя қилиш тизимлари, таълим тизими ҳамда жамиятимизнинг турли сохларида уларни қўллаш ва усулларини яратиш ушбу масалаларни долзарблигини вужудга келтиради. Шу нуқтаи назардан хар бир ташкилот ва корхоналарни ўзига тегишли ахборот тизимлари ва технологияларидан тўғри, самарали, муваффақиятли фойдаланиши уларни қандай ва нима асосга қурилишига боғлиқдир. Хозирги кунда қўлланилаётган кўплаб ахборотларни қайта ишлаш воситалари тасодифий рақамлар генераторлари (ТРГ) асосида қурилмоқда. Масалан тест ўтказиш ва ўқитишнинг компьютерли дастурларида тасодифий герациялаш, электрон рақамли имзо (ЭРИ) олишда калит хабарларини генерациялаш, ахборотни ҳимоялашда генерация, компьютер графикасида ранглар генерацияси, криптографияда киптоалгаритмларни тузиш ва шу каби бошқа мисолларни келтириш мумкин.

Ўзбекистон Республикасида ахборот технологиясининг миллий инфраструктураси жадаллик билан ривожланмоқда. Бу республикамизнинг мустақилликка эришганидан бери жамиятимиз ҳаётида тубдан ўзгаришлар содир бўлганидан дарак берадики, ҳозирда иқтисодиёт, телекоммуникация соҳаси ахборот индустрияси олдидаги мақсад ва масалалар ўзгарди. Ҳажми муттасил ошувчи ахборотни сақлаш ва узатиш жараёнларини автоматлаштириш масаласини ечишга имкон берувчи компьютер тармоқлари маълумотларини автоматлаштирилган ишлаш воситаларининг пайдо бўлиши ва тарқалиши ушбу жараёнларни тажовузкор ахборот таъсирига нисбатан заиф қилиб қўйди. Натижада файлларни ва компьютерда сақланувчи бошқа ахборотни ҳимоялаш воситаларига эҳтиёж туғилди. Айниқса кўпчилик фойдаланувчи тизимларда, вақти бўлинишли тизимларда ҳамда очиқ

тармоқлар орқали фойдаланувчи тизимларда ҳимоялаш воситаларига эҳтиёж кучли сезилди.

Тадқиқотчи ташкилотлар томонидан тақдим этилган хавфсизлик бузилишининг статистикасига биноан бузилишларнинг экспоненциаль ўсиши кузатилмоқда. Ушбу бузилишлар пайдо бўлиши сабабларининг чуқур тахлили бу бузилишлар компьютер тармоқларини яратиш босқичида йўл тутилган хатоликлар натижаси эканлигини кўрсатди. (8% - талаблар тахлили; 56 % - лойиҳалаш; 16 % - амалга ошириш ва фақат 17% - эксплуатация). Аммо, компьютер тармоқларини ҳимоялаш воситаларининг аксарият камчиликлари фойдаланишни назорати билан боғлиқ – 89%. Идентификация/аутентификация ва яхлитликни назоратлашга хатоликларнинг жуда кам қисми тўғри келади. Демак, компьютер тармоқлари хавфсизлигининг бузилишига олиб келувчи заифликларнинг пайдо бўлиш сабаби – тармоқни қуришнинг дастлабки босқичларида йўл қўйилган хатоликлар натижасидаги яратилувчи фойдаланишни назоратловчи ва бошқарувчи тизимлар сифатининг пастлигидир. Бундай вазиятдан қутилиш учун ҳимояланган компьютер тармоқларини қуришда, айниқса лойиҳалаш босқичида, хавфсизликнинг формал моделларидан фойдаланиш лозим.[65]

Маълумки, ҳар қандай давлатнинг ахборот ресурслари унинг иқтисодий ва ҳарбий салоҳиятини белгиловчи омилларидан бири ҳисобланади. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантирилишини таъминлайди. Бундай жамиятда, ахборот алмашинув тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот коммуникациялар технологияларини қўллаш кенг кўламда амалга оширилади.

Ахборотлашган жамият тезлик билан шаклланиб бормоқда. Ахборот дунёсида давлат чегаралари деган тушунча йўқолиб бормоқда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда.

