ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

Ганиев Салим Каримович, Каримов Маджит Маликович,

Ташев Комил Ахматович

АХБОРОТ ХАВФСИЗЛИГИ

Дарслик

Тошкент-2015

“Ахборот хавфсизлиги” фани бўйича дарслик таянч олий ўқув юрти Тошкент ахборот технологиялари университетининг “Ахборот хавфсизлиги” кафедраси профессор-ўқитувчилари томонидан тайёрланган бўлиб, унда ахборот хавфсизлиги тушунчаси ва унинг вазифалари, ахборот хавфсизлигига бўладиган тахдидлар, хужумлар ва заифликлар, ахборот хавфсилиги соҳасига оид халқаро ва миллий меъёрий-хуқуқий база, хавфсизлик моделлари, ахборотни криптографик ҳимоялаш, идентификация ва аутентификация, компьютер вируслари ва зараркунанда дастурлар билан курашиш механизмлари, ахборотни ҳимоялашда тармоқлараро экранларнинг ўрни, операцион тизим ҳимояси, ахборот сирқиб чиқиш каналлари ва уларни аниқлаш ҳамда объектларни инженер ҳимоялаш ва техник қўриқлаш масалалари келтирилган.

Дарслик олий ўқув юртининг “330000 – Компьютер технологиялари ва информатика” таълим соҳасининг “5330500 – Компъютер инжинирнги”, “5330600 – Дастурий инжинирнги” таълим йўналишлари ҳамда “350000 – Алоқа ва ахборотлаштириш, телекоммуникация” таълим соҳасининг “5330100 – Телекоммуникация технологиялари”, “5350200 – Телевизион технологиялар”, “5350300 – Ахборот коммуникация технологиялари соҳасида иқтисодиёт ва менежмент”, “5350400 – Ахборот технологиялари соҳасида касб таълим”, “5350500 – Почта алоқаси технологияси”, “5350600 – Ахборотлаштириш ва кутубхонашунослик” таълим йўналишлари талабалари учун мўлжалланган бўлиб, ундан ахборот технологиялари, компьютер тизимлари хавфсизлиги соҳасида фаолият кўрсатувчилар фойдаланишлари мумкин.

***

Учебник по дисциплине "Информационная безопасность" подготовлен профессорско-преподавательским составом кафедры "Информационная безопасность" Ташкентского университета информационных технологий, являющимся базовым высшим учебным заведением по данному направлению. В учебнике раскрыто понятие информационной безопасности,

рассмотрены задачи обеспечения безопасности, виды угроз, атак и присущие средствам защиты недостатки. Рассмотрены также международные и национальные нормативно-правовые документы по безопасности, модели безопасности, криптографическая защита информации, вопросы идентификации и аутентификации, методы и механизмы борьбы с компьютерными вирусами и вредоносными программами, роль межсетевых экранов, методы защиты операционных систем, каналы утечки информации и способы их выявления, методы инженерной защиты объектов и их технической охраны.

Учебник предназначен для студентов, обучающихся в области образования "330000 - Компьютерная технология и информатика", по направлениям образования: "5330500 - Компьютер инжиниринг", "5330600 - Программный инжиниринг", а также в области образования "350000 - Связь, информатизация и телекоммуникация" по направлениям образования: "5330100 - Телекоммуникационные технологии", "5350200 - Телевизионная технология", "5350300 - Экономика и менеджмент в информационных и коммуникационных технологиях", "5350400 - Профессиональное образование в информационных технологиях", "5350500 - Технология почтовой связи", "5350600 - Информатизация и библиотечное дело".

Учебник будет полезен для всех специалистов, профессиональная деятельность которых связана с обеспечением информационной безопасности в компьютерных системах и сетях.

***

Textbook based on subject "Information security" for higher educational institution of the Tashkent University of Information Technologies which is prepared by the department “Information security", there was given concept of information security and its objectives, threats, attacks and vulnerabilities in information security, international and national normative-juridical base which related to information security sphere, security models, cryptographic protection of information, identification and authentication, mechanisms to combat with

computer viruses and harmful programs, the role firewalls to protect information, protection of operation system, information leakage channels and determine them also engineer protection and technical defending of objects.

Textbook is made for directions of higher educational institution “330000 – Computer technologies and informatics” “5330500 – Computer engineering”, “5330600 – Software engineering”, “350000 – Communication and informatization, telecommunication”, “5330100 – Telecommunication technologies”, “5350200 – Television technologies”, “5350300 – Economics and management in Information Communication sphere”, “5350400 –Professional education in Information Technology sphere”, “5350500 –Automation of post services”, “5350600 – Information library systems” also this textbook can be used by people who works in information technologies, security of computer systems sphere.

Тақризчилар: проф. **Игамбердиев Х.З. –** Тошкент давлат техника университети “Бошқаришда ахборот технологиялари” кафедраси профессори, техника фанлари доктори;

Аҳмедова О.П. - “Unicon.UZ” ДУК, Криптография илмий-тадқиқот бўлими бошлиғи, т.ф.н.;

МУНДАРИЖА

ОГЛАВЛЕНИЕ

CONTENTS

МУҚАДДИМА

Компьютер техникаси ва ахборот тизимларининг иқтисодда, бошқаришда, алоқада, илмий тадқиқотларда, таълимда, хизмат кўрсатиш соҳасида, тижорат, молия ва инсон фаолиятининг бошқа соҳаларида қўлланилишининг ривожи ахборотлаштириш ва, умуман, жамият ривожини белгиловчи йўналиш ҳисобланади. Компьютер техникасининг қўлланиши эвазига эришилувчи самара ахборот ишланиши кўламининг ошиши билан ортиб боради. Ушбу техниканинг қўлланиш соҳалари ва кўлами унинг ишлашининг ишончлилиги ва барқарорлиги муаммолари билан бир қаторда унда айланувчи ахборот хавфсизлигини таъминлаш муаммосини туғдиради.

Ахборот хавфсизлиги – ахборотнинг номақбул (ахборот муносабатларининг тегишли субъектлари учун) ошкор қилинишидан (конфиденциаллигининг бузилишидан), бузилишидан (яхлитлигининг бузилишидан), сирқиб чиқишидан, йўқотилишидан, модификацияланишидан ёки фойдаланувчанлик даражасининг пасайишидан ҳамда ноқонуний тиражланишидан ҳимояланганлиги. Ушбу ходисаларнинг сабабчиси тасодифий таъсирлар ёки бузғунчининг (нияти бузуқнинг) атайин рухсатсиз фойдаланиши натижасидаги таъсирлар бўлиши мумкин.

Жамиятнинг жадал суръатларда ахборотлаштирилиши сабабли ахборот хавфсизлиги муаммоси ниҳоятда долзарб ва доимо шундай бўлиб қолади.

Китобнинг биринчи бобида ахборот хавфсизлиги тушунчаси ва унинг вазифалари баён этилган. Миллий хавфсизлик тушунчасига таъриф берилиб, унинг ташкил этувчилари батафсил ёритилган. Ахборот хавфсизлигини таъминлашнинг асосий вазифалари келтирилиб, шахснинг, жамиятнинг ва давлатнинг ахборот муҳитидаги манфаатлари баён этилган. Хавфсизлик сиёсати, ахборот хавфсизлиги архитектураси ва стратегияси ва улар орасидаги боғлиқлик масалалари ҳам ушбу бобдан ўрин олган.

Китобнинг иккинчи боби ахборот хавфсизлигига бўладиган тахдидлар, хужумлар ва заифликларга бағишланган. Ахборот хавфсизлигига тахдидлар ва заифликлари таҳлил этилиб, уларнинг активларга зарар етказа олишлари

учун бирлашишлари лозимлиги мисоллар ёрдамида кўрсатилган. Ахборотнинг маҳфийлигини, яхлитлигини ва фойдаланувчанлигини бузиш усулларига алоҳида эътибор берилган.

Китобнинг учинчи боби ахборот коммуникация тизимларида ахборот хавфсизлигини таъминлаш, бошқариш соҳасига оид ҳалқаро ва миллий маъёрий-хуқуқий базага бағишланган. Давлат ва хусусий корхона ва ташкилотларда мавжуд ахборот коммуникация тизмларида ахборот хавфсизлигини таъминлашда қўлланиладиган меъёрий хуқуқий хужжатлар кўриб чиқилган.

Китобнинг тўртинчи боби хавфсизлик моделлари – дискрецион, мандатли ва ролли моделларга бағишланган. Дискрецион моделларда фойдаланишни бошқариш фойдаланувчиларга маълум объектлар устида маълум амалларни бажариш ваколатини бериш йўли билан амалга оширилиши, мандатли моделларнинг фойдаланишни хуфия ҳолда – тизимнинг барча субъект ва объектларига хавфсизлик сатҳларини белгилаш орқали бошқариши, ролли моделнинг хавфсизликнинг татбиқий сиёсатини акслантириши батафсил баён этилган.

Китобнинг бешинчи боби ахборотни криптографик ҳимоялаш усуллари ва воситаларига бағишланган бўлиб, узатиладиган маълумотларни ҳимоялашда қўлланиладиган симметрик шифрлаш тизимларининг структураси, алгоритмлари ва улар учун фойдаланиладиган калитларни тақсимлаш схемалари келтирилган. Асимметрик шифраш тизимларига оид криптографик ўзгартириш схемалари ва шифрлаш алгоритмларининг математик асослари ҳақида сўз юритилиб, асимметрик алгоритмлар мисол тариқасида келтирилган. Электрон рақамли имзоларни шакллантириш ва ҳақиқийлигини тасдиқлаш жараёнларини ташкил этувчи алгоритмлар тавсифланган, ривожланган давлатларнинг электрон рақамли имзолари ҳақидаги стандартлари келтириб ўтилган. Ундан ташқари ушбу бобда криптографиянинг стеганографик усуллари, уларнинг турлари ва технологиялари ҳақида қисқача тўхталиб ўтилган. Ушбу бобдан

криптографик алгоритмларни таҳлиллаш усуллари ва воситалари ҳам ўрин олган.

Китобнинг олтинчи бобида тизимнинг фойдаланувчилар билан ўзаро алоқасидаги асосий жараёнлар – фойдаланувчи ҳаракатини аутентификациялаш, авторизациялаш ва маъмурлаш, бир ва кўп мартали пароллар ҳамда рақамли сертификатлар асосидаги аутентификациялаш хусусиятларининг таҳлили ўрин олган. Фойдаланувчини идентификациялаш ва аутентификациялашнинг намунавий схемалари келтирилган. Симметрик ва асимметрик криптоалгоритмларга асосланган қатъий аутентификациялашга алоҳида эътибор берилиб, жумладан, Kerberos протоколи муҳокама этилган. Ушбу бобдан биометрик идентификациялаш ва аутентификациялаш воситаларининг тавсифи ҳам ўрин олган.

Китобнинг еттинчи боби компьютер вируслари ва зараркунанда дастурлар билан курашиш механизмларига бағишланган. Компьютер вирусларининг таснифи келтирилиб, вирус ҳаёт цикли босқичлари таҳлилланган, вируслар ва бошқа зарар келтирувчи дастурларнинг асосий тарқалиш каналлари кўрилган. Вирусга қарши дастурларнинг асосийлари муҳокама этилиб, ҳимоянинг профилактик чоралари ёритилган. Вирусга қарши ҳимоя тизимини қуришдаги асосий босқичлар батафсил баён этилган.

Китобнинг саккизинчи боби ахборотни ҳимоялашда тармоқлараро экранларнинг ўрнига бағишланган. Тармоқлараро экранларнинг функциялари таҳлили, уларнинг OSI моделининг сатҳларида ишлаши бўйича, хусусиятлари мухокама этилган. Тармоқлараро экранлар асосидаги тармоқ ҳимоясининг схемалари келтирилган.

Китобнинг тўққизинчи боби операцион тизим хавфсизлигини таъминлаш муаммоларига бағишланган бўлиб, ҳимояланган операцион тизим тушунчаси, ҳимояланган операцион тизимни яратишдаги ёндашишлар ва ҳимоялашнинг маъмурий чоралари баён этилган. Операцион тизимни ҳимоялаш қисмтизимининг асосий функциялари ҳамда ахборотни ҳимоялашда дастурий иловаларнинг қўлланилиши масалаларига алоҳида

эътибор берилган.

Китобнинг ўнинчи боби ахборот сирқиб чиқиш каналларига бағишланган бўлиб, ахборот сирқиб чиқадиган техник каналлар ва уларнинг таснифи келтирилган. Ахборот сирқиб чиқадиган радиоэлектрон, акустик, оптик, моддий каналларнинг ахборот элтувчилари, информативлиги, даврийлиги ва структуралари ёритилган. Ахборот сирқиб чиқадиган техник каналларни аниқлаш усуллари ва воситалари баён этилган. Ушбу бобдан объектларни инженер ҳимоялаш ва техник қўриқлаш масалалари ҳам ўрин олган.

Иловаларда ахборотни ҳимоялашнинг дастурий воситаларини яратиш намуналари ва атамаларнинг ўзбек, рус, инглиз тилларидаги изоҳли луғати келтирилган.

I боб. АХБОРОТ ХАВФСИЗЛИГИ ТУШУНЧАСИ ВА УНИНГ ВАЗИФАЛАРИ

1.1. Миллий хавфсизлик тушунчаси

Ҳозирда 29 август 1997 йили қабул қилинган “Ўзбекистон Республикасининг миллий хавфсизлиги концепциясини тасдиқлаш тўғрисида” қонуни амалда. Ушбу қонунга асосланиб миллий хавфсизлик тушунчасига қуйидагича таъриф бериш мумкин.

Ўзбекистон Республикасининг миллий хавфсизлиги деганда Ўзбекистон Республикасининг суверенитетини ифодаловчи ва ҳокимиятнинг ягона манбаи ҳисобланувчи кўп миллатли халқининг хавфсизлиги тушунилади.

Миллий хавфсизликнинг, шартли равишда, қуйидаги ташкил этувчиларини кўрсатиш мумкин:

- иқтисодий хавфсизлик;
- ички сиёсий хавфсизлик;
- ижтимоий хавфсизлик;
- маънавий хавфсизлик;
- ҳалқаро хавфсизлик;
- ахборот хавфсизлиги;
- харбий хавфсизлик;
- чегаравий хавфсизлик;
- экологик хавфсизлик.

Иқтисодий хавфсизлик – шахс, жамият ва давлатнинг иқтисодий соҳадаги ҳаётий муҳим манфаатларининг ички ва ташқи таҳдидлардан ҳимояланганлиги. Иқтисодий хавфсизликка биноан халқ ўзининг иқтисодий ривожланиш йўллари ва шаклларини ташқаридан аралашишсиз ва босимсиз мустақил равишда аниқлай олади.

Ички сиёсий хавфсизлик – ҳокимият институтларининг барқарорлиги ва самарадорлиги, ҳокимият тузилмаларининг сиёсий жараёнларни назоратлаш

қобилияти, аксарият фуқаролар томонидан мададлашга эришиш, жамиятда сиёсий барқарорликни таъминловчи, самарали фаолият юритувчи нодавлат сиёсий институтларнинг мавжудлиги билан характерланади. Ички сиёсий хавфсизликка биноан сиёсий муносабатлар соҳасида қарама-қаршилик, сиёсий экстремизмнинг оммавий тус олиши, ҳокимият билан халқ орасида қарама-қаршилик бўлмайди.Фуқароларнинг сиёсий онги ҳолати ва жамиятнинг сиёсий маданияти жамиятнинг хавфсиз сиёсий ривожига жиддий таъсир кўрсатади.

Ижтимоий хавфсизлик – шахс, оила ва жамиятнинг ҳаётий муҳим манфаатларининг ички ва ташқи таҳдидлардан ҳимояланганлиги. Ижтимоий хавфсизликнинг объекти - миллий ва ижтимоий сиёсат томонидан тартибга солинувчи халқ турмуши сифати ва даражасини таъминловчи ижтимоий тизимнинг барча асосий элементлари. Ижтимоий ривожланиш стратегияси, уларнинг узоқлигига, камабағаллик даражасига, турмуш даражасидаги минтақавий мутаносиблигига, таълим ва соғлиқни сақлаш сифатига, жамиятдаги маънавият ва маданиятнинг умумий даражасига ва, ниҳоят, демографик муаммоларига таъсири маълум.

Маънавий хавфсизлик – бугунги кунда инсон маънавиятига қарши йўналтирилган, бир қарашда арзимас бўлиб туюладиган кичкина хабар ҳам ахборот оламидаги глобаллашув шиддатидан куч олиб, кўзга кўринмайдиган, лекин зарарини ҳеч нарса билан қоплаб бўлмайдиган улкан зиён етказиши мумкин. Айниқса, оммавий маданият деган ниқоб остида аҳлоқий бузуқлик ва зўравонлик, индивидуализм, эгоцентризм ғояларини тарқатиш, керак бўлса, шунинг ҳисобидан бойлик орттириш, бошқа халқларнинг неча минг йиллик анъана ва қадриятларини, турмуш тарзининг маънавий негизларига беписандлик, уларни қўпоришга қаратилган хатарли таҳдидлар одамни ташвишга солмай қўймайди.Ҳозирги вақтда аҳллоқсизликни маданият деб билиш ва аксинча, асл маънавий қадриятларни менсимасдан, эскилик сарқити деб қараш билан боғлиқ ҳолатлар бугунги тараққиётга, инсон ҳаёти, оила муқаддаслиги ва ёшлар тарбиясига катта хавф солмоқда ва кўпчилик

бутун жаҳонда бамисоли бало-қазодек тарқалиб бораётган бундай хуружларга қарши курашиш нақадар муҳим эканини англаб олмоқда.

Халқаро хавфсизлик – халқаро муносабатлар назариясида халқаро хавфсизлик деганда дунё ҳамжамиятининг барқарорлигини таъминловчи халқаро муносабатлар ҳолати тушунилади. Бошқача айтганда, халқаро хавфсизлик – халқаро муносабатлар субъектларига уруш хавфи ёки суверен хаётига ва мустақил ривожига ташқаридан бошқа тажовуз хавфи бўлмаган ҳолат. БМТ Низомига биноан, ҳозирда ҳалқаро тинчликни сақлашга асосий жавобгар сифатида Хавфсизлик Кенгаши белгиланган. Фақат айнан ушбу Кенгаш агрессорга нисбатан санкция қўллаш хуқуқига эга.

Ахборот хавфсизлиги – мамлакат маданий мулкининг, хўжалик субъектлари ва фуқаролар интеллектуал мулкининг, давлат ва касбий сирга эга махсус маълумотларнинг ишончли ҳимояланганлиги ҳолати.

Харбий хавфсизлик – харбий сиёсат Ўзбекистон Республикаси харбий доктринасида ишлаб чиқилган низомларга асосан юритилади. Харбий доктрина – Ўзбекистон Республикасининг харбий хавфсизлигининг харбий-сиёсий, харбий-стратегик ва харбий-иқтисодий асосларини белгиловчи расмий қарашлар мужмуи. Харбий доктринанинг хуқуқий асосини Ўзбекистон Республикаси Конституцияси, қонунлар ҳамда харбий хавфсизликни таъминлаш соҳасидаги Ўзбекистон Республикасининг халқаро шартномалари ташкил этади. Ўзбекистон Республикасининг харбий хавфсизлигини таъминлашга раҳбарлик Қуролли Кучларнинг Олий Бош қўмондони ҳисобланувчи Ўзбекистон Республикаси Президенти томонидан амалга оширилади.

Чегаравий хавфсизлик – Ўзбекистон Республикаси давлат чегараси ва чегара олди худудларининг ҳимояланганлик ҳолати. Чегаравий хавфсизлик шахс, жамият ва давлат хавфсизлигининг жуда муҳим ташкил этувчиларидан бири ҳисобланади, чунки давлат барқарорлиги унинг чегараларининг хавфсизлиги билан узвий боғланган. Чегара хавфсизлигини таъминлаш зарурияти давлат чегараси ва чегара олди худудларда юзага келган таҳдидлар

тизимига асосланган.

Экологик хавфсизлик.Цивилизациянинг атроф – муҳитга фаол таъсири натижасида унинг ифлосланиши йилдан-йилга ошиб бормоқда. Ушбу салбий таъсир айниқса экологик ҳалокат жойларда, минерал ресурслардан ва ишлаб чиқаришнинг зарарли чиқиндиларидан оқилона фойдаланилмайдиган жойларда кучли бўлади.

Назорат саволлари:

1. Миллий хавфсизлик тушунчаси нима?
2. Миллий хавфсизликни шартли равишда ташкил этувчиларини санаб ўтинг.
3. Маънавий хавфсизликнинг оқибатларини тушунтириб беринг.
4. Ҳалқаро хавфсизлигини жаҳон цивилизациясида тутган ўрни?
5. Ахборот хавфсизлигининг моҳияти нима?

1.2. Ахборот хавфсизлигини таъминлашнинг асосий вазифалари ва даражалари

Ахборот хавфсизлигини таъминлаш мунтазам ва комплекс характерга эга кўп қиррали фаолиятни амалга оширишни кўзда тутади. Уни амалга оширишда ахборот хавфсизлигидан манфаатдор тарафлар олдига қўйиладиган вазифаларга алоҳида эътибор бериш зарур. Ушбу турли-туман вазифаларни бир неча қуйидаги асосий гуруҳларга ажратиш мумкин:

1) *ахборотдан фойдалнишни таъминлаш*, яъни мақбул вақт мобайнида ахборот хизматини олиш ҳамда ахборотни олишда рухсатсиз тақиқлашни бартараф этиш;

2) *ахборот яхлитлилигини таъминлаш,* яъни ахборотнинг рухсатсиз модификацияланишини ёки бузилишини бартараф этиш;

3) *ахборот конфиденциаллигини таъминлаш,* яъни ахборотдан рухсатсиз танишишни бартараф этиш.

Одатда, бир-биридан ахборот хавфсизлигининг хуқуқий, техник,

молиявий, ташкилий ва бошқа ресурсли таъминоти билан фарқланувчи ахборот хавфсизлиги субъектларининг қуйидаги тўртта категорияси ажратилади:

- бутун бир давлат;
- давлат ташкилотлари;
- тижорат тузилмалари;
- алоҳида фуқаролар.

Юқорида келтирилган ахборот хавфсизлигини таъминлашдаги асосий вазифалар қамраб олган қуйидаги кенг спектрли масалаларни кўриб чиқиш жоиз ҳисобланади:

- конфиденциаллик;
- яхлитлик;
- идентификация;
- аутентификация;
- ваколат бериш;
- фойдаланишни назоратлаш;
- мулклик хуқуқи;
- сертификация;
- имзо;
- воз кечмаслик;
- санасини ёзиш;
- олганлигига тилхат бериш;
- бекор қилиш;
- анонимлик.

Ахборотнинг конфиденциаллиги – ҳимоянинг энг керакли вазифаларидан бири. Ҳар бир инсонда ёки ташкилотда шундай хужжатлар борки, уларнинг жамоа мулкига айланмаслиги таъминланиши шарт. Бундай хужжатларни сақлашда қоғоз, фотопленка ишлатилса, конфиденциаллик маъмурий усуллар ёрдамида амалга оширилади. Аммо ахборот компьютерда ишланиб, очиқ алоқа канали орқали узатилса, маъмурий усуллар ожизлик

қилади ва ёрдамга ахборот хавфсизлигини таъминлаш усуллари келади. Конфиденциалликни таъминлаш масаласига биноан маълумотлар шундай кўринишда узатиладики, ҳатто нияти бузуқ элтувчидан ёки узатиш муҳитидан фойдалана олганида ҳам ҳимояланган маълумотларни олаолмайди.

Ахборотнинг яхлитлиги. Маълумотлар, ишланиши ва алоқа канали бўйича узатилиши жараёнида, тасодифан ёки атайин бузилиши мумкин. Ахборот элтувчида сақланадиган жойидаёқ бузилиши мумкин. Яхлитликни таъминлашга (яхлитликни назоратлашга) биноан маълумотлар сақланиши ва узатилиши жараёнида модификацияланмаганлигини тасдиқлаш ёки маълумотлар бузилганлигини аниқлаш талаб этилади. Бошқача айтганда, маълумотларнинг ҳар қандай ўзгариши сезилмасдан қолмаслиги зарур.

Идентификация фойдаланувчини қандайдир ноёб идентификатор билан айнанлигини тасдиқлаш учун керак. Ундан сўнг идентификаторга юкланган барча ҳаракатларга ушбу идентификатор бириктирилган фойдаланувчи жавобгар ҳисобланади.

Аутентификация идентификацияга зарурий қўшимча ҳисобланади ва идентификаторни тақдим этган фойдаланувчининг ҳақиқийлигини (аутентлигини) тасдиқлашга мўлжалланган. Аноним бўлмаган фойдаланувчи аутентификациядан муваффақиятли ўтгандагина ишлаш имкониятига эга бўлиши шарт.

Ваколат беришга биноан бирорта ҳам фойдаланувчи аутентификациядан муваффақиятли ўтмагунича тизимдан фойдаланмаслиги ва бирорта ҳам фойдаланувчи, агар у махсус рухсатнома билан ваколатга эга бўлмаса, русурслардан фойдаланмаслиги шарт.

Фойдаланишни назоратлаш комплекс тушунча ҳисобланади ва ресурслардан фойдаланишни чеклашга мўлжалланган усуллар ва воситаларни англатади.

Мулклик ҳуқуқи фойдаланувчига қандайдир ресурслардан фойдаланишга қонуний хуқуқни ва, у истаса, ушбу ресурсни бошқа

фойдаланувчига ўтказиш имкониятини тақдим этишга мўлжалланган. Мулклик хуқуқи одатда фойдаланишни назоратлаш тизимининг таркибий қисми ҳисобланади.

Сертификация – фойдаланувчи ишонадиган тараф томонидан қандайдир фактни тасдиқлаш жараёни. Кўпинча сертификация очиқ калитнинг муайян фойдаланувчига ёки ширкатга тегишли эканлигини тасдиқлашда ишлатилади, чунки очиқ калитлар инфраструктурасидан фақат сертификация тизимининг мавжудлигида самарали фойдаланиш мумкин. Сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот – сертификация маркази томонидан, маълум шартлар бажарилганида берилади.

Имзо хужжат қабул қилувчига ушбу хужжатнинг айнан узатувчи томонидан имзоланганлигини исботлашга имкон беради. Бунда имзони бошқа хужжатга ўтказиш ва узатувчи ўзининг имзосидан воз кечиши мумкин эмас. Хужжатнинг ҳар қандай ўзгариши имзонинг бузилишига сабаб бўлади ва ҳар қандай фойдаланувчи мустақил тарзда имзонинг ҳақиқийлигини текшириши мумкин.

Воз кечмаслик ахборот алмашиш схемасининг хусусияти ҳисобланади. Унга биноан хабар қабул қилувчининг учинчи тарафнинг хабар узатувчининг кимлигини текширишга жалб қилиши қобилиятига эга эканлигининг исботи мавжуд. Бошқача айтганда, хабарни узатувчи муаллифликдан воз кечиш имкониятига эга эмас.

Санасини ёзиш кўпинча имзо билан биргаликда ишлатилади ва хужжат имзоланган онни қайдлайди. Бу битта хужжат бир неча фойдаланувчилар томонидан имзоланганда, биринчиликни исбот қилишда фойдали ҳисобланади, чунки ҳар бир фойдаланувчи хужжат муаллифлигига даъво қилади. Ундан ташқари санасини ёзиш муддатли сертификатларда кенг қўлланилади.

Олганлигига тилхат бериш қабул қилувчидан узатувчига узатилади ва узатувчи томонидан узатилган ахборот қабул қилувчига тилхатда

кўрсатилган ондан кечикмасдан етказганлигини исботлашда ишлатилиши мумкин.

Бекор қилиш – сертификатлар, ваколатлар ва имзолар таъсир кучини бекор қилиш. Агар ахборот алмашишда иштирок этувчи ёки унга тегишли калитлар ва сертификатлар обрўсизланса, ушбу фойдаланувчини ресурслардан фойдаланишга йўл қўймаслик ва мос сертификатларга ишонмаслик зарур, чунки бу сертификатлардан нияти бузуқ фойдаланиши мумкин. Бекор қилиш муолажаси сертификация марказига нисбатан ҳам қўлланиши мумкин.

Анонимлик камдан кам учрайди. Хукуматлар ва ширкатлар учун фойдаланувчининг ахборот муҳитида қандайдир ҳаракатларининг аноним бўлиб қолишлиги фойда бермайди. Шу сабабли анонимликни таъминловчи лойиҳалар камдан кам учрайди ва, одатда, узоқ яшамайди. Зеро коммуникация воситалари кўпинча у ёки бу хабарнинг узатилиши маршрутини ва, демак, узатувчини аниқлашга имкон беради.

Юқорида келтирилган вазифалар мавжуд ахборот дунёси эҳтиёжига асосан тавсифланган.Вақт ўтиши билан баъзи вазифалар ўз долзарблигини йўқотиши ва, аксинча, ечимини кутувчи янги вазифалар пайдо бўлиши мумкин.

Цивилизация ривожининг замонавий босқичида ахборот нафақат жамият ва давлат институтлари фаолиятида, балки ҳар бир шахс ҳаётида хал қилувчи ролни ўйнайди.

Шахснинг ахборот муҳитидаги манфаатлари инсон ва фуқаронинг ахборотдан фойдаланишдаги конституциявий хуқуқларининг амалга оширилишини, қонун тақиқламаган фаолиятни, физик, маънавий ва интеллектуал ривожини ҳамда шахсий хавфсизлигини таъминлашни кўзда тутади.

Жамиятнинг ахборот муҳитидаги манфаатлари ушбу муҳитда шахс манфаатларини таъминлашни, демократияни мустаҳкамлашни, хуқуқий ижтимоий давлатни яратишни, жамият иноқлигига эришиш ва уни

мададлашни, мамлакатнинг маънавий янгиланишини кўзда тутади.

Давлатнинг ахборот муҳитидаги манфаатлари инсон ва фуқаронинг ахборот олишидаги конституциявий ҳуқуқ ва эркинлигини таъминлашни, олинган ахборотдан конституциявий тузумнинг мустахкамлигини, давлат суверенитети ва худудий яхлитлигини, сиёсий, иқтисодий ва ижтимоий барқарорликни ҳамда қонунийликни ва ҳуқуқий тартибни, тенг ҳуқуқли ва ўзаро фойдали халқаро ҳамкорликни таъминлаш мақсадида фойдаланишдаги шарт-шароитларни яратиш учун ахборот инфраструктурасининг гармоник ривожини кўзда тутади.

Назорат саволлари:

1. Ахборот хавфсизлигини таъминлаш вазифалари нима ва у қайси асосий гуруҳларни ўз ичига олади?
2. Ахборот хавфсизлиги субъектларининг категорияларини тушунтириб беринг.
3. Ахборот хавфсизлигини таъминлаш асосий вазифалари қамраб олган конфиденциаллик, яхлитлик, идентификация ва аутентификация каби масалаларини ёритиб беринг.
4. Ахборот хавфсизлигини таъминлаш асосий вазифалари қамраб олган ваколат бериш, фойдаланишни назоратлаш, мулклик ҳуқуқи, сертификация каби масалаларини ёритиб беринг.
5. Ахборот хавфсизлигини таъминлаш асосий вазифалари қамраб олган имзо, воз кечмаслик, санасини ёзиш каби масалаларини ёритиб беринг.
6. Ахборот хавфсизлигини таъминлаш асосий вазифалари қамраб олган олганлигига тилхат бериш, бекор қилиш, анонимлик каби масалаларини ёритиб беринг.
7. Ахборот хавфсизлигини таъминлаш даражаларини тавсифлаб беринг.

1.3. Хавфсизлик сиёсати

Ахборот хавфсизлиги сиёсати (ёки хавфсизлик сиёсати) – ташкилотнинг мақсадлари ва вазифалари ҳамда хавфсизликни таъминлаш соҳасидаги тадбирлар тавсифланадиган юқори даражадаги режа. Сиёсат хавфсизликни умумлашган атамаларда, специфик деталларсиз тавсифлайди. У хавфсизликни таъминлашнинг барча дастурларини режалаштиради. Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт. Шу сабабли асосий вазифа сифатида тизимни (жумладан тармоқ харитасини) тўлиқ инвентаризациялашни кўзда тутиш лозим. Тармоқ харитасини тузишда ҳар бир тизимдаги ахборот оқимини аниқлаш лозим. Ахборот оқимлари схемаси ахборот оқимлари бизнес-жараёнларни қанчалик таъминлаётганини кўрсатиши мумкин, ҳамда ахборотни ҳимоялаш ва яшовчанлигини таъминлаш учун қўшимча чораларни кўриш муҳим бўлган сохани кўрсатиши мумкин. Ундан ташқари бу схема ёрдамида ахборот ишланадиган жойни, ушбу ахборот қандай сақланиши, қайдланиши, жойини ўзгартириши ва назоратланиши лозимлигини аниқлаш мумкин.

Инвентаризация аппарат ва дастурий воситалардан ташқари дастурий хужжат, аппаратура хужжатлари, технологик хужжат ва ҳ. каби компьютерга тааллуқли бўлмаган ресурсларни ҳам қамраб олиши шарт. Ушбу хужжатлар таркибида тижоратни ташкил этиш хусусиятлари тўғрисидаги ахборот бўлиши мумкин ва бу хужжатлар бузғунчилар фойдаланиши мумкин бўлган жойларни кўрсатади.

Ахборот хавфсизлиги сиёсатини аниқлашда қуйидагилар амалга оширилиши лозим:

1. Ахборот хавфсизлиги соҳасида амал қилинадиган хужжатлар ва стандартларни, ҳамда ахборот хавфсизлиги сиёсатининг асосий низомларини

аниқлаш, яъни:

- компьютер техникаси воситаларидан, дастурлардан ва маълумотлардан фойдаланишни бошқариш;
- вирусга қарши ҳимоя;
- резервли нусҳалаш масалалари;
- таъмирлаш ва тиклаш ишларини ўтказиш;
- ахборот хавфсизлиги соҳасидаги можаролар хусусида хабардор қилиш.

2. Хавф-хатарларни бошқаришга ёндашишларни аниқлаш, яъни ҳимояланганликнинг базавий сатҳи етарли эканлигини ёки хавф-хатарларни тахлиллашнинг тўлиқ вариантини ўтказиш талаб этилишини аниқлаш.

3. Ахборот хавфсизлиги режимига қуйиладиган талабларни аниқлаш.

4. Сатҳлар бўйича қарши чораларни структуризациялаш.

5. Ахборот хавфсизлиги соҳасида сертификациялаш тартибининг стандартларга мослигини аниқлаш.

6. Раҳбариятда ахборот хавфсизлиги мавзуи бўйича кенгашлар ўтказиш даврийлигини, хусусан, ахборот хавфсизлиги сиёсатининг низомларини қайта кўриш, ҳамда ахборот тизимининг барча категорияли фойдаланувчиларини ахборот хавфсизлиги масалалари бўйича ўқитиш тартибини аниқлаш.

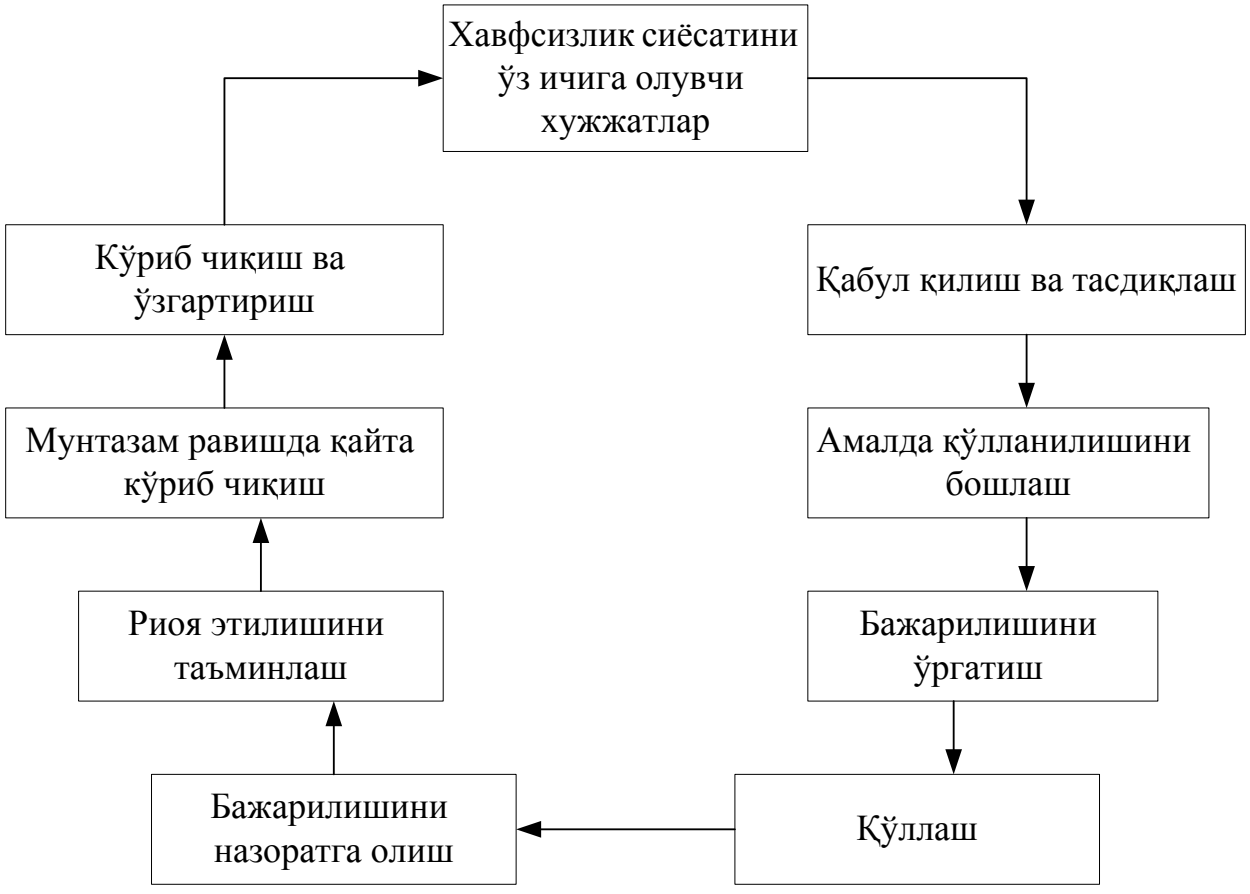
Ташкилотнинг реал хавфсизлик сиёсати қуйидаги бўлимларни ўз ичига олиши мумкин:

- умумий қоидалар;
- паролларни бошқариш сиёсати;
- фойдаланувчиларни идентификациялаш;
- фойдаланувчиларнинг ваколатлари;
- ташкилот ахборот ресурсларини компьютер вирусларидан ҳимоялаш;
- тармоқ боғланишларини ўрнатиш ва назоратлаш қоидалари;
- электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати

қоидалари;

- ахборот ресурслари хавфсизлигини таъминлаш қоидалари;
- фойдаланувчиларнинг хавфсизлик сиёсати қоидаларини бажариш бўйича мажбуриятлари ва ҳ.

Қоидалар ташкилотнинг ривожланишига, янги технологиялар, тизимлар ва лойиҳалар пайдо бўлишига мувофиқ ўзгариши лозим. Бунинг учун қоидаларни даврий равишда қайта кўриб чиқиш лозим. Хавфсизлик сиёсатини қайта кўриб чиқиш усулларидан бири ахборот коммуникация тизимлари аудити ҳисобланади. Шу сабабли ташкилот хавфсизлик сиёсати ва, табиийки, ахборот хавфсизлиги сиёсати ўзининг хаётий циклига эга дейиш мумкин (1.1-расм).



1.1-расм. Хавфсизлик сиёсатининг хаётий цикли

Хавфсизлик сиёсати қоидаларини қайта кўриб чиқиш муддатлари

хусусида аниқ бир кўрсатма мавжуд эмас. Аммо ушбу муддат олти ойдан бир йилгача белгиланиши тавсия этилади.

Хавфсизлик қоидалари ишлаб чиқилганидан ва амалга киритилганидан сўнг фойдаланучилар ахборот хавфсизлиги талаблари билан танишиб чиқишлари, ходимлар эса қоидаларни ўрганишлари лозим. Можаролар пайдо бўлганда ишлаб чиқилган режа бўйича ҳаракатланиш тавсия этилади.

Ахборот хавфсизлигини таъминлаш масалалари бўйича шуғулланадиган етакчи ташкилотлар хавфсизлик сиёсати шаблонларини ишлаб чиқдилар. Масалан SANS (System Administration Networking and Security) институти турли хавфсизлик сиёсатининг шаблонлари сериясини ишлаб чиқди (www.sans.org/resources/policies/).

Ушбу шаблонлар таркибига қуйидаги сиёсатлар киради:

- *жоиз шифрлаш сиёсати* – ташкилотда ишлатилувчи криптографик алгоритмларга қуйиладиган талабларни аниқлайди;
- *жоиз фойдаланиш сиёсати* – фойдаланувчиларни, ташкилот ресурсларини ва ахборотнинг ўзини ҳимоялаш учун қурилмалардан ва компьютер хизматларидан фойдаланишни аниқлайди;
- *вирусга қарши ҳимоя* – ташкилот тармоғига бўладиган компьютер вируслари таҳдидларини самарали камайтиришнинг асосий принципларини белгилайди;
- *харид имкониятларини баҳолаш сиёсати* – ташкилот томонидан ҳимоя воситаларини харид қилиш имкониятларини ва ахборот хавфсизлиги гуруҳи томонидан бажариладиган харид қилинганларни баҳолашга қуйиладиган минимал талабларни аниқлайди;
- *заифликларни сканерлаш аудити сиёсати* – ахборот ресурсларининг яхлитлигига ишонч ҳосил қилиш, мувофиқликни ўрнатиш ёки фойдаланиш ва тизим фаоллигининг мониторингини ўтказиш мақсадида аудитни кузатиш ва хавф-хатарни баҳолаш учун талабларни аниқлайди ва масъул шахсни тайинлайди;
- *автоматик тарзда узатиладиган почта сиёсати* – менеджер ёки

директорнинг рухсатисиз ҳеч қандай почта ташқи манбага автоматик тарзда йўналтирилмаслиги талабларини хужжатлаштиради;

- *маълумотлар базасидаги ваколатларни кодлаш сиёсати* – маълумотлар базасидаги фойдаланувчилар номини ва паролларни хавфсиз сақлаш ва олиш учун талабларни аниқлаш;

- *телефон линияси орқали фойдаланиш сиёсати* – тегишли фойдаланишни ва ундан авторизацияланган ходимлар томонидан фойдаланишни аниқлайди;

- *демилитаризацияланган зона хавфсизлиги сиёсати* – демилитаризацияланган зонада ёки ташқи тармоқ сегментларида жойлашган лабораторияларда ишлатиладиган барча тармоқ ва қурилмалар учун стандартларни белгилайди;

- *жиддий ахборот сиёсати* – конфиденциалликнинг мос даражаларини бериш йўли билан ташкилот ахборотини таснифлашга ва хавфсизлигига қўйиладиган талабларни белгилайди;

- *паролларни ҳимоялаш сиёсати* – паролларни ҳосил қилиш, ҳимоялаш ва алмаштириш стандартларини аниқлайди;

- *масофадан фойдаланиш сиёсати* – ташкилот учун ташқи ҳисобланувчи ҳар қандай хостнинг ёки тармоқнинг ташкилот тармоғига уланиш стандартларини аниқлайди;

- *хавф-хатарни баҳолаш сиёсати* – тижорат ҳамкорлиги билан ассоцияцияланган ташкилот ахборот инфратузилмасида хавф-хатарни идентификациялаш, баҳолаш ва камайтириш учун талабларни аниқлайди ва масъул шахсларни тайинлайди;

- *маршрутизатор хавфсизлиги сиёсати* – ташкилот ички тармоғи ёки фаолият (маҳсулотни тайёрлаш) учун ишлатиладаган маршрутизаторлар ва коммутаторлар учун хавфсизликнинг минимал конфигурацияси стандартларини аниқлайди;

- *сервер хавфсизлиги сиёсати* – ташкилот ички тармоғи ёки махсулот сифатида ишлатиладиган серверлар учун хавфсизликнинг минимал

конфигурацияси стандартларини аниқлайди;

- *VPN хавфсизлиги сиёсати* – ташкилот тармоғи билан IPSec ёки L2TPVPN уланишлардан масофадан фойдаланиш учун талабларни аниқлайди;

- *симсиз уланишлар сиёсати* – ташкилот тармоғи билан уланиш учун ишлатиладиган симсиз тизим учун стандартларни аниқлайди.

Таъкидлаш лозимки, ташкилот қурилишининг ва фаолият юритишининг ўзига хос хусусиятларига боғлиқ ҳолда ташкилотнинг хавфсизлик сиёсати набори шакллантирилади.

Назорат саволлари:

1. Хавфсизлик сиёсатини ва унинг аҳамиятини изоҳлаб беринг.
2. Хавфсизлик сиёсатини аниқлашда қандай амаллардан фойдаланилади?
3. Хавфсизлик сиёсати қайси бўлимларни ўз ичига олиши мумкинлигини ва уларни моҳиятини тушунтириб беринг
4. Хавфсизлик сиёсатининг ҳаётий цикли қандай ифодаланади?
5. SANS институти тақдим этган хавфсизлик сиёсати шаблонларини ёритиб беринг.

1.4. Ахборот хавфсизлиги архитектураси ва стратегияси

Замонавий тижорат олдида мураккаб масалалар тўплами кўндалангки, беқарор иқтисодий вазиятда уларнинг долзарблиги янада ошади. Бундай масалаларга қуйидагиларни киритиш мумкин:

- даромаднинг ошиши;
- ўзгарувчи вазиятларга реакция тезлигининг ошиши;
- ҳаражат ва чиқимларнинг пасайиши;
- инновациянинг тезлашиши;
- бозорга маҳсулот ва хизматларни тақдим этиш вақтининг қисқариши;

- буюртмачилар ва шериклар холислигининг ошиши;
- рақобатлик қобилиятининг ошиши;
- меъёрий талабларга мосликни таъминлаш.

Юқорида келтирилган барча масалаларни ечишда корхона архитектурасидан фойдаланилади (1.2 -расм). Корхона архитектураси принциплар, ёндашишлар ва технологиялар наборини шакллантиришга имкон берадики, улар ташкилотнинг жорий ҳолатини ҳисобга олган ҳолда унинг келгуси трансформацияси, ўсиши ва ривожланиши асосини белгилайди.

1.2-расм. Корхона архитектураси ва унинг бошқа архитектуралар билан боғлиқлиги.

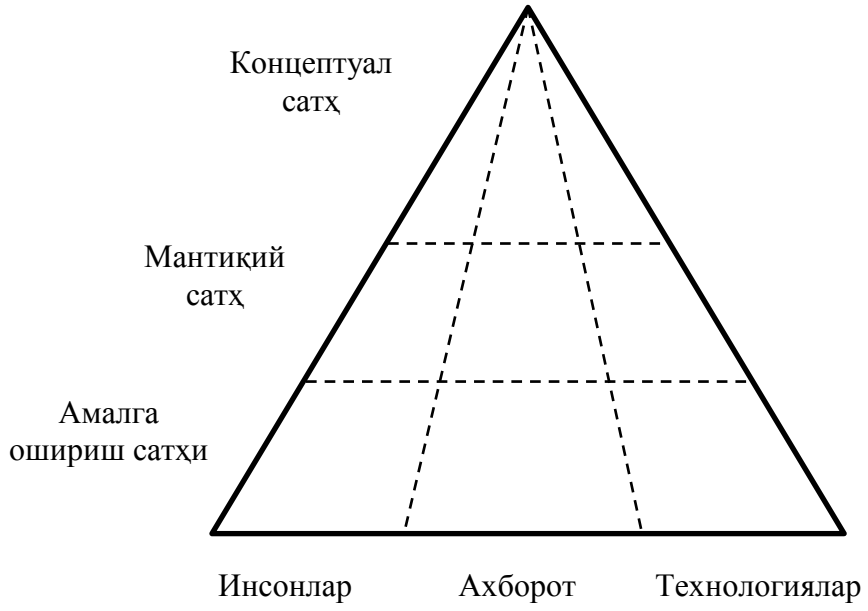
Ҳозирда бундай архитектураларни яратишда бир неча ёндашишлар мавжуд, масалан TOGAF, Zachman Framework, FEAF, DoDAF ва ҳ.

Аммо, қайси бир ёндашиш танланмасин, ҳозирги шароитда ахборотдан ва ахборот тизимидан фойдаланмай ривожланиш мумкин эмас. Ахборот ва ахборот тизимлари нафақат тижоратдаги ҳар қандай ўзгаришларни мададлайди, балки уларни олдиндан сезади, уларга олдиндан тайёрланади, баъзи холларда эса янги тижорат-имкониятларининг пайдо бўлишига ёрдам беради. Бироқ тижорат доимо исталганча ривожланмайди. Бунда

маълумотларнинг сирқиб чиқиши, ахборот технологиялари инфраструктураси элементларининг ишдан чиқиши ва ҳ. билан боғлиқ ахборот операцион хавф-хатарлар анчагина рол ўйнайди. Ҳозирги ва келажак хавф-хатарга тайёр бўлиш учун корхонанинг бошқа архитектуралари билан узвий боғланган ахборот хавфсизлиги архитектураси зарур.

Ахборот хавфсизлиги архитектураси жараёнларни, инсон ролини, технологияларни ва турли хил ахборотни тавсифлайди, ҳамда замонавий корхонанинг мураккаблигини ва ўзгарувчанлигини ҳисобга олади. Бошқача айтганда, ахборот хавфсизлигининг архитектураси ташкилотнинг ва у билан боғлиқ бошқа компонентлар ва интерфейсларнинг исталган ахборот хавфсизлиги тизими холатини тавсифлайди. Бунда ахборот хавфсизилиги архитектураси тижоратнинг жорий ва энг муҳими, келгусидаги эҳтиёжини акслантиради.

Одатда архитектуранинг 3 та сатҳи ажратилади – концептуал, мантиқий ва амалга ошириш (технологик). 1.3-расмда бундай архитектура келтирилган бўлиб, одатда технологиялар жиҳатидаги қисми хавфсизлик хизмати назоратидан четда қолади.

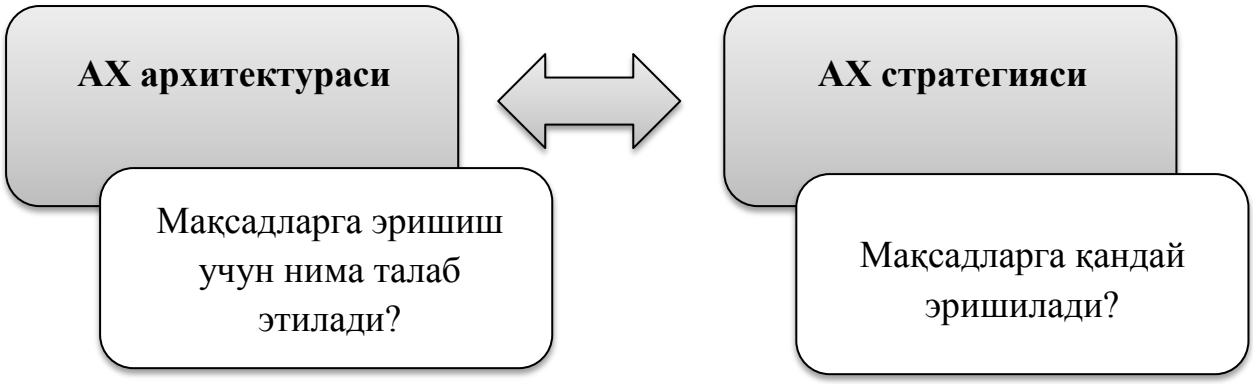


1.3-расм. Ахборот хавфсизлиги архитектураси

Жорий ҳолатдан қандай қилиб янги, мукаммалроқ ва қуйилган

мақсадларга мос ҳолатга ўтиш мумкин? Бунинг учун стратегия, яъни қуйилган мақсадларга эришиш учун ҳаракат йўналиши мавжуд.

Стратегия – корхонанинг давомли муваффақият билан фаолият юритишини таъминлашга мўлжалланган структураланган ва ўзаро боғланган ҳаракатлар тўплами. 1.4-расмда архитектура билан стратегиянинг ўзаро боғлиқлиги келтирилган. Стратегия ахборот хавфсизлиги архитектураси кўринишидаги мақсадга эга бўлган ҳолда унга эришишнинг оптимал йўлини белгилайди.



1.4-расм. Архитектура билан стратегиянинг ўзаро боғлиқлиги.

Кўпинча стратегия ва архитектура тушунчаларини фарқламай архитектура тавсифини ўз ичига олган ахборот хавфсизлиги стратегияси ишлаб чиқилади. Бу унчалик тўғри эмас, чунки архитектура, яъни мақсадлар вақт ўтиши билан ўзгармаслиги, бу мақсадларга эришишдаги стратегия эса ташқи ва ички омилларга боғлиқ ҳолда жиддий ўзгариши мумкин. Стратегия ва архитектура битта хужжатда тавсифланса, стратегия ўзгарганида архитектурани ҳам ўзгартиришга тўғри келади.