Ҳудудий жойлашишидан қатъи назар, кундалик ҳаётимизга турли хилдаги ахборотлар Internet халқаро компьютер тармоғи орқали кириб келди. Шунинг учун ҳам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва ўзгартириш, йўқотиш каби муаммолардан ҳимоя қилиш долзарб масала бўлиб қолди. Ахборотлаштириш соҳасидаги давлат сиёсати ахборот ресурслари, ахборот технологиялари ва ахборот тизимларини ривожлантириш ҳамда такомиллаштиришнинг замонавий жаҳонтамойилларини ҳисобга олган ҳолда миллий ахборот тизимини яратишга қаратилган [66]

Келтирилган фикр ва мулохазалар асосида диссертация ишини ёртиш жараёнида ишлаб чиқариш учун дастурий таъминот яратишда ахборотларни ҳимоялаш муаммолари бўйича дастурлаш тилларида қўлланиладиган тасодифий рақамлар генераторлари сифатини тадқиқ этиш ва маълумотларнинг муҳофазасини таъминловчи аппарат-дастурий криптографик воситаларда қулай ҳамда самарали қўлланувчи криптобардошли ТРГ лар алгоритмларини яратиш, уларнинг самарадорлигини баҳолаш усулларини ва дастурий таъминотларини таклиф этилди. Натижада ўз олдига қўйган бир қатор вазифаларни бажаришга муваффақ бўлди:

1. Мавжуд ахборот хавфсизлиги муаммоларини ўрганиш ва яратиш йўналишларини туркумланди.
2. Ахборот хавфсизлигини таъминлашнинг асосий йўллари ҳамда хуқуқий ва ташкилий таъминотини назарий жихатларини ўрганилди.
3. Ахборотни ҳимоялашнинг криптографик усуллари, криптографик воситаларида самарали қўлланувчи криптобардошли акслантиришлардан фойдаланиб ТРГ алгоритмларини яратиш ва жараён босқичларининг функционал схемасини тузилди
4. Яратилган алгоритмларнинг самарадорлигини баҳолаш талабларини ва усулини ишлаб чиқилди.

5. Тасодифий рақамлар генераторлари ва уларнинг турларини ўрганиш ва шу асосида янги кўринишдаги криптобардошлик ва самарадорликни баҳолаш усулларининг дастурий таъминотларини ишлаб чиқилди
6. Псевдотасодифий кетма-кет рақамли генереторларни тузилиши ва хусусиятларини ўрганиш ва янги характерли псевдотасодифий ТРГ лар таклиф қилинди.
7. Тасодифий рақамлар генераторлари сифатини бахолаш мезонларини ишлаб чиқиш асосида юқори тезликдаги квантли тасодифий рақамлар генераторлари ва ахборотларни ҳимоя қилиш услубларини яратилди.
8. Яратилган ТРГ криптографияда ва ахборотни ҳимоялаш тизимларида қўллаш алгоритмларнинг криптобардошлиги ва самарадорлиги кўрсаткичлари хақида аниқ натижаларга эришилди.

Диссертация доирасида яратилган дастурий таъминот, 1С8.2 дастурий платформаси мисолида Ўзбекистон Республикаси ишлаб чиқариш корхоналарида, жумладан “Фарғонаёғмой” МЧЖ, “Фарғонапиво” МЧЖ ва “Қувасойшифер” АОЖ ларида бухгалтерия ҳисоби бўйича олинган маълумотларни ҳимоялашга тадбиқ этилди. Ундан ташқари Фарғона компьютер технологиялари касб-ҳунар коллежи, ФарДУ қошидаги академик лицейнинг ўқув жараёнида қўлланилди ва тадбиқ этилди. Бажарилган ишлар ва ўтказилган илмий тадқиқот натижаларига асосланиб, келгусида ушбу магистрлик диссертацияси ахборот технологияларининг ривожига ўзининг оз бўлсада хиссасини қўшади.

Зеро, мухтарам юртбошиз Ислом Каримов “XXI аср – шиддаткор, тезкорлик асри, ахборот ва ахборот технологиялари асри, интелектуал ресурслар, юксак технология ва замонавий билимлар инсоният тараққиётининг асосий ва хал қилувчи омилларига айланган давр” деб таъкидлаб ўтганлар. [67]

Ушбу фикрлардан келиб чиқиб, Тошкент ахборот технологиялари универстиети Фарғона филиали магистрлари ва олимлари томонидан замонавий тасодифий рақамлар генераторларини жамиятимизни турли

сохаларига жумладан ахборот хавфсизлиги муаммоларини бартараф қилишда қўллаш борасида дастурий воситалар ва илмий изланишлар устида олиб борилаётган ишлари илм-фаннинг ривожи ва мамлакатимиз турмиш тарзини ислоҳ қилишда ўз ўрнига эгадир.*

* Диссертация ишини тщлиы мазмунини ёртишда фойдаланилган адабиётлар рщйхатида берилган 68 дан 92 рақамгача бўлган адабиётлар ва интернет ресурсларидан қўшмча манба сифатида фойдаланилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. *Каримов И.А.* Мамлакатимизда демократик ислоҳотларни янада чуқурлаштириш ва фуқаролик жамиятини ривожлантириш Концепцияси. – Т., 2010.
2. *Каримов И.А.* Мамлакатимизни модернизация қилиш ва иқтисодиётимизни барқарор ривожлантириш йўлида. Т.16. – Т., 2008.
3. Ғаниев С.К., Каримов М.М. “Ҳисоблаш системалари ва тармоқларида информация ҳимояси. Олий ўқув юртлари учун ўқув қўлланама. Тошкент Давлат Техника университети, 2003 йил.
4. Мусаев А.И. «Узлуксиз шифрлашнинг криптобардошли алгоритмлари ва уларнинг самарадорлигини баҳолаш», илмий тадқиқот иши, Тошкент 2011 й. (Илмий мақола ва тадқиқот)
5. Ўзбекистон Республикаси Президенти И.А. Каримовнинг 2007 йил 3 апрелдаги ПҚ-614–сон «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» қарори.
6. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С, часть 3. - М.: Триумф, 2002. - 816 с.
7. Ғаниев С.К., Каримов М.М. “Ахборот хавфсизлиги”, Олий ўқув юртлари учун ўқув қўлланама. Тошкент 2012 йил.
8. Ўзбекистон Республикаси қонун ҳужжатлари тўплами. – 2012. – № 52.– 583-м.
9. Каримов И.М., Тургунов Н.А., Кадиров Ф. ва бошқалар “АХБОРОТ ХАВФСИЗЛИГИ АСОСЛАРИ”, маърузалар курси, ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ИЧКИ ИШЛАР ВАЗИРЛИГИ А К А Д Е М И Я, Тошкент-2013 й.
10. Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – №5. – 136-м.

11. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С, часть 3. - М.: Триумф, 2002. - 816 с.
12. Иванов, М.А. Криптографические методы защиты информации / М.А. Иванов.- М.: КУДИЦ-ОБРАЗ, 2001.-368с. (Илмий мақола ва тадқиқот)
13. Варфоломеев, А.А. Управление ключами в системах криптографической защиты банковской информации / А.А. Варфоломеев, О.С. Домина, М.Б. Пеленицын.- М.: МИФИ, 1996.- 128 с. (Илмий мақола ва тадқиқот)
14. Месси, Дж.Л. Защита информации. Введение в современную криптологию / Дж.Л. Месси//ТИИЭР.- 1988.-Т.76.-№5.- С.24-41. (Илмий мақола ва тадқиқот)
15. Хоффман, Л.Дж. Современные методы защиты информации / Л.Дж. Хоффман.-М.: Советское радио, 1980.-264 с.
16. Шифрование — асимметричные методы. Глава 8 ("Шифрование с открытым ключом", "Обмен ключом без обмена ключем", "Криптографическая стойкость", "Задача Диффи-Хеллмана и задача дискретного логарифмирования")
17. Брюс Шнайер. Прикладная криптография
18. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.
19. Кон П. Универсальная алгебра. - М.: Мир. - 1968.
20. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002.
21. Ричард Э. Смит Аутентификация: от паролей до открытых ключей = Authentication: From Passwords to Public Keys First Edition. — М.: Вильямс, 2002. — С. 432. — ISBN 0-201-61599-1 (Илмий мақола ва тадқиқот)
22. Anderson, B., TACACS User Identification Telnet Option. — December 1984.
23. Tardo J. and K. Alagappan SPX: Global Authentication Using Public Key Certificates. — M.California, 1991. — С. pp.232-244

24. А.А. Гладких, В.Е. Дементьев Базовые принципы информационной безопасности вычислительных сетей.. — Ульяновск: УлГТУ, 2009. — С. 156.
25. Ministerial Declaration on Authentication for Electronic Commerce 7–9 October 1998
26. CWA 14365. Guide of use of Electronic Signature. Jan.2003.
27. Homeland Security Presidential Directive 12 (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors. August 27, 2004.
28. NISTSpecialPublication 800-63 April 2006.
29. OECD Recommendation on Electronic Authentication. June 12, 2007
30. *Каримов И.А.* Ўзбекистон: миллий истиқлол, иқтисод, сиёсат,мафкура. Т.1. – Т., 1996.
31. *Каримов И.А.* Биздан озод ва обод Ватан қолсин. Т. 2. – Т., 1996.
32. *Каримов И.А.* Ватан саждагоҳ каби муқаддасдир. Т. 3. – Т., 1996.
33. *Каримов И.А*. Бунёдкорлик йўлидан. Т.4. – Т., 1996.
34. Архангельская Анна Васильевна. Диссертация на тему: “Построение высокоскоростных квантовых генераторов случайных чисел для систем защиты информации”. 2008 г.
35. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел. (Интернет ресурслари)
36. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/Аппаратный_генератор_случайных_чисел (Интернет ресурслари)
37. Псевдослучайные последовательности /http://www.hardline.ru/selfteachers/Info/Security/Protection_to_ information /6/Index5.htm. (Интернет ресурслари)
38. Колесова Н. А., Ажмухамедов И. М. Методика оценки качества последовательности случайных чисел // Вестн. Астрахан. гос. техн. ун-

та. Сер.: Управление, вычислительная техника и информатика. -2010. - № 2. - С. 141-148.