Назорат саволлари:

1. Ахборот хавфсизлиги архитектураси ва унинг сатҳлари моҳияти.
2. Ахборот хавфсизлиги стратегияси тушунчаси.
3. Корхона архитектурасини тузишда хавфсизлик стратегияси ва архитектурасининг ўрни.

II боб. АХБОРОТ ХАВФСИЗЛИГИГА БЎЛАДИГАН ТАХДИДЛАР, ХУЖУМЛАР ВА ЗАИФЛИКЛАР

2.1. Ахборот хавфсизлигига таҳдидлар ва уларнинг таҳлили

Ахборот хавфсизлигига бўлиши мумкин бўлган тахдидларни таҳлиллаш яратилаётган ҳимоялаш тизимига қўйиладиган талабларнинг тўлиқ тўпламини аниқлаш мақсадида амалга оширилади. Одатда *таҳдид* деганда (умумий маънода) кимнингдир манфаатларига зарар етказувчи ҳодиса (таъсир, жараён ёки воқеа) тушунилади. *Ахборот тизимига тахдид* деганда эса ахборот тизимининг хавфсизлигига бевосита ёки билвосита зарар етказувчи таъсир имкони тушунилади.

Замонавий ахборот тизимида сақланувчи ва ишланувчи ахборот жуда кўп омилларнинг таъсирига дучор бўлишлиги сабабли таҳдидларнинг тўлиқ тўпламини тавсифлаш масаласини формаллаштириш мумкин эмас. Шунинг учун тахдидларнинг тўлиқ руйхатини эмас, балки тахдидлар синфининг руйхатини аниқлаш мақсадга мувофиқ ҳисобланади.

Ахборот тизимига бўлиши мумкин бўлган тахдидларни таснифлашни уларнинг қуйидаги аломатлари бўйича амалга ошириш мумкин:

1. *Пайдо бўлиш табиати бўйича* қуйидагилар фарқланади:

- ахборот тизимига объектив физик жараёнлар ёки табиий ходисалар таъсирида пайдо бўлувчи *табиий тахдидлар*;
- инсон фаолияти сабаб бўлувчи ахборот тизимига *сунъий тахдидлар*.

2. *Намоён бўлишининг атайинлиги даражаси бўйича* қуйидагилар фарқланади:

- *ходимнинг хатоси ёки лоқайдлиги туфайли пайдо бўлувчи тахдидлар,* масалан ҳимоя воситасидан нотўғри фойдаланиш; хатоли маълумотларни киритиш ва ҳ.;
- *атайин қилинган ҳаракат натижасида пайдо бўлувчи тахдидлар,* масалан нияти бузуқларнинг ҳаракати.

3. *Тахдидларнинг бевосита манбаи бўйича* қуйидагилар фарқланади:

- *табиий муҳит,* масалан табиий офат, магнит бўрони ва ҳ.;
- *инсон,* масалан ходимнинг ёлланиши, конфиденциал маълумотларнинг ошкор этилиши ва ҳ.;
- *рухсат этилмаган дастурий-аппарат воситалар,* масалан компьютернинг бузғунчи функцияли вируслар билан захарланиши.

4. *Тахдидлар манбаининг ҳолати бўйича* қуйидагилар фарқланади:

- *назоратланувчи ахборот тизими зонасидан ташқарисидаги манба*, масалан алоқа канали бўйича узатилувчи маълумотларни, қурилмаларнинг электромагнит, акустик ва бошқа нурланишларини ушлаб қолиш;
- *назоратланувчи ахборот тизими чегарасидаги манба,* масалан яширинча эшитиш қурилмаларидан фойдаланиш, ёзувларни, ахборот элтувчиларни ўғрилаш ва ҳ.
- *бевосита ахборот тизимидаги манба,* масалан ахборот тизими ресурсларидан нотўғри фойдаланиш.

5. *Ахборот тизими фаоллигининг даражасига боғлиқлиги бўйича* қуйидагилар фарқланади:

- *ахборот тизими фаоллигига боғлиқ бўлмаган тахдидлар*, масалан ахборот криптоҳимоясининг фош этилиши;
- *фақат маълумотларни ишлаш жараёнидаги тахдидлар,* масалан дастурий вирусларни яратиш ва тарқатиш тахдиди.

6. *Ахборот тизимига таъсир даражаси бўйича* қуйидагилар фарқланади:

- *пассив тахдидлар,* ушбу тахдидлар амалга оширилганида ахборот тизими структураси ва мазмунида ҳеч нарса ўзгармайди, масалан махфий маълумотларни нусхалаш тахдиди;
- *актив тахдидлар,* ушбу тахдидлар амалга оширилганида ахборот тизими ва структураси ва мазмунига ўзгаришлар киритилади, масалан троян

оти ва вирусларнинг киритилиши.

7. *Фойдаланувчиларнинг ёки дастурларнинг ахборот тизими ресурсларидан фойдаланиш босқичлари бўйича* қуйидагилар фарқланади:

- *ахборот тизими ресурсларидан фойдаланиш босқичида намоён булувчи тахдидлар,* масалан ахборот тизимидан рухсатсиз фойдаланиш тахдидлари;

- *ахборот тизими ресурсларидан фойдаланишга рухсат берилганидан кейинги тахдидлар,* масалан ахборот тизими ресурсларидан рухсатсиз ёки нотўғри фойдаланиш тахдидлари.

8. *Ахборот тизими ресурсларидан фойдаланиш усуллари бўйича* қуйидагилар фарқланади:

- *ахборот ресурсларидан фойдаланишнинг стандарт йўлини ишлатадиган таҳдидлар*, масалан паролларга ва фойдаланишни чегаралашнинг бошқа реквизитларига ноқонуний эга бўлиб, руйхатга олинган фойдаланувчи сифатида ниқобланиш тахдиди;

- *ахборот ресурсларидан фойдаланишнинг яширин ностандарт йўлини ишлатадиган тахдидлар*, масалан операцион тизимнинг хужжатланмаган имкониятларини ишлатиб ахборот тизими ресурсларидан фойдаланиш тахдиди.

9. *Ахборот тизимида сақланадиган ва ишланадиган ахборотнинг жорий жойланиш жойи бўйича* қуйидагилар фарқланади:

- *ташқи хотира қурилмаларидаги ахборотдан фойдаланиш тахдиди*, масалан қаттиқ дискдан махфий ахборотни рухсатсиз нусхалаш;

- *асосий хотира ахборотидан фойдаланиш тахдиди*, масалан асосий хотиранинг қолдиқ ахборотини ўқиш;

- *алоқа каналларида айланувчи ахборотдан фойдаланиш тахдиди,* масалан алоқа каналига ноқонуний уланиб ёлғон хабарларни киритиш ёки узатилаётган хабарларни модификациялаш;

- *терминалда ёки принтерда акс эттирилган ахборотдан фойдаланиш тахдиди*, масалан акс эттирилган ахборотни яширинча

видеокамера ёрдамида ёзиб олиш.

Юқорида қайд этилганидек, ахборот тизимига хавфли таъсирлар тасодифийларига ёки атайинларига бўлинади. Ахборот тизимини лойиҳалаш, яратиш ва эксплуатация қилиш тажрибасининг таҳлили кўрсатадики, ахборот ахборот тизиминининг барча ишлаш босқичларида турли тасодифий таъсирлар остида бўлади.

Ахборот тизимининг эксплуатациясида *тасодифий таъсир* сабаблари қуйидагилар бўлиши мумкин:

- табиий офат ва электр таъминотининг узилиши сабабли авария ҳолатлари;
- аппаратуранинг ишдан чиқиши;
- дастурий таъминотдаги хатоликлар;
- хизматчи ходим ва фойдаланувчилар фаолиятидаги хатоликлар;
- ташқи муҳит таъсири сабабли алоқа каналидаги халаллар.

Дастурий таъминотдаги хатоликлар энг кўп учрайди. Чунки, серверлар, ишчи станциялар, маршрутизаторлар ва хакозоларнинг дастурий таъминоти инсон тарафидан ёзилади ва, демак, уларда деярли доимо хатоликлар мавжуд. Дастурий таъминот қанча мураккаб бўлса, ундаги хатоликларни ва заифликларни аниқлаш эҳтимоллиги шунча катта бўлади. Уларнинг аксарияти ҳеч қандай хавф туғдирмайди, баъзилари эса нияти бузуқнинг серверни назоратлаши, сервернинг ишдан чиқиши, ресурслардан рухсатсиз фойдаланиш каби жиддий оқибатларга сабаб бўлиши мумкин. Одатда бундай хатоликлар дастурий таъминот ишлаб чиқарувчилар томонидан мунтазам тақдим этилувчи янгилаш пакети ёрдамида бартараф этилади. Бундай пакетларнинг ўз вақтида ўрнатилиши ахборот хавфсизлигининг зарурий шарти ҳисобланади.

Атайин қилинадиган тахдидлар нияти бузуқнинг мақсадга йўналтирилган ҳаракатлари билан боғлиқ. Нияти бузуқ сифатида ташкилот ходимини, қатновчини, ёлланган кишини ва ҳ. кўрсатиш мумкин. Аввало ташкилот ходимининг нияти бузуқ билан тушунган ҳолда ҳамкорлик

қилишига эътибор бериши лозим. Бундай ҳамкорликка ундовчи сабаблар қуйидагилар:

- ташкилот ходимининг раҳбариятга қасдлик қилиш мақсадида;
- нияти бузуқ қарашларнинг ҳаққонийлигига ишонган ҳолда;
- ходимнинг ташкилот раҳбариятининг ноқонуний фаолият юритилаётганлигига ишонган ҳолда;
- ёлғон ҳаракатлар, таъмагирлик, шантаж, характернинг салбий жиҳатларидан фойдаланиш, зўрлаш йўли билан ҳамкорликка ундаш ва ҳ.

Назорат саволлари:

1. Ахборот хавфсизлигига бўладиган тахдидлар тушунчаси қандай ифодаланади?
2. Тахдидларни таснифлашда қандай аломатлари асос қилиб олинади?
3. Табиий ва сунъий тахдидларни тушунтириб беринг.
4. Билмасдан ва атайин қилинадиган тахдидларни тушунтириб беринг.

2.2. Ахборот хавфсизлигининг заифликлари

Заифликлар ташкилот активлари билан ассоцияцияланган ҳимоянинг кучсизликларини ифодалайди. Ушбу кучсизликлар номақбул можароларга сабаб бўлувчи битта ёки бир неча таҳдидлар томонидан фойдаланиши мумкин. Заифликнинг ўзи зарар етказмайди, аммо активларга зарар етказишга имкон берувчи шароит ёки шароитлар тўплами ҳисобланади. Бошқача айтганда, заифликлар – таҳдидларнинг муваффақиятли амалга оширилишига имкон берувчи ҳар қандай омиллар. Шу сабабли заифликларни баҳолаш учун мавжуд хавфсизлик механизмларини идентификациялаш ва уларнинг самарадорлигини баҳолаш зарур.

Активларга зарар етказа олувчи можароларга сабаб бўлиш учун тахдидлар ва заифликлар бирлашишлари лозим. Шунинг учун тахдидлар

билан заифликлар орасидаги боғлиқликни аниқлаш зарур. Қуйида хавфсизликнинг турли жабхаларидаги заифликларга ва улардан фойдалана оладиган тахдидларга мисоллар келтирилган.

1. Кадр ресурсларининг хавфсизлиги (ISO/IEC 27002:2005, 8-бўлим)	
Заифлик	***Заифликдан фойдаланувчи таҳдид***
Хавфсизликни етарлича ўргатилмаслиги	Техник мададлаш ходимининг хатоси.
Хавфсизлик масалалаларидан бехабарлиги	Фойдаланувчилар хатоси
Мониторинг механизмларининг мавжуд эмаслиги	Дастурий таъминотдан рухсатсиз фойдаланиш
Телекоммуникация ва хабарларни узатиш воситаларидан коррект (тўғри) фойдаланиш бўйича сиёсатнинг мавжуд эмаслиги	Тармоқ ускунасидан рухсатсиз фойдаланиш
Ишдан бўшатилганда фойдаланиш хуқуқи бекор қилинмайди	Рухсатсиз фойдаланиш
Ишдан бўшатилганда ресурсларни қайтаришни кафолатловчи муолажа мавжуд эмас	Ўғрилик
Асоссиз ёки норози ходим	Ахборотни ишловчи воситаларнинг суиистеъмол қилиниши
Бегона ходимнинг ёки ишдан кейин ишловчи ходимнинг назоратсиз ишлаши.	Ўғрилик

2. Физик хавфсизлик ва атроф муҳит хавфсизлиги (ISO/IEC 27002:2005, 9-бўлим)	
Заифлик	***Заифликдан фойдаланувчи***

	таҳдид
Бинодан, хоналардан, офислардан адекват бўлмаган ёки эътиборсиз физик назоратлаш механизмларидан фойдаланиш	Атайин зарар етказиш
Бинони, эшикларни ва дереазаларни физик ҳимоялашнинг йўқлиги	Ўғрилик
Сув тошишига дучор зонада жойланиши	Чўкиш
Ҳимояланмаган сақлаш	Ўғрилик
Ахборотни сақлаш воситаларининг номувофиқ ўрнатилиши/номуносиб олиб юрилиши	Олиб юрилиши жараёнида хатолик
Ускунани даврий алмаштириш схемасининг йўқлиги	Ахборотни сақлаш воситаларининг эскириши
Ускунанинг намликка, чангликка ва ифлосланишга дучор бўлиши	Чанг босиши
Ускунанинг харорат ўзгаришига дучор бўлиши	Харорат режимининг бузилиши
Ускунанинг кучланиш ўзгаришига дучор бўлиши	Электр манбаининг флуктуацияси
Беқарор электр манбаи	Электр манбаининг флуктуацияси

3. Коммуникацияларни ва амалларни бошқариш (ISO/IEC 27002:2005, 10-бўлим)	
Заифлик	***Заифликдан фойдаланувчи таҳдид***
Мураккаб фойдаланувчи интерфейси	Ходим хатоси
Ахборотни сақлаш воситаларини	Ахборотдан рухсатсиз фойдаланиш

тегишлича тозаламасдан ўтказиш ёки улардан такроран фойдаланиш	
Ўзгаришларнинг адекват бўлмаган назорати	Хавфсизлик тизимининг тўхтаб қолиши
Тармоқни адекват бўлмаган бошқариш	Трафикнинг ортиқча юкланиши
Захирали нусхалаш муолажаларининг йўқлиги	Ахборотнинг йўқолиши
Хабарнинг жўнатилганлиги ёки олинганлиги хусусидаги исботнинг йўқлиги	Жавобгарликдан бош тортиш
Зарар келтирувчи коддан ҳимоялашда ишлатилувчи дастурий таъминотнинг янгиланмаслиги	Вирус инфекцияси
Вазифларнинг тақсимланмаганлиги	Тизимни суиистеъмол қилиш (тасодифий ёки атайин)
Тест ва ишчи ускунанинг ажратилмаганлиги	Ҳаракатдаги тизимни рухсатсиз модификациялаш
Назоратсиз нусхалаш	Ўғрилик
Умумфойдаланувчи тармоқларга ҳимояланмаган уланишлар	Дастурий таъминотдан авторизацияланмаган фойдаланувчиларнинг фойдаланиши

4. Фойдаланиш назорати (ISO/IEC 27002:2005, 11-бўлим)	
Заифлик	***Заифликдан фойдаланувчи таҳдид***
Тармоқдарда фойдаланишни нотўғри чеклаш	Тармоққа рухсатсиз уланиш
Тоза столлар ва тоза экранлар	Ахборотнинг йўқолиши ёки

сиёсатининг йўқлиги	шикастланиши
Фойдаланувчиларнинг аутентификацияси каби идентификация ва аутентификация механизмларининг йўқлиги	Бегона фойдаланиш идентификаторини ўзлаштириш.
Мобил компьютер ускуна ҳимоясининг йўқлиги	Ахборотдан рухсатсиз фойдаланиш
Ишчи станция алоқани узганида тизимдан чиқаолмаслиги	Авторизацияланмаган фойдаланувчилар томонидан дастурий таъминотнинг ишлатилиши.
Дастурий таъминотни тестлашнинг номувофиқ хажмда ўтказилиши ёки йўқлиги	Авторизацияланмаган фойдаланувчилар томонидан дастурий таъминотнинг ишлатилиши.
Фойдаланувчиларнинг фойдаланиш хуқуқлари назоратининг ва таҳлилининг йўқлиги	Ташкилотни тарк этган ёки иш жойини ўзгартирган фойдаланувчилар томонидан фойдаланиш
Паролларни ёмон бошқариш (осонгина аниқланадиган пароллар, тез-тез алмаштирмаслик ва ҳ.)	Бегона фойдаланиш идентификаторини ўзлаштириш
Тизим утилиталаридан назоратсиз фойдаланиш	Тизим ёки иловани назоратлаш механизмларига риоя қилмаслик

5. Ахборот тизимларига эришиш(харид қилиш), ишлаб чиқиш ва кузатиш (ISO/IEC 27002:2005, 12-бўлим)	
Заифлик	***Заифликдан фойдаланувчи таҳдид***
Крипографик калитларни номувофиқ ҳимоялаш	Ахборотнинг ошкор этилиши

Криптографиядан фойдаланиш соҳасидаги мукаммал бўлмаган сиёсат	Қонунларнинг ёки маъёрий асосларнинг бузилиши
Кирувчи ёки чиқувчи маълумотлар назоратининг йўқлиги	Хатолик
Ишланадиган маълумотларнинг текширилмаслиги	Ахборотнинг бузилиши
Дастурий таъминотни тестлашнинг йўқлиги ёки етарлича хажмда бажарилмаслиги	Авторизацияланмаган фойдаланувчиларнинг дастурий таъминотдан фойдаланиши.
Ёмон хужжатланган дастурий таъминот	Техник мададловчи ходимнинг хатоси
Ишлаб чиқарувчилар учун тушунарсиз ёки тўлиқ бўлмаган спецификациялар	Дастурий таъминотнинг адашиши
Дастурий таъминотнинг назоратсиз юкланиши ва ишлатилиши	Зарар етказувчи дастурий таъминот
Корпоратив иловаларда шартли текин ёки текин дастурий таъминотдан назоратсиз фойдаланиш	Хуқуқий жавобгарлик
Дастурий таъминотдаги маълум нуқсонлар	Дастурий таъминотдан авторизацияланмаган фойдаланувчиларнинг фойдаланиши
Тест маълумотларини нотўғри танлаш	Шахсий маълумотлардан рухсатсиз фойдаланиш.

Назорат саволлари:

1. Ахборот хавфсизлигида заифлик тушунчаси.
2. Кадр ресурсларининг хавфсизлиги жиҳатидан келиб чиқадиган заифликларни тавсифлаб беринг.

3. Физик хавфсизлик ва атроф муҳит хавфсизлиги жиҳатидан келиб чиқадиган заифликларни тавсифлаб беринг.

4. Коммуникацияларни ва амалларни бошқариш жиҳатидан келиб чиқадиган заифликларни тавсифлаб беринг.

5. Фойдаланишларни назоратлаш жиҳатидан келиб чиқадиган заифликларни тавсифлаб беринг.

6. Ахборот коммуникация тизимларини харид қилиш, ишлаб чиқиш ва кузатиш жиҳатидан келиб чиқадиган заифликларни тавсифлаб беринг.

2.3. Ахборотнинг маҳфийлигини, яхлитлигини ва фойдаланувчанлигини бузиш усуллари

Барча хужумлар Internet ишлаши принципларининг қандайдир чегараланган сонига асосланганлиги сабабли масофадан бўладиган намунавий хужумларни ажратиш ва уларга қарши қандайдир комплекс чораларни тавсия этиш мумкин. Бу чоралар, ҳақиқатан, тармоқ хавфсизлигини таъминлайди.

Internet протоколларининг мукаммал эмаслиги сабабли тармоқдаги ахборотга масофадан бўладиган асосий намунавий хужумлар қуйидагилар:

- тармоқ трафигини тахлиллаш;
- тармоқнинг ёлғон обьектини киритиш;
- ёлғон маршрутни киритиш;
- хизмат қилишдан воз кечишга ундайдиган хужумлар.

Тармоқ трафигини тахлиллаш. Сервердан Internet тармоғи базавий протоколлари FTP (Файлларни узатиш протоколи) ва TELNET (Виртуал терминал протоколи) бўйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини ўтиши лозим. Фойдаланувчини идентификациялашда ахборот сифатида унинг идентификатори (исми) ишлатилса, аутентификациялаш учун *парол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдалувчиларнинг пароли ва идентификатори тармоқ орқали очиқ, шифрланмаган кўринишда узатилади. Де-

мак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

Ахборот алмашинувида Internetнинг масофадаги иккита узели алмашинув ахборотини *пакетларга* ажратади. Пакетлар алоқа каналлари орқали узатилади ва шу пайтда ушлаб қолиниши мумкин.

FTP ва TELNET протоколларининг тахлили кўрсатадики, TELNET паролни символларга ажратади ва паролнинг ҳар бир символини мос пакетга жойлаштириб битталаб узатади, FTP эса, аксинча, паролни бутунлайича битта пакетда узатади. Пароллар шифрланмаганлиги сабабли пакетларнинг махсус сканер-дастурлари ёрдамида фойдаланувчининг исми ва пароли бўлган пакетни ажратиб олиш мумкин. Шу сабабли, ҳозирда оммавий тус олган ICQ (Бир лаҳзали алмашиш хизмати) дастури ҳам ишончли эмас. ICQнинг протоколлари ва ахборотларни сақлаш, узатиш форматлари маълум ва демак, унинг трафиги ушлаб қолиниши ва очилиши мумкин.

Асосий муаммо алмашинув протоколида. Базавий татбиқий проколларнинг TCP/IP оиласи анча олдин (60-йилларнинг охири ва 80-йилларнинг боши) ишлаб чиқилган ва ундан бери умуман ўзгартирилмаган. Ўтган давр мобайнида тақсимланган тармоқ хавфсизлигини таъминлашга ёндашиш жиддий ўзгарди. Тармоқ уланишларини ҳимоялашга ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чиқилди. Аммо бу протоколлар эскиларининг ўрнини олмади (SSL бундан истисно) ва стандарт мақомига эга бўлмади. Бу протоколларнинг стандарт бўлиши учун эса тармоқдан фойдаланувчиларнинг барчаси уларга ўтишлари лозим. Аммо, Internetда тармоқни марказлашган бошқариш бўлмаганлиги сабабли бу жараён яна кўп йиллар давом этиши мумкин.

Тармоқнинг ёлғон объектни киритиш. Ҳар қандай тақсимланган тармоқда қидириш ва адреслаш каби "нозик жойлари" мавжуд. Ушбу жараёнлар кечишида тармоқнинг ёлғон объектини (одатда бу ёлғон хост) киритиш имконияти туғилади. Ёлғон обьектнинг киритилиши натижасида адресатга узатмоқчи бўлган барча ахборот аслида нияти бузуқ одамга тегади. Тахминан

буни тизимингизга, одатда электрон почтани жўнатишда фойдаланадиган провайдерингиз сервери адреси ёрдамида, киришга кимдир уддасидан чиққани каби тасаввур этиш мумкин. Бу ҳолда нияти бузуқ одам унчалик қийналмасдан электрон хат-хабарингизни эгаллаши мумкин, сиз эса хатто ундан шубхаланмасдан ўзингиз барча электрон почтангизни жўнатган бўлар эдингиз.

Қандайдир хостга мурожаат этилганида адресларни махсус ўзгартиришлар амалга оширилади (IP-адресдан тармоқ адаптери ёки маршрутизаторининг физик адреси аниқланади). Internetда бу муаммони ечишда ARP (Канал сатҳи протоколи) протоколидан фойдаланилади. Бу қуйидагича амалга оширилади: тармоқ ресурсларига биринчи мурожаат этилганида хост кенг кўламли ARP-сўровни жўнатади. Бу сўровни тармоқнинг берилган сегментидаги барча станциялар қабул қилади. Сўровни қабул қилиб, хост сўров юборган хост хусусидаги ахборотни ўзининг ARP-жадвалига киритади, сўнгра унга ўзининг Ethernet-адреси бўлган ARP-жавобни жўнатади. Агар бу сегментда бундай хост бўлмаса, тармоқнинг бошқа сегментларига мурожаатга имкон берувчи маршрутизаторга мурожаат қилинади. Агар фойдаланувчи ва нияти бузуқ одам бир сегментда бўлса, ARP-сўровни ушлаб қолиш ва ёлғон ARP-жавобни йўллаш мумкин бўлади. Бу усулнинг таъсири фақат битта сегмент билан чегараланганлиги тасалли сифатида хизмат қилиши мумкин.

ARP билан бўлган холга ўхшаб DNS-суровни ушлаб қолиш йўли билан Internet тармоғига ёлғон DNS-серверни киритиш мумкин.

Бу қуйидаги алгоритм бўйича амалга оширилади:

- DNS-сўровни кутиш;

- олинган сўровдан керакли маълумотни чиқариб олиш ва тармоқ бўйича сўров юборган хостга ёлғон DNS-жавобни ҳақиқий DNS-сервер номидан узатиш. Бу жавобда ёлғон DNS-сервернинг IP-адреси кўрсатилган бўлади;

- хостдан пакет олинганида пакетнинг IP-сарлавхасидаги IP-адресни ёлғон DNS сервернинг IP-адресига ўзгартириш ва пакетни серверга узатиш

(яъни ёлғон DNS-сервер ўзининг номидан сервер билан иш олиб боради);

- сервердан пакетни олишда пакетнинг IP-сарлавҳасидаги IP-адресни ёлғон DNS-серверинг IP-адресига ўзгартириш ва пакетни хостга узатиш (ёлғон DNS серверни хост ҳақиқий ҳисоблайди).

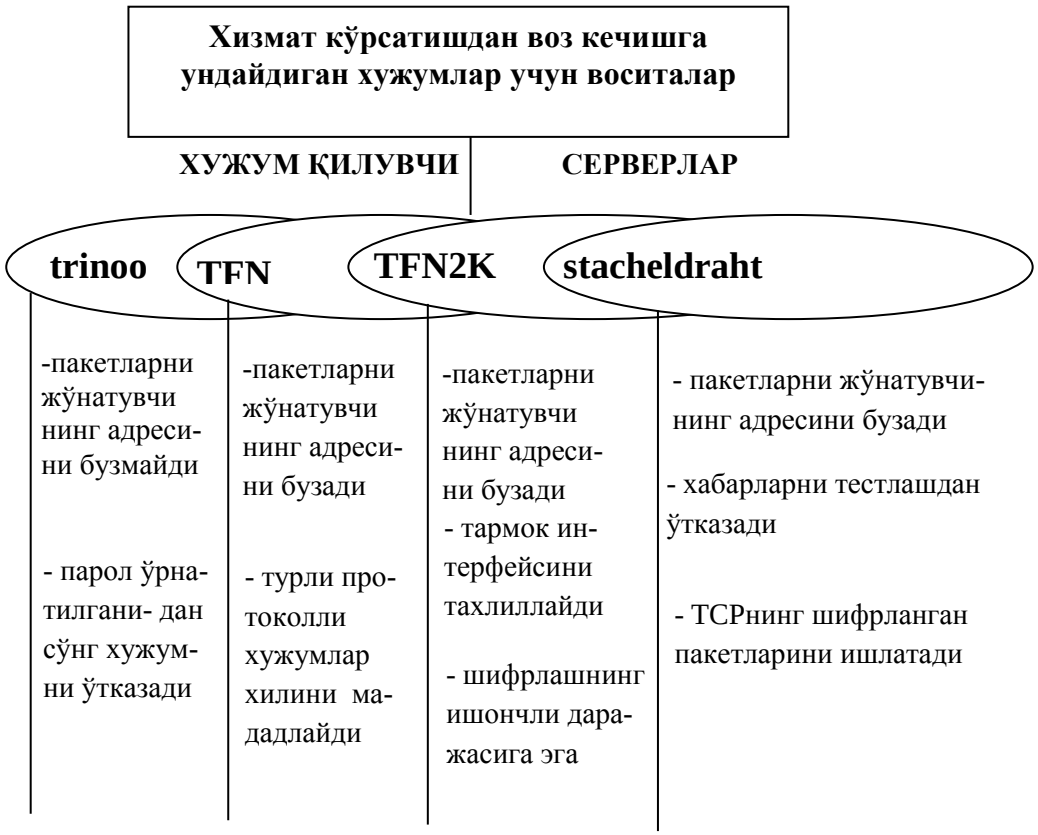
Ёлғон маршрутни киритиш. Маълумки, замонавий глобал тармоқлари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармоқ сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан қабул қилувчига узатишга хизмат қилувчи тармоқ узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи махсус протоколлар мавжуд. Internetдаги бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи – ICMP (Тармоқлараро бошқарувчи хабарлар протоколи) ва маршрутизаторларни масофадан бошқариш протоколи SNMP (Тармоқни бошқаришнинг оддий протоколи) мисол бўлаолади. Маршрутни ўзгартириш хужум қилувчи ёлғон хостни киритишидан бўлак нарса эмас. Хатто охирги обьект ҳақиқий бўлса ҳам маршрутни ахборот бари бир ёлғон хостдан ўтадиган қилиб қуриш мумкин.

Маршрутни ўзгартириш учун хужум қилувчи тармоққа тармоқни бошқарувчи қурилмалар (масалан, маршрутизаторлар) номидан берилган тармоқни бошқарувчи протоколлар орқали аниқланган махсус хизматчи хабарларни жўнатиши лозим. Маршрутни муваффақиятли ўзгартириш натижасида хужум қилувчи тақсимланган тармоқдаги иккита обьект алмашадиган ахборот оқимидан тўла назоратга эга бўлади, сўнгра ахборотни ушлаб қолиши, тахлиллаши, модификациялаши ёки оддийгина йўқотиши мумкин. Бошқача айтганда, тахдидларнинг барча турларини амалга ошириш имконияти туғилади.

Хизмат қилишдан воз кечишга ундайдиган тақсимланган хужумлар – DdoS (Хизмат қилишдан тақсимланган воз кечиш) компьютер жиноятчилигининг нисбатан янги хили бўлсада, қўрқинчли тезлик билан тарқалмоқда. Бу хужумларнинг ўзи анчагина ёқимсиз бўлгани етмаганидек,

улар бир вақтнинг ўзида масофадан бошқарилувчи юзлаб хужум қилувчи серверлар томонидан бошланиши мумкин. Хакерлар томонидан ташкил этилган узелларда DDoS хужумлар учун учта инструментал воситани топиш мумкин: trinoo, TribeFloodNet (TFN) ва TFN2K. Яқинда TFN ва trinoонинг энг ёқимсиз сифатларини уйғунлаштирган яна биттаси stacheldraht ("тикон симлар") пайдо бўлди.

2.1-расмда хизмат қилишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари келтирилган.



2.1-расм. Хизмат килишдан воз кечишга ундайдиган хужум воситаларининг характеристикалари

Назорат саволлари:

1. Тармоқ трафигини таҳлиллашга асосланган бузиш усулларини тушунтириб беринг.
2. Тармоқнинг ёлғон объектини киритишга асосланган бузиш усулини ишлаш принципини тушунтириб беринг.
3. Ёлғон маршрутни киритиш қандай амалга оширилади?

4. Хизмат қилишдан воз кечишга ундайдиган бузиш усули турларини тавсифлаб беринг.

III боб. АХБОРОТ ХАВФСИЗЛИГИ СОҲАСИГА ОИД ХАЛҚАРО ВА МИЛЛИЙ МЕЪЁРИЙ-ХУҚУҚИЙ БАЗА

3.1. Ахборот хавфсизлиги соҳасига оид ҳалқаро стандартлар

ISO/IEC 27001:2005 – “Ахборот технологиялари. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқариш тизимлари. Талаблар”. Ушбу стандарт ахборот хавфсизлигини бошқариш тизимини (АХБТ) ишлаб чиқиш, жорий этиш, унинг ишлаши, мониторинги, таҳлили, унга хизмат кўрсатиш ва уни такомиллаштириш модели ва талабларидан иборат. АХБТ жорий этилиши ташкилотнинг стратегик қарори бўлиб қолиши керак. АХБТни ишлаб чиқиш ва жорий этишда хавфсизликнинг эҳтиёжлари, мақсадлари, фойдаланиладиган жараёнлари, ташкилотнинг кўлами ва структураси ҳисобга олиниши керак. АХБТ ва унинг ёрдамчи тизимлари вақт ўтиши билан ўзгаради деган тахмин бор. Шунингдек, АХБТни кенгайтириш масштаблари ташкилотнинг эҳтиёжларига боғлиқ бўлади, масалан, оддий вазият АХБТ учун оддий ечимни талаб қилади. Мувофиқликни баҳолаш учун ушбу стандартдан ички ва ташқи томонлар фойдаланиши мумкин.

Жараёнли ёндашув. Ушбу стандарт ташкилот АХБТни ишлаб чиқиш, жорий этиш, унинг ишлаши, мониторинги, таҳлили, унга хизмат кўрсатиш ва уни такомиллаштиришда жараёнли ёндашувнинг қўлланишига йўналтирилган.

Ташкилот муваффақиятли ишлаши учун фаолиятнинг кўп сонли ўзаро боғлиқ турларини аниқлаши ва уларни бошқаришни амалга ошириши керак. Активлардан фойдаланувчи ва киришларни чиқишларга ўзгартириш мақсадида бошқариладиган фаолиятнинг барча турларига жараёнлар сифатида қараш мумкин. Кўпинча бир жараённинг чиқиши кейинги жараённинг бевосита киришини ҳосил қилади.

Ташкилотда жараёнлар тизимини идентификациялаш ва уларнинг ўзаро ҳаракати билан бир қаторда жараёнлар тизимидан фойдаланиш,

шунингдек, жараёнларни бошқариш *жараёнли ёндашув* деб ҳисобланиши мумкин.

Бундай ёндашув ахборот хавфсизлигида қўлланганда қуйидагиларнинг муҳимлигини таъкидлайди:

- ташкилотнинг ахборот хавфсизлиги талабларини ва ахборот хавфсизлиги сиёсати ва мақсадларини белгилаш зарурлигини тушуниш;

- ташкилот барча бизнес-таваккалчиликларнинг умумий контекстида ташкилот ахборот хавфсизлиги хатарларини бошқариш чораларини жорий этиш ва қўллаш;

- АХБТ унумдорлиги ва самарадорлигининг доимий мониторинги ва таҳлили;

- объектив ўлчашлар натижаларига асосланган узлуксиз такомиллаштириш.

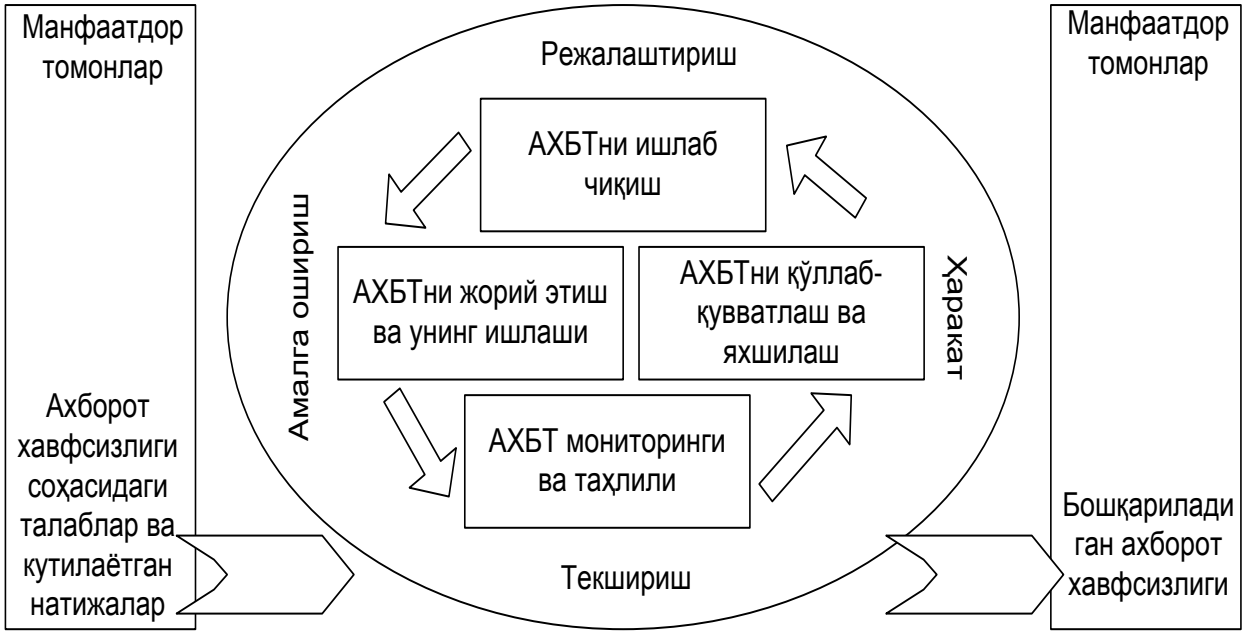
Ушбу стандартда АХБТ ҳар бир жараёнини ишлаб чиқишда қўлланиши мумкин бўлган *режалаштириш – амалга ошириш – текшириш - ҳаракат* [«Plan-Do-Check-Act» (PDCA)] модели келтирилган.

Ушбу модель АХБТ ахборот хавфсизлиги талаблари ва манфаатдор томонларнинг кутилаётган натижаларидан кирувчи маълумотлар сифатида қандай фойдаланишини ва зарур хатти-ҳаракатлар ва жараёнларни амалга ошириш натижасида эълон қилинган талаблар ва кутилаётган натижаларни қаноатлантиришидан далолат берадиган маълумотларни олишини кўрсатади.

Бундан ташқари, PDCA модели «Ахборот тизимлари ва тармоқлари хавфсизлиги бўйича иқтисодий ҳамкорлик ва ривожланиш ташкилотининг амалдаги кўрсатмаларига мос келади. Ушбу стандарт хатарларни бошқариш, хавфсизлик чораларини режалаштириш ва амалга ошириш, хавфсизликни бошқариш ва қайта баҳолашда ушбу принципларни қўллашнинг амалий моделини тақдим этади.

1-мисол. Ахборот хавфсизлигининг бузилиши ташкилот учун жиддий молиявий йўқотишларнинг ва/ёки қандайдир қийинчиликларнинг сабаби бўла олмайди деган талаб қўйилиши мумкин.

2-мисол. Қандайдир жиддий можаро, масалан, сайт ёрдамида электрон савдони амалга ошираётган ташкилот сайтининг бузилиши натижасида юзага келадиган ҳолат учун – ташкилот бузилиш оқибатларини минимумга келтириш учун етарли билим ва тажрибага эга бўлган мутахассисларга эга бўлиши керак.



3.1-расм. АХБТ жараёнларига PDCA моделини қўллаш.

Бошқа бошқариш тизимлари билан мослашув. Ушбу стандарт бошқа бошқарув стандартлари билан мослашувини яхшилаш ва интеграция қилиш учун ИСО 9001:2000 [2] ва ИСО 14001:2004 [3] стандартлари билан мувофиқлаштирилган. Керакли тарзда лойиҳалаштирилган битта бошқарув тизими барча ушбу стандартларнинг талабларига жавоб беришга қодир. 3.1-жадвалда ушбу стандартнинг ISO 9001:2000 ва ISO 14001:2004 стандартлари билан ўзаро боғлиқлиги кўрсатилган.

Ушбу стандарт ташкилотга амалдаги АХБТни бошқа бошқарув тизимларининг тегишли талаблари билан мослаштириш ёки интеграция қилиш имконини беради.

3.1-жадвал.

Режалаштириш (АХБТни ишлаб чиқиш)	Ташкилотнинг умумий сиёсати ва мақсадларида эълон қилинган натижаларга эришиш мақсадида сиёсат ва мақсадларни белгилаш, хатарларни бошқариш ва ахборот хавфсизлигини такомиллаштириш билан боғлиқ бўлган жараёнлар ва процедураларни аниқлаш.
Амалга ошириш (АХБТни жорий этиш ва унинг ишлаши)	АХБТ сиёсати, методлари, жараёнлари ва процедураларини жорий этиш ва унинг ишлаши.
Текшириш (АХБТ мониторинги ва таҳлили)	Жараёнларнинг АХБТ сиёсати ва мақсадларига мувофиқлигини баҳолаш ва зарурат бўлганида самарадорлигини ўлчаш. Натижаларнинг юқори раҳбарият томонидан таҳлил қилиниши.
Ҳаракат (АХБТни қўллаб қувватлаш ва такомиллаштириш)	АХБТ ички аудитлари натижаларига, раҳбарият томонидан қилинган таҳлил ёки узлуксиз такомиллаштириш мақсадида бошқа манбалардан олинган маълумотларга асосланган тузатувчи ва огоҳлантирувчи ҳаракатларни бажариш

ISO/IEC 27002:2005 – “Ахборот технологияси. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари.

Ахборот - бизнеснинг бошқа муҳим активлари каби қийматга эга бўлган актив ва шундай экан, у тегишли равишда муҳофаза қилинган бўлиши керак. Бу ўзаро алоқалар билан доимо ривожланаётган амалий иш муҳитида айниқса муҳим. Ҳозирги вақтда ушбу ўзаро алоқалар

натижасида ахборот таҳдидлар ва заифликларнинг ўсиб бораётган сони ва турли хилига дучор бўлмоқда.

Ахборот турли шаклларда мавжуд бўлиши мумкин. У қоғоз элтувчида жойлаштирилган бўлиши, электрон кўринишда сақланиши, почта орқали ёки телекоммуникациянинг электрон воситаларидан фойдаланиб узатилиши, пленкадан намойиш қилиниши ёки оғзаки ифодаланиши мумкин. Ахборот мавжудлигининг шаклидан, уни тарқатиш ёки сақлаш усулидан қатъи назар у доим адекват муҳофазаланган бўлиши керак.

Ахборот хавфсизлиги - ахборотни бизнеснинг узлуксизлигини таъминлаш, бизнес хавфларини минимумга келтириш ва инвестицияларни қайтаришни ҳамда бизнес имкониятларини максимал ошириш мақсадида таҳдидларнинг кенг спектридан муҳофаза қилиш демакдир.

Ахборот хавфсизлигига дастурий таъминотнинг сиёсатлари, методлари, муолажалари, ташкилий тузилмалари ва дастурий таъминот функциялари томонидан тақдим этилиши мумкин бўлган ахборот хавфсизлигини бошқариш бўйича тадбирларнинг тегишли комплексини амалга ошириш йўли билан эришилади. Кўрсатилган тадбирлар ташкилотнинг ахборот хавфсизлиги мақсадларига эришишини таъминлаши керак.

Ахборот хавфсизлигининг зарурати. Ахборот ва уни сақлаб турувчи жараёнлар, ахборот тизимлари ва тармоқ инфратузилмаси бизнеснинг бебаҳо активлари бўлиб ҳисобланади. Ахборот хавфсилигини аниқлаш, таъминлаш, сақлаб туриш ва яхшилаш ташкилотнинг рақобатбардошлилиги, қадрлилиги, даромадлилиги, қонун ҳужжатларига мувофиқлигини ва ишбилармонлик обрўсини таъминлашда катта аҳамиятга эга.

Ташкилотлар, уларнинг ахборот тизимлари ва тармоқлар хавфсизликнинг турли компьютер фирибгарлиги, айғоқчилик, зараркунандалик, вандализм, ёнғинлар ёки сув тошқинлари каби таҳдидлар билан кўпроқ тўқнашмоқдалар. Зарарнинг бундай компьютер

вируслари, компьютерни бузиб очиш ва « хизмат кўрсатишдан бош тортиш» каби ҳужумлар манбалари кенг тарқалмоқда, тажовузкор бўлиб бормоқда ва кўпроқ маҳорат билан шаклланмоқда.

Ахборот хавфсизлиги бизнеснинг жамоат ва хусусий секторида, шунингдек критик инфратузилмаларни муҳофаза қилишда муҳим. Ахборот хавфсизлиги иккала секторда ҳам ёрдам бериши керак, масалан электрон ҳукуматни ёки электрон бизнесни жорий қилишда тегишли хавфлардан мустасно бўлиш ёки уларни камайтириш учун. Умумий фойдаланишдаги тармоқларнинг ва хусусий тармоқларнинг биргаликда ишлаши, шунингдек, ахборот ресурсларидан биргаликда фойдаланиши ахборотдан фойдаланишни бошқаришни қийинлаштиради. Маълумотларга тақсимлаб ишлов беришдан фойдаланиш тенденцияси марказлаштирилган назорат самарадорлигини сусайтиради.

Кўпгина ахборот тизимларини лойиҳалашда хавфсизлик масалалари эътиборга олинмас эди. Техник воситалар билан эришилиши мумкин бўлган хавфсизлик даражаси бир қатор чеклашларга эга бинобарин, тегишли бошқарув воситалари ва процедуралар билан таъминланиши керак. Ахборот хавфсизлигини бошқариш бўйича зарур тадбирларни танлаш пухталик билан режалаштириш ва деталлаштиришни талаб қилади.

Ахборот хавфсизлигини бошқариш, камида ташкилот барча ходимларининг иштирок этишига муҳтож. Шунингдек, етказиб берувчилар, мижозлар ёки акциядорларнинг иштирок этиши ҳам талаб қилиниши мумкин. Бундан ташқари, бегона ташкилот мутахассисларининг маслаҳатлари керак бўлиб қолиши мумкин.

Агар ахборот хавфсизлиги соҳасини бошқариш бўйича тадбирлар ахборот тизимини лойиҳалаштириш босқичида техник топшириққа киритилса, анча арзонга тушади ва самаралироқ бўлади.

Ахборот хавфсизлиги талабларини аниқлаш. Ташкилот ўзининг ахборот хавфсизлигига бўлган талабларини қуйидаги учта муҳим омилни ҳисобга олиб аниқлаши муҳим:

- бизнеснинг глобал стратегияси ва ташкилотнинг мақсадларини эътиборга олиб, ташкилотда олинган хавфларни баҳолаш ёрдамида ташкилот активларига таҳдидлар аниқланади, тегишли активларнинг заифлиги ва таҳдидлар пайдо бўлиш эҳтимоли, шунингдек келиб чиқиши мумкин бўлган оқибатлар баҳоланади;

-ташкилот, унинг савдо шериклари, пудратчилар ва хизматларни етказиб берувчилар, қониқтириши керак бўлган юридик талаблар, қонун ҳужжатларининг талаблари, тартибга солувчи ва шартномавий талаблар, шунингдек, ушбу томонларинг ижтимоий маданий муҳити бошқа омил бўлиб ҳисобланади;

-ўзининг ишлашини таъминлаш учун ташкилот томонидан ишлаб чиқилган принциплар, мақсадлар ва талабларнинг махсус тўплами яна бир омил бўлиб ҳисобланади.

Ахборот хавфсизлиги хавфларини баҳолаш. Ахборот хавфсизлигига қўйиладиган талаблар хавфларни мунтазам баҳолаш ёрдамида аниқланади. Ахборот хавфсизлигини бошқариш бўйича тадбирларга кетган сарф-харажатлар ахборот хавфсизлигининг бузилиши натижасида ташкилотга етказилиши мумкин бўлган зарар миқдорига мутаносиб бўлиши лозим.

Ушбу баҳолашнинг натижалари ахборот хавфсизлиги билан боғлиқ хавфларни бошқариш соҳасида аниқ чоралар ва устуворликларни белгилашга, шунингдек, ушбу хавфларни минимумга келтириш мақсадида ахборот хавфсизлигини бошқариш бўйича тадбирларни жорий қилишга ёрдам беради. Мавжуд тадбирларнинг самарадорлилигига таъсир кўрсатиши мумкин бўлган ҳар қандай ўзгаришларни ҳисобга олиш учун хавфлар таҳлилини вақти-вақти билан такрорлаб туриш керак.

Ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш. Ахборот хавфсизлигига қўйиладиган талаблар белгиланганидан ва хавфлар аниқланганидан сўнг хавфларни қабул қилса бўладиган даражагача пасайишини таъминлайдиган, ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш ва жорий этиш керак. Ушбу тадбирлар ушбу

стандартдан, бошқа манбалардан танлаб олиниши, шунингдек, ахборот хавфсизлигини бошқариш бўйича ташкилотнинг ўзига хос эҳтиёжларини қондирадиган тадбирлар ишлаб чиқилиши мумкин. Ахборот хавфсизлигини бошқариш бўйича тадбирларни танлаш хавфларни қабул қилиш мезонларига, хавфларга баҳо бериш вариантларига асосланган ташкилий қарорларга ва хавфларни ташкилотда қабул қилинган бошқаришга умумий ёндашишга боғлиқ. Ушбу танловни тенгишли миллий ва халқаро қонун ҳужжатлари ва нормалар билан мувофиқлаштириш керак.

Ушбу стандартда келтирилган ахборот хавфсизлигини бошқариш бўйича баъзи тадбирлар ахборот хавфсизлигини бошқариш учун амал қилинадиган принциплар сифатида қабул қилиниши ва кўпгина ташкилотлар учун қўлланиши мумкин. Бундай тадбирлар қуйироқда «Ахборот хавфсизлигини жорий қилиш учун таянч нуқта» сарлавҳаси остида батафсилроқ кўриб чиқилади.

Ахборот хавфсизлигини жорий қилиш учун таянч нуқта. Ахборот хавфсизлигини бошқариш бўйича алоҳида тадбирлар ахборот хавфсизлигини бошқариш учун амал қилинадиган принциплар сифатида қабул қилиниши ва уни жорий қилиш учун таянч нуқта бўлиб хизмат қилиши мумкин. Бундай тадбирлар қонун ҳужжатларининг асосий талабларига асосланади ёки ахборот хавфсизлиги соҳасида умумий қабул қилинган амалиёт сифатида қабул қилиниши мумкин.

Қонунчилик нуқтаи назаридан ахборот хавфсизлигини бошқариш бўйича асосий чоралар қуйидагилар ҳисобланади:

- маълумотларни муҳофаза қилиш ва шахсий ахборотнинг конфиденциаллиги;

- ташкилот ҳужжатларини муҳофаза қилиш;

- интеллектуал мулкка эгалик қилиш ҳуқуқи.

Ахборот хавфсизлиги соҳасида умумий қабул қилинган амалиёт сифатида ҳисобланган ахборот хавфсизлигини бошқариш бўйича тадбирлар қуйидагиларни ўз ичига олади:

- ахборот хавфсизлиги сиёсатини ҳужжатлаштириш;

- ахборот хавфсизлигини таъминлаш бўйича мажбуриятларни тақсимлаш;

- ахборот хавфсизлиги қоидаларига ўқитиш;

- иловалардаги ахборотга тўғри ишлов бериш;

- техник заифликларни бошқариш стратегияси;

- ташкилотнинг узлуксиз ишини бошқариш;

- ахборот хавфсизлиги можароларини ва такомиллаштиришларини бошқариш.

Санаб ўтилган тадбирларни кўпгина ташкилотлар ва ахборот муҳити учун қўлласа бўлади. Ушбу стандартда келтирилган барча тадбирлар муҳим ҳисобланса ҳам, қандайдир чоранинг ўринли бўлиши ташкилот тўқнаш келадиган муайян хавфлар нуқтаи назаридан белгиланиши керак. Демак, юқорида таърифланган ёндашиш ахборот хавфсизлигини таъминлаш бўйича тадбирларни жорий қилиш учун таянч нуқта бўлиб ҳисобланишига қарамай, у хавфларни баҳолашга асосланган ахборот хавфсизлигини бошқариш бўйича тадбирларни танлашнинг ўрнини босмайди.

Муваффақиятнинг энг муҳим омиллари. Тажриба шуни кўрсатадики, ташкилотда ахборот хавфсизлигини таъминлаш бўйича тадбирларни муваффақиятли жорий қилиш учун қуйидаги омиллар ҳал қилувчи ҳисобланади:

- ахборот хавфсизлиги мақсадлари, сиёсатлари ва муолажаларининг бизнес мақсадларига мувофиқлиги;

- хавфсизлик тизимини жорий қилиш, мададлаш, мониторингини ўтказиш ва модернизация қилишга ёндашишнинг корпоратив маданият билан мувофиқлиги;

- раҳбарият томонидан реал қўллаб-қувватлаш ва манфаатдорлик;

- хавфсизлик талабларини, хавфларни баҳолаш ва хавфларни бошқаришни аниқ тушуниш;

- ташкилот раҳбарлари ва ходимлари томонидан ахборот хавфсиз-

лигининг самарали маркетингини ўтказиш, шунингдек, ахборот хавфсизлигининг чораларини қўллаш заруратини тушунишни таъминлаш;

- ахборот хавфсизлиги сиёсатига тегишли йўриқномалар, тавсияларни ва тегишли стандартларни барча ходимлар ва субпудратчиларга бериш;

- ахборот хавфсизлигини бошқариш бўйича тадбирларни молиялаштириш шарти;

- ўқитиш ва тайёрлашнинг зарур даражасини таъминлаш;

- ахборот хавфсизлиги можароларини бошқаришнинг самарали жараёнини тасдиқлаш;

- ўлчанадиган кўрсаткичларнинг ахборот хавфсизлигини бошқаришнинг самарадорлилигини ва уни яхшилаш бўйича бажарувчилардан тушган таклифларни баҳолаш учун фойдаланиладиган ҳар томонлама ва балансланган тизими.