39. Ферапонтов М. М. Моделирование случайных воздействий на ЭВМ. М.: Изд-во МТУ, 1995.
40. Кнут Д. Э. Искусство программирования. - Т. 2. - М.: Вильямс, 2000. - 832 с.
41. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/Аппаратный_генератор_случайных_чисел. (Интернет ресурслари)
42. Колесова Н. А., Ажмухамедов И. М. Методика оценки качества последовательности случайных чисел // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. -2010. - № 2. - С. 164-171.
43. Свидетельство об официальной регистрации программы для ЭВМ № 2010614210. Программа для комплексной оценки качества последовательностей случайных чисел / Н. А. Колесова, И. М. Ажмухамедов; зарег. в реестре программ для ЭВМ 30.06.2010.
44. Сяо, Д. Защита ЭВМ / Д. Сяо, Д. Керр, С. Мэдник.- М.: Мир, 1982.-264 с.
45. Петров, В.А. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах / В.А. Петров, А.С.Пискарев, А.В. Шеин.- М.: МИФИ, 1995.- 84 с
46. Мафтик, С. Механизмы защиты в сетях ЭВМ / С. Мафтик.- М.: Мир, 1993.-216 с.
47. Об одном подходе к построению генератора случайных чисел. //А.В.Архангельская// Методы и технические средства обеспечения безопасности информации. Материалы XIII−Общероссийской научно-технической конференции. /сб.науч.тр./ Санкт-Петербургский государственный политехнический университет - СПб , 2004 - С 51 - Библиогр с. 51. (Илмий мақола ва тадқиқот)

48. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с. — ISBN 5-8459-0323-8, ISBN 1-57870-264-X. (Илмий мақола ва тадқиқот)
49. Шнайер Б. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С, часть 2. - М.: Триумф, 2002. - 524 с
50. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/Криптография. (Интернет ресурслари)
51. Материал из Википедии — свободной энциклопедии. http://ru.wikipedia.org/wiki/Генератор_псевдослучайных_чисел. (Интернет ресурслари)
52. Wikipedia: Random number generator attack. 2007. Retrieved Nov.27, 2007. (Интернет ресурслари)
53. *Каримов И.А*. Янгича ишлаш ва фикрлаш – давр талаби. Т. 5. – Т.,1997.
54. *Каримов И.А.* Хавфсизлик ва барқарор тараққиёт йўлида. Т. 6. –Т., 1998.
55. *Каримов И.А.* Биз келажагимизни ўз қўлимиз билан қурамиз. Т. 7.–Т., 1999.
56. *Каримов И.А*. Озод ва обод Ватан, эркин ва фаровон ҳаёт –пировард мақсадимиз . Т.8. –Т., 2000.
57. *Каримов И.А*. Ватан равнақи учун ҳар биримиз масъулмиз. Т. 9. 2001.
58. *Каримов И.А.* Хавфсизлик ва тинчлик учун курашмоқ керак. Т. 2002.
59. *Каримов И.А.* Биз танлаган йўл – демократик тараққиёт ва маърифий дунё билан ҳамкорлик йўли. Т. 11. – Т., 2003.
60. Haahr, M. 2007. Random.org. Retrieved November 27, 2007. Random.org. (Интернет ресурслари)
61. California Soil Resource Lab. 2007. Retrieved November 27, 2007. (Интернет ресурслари)
62. HotBits. 2007. Retrieved November 27, 2007. (Интернет ресурслари)
63. Wikipedia: Blum Blum Shub. 2007. Retrieved November 27, 2007. (Интернет ресурслари)