Ташкилотга тегишли қўлланмаларни ишлаб чиқиш. Ушбу стандарт ташкилотнинг муайян эҳтиёжлари учун қўлланмалар ишлаб чиқиш учун таянч нуқта сифатида баҳоланиши керак. Ушбу стандартда келтирилган йўриқномалар ва тадбирларнинг ҳаммаси ҳам қўллашга яроқли бўлавермайди.

Бундан ташқари, ушбу стандартга киритилмаган қўшимча чоралар керак бўлиб қолиши мумкин. Бу ҳолда аудиторлар ва бизнес бўйича шериклар томонидан ўтказиладиган мувофиқлик текширувини енгиллаштирадиган, бир вақтда бир неча томондан қилинган ҳаволаларнинг сақланиши фойдали бўлиши мумкин.

O‘zDStISO/IEC 27005:2013 – “Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборотхавфсизлиги рискларини бошқариш”

Ушбу стандарт ташкилотда ахборот хавфсизлиги рискларини бошқариш бўйича тавсияларни ўз ичига олади.

Ушбу стандарт O‘z DSt ISO/IEC 27001 да белгиланган умумий

концепцияларни қўллаб-қувватлайди ва рискларни бошқариш билан боғлиқ ёндашув асосида ахборот хавфсизлигини айнан бир хил таъминлашни амалга ошириш учун мўлжалланган.

Ушбу стандартни, тўла тушуниб етиш учун O‘z DSt ISO/IEC 27001 ва O‘z DSt ISO/IEC 27002да баён қилинган концепцияларни, моделларни, жараёнларни ва терминологияни билиш зарур.

Ушбу стандарт ташкилотнинг ахборот хавфсизлигини обрўсизлантириши мумкин бўлган рискларни бошқаришни амалга оширишни режалаштирадиган барча турдаги ташкилотлар (масалан, тижорат корхоналари, давлат муассасалари, нотижорат ташкилотлар) учун қўлланилади.

Ушбу стандартда қуйидаги стандартларга бўлган ҳаволалардан фойдаланилган:

O‘z DSt ISO/IEC 27001:2009 Ахборот технологиялари. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқариш тизимлари. Талаблар.

O‘z DSt ISO/IEC 27002:2008 Ахборот технологияси. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари

Ушбу стандартдан фойдаланилганда ҳавола қилинган стандартларнинг Ўзбекистон ҳудудида амал қилишини жорий йилнинг 1 январигача бўлган ҳолати бўйича тузилган стандартларнинг тегишли кўрсаткичи ва жорий йилда эълон қилинган тегишли ахборот кўрсаткичлари бўйича текшириш мақсадга мувофиқдир. Агар ҳавола қилинган ҳужжат алмаштирилган (ўзгартирилган) бўлса, у ҳолда ушбу стандартдан фойдаланилганда алмаштирилган (ўзгартирилган) стандартга амал қилиш лозим. Агар ҳавола қилинган ҳужжат алмаштирилмасдан бекор қилинган бўлса, у ҳолда унга ҳавола қилинган қоида, ушбу ҳаволага тааллуқли бўлмаган қисмида қўлланилади.

O‘zDStISO/IEC 27006:2013 – “Ахборот технологияси.

Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқариш тизимларининг аудити ва уларни сертификатлаштириш органларига қўйиладиган талаблар”

O‘z DSt ISO/IEC 17021 - бу ташкилотларни бошқариш тизимларининг аудитини ва сертификатлаштирилишини амалга оширадиган органлар учун мезонларни ўрнатадиган стандартдир. Агар бу органлар O‘z DSt ISO/IEC 27001 га мувофиқ, ахборот хавфсизлигини бошқариш тизимлари (АХБТ)нинг сертификатлаштирилишини ва аудитини ўтказиш мақсадида, O‘z DSt ISO/IEC 17021 мувофиқ келадиган органлар сифатида аккредитланадиган бўлса, у ҳолда O‘z DSt ISO/IEC 17021 га қўлланма ва қўшимча талаблар зарур. Улар ушбу стандартда тақдим этилган.

Ушбу стандартнинг матни O‘z DSt ISO/IEC 17021 структурасини такрорлайди, АХБТ учун специфик бўлган қўшимча талаблар ва АХБТни сертификатлаштириш учун O‘z DSt ISO/IEC 17021 ни қўллаш бўйича қўлланма эса, «АХ» аббревиатураси билан белгиланади.

«Керак» атамасидан ушбу стандартда O‘z DSt ISO/IEC 17021 ва O‘z DSt ISO/IEC 27001 талабларини акс эттирган ҳолда мажбурий бўлган шартларни кўрсатиш учун фойдаланилади. «Зарур» атамасидан, гарчи бу талабларни қўллаш бўйича қўлланма бўлса ҳам, сертификатлаштириш органи томонидан қабул қилиниши кўзда тутиладиган шартларни белгилаш учун фойдаланилади.

Ушбу стандартнинг мақсади - аккредитлаш органларига, сертификатлаштириш органларини баҳолашлари шарт бўлган стандартларни янада самарали қўллаш имкониятини беришдир. Бу контекстда сертификатлаштириш органининг қўлланмадан ҳар қандай четга чиқиши истисно ҳисобланади. Бундай четга чиқишларга ҳар бир ҳолат алоҳида кўриб чиқилиши асосидагина рухсат берилиши мумкин, бунда сертификатлаштириш органи аккредитлаш органига бу истисно қандайдир эквивалант тарзда O‘z DSt ISO/IEC 17021, O‘z DSt ISO/IEC 27001 талабларининг тегишли бандини ва ушбу стандарт талабларини

қаноатлантиришини исботлаб бериши керак.

Изоҳ - Ушбу стандартда «бошқариш тизими» ва « тизим» атамаларидан бир-бирини алмаштириб фойдаланилади. Бошқариш тизимлари таърифини O‘z DSt ISO 9000 да топиш мумкин. Бу халқаро стандартда фойдаланилаётган бошқариш тизимини ахборот технологиялари тизимлари каби, тизимларнинг бошқа турлари билан адаштирмаслик зарур.

ISO/IEC 15408-1-2005 – “Ахборот технологияси. Хавфсизликни таъминлаш методлари ва воситалари. Ахборот технологиялари хавфсизлигини баҳолаш мезонлари”

ISO/IEC 15408-2005 халқаро стандарти ISO/IEC JTC 1 «Ахборот технологиялари» Биргаликдаги техник қўмита, SC 27 «АТ хавфсизлигини таъминлаш методлари ва воситалари» кичик қўмита томонидан тайёрланган. ISO/IEC 15408-2005 га ўхшаш матн «Ахборот технологиялари хавфсизлигини баҳолашнинг умумий мезонлари» 2.3-версия (2.3 УМ деб номланади) сифатида «Умумий мезонлар» лойиҳасининг ҳомий-ташкилотлари томонидан эълон қилинган.

Стандартнинг иккинчи таҳрири техник жиҳатдан қайта ишлашга тўғри келган биринчи таҳрир (ISO/IEC 15408:1999)ни бекор қилади ва уни алмаштиради.

ISO/IEC 15408-2005 га ўхшаш бўлган O‘z DSt ISO/IEC 15408 «Ахборот технологиялари - Хавфсизликни таъминлаш методлари ва воситалари - Ахборот технологиялари хавфсизлигини баҳолаш мезонлари» умумий сарлавҳа остидаги қуйидаги қисмлардан ташкил топган:

1-қисм: Кириш ва умумий модел;

2-қисм: Хавфсизликка қўйиладиган функционал талаблар;

3-қисм: Хавфсизликка қўйиладиган ишонч талаблари.

O‘z DSt ISO/IEC 15408 хавфсизликни мустақил баҳолаш натижаларини қиёслаш имкониятини беради. Бунга АТ маҳсулотлари ва тизимларининг хавфсизлик функцияларига ва хавфсизликни баҳолашда уларга

қўлланиладиган ишонч чораларига қўйиладиган талаблар умумий тўпламининг тақдим этилиши билан эришилади.

Бундай маҳсулотлар ёки тизимларнинг хавфсизлик функциялари, шунингдек олдиндан қўлланиладиган ишонч чоралари қўйиладиган талабларга жавоб бериши боис, баҳолаш жараёнида белгиланган ишонч даражасига эришилади. Баҳолаш натижалари истеъмолчиларга АТ маҳсулотлари ёки тизимлари уларнинг тахмин қилинаётган қўлланилиши учун етарли даражада хавфсиз эканлигига ва улардан фойдаланишда башоратқилинаётган хавф-хатарларнинг мақбуллигига ишонч ҳосил қилишларига ёрдам бериши мумкин.

O‘z DSt ISO/IEC 15408 АТ маҳсулотлари ва тизимларининг хавфсизлик функциялари билан ишлаб чиқилишидаги каби, шундай функцияли тижорат маҳсулотлари ва тизимларининг сотиб олинишида ҳам қўлланма сифатида фойдали. АТнинг бундай маҳсулоти ёки тизимининг баҳоланиши баҳолаш объекти (БО) деб аталади. Бундай БОга, масалан, операцион тизимлар, ҳисоблаш тармоқлари, тақсимланган тизимлар ва иловалар киради.

O‘zDStISO/IEC 15408 ахборотни рухсат этилмаган тарзда очиш, модификация қилиш ёки ундан фойдаланиш имкониятини йўқотишдан муҳофаза қилинишига йўналтирилган. Хавфсизлик бузилишининг ушбу учта турига тааллуқли бўлган муҳофаза тоифалари, одатда, мос равишда, конфиденциаллик, бутунлик ва фойдалана олишлик деб аталади. Шунингдек, O‘zDStISO/IEC 15408 АТ хавфсизлигининг ушбу учта тушунча доирасидан ташқаридаги жиҳатларига қўлланилиши мумкин. O‘z DSt ISO/IEC 15408 инсоннинг ғараз ниятли ҳаракатлари каби, бошқа ҳаракатлар натижасида юзага келадиган ахборот таҳдидларига қаратилган, шунингдек O‘z DSt ISO/IEC 15408 инсон омили билан боғлиқ бўлмаган баъзи бир таҳдидлар учун ҳам қўлланилиши мумкин. Бундан ташқари, O‘z DSt ISO/IEC 15408 АТнинг бошқа соҳаларида қўлланилиши мумкин, бироқ уларнинг ваколати қатъий чегараланган АТ хавфсизлиги соҳасидан ташқарида декларация қилинмайди.

O‘zDStISO/IEC 15408 аппарат, дастурий-аппарат ва дастурий воситалар

томонидан амалга ошириладиган АТ хавфсизлиги чораларига қўлланилади. Агар, айрим баҳолаш жиҳатлари фақат амалгаоширишнинг баъзи бир усуллари учун қўлланилиши тахмин қилинса, бу тегишли мезонларни баён қилишда кўрсатиб ўтилади.

Назорат саволлари:

1. Ахборот хавфсизлиги соҳасида стандартлар ва меъёрий хужжатларнинг тутган ўрни.
2. ISO/IEC 27001:2005 ҳалқаро стандартининг моҳиятини тушунтириб беринг.
3. ISO/IEC 27002:2005 ҳалқаро сандартининг вазифаларини тавсифлаб беринг.
4. O‘zDStISO/IEC 27005:2013 ҳалқаро стандартини амалга киритилиши моҳияти нимада?
5. O‘zDStISO/IEC 27006:2013 ҳалқаро стандарти ахборот хавфсизлиги соҳасидаги қандай муаммоларни ечишга ёрдам беради?
6. O‘z DSt ISO/IEC 15408:2008 ҳалқаро стандарти нечта қисмдан иборат ва уларда ёритилган масалалар нималардан иборат?

3.2. Ахборот хавфсизлиги соҳасига оид миллий стандартлар

Ушбу бўлимда келтирилган стандартлар замон талаблари томонидан келиб чиққан ҳолда амалга оширилган бўлиб, асос сифатида Ўзбекистон Республикасининг "Электрон рақамли имзо хусусида"ги ва "Электрон хужжат алмашинуви хусусида"ги қонунларини келтиришимиз мумкин.

Ушбу стандартлар ЭҲМ тармоқларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ЭҲМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш қоидасини белгилайди.

O‘z DSt 1092:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш

ва текшириш жараёнлари”

Ушбу стандарт умумий фойдаланишдаги муҳофазаланмаган телекоммуникация каналлари орқали узатиладиган, берилган хабар (электрон ҳужжат) остига қўйилган электрон рақамли имзо (ЭРИ)ни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш учун электрон рақамли имзо алгоритми (ЭРИА)ни белгилайди.

Стандарт электрон рақамли имзони шакллантириш ва унинг ҳақиқийлигини тасдиқлашда турли мақсадлар учун мўлжалланган ахборотларни қайта ишлаш тизимларида қўллаш учун мўлжалланган.

Ушбу стандартда қуйидаги стандартларга ҳаволалардан фойдаланилган:

O‘z DSt 1047:2003 Ахборот технологиялари. Атамалар ва таърифлар.

O‘z DSt 1109:2006 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар.

O‘z DSt 1105:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми”

Ушбу « Маълумотларни шифрлаш алгоритми» (МША) стандарти электрон маълумотларни муҳофаза қилиш учун мўлжалланган криптографик алгоритмни ифодалайди. МША - симметрик блокли шифр бўлиб, ахборотни шифрматнга ўгириш ва дастлабки матнга ўгириш учун фойдаланилади. МША 256 bit узунликдаги маълумотлар блокини шифрматнга ўгириш ва шифрматнни дастлабки матнга ўгириш учун 256 ёки 512 bit узунликдаги криптографик калитдан фойдаланиши мумкин.

Стандарт, электрон ҳисоблаш машиналари (ЭҲМ) тармоқларида, алоҳида ҳисоблаш комплекслари ва ЭҲМда ахборотга ишлов бериш тизимларида ахборотни шифрлашнинг ягона алгоритмини ўрнатиб, маълумотларни шифрлаш қоидаларини белгилайди.

Маълумотларни шифрлаш алгоритми дастурий, аппарат ёки аппарат-дастурий криптографик модулларда амалга ошириш учун мўлжалланган.

Ташкилотлар, корхоналар ва муассасалар ЭҲМ тармоқларида,

алоҳида ҳисоблаш комплексларида ёки ЭҲМда сақланувчи ва узатилувчи маълумотларнинг криптографик муҳофазасини амалга оширишда мазкур стандартдан фойдаланишлари мумкин.

Ушбу стандартда қуйидаги стандартларга ҳаволалардан фойдаланилган:

O‘z DSt 1047:2003 Ахборот технологиялари. Атамалар ва таърифлар.

O‘z DSt 1109:2006 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар.

O‘z DSt 1106:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси”

Ушбу стандарт ахборотни қайта ишлаш ва муҳофаза қилишнинг криптографик методларида, шу жумладан автоматлаштирилган тизимларда ахборот узатиш, қайта ишлаш ва сақлашда электрон рақамли имзо (бундан кейин - ЭРИ) процедураларини амалга ошириш учун қўлланиладиган иккилик символларининг исталган кетма-кетлиги учун хэшлаш функциясининг (бундан кейин - ХФ) алгоритмини ва ҳисоблаш процедурасини белгилайди.

Ушбу стандартда қуйидаги стандартларга ҳаволалардан фойдаланилган:

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования

O‘z DSt 1047:2003 Ахборот технологиялари. Атамалар ва таърифлар

O‘z DSt 1109:2006 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар

O‘z DSt 1204:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Криптографик модулларга хавфсизлик талаблари”

Ушбу стандарт очиқ ва симметрик калитли криптографик модулларга қўйиладиган ягона хавфсизлик талабларини белгилайди ҳамда ахборотнинг криптографик муҳофаза қилиш воситаларини лойиҳалаш, ишлаб чиқиш,

сотиш (элтиб бериш) ва ундан фойдаланиш учун мўлжалланган. Стандарт ЭҲМ, телекоммуникация тармоқлари, айрим ҳисоблаш комплекслари ёки ЭҲМда сақланадиган ва узатиладиган конфиденциал ахборотни муҳофаза қиладиган криптографик модулларга қўйиладиган хавфсизлик талабларини белгилайди.

Ушбу стандартда қуйидаги стандартларга ҳаволалардан фойдаланилган:

O‘z DSt 1092:2005 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари.

O‘z DSt 1105:2006 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми.

O‘z DSt 1109:2006 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар.

Назорат саволлари:

1. Ўзбекистон Республикасининг O‘z DSt 1092:2009, O‘z DSt 1105:2009 ва O‘z DSt 1106:2009 миллий стандартларининг моҳиятини тушунтириб беринг.
2. O‘z DSt 1204:2009 миллий стандартида қандай масалалар ёритиб берилган?

3.3. Ахборот хавфсизлиги соҳасига оид меъёрий хужжатлар

RH 45-215:2009 - Раҳбарий ҳужжат. Маълумотлар узатиш тармоғида ахборот хавфсизлигини таъминлаш тўғрисида Низом. Ушбу ҳужжат N 100:2002 «Маълумотлар узатиш миллий тармоғида ахборот хавфсизлигини таъминлаш тўғрисида низом» ўрнига амалга киритилган бўлиб, маълумотлар узатиш тармоғида (МУТ) ахборот хавфсизлигини таъминлаш бўйича асосий мақсадлар, вазифалар, функциялар ва ташкилий-техник тадбирларни белгилайди.

Низом хонанинг муҳофаза қилинишини ташкил қилиш, тармоқ компонентларининг сақланганлиги ва физик яхлитлигини таъминлаш, табиий офатлар, энергия таъминоти тизимида ишламай қолишлардан муҳофаза қилиш масалалари, ходимлар ва МУТ мижозларининг шахсий хавфсизлигини таъминлаш бўйича чоралари, шунингдек Тезкор-қидирув тадбирлар тизимини (ТҚТТ) ташкил қилиш масалалари ва унинг ишлашини тартибга солмайди.

Ушбу ҳужжат талаблари МУТ нормал ишлашини кузатиш, хизмат кўрсатиш ва таъминлаш ишларини амалга оширувчи мутасадди қўмита ва вазирликларнинг барча корхоналарига тааллуқлидир.

Ушбу Низомга ахборот муҳофазаси бўйича хизматлар рўйхати ўзгарганда ёки МУТни модернизация қилиш ва ривожлантиришда ўзгартириш ёки қўшимчалар киритилган бўлиши мумкин.

Ушбу Низом ахборотни муҳофаза қилишнинг ҳуқуқий, ташкилий, режимли, техник, дастурий ва бошқа методлари ва воситалари жамидан фойдаланиш, шунингдек ахборот хавфсизлигини таъминлаш қисмида амалга оширилган чораларнинг самарадорлиги учун ҳар томонлама узлуксиз назорат қилишни амалга ошириш асосида МУТда ахборот хавфсизлигини таъминлаш кўзда тутилади.

МУТда ахборот хавфсизлигини таъминлаш АХТТни яратиш йўли билан комплексли ва МУТ ҳаётий циклининг барча босқичларида ташкилий-техник тадбирларни доимо ўтказиш билан ҳал этилади.

МУТ АХТТ самарали ишлашини таъминлаш функциялари корхона раҳбарига бевосита бўйсунадиган корхонанинг МУТ ахборот хавфсизлигини таъминлаш хизмати (бўлими)га юклатилади.

Корхонанинг МУТ ахборот хавфсизлигини таъминлаш хизмати (бўлими) ўз фаолиятида Ўзбекистон Республикасининг қонун ҳужжатлари ва норматив ҳужжатлари, Президент фармонлари, Ўзбекистон Республикаси Вазирлар Маҳкамасининг қарорлари, Агентликнинг норматив-ҳуқуқий ҳужжатлари, корхона раҳбарларининг буйруқлари ва фармойишлари,

шунингдек ушбу Низомга амал қилади.

Ахборот хавфсизлигини таъминлаш хизмати (бўлими) МУТ серверларида сақланадиган ва МУТ телекоммуникация каналлари ва воситалари бўйлаб узатиладиган, агар бу шартномада кўзда тутилган бўлса, абонентлар ахборотининг конфиденциаллиги, яхлитлиги ва ундан эркин фойдаланиш учун жавобгар бўлади.

Ахборот хавфсизлигини таъминлаш хизмати (бўлими) абонент терминалларида сақланадиган абонент ахборотининг конфиденциаллиги, яхлитлиги ва ундан эркин фойдаланиш учун жавобгар бўлмайди.

Ахборот хавфсизлигини таъминлаш хизмати (бўлими) вируслар билан зарарланган ва зарарли дастурларни ўз ичига олган фойдаланувчи ва абонентларнинг ахборот ресурслари (МУТ серверларида жойлашадиган ва сақланадиган ва МУТ телекоммуникация каналлари ва воситалари бўйлаб узатиладиган), шунингдек Ўзбекистон Республикасининг амалдаги қонун ҳужжатлари билан тақиқланган ахборот ресурслари тарқалишининг олдини олиш бўйича чораларни қабул қилиш ҳуқуқига эга.

Абонентларга ахборотни муҳофаза қилиш бўйича қўшимча хизматларни тақдим этиш шартномада баён этилади.

МУТ фойдалнувчилари ва абонентлари ўз даражасида ахборотни муҳофаза қилиш тизимлари ёки воситаларини қўллаш (улардан фойдаланиш) ҳуқуқига эга.

RH 45-185:2011-Раҳбарий ҳужжат. Давлат ҳокимияти ва бошқарув органларининг ахборот хавфсизлигини таъминлаш дастурини ишлаб чиқиш тартиби. Ушбу ҳужжат RH 45-185:2006 ҳужжати ўрнига амалга киритилган бўлиб, давлат ҳокимияти ва бошқарув органларининг ахборот хавфсизлигини таъминлаш дастурларини ишлаб чиқиш тартибини белгилайди.

Ҳужжат ахборот хавфсизлигини таъминлаш дастурлари доирасида ишлаб чиқиладиган чора-тадбирларнинг мақсадлари, вазифалари, тузилмаси ва рўйхатига қўйиладиган намунавий талабларни белгилайди.

Ушбу ҳужжат талаблари Ўзбекистон Республикасининг давлат ҳокимияти ва бошқарув органларига тааллуқли ва ушбу органларнинг ахборот хавфсизлигини таъминлаш дастурларини яратиш учун асос бўлиб ҳисобланади.

Ушбу ҳужжатни ишлаб чиқиш ва жорий этишдан мақсад:

- ахборот хавфсизлигини таҳдидлардан муҳофаза қилиш бўйича чораларнинг адекватлигига эришиш;

- давлат ҳокимияти ва бошқарув органларининг ишларидаги барқарорлик даражасини ошириш;

- хавфсизлик можароларидан юзага келган зиён даражасини пасайтириш;

- ахборот хавфсизлиги инфратузилмасини яратиш;

- бошқа ташкилотларнинг фойдаланиш хавфсизлигини таъминлаш;

- бошқа ташкилотларнинг уланиши билан боғлиқ бўлган эҳтимолий хавфларни идентификация қилиш;

- ахборот ресурсларига масъул шахсларни белгилаш;

- давлат ҳокимияти органлари фаолиятида давлат ахборот ресурсларининг очиқлиги ва оммабоплигини таъминлаш, ахборот ва коммуникация технологияларидан фойдаланиш асосида давлат ҳокимияти органлари билан фуқаролар ўртасидаги самарали ўзаро ҳамкорлик учун, уларнинг ахборот хавфсизлигини таъминлаган ҳолда, шароитлар яратиш;

- муҳофаза қилинган ахборот ва коммуникация технологияларидан фойдаланиш асосида давлат органлари фаолиятини такомиллаштириш;

- давлат органларида АХ бўйича мутахассисларни тайёрлаш тизимини ривожлантиришдир.

Ушбу раҳбарий ҳужжатнинг асосий мақсади - давлат ҳокимияти ва бошқарув органларини АХ таҳдидларидан уларга мумкин бўлган зарар етказилишидан муҳофаза қилинишини таъминлашдир.

Раҳбарий ҳужжатнинг асосий вазифаси давлат органларининг ахборот хавфсизлигини таъминлаш дастурини белгилаш ҳисобланади.

RH 45-193:2007 - Раҳбарий ҳужжат. Давлат органлари сайтларини жойлаштириш учун провайдерлар серверлари ва техник майдонларнинг ахборот хавфсизлигини таъминлаш даражасини аниқлаш тартиби. Ушбу ҳужжат давлат органлари сайтларини жойлаштириш учун провайдерлар серверлари ва техник майдонларнинг ахборот хавфсизлигини таъминлаш даражасини аниқлашнинг намунавий тартибини белгилайди.

Ушбу ҳужжат талаблари давлат органларининг сайтлари учун хостинг хизматларини тақдим этувчи барча ҳўжалик юритувчи субъектлар томонидан қўлланилиши мажбурийдир.

Ҳужжатда Давлат органларининг сайтларини жойлаштириш учун провайдерлар серверлари ва техник майдонларнинг ахборот хавфсизлигини (АХ) таъминлаш даражасини белгилаш, ахборот ресурсларини яратиш ва фойдаланишнинг барча аспектларини ҳисобгаолган ҳолда, ушбу вазифага комплекс ёндошилишига асосланади. Бу учун ташкилий, техник ва дастурий муҳофаза қилиш чораларини, хавф-хатарлар ва ахборотнинг муҳофазаланганлик даражасини баҳолаш ва прогноз қилиш бўйича тадбирларни доимо ривожланиб бораётган ягона тизимга умумлаштириш талаб этилади.

Ахборотни муҳофаза қилиш ўз ичига АХни таъминлашга қаратилган чора-тадбирлар комплексини олади: маълумотларни киритиш, сақлаш, қайта ишлаш ва узатиш учун фойдаланиладиган ахборот ва ресурсларнинг бутунлиги, улардан фойдалана олишлик ва, зарур ҳолда, конфиденциаллигини қўллаб-қувватлаш.

Ахборотни муҳофаза қилиш мақсади қуйидагилар ҳисобланади:

- ахборотнинг чиқиб кетиши, ўғирланиши, йўқолиши, бузилиши,қалбакилаштирилишини олдини олиш;

- ахборотни йўқ қилиш, модификация қилиш, бузиш. нусха кўчириш, блокировка қилиш бўйича рухсат этилмаган ҳаракатларнинг олдини олиш;

- ахборот ресурслари ва ахборот тизимларига (АТ) ноқонуний аралашишнинг бошқа шаклларини олдини олиш.

TSt 45-010:2010 – Тармоқ стандарти. Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Атамалар ва таърифлар. Ушбу тармоқ стандарти Ўзбекистон Республикаси Вазирлар Маҳкамаси ҳузуридаги давлат стандартлаштириш, метрология ва сертификатлаштириш маркази («Ўздавстандарт») томонидан 2002 йил 6 августда 112/066-сон билан рўйхатга олинган TSt 45.010:2002 «Отраслевой стандарт. Информационная безопасность в сфере связи и информатизации. Термины и определения» ўрнига амалга киритилган бўлиб, алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлигидаги асосий атама ва таърифларни белгилайди.

Белгиланган атамалар барча турдаги ҳужжатларда қўлланилиши учун мажбурийдир. Стандартда маълумотнома сифатида стандартлаштирилган атамаларнинг хорижий эквиваленти рус (Р) ва инглиз (Е) тилларида келтирилган.

Стандартдан фойдаланиш қулайлиги учун атама моддаларининг тегишли рақамларини кўрсатган ҳолда ўзбек, рус ва инглиз тилларидаги амаларни ўз ичига олган алифбо кўрсаткичи келтирилган.

Назорат саволлари:

1. RH 45-215:2009 - Раҳбарий ҳужжат ўз ичига олган масалалар нималардан иборат?
2. RH 45-185:2011 - Раҳбарий ҳужжат ўз ичига олган масалалар нималардан иборат?
3. RH 45-193:2011 - Раҳбарий ҳужжат ўз ичига олган масалалар нималардан иборат?
4. TSt 45-010:2010 – Тармоқ стандарти ўз ичига олган масалалар нималардан иборат?

IV боб. ХАВФСИЗЛИК МОДЕЛЛАРИ

4.1. Харрисон-Руззо-Улманнинг дискрецион модели

Маълумки, хавфсизлик сиёсати деганда ахборотни ишлаш жараёнини қатъий белгиловчи умумий тартиб ва қоидалар мажмуи тушуниладики, уларнинг бажарилиши маълум таҳдидлар тўпламидан ҳимояланишни таъминлайди ва тизим хавфсизлигининг зарурий (баъзида етарли) шартини ташкил этади. Хавфсизлик сиёсатининг формал ифодаси хавфсизлик сиёсатининг модели деб аталади.

Ҳимояланган ахборот тизимларини ишлаб чиқарувчилар хавфсизлик моделидан қуйидаги ҳолларда фойдаланишади:

- ишлаб чиқариладиган тизим хавфсизлиги сиёсатининг формал спецификациясини (тафсилотли рўйхатини) тузишда;
- ҳимоя воситаларини амалга ошириш механизмларини белгиловчи ҳимояланган тизим архитектурасининг базавий принципларини танлаш ва асослашда;
- тизим хавфсизлигини эталон модел сифатида таҳлиллаш жараёнида;
- хавфсизлик сиёсатига риоя қилишнинг формал исботи йўли билан ишлаб чиқариладиган тизим хусусиятларини тасдиқлашда.

Истеъмолчилар хавфсизликнинг формал моделларини тузиш йўли билан ишлаб чиқарувчиларга ўзларининг талабларини аниқ ва зиддиятли бўлмаган шаклда етказиш ҳамда ҳимояланган тизимларнинг ўзларининг эҳтиёжларига мослигини баҳолаш имкониятига эга бўладилар.

Квалификация (Малака) бўйича экспертлар ҳимояланган тизимларда хавфсизлик сиёсатининг амалга оширилиш адекватлигини тахлиллаш мобайнида хавфсизлик моделидан эталон сифатида фойдаланадилар.

Хавфсизлик модели қуйидаги базавий тасаввурларга асосланган.

1. Тизим ўзаро ҳаракатдаги “субъектлар” ва “объектлар” мажмуасидан иборат. Объектларни интуитив равишда ахборотли

контейнерлар кўринишида тасаввур этиш мумкин, субъектларни эса объектларга турли усуллар билан таъсир этувчи бажарилувчи дастурлар деб ҳисоблаш мумкин. Тизимни бундай тасаввур этишда ахборотни ишлаш хавфсизлиги хавфсизлик сиёсати шакллантирувчи қоидалар ва чеклашлар тўпламига мос ҳолда субъектларнинг объектлардан фойдаланишни бошқариш масаласини ечиш орқали таъминланади. Агар субъектлар хавфсизлик сиёсати қоидаларини бузиш имкониятига эга бўлмаса, тизим хавфсиз ҳисобланади. Таъкидлаш лозимки, “объект” ва “субъект” тушунчаларининг тавсифи турли моделларда жиддий фарқланиши мумкин.

2. Тизимдаги барча ўзаро ҳаракатлар субъектлар ва объектлар орасида маълум хилдаги муносабатларни ўрнатиш орқали моделлаштирилади.

3. Барча амаллар ўзаро ҳаракат монитори ёрдамида назоратланади ва хавфсизлик сиёсати қоидаларига мувофиқ маън этилади ёки рухсат берилади.

4. Хавфсизлик сиёсати қоидалар кўринишида берилади, бу қоидаларга мос ҳолда субъектлар ва объектлар орасида барча ўзаро ҳаракатлар амалга оширилиши шарт. Ушбу қоидаларни бузилишига олиб келувчи ўзаро ҳаракатлар фойдаланишни назоратловчи воситалар ёрдамида тўсиб қўйилади ва амалга оширилиши мумкин эмас.

5. Субъектлар, объектлар ва улар орасидаги муносабатлар (ўрнатилган ўзаро ҳаракат) тўплами тизим “ҳолатини” белгилайди. Тизимнинг ҳар бир холати моделда таклиф этилган хавфсизлик мезонига мувофиқ хавфсиз ёки тахликали бўлади.

6. Хавфсизлик моделининг асосий элементи – хавфсиз холатидаги тизим барча ўрнатилган қоида ва чеклашларга риоя қилинганида тахликали ҳолатга ўтиш мумкин эмаслиги тасдиғининг (теоремасининг) исботи.

Харрисон-Руззо-Улманнинг дискрецион модели классик (мумтоз) дискрецион модел ҳисобланиб, субъектларнинг объектлардан фойдаланишни ихтиёрий бошқаришни ва фойдаланиш хуқуқларининг тарқалиши

назоратини амалга оширади.

Ушбу модел доирасида ахборотни ишлаш системаси ахборотдан фойдаланувчи субъектлар (S тўплам), ҳимояланувчи ахборотга эга бўлган объектлар (O тўплам) ва мос ҳаракатларни, (масалан ўқиш (R), ёзиш (W), дастурни бажариш(E)) ваколатини англатувчи фойдаланиш ҳуқуқларининг чекли тўплами $R = \{r_1, r_2, \dots, r_n\}$ мажмуи кўринишида ифодаланади.

Шу билан бирга модел таъсири доирасига субъектлар орасидаги муносабатларни киритиш учун барча субъектлар бир вақтнинг ўзида объектлар ҳисобланади - $S \subset O$. Тизим аҳволи ҳолат тушунчаси ёрдамида моделлаштирилади. Тизим ҳолати макони уни ташкил этувчи объектлар, субъектлар ва ҳуқуқлар тўпламларининг декарт кўпайтмаси сифатида шакллантирилади - $O \times S \times R$. Бу маконда тизимнинг жорий ҳолати учлик орқали аниқланади. Бу учликка субъектлар тўплами, объектлар тўплами ва субъектларнинг объектлардан фойдаланиш ҳуқуқларини тавсифловчи фойдаланиш матрицаси киради - $Q = (S, O, M)$. Матрица қаторлари субъектларга, устунлари эса объектларга мос келади. Объектлар тўплами ўз ичига субъектлар тўпламини олганлиги сабабли матрица тўғри тўртбурчак кўринишида бўлади. Матрицанинг ихтиёрий ячейкаси $M[S, O]$ субъект "S"нинг объект "O"дан, фойдаланиш ҳуқуқлари тўплами Rга тегишли фойдаланиш ҳуқуқлари наборига(тўпламига) эга. Тизимнинг вақт бўйича аҳволи турли ҳолатлар орасидаги ўтишлар ёрдамида моделлаштирилади. Ўтиш матрица Mга қуйидаги кўринишлардаги командалар ёрдамида ўзгартириш киритиш йўли билан амалга оширилади:

$$command\alpha(x_1, \dots, x_k)$$

if $r_1$in $M[x_{s'_1}, \dots, x_{o_1}]$ and

$r_2$in $M[x_{s'_2}, \dots, x_{o_2}]$ and

...

$r_m$in $M[x_{s'_m}, \dots, x_{o_m}]$ and

then

$$op_1, op_2, \dots, op_n$$

Бу ерда α – команда номи; x_i – команда параметрлари бўлиб, субъектлар ва объектларнинг идентификаторлари ҳисобланади; s_iва o_i– “1”дан “k”гача диапазонда субъектлар ва объектларнинг индекслари; op_i – элементар амаллар. Команда таркибидаги элементар амаллар M матрица ячейкаларида кўрсатилган фойдаланиш хуқуқларининг мавжудлигини англатувчи барча шартлар ҳақиқий бўлганидагина бажарилади.

Классик (мумтоз) моделда фақат қуйидаги элементар амаллар жоиз ҳисобланади:

enter “r” into $M[s\ \ ,o]$ (“s” субъектга “o” объект учун “r” хуқуқни қўшиш(киритиш))

delete “r” from $M[s,o]$ (“s” субъектдан “o” объект учун “r” хуқуқни йўқ қилиш)

create subject “s” (янги “s” субъектни яратиш)

create subject “o” (янги “o” объектни яратиш)

destroy subject “s” (мавжуд “s” субъектни йўқ қилиш)

destroy subject “o” (мавжуд “o” объектни йўқ қилиш)

$Q = (S, O, M)$ ҳолатда бўлган тизимда ихтиёрий элементар амал “op”нинг ишлатилиши тизимнинг бошқа $Q'(S', O', M')$ ҳолатга ўтишига сабаб бўладики, бу ҳолат олдинги ҳолатдан бўлмаганида битта компоненти билан фарқланади. Базавий амалларнинг ишлатилиши тизим ҳолатида қуйидаги ўзгаришларга олиб келади:

enter “r” into $M[s,o]$ (бу ерда $s \in S, o \in O$)

$O' = O$

$S' = S$

$M'[x_s, x_o] = M[x_s, x_o]$ агар $(x_s, x_o) \neq (s, o)$ бўлса,

$M'[s,o] = M[s,o] \cup \{r\}$.

“enter” амали фойдаланиш матрицасининг мавжуд ячейкасига “r” хуқуқини киритади. Ҳар бир ячейканинг таркиби фойдаланиш хуқуқи

тўплами сифатида кўрилади, яъни агар киритилаётган хуқуқ бу тўпламда бўлса, ячейка ўзгармайди. “enter” амали фойдаланиш матрицасига фақат хуқуқ қўшади ва ҳеч нарсани йўқ қилмайди. Шу сабабли бу амални “монотон” амал деб аташади.

delete “r” from $M[s,o]$ (бу ерда $s \in S, o \in O$)

$O' = O$

$S' = S$

$M'[x_s, x_o] = M[x_s, x_o]$ агар $(x_s, x_o) \neq (s, o)$,

$M'[s,o] = M[s,o] \backslash \{r\}$.

“delete” амалининг таъсири “enter” амалининг таъсирига тескари. Бу амал фойдаланиш матрицасининг ячейкасидаги хуқуқни йўқ қилади, агар бу хуқуқ ушбу ячейкада бўлса, ҳар бир ячейканинг таркиби фойдаланиш хуқуқи тўплами сифатида кўрилганлиги сабабли, йўқ қилинадиган хуқуқ ушбу ячейкада бўлмаса, “delete” амали ҳеч нарса қилмайди. “delete” амали фойдаланиш матрицасидан ахборотни йўқ қилиши сабабли, бу амал “монотон бўлмаган” амал деб аталади.

$create\ subject$ "s" (бу ерда $s \notin S$)

$O' = O \cup \{s\}$

$S' = S \cup \{s\}$

$M'[x_s, x_o] = M[x_s, x_o]$барча $(x_s, x_o) \in S \times O$ учун

$M'[s, x_o] = \emptyset$ барча $x_o \in O'$ учун

$M'[s, x_s] = \emptyset$ барча $x_s \in S'$ учун

$destroy\ subject$ "s" (бу ерда $(s \in S)$)

$O' = O \backslash \{s\}$

$S' = S \backslash \{s\}$

$M[x_s, x_o]' = M(x_s, x_o)$барча $(x_s, x_o) \in S' \times O'$

$create\ object$ "o" (бу ерда $o \notin O$)

$O' = O \cup \{o\}$

$S' = S$

$M'[x_s, x_o] = M[x_s, x_o]$барча $(x_s, x_o) \in S \times O$

$$M'[x_s, o] = \emptyset \text{ барча } x_s \in S' \text{учун}$$

$destory\ object$ "o" (бу ерда ($o \in O \backslash S$))

$O' = O \backslash \{o\}$

$S' = S$

$M'[x_s, x_o] = M[x_s, x_o]$барча $(x_s, x_o) \in S' \times O'$

$create\ subject$ ва $destory\ subject$ амаллари монотон ва монотон бўлмаган амалларнинг ўхшаш жуфтларини ифодалайди.

Таъкидлаш лозимки, ҳар бир амал учун уни бажаришга яна олдиндан қуйиладиган шарт мавжуд: $enter$ ёки $delete$ амаллари ёрдамида фойдаланиш матрицасининг ячейкасини ўзгартириш учун ушбу ячейка мавжуд бўлиши, яъни мос субъект ва объектнинг мавжуд бўлиши шарт. Шунга ўхшаш $create\ subject/object$ яратиш амаллари учун яратилувчи субъект/объектнинг мавжуд бўлмаслиги, $destory\ subject/object$ йўқ қилиш амали учун йўқотилувчи субъект/объектнинг мавжудлиги шарт. Ихтиёрий амалга олдиндан қуйиладиган шарт бажарилмаса у амалнинг бажарилиши натижа бермайди.

Расман $\sum(Q, R, C)$тизим тавсифи қуйидаги элементлардан ташкил топган:

- фойдаланиш хуқуқларининг чекли тўплами $R = \{r_1, \dots, r_n\}$;
- дастлабки субъектлар $S_0 = \{s_1, \dots, s_n\}$ ва объектлар$O_0 = \{o_1, \dots, o_m\}$нинг чекли тўпламлари, бу ерда $S_0 \subseteq O_0$;
- таркибида субъектларнинг объектлардан фойдаланиш хуқуқлари бўлган дастлабки фойдаланиш матрицаси - M_0;
- ҳар бири юқорида санаб ўтилган элементар амаллар терминалларида бажариш ва шархлаш шартларидан ташкил топган – буйруқларнинг чекли тўплами - $C = \{\propto_i (x_1, \dots, x_k)\}$.

Тизимнинг вақт бўйича аҳволи ҳолатлар $\{Q_i\}$ кетма-кетлиги ёрдамида моделлаштирилади. Ҳар бир кейинги ҳолат C тўпламдаги қандайдир команданинг олдинги ҳолатга қўллаш натижаси ҳисобланади - $Q_{n+1} = C_n(Q_n)$. Шундай қилиб тизимнинг у ёки бу ҳолатга тушиши ёки тушмаслиги

C даги командалар ва улар таркибидаги амалларга боғлиқ. Ҳар бир ҳолат субъектлар, объектлар тўпламлари ва хуқуқлар матрицаси орасидаги мавжуд фойдаланиш муносабатларини белгилайди. Хавфсизликни таъминлаш учун баъзи фойдаланиш муносабатларини таъқиқлаб қўйиш лозимлиги сабабли тизимнинг берилган дастлабки ҳолати учун у тушиши мумкин бўлмаган ҳолатлар тўпламини аниқлаш имконияти мавжуд бўлиши шарт. Бу шундай дастлабки шартларни (C командалар O_0 объектлар тўпламининг, S_0 субъектлар тўпламининг M_0 фойдаланиш матрицанинг шартини) беришга имкон берадики, бу шартларда тизим хавфсизлик нуқтаи назаридан номақбул ҳолатга туша олмайди. Демак, аҳволи олдиндан башорат қилинувчи тизимни қуриш учун қуйидаги саволга жавоб бериш лозим: қандайдир субъект "s" қачондир қандайдир объект "o"дан фойдаланиш хуқуқига эга бўлиши мумкинми?

Шу сабабли Харрисон-Руззо-Ульман моделининг хавфсизлик мезони қуйидагича таърифланади:

Берилган тизим учун дастлабки ҳолат $Q_0 = (S_0, O_0, M_0)$ "r" *хуқуққа нисбатан хавфсиз ҳисобланади, агар қўлланилиши натижасида* "r" *хуқуқ M матрица ячейкасига киритиладиган* Q_0 *командалар кетма-кетлиги мавжуд бўлмаса (*Q_0 *ҳолатда M матрицада ушбу хуқуқ бўлмаган).*

Ушбу мезоннинг моҳияти қуйидагича: агар субъект олдиндан объектдан фойдаланиш хуқуқи "r"га эга бўлмаса, тизимнинг хавфсиз конфигурацияси учун у ҳеч қачон объектдан фойдаланиш хуқуқи "r" га эга бўлмайди. Биринчи қарашда бундай таъриф жуда ғайриоддий туюлади, чунки "r" хуқуқига эга бўлаолмаслик таркибида enter “r” into $M[s, o]$ амали бўлган командалардан фойдаланишдан воз кечишга олиб келадигандек, аммо аслида бундай эмас. Масала шундаки, субъект ёки объектнинг йўқ қилиниши матрицанинг мос қатор ёки устунидаги барча хуқуқларнинг йўқ қилинишига олиб келади, аммо қатор ёки устуннинг ўзини йўқ қилинишига ва матрица ўлчамларининг қисқаришига олиб келмайди. Демак, дастлабки ҳолатда қандайдир ячейкада “r” хуқуқ мавжуд бўлган бўлса, бу хуқуққа тааллуқли

бўлган субъект ёки объект йўқ қилинганидан сўнг ячейка тозаланади, аммо субъект ёки объект яратилиши натижасида мос *enter* командаси ёрдамида ушбу ячейкага яна “*r*” хуқуқ киритилади. Бу хавфсизликнинг бузилишини англатмайди.

Хавфсизлик мезонидан келиб чиқадики, ушбу модел учун фойдаланиш хуқуқлар қийматини танлаш ва улардан командалар шартида фойдаланиш муҳим аҳамиятга эга. Модель хуқуқлар маъносига ҳеч қандай чеклашлар қўймай ва уларни тенг қийматли ҳисобласада, командалар бажарилиши шартида қатнашувчи хуқуқлар аслида объектлардан фойдаланиш хуқуқлари (масалан, ўқиш ва ёзиш) эмас, балки фойдаланишни бошқариш хуқуқлари, ёки фойдаланиш матрицаси ячейкаларини модификациялаш хуқуқлари ҳисобланади. Шундай қилиб, ушбу модел моҳиятан нафақат субъектларнинг объектлардан фойдаланишни, балки субъектдан объектга фойдаланиш хуқуқларини тарқалишини тавсифлайди. Чунки айнан фойдаланиш матрицаси ячейкаларининг мазмунининг ўзгариши командалар, жумладан хавфсизлик мезонининг бузилишига олиб келувчи, фойдаланиш матрицасининг ўзини модификацияловчи командалар бажарилиши имконини белгилайди.

Таъкидлаш лозимки, мухофазаланган тизимни қуриш амалиёти нуқтаи назаридан Харрисон-Руззо-Ульман модели амалга оширишда энг оддий ва бошқаришда самарали ҳисобланади, чунки ҳеч қандай мураккаб алгоритмларни талаб қилмайди, ва фойдаланувчилар ваколатларини объектлар устида амал бажарилишигача аниқликда бошқаришга имкон беради. Шу сабабли, ушбу модел замонавий тизимлар орасида кенг тарқалган. Ундан ташқари ушбу моделда таклиф этилган хавфсизлик мезони амалий жиҳатдан жуда кучли ҳисобланади, чунки олдиндан тегишли ваколатлар берилмаган фойдаланувчиларнинг баъзи ахборотдан фойдалана олмасликларини кафолатлайди.

Барча дискрецион моделлар “троян оти” ёрдамидаги хужумга нисбатан заиф, чунки уларда фақат субъектларнинг объектлардан фойдаланиш

амаллари назоратланади (улар орасидаги ахборот оқими эмас). Шу сабабли, бузғунчи қандайдир фойдаланувчига унга билдирмай “троян” дастурини қистирса, бу дастур ушбу фойдаланувчи фойдалана оладиган объектдан бузғунчи фойдалана оладиган объектга ахборотни ўтказади. Натижада хавфсизликнинг дискрецион сиёсатининг ҳеч қандай қоидаси бузилмайди, аммо ахборотнинг сирқиб чиқиши содир бўлади.

Шундай қилиб, Харрисон-Руззо-Ульманнинг дискрецион модели умумий қуйилишида тизим хавфсизлигини кафолатламайди, аммо айнан ушбу модель хавфсизлик сиёсати моделларининг бутун бир синфига асос бўлиб хизмат қиладики, улар фойдаланишни бошқаришда ва хуқуқларни тарқалишини назоратлашда барча замонавий тизимларда ишлатилади.

Назорат саволлари:

1. Хавфсизлик моделлари ва улардан фойдаланиш ҳолатларини тавсифлаб беринг.
2. Харрисон-Руззо-Улманнинг дискрецион моделида бажариладиган амалларни тушунтириб беринг.
3. Харрисон-Руззо-Улманнинг дискрецион моделида хавфсизлик мезонини таърифлаб беринг.
4. Харрисон-Руззо-Улманнинг дискрецион моделининг афзалликлари ва камчиликларини тушунтириб беринг.

4.2.Белла-ЛаПадуланинг мандатли модели.

Фойдаланишни бошқаришнинг мандатли модели кўпгина мамлакалтларнинг давлат ва ҳукумат муассасаларида қабул қилинган махфий хужжат алмашиш қоидаларига асосланган. Белла Лападула сиёсатининг асосий мазмуни амалий ҳаётдан олинган бўлиб, ҳимояланувчи ахборотни ишлашда қатнашувчиларга ва бу ахборот мавжуд бўлган хужжатларга хавфсизлик сатхи номини олган махсус белги, масалан “махфий”, “мутлақо махфий” ва ҳ. кабиларни тайинлашдан иборат. Хавфсизликнинг барча

сатхлари ўрнатилган устунлик муносабати асосида тартибланади, масалан, “мутлақо махфий” сатхи “махфий” сатхидан юқори ёки ундан устун туради. Фойдаланишни назоратлаш ўзаро ҳаракатдаги томонларнинг хавфсизлик сатҳларига боғлиқ ҳолда қуйидаги иккита оддий қоида асосида амалга оширилади:

1. Ваколатли шахс (субъект) фақат хавфсизлик сатхи ўзининг хавфсизлик сатхидан юқори бўлмаган хужжатлардан ахборотни ўқишга ҳақли.

2. Ваколатли шахс (субъект) хавфсизлик сатҳи ўзининг хавфсизлик сатхидан паст бўлмаган хужжатларга ахборот киритишга хақли.

Биринчи қоида юқори сатх шахслари томонидан ишланадиган ахборотдан паст сатх шахслари томонидан фойдаланишдан ҳимоялашни таъминлайди. Иккинчи қоида (жуда муҳим қоида) ахборотни ишлаш жараёнида юқори сатх иштирокчиларига ахборотнинг сирқиб чиқишини (билиб ёки билмасдан) бартараф этади.

Шундай қилиб, дискрецион моделларда фойдаланишни бошқариш фойдаланувчиларга маълум объектлар устида маълум амалларни бажариш ваколатини бериш йўли билан амалга оширилса, мандатли моделлар фойдаланишни хуфия ҳолда – тизимнинг барча субъект ва объектларига хавфсизлик сатҳларини белгилаш ёрдамида бошқаради. Ушбу хавфсизлик сатҳлари субъектлар ва объектлар орасидаги жоиз ўзаро ҳаракатларни аниқлайди. Демак, фойдаланишни мандатли бошқариш бир хил хавфсизлик сатхи берилган субъектлар ва объектларни фарқламайди ва уларнинг ўзаро ҳаракатига чеклашлар мавжуд эмас. Шу сабабли фойдаланишни бошқариш мосланувчанликни талаб қилганида мандатли модель қандайдир дискрецион модель билан биргаликда қўлланилади. Бунда дискрецион модель бир сатхдаги субъект ва объектлар орасидаги ўзаро ҳаракатни назоратлашда ва мандатли моделни кучайтирувчи қўшимча чеклашларни ўрнатишда ишлатилади.

Хавфсизликнинг Белла-Лападула моделида тизим Харрисон-Руззо-

Ульман моделига ўхшаш субъектлар S, объектлар O ва фойдаланиш хуқуқлари тўплами кўринишида ифодаланади. Объектлар тўплами субъектлар тўпламини ўз ичига олади $S \subset O$ ва фойдаланишнинг фақат иккита хили *read (ўқиш), write (ёзиш)* кўрилади. Аммо ушбу модел қўшимча хуқуқларни (масалан, ахборотни қўшиш, дастурни бажариш ва ҳ.) киритиш билан кенгайтирилиши мумкин бўлсада, улар базавий (ўқиш ва ёзиш) хуқуқлар орқали акслантирилади. Фойдаланишни мосланувчан бошқаришни таъминлашга имкон бермайдиган бундай қатъий ёндашишнинг ишлатилиши мандатли моделда субъектнинг объект устида бажариладиган амал назоратланмаслиги, балки ахборот оқими назоратланиши билан изоҳланади. Ахборот оқими фақат икки хил бўлиши мумкин: субъектдан объектга (ёзиш), ёки объектдан субъектга (ўқиш).

Назорат саволлари:

1. Белла-Лападуланинг мандатли моделини тушунтириб беринг.
2. Харрисон-Руззо-Улманнинг дискрецион модели ва Белла-Лападуланинг мандатли моделларининг ўзаро фарқи.
3. Мандатли модел асосида фойдаланишни назоратлашда қўлланиладиган асосий қоидаларни тушунтириб беринг.

4.3. Хавфсизликнинг ролли модели

Ролли модел хавфсизлик сиёсатининг мутлақо ўзгача хили ҳисобланидики, бу сиёсат дискрецион моделга хос фойдаланишни бошқаришдаги мосланувчанлик билан мандатли моделга хос фойдаланишни назоратлаш қоидаларининг қатъийлиги орасидаги муросага асосланган.

Ролли моделда “субъект” тушунчаси “фойдаланувчи” ва “рол” тушунчалари билан алмаштирилади. Фойдаланувчи – тизим билан ишловчи ва маълум хизмат вазифаларини бажарувчи одам. Рол – тизимда фаол иштирок этувчи абстракт тушунча бўлиб, у билан маълум фаолиятни амалга ошириш учун зарур ваколатларининг чегараланган, мантиқий боғлиқ

тўплами боғланган.

Рол сиёсати кенг тарқалган, чунки бу сиёсат бошқа қатъий ва расмий сиёсатлардан фарқли ўлароқ реал ҳаётга жуда яқин. Ҳақиқатан, тизимда ишловчи фойдаланувчилар шахсий исмидан ҳаракат қилмай, маълум хизмат вазифаларни амалга оширади, яъни ўзларининг шахси билан боғлиқ бўлмаган қандайдир ролларни бажаради.