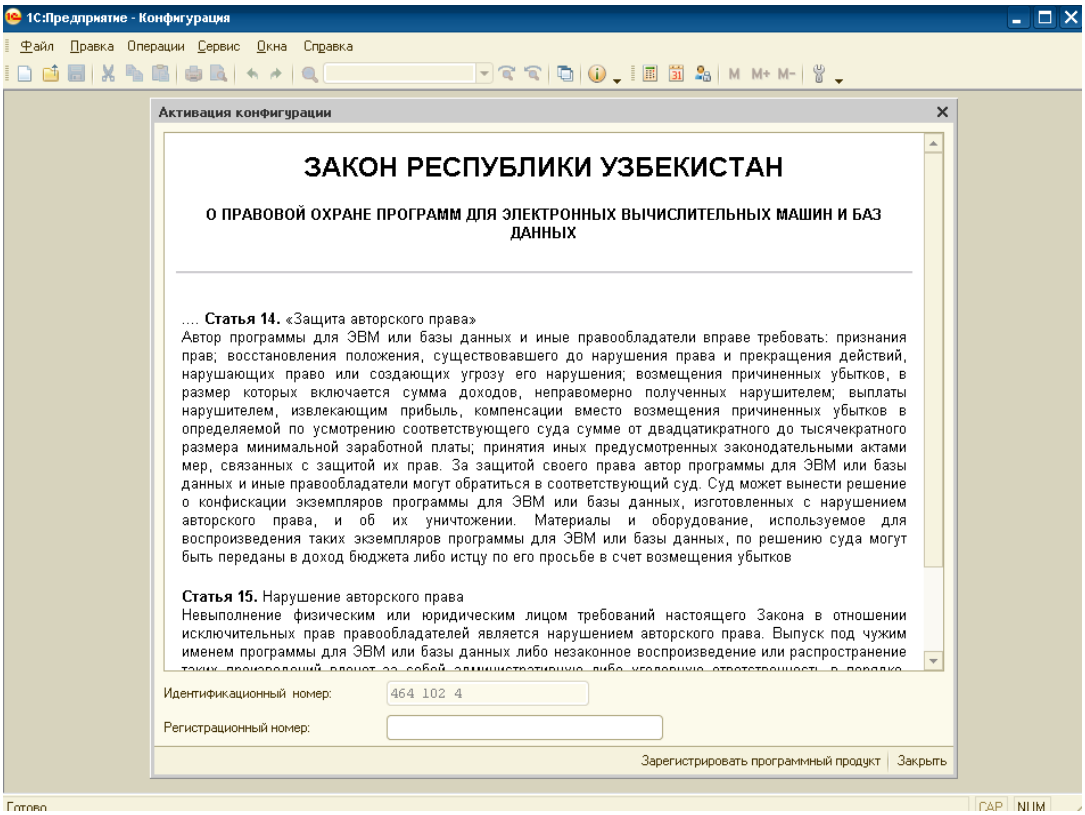
64. Bishop, M. 2004. Introduction to Computer Security. Prentice Hall PTR. (Интернет ресурслари)
65. Д.Я.Иргашева., “Компьютер тармоқларининг ҳимояланишини оширувчи фойдаланишни ролли чеклашли структуравий усуллар”, илмий тадқиқот иши, Тошкент 2012 й. (Илмий мақола ва тадқиқот)
66. Ўзбекистон Республикасининг «Ахборотлаштириш тўғрисида»ги қонуни// Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2004. – №1–2.– 10-м.
67. *Каримов И.А.*“Мамлакатимизни модеринизация қилиш ва иқтисодиётимизни барқарор ривожлантириш йўлида.” Т-16, Тошкент - 2008 й.
68. Методы генерации псевдослучайных чисел: Дзехо серес /Fushimi Masa-nori //ВЦП.-1980.-№Г-32668, Vol.21,№9.-P.968-974. (Илмий мақола ва тадқиқот)
69. Свидетельство об официальной регистрации программы для ЭВМ № 2010614210. Программа для комплексной оценки качества последовательностей случайных чисел / Н. А. Колесова, И. М. Ажмухамедов; зарег. в реестре программ для ЭВМ 30.06.2010. (Илмий мақола ва тадқиқот)
70. Псевдослучайные последовательности / http://www.hardline.ru/ selftea chers/Info/Security/Protection_to_ information /6/Index5.htm. (Интернет ресурслари)
71. Wikipedia: Random Number Generation. 2007. Retrieved November 27, 2007. (Интернет ресурслари)
72. Ўзбекистон Республикасининг «Давлат сирларини сақлаш тўғрисида»ги 1993 йил 7 май 848-XII-сон қонуни // Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси. – 1993. – №5. – 232-м.
73. Ўзбекистон Республикасининг «Электрон ҳисоблаш машиналари учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси тўғрисида»ги 1994 йил 6 май 1060-XII-сон қонуни //

74. Beker H., Piper F. Cipher Systems: The Protection of Communications. London Northwood Books, 1982.
75. Cover T. M. and King R. C. A Convergent Gambling Estimate of the Entropy of English // IEEE Transactions on Information Theory. v. IT-24, n. 4.-Jul 1978.-pp. 413-421.
76. Cover T.M., Thomas J.A. Elements of Information Theory. Wiley. -New York, 1991.
77. Devroye L., Gyorfi L., Lugosi G. A probabilistic theory of pattern recognition. — New York : Springer, 1996.
78. Kendall M.G., Stuart A. The advanced theory of statistics; Vol.2: Inference and relationship. London, 1961.
79. Knudsen L. R., Meier W. Correlations in RC6. // 1999. - http://www.ii.uib.no/~larsr/papers/rc6.ps
80. Knuth D.E. The art of computer programming. // Vol.2. — Addison Wesley, 1981.
81. Lehmann E.L. Testing Statistical Hypotheses. Wiley. - New York, 1959.
82. L'Ecuyer P., Simard R. Beware of linear congruential generators with multipliers of the form a = ±28 ± 2r. ACM Trans. Model. Comput. Simul. 25(3), 1999. - pp.367-374.
83. Marsaglia George, The Marsaglia Random Number CDROM // http://stat.fsu.edu/~geo/
84. Marsaglia G., Bray C., On-Line Random Number Generators and their Use in Combinations. Communications of the ACM, v. 11, m 11, 1968-pp. 757-759.
85. Maurer U. A universal statistical test for random bit generators // Journal of Cryptology. v.5, n.2, 1992. - pp. 89-105.
86. Menezes A., P. van Oorshot, Vanstone S. Handbook of Applied Cryptography. CRC Press. - 1997. - P. 780.
87. Nechvatal J. and others. Report on the Development of the Advanced Encryption Standart (AES). 2000. // http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