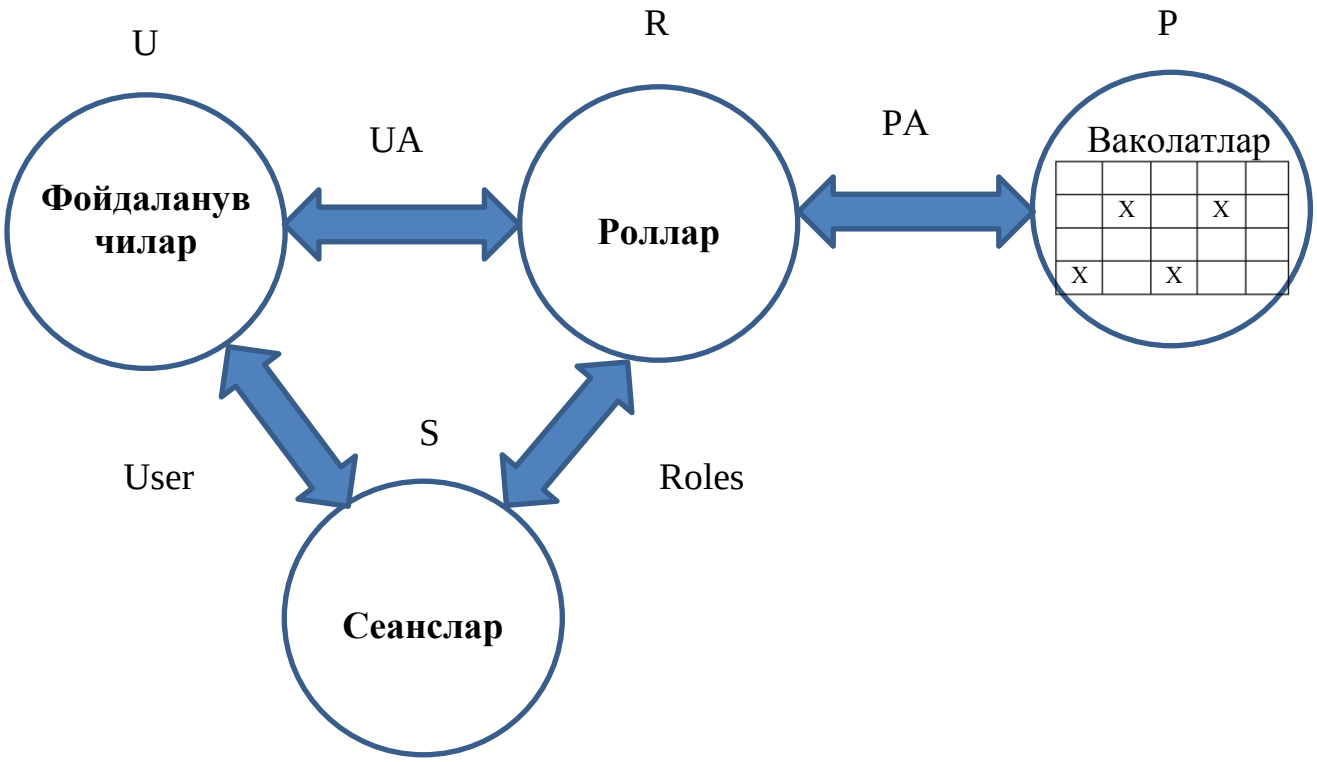
Шу сабабли фойдаланишни бошқариш ва ваколатларни бериш реал фойдаланувчиларга эмас, балки ахборот ишлашнинг маълум жараёнлари қатнашчиларини ифодаловчи абстракт ролларга бериш мантиққа тўғри келади. Хавфсизлик сиёсатига бундай ёндашиш татбиқий ахборот жараён қатнашчилари орасида вазифа ва ваколатларининг бўлинишини ҳисобга олишга имкон беради, чунки ролли сиёсат нуқтаи назаридан ахборотдан фойдаланишни амалга оширувчи фойдаланувчининг шахси эмас, балки унга хизмат вазифасини ўташга қандай ваколатлар зарурлиги аҳамиятлидир. Масалан, ахборотни ишловчи реал тизимда тизим маъмури, маълумотлар базаси менеджери ва оддий фойдаланувчилар ишлаши мумкин.

Бундай вазиятда ролли сиёсат ваколатларни уларнинг хизмат вазифаларга мос ҳолда тақсимлашга имкон беради: маъмур ролига унга тизим ишини назоратлашга ва тизим конфигурациясини бошқаришга имкон берувчи махсус ваколатлар берилади, маълумотлар базасининг менеджери маълумотлар базаси серверини бошқаришни амалга оширишга имкон беради, оддий фойдаланувчиларнинг хуқуқи эса татбиқий дастурларни ишга тушириш имконини берувчи минимум орқали чегараланади. Ундан ташқари, тизимда роллар сони реал фойдаланувчилар сонига мос келмаслиги мумкин – битта фодаланувчи, агар унга турли ваколатларни талаб қилувчи турли вазифалар юкланган бўлса, бир нечта ролни (кетма-кет ёки параллель) бажариши мумкин, бир нечта фойдаланувчилар бир хил ишни бажарса, улар бир хил ролдан фойдаланишлари мумкин.

Ролли сиёсат ишлатилганида фойдаланишни бошқариш икки босқичда амалга оширилади: биринчи босқичда ҳар бир роль учун объектдан

фойдаланиш хуқуқлари тўпламидан иборат ваколатлар тўплами кўрсатилади, иккинчи босқичда ҳар бир фойдаланувчига унинг қўлидан келадиган роллар рўйхати тайинланади. Ролларга ваколатлар энг кичик имтиёз принципида тайинланади, яъни ҳар бир фойдаланувчи ўзининг ишини бажариш учун фақат минимал зарур ваколатлар тўпламига эга бўлиши шарт.

Ролли модел тизимни қуйидаги тўпламлар кўринишида тавсифлайди (4.1-расмга қаралсин):



4.1-расм. Фойдаланишни бошқаришнинг ролли модели

U – фойдаланувчилар тўплами;

R – роллар тўплами;

P – объектдан фойдаланиш ваколатлари тўплами (масалан, фойдаланиш хуқуқлари матрицаси кўринишида);

S – фойдаланувчиларни тизим билан ишлаш сеанслари тўплами.

Юқорида санаб ўтилган тўпламлар учун қуйидаги муносабатлар белгиланади:

$PA \subseteq P \times R$- ҳар бир ролга унга берилган ваколатларни тайинлаб,

ваколатлар тўпламини роллар тўпламига акслантирилади;

$UA \subseteq U \times R$- ҳар бир фойдаланувчи учун унинг қўлидан келадиган роллар наборини аниқлаб, фойдаланувчилар тўпламини роллар тўпламига акслантиради.

Хавфсизликнинг ролли сиёсатида фойдаланишни бошқариш қоидалари қуйидаги функциялар орқали аниқланади:

$user: S \to U$ - ҳар бир сеанс S учун ушбу функция фойдаланувчини аниқлайди, бу фойдаланувчи тизим билан ушбу сеансни амалга оширади: $user\ (s) = u$;

$roles: S \to P(R)$ – ҳар бир сеанс S учун ушбу функция R тўпламдан роллар тўпламини аниқлайди, бу роллардан фойдаланувчи бир вақтда фойдаланиши мумкин: $roles\ (s) = \{r_i | (user(s_i, r_i) \in UA\}$.

$permissions: S \to P$ – ҳар бир сеанс S учун ушбу функция ушбу сеансга жоиз ваколатлар тўпламини беради, бу тўплам ушбу сеансда жорий этилган барча роллар ваколатларининг мажмуи сифатида аниқланади: $permissions(S) \to U_{r \in roles(S)}\{p_i | (p_i, r) \in PA\}$.

Ролли моделнинг хавфсизлик мезони сифатида қуйидаги қоида ишлатилади: тизим хавфсиз ҳисобланади, агар сеанс S да ишловчи ихтиёрий фойдаланувчи ваколат p ни талаб қилувчи ҳаракатларни фақат $p \in permissions(s)$ бўлганида амалга ошираолса.

Ролли моделнинг хавфсизлик мезони таърифидан келиб чиқадики, фойдаланишни бошқариш асосан ролларга ваколатларни бериш билан эмас, балки фойдаланувчиларга ролларни тайинловчи UA муносабатни ва сеансдаги жоиз роллар тўпламини аниқловчи $roles$ функциясини бериш орқали амалга оширилади. Шу сабабли ролли моделнинг кўп сонли талқини $user, roles$ ва $permission$ функциялар хили ҳамда PA ва UA муносабатларга қўйиладиган чеклашлар орқали фарқланади.

Хулоса сифатида таъкидлаш лозимки, фойдаланишни бошқаришнинг ролли сиёсати бошқа сиёсатлардан фарқли ўлароқ расмий исбот ёрдамида хавфсизликни амалда кафолатламай, фақат чеклашлар характерини

аниқлайди. Чеклашлар характерига риоя қилиш эса тизим хавфсизлигининг мезони хизматини ўтайди. Бундай ёндашиш фойдаланишни назоратлашнинг амалда осонгина қўллаш мумкин бўлган оддий ва тушунарли қоидаларини олишга имкон беради, аммо тизимни назарий исботий базадан махрум этади. Баъзи вазиятларда бу ҳол ролли сиёсатдан фойдаланишни қийинлаштиради, аммо ҳар қандай ҳолда роллардан фойдаланиш субъектлардан фойдаланишга қараганда қўлайроқ, чунки бу фойдаланувчилар орасида вазифаларни ва жавобгарлик доирасини тақсимлашни кўзда тутувчи ахборот ишлашнинг кенг тарқалган технологияларга жуда мос келади. Ундан ташқари, ролли сиёсат фойдаланувчиларга тайинланган роллар ваколатлари дискрецион ёки мандатли сиёсат томонидан назоратланганида бошқа хавфсизлик сиёсатлари билан биргаликда ишлатилиши мумкин. Бу эса фойдаланишни назоратлашни кўп сатхли схемасини қуришга имкон беради.

Хавфсизлик сиёсати моделлари бўйича хулосалар.

Хавфсизликнинг дискрецион ва мандатли сиёсатлари мавжуд автоматлаштирилган ахборот тизимларда қабул қилинган анъанавий механизмларга мос келади. Дискрецион моделлар учун объектларга (файлларга) хуқуқлар улар тегишли бўлган фойдаланувчилар томонидан тайинланади, жараён ваколатлари эса уни фойдаланувчи номидан бажарилаётган фойдаланувчи идентификатори орқали аниқланади. Мандатли модел учун объектларнинг хавфсизлик даражаси уларда сақланаётган хужжатларнинг махфийлик грифига мос келади, субъектларнинг хавфсизлик даражаси эса фойдаланувчиларнинг “рухсат(допуск)” категориясига асосан аниқланади. Аксинча, ролли сиёсат хавфизликнинг татбиқий сиёсатини акслантиради. Шу сабабли бу сиёсатда аниқ мослик мавжуд эмас. Ушбу сиёсатни амалга ошириш механизмини татбиқий масала шартлари ҳамда роллар ва ваколатларни тайинлаш методикасига асосан ишлаб чиқиш зарур.

Моделларнинг турли-туманлиги ва уларни амалга оширишдаги ёндашишларнинг кўплиги қайси моделлар бошқаларидан яхши ва қайсиларини у ёки бу ҳолда ишлатиш афзал ҳисобланади мазмундаги савол

туғилишига сабаб бўлади. Бу саволга жавоб қуйидагича. Хавфсизлик – тахдидларга муваффақиятли қаршилик кўрсатиш. Шу сабабли хавфсизлик моделининг ўзи ҳимояни таъминламайди, фақат тизим архитектурасининг асос бўладиган принципини тақдим этади. Бу принципнинг амалга оширилиши моделдаги мавжуд хавфсизлик хусусиятини таъминлайди. Демак, тизимнинг хавфсизлиги бир хилда учта омил орқали аниқланади: моделнинг хусусияти, унинг тизимга таъсир этувчи тахдидларга адекватлиги ва тизим қанчалик коррект амалга оширилганлиги. Ахборот хавфсизлиги назарияси соҳасидаги турли-туман назарий ишланмаларнинг мавжудлиги маълум тахдидларга адекват моделни танлаш муаммо эмас, охирги ҳал этувчи сўз танланган моделни ҳимояланган тизимда амалга оширишда қолган.

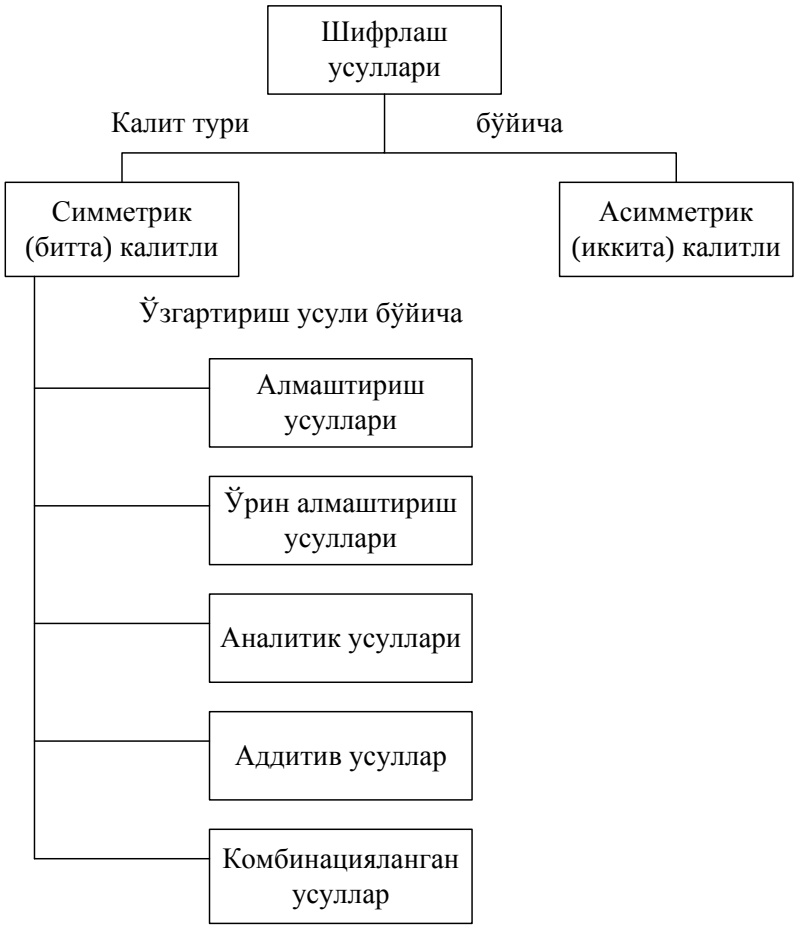
Назорат саволлари:

1. Ролли моделнинг хавфсиз ахборот коммуникация тизимларини лойиҳалашдаги ўрни.
2. Хавфсизликнинг ролли модели тизимни қандай тўпламлар кўринишида тавсифлайди?
3. Ролли моделнинг хавфсизлик мезонини тушунтириб беринг.
4. Ролли моделнинг дискрецион ва мандатли моделлардан фарқи нимада?

V боб. АХБОРОТНИ КРИПТОГРАФИК ҲИМОЯЛАШ

5.1. Шифрлаш усуллари

Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш вариантларидан бири 5.1–расмда келтирилган.



5.1-расм. Шифрлаш усулларининг туркумланиши.

Алмаштириш усуллари. Алмаштириш (подстановка) усулларининг моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит символлари билан маълум қоида бўйича алмаштиришдан иборатдир. Энг содда усул сифатида ***тўғридан тўғри алмаштиришни*** кўрсатиш мумкин. Дастлабки ахборот ёзилувчи A_0 алфавитнинг s_{0i} символларига шифрловчи A_1 алфавитнинг s_{1i} символлари мос қуйилади. Оддий ҳолда иккала алфавит ҳам бир хил символлар тўпламига эга бўлиши мумкин.

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича К символлар узунлигига эга бўлган дастлабки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади.

Моноалфавитли алмаштириш алгоритми қуйидаги қадамлар кетма-кетлиги кўринишда ифодаланиши мумкин

1-қадам. [1xR] ўлчамли дастлабки A_0 алфавитдаги ҳар бир символ s_0 Є T(i=$\overline{1,K}$) ни A_0 алфавитдаги s_{0i}символ тартиб рақамига мос келувчи $h_{0i}(s_{0i})$сонга алмаштириш йўли билан рақамлар кетма-кетлиги L_{0h} ни шакллантириш.

2-қадам.L_{0h} кетма-кетлигининг ҳар бир сонини $h_{1i}=(k_1 x h_{0i}(s_{0i})+k_2)(\mathrm{mod}R)$ формула орқали ҳисобланувчи L_{1h} кетма-кетликнинг мос сони h_{1i} га алмаштириш йўли билан L_{1h} сон кетма-кетлигини шакллантириш, бу ерда k_1-ўнлик коэффицент; k_2-силжитиш коэффициенти. Танланган k_1,k_2 коэффицентлар h_{0i}, h_{1i} сонларнинг бир маъноли мослигини таъминлаши лозим, $h_{1i}=0$ олинганида эса $h_{1i}=R$ алмашинуви бажарилиши керак.

3-қадам.L_{1h} кетма-кетликнинг ҳар бир сони $h_{1i}(s_{1i})$ни [1xR] ўлчамли шифрлаш алфавитнинг мос s_{1i} Є $T_1(i=\overline{1,K})$ символи билан алмаштириш йўли билан T_1 шифрматнни ҳосил қилиш.

4-қадам. Олинган шифрматн ўзгармас b узунликдаги блокларга ажратилади. Агар охирги блок тўлиқ бўлмаса блок орқасига махсус символ-тўлдирувчилар жойлаштирилади(масалан, *).

Мисол. Шифрлаш учун дастлабки маълумотлар қуйидагилар:

T_0=<ҲИМОЯ_ХИЗМАТИ>

A_0=<АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_>

A_1=<ОРЁЬЯТЭ-ЖМЧХАВДЙФҚКСЕЗПИЦГҲЛЪШБУЮ_ГН>

R=36; k_1=3; k_2=15; b=4

Алгоритмнинг қадамба-қадам бажарилиши қуйидаги натижаларни олинишига олиб келади.

1-қадам.L_{oh}=<35,10,14,16,31,36,23,10,9,14,1,20,10>

2-қадам.L_{1h}=<12,9,21,17,36,14,12,9,6,21,18,3,9>

3-қадам.T_1=<ХЖЕФНВҲЖТЕҚЁЖ>

4-қадам.T_1=<ХЖЕФ НВҲЖ ТЕҚЁ Ж***>

Расшифровка қилишда блоклар бирлаштирилиб *K* символли шифрматн T_1ҳосил қилинади. Расшифровка қилиш учун қуйидаги бутун сонли тенгламани ечиш лозим:

$$k_1h_{01}+k_2=nR+h_{1i}$$

k_1, k_2,h_{11}ва *R* бутун сонлар маълум бўлганда h_{0i} катталиги n ни саралаш орқали ҳисобланади. Бу муолажани шифрматннинг барча символларига татбиққилиш унинг расшифровка қилинишига олиб келади.

Алмаштириш усулининг камчилиги сифатида дастлабки ва берилган матнлар статистик характеристкаларининг бир хиллигидир. Дастлабки матн қайси тилда ёзилганлигини билган криптотаҳлилловчи ушлаб қолинган ахборотни статистик ишлаб, иккала алфавитдаги символлар ўртасидаги мувофиқликни аниқлаши мумкин.

Полиалфавитли алмаштириш усуллари айтарлича юқори криптобардошликка эга. Бу усуллар дастлабки матн символларини алмаштириш учун бир неча алфавитдан фойдаланишга асосланган. Расман полиалфавитли алмаштиришни қуйидагича тасаввур этиш мумкин. *N*-алфавитли алмаштиришда дастлабки A_0 алфавитдаги s_{01} символи A_1алфавитдаги s_{11}символи билан алмаштирилади ва ҳ. s_{0N} ни s_{NN}символ билан алмаштирилганидан сўнг $S_{0(N+1)}$символнинг ўрнини A_1 алфавитдаги $S_{1(N+1)}$символ олади ва ҳ.

Полиалфавитли алмаштириш алгоритмлари ичида ***Вижинер жадвали (матрицаси)*** T_B ни ишлатувчи алгоритм энг кенг тарқалган. Вижинер жадвали [*R*x*R*] ўлчамли квадрат матрицадан иборат бўлиб, (*R*-ишлатилаётган алфавитдаги символлар сони) биринчи қаторида символлар алфавит тартибида жойлаштирилади. Иккинчи қатордан бошлаб символлар чапга битта ўринга силжитилган ҳолда ёзилади. Сиқиб чиқарилган символлар ўнг тарафдаги бўшаган ўринни тўлдиради (циклик силжитиш). Агар ўзбек

алфавити ишлатилса, Вижинер матрицаси [36х36] ўлчамга эга бўлади (5.2-расм).

АБВГД.....	.....	.....ЎҚҒҲ_
БВГДЕ.....	.....	.....ҚҒҲ_А
ВГДЕЖ.....	.....	.....ҒҲ_АБ
.....		
_АБВГ.....	.....	.....ЯЎҚҒҲ

5.2-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиган *M* символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тўлиқ матрицасидан [*(M+1),R*] ўлчамли шифрлаш матрицаси $T_{(Ш)}$ажратилади. Бу матрица биринчи қатордан ва биринчи элементлари калит символларига мос келувчи қаторлардан иборат бўлади.

Агар калит сифатида <ҒЎЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта қатордан иборат бўлади. (5.3-расм)

$T_ш$

АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪ
ЭЮЯЎҚҒҲ_
ҒҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШ
ЬЪЭЮЯЎҚ
ЎҚҒҲ_АБВДЕЁЖЗИЙКЛМНОПРСТУФХЦ
ЧШЬЪЭЮЯ
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ
_АБВДЕЁЖ
АБВДЕЁЖЗИЙКЛМНОПРСТУФ-
ХЦЧШЬЪЭЮЯЎҚҒҲ_

5.3-расм. «Ғўза» калити учун шифрлаш матрицаси.

Вижинер жадвали ёрдамида шифрлаш алгоритми қуйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги *M* символли калит *K* ни танлаш.

2-қадам. Танланган калит *K* учун [(*M*+1),*R*] ўлчамли шифрлаш матрицаси $T_ш=(b_{ij})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи s_{0r} тагига калит символи k_m жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастлабки матн символлари шифрлаш матрицаси $T_ш$ дан қуйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

1) *K* калитнинг алмаштирилувчи s_{0r} символга мос k_mсимволи аниқланади;

2) шифрлаш матрицаси $T_ш$ даги $k_m= b_{j1}$шарт бажарилувчи *i*қатор топилади.

3) $s_{or}= b_{i1}$ шарт бажарилувчи *j* устун аниқланади.

4) s_{or} символи b_{ij}символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг бўш жойлари махсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан s_{1r} символлари ва мос калит символлари k_m кетма-кет танланади. $T_ш$ матрицада $k_m= b_{ij}$шартни қаноатлантирувчи *i*қатор аниқланади. *i*-қаторда $b_{ij}=s_{1r}$элемент аниқланади. Расшифровка қилинган матнда *r* - ўрнига b_{ij} символи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Мисол. К=<ҒЎЗА> калити ёрдамида Т=<ПАХТА ҒАРАМИ> дастлабки матнни шифрлаш ва расшифровка қилиш талаб этилсин. Шифрлаш ва рас-

шифровка қилиш механизми 5.4-расмда келтирилган.

Полиалфавитли алмаштириш усулларининг криптобардошлиги оддий алмаштириш усулларига қараганда айтарлича юқори, чунки уларда дастлабки кетма-кетликнинг бир хил символлари турли символлар билан алмаштирилиши мумкин. Аммо шифрнинг статистик усулларига бардошлилиги калит узунлигига боғлиқ.

Дастлабки матн	ПАХТА_ҒАРАМИ
Калит	Ғ ЎЗАҒЎЗАҒЎЗ А
Алмаштирилган сўнгги матн	МЎЯТҒЯЕАНЎФИ
Шифрматн	МЎЯТ ҒЯЕА НЎФИ
Калит	ҒЎЗА ҒЎЗА ҒЎЗА
Расшифровка қилинган матн	ПАХТ А_ҒА РАМИ
Дастлабки матн	ПАХТА_ҒАРАМИ

5.4-расм. Вижинер матрицаси ёрдамида шифрлаш мисоли.

Ўрин алмаштириш усуллари.Ўрин алмаштириш усулларига биноан дастлабки матн белгиланган узунликдаги блокларга ажратилиб ҳар бир блок ичидаги символлар ўрни маълум алгоритм бўйича алмаштирилади.

Энг осон ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокини матрицага қатор бўйича ёзишни, ўқишни эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица улчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8х8) учун калитнинг $1{,}6 \bullet 10^{9}$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16х16) калитнинг мумкин бўлган комбинацияси $1{,}4 \bullet 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЭҲМлар учун ҳам мураккаб ҳисобланади.

Гамильтон маршрутларига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади. Ушбу усул қуйидаги қадамларни бажариш орқали амалга оширилади.

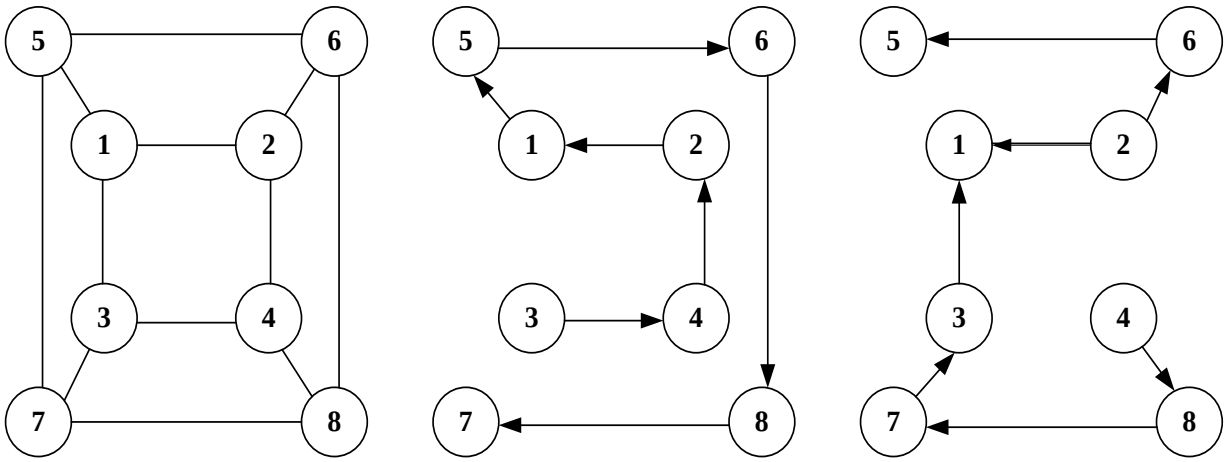
1-қадам. Дастлабки ахборот блокларга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охирги блокдаги бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади (масалан, *).

2-қадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади (5.5-расм).

3-қадам. Жадвалдаги символларни ўқиш маршрутларнинг бири бўйича амалга оширилади. Маршрутлар сонининг ошиши шифр криптобардошлигини оширади. Маршрутлар кетма-кет танланади ёки уларнинг навбатланиши калит ёрдамида берилади.

4-қадам. Символларнинг шифрланган кетма-кетлиги белгиланган *L* узунликдаги блокларга ажратилади. *L* катталик 1-қадамда дастлабки ахборот бўлинадиган блоклар узунлигидан фарқланиши мумкин.

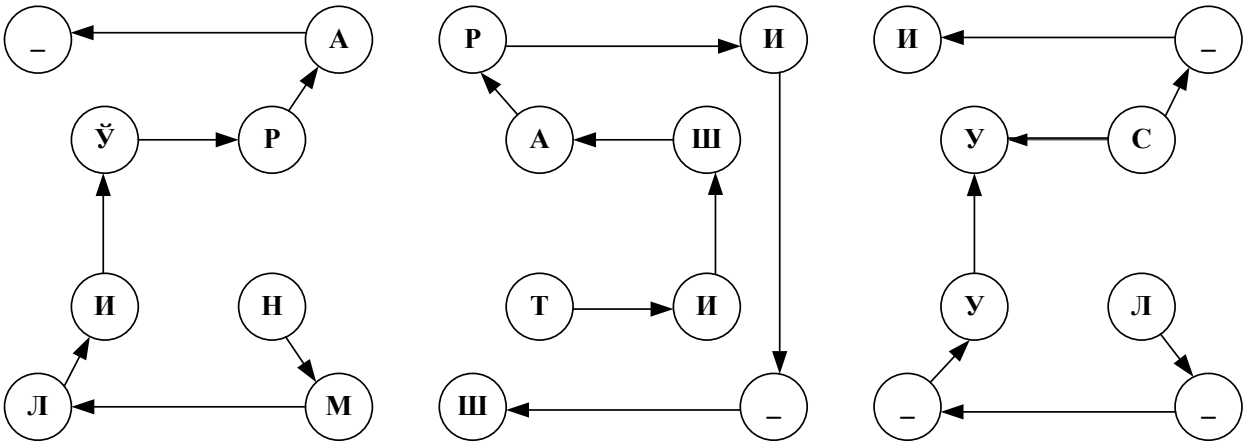
Расшифровка қилиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



5.5-расм. 8-элементли жадвал ва Гамильтон маршрутлари вариантлари.

Жадвалдан символлар элемент номерлари келиши тартибида ўқилади.

Мисол. Дастлабки матн T_0 «ЎРИН АЛМАШТИРИШ УСУЛИ»ни шифрлаш талаб этилсин. Калит ва шифрланган блоклар узунлиги мос ҳолда қуйидагиларга тенг: K=<2,1,1>, L=4. Шифрлаш учун 5.6-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрицалари тўлдирилган маршрутлар 5.10-расмда келтирилган кўринишга эга.



5.6-расм. Гамильтон маршрути ёрдамида шифрлаш мисоли.

1-қадам. Дастлабки матн учта блокка ажратилади. *Б1*=<ЎРИН_АЛМ>, *Б2*=<АШТИРИШ->, *Б3*=<УСУЛИ**>;

2-қадам. 2,1,1 маршрутли учта матрица тўлдирилади;

3-қадам. Маршрутларга биноан символларни жой-жойига қўйиш орқали шифрматнни ҳосил қилиш.

T_1=<НМЛИЎРА_ТИШАРИ_ШЛ__УУС_И>

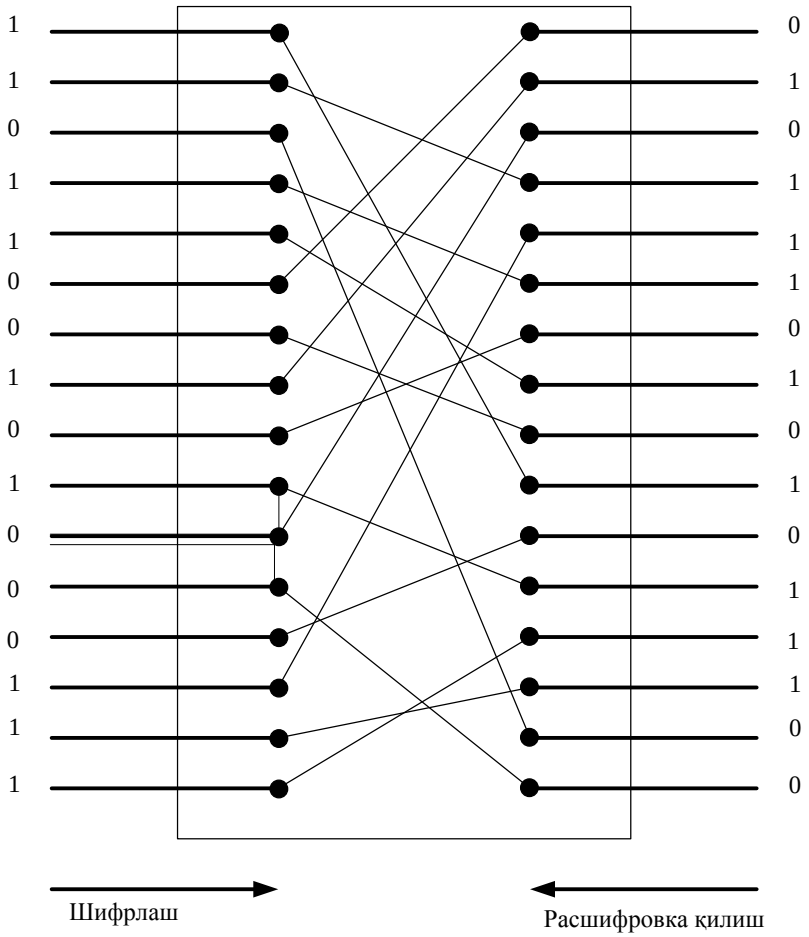
4-қадам. Шифрматнни блокларга ажратиш.

T_1=<НМЛИ ЎРА_ ТИША РИ_Ш Л__У УС_И>

Амалиётда ўрин алмаштириш усулини амалга оширувчи махсус аппарат воситалар катта аҳамиятга эга (5.7-расм).

Дастлабки ахборот блокининг параллел иккили коди (масалан, икки байт) схемага берилади. Ички коммутация ҳисобига схемада битларнинг блоклардаги ўринлари алмаштирилади. Расшифровка қилиш учун эса сҳеманинг кириш ва чиқиш йўллари ўзаро алмаштирилади.

Ўрин алмаштириш усулларининг амалга оширилиши содда бўлсада, улар иккита жиддий камчиликларга эга. Биринчидан, бу усулларни статистик ишлаш орқали фош қилиш мумкин. Иккинчидан, агар дастлабки матн узунлиги *K* символлардан ташкил топган блокларга ажратилса, шифрни фош этиш учун шифрлаш тизимига биттасидан бошқа барча символлари бир хил бўлган тест ахборотининг *K-1* блокини юбориш кифоя.



5.7-расм. Ўрин алмаштириш схемаси.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асосланган шифрлаш усуллари энг кўп тарқалган. Дастлабки ахборотнинг $B_к=||b_j||$ вектор кўринишида берилган *k*- блокини шифрлаш $A=||a_{ij}||$ матрица калитни $B_к$ векторга кўпайтириш орқали амалга оширилади. Натижада $C_k=||c_i||$ вектор кўринишидаги шифрматн блоки ҳосил қилинади. Бу векторнинг элементлари $c_i = \sum_j a_{ij} b_j$ ифодаси орқали аниқланади.

Ахборотни расшифровка қилиш C_k векторларини A матрицага тескари бўлган A^{-1} матрицага кетма-кет кўпайтириш орқали аниқланади.

Мисол. T_0=<АЙЛАНА> сўзини матрица-калит

$$A=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}$$

ёрдамида шифрлаш ва расшифровка қилиш талаб этилсин.

Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквивалентини аниқлаш.

$$T_э=<1,10,12,1,14,1>$$

2-қадам. A матрицани B_1={1,10,12} ва B_2={1,14,1} векторларга кўпайтириш.

$$C_1=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}\cdot\begin{vmatrix}1\\ 10\\ 12\end{vmatrix}=\begin{vmatrix}137\\ 97\\ 156\end{vmatrix}$$

$$C_2=\begin{vmatrix}1 & 4 & 8\\ 3 & 7 & 2\\ 6 & 9 & 5\end{vmatrix}\cdot\begin{vmatrix}1\\ 14\\ 1\end{vmatrix}=\begin{vmatrix}65\\ 103\\ 137\end{vmatrix}$$

3-қадам. Шифрланган сўзни кетма-кет сонлар кўринишида ёзиш.

$$T_1=<137,97,156,65,103,137>$$

Шифрланган сўзни расшифровка қилиш қуйидагича амалга оширилади:

1-қадам. A матрицанинг аниқловчиси ҳисобланади:

$$|A|=-115\ .$$

2-қадам. Ҳар бир элементи А матрицадаги a_{ij} элементнинг алгебраик тўлдирувчиси бўлган бириктирилган матрица A^* аниқланади.

$$A^*=\begin{vmatrix}17 & -3 & -15\\ 52 & -43 & 15\\ -48 & 22 & -5\end{vmatrix}$$

3-қадам. Транспонирланган матрица A^T аниқланади.

$$A^T = \begin{vmatrix} 17 & 52 & -48 \\ -3 & -43 & 22 \\ -15 & 15 & -5 \end{vmatrix}$$

4-қадам. Қуйидаги формула бўйича тескари матрица A^{-1} ҳисобланади:

$$A^{-1} = \frac{A^t}{|A|}$$

Ҳисоблаш натижасида қуйидагини оламиз.

$$A^{-1} = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix}$$

5-қадам. B_1 ва B_2 векторлар аниқланади:

$$B_1 = A^{-1}C_1; \qquad B_2 = A^{-1}C_2.$$

$$B_1 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 137 \\ 97 \\ 156 \end{vmatrix} = \begin{vmatrix} 1 \\ 10 \\ 12 \end{vmatrix}$$

$$B_2 = \begin{vmatrix} -17/115 & -52/115 & 48/115 \\ 3/115 & 43/115 & -22/115 \\ 15/115 & -15/115 & 5/115 \end{vmatrix} \cdot \begin{vmatrix} 65 \\ 103 \\ 137 \end{vmatrix} = \begin{vmatrix} 1 \\ 14 \\ 1 \end{vmatrix}$$

6-қадам. Расшифровка қилинган сўзнинг сон эквиваленти $T_э$=<1,10,12,1,14,1> символлар билан алмаштирилади. Натижада дастлабки сўз T_0=<АЙЛАНА>ҳосил бўлади.

Шифрлашнинг аддитив усуллари. Шифрлашнинг ***аддитив усулларига*** биноан дастлабки ахборот символларига мос келувчи рақам кодларини кетма-кетлиги ***гамма*** деб аталувчи қандайдир символлар кетма-кетлигига мос келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашиннг аддитив усуллари ***гаммалаш*** деб ҳам аталади.

Ушбу усуллар учун калит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги калит узунлигига ва унинг статистик характеристикаларининг текислигига боғлиқ. Агар калит шифрланувчи символлар кетма-кетлигидан қисқа бўлса, шифрматн криптотахлилловчи томонидан статистик

усуллар ёрдамида расшифровка қилиниши мумкин. Калит ва дастлабки ахборот узунликлари қанчалик фарқланса, шифр-матнга муваффақиятли хужум эҳтимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан иборат бўлса, калитни билмасдан туриб шифрматнни расшифровка қилиш амалий жиҳатдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда калит сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг кўп тарқалган ва самарали ҳисобланади. Генератор псевдотасодифий сонларнинг чексиз кетма-кетлигини шакллантиришда нисбатан қисқа узунликдаги дастлабки ахборотдан фойдаланади.

Псевдотасодифий сонлар кетма-кетлигини шакллантиришда конгруэнт генераторлардан ҳам фойдаланилади. Бу синф генераторлари сонларнинг шундай псевдотасодифий кетма-кетликларини шакллантирадики, улар учун генераторларнинг даврийлиги ва чиқиш йўли кетма-кетликларининг тасодифийлиги каби асосий характеристкаларини қатъий математик тарзда ифодалаш мумкин.

Конгруэнт генераторлар ичида ўзининг соддалиги ва самаралилиги билан чизиқли генератор ажралиб тўради. Бу генератор қуйидаги муносабат бўйича сонларнинг псевдотасодифий кетма-кетликларини шакллантиради.

$$T(i+1) = (a \cdot T(i) + c) \bmod m;$$

бу ерда a ва c – ўзгармаслар, T(0) –туғдирувчи(сабаб бўлувчи) сон сифатида танланган дастлабки катталик.

Бундай датчикнинг такрорланиш даври a ва c катталикларига боғлиқ. mқиймати одатда 2^S га тенг қилиб олинади, бу ерда *s*-компьютердаги сўзнинг битлардаги узунлиги. Шакллантирувчи сон кетма-кетликларининг такрорланиш даври *c*-тоқ сон ва a (mod4)=1 бўлгандагина максималь бўлади. Бундай генераторларни аппарат ёки программ воситалари орқали осонгина яратиш

мумкин.

Шифрлашнинг комбинацияланган усуллари. Қудратли компьютерлар, тармоқ технологиялари ва нейронли ҳисоблашларнинг пайдо бўлиши ҳозиргача умуман фош қилинмайди деб ҳисобланган криптографик тизимларни обрўсизлантирилишига сабаб бўлди. Бу эса ўз навбатида юқори бардошликка эга криптографик тизимларни яратиш устида ишлашни тақозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. Қуйида энг кам вақт сарфида криптобардошликни жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу комбинацияланган усулига биноан маълумотларни шифрлаш икки босқичда амалга оширилади. Биринчи босқичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи босқичда шифрланган маълумотлар махсус усул бўйича қайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фарқли бўлган сон матрицасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни қўллашда агар шифр гаммаси сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош этиш жуда қийин. Одатда шифр гаммаси ҳар бир шифрланувчи сўз учун тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг ҳеч қандай қисми маълум бўлмаса, шифрни фақат тўғридан-тўғри саралаш орқали фош этиш мумкин. Бунда криптобардошлик калит ўлчами орқали аниқланади. Шифрлашнинг бу усулидан кўпинча ҳимоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз Кбайтини шифрлаш имконияти мавжуд. Расшифровка қилиш жараёни-калит маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Шифрланган маълумотлар векторини матрицага кўпайтиришни қўллашда шифрланган матн бир байт узунликдаги f_i векторларга ажратила-

ди ва ҳар бир вектор квадрат матрица $\|M_{ij}\|$ га кўпайтирилади ва шифрланган векторлар шакллантирилади:

$$f_i^* = f_i \cdot \|M_{ij}\|$$

Бу усулнинг асосий афзаллиги сифатида унинг маълумотлар ишланишининг турли жабхаларидаги мосланувчанлигини кўрсатиш мумкин. Ҳар бир вектор алоҳида шифрланганлиги сабабли маълумотлар блокини узатиш ва дастурланган маълумотлардан ихтиёрий фойдаланиш имконияти туғилади. Ушбу усулни аппарат ёки дастурий усулда амалга ошириш мумкин.

Расшифровка қилиш жараёнида шифрланган f^* векторларни тескари матрица $\left(\|M_{ij}^{-1}\|\right)$ га кўпайтирилади.

$$f_i = f_i^* \cdot \|M_{ij}^{-1}\|$$

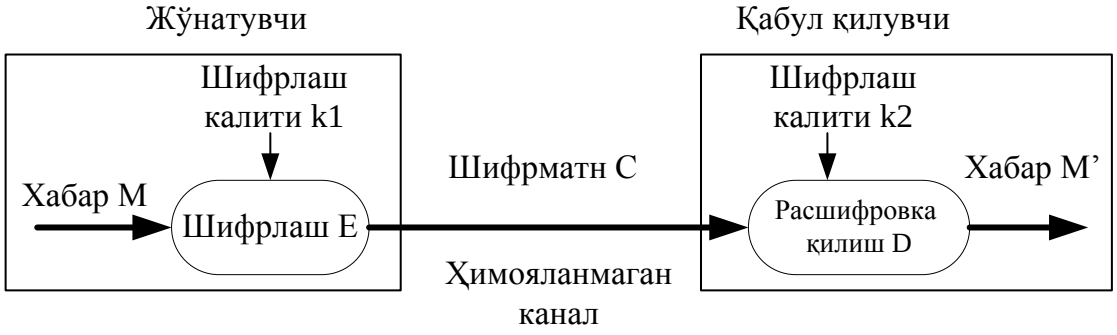
Комбинацияланган усулларнинг юқори самарадорлигига унинг иккала босқичини аппарат усулда амалга ошириш орқали эришиш мумкин. Аммо бу ускуна харажатларининг жиддий ошишига олиб келади. Дастурий усулда амалга оширилишида эса маълумотларни шифрлаш ва расшифровка қилиш вақти ошиб кетади. Шу сабабли комбинацияланган усуларни аппарат-дастурий усулда, яъни усулнинг бир босқичи аппарат усулда, иккинчи босқичи дастурий усулда амалга оширилиши мақсадга мувофиқҳисобланади.

Назорат саволлари:

1. Шифрлашнинг моноалфавитли алмаштириш усулини тушунтириб беринг.
2. Полиалфавитли алмаштириш усулининг ишлаш принципи.
3. Ўрин алмаштириш усуллари қандай амалга оширилади?
4. Шифрлашнинг аналитик усулини тушунтириб беринг.
5. Шифрлашнинг аддитив усули қандай амалга оширилади?
6. Шифрлашнинг комбинацияланган усулини ёритиб беринг.

5.2. Симметрик шифрлаш тизимлари

Ахборотнинг ҳимоялашнинг аксарият механизмлари асосини шифрлаш ташкил этади. *Ахборотни шифрлаш* деганда очиқ ахборотни (дастлабки матнни) шифрланган ахборотга ўзгартириш (шифрлаш) ва аксинча (расшифровка қилиш) жараёни тушунилади. Шифрлаш криптотизимининг умумлаштирилган схемаси 5.8-расмда келтирилган.



5.8-расм. Шифрлаш криптотизимининг умумлаштирилган схемаси.

Узатилувчи ахборот матни M криптографик ўзгартириш E_{k1} ёрдамида шифрланади, натижада шифрматн C олинади:

$$C = E_{k1}(M)$$

бу ерда $k1$ – шифрлаш калити деб аталувчи E функциянинг параметри.

Шифрлаш калити ёрдамида шифрлаш натижаларини ўзгартириш мумкин. Шифрлаш калити муайян фойдаланувчига ёки фойдаланувчилар гуруҳига тегишли ва улар учун ягона бўлиши мумкин. Муайян калит ёрдамида шифрланган ахборот фақат ушбу калит эгаси (ёки эгалари) томонидан расшифровка қилиниши мумкин.

Ахборотни тескари ўзгартириш қуйидаги кўринишга эга:

$$M' = D_{k2}(C)$$

D функцияси E функцияга нисбатан тескари функция бўлиб, шифр матнни расшифровка қилади. Бу функция ҳам $k2$ калит кўринишидаги қўшимча параметрга эга. $k1$ ва $k2$ калитлар бир маъноли мосликка эга бўлишлари шарт. Бу ҳолда расшифровка қилинган M' ахборот M га эквивалент бўлади. $k2$ калити ишончли бўлмаса D функция ёрдамида $M' = M$ дастлабки матнни олиб бўлмайди.

Криптотизимларнинг иккита синфи фарқланади:

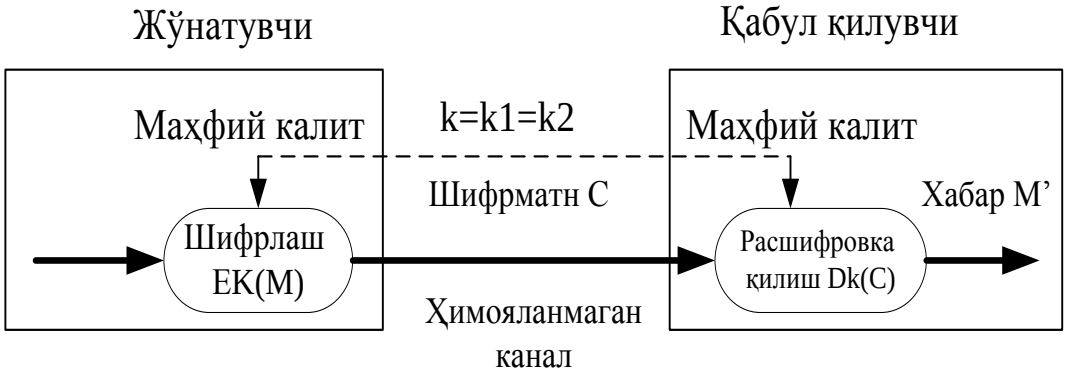
- симметрик криптотизим (бир калитли);

- асимметрик криптотизим (иккита калитли).

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка қилиш учун битта калитнинг ўзи ишлатилади. Демак, шифрлаш калитидан фойдаланиш хуқуқига эга бўлган ҳар қандай одам ахборотни расшифровка қилиши мумкин. Шу сабабли, симметрик криптотизимлар маҳфий калитли криптотизимлар деб юритилади. Яъни шифрлаш калитидан фақат ахборот аталган одамгина фойдалана олиши мумкин. Шифрлашнинг симметрик криптотизими схемаси 5.9-расмда келтирилган.

Электрон хужжатларни узатишнинг конфиденциаллигини симметрик криптотизим ёрдамида таъминлаш масаласи шифрлаш калити конфиденциаллигини таъминлашга келтирилади. Одатда, шифрлаш калити маълумотлар файли ва массивидан иборат бўлади ва шахсий калит элтувчисидан масалан, дискетда ёки смарт-картада сақланади. Шахсий калит элтувчиси эгасидан бошқа одамларнинг фойдаланишига қарши чоралар кўрилиши шарт.

Симметрик шифрлаш ахборотни "ўзи учун", масалан, эгаси йўқлигида ундан рухсатсиз фойдаланишни олдини олиш мақсадида, шифрлашда жуда қулай хисобланади. Бу танланган файлларни архивли шифрлаш ва бутун бир мантиқий ёки физик дискларни шаффоф(автоматик) шифрлаш бўлиши мумкин.



5.9-расм. Симметрик шифрлаш криптотизимининг схемаси.

Симметрик шифрлашнинг ноқулайлиги - ахборот алмашинуви бошланмасдан олдин барча адресатлар билан махфий калитлар билан айирбошлаш заруриятидир. Симметрик криптотизимда махфий калитни алоқанинг умумфойдаланувчи каналлари орқали узатиш мумкин эмас. Махфий калит жўнатувчига ва қабул қилувчига калитлар тарқатилувчи ҳимояланган каналлар орқали узатилиши керак.

Симметрик шифрлаш алгоритмининг маълумотларни абонентли шифрлашда, яъни шифрланган ахборотни абонентга, масалан Internet орқали, узатишда амалга оширилган вариантлари мавжуд. Бундай криптографик тармоқнинг барча абонентлари учун битта калитнинг ишлатилиши хавфсизлик нуқтаи назаридан ножоиздир. Хақиқатан, калит обрўсизлантирилганда (йўқотилганида, ўғриланганда) барча абонентларнинг хужжат алмашиши хавф остида қолади. Бу ҳолда калитларнинг матрицаси (5.10-расм) ишлатилиши мумкин.

Калитлар матрицаси абонентларнинг жуфт-жуфт боғланишли жадвалидан иборат. Жадвалнинг ҳар бир элементи *i* ва *j* абонентларни боғлашга мўлжалланган ва ундан фақат ушбу абонентлар фойдалана оладилар. Мос ҳолда, калитлар матрицаси элементлари учун қуйидаги тенглик ўринли.

$$K_{ij} = K_{ji}.$$

Матрицанинг ҳар бир *i*-қатори муайян *i* абонентнинг қолган *N*-1 абонентлар билан боғланишини таъминловчи калитлар наборидан иборат. Калитлар набори (тармоқ наборлари) криптографик тармоқнинг барча абонентлари ўртасида тақсимланади. Тақсимлаш алоқанинг *ҳимояланган каналлари* орқали ёки қўлдан-қўлга тарзда амалга оширилади.

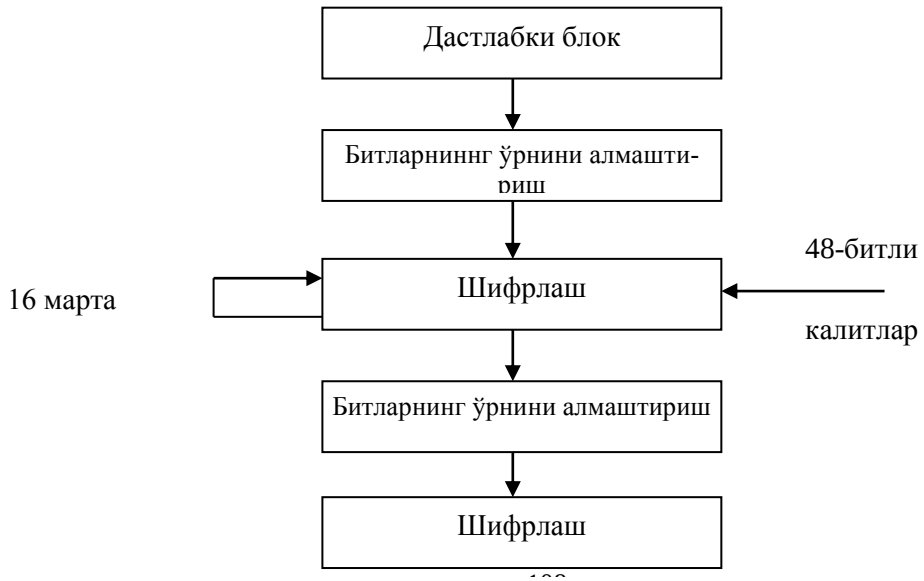
	1	2	3	…	n	
1	k_{11}	k_{12}	k_{13}	…	k_{1n}	1-абонент учун калитлар
2	k_{21}	k_{22}	k_{23}	…	k_{2n}	2-абонент учун калитлар
3	k_{31}	k_{32}	k_{33}	…	k_{3n}	3-абонент учун калитлар
…	…	…	…	…	…	…
n	k_{n1}	k_{n2}	k_{n3}	…	k_{nn}	n-абонент учун калитлар

АҚШнинг ахборотни шифрлаш стандарти. АҚШда давлат стандарти сифатида DES(Data Encryption Standart) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чиқилган бўлиб, АҚШ Миллий Хавфсизлик Агентлигининг мутахасислари томонидан текширилгандан сўнг давлат стандарти мақомини олган. DES стандартидан нафақат федерал департаментлар, балки нодавлат ташкилотлар, нафақат АҚШда, балки бутун дунёда фойдаланиб келинган.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади.

Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

DES алгоритмидаги шифрлаш жараёнининг блок-схемаси 5.11–расмда келтирилган.



5.11- расм. DES алгоритмида шифрлаш жараёнининг блок-схемаси

Расшифровка жараёни шифрлаш жараёнига инверс бўлиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.

Ҳозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроқсиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу компьютерларнинг замонавий ривожи учун жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вақт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).

Бу сабаблар АҚШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон қилишигаолиб келди. Танлов шартларига биноан алгоритмга қуйидаги талаблар қўйилган эди:

- алгоритм симметрик бўлиши керак;
- алгоритм блокли шифр бўлиши керак;
- блок узунлиги 128 бит бўлиб, 128, 192, ва 256 битли калит узунликларини таъминлаши лозим.

Ундан ташқари танловда иштирок этувчилар учун қуйидаги тавсиялар берилган эди:

- ҳам аппарат усулда ҳам программ усулда осонгина амалга оширилувчи амаллардан фойдаланиш;
- 32 хонали процессорлардан фойдаланиш;
- иложи борича шифр структурасини мураккаблаштирмаслик. Бу ўз навбатида барча қизиқувчиларнинг алгоритмни мустақил тарзда криптотахлил қилиб, унда қандайдир хужжатсиз имкониятлар йўқлигига ишонч ҳосил қилишлари учун зарур ҳисобланади.

2000 йил 2 октябрда танлов натижаси эълон қилинди. Танлов Ғолиби деб Бельгия алгоритми RIJNDAEL топилди ва шу ондан бошлаб алгоритм-

Ғолибдан барча патент чегараланишлари олиб ташланди.

Ҳозирда AES (Advanced Encryption Standard) деб аталувчи ушбу алгоритм Дж.Деймен (J. Daemen) ва В. Райджмен (V.Rijmen) томонидан яратилган. Бу алгоритм ноанъанавий блокли шифр бўлиб, кодланувчи маълумотларнинг ҳар бир блоки қабул қилинган блок узунлигига қараб 4x4, 4x6 ёки 4x8 ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

Шифрдаги барча ўзгартиришлар қатъий математик асосга эга. Амалларнинг структураси ва кетма-кетлиги алгоритмнинг ҳам 8-битли, ҳам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм структурасида баъзи амалларнинг параллел ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Ушбу алгоритмнинг шифрлаш жараёни қуйидаги блок схема орқали ифодаланган (5.12-расм).

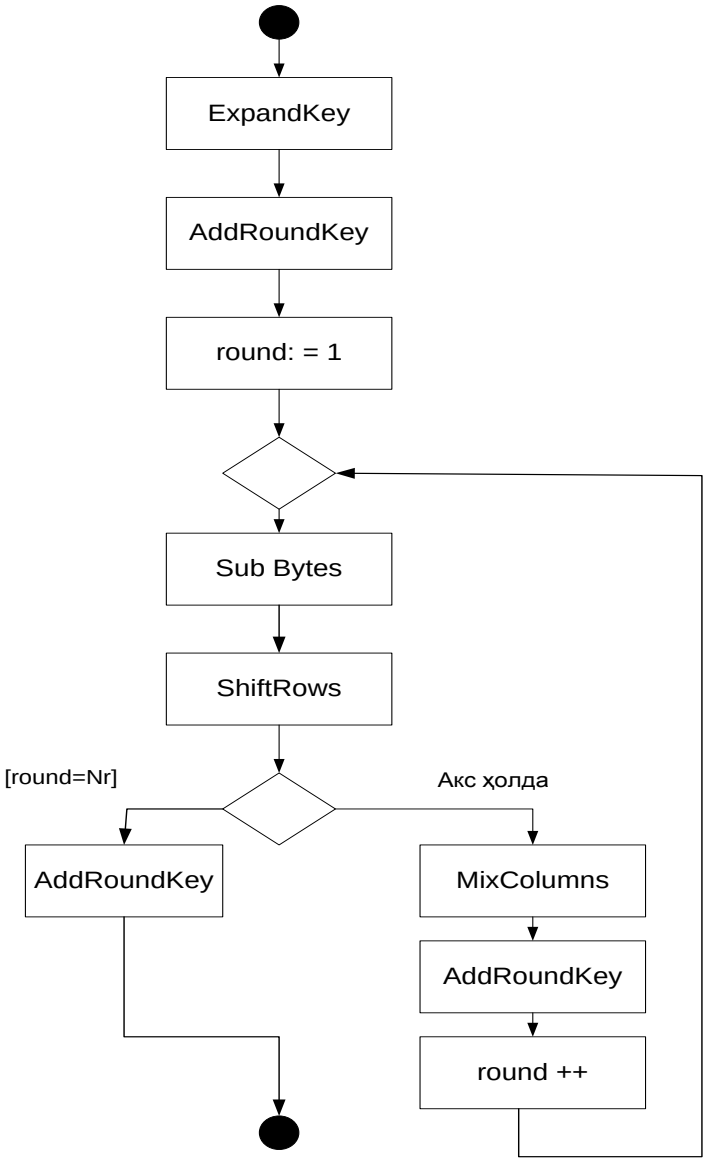
Шифрлаш жараёнининг ҳар бир раунд шифрлаш жараёнлари қуйида келтирилган тўртта акслантиришлардан фойдаланилган ҳолда амалга оширилади:

- *Sub Bytes* – алгоритмда жадвал асосида байтларни алмаштиради, яъни S-блок акслантиришларини амалга оширади;

- *ShiftRows* – алгоритмда берилган жадвалга кўра ҳолат байтларини циклик суриш;

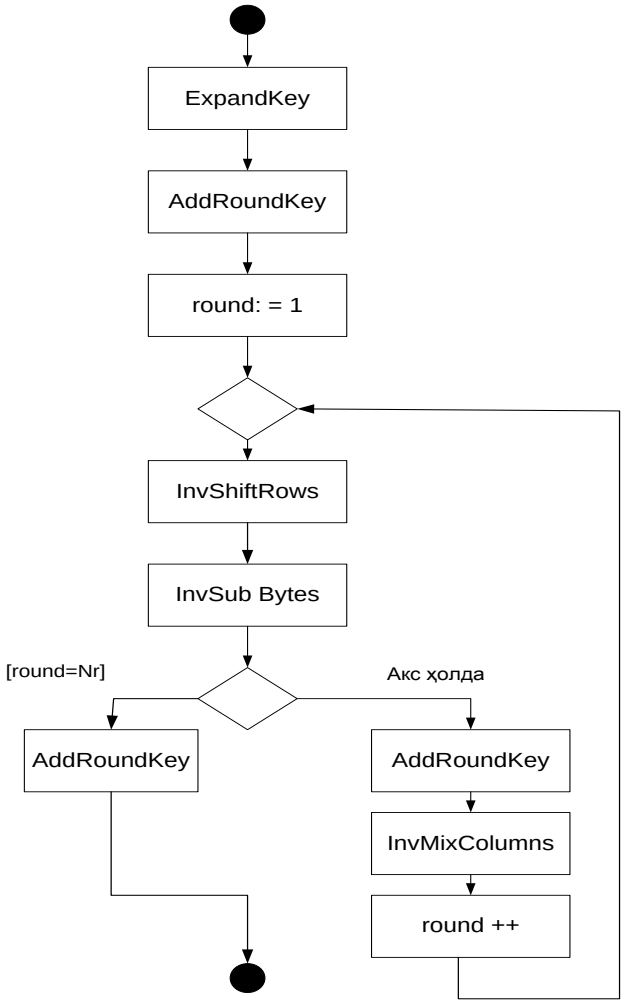
- *MixColumns* – устун элементларини аралаштиради, яъни алгоритмда берилган матрица бўйича акслантиришни амалга оширади;

- *AddRoundKey* – раунд калитларини қўшиш, яъни блоклар мос битларини *XOR* амали билан қўшиш.



5.12-расм. Шифрлаш жараёни

Дешифрлаш жараёнида шифрлаш жараёнидаги *Sub Bytes*, *ShiftRows*, *MixColumns* ва *AddRoundKey* функциялари ўрнига мос равишда *invSub Bytes*, *invShiftRows*, *invMixColumns* ва *AddRoundKey* тескари алмаштириш функциялари қўлланилади (5.13-расм).



5.13-расм. Дешифрлаш жараёни

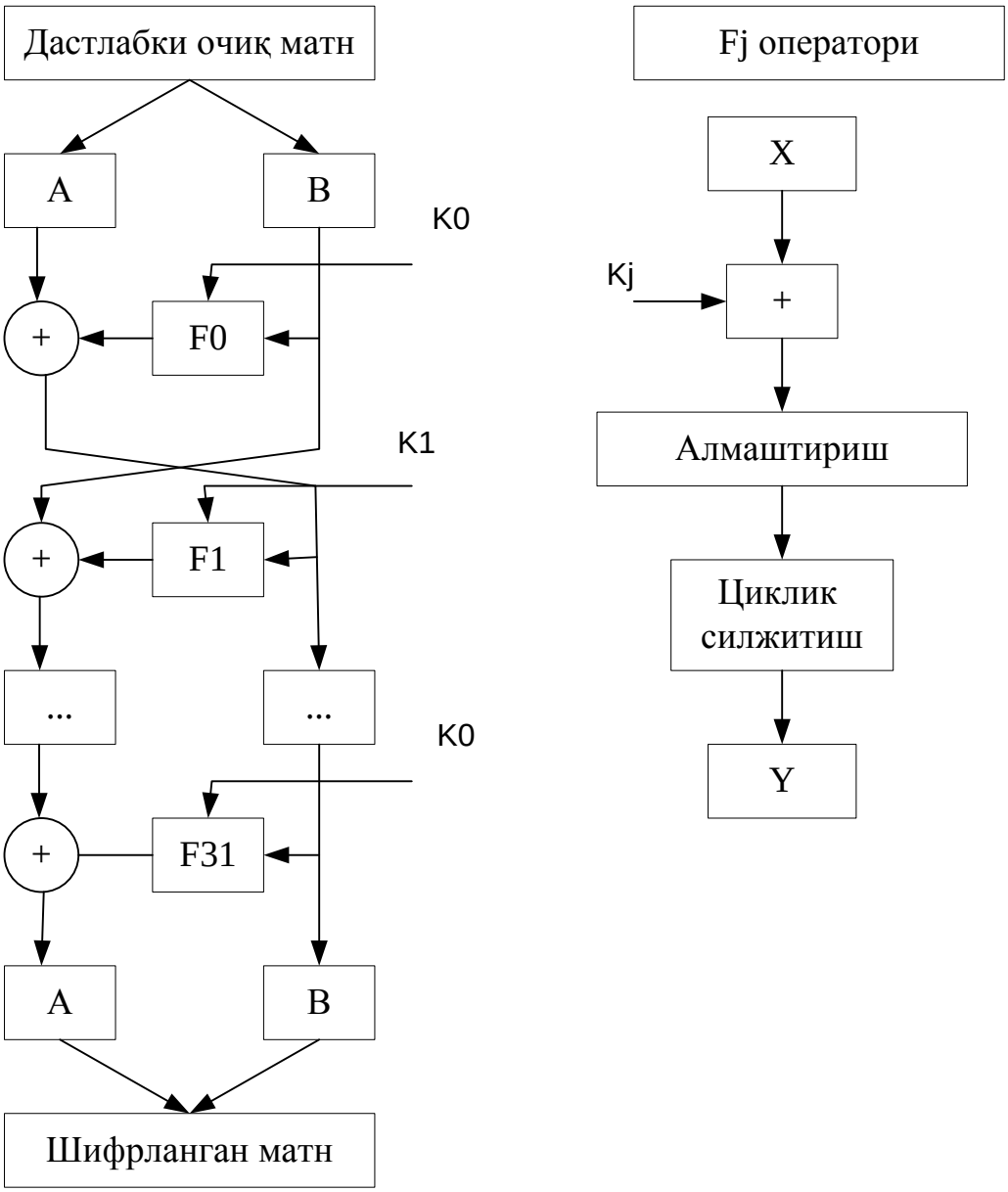
Россиянинг ахборотни шифрлаш стандарти. Росссия Федерациясида ҳисоблаш машиналари, комплекслари ва тармоқларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар махфийлик даражаси ихтиёрий бўлган ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва дастурий усулларида амалга оширилиши мумкин.

Стандартда ахборотни криптографик ўзгартиришнинг қуйидаги алгоритмлари мавжуд:

- оддий алмаштириш;
- гаммалаш;
- тескари боғланишли гаммалаш;
- имитовставка.

Бу алгоритмлар учун 8 та 32 хонали иккили сўзларга ажратилган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий ҳисобланади.

Оддий алмаштириш алгоритмининг моҳияти қуйидагича (5.14-расм).



5.14-расм. Оддий алмаштириш алгоритмида шифрлаш жараёнининг блок-схемаси.

Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали A ва B иккили сўзларга ажратилади. A сўзлар блокнинг кичик хоналарини B сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони i=32 бўлган циклик итерация оператори F_i қўлланилади. Блокнинг кичик битларидаги сўз (би-

ринчи итерациядаги А сўзи) калитининг 32 хонали сўзи билан mod2^{32} бўйича жамланади; ҳар бири 4 битдан иборат қисмларга (4 хонали кириш йўли векторлари) ажратилади; махсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилади; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги *B* сўзи) билан mod 2 бўйича жамланади.

Биринчи итерация тугаганидан сўнг кичик битлар ўрнида В сўз жойланади, чап тарафда эса *A* сўз жойланади. Кейинги итерацияларда сўзлар устидаги амаллар такрорланади.

Ҳар бир *i*-итерацияда K_j калитнинг (калитлар 8 та) 32 хонали сўзи қуйидаги қоидага биноан танланади

$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \le i \le 24 \quad \textit{бўлганда}, \\ 32 - i, & i \ge 25 \quad \textit{бўлганда}, \\ 0, & i = 32 \quad \textit{бўлганда}, \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби қуйидаги кўринишда бўлади:

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7,$

$K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_7, K_6, K_5, K_4, K_3, K_2, K_1, K_0,.$

Расшифровка қилишда калитлар тескари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узелларидан иборат. Алмаштириш узели ҳар бирида алмаштириш вектори (4 бит) жойлашган 16 қаторли жадвалдан иборат. Кириш йўли вектори жадвалдаги қатор адресини аниқласа, қатордаги сон алмаштиришнинг чиқиш йўли вектори ҳисобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам ўзгартирилади.

Гаммалаш алгоритмида дастлабки битларнинг кетма-кетлиги гаммаининг битлари кетма-кетлиги билан mod2 бўйича жамланади. Гамма оддий алмаштириш алгоритмига биноан ҳосил қилинади. Гаммани шаклантиришда иккита махсус доимийлардан ҳамда 64-хонали иккили кетма-кетлик

синхропосилкадан фойдаланилади. Ахборотни фақат синхропосилка борлигида расшифровка қилиш мумкин.

Синхропосилка махфий бўлмайди ва очиқҳолда компьютер хотирасида сақланиши ёки алоқа канали орқали узатилиши мумкин.

Тескари боғланишли гаммалаш алгоритми гаммалаш алгоритмидан фақат шифрлаш жараёнининг биринчи қадамидаги ҳаракатлар билан фарқланади.

Имитовставка нотўғри ахборотни зўрлаб киритилишидан ҳимоялашда ишлатилади. Имитовставка дастлабки ахборот ва махфий калитни ўзгартириш функцияси хисобланади. У *k* бит узунликдаги иккили кетма-кетликдан иборат бўлиб, *k* нинг қиймати нотўғри ахборотнинг зўрлаб киритилиши эҳтимоллиги $P_{зк}$ билан қуйидаги муносабат билан боғланган.

$$P_{зк}= \frac{1}{2^k}$$

Имитоставкани шакллантириш алгоритми қуйидаги харакатларнинг кетма-кетлигидан иборат. Очиқ ахборот 64 битли $T(i)$ (i=1,2,3,....,m) блокларга ажратилади, бу ерда m-шифрланувчи ахборот хажми орқали аниқланади. Биринчи блок $T(1)$ оддий алмаштириш алгоритмининг биринчи 16 итерацияларига биноан ўзгартирилади. Калит сифатида дастлабки ахборот шифрланишда ишлатиладиган калит олинади. Олинган 64 битли иккили сўз иккинчи блок $T(2)$ билан mod2 бўйича жамланади. $T(1)$ блок устида қандай итерация ўзгартиришлари бажарилган бўлса жамлаш натижаси устида ҳам шундай ўзгартиришлар амалга оширилади ва охирида $T(3)$ блок билан mod2 бўйича жамланади. Бундай харакатлар дастлабки ахборотнинг m-1 блоки бўйича такрорланади. Агар охирги $T(m)$ блок тўлиқ бўлмаса, у 64 хонагача ноллар билан тўлдиради. Бу блок $T(m\text{-}1)$ блок ишланиш натижаси билан mod2 бўйича жамланади ва оддий алмаштириш алгоритмининг биринчи 16 итерациялари бўйича ўзгартирилади. Ҳосил бўлган 64 хонали блокдан к бит узунликдаги сўз ажратиб олинади ва бу сўз имитовставка ҳисобланади.

Имитовставка шифрланган ахборотнинг охирига жойлаштирилади. Бу

ахборот олингандан сўнг, у расшифровка қилинади. Расшифровка қилинган ахборот бўйича имитовставка аниқланади ва олингани билан солиштирилади. Агар имитовставкалар мос келмаса, расшифровка қилинган ахборот нотўғри деб ҳисобланади.

Ўзбекистоннинг маълумотларни шифрлаш стандарти. O'z DSt 1105-2009 маълумотларни шифрлаш алгоритми диаматрицавий функцияларни қўллаган ҳолда 256 бит узунликдаги маълумотлар блокини шифрматнга ўгириш ва шифрматнни дастлабки матнга угириш учун 256 ёки 512 бит узунликдаги криптографик калитлардан фойдаланишга мўлжалланган.

Ушбу стандартда O'z DSt 1109 бўйича атамалар, ҳамда қуйидаги атамалар мос таърифлари билан қўлланилган:

- *инициализациялаш вектори:* Криптографик алгоритм доирасида криптографик жараённинг таянч нуқтасини аниқлаш учун ишлатиладиган вектор;

- *сеанс калити:* Шифрлаш калити ва функционал калит асосида шаклланадиган махфий калитларнинг икки ўлчамли массиви;

- *шифрлаш воситалари:* Ахборот алмаштиришнинг криптографик алгоритмларини амалга оширувчи ва уларни қайта ишлашда, сақлашда ва телекоммуникация каналлари бўйлаб узатишда ахборотни рухсат этилмаган фойдалана олишдан муҳофаза қилиш учун мўлжалланган аппарат, дастурий ва аппарат-дастурий воситалар;

- *шифрматн блокларини илактириш режими:* Ҳар бир шифрланган (дастлабки матнга ўгирилган) криптографик блок олдинги шифрланган (дастлабки матнга ўгирилган) блокка боғлиқ бўлган шифрлаш режими. Биринчи блок учун шифрматннинг олдинги блоки сифатида инициализациялаш векторидан фойдаланилади. Очиқ матннинг охирги блоки тўлиқ бўлмаган ҳолатда, у зарур узунликкача тўлдирилади;

- *электрон код китоби режими:* Очиқ матннинг барча блоклари маълумотларини шифрлаш алгоритмларига мувофиқ бир-биридан

мустақил, битта калит билан шифрланадиган шифрлаш режими.

Маълумотларни шифрлаш алгоритми қуйидаги функциялардан фойдаланади[9]:

- ***Aralash()*** – оддий шифр алмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштириш учун диаматрицавий қисмлар устида амалга оширилади; мазкур шифралмаштириш кириши Holat массивининг диаматрицавий қисмлари ҳамда K1 ва K2 массивлари бўлиб, чиқиши Holat массивидир;
- ***BaytAlmash()*** – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда Holat массиви элементларини алмаштириш массиви элементлари билан байт сатҳида алмаштириш учун фойдаланилади; мазкур шифралмаштириш кириши байт сатҳида Holat массиви, алмаштириш масиви чизиқли массив BsA [256] ёки BsAD [256] бўлиб, чиқиши байт сатҳида Holat массивидир;
- ***Sur()*** – Holat массиви элементларини янада яхшироқ аралаштириш учун, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда фойдаланилади; мазкур алмаштириш кириши байт сатҳида Holat массиви, чиқиши устун бўйлаб шифрлашда пастга ва сатр бўйлаб ўнгга ёки шифрни очишда устун бўйлаб юқорига ва сатр бўйлаб чапга сурилган байт сатҳида Holat массивидир;
- ***ShaklSeansKalitBayt()*** – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда BaytAlmash() шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши шифрлаш калити k ва функционал калит kf бўлиб, чиқиши байт сатҳида чизиқли массивлар B_{sA} [256] ва B_{sAD} [256];
- ***ShaklSeansKalit()*** – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда Aralash() шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши байтли элементлардан таркиб топган чизиқли массив Kst=[32] бўлиб, чиқиши махсус тузилмали диаматрицалардан ташкил

топган (K1t , K2) ёки (K1 , K2t) массивлар жуфтликларидир;

- ***ShaklBosqichKalit()*** – сеанс давомида сеанс-босқич калитидан босқич калитини шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда Qo'shBosqichKalit() алмаштиришини бажариш учун фойдаланилади; мазкур алмаштириш кириши чизиқли сеанс-босқич калити массиви kse, чиқиши байт сатҳида берилган икки ўлчамли Ke[8,4] массивидир;
- ***Qo'shBosqichKalit()*** – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда Holat ва босқич калити массиви Ke элементлари устида истисноли ЁКИ (2 модули бўйича битлаб қўшиш) амалини бажаришдан иборат; мазкур шифралмаштириш кириши байт сатҳида Holat массиви, Ke массиви бўлиб, чиқиши байт сатҳида Holat массивидир;
- ***Qo'shHolat()*** – оддий шифралмаштириш бўлиб, шифрлаш блоклари устида амалга ошириладиган электрон код китоби режимидан бошқа режимларда дастлабки матнни шифрматнга ва тескари йўналишда XOR амали иштирокида фойдаланиладиган алмаштириш.

Шифрлаш криптографик модулини ишга туширишда аввало модулга шифрлаш калити k ва функционал калит k_f, ўрнатилган босқичлар сони e ҳамда режим *m=ShBil* учун инициализациялаш вектори IV юкланади. Шунингдек, дастлабки матнни шифрматнга алмаштириш режимида дастлабки матн, шифрматнни дастлабки матнга алмаштириш режимида эса шифрматн криптографик модулнинг *Holat* массивига юкланади. Шифрлаш жараёнининг бошланишида ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit(K_{st}) ва ShaklBosqichKalit(k_{se}) ишга туширилади. ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit(K_{st}) шифралмаштиришлари чиқишида байт сатҳида алмаштириш массивлари ва диаматрицавий қисмлардан таркиб топган сеанс калити массивлари шакллантирилади. Бу массивлар токи k, k_f лар ўзгармас бўлиб қолар экан, кейинги сеансларда ҳам фойдаланилаверади. ShaklBosqichKalit(k_{se}) шифралмаштириши чиқишида бошлангич ва ҳар бир

босқич учун шакллантирилган босқич калитлари тўплами шакллантирилади.

Электрон код китоби (Elektron kod kitobi) m=Ekk ва шифр блокларни илактириш (ShifrBloklarni ilaktirish) m=ShBil режимларига тегишли псевдокод келтирилган.

Aralash(Holat,Ks), BaytAlmash(Holat,Ba), Qo'shBosqichKalit(Holat, Ke), Sur(Holat) оддий шифралмаштиришлари ва ShaklSeansKalitBayt(k,kf), ShaklSeansKalit(Kst), ShaklBosqichKalit(kse) ва Qo'shHolat(Holatт, Holat) алмаштиришлари кейинги бандда келтирилган.

Шифрлаш модулининг дастурий-аппаратли шаклида функционал калит янгилаш жараёнини ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit (K_{st}), ShaklBosqichKalit(k_{se}) алмаштириш жараёнлари билан қўшиб олиб бориш мақсадга мувофиқдир. Унда шифр процедурасига ShaklSeansKalitBayt(k,k_f), ShaklSeansKalit (K_{st}), ShaklBosqichKalit(k_{se}) натижаларини киритиш назарда тутилиши лозим.

Шифрлашп роцедурасининг псевдокоди қуйида келтирилган:

```
Shifr (int blok soni, byte IV[32], byte kirish [blok soni] [32], byte chiqish [blok soni] [32], byte k[32], byte kf [32], byte e)
begin
        byte ke [8, 4], Ks [8, 4], Ke [8, 4]
        Holat [8, 4], Holatn [8, 4]
if (m=Sh)
        ShaklSeansKalitBayt (k, kf)
        ShaklSeansKalit (Kst)
        ShaklBosqichKalit (kse)
        for blok=1 step 1 to blok_soni
        Holat=kirish[blok]
        if (m=ShBil)
                if (blok=1)
                        Holatn=IV
                else
```

```
                Holatn=chiqish[blok-1]
            end if
            Qo'shHolat (Holat, Holatn)
        end if
        for   bosqich=1 step 1 to e
            Qo'shBosqichKalit (Holat, Ke)
            Aralash (Holat, Ks)
            Sur (Holat)
            BaytAlmash (Holat, Ba)
        end for
        Qo'shBosqichKalit (Holat, Ke)
        Aralash (Holat, Ks)
        Chiqish [blok]=Holat
        end for
else
        ShaklSeansKalitBayt (k, kf)
        ShaklSeansKalit (Kst)
        ShaklBosqichKalit (kse)
        for blok=1 step 1 to blok_soni
            Holat=kirish [blok]
            Aralash (Holat, Ks)
            Qo'shBosqichKalit (Holat, Ke)
            for bosqich=1 step 1 to e
                BaytAlmash (Holat, Ba)
                Sur (Holat)
                Aralash (Holat, Ks)
                Qo'shBosqichKalit (Holat, Ke)
            end for
            if (m=ShBil)
                if (blok=1)
```

```
                    Holatn=IV
                else
                    Holatn=kirish[blok-1]
                end if
                Qo'shHolat (Holat, Holatn)
            end if
            chiqish[blok]=Holat
        end for
    end if
    end
```

Симметрик шифрлашнинг барча тизимлари қуйидаги камчиликларга эга:

- ахборот алмашувчи икала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига қуйиладиган талабларнинг қатъийлиги;
- калитларни яратиш ва тақсимлаш хизматига қуйиладиган талабларнинг юқорилиги.

Сабаби, ўзаро алоқанинг «ҳар ким – хар ким билан» схемасида «*n*» та абонент учун $n(n-1)/2$ та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғлиқлиги квадратли. Масалан, $n=1000$ абонент учун талаб қилинадиган калитлар сони $n(n-1)/2=499500$. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва воситаларсиз қўллашнинг иложи йўқ.

Назорат саволлари:

1. Симметрик шифрлаш тизимларининг ишлаш схемасини тушунтириб беринг.
2. АҚШнинг ахборотни шифрлаш стандарти DES алгоритмини тушунтириб беринг.
3. АҚШнинг ахборотни шифрлаш стандарти AES алгоритмини

тушунтириб беринг.

4. Россиянинг ахборотни шифрлаш стандарти ГОСТ 2814-89 алгоритмини ишлаш схемасини тушунтириб беринг.

5. Ўзбекистон Республикасининг маълумотларни шифрлаш стандарти O'z DSt 1105-2009 алгоритмини ишлаш схемасини тушунтириб беринг.

6. Симметрик шифрлаш тизимларининг афзалликлари ва камчиликлари.

5.3. Асимметрик шифрлаш тизимлари

Асимметрик криптотизимларда ахборотни шифрлашда ва расшифровка қилишда турли калитлардан фойдаланилади:

- *очиқ калит* K ахборотни шифрлашда ишлатилади, махфий калит k дан ҳисоблаб чиқарилади;
- *махфий калит* k, унинг жуфти бўлган очиқ калит ёрдамида шифрланган ахборотни расшифровка қилишда ишлатилади.

Махфий ва очиқ калитлар жуфт-жуфт генерацияланади. Махфий калит эгасида қолиши ва уни рухсатсиз фойдаланишдан ишончли химоялаш зарур (симметрик алгоритмдаги шифрлаш калитига ўхшаб). Очиқ калитнинг нусхалари махфий калит эгаси ахборот алмашинадиган криптографик тармоқ абонентларининг ҳар бирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 5.15-расмда келтирилган. Асимметрик криптотизимда шифрланган ахборотни узатиш қуйидагича амалга оширилади:

1. Тайёргарлик босқичи:

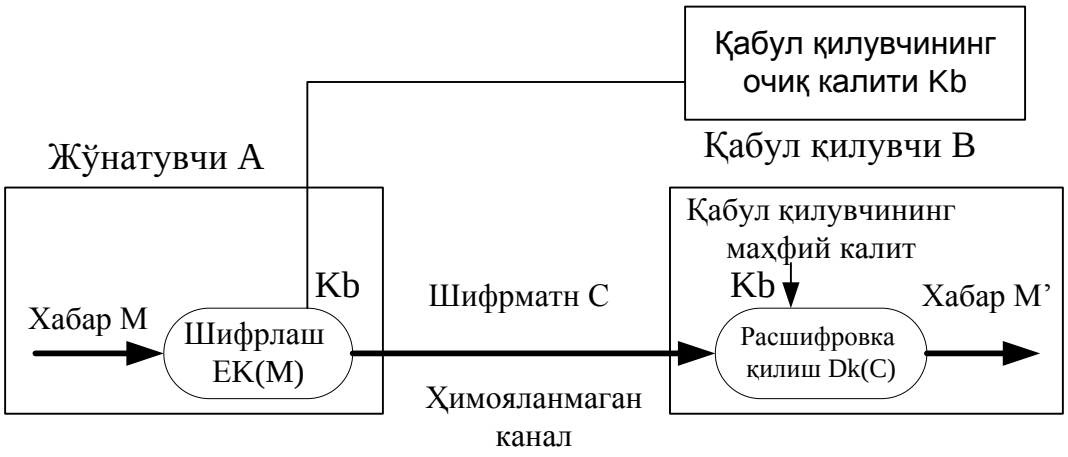
- абонент *B* жуфт калитни генерациялайди: махфий калит k_B ва очиқ калит K_B;

- очиқ калит K_Bабонент *A* га ва қолган абонентларга жўнатилади.

2. *A* ва *B* абонентлар ўртасида ахборот алмашиш:

- абонент *A* абонент *B*нинг очиқ калити K_B ёрдамида ахборотни шифрлайди ва шифрматнни абонент *B*га жўнатади;

- абонент *B* ўзининг махфий калити k_Bёрдамида ахборотни расшифровка қилади. Ҳеч ким (шу жумладан абонент *A* ҳам) ушбу ахборотни расшифровка қилаолмайди, чунки абонент *B*нинг маҳфий калити унда йўқ.



5.15-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси.

Асимметрик криптотизимда ахборотни химоялаш ахборот қабул қилувчи калити k_B нинг маҳфийлигига асосланган.

Асимметрик криптотизимларнинг асосий ҳусусиятлари қуйидагилар:

1. Очиқ калитни ва шифр матнни ҳимояланган канал орқали жўнатиш мумкин, яъни нияти бузуқ одамга улар маълум бўлиши мумкин.

2. Шифрлаш $E_B : M \rightarrow C$ ва расшифровка қилиш $D_B: C \rightarrow M$ алгоритмлари очиқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криптоалгоритми RSA 1993 йилда стандарт сифатида қабул қилинди. Ушбу криптоалгоритм ҳар тарафлама тасдиқланган ва калитнинг етарли узунлигида бардошлиги эътироф этилган. Ҳозирда 512 битли калит бардошликни таъминлашда етарли ҳисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор қувватининг ошиши RSAкриптоалгоритмининг тўлиқ саралаш хужумларга бардошлигининг йўқолишига олиб келади. Аммо, процессор қувватининг ошиши янада узун калитлардан фойдаланиш-

га, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

- калитларни маҳфий тарзда етказиш зарурияти йўқ; асимметрик шифрлаш очиқ калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса ҳимояланган алоқа сеанси бошланишидан аввал маҳфий калитлар алмашиниши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли боғланишлиги йўқолади; RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига боғлиқлиги чизиқли кўринишга эга (N фойдаланувчиси бўлган тизимда $2N$ калит ишлатилади).

Аммо асимметрик криптотизимлар, хусусан RSA криптотизими, камчиликлардан ҳоли эмас:

- ҳозиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтарилмаслигининг математик исботи йўқ;
- асимметрик шифрлаш симметрик шифрлашга нисбатан секин амалга оширилади, чунки шифрлашда ва расшифровка қилишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, RSAда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;
- очиқ калитларни алмаштириб қуйилишидан ҳимоялаш зарур. Фараз қилайлик "A" абонентнинг компьютерида "B" абонентнинг очиқ калити "K_B" сақланади. "n" нияти бузуқ одам "A" абонентда сақланаётган очиқ калитлардан фойдалана олади. У ўзининг жуфт (очиқ ва махфий) "K_n" ва "k_n" калитларини яратади ва "A" абонентда сақланаётган "B" абонентнинг "K_B" калитини ўзининг очиқ "K_n" калити билан алмаштиради. "A" абонент қандайдир ахборотни "B" абонентга жўнатиш учун уни "K_n" калитда (бу "K_B" калит деб ўйлаган ҳолда) шифрлайди. Натижада, бу хабарни "B" абонент ўқий олмайди, "n" абонент осонгина расшифровка қилади ва ўқийди. Очиқ калитларни ал-

маштиришни олдини олишда калитларни сертификациялашдан фойдаланилади.

Асимметрик шифрлаш тизимлари очиқ калитли шифрлаш тизимлари деб ҳам юритилади.Очиқ калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функциялардан фойдаланиш ётади. Бундай функциялар қуйидаги хусусиятларга эга. Маълумки x маълум бўлса $y=f(x)$ функцияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жихатдан мумкин эмас. Криптографияда яширин деб аталувчи йўлга эга бўлган бир томонли функциялар ишлатилади. z параметрли бундай функциялар қуйидаги хусусиятларга эга. Маълум z учун E_z ва D_z алгоритмларини аниқлаш мумкин. E_z алгоритми ёрдамида аниқлик соҳасидаги барча x учун $f_Z(x)$ функцияни осонгина олиш мумкин. Худди шу тариқа D_z алгоритми ёрдамида жоиз қийматлар соҳасидаги барча y учун тескари функция $x=f^{-1}(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча z ва деярли барча, y учун хатто E_z маълум бўлганида ҳам $f^{-1}(y)$ни ҳисоблашлар ёрдамида топиб бўлмайди. Очиқ калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

Очиқ калитни ишлатиб шифрлаш амалга оширилганда ўзаро мулоқатда бўлган субъектлар ўртасида махфий калитни алмашиш зарурияти йўқолади. Бу эса ўз навбатида узатилувчи ахборотнинг криптоҳимоясини соддалаштиради.

Очиқ калитли криптотизимларни бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алохида тилга олиш ўринли. Ҳозирда энг самарали ва кенг тарқалган очиқ калитли шифрлаш алгоритми сифатида RSA алгоритмини кўрсатиш мумкин. RSA номи алгоритмни яратувчилари фамилияларининг биринчи харфидан олинган (Rivest, Shamir ва Adleman).

Алгоритм модуль арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги қадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-қадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-қадам. Калитнинг очиқ ташкил этувчиси n ҳосил қилинади

$$n=p*q.$$

3-қадам. Қуйидаги формула бўйича Эйлер функцияси ҳисобланади:

$$f(p,q)=(p-1)(q-1).$$

Эйлер функцияси n билан ўзаро туб, 1 дан n гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига эга бўлмаган сонлар тушунилади.

4-қадам. $f(p,q)$қиймати билан ўзаро туб бўлган катта туб сон d танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи e сони аниқланади

$$e \cdot d = 1 (mod f(p,q)).$$

Бу шартга биноан $e \cdot d$ кўпайтманинг $f(p,q)$ функцияга бўлишдан қолган қолдиқ 1га тенг. e сони очиқ калитнинг иккинчи ташкил этувчиси сифатида қабул қилинади. Махфий калит сифатида d ва n сонлари ишлатилади.

6-қадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги L бит узунликдаги блокларга ажратилади, бу ерда $L–L \geq \log_2(n+1)$ шартини қаноатлантирувчи энг кичик бутун сон. Ҳар бир блок [0, n-1] оралиққа тааллуқли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот $X(i)$, i=$\overline{1, I}$ сонларнинг кетма-кетлиги орқали ифодаланади. i нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи $Y(i)$ сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e (\mathrm{mod} n).$$

Ахборотни расшифровка қилишда қуйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d (\mathrm{mod} n).$$

Мисол.<ГАЗ> сўзини шифрлаш ва расшифровка қилиш талаб этилсин.

Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. p=3 ва q=11 танлаб олинади.

2-қадам. $n = 3 \cdot 11 = 33$ ҳисобланади.

3-қадам. Эйлер функцияси аниқланади.

$$f(p,q) = (3-1) \cdot (11-1) = 20$$

4-қадам. Ўзаро туб сон сифатида d=3 сони танлаб олинади.

5-қадам. $(e \cdot 3) \cdot (\mathrm{mod} 20) = 1$ шартини қаноатлантирувчи е сони танланади. Айтайлик, e=7.

6-қадам. Дастлабки сўзнинг алфавитдаги харфлар тартиб рақами кетма-кетлигига мос сон эквиваленти аниқланади. А харфига –1, Г харфига-4, З харфига –9. Ўзбек алфавитида 36та харф ишлатилиши сабабли иккили кодда ифодалаш учун 6 та иккили хона керак бўлади. Дастлабки ахборот иккили кодда қуйидаги кўринишга эга бўлади:

000100 000001 001001.

Блок узунлиги L бутун сонлар ичидан $L \geq \log_2(33+1)$ шартини қаноатлантирувчи минималь сон сифатида аниқланади. n=33 бўлганлиги сабабли L =6.

Демак, дастлабки матн $X(i) =< 4,1,9 >$ кетма-кетлик кўринишида ифодаланади.

7-қадам. $X(i)$ кетма-кетлиги очиқ калит {7,33} ёрдамида шифрланади:

$$Y(1) = (4^7)(\mathrm{mod} 33) = 16384(\mathrm{mod} 33) = 16$$

$$Y(2) = (1^7)(\mathrm{mod} 33) = 1(\mathrm{mod} 33) = 1$$

$$Y(1) = (9^7)(\mathrm{mod} 33) = 4782969(\mathrm{mod} 33) = 15$$

Шифрланган сўз $Y(i)$=<16,1,15>

Шифрланган сўзни расшифровка қилиш махфий калит {3,33} ёрдамида бажарилади:

$$Y(1) = (16^3)(\mathrm{mod} 33) = 4096(\mathrm{mod} 33) = 4$$

$$Y(1) = (1^3)(\mathrm{mod} 33) = 1(\mathrm{mod} 33) = 1$$

$$Y(1) = (15^3)(\mathrm{mod} 33) = 3375(\mathrm{mod} 33) = 9$$

Дастлабки сон кетма-кетлиги расшифровка қилинган $X(i)$=<4,1,9> кўринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Келтирилган мисолда ҳисоблашларнинг соддалигини таъминлаш мақсадида мумкин бўлган кичик сонлардан фойдаланилди.

Эль-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. RSA ва Эль-Гамал тизимларининг асосий камчилиги сифатида модуль арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш мумкин. Бу ўз навбатида анчагина ҳисоблаш ресурсларини талаб қилади.

Мак-Элис криптотизимида хатоликларни тузатувчи кодлар ишлатилади. Бу тизим RSA тизимига нисбатан тезроқ амалга оширилсада, жиддий камчиликка эга. Мак-Элис криптотизимсида катта узунликдаги калит ишлатилади ва олинган шифрматн узунлиги дастлабки матн узунлигидан икки марта катта бўлади.

Барча очиқ калитли шифрлаш усуллари учун *NP*-тўлиқ масалани (тўлиқ саралаш масаласини) ечишга асосланган криптотахлил усулидан бошқа усулларининг йўқлиги қатъий исботланмаган. Агар бундай масалаларни ечувчи самарали усуллар пайдо бўлса, бундай хилдаги криптотизим обрўсизлантирилади.

Юқорида кўрилган шифрлаш усулларининг криптобардошлиги калит узунлигига боғлиқ бўлиб, бу узунлик замонавий тизимлар учун, лоақал, 90 битдан катта бўлиши шарт.

Айрим муҳим қўлланишларда нафақат калит, балки шифрлаш алгоритми ҳам маҳфий бўлади. Шифрларнинг криптобардошлигини ошириш учун бир неча калит (одатда учта) ишлатилиши мумкин. Биринчи калит ёрдамида шифрланган ахборот иккинчи калит ёрдамида шифрланади ва ҳ.

Назорат учун саволлар:

1. Асимметрик шифрлаш тизимларини ишлаш принципини тушунтириб беринг.
2. RSA асимметрик алгоритмининг ширфлаш қадамларини ёритиб

беринг.

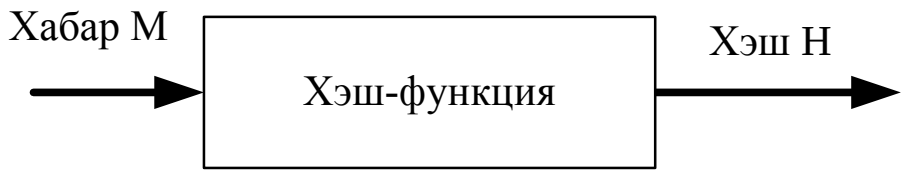
3. Эль Гамал асимметрик шифрлаш алгоритми қандай математик муаммоларга асосланган?

4. Асиммтерик ширфлаш алгоритмлари турига кирувчи қандай алгоритмларни биласиз?

5. Асиммтерик ширфлаш алгоритмларининг афзалликлари ва камчилилклари.

5.4.Хэшлаш функцияси

Хэшлаш функцияси (хэш-функцияси) шундай ўзгартиришки, кириш йўлига узунлиги ўзгарувчан хабар *M* берилганида чиқиш йўлида белгиланган узунликдаги қатор *h*(*M*) ҳосил бўлади. Бошқача айтганда, хеш-функция *h*(.) аргумент сифатида узунлиги ихтиёрий хабар (хужжат) *M* ни қабул қилади ва белгиланган узунликдаги хеш-қиймат (хеш) *H*=*h*(*M*)ни қайтаради (5.16-расм).



5.16-расм. Хэшни шакллантириш схемаси

Хэш-қиймат h(M) – хабар M нинг дайджести, яъни ихтиёрий узунликдаги асосий хабар *M*нинг зичлантирилган иккилик ифодаси. Хэшлаш функцияси ўлчами мегабайт ва ундан катта бўлган имзо чекилувчи хужжат *M*ни 128 ва ундан катта битга (хусусан, 128 ёки 256 бит) зичлашга имкон беради. Таъкидлаш лозимки, хеш-функция *h(M)*қийматининг хужжат *M*га боғлиқлиги мураккаб ва хужжат *M*нинг ўзини тиклашга имкон бермайди.

Хэшлаш функцияси қуйидаги хусусиятларга эга бўлиши лозим:

1. Хэш-функция ихтиёрий ўлчамли аргументга қўлланиши мумкин.
2. Хэш-функция чиқиш йўлининг қиймати белгиланган ўлчамга эга.
3. Хэш-функция *h*(*x*) ни ихтиёрий *"x"* учун етарлича осон ҳисоблан-

ади. Хэш-функцияни ҳисоблаш тезлиги шундай бўлиши керакки, хэш-функция ишлатилганида электрон рақамли имзони тузиш ва текшириш тезлиги хабарнинг ўзидан фойдаланилганига қараганда анчагина катта бўлсин.

4. Хэш-функция матн *M* даги орасига қўйишлар (вставки), чиқариб ташлашлар (выбросы), жойини ўзгартиришлар ва ҳ. каби ўзгаришларга сезгир бўлиши лозим.

5. Хэш-функция қайтарилмаслик хусусиятига эга бўлиши лозим.

6. Иккита турли хужжатлар (уларнинг узунлигига боғлиқ бўлмаган ҳолда) хэш-функциялари қийматларининг мос келиши эҳтимоллиги жуда кичкина бўлиши шарт, яъни ҳисоблаш нуқтаи назаридан $h(x')=h(x)$ бўладиган $x' \neq x$ ни топиш мумкин эмас.

Иккита турли хабарнинг битта тугунчага (свертка) зичлаш назарий жиҳатдан мумкин. Бу коллизия ёки тўқнашиш деб аталади. Шунинг учун хэшлаш функциясининг бардошлигини таъминлаш мақсадида тўқнашишларга йўл қўймасликни кўзда тутиш лозим. Тўқнашишларга бутунлай йўл қўймаслик мумкин эмас, чунки умумий ҳолда мумкин бўлган хабарлар сони хэшлаш функциялари чиқиш йўллари қийматларининг мумкин бўлган сонидан ортиқ. Аммо, тўқнашишлар эҳтимоллиги паст бўлиши лозим.

5-хусусият $h(.)$ бир томонлама эканлигини билдирса, 6 хусусият битта бир хил тугунчани берувчи иккита ахборотни топиш мумкин эмаслигини кафолатлайди. Бу сохталаштиришни олдини олади.

Шундай қилиб, хэшлаш функциясидан хабар ўзгаришини пайқашда фойдаланиш мумкин, яъни у *криптографик назорат йиғиндисини* (ўзгаришларни пайқаш коди ёки *хабарни аутентификациялаш коди* деб ҳам юритилади) шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлашда, электрон рақамли имзони шакллантаришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентифкациялашда ҳам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули *бир томонлама хеш-функция ёрдамида шифрлаш* ишлатила-

ди. Бу шифрлашнинг ўзига хослиги шундан иборатки, у моҳияти бўйича, бир томонламадир, яъни тескари муолажа – қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланади.

Энг оммабоп хэш-функциялар –MD4, MD5,SHA1, SHA2.

MD4 ва MD5 – Р.Райвест томонидан ишлаб чиқилган ахборот дайджестини ҳисобловчи алгоритм. Уларнинг ҳар бири 128 битли хэш-кодни тузади. MD2 алгоритми энг секин ишласа, MD4 алгоритми тезкор ишлайди. MD5 алгоритми MD4 алгоритмининг модификацияси бўлиб, MD4 алгоритмида хавфсизликнинг оширилиши эвазига тезликдан ютқазилган. SHA(SecureHashAlgorithm) – 160 битли *хэш-код*ни тузувчи ахборот дайджестини ҳисобловчи алгоритм. Бу алгоритм MD4 ва MD5 алгоритмларига нисбатан ишончлироқ.

SHA-1 хэшлаш функцияси алгоритми. Кафолатланган бардошлиликка эга бўлган хэшлаш алгоритми SHA (SecureHashAlgorithm) АҚШнинг стандартлар ва технологиялар Миллий институти (NIST) томонидан ишлаб чиқилган бўлиб, 1992 йилда ахборотни қайта ишлаш федерал стандарти (PUBFIPS 180) кўринишида нашр қилинди. 1995 йилда бу стандарт қайтадан кўриб чиқилди ва SHA-1 деб номланди (PUB FIPS 180). SHA алгоритми MD4 алгоритмига асосланади ва унинг тузилиши MD4 алгоритмининг тузилишига жуда яқин. Бу алгоритм электрон рақамли имзони шакллантириш бўйича DSS стандартида қўллаш учун мўлжалланган. Бу алгоритмда кирувчи маълумот узунлиги 2^{64} битдан кичик, хэш қиймат узунлиги 160 бит бўлади. Киритилаётган маълумот 512 битлик блокларга ажратилиб қайта ишланади.

Хэш қийматни ҳисоблаш жараёни қуйидагича босқичлардан иборат:

1-босқич: Тўлдириш битларини қўшиш.

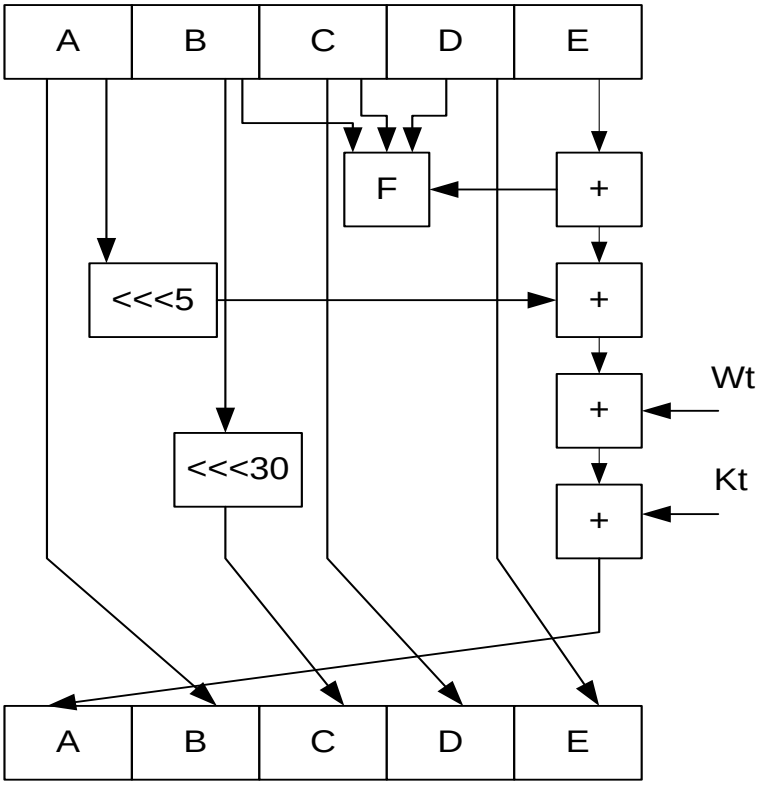
2-босқич: Маълумотнинг узунлигини қўшиш.

3-босқич: Хэш қиймат учун буфер инициализация қилиш.

4-босқич: Маълумотни 512 битлик блокларга ажратиб қайта ишлаш.

5-босқич: Натижа.

SHA-1 алгоритмидаги бир итерация схемаси 5.17-расмда келтирилган.

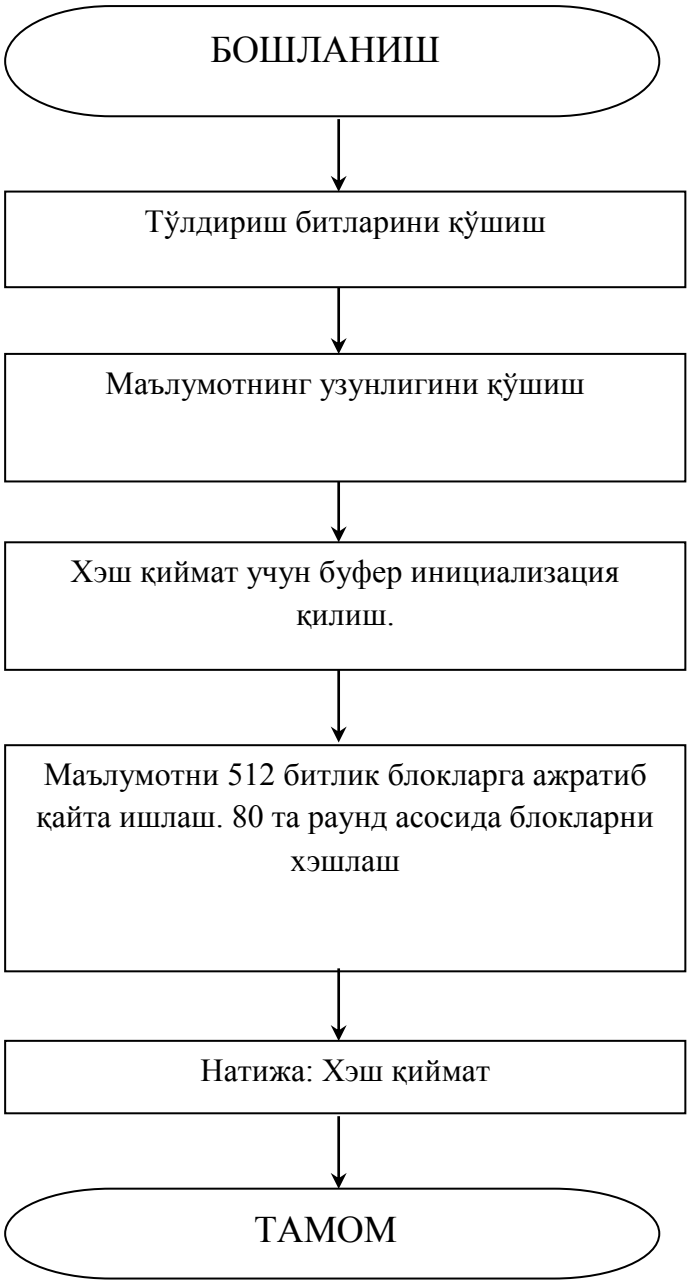


5.17-расм. SHA-1 алгоритмида бир итерациясининг схемаси.