88. Park S. K., Miller K. W. Random Number Generators: Good Ones Are Hard to Find. // Communications of the ACM. v. 31, n. 10, Oct 1988.-pp. 1192-1201.
89. Peterson I. Monte Carlo Physics: A Cautionary Lesson. // Science News. v. 142, n. 25.- 19 Dec 1992.-p. 422.
90. Rogaway Phillip. Software-Optimized Encryption Algorithm// J. CRYPTOLOGY. 1998. - N 11. - p. 273-287.
91. Schneier B. Applied Cryptography. Wiley, 1996.
92. Shimoyama T., Takeuchi K., Hayakawa J. Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6 // Proceeding NIST Conference. 2000.

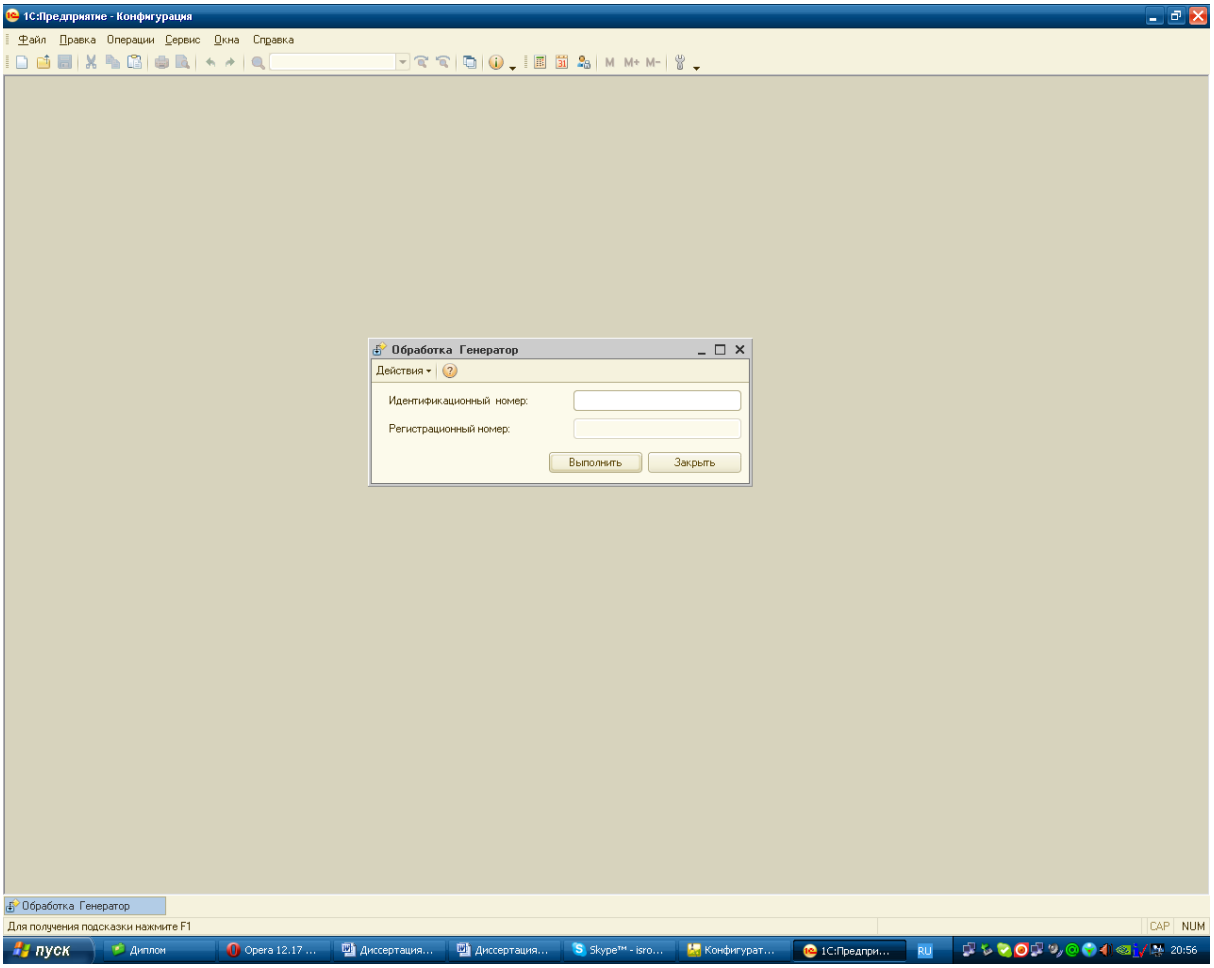
ИЛОВАЛАР

1-ИЛОВА. Базани бузилган холатидаги активлаштириш сўрови ойнаси.