SHA1 хэшлаш функцияси алгоритмининг ишлаш блок схемаси 5.18-расмда келтирилган.

ГОСТ Р34.11-94 хэшлаш функцияси алгоритми. Россиянинг ГОСТ Р 34.11-94 хэш функция стандарти ахборотни криптографик усулда муҳофаза қилиш учун, хусусан ГОСТ Р 34.11-94 ва ГОСТ Р 34.10-2001 электрон рақамли имзо алгоритмларида ишлатиш учун мўлжалланган. Хэш функциянинг қийматини ҳисоблаш жараёнида ГОСТ 28147-89 шифрлаш стандартидан фойдаланилади.

ГОСТ Р 34.11-94 хэш функция стандартида чиқиш узунлиги белгиланган қадамли хэшлаш функциясидан фойдаланувчи кетма-кет хэшлаш усулидан фойдаланилади. Хэш-функция аргументининг узунлиги 256 бит бўлган функция бўлиб, хэш қиймат узунлиги 256 бит бўлади.



5.18-расм. SHA1 алгоритми ишлаш блок схемаси

Хэшланадиган маълумот узунлиги ихтиёрий бўлиб, маълумот узунлиги 256 бит бўлган блокларга ажратилади. Охирги блок узунлиги 256 битдан кичик бўлса, 256 битгача ноль билан тўлдирилади.ундан ташқари, бу блокларнинг охирига маълумот узунлигининг кодини билдирувчи ва назорат йиғиндисини билдирувчи яна иккита 256 битлик блокларга қўшилади. Маълумот узунлигининг кодини блок хэшланадиган маълумотнинг бит узунлиги $mod2^{256}$бўйича ҳисобланиб (бу процедура MD кучайтириш

дейилади) ҳосил қилинади. Назорат йиғиндисининг кодини билдирувчи блок эса, охирги тўлиқмас блок ноль билан тўлдирилгандан кейин барча блокларнинг йиғиндиси $\mathrm{mod}2^{256}$ бўйича ҳисобланиб ҳосил қилинади.

ГОСТ Р 34.11-94 хэшлаш функциясини ҳисоблашда қуйидаги белгилашлардан фойдаланилади:

M – хэшланиши керак бўлган маълумот;

h – M маълумотни $h(M) \in V_{256}(2)$га акслантирувчи хэш-функция, бу ерда $V_{256}(2)$ – узунлиги 256 бит бўлган барча иккилик сўзлар тўплами,

$E_K(A)$ – A ни ГОСТ 28147-89 шифрлаш алгоритмидан фойдаланиб K калитда шифрлаш натижаси,

$H \in V_{256}(2)$–берилган бошланғич вектор.

ГОСТ Р 34.11-94 хэшлаш функциясини ҳисоблаш учун қуйидагилар зарур:

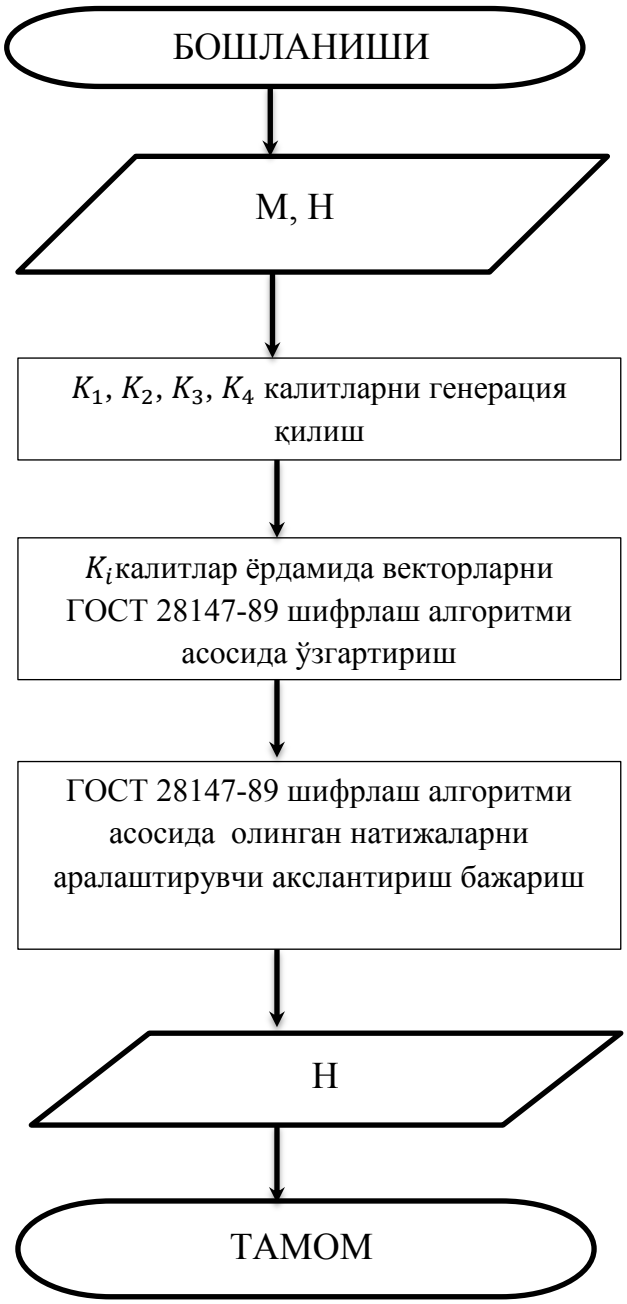
- қадамли хэшлаш функцияси $\chi: V_{256}(2) \times V_{256}(2) \to V_{256}(2)$ни ҳисоблаш алгоритми;

- хэш қийматни итератив ҳисоблаш жараёни.

Қадамли хэшлаш функцияси уч босқичда ҳисобланади. Биринчи босқичда узунликлари 256 бит бўлган тўртта K_1, K_2, K_3, K_4калит генерация қилинади. Иккинчи босқичда бошланғич H вектор ҳар бирининг узунлиги 64 бит бўлган тўртта блокка ажратилади ва бу блоклар мос K_1, K_2, K_3, K_4 калитлар билан ГОСТ 28147-89 алгоритми ёрдамида шифрланади. Учинчи босқичда шифрлаш натижасини аралаштирувчи акслантириш бажарилади.

Қадамли хэшлаш функциясини ҳисоблаш алгоритмининг блок-схемаси 5.19-расмда келтирилган.

Ҳозирги кунда ГОСТ Р 34.11-94 хэшлаш функциясининг ўрнига ГОСТ Р 34-10-2012 электрон рақамли имзони шакллантириш ва текшириш бўйича стандарти талабларидан келиб чиққан ҳолда ГОСТ Р 34.11-2012 хэшлаш функцияси амалда қўлланилиб келинмоқда. Ушбу алгоритмда иккита хэшлаш функциясидан фойдаланган ҳолда 256 ва 512 битли хэш қийматларни ҳисоблашни кўзда тутади.



5.19-расм. Хэш қийматни ҳисоблаш алгоритмининг блок-схемаси

“O‘z DSt 1106:2009” Ўзбекистон давлат стандарти ҳисобланади. Ушбу стандартда хэш-функцияни хисоблашнинг икки хил алгоритми келтирилган.

1-алгоритмда модуль арифметикасининг бир томонлама функцияси қўлланилади, у бўйича ҳисоблашлар даражага кўтариш амалларидаги каби айнан ўша меҳнат сарфи даражасида осон амалга оширилади, функцияни инвертирлаш (тескарилаш) эса, ***(A, B)*** номаълум параметрда дискрет логарифм муаммосини ечиш жараёнига нисбатан кўпроқ ҳисоблашлар сарфи

ва вақтни талаб қилади. Кўпайтириш, даражага кўтариш ва тескарилаш каби асосий амаллар янги бир томонлама функцияда параметр билан кўпайтириш, даражага кўтариш ва тескарилаш деб номланган. Даражага кўтаришнинг бир томонлама функцияси ушбу бир томонлама функциянинг хусусий ҳолидир. Хэшлаш функциясида параметр (коэффициент) сифатида натурал сонлар учлигидан ***(A, B, R)*** фойдаланилади.

Ушбу алгоритмда кириш блокининг узунлиги ***128*** ёки ***256*** битга каррали ҳамда чиқиш блоки ва хэшлаш калитининг узунлиги ***128*** ёки ***256*** бит. Ҳар бир блок учун криптографик алмаштиришлар ***10*** та босқичда амалга оширилади.Хэш-функцияси алгоритмининг маълумотларини хэшлаш процедурасида хэшлаш калити ***k*** ва хэшлашнинг оралиқ натижаси асосида шаклланган босқич калитлари k_eдан фойдаланилади.

Хэш қийматни хисоблаш ***holat*** массиви устида криптографик ўзгартиришларни бажариш билан амалга оширилади. ***holat*** массиви тўртта сатр (қатор) ва саккизта устунда жойлашган ярим байтлардан (байтлардан) иборат, бунда ҳар бир сатр *32 (64)*битдан иборат.

Хэш қийматни хисоблашда дастлаб кирувчи маълумот ***128*** ёки ***256*** бит узунликдаги ***b*** таблокларга бўлинади, тўлмай қолган блок ***0*** лар билан тўлдирилади. ***Holat*** массиви дастлабки блок билан; асосий қисмнинг умумий узунлиги 2^{256} модуль бўйичабитларда аниқланади, бу қисм **256**бит узунликдаги ***uzunlik*** блокидан иборат; кейин 2^{256} модуль бўйича асосий қисм блоклари қийматларининг суммаси ҳисобланади, у ***256*** бит узунликдаги *назорат суммасининг* блокидан (***NY)*** иборат; асосий қисм, ***uzunlik*** блоки ва ***b+2*** блоклардаги ярим байт (байт) даражасидаги икки ўлчамли элементлар шаклидаги ***NY*** блок хэшлаш функцияси кириш маълумотларидан иборат. Дастлабки босқич ***128 (256)*** бит узунликдаги ***k*** хэшлаш калитининг нусхасини икки ўлчамли k_e массивга кўчириш билан тугалланади.

Кириш маълумотларининг ҳар бир блокларига нисбатан хэшлаш жараёнлари иккита блок: ***holat*** ҳамда ***holatn*** устида ***Qo'sh (holat, holatn)***, ***BaytZichlash(holat, holatn)*** ўзгартиришлар жуфтининг занжирини

бажаришдан бошланади ва 10 та босқич давомида ***holat*** жорий хэш-қийматини шакллантириш билан тугалланади. Хэшлаш жараёнларининг энг аввалида дастлабки хэш-қиймат сифатида 1-блокдан ***holat*** блоки сифатида, 2-блокдан эса - ***holatn*** блоки сифатида фойдаланилади; агар кириш маълумотлари фақат битта блокдан иборат бўлса, 2-блок сифатида ***uzunlik*** блокидан фойдаланилади[10].

Сўнгра ***holatn*** массивига навбатдаги блокдан нусха кўчирилади ва ***Qo'sh(holat, holatn)***, ***BaytZichlash(holat, holatn)*** ўзгартиришлар жуфтлиги натижаси, жорий хэш-қиймат ***holat*** ва ***holatn*** устида хэшлаш процедурасининг 10босқичи амалга оширилади ва ҳ.к. ***holatn*** массивига нусха олинадиган охирги блок сифатида ***NY*** блоки ҳисобланади. Шундай қилиб, хэшлаш босқичларининг умумий сони ***(b+2)10*** га тенг бўлади.

Хэшлаш процедурасининг ҳар бир босқичи (раунди) дастлабки ***Qo'sh (holat, holatn)***, ***BaytZichlash (holat, holatn)*** ўзгартиришлар жуфтлиги билан бирга блокларга нисбатан циклик тартибда амалга оширилувчи ***Aralash(holat,k_e), Qo'sh(holat,holatn), SurHolat(holat)), SurKalit(k_e), TuzilmaKalit(k_e, k)*** ўзгартиришлардан иборат.

2-алгоритм ГОСТ Р 34.11-94 каби амалга оширилади[10].

Назорат саволлари:

1. Хэшлаш функциясининг ишлаш схемасини тушунтириб беринг.
2. SHA-1 хэшлаш функцияси алгоритмини тушунтириб беринг.
3. ГОСТ Р 34.11 Россиянинг хэшлаш функцияси алгоритми ишлаш схемасини тавсифлаб беринг.
4. "O'z DSt 1106:2009" Ўзбекистон Республикаси давлат стандарти ўз ичига оладиган хэшлаш функциясининг иккита алгоритмини ёритиб беринг.

5.5. Электрон рақамли имзо

Электрон хужжатларни тармоқ орқали алмашишда уларни ишлаш ва

сақлаш харажатлари камаяди, қидириш тезлашади.Аммо, электрон хужжат муаллифини ва хужжатнинг ўзини аутентификациялаш, яъни муаллифнинг хақиқийлигини ва олинган электрон хужжатда ўзгаришларнинг йўқлигини аниқлаш муаммоси пайдо бўлади.

Электрон хужжатларни ауентификациялашдан мақсад уларни мумкин бўлган жинояткорона харакатлардан ҳимоялашдир. Бундай харакатларга қуйидагилар киради:

- *фаол ушлаб қолиш* - тармоққа уланган бузғунчи хужжатларни (файлларни) ушлаб қолади ва ўзгартиради.

- *маскарад* – абонент *C* хужжатларни абонент *B* га абонент *A* номидан юборади;

- *ренегатлик* – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;

- *алмаштириш* – абонент *B* хужжатни ўзгартиради, ёки янгисини шакллантиради ва уни абонент *A* дан олганман дейди;

- *такрорлаш* – абонент *A* абонент *B* га юборган хужжатни абонент *C* такрорлайди.

Жинояткорона харакатларнинг бу турлари ўз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат структураларига, давлат корхона ва ташкилотларига хусусий шахсларга анча-мунча зарар етказиши мумкин.

Электрон рақамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хақиқийлигини текшириш муаммосини самарали ҳал этишга имкон беради.

Электрон рақамли имзо телекоммуникация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қуйидаги афзалликларга эга:

- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;

- бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;

- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон рақамли имзо-имзо чекилувчи матн билан бирга узатилувчи қўшимча рақамли хабарнинг нисбатан катта бўлмаган сонидир.

Электрон рақамли имзо асимметрик шифрларнинг қайтарувчанлигига ҳамда хабар таркиби, имзонинг ўзи ва калитлар жуфтининг ўзаро боғлиқлигига асосланади. Бу элементларнинг хатто бирининг ўзгариши рақамли имзонинг ҳақиқийлигини тасдиқлашга имкон бермайди. Электрон рақамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш–функциялари ёрдамида амалга оширилади.

Электрон рақамли имзо тизимининг қўлланишида бир- бирига имзо чекилган электрон хужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз қилинади. Ҳар бир абонент учун жуфт – маҳфий ва очиқ калит генерацияланади. Маҳфий калит абонентда сир сақланади ва ундан абонент электрон рақамли имзони шакллантиришда фойдаланади.

Очиқ калит бошқа барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон хужжатни қабул қилувчи электрон рақамли имзони текширишда фойдаланади.

Электрон рақамли имзо тизими иккита асосий муолажани амалга оширади:

- рақамли имзони шакллантириш муолажаси;

- рақамли имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очиқ калитидан фойдаланилади.

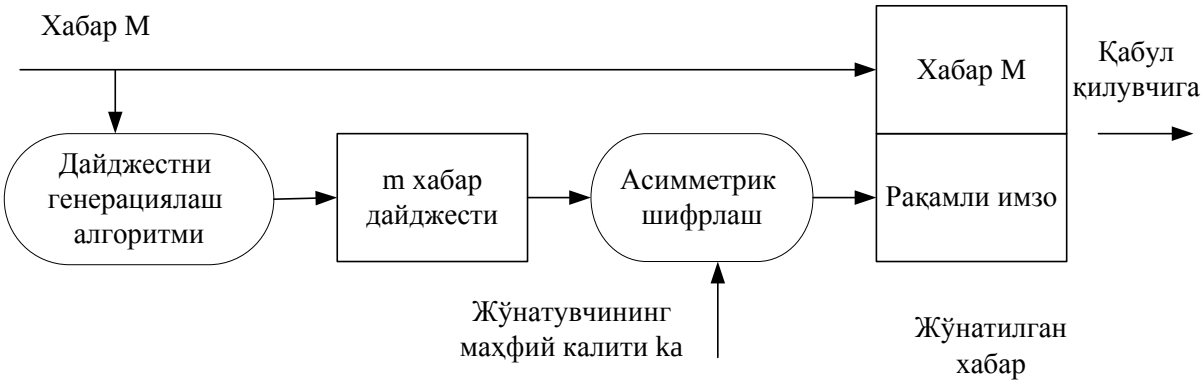
Рақамли имзони шакллантириш муолажаси.

Ушбу муолажани тайёрлаш босқичида хабар жўнатувчи абонент A иккита калитни генерациялайди: маҳфий калит $k_{A.}$ ва очиқ калит K_A. Очиқ калит K_A унинг жуфти бўлган махфий калити $k_{A.}$ дан ҳисоблаш орқали

олинади. Очиқ калит K_A тармоқнинг бошқа абонентларига имзони текширишда фойдаланиш учун тарқатилади.

Рақамли имзони шакллантириш учун жўнатувчи *A* аввало имзо чекилувчи матн *M* нинг хеш функцияси *L(M)*қийматини ҳисоблайди (5.20-расм).

Хеш-функция имзо чекилувчи дастлабки матн *M*ни дайджест *m*га зичлаштиришга хизмат қилади. Дайджест *M*–бутун матн *M*ни характерловчи битларнинг белгиланган катта бўлмаган сонидан иборат нисбатан қисқа сондир. Сўнгра жўнатувчи *A* ўзининг маҳфий калити k_Aбилан дайджест *m*ни шифрлайди. Натижада олинган сонлар жуфти берилган *M* матн учун рақамли имзо ҳисобланади. Хабар *M* рақамли имзо билан биргаликда қабул қилувчининг адресига юборилади.

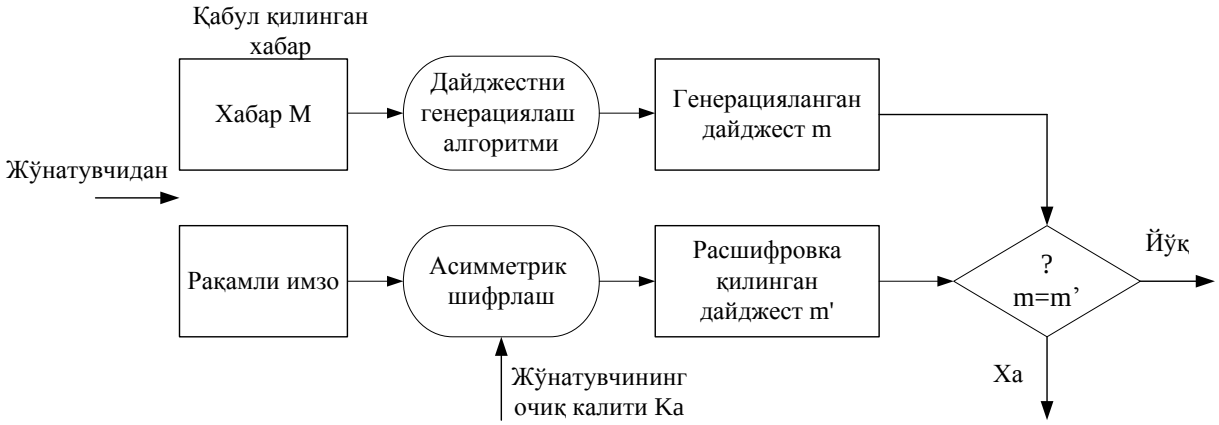


5.20-расм. Электрон рақамли имзони шакллантириш схемаси.

Рақамли имзони текшириш муолажаси. Тармоқ абонентлари олинган хабар *M*нинг рақамли имзосини ушбу хабарни жўнатувчининг очик калити K_A ёрдамида текширишлари мумкин (5.21-расм).

Электрон рақамли имзони текширишда хабар *M*ни қабул қилувчи *B*қабул қилинган дайджестни жўнатувчининг очиқ калити K_A ёрдамида расшифровка қилади. Ундан ташқари, қабул қилувчини ўзи хеш-функция *h(M)* ёрдамида қабул қилинган хабар *M*нинг дайджести *m*ни ҳисоблайди ва уни расшифровка қилингани билан таққослайди. Агар иккала дайджест *m* ва *m'* мос келса рақамли имзо ҳақиқий ҳисобланади. Акс ҳолда имзо

қалбакилаштирилган, ёки ахборот мазмуни ўзгартирилган бўлади.



5.21-расм. Электрон рақамли имзони текшириш схемаси

Электрон рақамли имзо тизимининг принципиал жиҳати – фойдаланувчининг электрон рақамли имзосини унинг имзо чекишдаги махфий калитини билмасдан қалбакилаштиришнинг мумкин эмаслигидир. Шунинг учун имзо чекишдаги махфий калитни рухсатсиз фойдаланишдан химоялаш зарур. Электрон рақамли имзонинг махфий калитини, симметрик шифрлаш калитига ўхшаб, шахсий калит элитувчисида, ҳимояланган ҳолда сақлаш тавфсия этилади.

Электрон рақамли имзо имзо чекилувчи хужжат ва махфий калит орқали аниқланувчи ноёб сондир. Имзо чекилувчи хужжат сифатида ҳар қандай файл ишлатилиши мумкин. Имзо чекилган файл имзо чекилмаганига бир ёки бир нечта электрон имзо қўшилиши орқали яратилади.

Имзо чекилувчи файлга жойлаштирилувчи электрон рақамли имзо имзо чекилган хужжат муаллифини идентификацияловчи қўшимча ахборотга эга. Бу ахборот хужжатга электрон рақамли имзо ҳисобланмасидан олдин қўшилади. Ҳар бир имзо қуйидаги ахборотни ўз ичига олади:

- имзо чекилган сана;

- ушбу имзо калити таъсирининг тугаши муддати;

- файлга имзо чекувчи шахс хусусидаги ахборот (Ф.И.Ш., мансаби, иш жойи);

- имзо чекувчининг индентификатори (очиқ калит номи);

- рақамли имзонинг ўзи.

Асимметрик шифрлашга ўхшаш, электрон рақамли имзони текшириш учун ишлатиладиган очиқ калитнинг алмаштирилишига йўл қўймаслик лозим. Фараз қилайлик, нияти бузуқ одам *n* абонент *B* компьютерида сақланаётган очиқ калитлардан, хусусан, абонент *A* нинг очиқ калити K_Aдан фойдалана олади. Унда у қуйидаги харакатларини амалга ошириши мумкин:

- очиқ калит K_Aсақланаётган файлдан абонент *A* хусусидаги инденцификация ахборотини ўқиши;

- ичига абонент *A* хусусидаги индентификация ахборотини ёзган ҳолда шахсий жуфт калитлари k_nва K_n ни генерациялаши;

- абонент *B*да сақланаётган очиқ калит K_Aни ўзининг очиқ калити K_n билан алмаштириши.

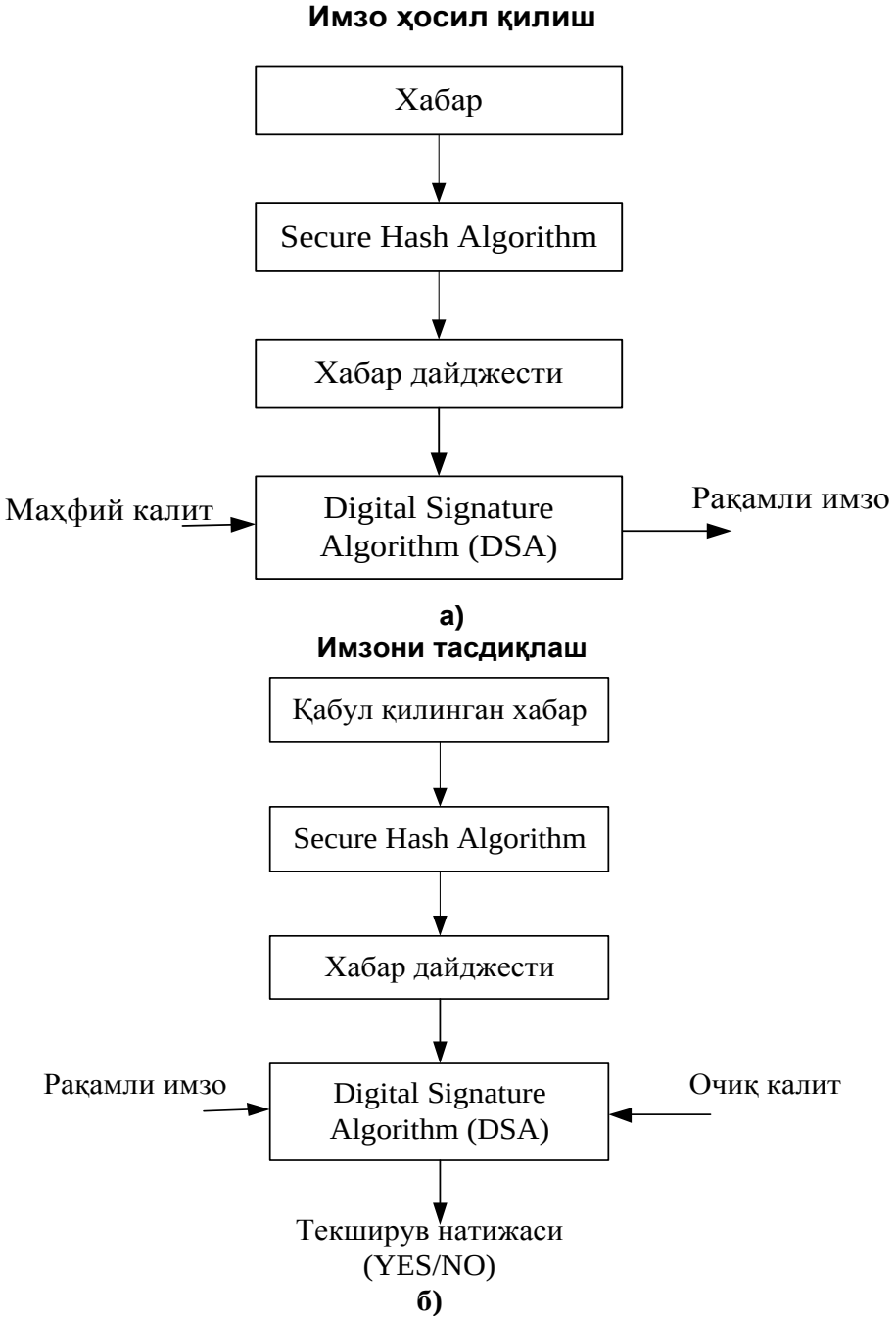
Сўнгра нияти бузуқ одам *n* абонент *B* га хужжатларни ўзининг махфий калити k_n ёрдамида имзо чекиб жўнатиши мумкин. Бу хужжатлар имзосини текширишда абонент *B* абонент *A* имзо чеккан хужжатларни ва уларнинг электрон рақамли имзоларини тўғри ва хеч ким томонидан модификацияланмаган деб ҳисоблайди. Абонент А билан муносабатларини бевосита ойдинлаштирилишигача В абонентда олинган хужжатларнинг хақиқийлигига шубҳа туғилмайди.

Электрон рақамли имзонинг қатор алгоритмлари ишлаб чиқилган. 1977 йилда АҚШ да яратилган RSA тизими биринчи ва дунёда машҳур электрон рақамли имзо тизими ҳисобланади ва юқорида келтирилган принципларни амалга оширади. Аммо рақамли имзо алгоритми RSA жиддий камчиликка эга. У нияти бузуқ одамга махфий калитни билмасдан, хешлаш натижасини имзо чекиб бўлинган хужжатларнинг хешлаш натижаларини кўпайтириш оркали ҳисоблаш мумкин бўлган хужжатлар имзосини шакллантиришга имкон беради.

АҚШнинг DSS стандарти. 1991 йилда NIST (National Institute of Standard and Technology) томонидан DSA (Digital Signature Algorithm) алгоритмига асосланган DSS (Digital Signature Standard) ЭРИ стандартининг

лойиҳаси муҳокамага қуйилди. Ушбу алгоритм бардошлилиги етарли катта туб характеристикага эга бўлган чекли майдонда дискрет логарифмлаш масаласининг мураккаблигига асосланган.

Ушбу электрон рақамли имзони шакллантириш ва текшириш стандартида 512 ёки 1024 бит узунликдаги калитлар қўлланилади ва электрон рақамли имзонинг 160 битли 2 та сондан иборат. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари 5.22-расмда келтирилган.



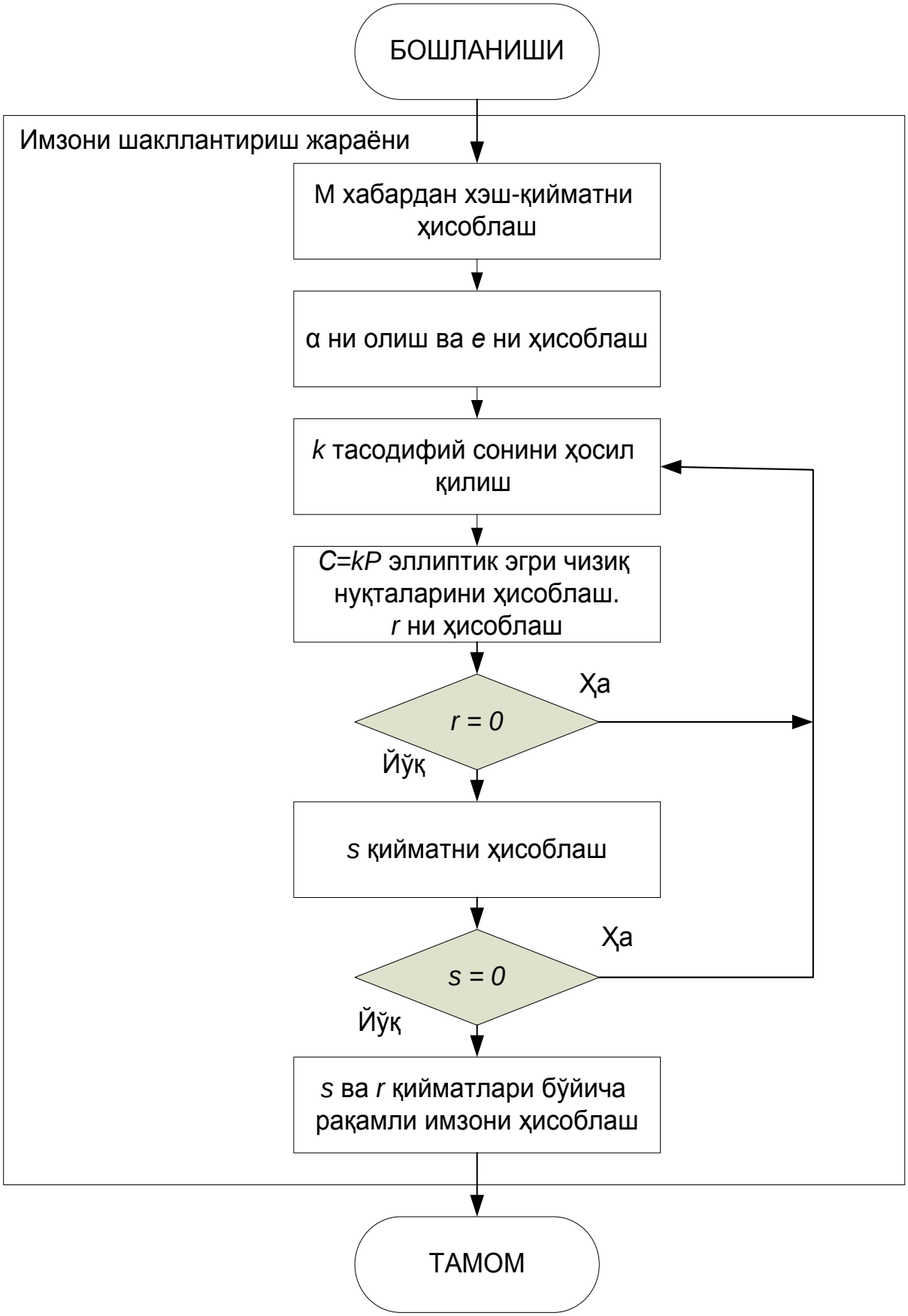
5.22-расм. Электрон рақамли имзони шакллантириш (а) ва текшириш (б) жараёнлари.

Эллиптик эгри чизиқларга асосланган рақамли имзо алгоритми ECDSA (Elliptic Curve Digital Signature Algorithm) — DSA алгоритмга тузилиш жиҳатидан аналог ҳисобланади, лекин ҳисоблашлар бутун сонлар майдонида эмас балки эллиптик эгри чизиқлар нуқталари гуруҳида бажарилади ва унинг криптобардошлилиги эллиптик эгри чизиқлар нуқталари гуруҳида дикрет логарифмлаш муаммолариги асосланади. ECDSA алгоритми 1999 йилда ANSI стандарти сифатида, 2000 йилда эса IEEE ва NIST стандартлари сифатида қабул қилинган.

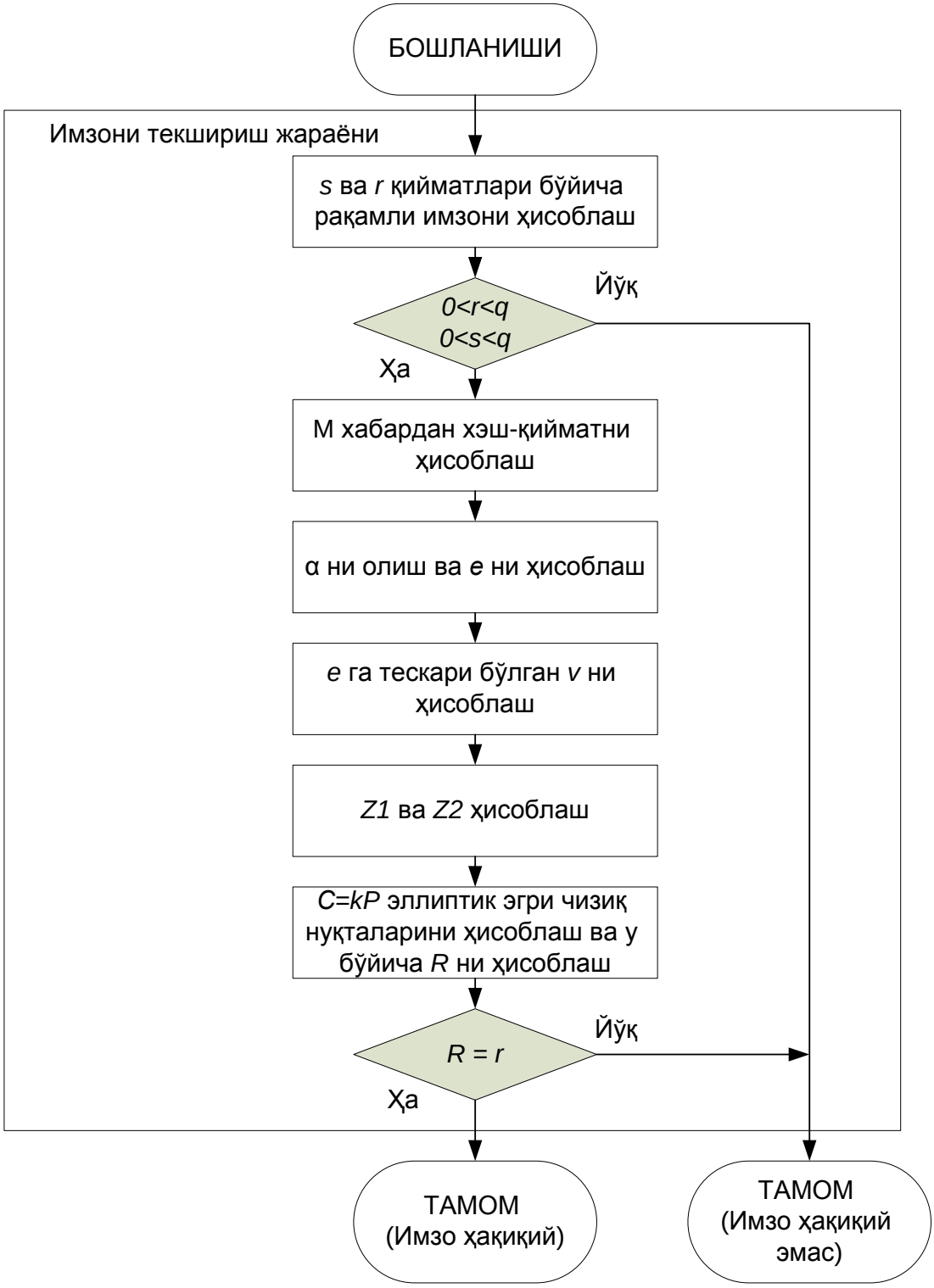
ГОСТ Р 34.10 электрон рақамли имзони шакллантириш ва текшириш алгоритми ГОСТ Р 34.10-94 рақамли стандарт ҳисобланиб, DSA алгоритмига ўхшаш ишлайди. Лекин ундан кейин ГОСТ 34.10-2001 стандарти ишлаб чиқилиб амалда 2011 йилгача қўлланилиб келинган. 2012 йилда ГОСТ 34.10-2012 стандарти қабул қилинган ва ГОСТ 34.10-2001 билан иккаласи эллиптик эгри чизиқлар муаммоларига асосланган ҳисобланади.

Ушбу стандартда электрон рачамли имзони шакллантириш аввалги алгоритмлардаги каби бўлиб хэшлаш функцияси сифатида ГОСТ Р 34.11-2012 алгоритми қўлланилади. Ушбу алгоритмда электрон рақамли имзони шакллантириш жараёни ва уни текшириш жараёни қуйидаги расмда келтирилган (5.23 ва 5.24-расм).

O’z DSt 1092-2009 алгоритми. Ушбу алгоритм 2005 йилда қабул қилинган 1092-2005 рақамли алгоритмнинг давомчиси бўлиб 2009 йилда ишлаб чиқилган ва электрон рақамли имзони (ЭРИ) шакллантириш ва уни ҳақиқийлигини текшириш учун мўлжалланган. 1092-2009 миллий стандарти ЭРИни шакллантириш ва ҳақиқийлигини текшириш учун иккита алгоритмни тавсифлаб беради. Биринчи алгоритм параметрлар даражаси муаммосининг қийинлигига асосланган бўлса, иккинчи алгоритм эллиптик эгри чизиқлар гуруҳи амалларини қўллаш билан боғлиқ муаммоларга асосланади. Бу ҳар иккала муаммо ҳам ҳозирги кунда электрон рақамли имзони шакллантиришда кенг қўлланилиб келинаётганлиги билан ажралиб туради.



5.23-расм. Электрон рақамли имзони шакллантириш жараёни.



5.24-расм. Электрон рақамли имзони текшириш жараёни

Электрон рақамли имзони шакллантириш. M хабар остига қўйиладиган электрон рақамли имзони олиш учун алгоритм бўйича қуйидаги амалларни (қадамларни) бажариш зарур:

1-қадам: хабарнинг хэш-функциясини ҳисобланади: m=H(M);

2-қадам: $e \equiv m \pmod{t}$ ни ҳисобланади. Агар $e=0$ бўлса, у ҳолда $e=1$ ни аниқланади;

3-қадам: ушбу $0<k<t$ тенгсизликни қаноатлантирувчи тасодифий (псевдотасодифий) k бутун сонини генерация қилинади;

4-қадам: эллиптик эгри чизиқнинг $C=[k]N$ нуқтасини ҳисобланади ва $r = x_c(mod\ t)$ни аниқланади, бу ерда $x_c - C$ нуқтанинг x координатаси. Агар $r = 0$ бўлса, у ҳолда 3-қадамга қайтилади;

5-қадам: $s \equiv (rd+ke) \pmod{t}$ ифоданинг қийматини ҳисобланади. Агар $s=0$ бўлса, 3-қадамга қайтилади;

6-қадам: r ва s ларни ЭРИ сифатида чиқишга берилади.

Ушбу жараён учун дастлабки (киришдаги) маълумотлар М хабар ва ЭРИнинг ёпиқ калити d, чиқиш натижаси бўлиб эса, (r, s) электрон рақамли имзо ҳисобланади.

Электрон рақамли имзонинг ҳақиқийлигини тасдиқлаш. Олинган М хабар остига қўйилган ЭРИ ҳақиқийлигини тасдиқлаш учун алгоритм бўйича қуйидаги амалларни (қадамларни) бажариш зарур:

1-қадам: агар $0 < r < t,\ 0<s<t$ тенгсизликлар бажарилса, навбатдаги қадамга ўтилади, акс ҳолда, “имзо ҳақиқий эмас” деб қабул қилинади;

2-қадам: M хабар бўйича хэш-функцияни ҳисобланади: m=H(M);

3-қадам: $e \equiv m \pmod{t}$ ни ҳисобланг. Агар $e=0$ бўлса, у ҳолда $e=1$ ни аниқланади;

4-қадам: $v \equiv e^{-1} \pmod{t}$ ифоданинг қиймати ҳисобланади;

5-қадам: ушбу $z_1 \equiv sv(mod\ t),\ z_2 \equiv -rv(mod\ t)$ ифодалар қийматлари ҳисобланади;

6-қадам: эллиптик эгри чизиқнинг $C = [z_1]N" + "[z_2]T$ нуқтасини ҳисобланади ва $R \equiv x_c(mod\ t)$ни аниқланг, бу ерда $x_c - C$ нуқтанинг х координатаси.

7-қадам: агар $R=r$ тенглик бажарилса, у ҳолда “имзо ҳақиқий”, акс ҳолда “имзо ҳақиқий эмас” деб қабул қилинади.

Ушбу жараён учун дастлабки (киришдаги) маълумотлар бўлиб,

имзоланган M хабар, (*r, s*) электрон рақамли имзо ва ЭРИ очиқ калити, чиқиш натижаси бўлиб эса, мазкур ЭРИ ҳақиқийлиги ёки ҳақиқий эмаслиги ҳақидаги ахборот ҳисобланади.

Назорат саволлари:

1. Электрон рақамли имзони шакллантириш схемасини тавсифлаб беринг.
2. Электрон рақамли имзони текшириш жараёнининг схемасини тушунтириб беринг.
3. АҚШнинг DSS стандартини ёритиб беринг.
4. ГОСТ Р 34.10 Россиянинг стандартини тавсифлаб беринг.
5. O’z DSt 1092-2009 алгоритми асосланган математик муаммоларни тушунтириб беринг.

5.6. Стеганография усуллари

Стеганография – сўзи Юнон тилида махфий белгилар билан ёзилган (steganos –сир, graphy - ёзув) маъносини билдиради, тарихи эса минг йилларни ўз ичига олади. Ахборотни стеганографик ҳимоялашни турли техникавий, кимёвий, физикавий ва психологик усуллар ёрдамида амалга ошириш мумкин.

Стеганография криптография ўрнини босмайди, балки уни тўлдиради. Стеганография усуллари ёрдамида хабарни бекитиш хабар узатилиши фактини аниқлаш эхтимоллигини анчагина пасайтиради. Агар ушбу хабар шифрланган бўлса у яна бир, қўшимча ҳимояланиш сатхига эга бўлади. Стеганографик усулларидан ахборотни рухсатсиз фойдаланишдан ҳимоялашда, тармоқларни мониторинглашга ва тармоқ ресурсларини бошқаришга қаршилик кўрсатишда, рўйхатда кўрсатилмаган фойдаланувчилардан дастурий таъминотни ниқоблашда, баъзи интеллектуал мулкка эгалик хуқуқини ҳимоялашда ҳамда рақамли объектларни аутентификациялашда фойдаланилади.

Маълум стеганографик усулларини қуйидаги иккита гуруҳга ажратиш мумкин:

- моддий стеганографик усуллар;
- ахборот стеганографик усуллари.

Моддий стеганографик усуллар стеганографик контейнернинг (махфий ахборот ўрнатиладиган объектнинг) физикавий ёки кимёвий хусусиятлари асосида ахборотни бекитиш учун ишлатилади. Бундай хусусиятларга мисол тариқасида габарит ўлчамларини, контейнер рангини ёки маълум таъсир натижасида ўрнатилган ахборотнинг намоён бўлиш қобилиятини кўрсатиш мумкин.

Бундай стеганографик усулларнинг тадқиқи ва яратилиши ахборотнинг турли моддий элтувчилари хусусиятларини ва ахборотни ўрнатишнинг норасмий усулларини ўрганиш билан боғлиқ.

Моддий стеганографик усулларга кўринмайдиган сиёҳлар, микронуқталар ва ҳ. тааллуқли. Ҳозирда аудиотехника, видеотехника ва ҳисоблаш техникаси ахборотни элтувчи стандарт воситалар ҳисобланади.

Ахборот стеганографик усуллар маълумотларни контейнернинг ахборот билан тўлдирилиши хусусияти асосида бекитиш учун ишлатилади. Ушбу усуллар лингвистик ва рақамлиларга ажратилади.

Лингвистик стеганографик усулларда тил ёки харфларни, рақамларни ўз ичига олмайдиган (расмлар, объектларнинг ўзаро жойлашиши ва ҳ.)бошқа муҳит ортиқчалиги ишлатилади. Ушбу синфга махфий хабарни бекитиш учун зарур матнни генерациялаш усулини ҳамда сахифадаги қатор холатини ёки гапдаги сўз холатини ўзгаришига ва ҳ. асосланувчи усулларни киритиш мумкин.

Рақамли стеганографик усуллар бир томондан абсолют аниқликка мухтож бўлмаган файлларнинг вазифасини йўқотмаган ҳолда шаклини бир мунча ўзгартириш мумкинлигига, иккинчи томондан бундай файллардаги бир мунча ўзгаришларни фарқловчи махсус асбобларни йўқлигига ёки инсон сезги органларининг қобилиятсизлигига асосланган.

Рақамли стеганографик усуллар қуйидаги турларни ўз ичига олади:

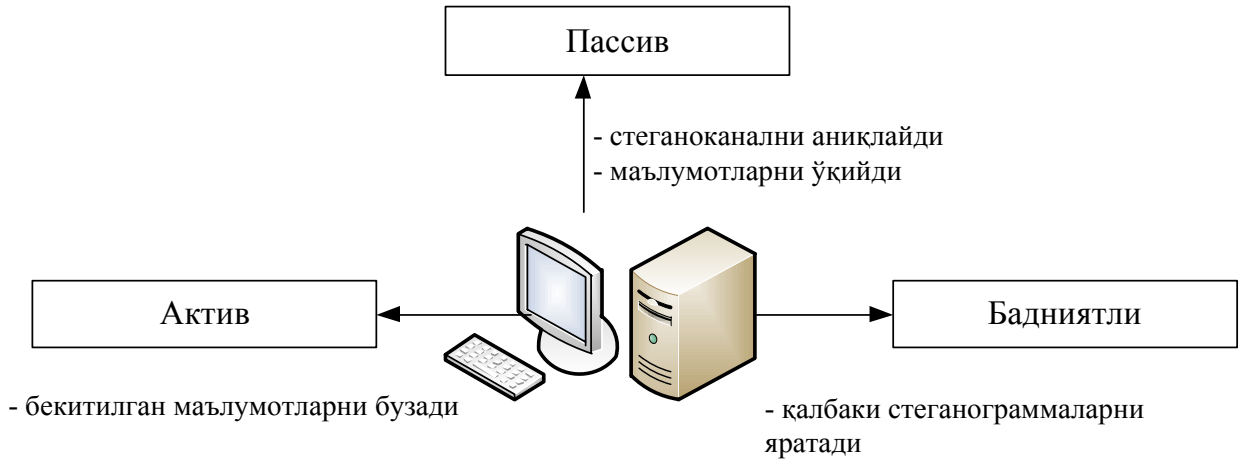
1. Контейнерни танлаш усули бўйича.
2. Ахборотдан фойдаланиш усули бўйича.
3. Контейнерни ташкил этиш усули бўйича.
4. Хабарни қайта тиклаш усули бўйича.
5. Контейнерни ишлаш усули бўйича.
6. Вазифаси бўйича.
7. Контейнер турига кўра.
8. Контейнерга ахборотни ўрнатиш усули бўйича.

Рақамли стеганографик усулларга мисол тариқасида LSB-усулни (Least Significant Bits – энг кичик қийматли бит)кўрсатиш мумкин. Ушбу усулга биноан файл-контейнердаги маълумотлар байтининг бир неча кичик битлари бекитилувчи хабар битлари билан алмаштирилади. Ушбу усул амалга оширилишининг соддалиги, демак, ушбу усулга асосланган дастурий махсулотнинг тезкорлиги, ҳамда яратилган стеганоканалнинг юқори ўтказиш қобилияти билан боғлиқ қатор афзалликларга эга. Аммо ушбу усулдан юқори стеганобардошлик талаб қилинмайдиган масалаларни ечишда фойдаланиш мумкин. Чунки LSB – усул нияти бузуқнинг актив хужумларига бардош бера олмайди.

Хабарни файл - контейнернинг *спектрал сохасида бекитувчи усуллар* стеганобардош усуллар ҳисобланади. Рақамли стеганографиянинг спектрал усуллари хилма-хил, баъзилари эса LSB-усул билан комбинациялаб ишлатилади.

Файл - контейнердаги маълумотларни частотали иофдалашда косинусни дискрет ўзгартириш, Фурьени дискрет ўзгартириш, вейвлет-ўзгартириш, Карунен-Лоев, Адамар ва Хаар ўзгартиришлар каби дискрет ортогонал ўзгартиришлардан фойдаланилади.

Стеганографик тизимларда ахборотни ҳимоялаш принциплари. Стеганографик тизимларни бузувчи пассив, актив ва бадниятли бўлиши мумкин (5.25- расм).



5.25-расм. Стеганографик тизимларни бузувчилар тури

Пассив бузувчи фақат стегоканал мавжудлиги фактини аниқлаши ва ўрнатилган маълумотларни ўқиши мумкин. Актив бузувчи нафақат бекитилган маълумотларни аниқлаши ва ўқиши, балки уларни тўлалигича ёки қисман бузиши мумкин. Бадниятли бузувчи энг хавфли ҳисобланади, чунки у нафақат стеганограммани бузади, балки қалбаки стеганограммани яратади.

Бузувчи (тахлилчи) у ёки бу тахдидни амалга ошириш учун қуйидаги хужумлардан фойдаланади:

- *маълум тўлдирилган контейнер асосидаги хужум.* Бузувчи бир ёки бир неча стеганограммага эга ва стеганоканал мавжудлиги фактини аниқлаш, ҳамда бошқа стеганограммаларни тахлиллаш имконияти учун очиқ матнни тиклаш ёки калитни аниқлаш топшириғини бажаради;

- *маълум ўрнатилган очиқ матн асосидаги хужум.* Бузувчи бир неча бекитилган очиқ матнлар ва мос стеганограмма намуналари асосида калитни олиш мақсадида мос тахлилни амалга оширади. Бундай хужумлар кўпинча интеллектуал мулкни ҳимоялаш тизимларига тааллуқли ҳисобланади;

- *танланган бекитилган очиқ матн асосидаги хужум.* Бунда тахлилчи (стеганотахлилчи) шахсий очиқ матнларини таклиф қилиш ва

стеганограммаларни тахлиллаш имкониятига эга бўлади;

- *танланган бекитилган очиқ матн асосидаги адаптив хужум.* Ушбу хужум олдинги хужумнинг хусусий холи ҳисобланади ва тахлилчининг аввалги стеганограммаларни тахлиллаш натижаларига боғлиқ холда тиқиштириш учун хабарни адаптив танлаш имконияти билан характерланади;

- *танланган тўлдирилган контейнер асосидаги хужум.* Стеганоаналитик стеганограмма намуналарини аниқлаш мақсадида ўзи танлаган очиқ матн учун стеганограммани яратиш имкониятига эга;

- *маълум бўш контейнер асосидаги хужум.* Бундай стеганотахлилчи маълум бўш контейнер билан назарда тутилган стеганограммани таққослаш билан стеганоканал мавжудлигини ҳар доим аниқлаши мумкин;

- *танланган бўш контейнер асосидаги хужум.* Бунда стеганотахлилчининг хабар жўнатувчисини тавсия этилган контейнердан фойдаланишга мажбур этиш имкониятига эга бўлиши шарт;

- *контейнернинг ёки унинг қисмининг маълум математик модели асосидаги хужум.* Бунда хужумчи ўрнатилган шубхали очиқ матннинг унга маълум моделдан фарқини аниқлашга уринади. Хабар жўнатувчиси ва хужумчи турли моделларга эга бўлиши мумкин. У ҳолда яхши модел эгаси ютиб чиқади.

Назорат саволлари:

1. Стеганографиянинг ахборотни криптографик ҳимоялаш соҳасидаги ўрни.
2. Моддий стеганографик усулларни тушунтириб беринг.
3. Ахборот стеганографик усулларнинг турларини тавсифлаб беринг.
4. Стеганографик тизимларда ахборотни ҳимоялаш принципини тушунтириб беринг.

5.7. Криптотахлил усуллари

Криптотахлил–шифрланган матндан махфий калитни (тиклаш алгоритмини ёки математик функцияни) билмай туриб очиқ матнни (фойдали хабарни) олиш ва тиклаш усуллари мажмуи.

Криптотахлилнинг муваффақиятли ўтказилиши натижасида очиқ матн олиниши ҳамда криптотизимнинг заиф жойлари аниқланиши мумкин.

Криптотахлилни амалга оширишга уриниш *фош этиш* деб юритилади. Очиқ матнни криптотахлил фош этишнинг қуйидаги хиллари мавжуд бўлиб, ҳар бирига нисбатан криптотахлилчининг ишлатилган шифрлаш алгоритми хусусида тўлиқ хабардорлиги назарда тутилади.

1. *Фақат шифрматн ёрдамида фош этиш*. Криптотахлилчи ихтиёрида бир неча хабарнинг битта шифрлаш алгоритми ёрдамида шифрланган шифрматнлари мавжуд. Криптотахлилчининг вазифаси иложи борича хабарларнинг катта сонининг очиқ матнини фош этиш ёки, яхшиси, хабарларни шифрлашда ишлатилган калитга (калитларга) эга бўлиш.

2. *Очиқ матн ёрдамида фош этиш*. Криптотахлилчининг ихтиёрида нафақат бир неча хабарнинг шифрматнлари, балки ушбу хабарларнинг очиқ матнлари мавжуд. Унинг вазифаси хабарларни шифрлашда ишлатилган калитга (калитларга) эга бўлиш.

3. *Танланган очиқ матн ёрдамида фош этиш*. Криптотахлилчи ихтиёрида нафақат шифрматнлар ва бир неча хабарнинг очиқ матнлари, балки шифрлаш учун очиқ матнни танлаш имконияти мавжуд. Унинг вазифаси хабарларни шифрлашда ишлатилган калитга (калитларга) ёки шу калит (калитлар) ёрдамида шифрланган янги хабарларни дешифрациялаш имконини берувчи алгоритмга эга бўлиш.

4. *Танланган очиқ матн ёрдамида адаптив фош этиш*. Бу танланган очиқ матн ёрдамида фош этишнинг хусусий холи. Криптотахлилчи нафақат шифрланган матнни танлаши, балки шифрлаш натижаси асосида ўзининг кейинги танлов режасини тузиши мумкин. Танланган очиқ матн

ёрдамида фош этишда криптотахлилчи шифрлаш учун очиқ матннинг фақат битта катта блокини танлаши мумкин бўлса, танланган очиқ матн ёрдамида адаптив фош этишда у очиқ матннинг кичик блокини, сўнгра биринчи танлаш натижасидан фойдаланиб кейинги блокни ва ҳ. танлаши мумкин.

5. *Танланган шифрматн ёрдамида фош этиш*. Криптотахлилчи дешифрациялаш учун турли шифрматнларни танлаши мумкин ва дешифрланган очиқ матнлардан фойдалана олади. Масалан, криптотахлилчи автоматик тарзда дешифрлашни бажарувчи “қора қути”дан фойдалана олади. Криптотахлилчининг вазифаси калитга эга бўлиш.

6. *Танланган калит ёрдамида фош этиш*. Бу хил фош этиш криптотахлилчи калитни танлаши мумкинлигини билдирмайди, балки унда турли калитлар орасидаги боғланиш хусусида қандайдир ахборот борлигини билдиради.

7. *Жиноий криптотахлил*. Криптотахлилчи калитга эга бўлиш мақсадида кимнидир қўрқитади, шантаж қилади, қийнайди. Порахўрлик баъзида калитни харид этиш ёрдамида фош этиш деб аталади. Бу каби қудратли фош этиш усуллари алгоритмни синдиришнинг энг яхши йўли ҳисобланади.

Турли алгоритмларга, уларни синдиришнинг қанчалик қийинлигига боғлиқ холда хавфсизликнинг турли сатхлари тақдим этилади. Алгоритмни қуйидаги холларда хавфсиз деб ҳисоблаш мумкин:

- алгоритмни синдириш қиймати шифрланган маълумотлар қийматидан катта бўлса;
- алгоритмни синдириш вақти шифрланган маълумотларнинг сир сақланиши шарт бўлган вақтидан катта бўлса;
- битта калит ёрдамида шифрланган маълумотлар хажми алгоритмни синдириш учун зарур маълумотлар хажмидан кам бўлса.

Фош этиш мураккаблигини қуйидаги коэффициентлар ёрдамида ўлчаш мумкин:

- маълумотлар мураккаблиги. Фош этиш амалининг кириш йўлида

фойдаланиладиган маълумотлар хажми;

- ишлаш мураккаблиги. Фош этиш учун керакли вақт. Кўпинча иш коэффициенти деб юритилади;
- хотирага талаблар. Фош этишга керакли хотира сиғими.

Фош этишнинг баъзи амаллари учун коэффициентларнинг ўзаро алоқаси жоиз ҳисобланади: тезроқ фош этишга хотирага талабларни кучайтириш эвазига эришиш мумкин.

Мураккаблик талайгина катталик орқали ифодаланади. Муайян алгоритм учун ишлаш мураккаблиги 2128ни ташкил этса, алгоритмни фош этиш учун 2128та амал керак бўлади (ушбу амаллар мураккаб ва давомли бўлиши мумкин). Масалан, агар ҳисоблаш қуввати секундига миллион амал бажарса ва масалани ечиш учун миллион параллел процессор ишлатилса, калитга эга бўлиш учун 1019 йилдан кўпроқ вақт талаб этилади. Бу коинот мавжуд бўлган вақтдан миллион марта кўпдир.

Фош этиш мураккаблиги ўзгармай қолганида компьютер қуввати ошиб боради. Охирги 50 йил мобайнида ҳисоблаш қуввати ниҳоятда ошиб кетди ва ушбу тенденция давом этишига шубҳа йуқ. Аксарият криптографик усуллар параллел компьютерлар учун яроқли ҳисобланади: масала миллиард кичик фрагментларга ажратиладики, уларни ечиш учун процессорлараро таъсирнинг кераги бўлмайди. Криптотизимларни синдиришга бардош қилиб лойиҳалашда ҳисоблаш воситалари келажагини ҳисобга олиш зарур.

Назорат саволлари:

1. Криптотаҳлил тушунчаси.
2. Крипотаҳлил усулларини санаб беринг.
3. Таҳлиллаш мураккаблигини қандай коэффициентлар ёрдамида ўлчаш мумкин.

VI боб. ИДЕНТИФИКАЦИЯ ВА АУТЕНТИФИКАЦИЯ

6.1. Идентификация ва аутентификация тушунчаси

Компьютер тизимида рўйхатга олинган ҳар бир субъект (фойдаланувчи ёки фойдаланувчи номидан ҳаракатланувчи жараён) билан уни бир маънода индентификацияловчи ахборот боғлиқ.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект *индентификатори* деб юритилади. Агар фойдаланувчи тармоқда рўйхатга олинган индентификаторга эга бўлса у легал (қонуний), акс ҳолда легал бўлмаган (ноқонуний) фойдаланувчи ҳисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) бўйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Аутентификация (Authentication) – маълум қилинган фойдаланувчи, жараён ёки қурилманинг ҳақиқий эканлигини текшириш муолажаси. Бу текшириш фойдаланувчи (жараён ёки қурилма) ҳақиқатан айнан ўзи эканлигига ишонч хосил қилишига имкон беради. Аутентификация ўтқазишда текширувчи тараф текширилувчи тарафнинг хақиқий эканлигига ишонч ҳосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол қатнашади.Одатда фойдаланувчи тизимга ўз хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлайди.

Идентификация ва аутентификация субъектларнинг (фойдаланувчиларнинг) ҳақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлиқ.

Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Авторизация (Authorization) – субектга тизимда маълум ваколат ва ресурсларни бериш муолажаси, яъни авторизация субъект ҳаракати доирасини ва у фойдаланадиган ресурсларни белгилайди. Агар тизим авторизацияланган шахсни авторизацияланмаган шахсдан ишончли ажрата олмаса бу тизимда ахборотнинг конфиденциаллиги ва яхлитлиги бузилиши мумкин. Аутентификация ва авторизация муолажалари билан фойдаланувчи ҳаракатини маъмурлаш муолажаси узвий боғланган.

Маъмурлаш (Accounting) – фойдаланувчининг тармоқдаги ҳаракатини, шу жумладан, унинг ресурслардан фойдаланишга уринишини қайд этиш. Ушбу ҳисобот ахбороти хавфсизлик нуқтаи назаридан тармоқдаги хавфсизлик ходисаларини ошкор қилиш, тахлиллаш ва уларга мос реакция кўрсатиш учун жуда муҳимдир.

Маълумотларни узатиш каналларини ҳимоялашда *субъектларнинг ўзаро аутентификацияси*, яъни алоқа каналлари орқали боғланадиган субъектлар хақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Хақиқийликнинг тасдиғи одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. “Улаш” атамаси орқали тармоқнинг иккита субъекти ўртасида мантиқий боғланиш тушунилади. Ушбу муолажанинг мақсади – улаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.

Ўзининг ҳақиқийлигини тасдиқлаш учун субъект тизимга турли ахборотни тақдим этади. Бундай ахборот тури “Аутентификация фактори” деб юритилади. Аутентификациялашнинг қуйидаги учта фактори фарқланади:

- *бирор нарсани билиш асосида.* Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) ҳамда “сўров жавоб” хилидаги протоколларда намойиш этилувчи махфий ва очиқ

калитларни кўрсатиш мумкин;

- *бирор нарсага эгалиги асосида.* Одатда булар магнит карталар, смарт- карталар, сертификатлар ва touch memory қурилмалари;

- *қандайдир дахлсиз характеристикалар асосида.* Ушбу фактор ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу факторда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Субъектнинг ҳақиқийлигини тасдиқлаш аутентификациянинг учта факторидан бири ёрдамида амалга оширилиши мумкин. Масалан, фойдаланувчини аутентификациялаш жараёнида ундан парол ёки бармоқ излари сўралиши мумкин. Аутентификация жараёнида фақат битта фактор ишлатилса, бундай аутентификация *бир факторли* деб юритилади.

Аутентификация жараёнида бир неча фактор ишлатилса, бундай аутентификация *кўп факторли* деб юритилади. Масалан, аутентификация жараёнида фойдаланувчи смарт-картадан ва қўшимча паролдан (ёки PIN-коддан) фойдаланиши лозим. Икки факторли ва уч факторли аутентификация тушунчалари ҳам ишлатилади.

NCSC-TG-017 хужжатда кўп факторли аутентификация турлари учун 1, 2 хилли, 2,3 хилли ва 1,2,3 хилли аутентификация атамалари киритилган. 1,2 хилли аутентификация (*бир икки хилли аутентификация* деб юритилади) масалан аутентификациянинг икки фактори ишлатади: биринчи (бир нарсани билиш асосида) ва иккинчи (бир нарсага эгалиги асосида).

1,2,3 хилли аутентификация (*бир икки уч хилли аутентификация* деб юритилади) аутентификациянинг учта факторининг комбинациясини ишлатади (бир нарса билиш асосида, бир нарсага эгалиги асосида ва қандайдир дахлсиз характеристикалар асосида).

Агар аутентификациялашда бир омилли аутентификация ишлатилса бундай аутентификация заиф ҳисобланади. Шу сабабли хавфсизликнинг

юқори даражасини таъминлаш учун кўп факторли аутентификациядан фойдаланиш мақсадга мувофиқ ҳисобланади.

Банкоматдан фойдаланувчини ҳақиқийлигини тасдиқлашда икки факторли аутентификация кенг тарқалган. Бу бир вақтда магнит хошияли карта ва PIN-код ишлатилади.

Парол – фойдаланувчи ҳамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул ҳисобланади. PIN – коднинг маҳфий қиймати фақат карта эгасига маълум бўлиши шарт.

Динамик – (бир марталик) парол- бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турувчи қиймат ишлатилади.

“Сўров-жавоб” тизими - тарафларнинг бири ноёб ва олдиндан билиб бўлмайдиган “сўров” қийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида ҳисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини тўғрилигини текшириши мумкин.

Сертификатлар ва рақамли имзолар - агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташқи ишончли ташкилот томонидан берилади. Internet доирасида очиқ калит сертификатларини тарқатиш учун очиқ калитларни бошқарувчи қатор тижорат инфраструктуралари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даража сертификатларини олишлари мумкин.

Аутентификация жарёнларини хавфсизликнинг таъминланиш даражаси бўйича ҳам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация

жараёнлари қуйидаги турларга бўлинади:

- пароллар ва рақамли сертификатлардан фойдаланувчи аутентификация;
- криптографик усуллар ва воситалар асосидаги қатьий аутентификация;
- нуллик билим билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуқтаи назаридан юқорида келтирилганларнинг ҳар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир қаторда таъкидлаш лозимки, нуллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга қизиқиш амалий характерга нисбатан кўпроқ назарий характерга эга. Балким, яқин келажакда улардан ахборот алмашинувини ҳимоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига бўладиган асосий хужумлар қуйидагилар:

- *маскарад* (impersonation). Фойдаланувчи ўзини бошқа шахс деб кўрсатишга уриниб, у шахс тарафидан харакатларнинг имкониятларига ва имтиёзларига эга бўлишни мўлжаллайди;
- аутентификация алмашинуви *тарафини алмаштириб қўйиш* (interleaving attack). Нияти бузуқ одам ушбу хужум мобайнида икки тараф орасидаги аутенфикацион алмашиниш жараёнида трафикни модификациялаш ниятида қатнашади. Алмаштириб қўйишнинг қуйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутентификация муваффақиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;
- *такрорий узатиш* (replay attack). Фойдаланувчиларнинг бири томонидан аутентификация маълумотлари такроран узатилади;

- *узатишни қайтариш* (reflection attak). Олдинги хужум вариантларидан бири бўлиб, хужум мобайнида нияти бузуқ протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни орқага қайтаради.

- *мажбурий кечикиш* (forced delay). Нияти бузуқ қандайдир маълумотни ушлаб қолиб, бирор вақтдан сўнг узатади.

- *матн танлашли хужум* (chosen text attack). Нияти бузуқ аутентификация трафигини ушлаб қолиб, узоқ муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юқорида келтирилган хужумларни бартараф қилиш учун аутентификация протоколларини қуришда қуйидаги усуллардан фойдаланилади:

- “сўров–жавоб”, вақт белгилари, тасодифий сонлар, индентификаторлар, рақамли имзолар каби механизмлардан фойдаланиш;

- аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги харакатларига боғлаш. Бундай ёндашишга мисол тариқасида аутентификация жараёнида фойдаланувчиларнинг кейинги ўзаро алоқаларида ишлатилувчи махфий сеанс калитларини алмашишни кўрсатиш мумкин;

- алоқанинг ўрнатилган сеанси доирасида аутентификация муолажасини вақти-вақти билан бажариб туриш ва ҳ.

“Сўров-жавоб” механизми қуйидагича. Агар фойдаланувчи *A* фойдаланувчи *B* дан оладиган хабари ёлғон эмаслигига ишонч хосил қилишни истаса, у фойдаланувчи *B* учун юборадиган хабарга олдиндан билиб бўлмайдиган элемент – *X* сўровини (масалан, қандайдир тасодифий сонни) қўшади. Фойдаланувчи В жавоб беришда бу амал устида маълум амални (масалан, қандайдир *f(X)* функцияни ҳисоблаш) бажариши лозим. Буни олдиндан бажариб бўлмайди, чунки сўровда қандай тасодифий сон *X* келиши фойдаланувчи *B* га маълум эмас. Фойдаланувчи *B* ҳаракати натижасини олган фойдаланувчи *A* фойдаланувчи *B* нинг хақиқий эканлигига ишонч хосил қилиши мумкин. Ушбу усулнинг камчилиги - сўров ва жавоб

ўртасидаги қонуниятни аниқлаш мумкинлиги.

Вақтни белгилаш механизми ҳар бир хабар учун вақтни қайдлашни кўзда тутади. Бунда тармоқнинг ҳар бир фойдаланувчиси келган хабарнинг қанчалик эскирганини аниқлаши ва уни қабул қилмаслик қарорига келиши мумкин, чунки у ёлғон бўлиши мумкин. Вақтни белгилашдан фойдаланишда сеанснинг хақиқий эканлигини тасдиқлаш учун *кечикишнинг жоиз вақт оралиғи* муаммоси пайдо бўлади. Чунки, “вақт тамғаси”ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташқари, қабул қилувчи ва жўнатувчининг соатлари мутлақо синхронланган бўлиши мумкин эмас.

Аутентификация протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

- *ўзаро аутентификациянинг мавжудлиги.* Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёқлама аутентификациянинг зарурлигини акс эттиради;
- *ҳисоблаш самарадорлиги*. Протоколни бажаришда зарур бўлган амаллар сони;
- *коммуникацион самарадорлик*. Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;
- *учинчи тарафнинг мавжудлиги*. Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;
- *хавфсизлик кафолати асоси.* Мисол сифатида нуллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;
- *сирни сақлаш*. Жиддий калитли ахборотни сақлаш усули кўзда тутилади.

Назорат саволлари:

1. Идентификация ва аутентификация тушунчаси.
2. Аутентификация технологиясининг турларини тушунтириб беринг.

3. Аутентификация протоколларига бўладиган хужумларни тавсифлаб беринг.

4. Аутентификация протоколларини танлашда қўлланиладиган мезонларни ёритиб беринг.

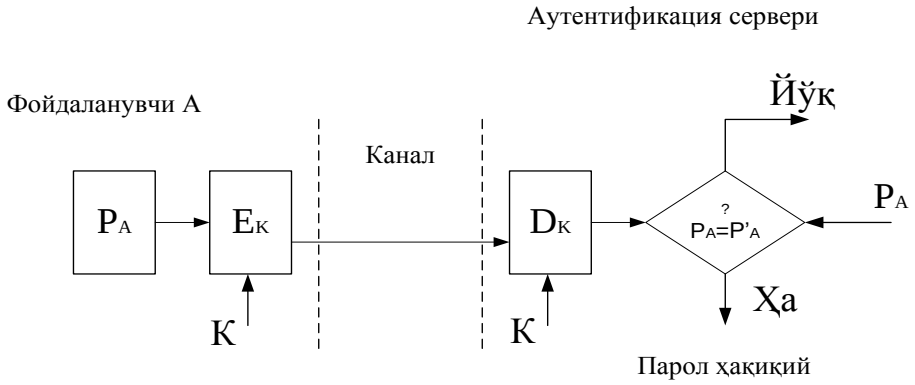
6.2. Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуйидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган ҳуқуқларни ва тармоқ ресурсларидан фойдаланишга рухсатни олади.

Паролдан фойдаланган ҳолда оддий аутентификациялаш схемаси 6.1–расмда келтирилган.

Равшанки, фойдаланувчининг паролини шифрламасдан узатиш орқали аутентификациялаш варианти хавфсизликнинг хатто минимал даражасини кафолатламайди. Паролни ҳимоялаш учун уни ҳимояланмаган канал орқали узатишдан олдин шифрлаш зарур. Бунинг учун схемага шифрлаш $E_к$ ва рас-шифровка қилиш $D_к$ воситалари киритилган. Бу воситалар бўлинувчи махфий калит К орқали бошқарилади. Фойдаланувчининг ҳақиқийлигини текшириш фойдаланувчи юборган парол P_A билан аутентификация серверида сақланувчи дастлабки қиймат $P_A^{'}$ ни таққослашга асосланган. Агар P_A ва $P_A^{'}$

қийматлар мос келса, парол P_A ҳақиқий, фойдаланувчи A эса қонуний ҳисобланади.



6.1-расм. Паролдан фойдаланган ҳолда оддий аутентификациялаш.

Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул – фойдаланувчилар паролини тизимли файлларда, очиқ ҳолда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан ҳимоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги – нияти бузуқнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.

Хавфсизлик нуқтаи назаридан паролларни бир томонлама функциялардан фойдаланиб узатиш ва сақлаш қулай ҳисобланади. Бу ҳолда фойдаланувчи паролнинг очиқ шакли ўрнига унинг бир томонлама функция h(.) дан фойдаланиб олинган тасвирини юбориши шарт. Бу ўзгартириш ғаним томонидан паролни унинг тасвири орқали ошкор қила олмаганлигини кафолатлайди, чунки ғаним ечилмайдиган сонли масалага дуч келади.

Кўп мартали паролларга асосланган оддий аутентификациялаш

тизимининг бардошлиги паст, чунки уларда аутентификацияловчи ахборот маъноли сўзларнинг нисбатан катта бўлмаган тўпламидан жамланади. Кўп мартали паролларнинг таъсир муддати ташкилотнинг хавфсизлиги сиёсатида белгиланиши ва бундай паролларни мунтазам равишда алмаштириб туриш лозим. Паролларни шундай танлаш лозимки, улар луғатда бўлмасин ва уларни топиш қийин бўлсин.

Бир мартали паролларга асосланган аутентификациялашда фойдаланишга ҳар бир сўров учун турли пароллар ишлатилади. Бир мартали динамик парол фақат тизимдан бир марта фойдаланишга яроқли. Агар, ҳатто кимдир уни ушлаб қолса ҳам парол фойда бермайди. Одатда бир мартали паролларга асосланган аутентфикациялаш тизими масофадаги фойдаланувчиларни текширишда қўлланилади.

Бир мартали паролларни генерациялаш аппарат ёки дастурий усул оқали амалга оширилиши мумкин. Бир мартали пароллар асосидаги фойдаланишнинг аппарат воситалари ташқаридан тўлов пластик карточкаларига ўхшаш микропроцессор ўрнатилган миниатюр қурилмалар кўринишда амалга оширади. Одатда калитлар деб аталувчи бундай карталар клавиатурага ва катта бўлмаган дисплей дарчасига эга.

Фойдаланувчиларни аутентификациялаш учун бир мартали паролларни қўллашнинг қуйидаги усуллари маълум:

1. Ягона вақт тизимига асосланган вақт белгилари механизмидан фойдаланиш.
2. Легал фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланиш.
3. Фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланиш.

Биринчи усулни амалга ошириш мисоли сифатида SecurID аутентикациялаш технологиясини кўрсатиш мумкин. Бу технология SecurityDynamics компанияси томонидан ишлаб чиқилган бўлиб, қатор компанияларнинг, ху-

сусан CiscoSystems компаниясининг серверларида амалга оширилган.

Вақт синхронизациясидан фойдаланиб аутентификациялаш схемаси тасодифий сонларни вақтнинг маълум оралиғидан сўнг генерациялаш алгоритмига асосланган. Аутентификация схемаси қуйидаги иккита параметрдан фойдаланади:

- ҳар бир фойдаланувчига аталган ва аутентификация серверида ҳамда фойдаланувчининг аппарат калитида сақланувчи ноёб 64-битли сондан иборат махфий калит;
- жорий вақт қиймати.

Масофадаги фойдаланувчи тармоқдан фойдаланишга уринганида ундан шахсий идентификация номери PINни киритиш таклиф этилади. PIN тўртта ўнли рақамдан ва аппарат калити дисплейида аксланувчи тасодифий соннинг олтита рақамидан иборат. Сервер фойдаланувчи томонидан киритилган PIN-коддан фойдаланиб маълумотлар базасидаги фойдаланувчининг махфий калити ва жорий вақт қиймати асосида тасодифий сонни генерациялаш алгоритмини бажаради. Сўнгра сервер генерацияланган сон билан фойдаланувчи киритган сонни таққослайди. Агар бу сонлар мос келса, сервер фойдаланувчига тизимдан фойдаланишга рухсат беради.

Аутентификациянинг бу схемасидан фойдаланишда аппарат калит ва сервернинг қатъий вақтий синхронланиши талаб этилади. Чунки аппарат калит бир неча йил ишлаши ва демак сервер ички соати билан аппарат калитининг мувофиқлиги аста-секин бузилиши мумкин.

Ушбу муаммони ҳал этишда SecurityDynamics компанияси қуйидаги икки усулдан фойдаланади:

- аппарат калити ишлаб чиқилаётганида унинг таймер частотасининг меъёридан четлашиши аниқ ўлчанади. Четлашишнинг бу қиймати сервер алгоритми параметри сифатида ҳисобга олинади;
- сервер муайян аппарат калит генерациялаган кодларни кузатади ва зарурият туғилганида ушбу калитга мослашади.

Аутентификациянинг бу схемаси билан яна бир муаммо боғлиқ. Аппа-

рат калит генерациялаган тасодифий сон катта бўлмаган вақт оралиғи мобайнида ҳақиқий парол ҳисобланади. Шу сабабли, умуман, қисқа муддатли вазият содир бўлиши мумкинки, хакер PIN-кодни ушлаб қолиши ва уни тармоқдан фойдаланишга ишлатиши мумкин. Бу вақт синхронизациясига асосланган аутентификация схемасининг энг заиф жойи ҳисобланади.

Бир мартали паролдан фойдаланиб аутентификациялашни амалга оширувчи яна бир вариант – «сўров-жавоб» схемаси бўйича аутентификациялаш. Фойдаланувчи тармоқдан фойдаланишга уринганида сервер унга тасодифий сон кўринишидаги сўровни узатади. Фойдаланувчининг аппарат калити бу тасодифий сонни, масалан DES алгоритми ва фойдаланувчининг аппарат калити хотирасида ва серверннинг маълумотлар базасида сақланувчи махфий калити ёрдамида расшифровка қилади. Тасодифий сон - сўров шифрланган кўринишда серверга қайтарилади. Сервер ҳам ўз навбатида ўша DES алгоритми ва серверннинг маълумотлар базасидан олинган фойдаланувчининг махфий калити ёрдамида ўзи генерациялаган тасодифий сонни шифрлайди. Сўнгра сервер шифрлаш натижасини аппарат калитидан келган сон билан таққослайди. Бу сонлар мос келганида фойдаланувчи тармоқдан фойдаланишга рухсат олади. Таъкидлаш лозимки, «сўров-жавоб» аутентификациялаш схемаси ишлатишда вақт синхронизациясидан фойдаланувчи аутентификация схемасига қараганда мураккаброқ.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг иккинчи усули фойдаланувчи ва текширувчи учун умумий бўлган тасодифий пароллар руйхатидан ва уларнинг ишончли синхронлаш механизмидан фойдаланишга асосланган. Бир мартали паролларнинг бўлинувчи рўйхати махфий пароллар кетма-кетлиги ёки набори бўлиб, ҳар бир парол фақат бир марта ишлатилади. Ушбу рўйхат аутентификацион алмашинув тарафлар ўртасида олдиндан тақсимланиши шарт. Ушбу усулнинг бир вариантига биноан сўров-жавоб жадвали ишлатилади. Бу жадвалда аутентификацилаш учун тарафлар томонидан ишлатилувчи сўровлар ва жавоблар мавжуд бўлиб, ҳар бир жуфт фақат бир марта ишлатилиши шарт.

Фойдаланувчини аутентификациялаш учун бир мартали паролдан фойдаланишнинг учинчи усули фойдаланувчи ва текширувчи учун умумий бўлган бир хил дастлабки қийматли псевдотасодифий сонлар генераторидан фойдаланишга асосланган. Бу усулни амалга оширишнинг қуйидаги вариантлари мавжуд:

- ўзгартирилувчи бир мартали пароллар кетма-кетлиги. Навбатдаги аутентификациялаш сессиясида фойдаланувчи айнан шу сессия учун олдинги сессия паролидан олинган махфий калитда шифрланган паролни яратади ва узатади;
- бир томонлама функцияга асосланган пароллар кетма-кетлиги. Ушбу усулнинг моҳиятини бир томонлама функциянинг кетма-кет ишлатилиши (Лампартнинг машҳур схемаси) ташкил этади. Хавфсизлик нуқтаи назаридан бу усул кетма-кет ўзгартирилувчи пароллар усулига нисбатан афзал ҳисобланади.

Кенг тарқалган бир мартали паролдан фойдаланишга асосланган аутентификациялаш протоколларидан бири Internet да стандартлаштирилган S/Key (RFC1760) протоколидир. Ушбу протокол масофадаги фойдаланувчиларнинг ҳақиқийлигини текширишни талаб этувчи кўпгина тизимларда, хусусан, Cisco компаниясининг TACACS+тизимида амалга оширилган.

Назорат саволлари:

1. Кўп мартали паролларга асосланган аутентификация технологияси.
2. Бир мартали паролларга асосланган аутентификация технологияси.
3. Бир мартали паролларни ҳосил қилишда псевдотасодифий сонлар генераторидан фойдаланиш.

6.3. Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида паролларнинг тайинланиши ва сақланиши билан боғлиқ фойдаланувчиларни дастлабки руйхатга олиш муолажаси жуда катта ва амалга оширилиши қийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива ҳисобланади.

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилар хусусидаги ҳеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда махфий ахборотни, хусусан махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкланади.

Фойдаланувчи шахсини тасдиқловчи рақамли сертификатлар фойдаланувчилар сўрови бўйича махсус ваколатли ташкилот-сертификация маркази CA (CertificateAuthority) томонидан, маълум шартлар бажарилганида берилади. Таъкидлаш лозимки, сертификат олиш муолажасининг ўзи ҳам фойдаланувчининг ҳақиқийлигини текшириш (яъни, аутентификациялаш) босқичини ўз ичига олади. Бунда текширувчи тараф сертификацияловчи ташкилот (сертификация маркази CA) бўлади.

Сертификат олиш учун мижоз сертификация марказига шахсини тасдиқловчи маълумотни ва очиқ калитини тақдим этиши лозим. Зарурий маълумотлар руйхати олинадиган сертификат турига боғлиқ. Сертификацияловчи ташкилот фойдаланувчининг ҳақиқийлиги тасдиғини текширганидан сўнг ўзининг рақамли имзосини очиқ калит ва фойдаланувчи хусусидаги маълумот бўлган файлга жойлаштиради ҳамда ушбу очиқ калитнинг муайян шахсга тегишли эканлигини тасдиқлаган ҳолда фойдаланувчига сертификат беради.

Сертификат электрон шакл бўлиб, таркибида қўйидаги ахборот бўлади:

- ушбу сертификат эгасининг очиқ калити;

- сертификат эгаси хусусидаги маълумот, масалан, исми, электрон почта адреси, ишлайдиган ташкилот номи ва ҳ.;

- ушбу сертификатни берган ташкилот номи;

- сертификацияловчи ташкилотнинг электрон имзоси – ушбу ташкилотнинг махфий калити ёрдамида шифрланган сертификациядаги маълумотлар.

Сертификат фойдаланувчини тармоқ ресурсларига мурожаат этганида аутентификацияловчи восита ҳисобланади. Бунда текширувчи тараф вазифасини корпоратив тармоқнинг аутентификация сервери бажаради. Сертификатлар нафақат аутентификациялашда, балки фойдаланишнинг маълум хуқуқларини тақдим этишда ишлатилиши мумкин. Бунинг учун сертификатга қўшимча ҳошиялар киритилиб уларда сертификация эгасининг фойдаланувчиларнинг у ёки бу категориясига мансублиги кўрсатилади.

Очиқ калитларнинг сертификатлар билан узвий боғлиқлигини алоҳида таъкидлаш лозим. Сертификат нафақат шахсни, балки очиқ калит мансублигини тасдиқловчи хужжатдир. Рақамли сертификат очиқ калит ва унинг эгаси ўртасидаги мосликни ўрнатади ва кафолатлайди. Бу очиқ калитни алмаштириш хавфини бартараф этади.

Агар абонент ахборот алмашинуви бўйича шеригидан сертификат таркибидаги очиқ калитни олса, у бу сертификатдаги сертификация марказининг рақамли имзосини ушбу сертификация марказининг очиқ калити ёрдамида текшириш ва очиқ калит адреси ва бошқа маълумотлари сертификатда кўрсатилган фойдаланувчига тегишли эканлигига ишонч ҳосил қилиши мумкин. Сертификатлардан фойдаланилганда фойдаланувчилар руйхатини уларнинг пароллари билан корпорация серверларида сақлаш зарурияти йўқолади. Серверда сертификацияловчи ташкилотларнинг номлари ва очиқ калитларининг бўлиши етарли.

Сертификатларнинг ишлатилиши сертификацияловчи ташкилотларнинг нисбатан камлигига ва уларнинг очиқ калитларидан қизиққан барча шахслар ва ташкилотлар фойдалана олиши (масалан, журналлардаги нашрлар ёрдамида) тахминига асосланган.

Сертификатлар асосида аутентификациялаш жараёнини амалга оши-

ришда сертификацияловчи ташкилот вазифасини ким бажариши хусусидаги масалани ечиш муҳим ҳисобланади. Ходимларни сертификат билан таъминлаш масаласини корхонанинг ўзи ечиши жуда табиий ҳисобланади. Корхона ўзининг ходимларини яхши билади ва улар шахсини тасдиқлаш вазифасини ўзига олиши мумкин. Бу сертификат берилишидаги дастлабки аутентификациялаш муолажасини осонлаштиради. Корхоналар сертификатларни генерациялаш, бериш ва уларга хизмат кўрсатиш жараёнларини автоматлаштиришни таъминловчи мавжуд дастурий махсулотлардан фойдаланишлари мумкин. Масалан, NetscapeCommunications компанияси серверларини корхоналарга шахсий сертификатларини чиқариш учун таклиф этади.

Сертификацияловчи ташкилот вазифасини бажаришда тижорат асосида сертификат бериш бўйича мустақил марказлар ҳам жалб этилиши мумкин. Бундай хизматларни, хусусан, Verisign компаниясининг сертификацияловчи маркази таклиф этади. Бу компаниянинг сертификатлари ҳалқаро стандарт X.509 талабларига жавоб беради. Бу сертификатлар маълумотлар ҳимоясининг қатор махсулотларида, жумладан ҳимояланган канал SSL протоколида ишлатилади.

Назорат саволлари:

1. Электрон сертификатлар таркибига қандай ахборотларни олади?
2. Электрон сертификатларни афзалликлари ва камчиликлари.
3. Электрон сертификатлар қайси асосий ҳалқаро стандарт талабларига жавоб бериши лозим.

6.4. Қатъий аутентификациялаш

Криптографик протоколларда амалга оширилувчи қатъий аутентификациялаш ғояси қуйидагича. Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган ҳолда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион

алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан тақсимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган ҳолда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг муҳими, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний сўров фақат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошланғич сўровга боғлиқ бўлади.

Аксарият ҳолларда қатъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг махфий калитига эгалиги аломати бўйича аутентификацияланади. Бошқача айтганда, фойдаланувчи унинг алоқа бўйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

X.509 стандарти тавсияларига биноан қатъий аутентификациялашнинг қуйидаги муолажалари фарқланади:

- бир томонлама аутентификация;
- икки томонлама аутентификация;
- уч томонлама аутентификация.

Бир томонлама аутентификациялаш бир томонга йўналтирилган ахборот алмашинувини кўзда тутади. Аутентификациянинг бу тури қуйидагиларга имкон яратади:

- ахборот алмашинувчининг фақат бир тарафини ҳақиқийлигини тасдиқлаш;
- узатилаётган ахборот яхлитлигининг бузилишини аниқлаш;
- "узатишнинг такрори" типидаги хужумни аниқлаш;
- узатилаётган аутентификацион маълумотлардан фақат текширувчи тараф фойдаланишини кафолатлаш.

Икки томонлама аутентификацилашда бир томонлилигига нисбатан исботловчи тарафга текширувчи тарафнинг қўшимча жавоби бўлади. Бу жавоб текширувчи томонни алоқанинг айнан аутентификация маълумотлари мўлжалланган тараф билан ўрнатилаётганига ишонтириш лозим.

Уч томонлама аутентификациялаш таркибида исботловчи тарафдан текширувчи тарафга қўшимча маълумотлар узатиш мавжуд. Бундай ёндашиш аутентификация ўтказишда вақт белгиларидан фойдаланишдан воз кечишга имкон беради.

Таъкидлаш лозимки, ушбу туркумлаш шартлидир. Амалда ишлатилувчи усул ва воситалар набори аутентификация жараёнини амалга оширишдаги муайян шарт-шароитларга боғлиқ. Қатъий аутентификациянинг ўтказилиши ишлатиладиган криптографик алгоритмлар ва қатор қўшимча параметрларни тарафлар томонидан сўзсиз мувофиқлаштиришни талаб этади.

Қатъий аутентификациялашнинг муайян вариантларини кўришдан олдин бир мартали параметрларнинг вазифалари ва имкониятларига тўхташ лозим. Бир мартали параметрлар баъзида "nonces" – бир мақсадга бир мартадан ортиқ ишлатилмайдиган катталик деб аталади.

Ҳозирда ишлатиладиган бир мартали параметрлардан тасодифий сонлар, вақт белгилари ва кетма-кетликларнинг номерларини кўрсатиш мумкин.

Бир мартали параметрлар узатишнинг такрорланишини, аутентификацион алмашинув тарафларини алмаштириб қўйишни ва очиқ матнни танлаш билан хужумлашни олдини олишга имкон беради. Бир мартали параметрлар ёрдамида узатиладиган хабарларнинг ноёблигини, бир маънолилигини ва вақтий кафолатларини таъминлаш мумкин. Бир мартали параметрларнинг турли хиллари алоҳида ишлатилиши, ёки бир-бирини тўлдириши мумкин.

Бир мартали параметрларнинг қуйидаги ишлатилиш мисолларини кўрсатиш мумкин:

- "сўров-жавоб" принципида қурилган протоколларда ўз вақтидалигини текшириш. Бундай текширишда тасодифий сонлар, соатларни синхронлаш

билан вақт белгилари ёки муайян жуфт (текширувчи, исботловчи) учун кетма-кетликларнинг номерларидан фойдаланиш мумкин;

- ўз вақтидалигини ёки ноёблик кафолатини таъминлаш. Протоколнинг бир мартали параметрларини бевосита (тасодифий сонни танлаш йўли билан) ёки билвосита (бўлинувчи сирдаги ахборотни тахлиллаш ёрдамида) назоратлаш орқали амалга оширилади;

- хабарни ёки хабарлар кетма-кетлигини бир маъноли идентификациялаш. Бир оҳангда ўсувчи кетма-кетликнинг бир мартали қийматини (масалан, серия номерлари ёки вақт белгилари кетма-кетлиги) ёки мос узунликдаги тасодифий сонларни тузиш орқали амалга оширилади.

Таъкидлаш лозимки, бир мартали параметрлар криптографик протоколларнинг бошқа вариантларида ҳам (масалан, калит ахборотини тақсимлаш протоколларида) кенг қўлланилади.

Қатъий аутентификациялаш протоколларини қўлланиладиган криптографик алгоритмларига боғлиқ ҳолда қуйидаги гуруҳларга ажратиш мумкин:

- шифрлашнинг симметрик алгоритмлари асосидаги қатъий аутентификациялаш протоколлари;

- бир томонлама калитли хеш-функциялар асосидаги қатъий аутентификациялаш протоколлари;

- шифрлашнинг асимметрик алгоритмлари асосидаги қатъий аутентификациялаш алгоритмлари;

- электрон рақамли имзо асосидаги қатъий аутентификациялаш алгоритмлари.

Симметрик алгоритмларга асосланган қатъий аутентификациялаш. Kerberos протоколи. Симметрик алгоритмлар асосида қурилган аутентификациялашнинг ишлаши учун текширувчи ва исботловчи айни бошидан битта махфий калитга эга бўлишлари зарур. Фойдаланувчилари кўп бўлмаган ёпиқ тизимлар учун фойдаланувчиларнинг ҳар бир жуфти махфий калитни ўзаро бўлиб олишлари мумкин. Симметрик шифрлаш технологиясини қўлловчи катта тақсимланган тизимларда ишончли сервер қатнашувидаги аутен-

тификациялаш протоколларидан фойдаланилади. Бу сервер билан ҳар бир тараф калитни билишлигини ўртоқлашишади.

Ушбу ёндашиш содда бўлиб туюлсада, аслида бундай аутентификациялаш протоколини ишлаб чиқиш мураккаб ва хавфсизлик нуқтаи назаридан *шубхасиз эмас.*

Қуйида шифрлашнинг симметрик алгоритмларига асосланган, ISO/IEC9798-2да спецификацияланган аутентификациялаш протоколларининг учта мисоли келтирилган. Бу протоколлар бўлинувчи махфий калитларни олдиндан тақсимланишини кўзда тутади. Аутентфикациялашнинг қуйидаги вариантларини кўриб чиқамиз.

- вақт белгиларидан фойдаланувчи бир томонлама аутентификациялаш.

- тасодифий сонлардан фойдаланувчи бир томонлама аутентификациялаш.

- икки томонлама аутентификациялаш.

Бу вариантларнинг ҳар бирида фойдаланувчи махфий калитни билишини намойиш қилган ҳолда, ўзининг ҳақиқийлигини исботлайди, чунки ушбу махфий калит ёрдамида сўровларни расшифровка қилади. Аутентификациялаш жараёнида симметрик шифрлашни қўллашда узатиладиган маълумотларнинг яхлитлигини таъминлаш механизмини расм бўлиб қолган усуллар асосида амалга ошириш ҳам зарур.

Қуйидаги белгилашларни киритамиз:

$г_A$- қатнашувчи А генерациялаган тасодифий сон;

$г_B$- қатнашувчи В генерациялаган тасодифий сон;

t_A- қатнашувчи А генерациялаган вақт белгиси;

E_K- калит Кда симметрик шифрлаш (калит К олдиндан А ва В ўртасида тақсимланиши шарт).

Вақт белгиларига асосланган бир томонлама аутентификациялаш:

$A \rightarrow B: E_K (t_A, B)$

Ушбу хабарни олиб расшифровка қилганидан сўнг қатнашувчи В вақт меткаси t_A ҳақиқий эканлигига ва хабарда кўрсатилган идентификатор ўзи-

ники билан мос келишига ишонч ҳосил қилади. Ушбу хабарни қайтадан узатишни олдини олиш калитни билмасдан туриб вақт меткаси t_A ни ва индентификатор Вни ўзгартириш мумкин эмаслигига асосланади.

Тасодифий сонлардан фойдаланишга асосланган бир томонлама аутентфикациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : E_K(r_B, B)$$

Қатнашувчи B қатнашувчи A га тасодифий сон r_B ни жўнатади. Қатнашувчи A олинган сон r_B ва идентификатор B дан иборат хабарни шифрлайди ва шифрланган хабарни қатнашувчи B га жўнатади. Қатнашувчи B олинган хабарни расшифровка қилади ва хабардаги тасодифий сонни қатнашувчи Ага юборгани билан таққослайди. Қўшимча у хабардаги исмни текширади.

Тасодифий қийматлардан фойдаланувчи икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : E_K(r_A, r_B, B)$$

$$A \leftarrow B : E_K(r_A, r_B)$$

Иккинчи ахборотни олиши билан қатнашувчи B олдинги протоколдаги текширишни амалга оширади ва қатнашувчи A га аталган учинчи хабарга киритиш учун қўшимча тасодифий сон r_A ни расшифровка қилади. Қатнашувчи A учинчи хабарни олганидан сўнг r_A ва r_B ларнинг қийматларини текшириш асосида айнан қатнашувчи B билан ишлаётганига ишонч ҳосил қилади.

Аутентификация жараёнида учинчи тарафни жалб этиш билан фойдаланувчиларни аутентификациялашни таъминловчи протоколларнинг машҳур намуналари сифатида Нидхэм ва Шредернинг махфий калитларни тақсимлаш протоколини ва Kerberos протоколини кўрсатиш мумкин.

Kerberos протоколи "мижоз-сервер" ва ҳам локал ва ҳам глобал тармоқларда ишловчи абонентлар орасида алоқанинг ҳимояланган каналини ўр-

натишга аталган калит ахборотини алмашиш тизимларида аутентификациялаш учун ишлатилади. Бу протоколнинг MicrosoftWindows 2000 ва UNIX BSD операцион тизимларига аутентификациялашнинг асосий протоколи сифатида ўрнатилганлиги алоҳида қизиқиш ўйғотади.

Kerberos ишонч қозонмаган тармоқларда аутентификациялашни таъминлайди, яъни Kerberos ишлашида нияти бузуқ одамлар қуйидаги ҳаракатларни бажаришлари мумкин:

- ўзини тармоқ уланишининг эътироф этилган тарафларидан бири деб кўрсатиш;

- уланишда иштирок этаётган компьютерларнинг биридан фойдалана олиш;

- ҳар қандай пакетни ушлаб қолиш, уларни модификациялаш ва/ёки иккинчи марта узатиш.

Kerberos протоколида хавфсизлик таъминоти юқорида келтирилган нияти бузуқ одамларнинг харакатлари натижасида пайдо бўладиган ҳар қандай муаммоларнинг бартарафланишини таъминлайди.

Kerberos протоколи олдинги асрнинг 80-йилларида яратилган ва шу пайтгача бешта версияда ўз аксини топган қатор жиддий ўзгаришларга дучор бўлди.

Kerberos TCP/IP тармоқлари учун яратилган бўлиб, протокол қатнашчиларининг учинчи(ишонилган) тарафга ишонишлари асосига қурилган. Тармоқда ишловчи Kerberos хизмати ишонилган воситачи сифатида ҳаракат қилиб, тармоқ ресурсларидан мижознинг (мижоз иловасининг) фойдалинишини авторизациялаш билан тармоқда ишончли аутентификациялашни таъминлайди. Kerberos хизмати алоҳида махфий калитни тармоқнинг ҳар бир субъекти билан бўлишади ва бундай махфий калитни билиш тармоқ субъекти ҳақиқийлигининг исботига тенг кучлидир.

Kerberos асосини Нидхем-Шредернинг учинчи ишонилган тараф билан аутентификациялаш ва калитларни тақсимлаш протоколи ташкил этади. Нидхем-Шредер протоколининг ушбу версиясини Kerberosга татбиқан

кўрайлик. Kerberos протоколида (5-версия) алоқа қилувчи иккита тараф ва калитларни тақсимлаш маркази KDC (Key Distribution Center) вазифасини бажарувчи ишонилган сервер KS иштирок этади.

Чақирувчи объект A орқали, чақирилувчи объект B орқали белгиланади. Сеанс қатнашчилари, мос ҳолда Id_A ва Id_B ноёб идентификаторларга эга. A ва B тарафлар, ҳар бири алоҳида, ўзининг махфий калитини сервер KS билан бўлишади.

Айтайлик, A тараф B тараф билан ахборот алмашиш мақсадида сеанс калитини олмоқчи. A тараф тармоқ орқали сервер KSга Id_A ва Id_B идентификаторларни юбориш билан калитлар тақсимланиши даврини бошлаб беради:

$$A \to KS : Id_A, Id_B$$

Сервер KS вақтий белги T, таъсир муддати L, тасодифий калит K ва идентфикатор Id_A бўлган хабарни генерациялаб, бу хабарни B тараф билан бўлинган махфий калит ёрдамида шифрлайди.

Сўнгра сервер KS B тарафга тегишли вақтий белги T, таъсир муддати L, тасодифий калит K, идентификатор Id_B ни олиб уни A тараф билан бўлинган махфий калит ёрдамида шифрлайди. Бу иккала шифрланган хабарларни A тарафга жўнатади.

$$KS \to A : E_A(T, L, K, Id_B), E_B(T, L, K, Id_A)$$

A тараф биринчи хабарни ўзининг махфий калити билан расшифровка қилади ва ушбу хабар калитлар тақсимотининг олдинги муолажасининг қайтарилиши эмаслигига ишонч ҳосил қилиш мақсадида вақт белгиси T ни текширади. Сўнгра A тараф ўзининг идентификатори Id_A ва вақт белгиси билан хабарни генерациялаб, уни сеанс калити K ёрдамида шифрлайди ва B тарафга узатади. Ундан ташқари, A тараф B тараф учун KS дан B тараф калити ёрдамида шифрланган хабарни жўнатади:

$$A \to B : E_K(Id_A, T), E_B(T, L, K, Id_A)$$

Бу хабарни фақат B тараф расшифровка қилиши мумкин. B тараф вақт белгиси T, таъсир муддати L, сеанс калити K ва идентификатор Id_A ни олади. Сўнгра B тараф сеанс калит K ёрдамида хабарнинг иккинчи қисмини рас-

шифровка қилади. Хабарнинг иккала қисмидаги T ва Id_A қийматларининг мос келиши A нинг B га нисбатан ҳақиқийлигини тасдиқлайди.

Хақиқийликни ўзаро тасдиқлаш мақсадида B тараф вақт белгиси T плюс 1 дан иборат хабар яратади, уни K калит ёрдамида шифрлайди ва A тарафга жўнатади.

$$B \to A : E_K(T+1)$$

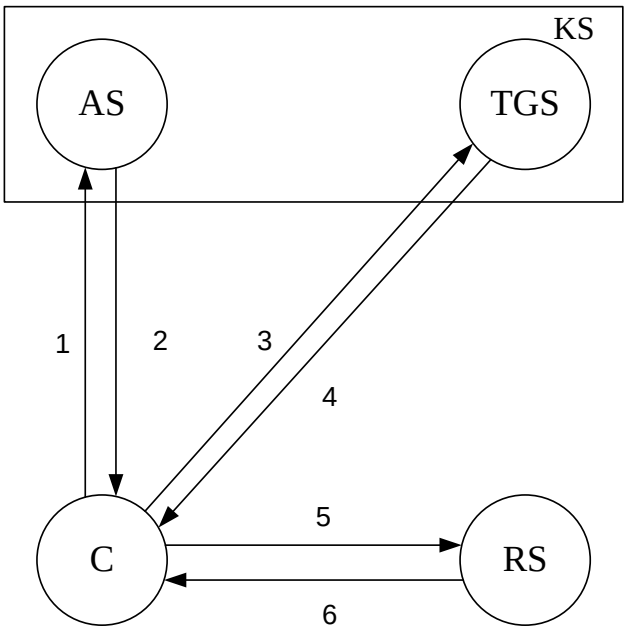
Агар бу хабар расшифровка қилингандан кейин A тараф кутилган натижани олса, у алоқа линиясининг бошқа тарафида ҳақиқатан B турганлигига ишонч ҳосил қилади.

Бу протокол барча қатнашувчиларнинг соатлари сервер KS соатлари билан синхронланганида муваффақиятли ишлайди. Таъкидлаш лозимки, бу протоколда A тарафнинг B тараф билан алоқа ўрнатишга ҳар бир хоҳишида сеанс калитини олиш учун KS билан алмашинув зарур бўлади. Протоколнинг A ва B объектларни ишончли улаши учун, ҳеч бир калит обрўсизланмаслиги ва сервер KS нинг ҳимояланиши талаб этилади.

Умуман *Kerberos* тизимида (5 версия) фойдаланувчини идентификациялаш ва аутентификациялаш жараёнини қуйидагича тавсифлаш мумкин (6.2-расм).

Мижоз C, тармоқ ресурсидан фойдаланиш мақсадида аутентификация сервери *AS*га сўров йўллайди. Сервер *AS* фойдаланувчини унинг исми ва пароли ёрдамида идентификациялайди ва мижозга мандат ажратиш хизмати сервери *TGS*дан (*Ticket Grating Service*) фойдаланишга мандат юборади.

Ахборот ресурсларининг муайян мақсадли сервери *RS*дан фойдаланиш учун мижоз C *TGS*дан мақсадли сервер *RS*га мурожаат қилишга мандат сўрайди. Ҳамма нарса тартибда бўлса *TGS* керакли тармоқ ресурсларидан фойдаланишга рухсат бериб, клиент C га мос мандатни юборади.



Белгилашлар:
KS – Kerberos тизими сервери
AS – Аутентификация сервери
TGS – Мандатларни ажратиш тизими сервери
RS – Ахборот ресурслари сервери
C – Kerberos тизими мижози

6.2-расм. Kerberos протоколининг ишлаш схемаси

Kerberos тизими ишлашининг асосий қадамлари (6.2.-расмга қаралсин):

1. $C \to AS$ - мижоз *C* нинг *TGS* хизматига мурожаат қилишга рухсат сўраб сервер *AS*дан сўрови.

2. $AS \to C$ - сервер *AS*нинг мижоз *C* га *TGS* хизматидан фойдаланишга рухсати (мандати).

3. $C \to TGS$ - мижоз *C* нинг ресурслар сервери *RS* дан фойдаланишга рухсат (мандат) сўраб, *TGS* хизматидан сўрови.

4. $TGS \to C$ - *TGS* хизматининг мижоз *C* га ресурслар сервери *RS* дан фойдаланишига рухсати (мандати).

5. $C \to RS$ - сервер *RS*дан ахборот ресурсининг (хизматнинг) сўрови.

6. $RS \to C$ - сервер *RS*нинг хақиқийлигини тасдиқлаш ва мижоз *C* га ахборот ресурсини (хизматни) тақдим этиш.

Мижоз билан сервер алоқасининг ушбу модели фақат узатиладиган бошқарувчи ахборотнинг конфиденциаллиги ва яхлитлиги таъминланганида ишлаши мумкин. Ахборот хавфсизлигини қатъий таъминламасдан *AS, TGS* ва *RS* серверларга мижоз *C* сўров юбораолмайди ва тармоқ хизматидан фойдаланишга рухсат ололмайди.