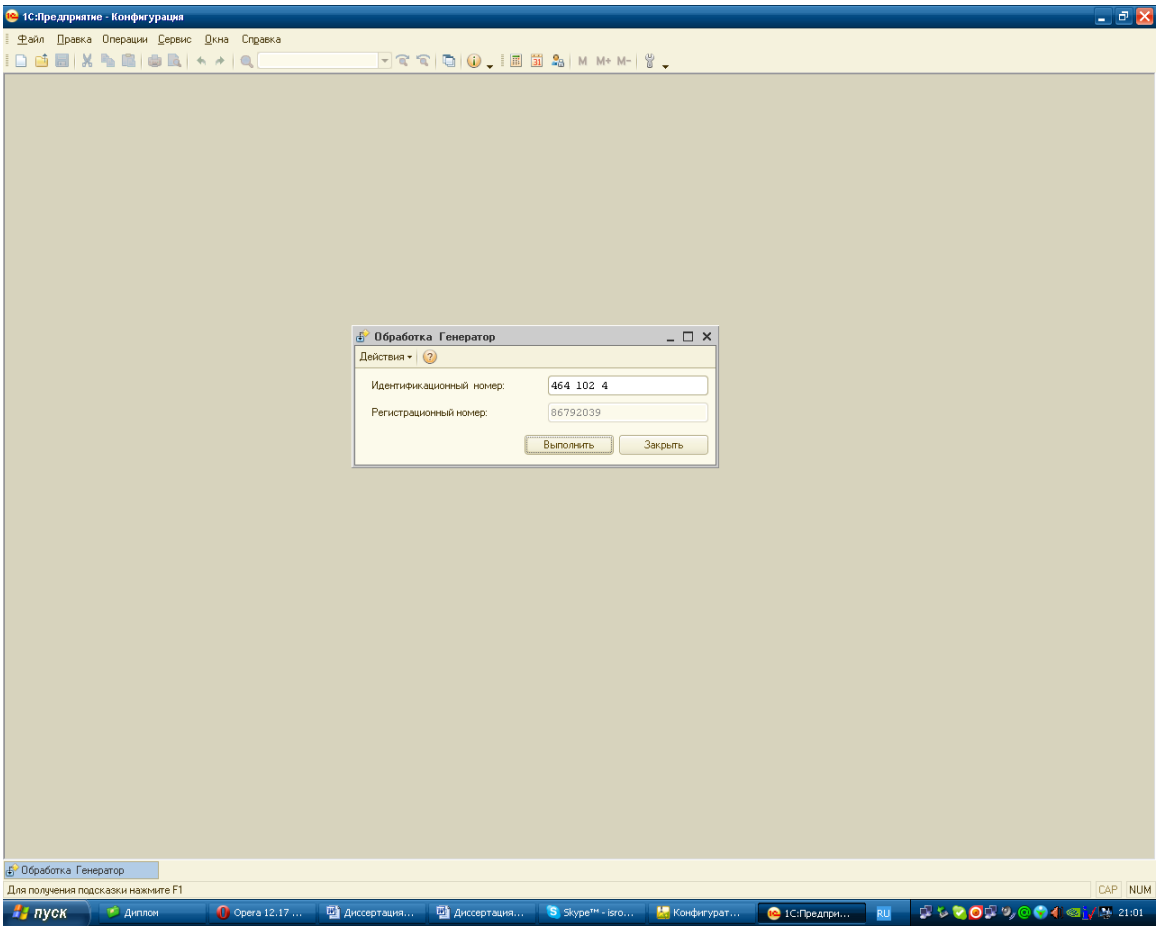


Бунда идентификацион рақам қаттиқ дискни серия рақамидир.

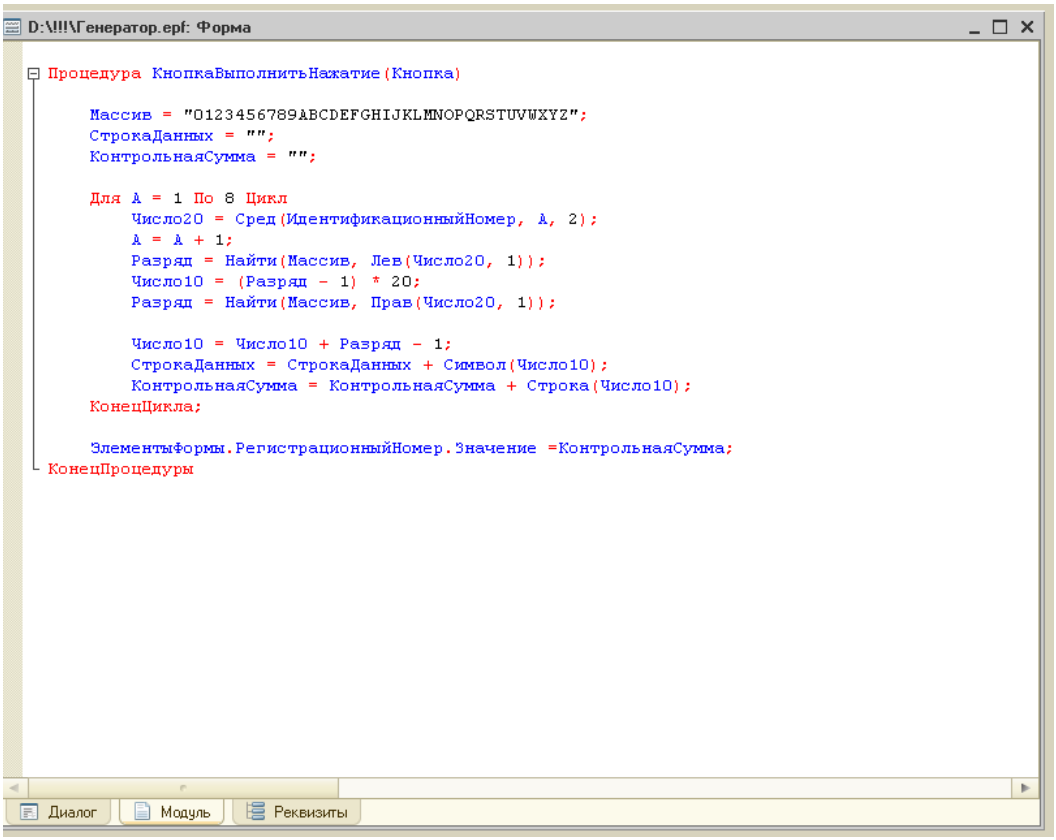
2-ИЛОВА.Генераторни ишчи ойнаси.



3-ИЛОВА. Генератор генерациялашан тасодифий рақам яъни аутидентификацион рақам (Регистрация номери).



4-ИЛОВА. 1с8.2.Бухгалтерия платформасида ёзилган ТРГ коди.



5-ИЛОВА. 1с8.2.Бухгалтерия платформасида ёзилган ТРГни кодлари.

```
Процедура КнопкаВыполнитьНажатие(Кнопка)

    Массив = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ";
    СтрокаДанных = "";
    КонтрольнаяСумма = "";

    Для А = 1 По 8 Цикл
        Число20 = Сред(ИдентификационныйНомер, А, 2);
        А = А + 1;
        Разряд = Найти(Массив, Лев(Число20, 1));
        Число10 = (Разряд - 1) * 20;
        Разряд = Найти(Массив, Прав(Число20, 1));

        Число10 = Число10 + Разряд - 1;
        СтрокаДанных = СтрокаДанных + Символ(Число10);
        КонтрольнаяСумма = КонтрольнаяСумма + Строка(Число10);
    КонецЦикла;

    ЭлементыФормы.РегистрационныйНомер.Значение
=КонтрольнаяСумма;
КонецПроцедуры
```

6-ИЛОВА. 1с8.2.Бухгалтерия платформасида ёзилган активлаштириш дастурининг кодлари

```
Процедура ПриОткрытии()
	ЭлементыФормы.ПолеHTMLДокумента.УстановитьТекст(ПолучитьОбщийМакет("АвторскиеПрава").ПолучитьТекст());

	Диск =ПолучитьСерийныйНомерЖесткогоДиска("C");

	ПолученныеДанные = ВРег(СокрЛП(СтрЗаменить(Диск, "-", "")));

	ЭлементыФормы.ИдентификационныйНомер.Значение =ПолученныеДанные;
КонецПроцедуры

Процедура ПроверитьЗаполненностьЗначений(Отказ)
	Если ПустаяСтрока(РегистрационныйНомер) Тогда
		Предупреждение("Регистрационный номер продукта на введен!"+Символы.ПС+"Чтобы зарегистрировать продукт необходимо указать регистрационный номер!", , "Активация конфигурации");
		Отказ=Истина;
	КонецЕсли;
КонецПроцедуры

Процедура ОсновныеДействияФормыЗарегистрировать(Кнопка)
	Отказ = Ложь;
	ПроверитьЗаполненностьЗначений(Отказ);
	Если Не Отказ Тогда
		ЭтаФорма.Закрыть(СокрЛП(РегистрационныйНомер));
	КонецЕсли;
КонецПроцедуры
```