Ахборотнинг ушлаб қолиниши ва рухсатсиз фойдаланиши имкониятларини бартараф этиш мақсадида Kerberos тармоқда ҳарқандай бошқариш ахбороти узатилганида махфий калитлар комплексини (мижознинг махфий калити, сервернинг махфий калити, мижоз-сервер жуфтининг махфий сеанс калитлари) кўп марта шифрлашни ишлатади. Kerberos шифрлашнинг турли алгоритмларидан ва хэш-функциялардан фойдаланиши мумкин, аммо мададлаш учун Triple DES ва MD5 алгоритмлари ўрнатилган.

Kerberos тизимида ишонч хужжатларининг икки туридан фойдаланилади: мандат (tricket) ва аутентификатор (authentificator).

Мандат серверга мандат берилган мижознинг идентификацион маълумотларини хавфсиз узатиш учун ишлатилади. Унинг таркибида ахборот ҳам бўлиб, ундан сервер мандатдан фойдаланаётган мижознинг хақиқий эканлигини текширишда фойдаланиши мумкин.

Аутентификатор – мандат билан бирга кўрсатилувчи қўшимча атрибут(аломат). Қуйида Kerberos хужжатларида ишлатилувчи белгилашлар тизими келтирилган:

C – мижоз;

S – сервер;

a – мижознинг тармоқ адреси;

v – мандат таъсири вақтининг бошланиши ва охири;

T – вақт белгиси;

K_x – махфий калит х;

K_{xy} – х ва у учун сеанс калити;

$\{m\}K_x$ – субъект x нинг махфий калити K_x билан шифрланган хабар m;

$T_{x,y}$ – y дан фойдаланишга мандат x;

$A_{x,y}$ – x ва y учун аутентификатор.

Kerberos мандати.

Kerberos мандати қуйидаги шаклга эга: $T_{c,s} = S,\{C,a,v,K_{C,S}\}K_S$.

Мандат битта мижозга қатъий белгиланган сервердан фойдаланиш учун қатъий белгиланган вақтга берилади. Унинг таркибида мижоз исми,

унинг тармоқ адреси, мижоз ҳаракатининг бошланиш ва тугаш вақти ва сервернинг махфий калити K_S шифрланган сеанс калити $K_{C,S}$ бўлади. Мижоз мандатни расшифровка қилаолмайди (у сервернинг махфий калитини билмайди), аммо у мандатни шифрланган шаклда серверга кўрсатиши мумкин. Мандат тармоқ орқали узатилаётганда тармоқдаги яширинча эшитиб турувчиларнинг бирортаси ҳам уни ўқий олмайди ва ўзгартира олмайди.

Kerberos аутентификатори.

Kerberos аутентификатори қуйидаги шаклга эга: $A_{C,S} = \{C, t, калит\}K_{C,S}$

Мижоз мақсадли сервердан фойдаланишни хоҳлаганида аутентификаторни яратади. Унинг таркибида мижоз исми, вақт белгиси, мижоз ва сервер учун умумий бўлган, сеанс калити $K_{C,S}$ да шифрланган, сеанс калити бўлади. Мандатдан фарқли ҳолда аутентификатор бир марта ишлатилади.

Аутентификаторнинг ишлатилиши иккита мақсадни кўзлайди. Биринчидан, аутентификаторда сеанс калитида шифрланган қандайдир матн бўлади. Бу калитнинг мижозга маълумлигидан далолат беради. Иккинчидан, шифрланган очиқ матнда вақт белгиси мавжуд. Бу вақт белгиси аутентификатор ва мандатни ушлаб қолган нияти бузуқ одамга улардан бирор вақт ўтганидан сўнг аутентфикациялаш муолжасини ўтишда ишлатишига имкон бермайди.

Kerberos хабарлари.

Kerberosнинг 5-версиясида хабарларнинг қуйидаги турлари ишлатилади (6.2-расмга қаралсин).

1. Мижоз – Kerberos: *C, tgs.*
2. Kerberos – мижоз : $\{K_{c,tgs}\}K_c\{T_{cftgs}\}K_{tgs}$.
3. Мижоз – $TGS : \{A_{C,S}\}K_{C,tgs}(T_{C,tgs})K_{tgs,S}$.
4. TGS – мижоз: $\{K_{C,S}\}K_{C,tgs}\{T_{C,S}\}K_S$,.
5. Мижоз – сервер: $\{A_{C,S}\}K_{C,S}\{T_{C,S}\}K_S$.

Ушбу хабарлардан фойдаланишни батафсил кўрайлик.

Дастлабки мандатни олиш.

Мижозда шахсини исботловчи ахборотнинг қисми – унинг пароли мавжуд. Мижозни паролини тармоқ орқали жўнатишига мажбур қилиб бўлмайди. Kerberos протоколи паролни обрўсизлантириш эҳтимолини минималлаштиради, аммо агар фойдаланувчи паролни билмаса унга ўзини тўғри идентификациялашга имкон бермайди.

Мижоз Kerberosнинг аутентификация серверига ўзининг исми, *TGS*серверининг (бир нечта сервер *TGS* бўлиши мумкин) хабарини жўнатади. Амалда фойдаланувчи кўпинча исмини ўзини киритади, тизимга кириш дастури эса сўров юборади.

Kerberosнинг аутентификациялаш сервери ўзининг маълумотлар базасида мижоз хусусидаги маълумотларни қидиради. Агар мижоз хусусидаги ахборот маълумотлар базасида бўлса, Kerberos мижоз ва *TGS* орасида маълумот алмашиш учун ишлатиладиган сеанс калитини генерациялайди. Kerberos бу сеанс калитини мижознинг махфий калити билан шифрлайди. Сўнгра у *TGS* хизматига мижознинг хақиқийлигини исботловчи *TGT* (*TicketGranting-Ticket*) мандатининг ажратилиши учун мижозга мандат яратади. *TGS* нинг махфий калитида *TGT* шифрланади ва унинг таркибида мижоз ва сервер идентификатори, *TGS* – мижоз жуфтининг сеанс калити, ҳамда *TGT* таъсирининг бошланиш ва охирги вақтлари бўлади. Аутентификациялаш сервери бу иккита шифрланган хабарни мижозга юборади.

Энди мижоз бу хабарларни қабул қилади, биринчи хабарни ўзининг махфий калити K_C билан расшифровка қилиб, сеанс калити $K_{C,tgs}$ни ҳосил қилади. Махфий калит мижоз паролининг бир томонлама хэш-функцияси бўлганлиги сабабли қонуний фойдаланувчида ҳеч қандай муаммо туғилмайди. Нияти бузуқ одам тўғри паролни билмайди ва, демак, аутентификациялаш серверининг жавобини расшифровка қила олмайди. Шу сабабли нияти бузуқ одам мандатни ёки сеанс калитини ола олмайди. Мижоз *TGT* мандатини ва сеанс калитини сақлаб, парол ва хэш-қийматни, уларнинг обрўсизланиш эҳтимолликларини пасайтириш мақсадида, ўчиради. Агар нияти бузуқ

одам мижоз хотираси таркибининг нусхасини олишга уринса, у фақат *TGT* ва сеанс калитини олади. Бу маълумотлар фақат *TGT* таъсири вақтидагина муҳим ҳисобланади. *TGT* таъсир муддати тугаганидан сўнг бу маълумотлар маънога эга бўлмайди. Энди мижоз *TGT* дан олинган мандат ёрдамида унда кўрсатилган *TGT* таъсирининг бутун муддати мобайнида сервер *TGS* да аутентификациялашдан ўтиш имкониятига эга.

Сервер мандатларини олиш.

Мижоз ўзига керак бўлган ҳар бир хизмат учун алоҳида мандат олиши мумкин. Шу мақсадда мижоз *TGS* хизматига *TGT* мандати ва аутентификатордан иборат сўров юбориши лозим. (Амалда сўровни дастурий таъминот автоматик тарзда, яъни фойдаланувчига билдирмасдан юборади.) Мижоз ва *TGS* сервери жуфтининг калитида шифрланган аутентификатор таркибида мижоз ва унга керакли сервернинг идентификатори, тасодифий сеанс калити ва вақт белгиси бўлади.

TGS сўровни олиб, ўзининг махфий калитида *TGT* ни расшифровка қилади. Сўнгра *TGS* аутентификаторни расшифровка қилишда *TGT*даги сеанс калитидан фойдаланади. Ниҳоясида аутентификатордаги ахборот мандат ахбороти билан таққосланади. Аниқроғи, чиптадаги мижознинг тармоқ адреси сўровда кўрсатилган тармоқ адреси билан, ҳамда вақт белгиси жорий вақт билан солиштирилади. Агар барчаси мос келса, *TGS* сўровни бажаришга рухсат беради.

Вақт белгиларини текширишда барча компьютерларнинг соатлари, бўлмаганда, бир неча минут аниқлигида синхронланганлиги кўзда тутилади. Агар сўровда кўрсатилган вақт жорий ондан анчагина фарқ қилса, TGS бундай сўровни олдинги сўровни қайтаришга уриниш деб ҳисоблайди.

TGS хизмати аутентификатор таъсири муддатининг тўғрилигини кузатиши лозим, чунки сервер хизматлар битта мандат, аммо турли аутентификаторлар ёрдамида кетма-кет бир неча марта сўралиши мумкин. Ўша мандат ва аутентификаторнинг ишлатилган вақт белгиси билан қилинган сўров рад қилинади.

Тўғри сўровга жавоб тариқасида *TGS* мижозга мақсад сервердан фойдаланиш учун мандат тақдим этади. *TGS* мижоз ва мақсад сервери учун мижоз ва *TGS* га умумий бўлган сеанс калитида шифрланган сеанс калитини ҳам яратади. Бу иккала хабар мижозга юборилади. Мижоз хабарни расшифровка қилади ва сеанс калитини чиқариб олади.

Хизмат сўрови.

Энди мижоз ўзининг ҳақиқийлигини мақсад серверига исботлаши мумкин. Мақсад серверида аутентификациядан муваффақиятли ўтиш учун мижоз таркибида ўзининг исми, тармоқ адреси, вақт белгиси бўлган ва сеанс калити "мижоз-сервер"да шифрланган аутентификаторни яратади ва уни TGS хизматидан олиб берилган мақсад серверининг махфий калитида шифрланган мандат билан бирга жўнатади.

Мақсад сервери мижоздан маълумотларни олиб, аутентификаторни ўзининг махфий калитида расшифровка қилади ва ундан "мижоз-сервер" сеанс калитини чиқариб олади. Мандат ҳам текширилади. Текшириш муолажаси "мижоз-TGS" сессиясида ўтказиладиган муолажага ўхшаш, яъни тармоқ адреслари ва вақт белгисининг мослиги текширилади. Агар барчаси мос келса, сервер мижознинг хақиқийлигига ишонч ҳосил қилади.

Агар илова ҳақиқийликнинг ўзаро текширилишини талаб этса, сервер мижозга таркибида сеанс калитида шифрланган вақт белгиси бўлган хабарни юборади. Бу серверга тўғри махфий калитнинг маълум эканлигини ва у мандат ва гувоҳномани расшифровка қила олишини исботлайди. Зарурият туғилганида мижоз ва сервер кейинги хабарларни умумий калитда шифрлашлари мумкин. Чунки бу калит фақат уларга маълум, бу калит билан шифрланган охирги хабар иккинчи тарафдан юборилганига иккала тараф ишонч ҳосил қилишлари мумкин. Амалда бу барча мураккаб муолажалар автоматик тарзда бажарилади ва мижозга қандайдир ноқулайликлар етказилмайди.

Доменлараро аутентификациялаш хусусиятлари.

Kerberos дан доменлараро аутентификациялашда ҳам фойдаланиш мумкин. Мижоз бошқа домендаги сервердан фойдаланиш мақсадида калит-

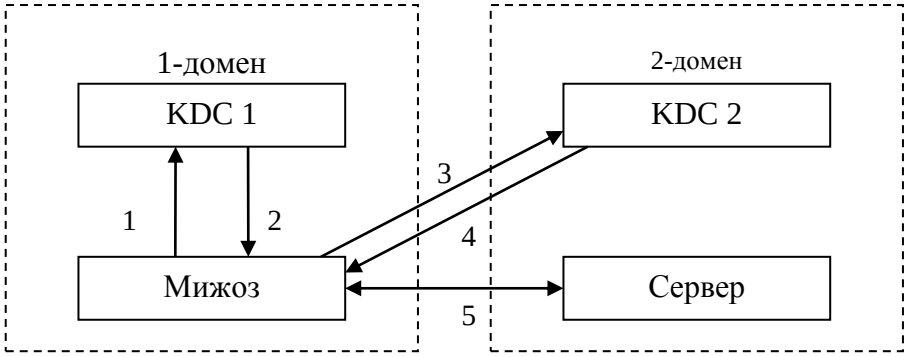
ларни тақсимлаш маркази *KDC* га мурожаат қилса, *KDC* мижозга суралаётган сервер жойлашган доменнинг *KDC* ига мурожаат этишга *қайта адреслаш мандатини* (referalticket) тақдим этади (6.3-расм).

Расмда қуйидаги белгилашлар қабул қилинган:

1. Аутентификациялашга сўров.
2. *KDC*1 учун *TGT*
3. *KDC*2 учун *TGT*.
4. Сервердан фойдаланиш мандати.
5. Маълумотларни аутентификациялаш ва алмашиш.

Қайта адреслаш мандати иккита домен KDCсининг жуфтли алоқа калитида шифрланган TGTдир. Бунда мижозга сервердан фойдаланишга мандатни сўралаётган сервер жойлашган KDC тақдим этади.

Жуда кўп доменли тармоқда аутентификациялаш учун Kerberosдан фойдаланиш назарий жиҳатдан мумкин бўлсада, мурожаатлар сонининг доменлар сонига мутаносиб равишда ошиши сабабли, сўровларни муайян KDCларга бир маънода қайта адресловчи қандайдир марказий домен қуришга тўғри келади.



6.3-расм. Kerberos протоколида доменлараро аутентификациялаш схемаси

Kerberos хавфсизлиги.

Kerberos, криптографик ҳимоялашнинг бошқа ҳарқандай дастурий воситаси каби ишончсиз дастурий муҳитда ишлайди. Ушбу муҳитнинг хужжатлаштирилмаган имкониятлари ёки нотўғри конфигурацияси жиддий ахборотнинг сирқиб чиқишига олиб келиши мумкин. Хатто калитлар фойдаланувчи ишлаш сеансида фақат оператив хотирада сақланса ҳам

операцион тизимдаги бузилиш калитларнинг қаттиқ дискда нусхаланишига олиб келиши мумкин.

Kerberos дастурий таъминоти ўрнатилган ишчи станциясидан кўпчилик фойдаланувчи режимнинг ишлатилиши ёки ишчи станциялардан фойдаланишнинг назорати бўлмаслиги дастур-закладкани киритиш ёки криптографик дастурий таъминотни модификациялаш имкониятини туғдиради.

Шу сабабли, Kerberos хавфсизлиги кўп жиҳатдан ушбу протокол ўрнатилган ишчи станцияси ҳимоясининг ишончлигига боғлиқ.

Kerberos протоколининг ўзига қуйидаги қатор талаблар қуйилади:

- Kerberos хизмати хизмат қилишдан воз кечишга йўналтирилган хужумлардан ҳимояланиши шарт;

- вақт белгиси аутентификация жараёнида қатнашиши сабабли, тизимдан фойдаланувчиларининг барчаси учун тизимли вақтни синхронлаш зарур;

- Kerberos паролни саралаш орқали хужумлашдан ҳимояламайди. Муаммо шундаки, *KDC* да сақланувчи фойдаланувчи калити унинг паролини хэш-функция ёрдамида қайта ишлаш натижасидир. Паролнинг бўшлигида уни саралаб топиш мумкин;

- Kerberos хизмати рухсатсиз фойдаланишининг барча турларидан ишончли ҳимояланиши шарт;

- мижоз олган мандатлар, ҳамда махфий калитлар рухсатсиз фойдаланишдан ҳимояланиши шарт.

Юқорида келтирилган талабларнинг бажарилмаслиги муваффақиятли хужумга сабаб бўлиши мумкин.

Ҳозирда Kerberos протоколи аутентификациялашнинг кенг тарқалган воситаси ҳисобланади. Kerberos турли криптографик схемалар, хусусан, очиқ калитли шифрлаш билан биргаликда ишлатилиши мумкин.

Бир томонлама калитли хэш-функциялардан фойдаланишга асосланган протоколлар. Бир томонлама хэш-функция ёрдамида шифрлашнинг

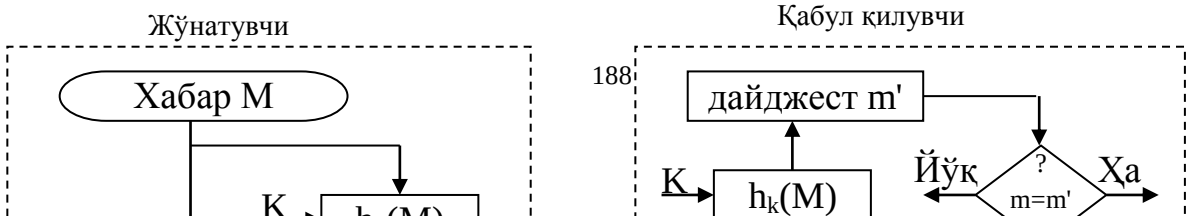
ўзига хос хусусияти шундаки, у моҳияти бўйича бир томонламадир, яъни тескари ўзгартириш-қабул қилувчи тарафда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) бир томонлама шифрлаш муолажасидан фойдаланади.

Шифрланаётган маълумот *М*га қўлланилган *К* параметр-калитли бир томонлама хэш-функция $h_k(.)$ натижада байтларнинг белгиланган катта бўлмагани сонидан иборат хэш-қиймат (дайджест) "*m*" ни беради (6.4-расм).

Дайджест "m" қабул қилувчига дастлабки хабар *М* билан бирга узатилади. Хабарни қабул қилувчи, дайджест олинишида қандай бир томонлама хэш-функция ишлатилганлигини билган ҳолда, расшифровка қилинган хабар *М* дан фойдаланиб, дайджестни бошқатдан ҳисоблайди. Агар олинган дайджест билан ҳисобланган дайджест мос келса, хабар *М* нинг таркиби ҳеч қандай ўзгаришга дучор бўлмаганини билдиради.

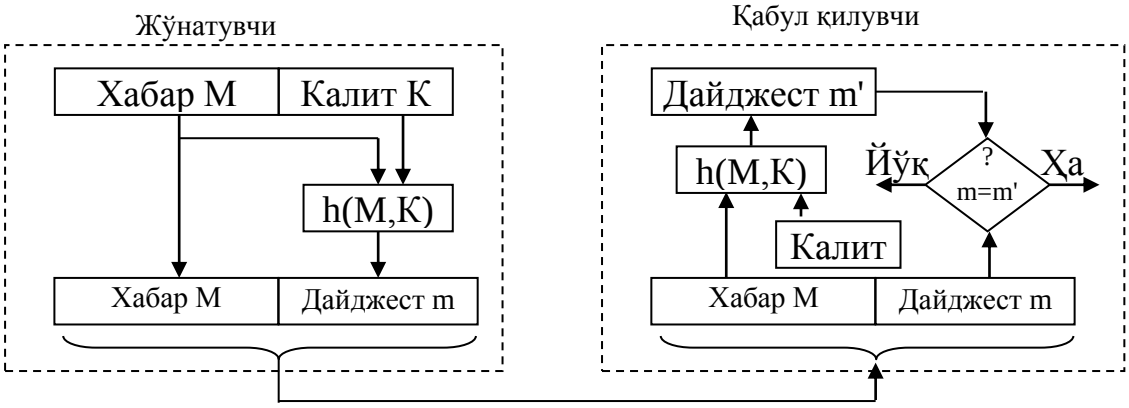
Дайджестни билиш дастлабки хабарни тиклашга имкон бермайди, аммо маълумотлар яхлитлигини текширишга имкон беради. Дайджестга дастлабки хабар учун ўзига хос назорат йиғиндиси сифатида қараш мумкин. Аммо, дайджест ва оддий назорат йиғиндиси орасида жиддий фарқ ҳам мавжуд. Назорат йиғиндисидан алоқанинг ишончсиз линияси бўйича узатиладиган хабарларнинг яхлитлигини текшириш воситаси сифатида фойдаланилади. Текширишнинг бу воситаси нияти бузуқ одамлар билан кўрашишга мўлжалланмаган. Чунки, бу ҳолда назорат йиғиндисининг янги қийматини қўшиб хабарни алмаштириб қўйишга уларга ҳеч ким халақит бермайди. Қабул қилувчи бунда ҳеч нарсани сезмайди.

Дайджестни ҳисоблашда, оддий назорат йиғиндисидан фарқли равишда, махфий калитлар ишлатилади. Агар дайджест олинишида фақат жўнатувчи ва қабул қилувчига маълум бўлган параметр-калитли бир томонлама хэш-функция ишлатилса, дастлабки хабарнинг ҳар қандай модификацияси дарҳол маълум бўлади.



6.5-расмда маълумотлар яхлитлигини текширишда бир томонлама хэш-функция ишлатилишининг бошқа варианти келтирилган.

Бу ҳолда бир томонлама хэш-функция *h(.)* параметр–калитга эга эмас, аммо у махфий калит билан тўлдирилган хабарга қўлланилади, яъни жўнатувчи дайджест m=h(M, K)ни ҳисоблайди. Қабул қилувчи дастлабки хабарни чиқариб олиб, уни ўша маълум махфий калит билан тўлдиради. Сўнгра олинган маълумотларга бир томонлама хэш-функция h(.)ни қўллайди. Ҳисоблаш натижаси – дайджест "m" тармоқ орқали олинган дайджест "m" билан таққосланади.



6.5–расм. Маълумотлар яхлитлигини текширишда бир томонлама хэш-функциянинг ишлатиши (II-вариант).

Асимметрик алгоритмларга асосланган қатъий аутентификациялаш.

Қатъий аутентификациялаш протоколларида очиқ калитли асимметрик алгоритмлардан фойдаланиш мумкин. Бу ҳолда исботловчи махфий калитни

билишлигини қуйидаги усулларнинг бири ёрдамида намойиш этиши мумкин:

- очиқ калитда шифрланган сўровни расшифровка қилиш;

- сўров сўзининг рақамли имзосини қўйиш.

Аутентификацияга зарур бўлган калитларнинг жуфти, хавфсизлик мулоҳазасига кўра, бошқа мақсадларга (масалан, шифрлашда) ишлатилмаслиги шарт. Очиқ калитли танланган тизим шифрланган матнни танлаш билан хужумларга, хатто бузғунчи ўзини текширувчи деб кўрсатиб ва унинг номидан ҳаракат қилганда ҳам, бардош бериши лозимлигига фойдаланувчиларни огоҳлантириш керак.

Шифрлашнинг асимметрик алгоритмларидан фойдаланиб аутентификациялаш.

Шифрлашнинг асимметрик алгоритмларидан фойдаланишга асосланган протоколга мисол тариқасида аутентификациялашнинг қуйидаги протоколини келтириш мумкин:

$$A \leftarrow B : h(r), B, P_A(r, B),$$

$$A \rightarrow B : r.$$

Қатнашувчи B тасодифий ҳолда r ни танлайди ва $x=h(r)$ қийматини ҳисоблайди (x қиймати r нинг қийматини очмасдан туриб r ни билишлигини намойиш этади), сўнгра у $e = P_A(r, B)$ қийматни ҳисоблайди. P_A орқали асимметрик шифрлаш алгоритми фараз қилинса, $h(.)$ орқали хэш-функция фараз қилинади. Қатнашувчи B хабарни қатнашувчи A га жўнатади. Қатнашувчи A $e = P_A(r, B)$ ни расшифровка қилади ва r' ва B' қийматларни олади, ҳамда $x' = h(r')$ни ҳисоблайди. Ундай кейин $x=x'$ эканлигини ва B' идентификатор ҳақиқатан қатнашувчи Bга кўрсатаётганини тасдиқловчи қатор таққослашлар бажарилади. Таққослаш муваффақиятли ўтса қатнашувчи A "r"ни қатнашувчи B га узатади. Қатнашувчи B "r"ни олганидан сўнг уни биринчи хабарда жўнатган қиймати эканлигини текширади.

Кейинги мисол сифатида асимметрик шифрлашга асосланган Нидхем ва Шредернинг модификацияланган протоколини келтирамиз. Фақат аутентификациялашда ишлатилувчи Нидхем ва Шредер протоколи вариантини

кўришда P_B орқали қатнашувчи Внинг очиқ калити ёрдамида шифрлаш алгоритми фараз қилинади. Протокол қуйидаги структурага эга:

$$A \to B : P_B(r_1, A)$$

$$A \leftarrow B : P_A(r_2, r_i)$$

$$A \leftarrow B : r_2$$

Рақамли имзодан фойдаланиш асосидаги аутентификациялаш

X.509 стандартининг тавсияларида рақамли имзо, вақт белгиси ва тасодифий сонлардан фойдаланиш асосидаги аутентификациялаш схемаси спецификацияланган. Ушбу схемани тавсифлаш учун қуйидаги белгилашларни киритамиз:

- t_A, r_A ва r_B – мос ҳолда вақт белгиси ва тасодифий сонлар;
- S_A - қатнашувчи A генерациялаган имзо;
- $cert_A$ – қатнашувчи A очиқ калитининг сертификати;
- $cert_B$ – қатнашувчи B очиқ калитининг сертификати;

Мисол тариқасида аутентификациялашнинг қуйидаги протоколларини келтирамиз:

1. Вақт белгисидан фойдаланиб бир томонлама аутентфикациялаш:

$$A \to B : cert_A, t_A, B, S_A(t_A, B)$$

Қатнашувчи B ушбу хабарни олганидан сўнг вақт белгиси t_A нинг тўғрилигини, олинган идентификатор B ни ва сертификат $cert_A$ даги очиқ калитдан фойдаланиб рақамли имзо $S_A(t_A,B)$ нинг корректлигини текширади.

2. Тасодифий сонлардан фойдаланиб бир томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \to B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

Қатнашувчи B қатнашувчи A дан хабарни олиб айнан у хабарнинг адресати эканлигига ишонч ҳосил қилади; сертификат $cert_A$ дан олинган қатнашувчи A очиқ калитидан фойдаланиб очиқ кўринишда олинган r_A сони, биринчи хабарда жўнатилган r_B сони ва ўзининг идентификатори B остидаги имзо $S_A(r_A, r_B, B)$ нинг корректлигини текширади. Имзо чекилган тасодифий

сон r_A очиқ матнни танлаш билан хужумни олдини олиш учун ишлатилади.

3. Тасодифий сонлардан фойдаланиб икки томонлама аутентификациялаш:

$$A \leftarrow B : r_B$$

$$A \rightarrow B : cert_A, r_A, B, S_A(r_A, r_B, B)$$

$$A \leftarrow B : cert_B, A, S_B(r_A, r_B, A)$$

Ушбу протоколдаги хабарларни ишлаш олдинги протоколдагидек бажарилади.

Назорат саволлари:

1. Қатъий аутентификациялаш муолажаларини тушунтириб беринг.
2. Симметрик алгоритмларга асосланган қатъий аутентификациялаш схемасини тушунтириб беринг.
3. Керберос протоколида доменлараро аутентификациялаш хусусиятилари нимада?
4. Бир томонлама калитли хэш функциялардан фойдаланишга асосланган қатъий аутентификациялаш схемасини тавсифланг.
5. Асимметрик алгоритмларга асосланган қатъий аутентификациялаш протоколлари ишлаш схемасини тушунтириб беринг.
6. Рақамли имзога асосланган қатъий аутентификациялаш протоколини ёритиб беринг.

6.5. Фойдаланувчиларни биометрик идентификациялаш ва аутентификациялаш

Охирги вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қуйидаги афзалликларга эга:

- биометрик аломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;

- биометрик аломатларнинг соғлом шахсдан ажратиб бўлмаслиги;

- биометрик аломатларни сохталаштиришнинг қийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик аломатлар қуйидагилар:

- бармоқ излари;
- қўл панжасининг геометрик шакли;
- юзнинг шакли ва ўлчамлари;
- овоз хусусиятлари;
- кўз ёйи ва тўр пардасининг нақши.

Аутентификациянинг биометрик қисмтизими ишлашининг намунавий схемаси қуйидагича. Тизимда рўйхатга олинишида фойдаланувчидан ўзининг характерли аломатларини бир ёки бир неча марта намойиш қилиниши талаб этилади. Бу аломатлар тизим томонидан қонуний фойдаланувчининг қиёфаси сифатида рўйхатга олинади. Фойдаланувчининг бу қиёфаси тизимда электрон шаклда сақланади ва ўзини қонуний фойдаланувчи деб даъво қилган ҳар бир одамни текширишда ишлатилади. Тақдим этилган аломатлар мажмуаси билан рўйхатга олинганларининг мослиги ёки мос келмаслигига қараб қарор қабул қилинади. Истеъмолчи нуқтаи назаридан биометрик аутенфикациялаш тизими қуйидаги иккита параметр орқали характерланади:

- хатолик инкорлар коэффициенти FRR (false-rejectrate);
- хатолик тасдиқлар коэффициентиFAR (false-alarmrate).

Хатолик инкор тизим қонуний фойдаланувчи шахсини тасдиқламаганда пайдо бўлади (одатда FRR қиймати тахминан 100 дан бирни ташкил этади). *Хатолик тасдиқ* тизим ноқонуний фойдаланувчи шахсини тасдиқлаганида пайдо бўлади (одатда FAP қиймати тахминан 10000 дан бирни ташкил этади). Бу иккала коэффициент бир бири билан боғлиқ: хатолик инкор коэффициентининг ҳар бирига маълум хатолик тасдиқ коэффициенти мос келади. Мукаммал биометрик тизимда иккала хатоликнинг иккала парамет-

ри нулга тенг бўлиши шарт. Афсуски, биометрик тизим идеал эмас, шу сабабли ниманидур қурбон қилишга тўғри келади. Одатда тизимли параметрлар шундай созланадики, мос хатолик инкорлар коэффициентини аниқловчи хатолик тасдиқларнинг исталган коэффициентига эришилади.

Биометрик аутентификациялашнинг дактилоскопик тизими. Биометрик тизимларнинг аксарияти идентификациялаш параметри сифатида бармоқ изларидан фойдаланади (аутентификациянинг дактилоскопик тизими). Бундай тизимлар содда ва қулай, аутентификациялашнинг юқори ишончлилигига эга. Бундай тизимларнинг кенг тарқалишига асосий сабаб бармоқ излари бўйича катта маълумотлар баъзасининг мавжудлигидир. Бундай тизимлардан дунёда асосан полиция, турли давлат ва баъзи банк ташкилотлари фойдаланади.

Аутентификациянинг дактилоскопик тизими қуйидагича ишлайди. Авал фойдаланувчи рўйхатга олинади. Одатда, сканерда бармоқнинг турли холатларида сканерлашнинг бир неча варианти амалга оширилади. Табиийки, намуналар бир–биридан бироз фарқланади ва қандайдир умумлаштирилган намуна, «паспорт» шакллантирилиши талаб этилади. Натижалар аутентификациянинг маълумотлар базасида хотирланади. Аутентификациялашда сканерланган бармоқ изи маълумотлар базасидаги «паспортлар» билан таққосланади.

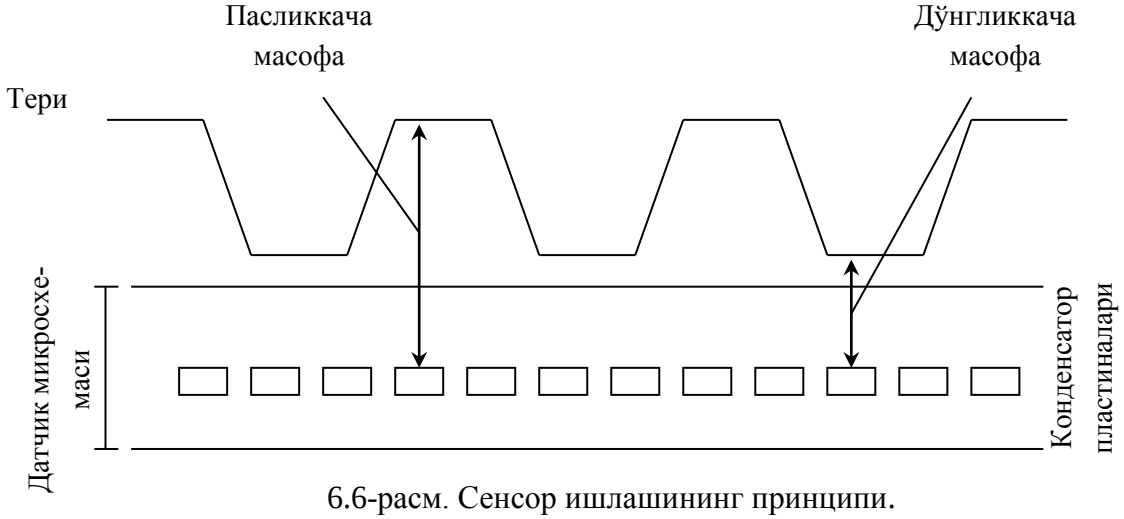
Бармоқ изларининг сканерлари. Бармоқ изларини сканерловчи анъанавий қурилмаларда асосий элемент сифатида бармоқнинг характерли расмини қайдловчи кичкина оптик камера ишлатилади. Аммо, дактилоскопик қурилмаларни ишлаб чиқарувчиларнинг кўпчилиги интеграл схема асосидаги сенсорли қурилмаларга эътибор бермоқдалар. Бундай тенденция бармоқ изларига асосланган аутентификациялашни қўллашнинг янги соҳаларини очади.

Бундай технологияларни ишлаб чиқувчи компаниялар бармоқ изларини олишда турли, хусусан электрик, электромагнит ва бошқа усулларни амалга оширувчи воситалардан фойдаланадилар.

Сканерлардан бири бармоқ изи тасвирини шакллантириш мақсадида тери қисмларининг сиғим қаршилигини ўлчайди. Масалан, Veridicom компаниясининг дактилоскопик қурилмаси ярим-ўтказгичли датчик ёрдамида сиғим қаршилигини аниқлаш орқали ахборотни йиғади. Сенсор ишлашининг принципи қуйидагича: ушбу асбобга қуйилган бармоқ конденсатор пластиналарининг бири вазифасини ўтайди (6.6-расм). Сенсор сиртида жойлашган иккинчи пластина конденсаторнинг 90000 сезгир пластинкали кремний микросхемасидан иборат. Сезгир сиғим датчиклари бармоқ сирти дўнгликлари ва пастликлари орасидаги электрик майдон кучининг ўзгаришини ўлчайди. Натижада дўнгликлар ва пастликларгача бўлган масофа аниқланиб, бармоқ изи тасвири олинади.

Интеграл схема асосидаги сенсорли текширишда AuthenTec компаниясида ишлатилувчи усул аниқликни яна ҳам оширишга имкон беради.

Қатор ишлаб чиқарувчилар биометрик тизимларни смарт-карталар ва карта–калитлар билан комбинациялайдилар.



6.6-расм. Сенсор ишлашининг принципи.

Интеграл схемалар асосидаги бармоқ излари датчикларининг кичик ўлчамлари ва юқори бўлмаган нархи уларни ҳимоя тизими учун идеал интерфейсга айлантиради. Уларни калитлар учун брелокларга ўрнатиш мумкин. Натижада фойдаланувчи компьютердан бошлаб то кириш йўли, автомобил-

лар ва банкоматлар эшикларидан ҳимояли фойдаланишни таъминлайдиган универсал калитга эга бўлади.

Қўл панжасининг геометрик шакли бўйича аутентификациялаш тизимлари. Қўл панжаси шаклини ўқувчи қурилмалар бармоқлар узунлигини, қўл панжа қалинлиги ва юзасини ўлчаш орқали қўл панжасининг ҳажмий тасвирини яратади. Масалан, Recognition Systems компаниясининг маҳсулотлари 90 дан ортиқ ўлчамларни амалга оширади. Натижада кейинги таққослаш учун 9-хонали намуна шакллантирилади. Бу натижа қўл панжасини индивидуал сканерида ёки марказлаштирилган маълумотлар базасида сақланиши мумкин. Қўл панжасини сканерловчи қурилмалар нархининг юқорилиги ва ўлчамларининг катталиги сабабли тармоқ муҳитида камдан-кам ишлатилсада, улар қатъий хавфсизлик режимига ва шиддатли трафикка эга бўлган ҳисоблаш муҳити (сервер хоналари ҳам бунга киради) учун қулай ҳисобланади. Уларнинг аниқлиги юқори ва инкор коэффициенти яъни инкор этилган қонуний фойдаланувчилар фоизи кичик.

Юзнинг тузилиши ва овоз бўйича аутентификацияловчи тизимлар.Бу тизимлар арзонлиги туфайли энг фойдаланувчан ҳисобланадилар, чунки аксарият замонавий компьютерлар видео ва аудео воситаларига эга. Бу синф тизимлари телекоммуникация тармоқларида масофадаги фойдаланувчи субъектни идентификациялаш учун ишлатилади. *Юз тузилишини сканерлаш технологияси* бошқа биометрик технологиялар яроқсиз бўлган иловалар учун тўғри келади. Бу ҳолда шахсни идентификациялаш ва верификациялаш учун кўз, бурун ва лаб хусусиятлари ишлатилади. Юз тузилишини аниқловчи қурилмаларни ишлаб чиқарувчилар фойдаланувчини идентификациялашда ҳусусий математик алгоритмлардан фойдаланадилар.

Маълум бўлишича, кўпгина ташкилотларнинг ҳодимлари юз тузилишини сканерловчи қурилмаларга ишонмайдилар. Уларнинг фикрича камера уларни расмга олади, сўнгра суратни монитор экранига чиқаради. Камеранинг сифати эса паст бўлиши мумкин. Ундан ташқари юз тузилишини

сканерлаш – биометрик аутентификациялаш усуллари ичида ягона, текширишга рухсатни талаб қилмайдиган (яширинган камера ёрдамида амалга оширилиши мумкин) усул ҳисобланали.

Таъкидлаш лозимки, юз тузилишини аниқлаш технологияси янада такомиллаштирилишни талаб этади. Юз тузилишини аниқловчи аксарият алгоритмлар қуёш ёруғлиги жадаллигининг кун бўйича тебраниши натижасидаги ёруғлик ўзгаришига таъсирчан бўладилар. Юз ҳолатининг ўзгариши ҳам аниқлаш натижасига таъсир этади. Юз ҳолатининг 45^0 га ўзгариши аниқлашни самарасиз бўлишига олиб келади.

Овоз бўйича аутентификациялаш тизимлари. Бу тизимлар арзонлиги туфайли фойдаланувчан ҳисобланадилар. Ҳусусан уларни кўпгина шахсий компьютерлар стандарт комплектидаги ускуна (масалан микрофонлар) билан бирга ўрнатиш мумкин. Овоз бўйича аутентификациялаш тизимлари ҳар бир одамга ноёб бўлган баландлиги, модуляцияси ва товуш частотаси каби овоз хусусиятларига асосланади. Овозни аниқлаш нутқни аниқлашдан фарқланади. Чунки нутқни аниқловчи технология абонент сўзини изохласа, овозни аниқлаш технологияси сўзловчининг шахсини тасдиқлайди. Сўзловчи шахсини тасдиқлаш баъзи чегараланишларга эга. Турли одамлар ўхшаш овозлар билан гапириши мумкин, ҳар қандай одамнинг овози вақт мобайнида кайфияти, ҳиссиётлик ҳолати ва ёшига боғлиқ ҳолда ўзгариши мумкин. Унинг устига телефон аппаратларнинг турли-туманлиги ва телефон орқали боғланишларининг сифати сўзловчи шахсини аниқлашни қийинлаштиради. Шу сабабли овоз бўйича аниқлашни юз тузилишини ёки бармоқ изларини аниқлаш каби бошқа усуллар билан биргаликда амалга ошириш мақсадга мувофиқ ҳисобланади.

Кўз ёйи тўр пардасининг шакли бўйича аутентификациялаш тизими. Бу тизимларни иккита синфга ажратиш мумкин:

- кўз ёйи расмидан фойдаланиш;
- кўз тўр пардаси қон томирлари расмидан фойдаланиш.

Одам кўз пардаси аутентификация учун ноёб объект ҳисобланади. Кўз

туби қон томирларининг расми ҳатто эгизакларда ҳам фарқланади. Идентификациялашнинг бу воситаларидан хавфсизликнинг юқори даражаси талаб этилганида (масалан ҳарбий ва мудофаа объектларининг режимли зоналарида) фойдаланилади.

Биометрик ёндашиш “ким бу ким” эканлигини аниқлаш жараёнини соддалаштиришга имкон беради. Дактилоскопик сканерлар ва овозни аниқловчи қурилмалардан фойдаланиш ходимларни тармоққа киришларида мураккаб паролларни эслаб қолишдан халос этади. Қатор компаниялар корхона масштабидаги бир мартали аутентификация SSO (Single Sign-On) га биометрик имкониятларни интеграциялайдилар. Бундай бириктириш тармоқ маъмурларига паролларни бир мартали аутентификациялаш хизматини биометрик технологиялар билан алмаштиришга имкон беради. Шахсни биометрик аутентификациялашнинг биринчилар қаторида кенг тарқалган соҳаларидан бири мобил тизимлари бўлди. Муаммо фақат компьютер ўғирланишидаги йўқотишларда эмас, балки ахборот тизимининг бузилиши катта зарарга олиб келиши мумкин. Ундан ташқари, ноутбуклар дастурий боғланиш (мобил компьютерларда сақланувчи пароллар ёрдамида) орқали корпоратив тармоқдан фойдаланишни тез-тез амалга оширади. Бу муаммоларни кичик, арзон ва катта энергия талаб этмайдиган бармоқ излари датчиклари ечишга имкон беради. Бу қурилмалар мос дастурий таъминот ёрдамида ахборотдан фойдаланишнинг мобил компьютерда сақланаётган тўртта сатхи - рўйхатга олиш, экранни сақлаш режимидан чиқиш, юклаш ва файлларни дешифрациялаш учун аутентификацияни бажаришга имкон беради.

Фойдаланувчини биометрик аутентификациялаш махфий калитдан фойдаланишни модул кўринишида шифрлашда жиддий аҳамиятга эга бўлиши мумкин. Бу модул ахборотдан фақат хақиқий хусусий калит эгасининг фойдаланишига имкон беради. Сўнгра калит эгаси ўзининг махфий калитини ишлатиб хусусий тармоқлар ёки Internet орқали узатилаётган ахборотни шифрлаши мумкин.

Назорат саволлари:

1. Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик аломатлар?
2. Биометрик аутентификациялашнинг дактилоскопик тизими ишлаш схемасини тушунтириб беринг.
3. Қўл панжасининг геометрик шакли бўйича аутентификациялаш тизимларини тушунтириб беринг.
4. Юз тузилиши бўйича аутентификациялаш тизимларининг ишлаш принципини тушунтириб беринг.
5. Овоз бўйича аутентификациялаш тизимлари хусусиятлари.
6. Кўз ёйи тўр пардасининг нақши бўйича аутентификациялаш тизимни ёритиб беринг.

VII боб. КОМПЬЮТЕР ВИРУСЛАРИ ВА ЗАРАРКУНАНДА ДАСТУРЛАР БИЛАН КУРАШИШ МЕХАНИЗМЛАРИ

7.1. Компьютер вируслари ва вирусдан ҳимояланиш муаммолари

Компьютер вирусининг кўп таърифлари мавжуд. Биринчи таърифни 1984 йили Фред Коэн берган: "Компьютер вируси – бошқа дастурларни, уларга ўзини ёки ўзгартирилган нусхасини киритиш орқали, уларни модификациялаш билан заҳарловчи дастур. Бунда киритилган дастур кейинги кўпайиш қобилиятини сақлайди". Вируснинг ўз-ўзидан кўпайиши ва ҳисоблаш жараёнини модификациялаш қобилияти бу таърифдаги таянч тушунчалар ҳисобланади. Компьютер вирусининг ушбу хусусиятлари тирик табиат организмларида биологик вирусларнинг паразитланишига ўҳшаш.

Ҳозирда компьютер вируси деганда қуйидаги хусусиятларга эга бўлган дастурий код тушунилади:

- аслига мос келиши шарт бўлмаган, аммо аслининг хусусиятларига (ўз-ўзини тиклаш) эга бўлган нусхаларни яратиш қобилияти;

- ҳисоблаш тизимининг бажарилувчи объектларига яратилувчи нусхаларнинг киритилишини таъминловчи механизмларнинг мавжудлиги.

Таъкидлаш лозимки, бу хусусиятлар зарурий, аммо етарли эмас. Кўрсатилган хусусиятларни ҳисоблаш муҳитидаги зарар келтирувчи дастур таъсирининг деструктивлик ва сир бой бермаслик хусусиятлари билан тўлдириш лозим.

Вирусларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

- яшаш макони;

- операцион тизим;

- ишлаш алгоритми хусусияти;

- деструктив имкониятлари.

Компьютер вирусларини яшаш макони, бошқача айтганда вируслар киритилувчи компьютер тизими объектларининг хили бўйича туркумлаш асосий ва кенг тарқалган туркумлаш ҳисобланади (7.1-расм).

7.1-расм. Яшаш макони бўйича компьютер вирусларининг туркумланиши.

Файл вируслари бажарилувчи файлларга турли усуллар билан киритилади (энг кўп тарқалган вируслар хили), ёки файл-йўлдошларни (компаньон вируслар) яратади ёки файлли тизимларни (link-вируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар ўзини дискнинг юклама секторига (boot - секторига) ёки винчестернинг тизимли юкловчиси (MasterBootRecord) бўлган секторга ёзади. Юклама вируслар тизим юкланишида бошқаришни олувчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макродастурларини ва файлларини, хусусан MicroSoftWord, MicroSoftExcel ва ҳ. каби оммавий муҳаррирларнинг файл-хужжатларини ва электрон жадвалларини заҳарлайди.

Тармоқ вируслари ўзини тарқатишда компьютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзида тармоқ

вирусларини "қурт" хилидаги дастурлар деб юритишади. Тармоқ вируслари Internet-қуртларга (Internet бўйича тарқалади), IRC-қуртларга (чатлар, InternetRelayChat) бўлинади.

Компьютер вирусларининг кўпгина комбинацияланган хиллари ҳам мавжуд, масалан – тармоқли макровирус таҳрирланувчи хужжатларни захарлайди, ҳамда ўзининг нусхаларини электрон почта орқали тарқатади. Бошқа бир мисол сифатида файл-юклама вирусларини кўрсатиш мумкинки, улар файлларни ҳамда дискларнинг юкланадиган секторини заҳарлайди.

*Вирусларнинг ҳаёт даври.*Ҳар қандай дастурдагидек компьютер вируслари ҳаёт даврининг иккита асосий босқичини - сақланиш ва бажарилиш босқичларини ажратиш мумкин.

Сақланиш босқичи вируснинг дискда у киритилган объект билан биргаликда шундайгина сақланиш даврига тўғри келади. Бу босқичда вирус вирусга қарши дастур таъминотига заиф бўлади, чунки у фаол эмас ва ҳимояланиш учун операцион тизимни назорат қила олмайди.

Компьютер вирусларининг *бажарилиш даври*, одатда, бешта босқични ўз ичига олади:

1. Вирусни хотирага юклаш.
2. Қурбонни қидириш.
3. Топилган қурбонни заҳарлаш.
4. Деструктив функцияларни бажариш.
5. Бошқаришни вирус дастур-элтувчисига ўтказиш.

Вирусни хотирага юклаш. Вирусни хотирага юклаш операцион тизим ёрдамида вирус киритилган бажарилувчи объект билан бир вақтда амалга оширилади. Масалан, агар фойдаланувчи вирус бўлган дастурий файлни ишга туширса, равшанки, вирус коди ушбу файл қисми сифатида хотирага юкланади. Оддий ҳолда, вирусни юклаш жараёни-дискдан оператив хотирага нусхалаш бўлиб, сўнгра бошқариш вирус бадани кодига узатилади. Бу ҳаракатлар операцион тизим томонидан бажарилади, вируснинг ўзи пассив ҳолатда бўлади. Мураккаброқ вазифаларда вирус бошқаришни олганидан сўнг

ўзининг ишлаши учун қўшимча ҳаракатлар бажариши мумкин. Бу билан боғлиқ иккита жиҳат кўрилади.

Биринчиси вирусларни аниқлаш муолажасининг максимал мураккаблашиши билан боғлиқ. Сақланиш босқичида баъзи вируслар ҳимояланишни таъминлаш мақсадида етарлича мураккаб алгоритмдан фойдаланади. Бундай мураккаблашишга вирус асосий қисмини шифрлашни киритиш мумкин. Аммо фақат шифрлашни ишлатиш чала чора ҳисобланади, чунки юкланиш босқичида расшифровкани таъминловчи вирус қисми очиқ кўринишда сақланиши лозим. Бундай ҳолатдан қутилиш учун вирусларни ишлаб чиқувчилар расшифровка қилувчи кодни "мутациялаш" механизмидан фойдаланади. Бу усулнинг моҳияти шундан иборатки, объектга вирус нусхаси киритилишида унинг расшифровка қилувчига тааллуқли қисми шундай модификацияланадики, оригинал билан матнли фарқланиш пайдо бўлади, аммо иш натижаси ўзгармайди.

Кодни мутациялаш механизмидан фойдаланувчи вируслар *полиморф вируслар* номини олган. Полиморф вируслар (polymorphic)-қийин аниқланадиган вируслар бўлиб, сигнатураларга эга эмас, яъни таркибида бирорта ҳам кодининг доимий қисми йўқ. Полиморфизм файлли, юкламали ва макровирусларда учрайди.

Стелс-алгоритмлардан фойдаланилганда вируслар ўзларини тизимда тўла ёки қисман бекитишлари мумкин. стелс-алгоритмларидан фойдаланадиган вируслар – *стелс-вируслар* (Stealth) деб юритилади. Стелс вируслар операцион тизимнинг шикастланган файлларга мурожаатини ушлаб қолиш йўли билан ўзини яшаш маконидалигини яширади ва операцион тизимни ахборотни шикастланмаган қисмига йўналтиради.

Иккинчи жиҳат *резидент вируслар* деб аталувчи вируслар билан боғлиқ. Вирус ва у киритилган объект операцион тизим учун бир бутун бўлганлиги сабабли, юкланишдан сўнг улар, табиий, ягона адрес маконида жойлашади. Объект иши тугаганидан сўнг у оператив хотирадан бўшалади. Бунда бир вақтнинг ўзида вирус ҳам бўшалиб сақланишнинг пассив босқичи-

га ўтади. Аммо баъзи вируслар хили хотирада сақланиш ва вирус элтувчи иши тугашидан сўнг фаол қолиш қобилиятига эга. Бундай вируслар резидент номини олган. Резидент вируслар, одатда, фақат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш маконини заҳарлайди ва маълум шароитларда зараркунандалик вазифасини бажаради. Резидент вируслар хотирада жойлашади ва компьютер ўчирилишигача ёки операцион тизим қайта юкланишигача фаол ҳолда бўлади.

Резидент бўлмаган вируслар фақат фаоллашган вақтларида хотирага тушиб заҳарлаш ва заракунандалик вазифаларини бажаради. Кейин бу вируслар хотирани бутунлай тарк этиб яшаш маконида қолади.

Таъкидлаш лозимки, вирусларни резидент ва резидент бўлмаганларга ажратиш фақат файл вирусларига тааллуқли. Юкланучи ва макровируслар резидент вирусларга тегишли.

Қурбонни қидириш.Қурбонни қидириш усули бўйича вируслар иккита синфга бўлинади. Биринчи синфга операцион тизим функцияларидан фойдаланиб фаол қидиришни амалга оширувчи вируслар киради. Иккинчи синфга қидиришнинг пассив механизмларини амалга оширувчи, яъни дастурий файлларга тузоқ қўювчи вируслар тааллуқли.

Топилган қурбонни заҳарлаш. Оддий ҳолда заҳарлаш деганда қурбон сифатида танланган объектда вирус кодининг ўз-ўзини нусхалаши тушунилади.

Аввал файл вирусларининг заҳарлаш хусусиятларини кўрайлик. Бунда иккита синф вируслари фарқланади. Биринчи синф вируслари ўзининг кодини дастурий файлга бевосита киритмайди, балки файл номини ўзгартириб, вирус бадани бўлган янги файлни яратади. Иккинчи синфга қурбон файлларига бевосита кирувчи вируслар тааллуқли. Бу вируслар киритилиш жойлари билан характерланади. Қуйидаги вариантлар бўлиши мумкин:

1. Файл бошига киритиш. Ушбу усул MS-DOSнинг *com*-файллари учун энг қулай ҳисобланади, чунки ушбу форматда хизматчи сарлавҳалар кўзда тутилган.

2. Файл охирига киритиш. Бу усул энг кўп тарқалган бўлиб, вируслар кодига бошқаришни узатиш дастурнинг биринчи командаси (*com*) ёки файл сарлавҳасини (*exe*) модификациялаш орқали таъминланади.

3. Файл ўртасига киритиш. Одатда бу усулдан вируслар структураси олдиндан маълум файлларга (масалан, *Command.com* файли) ёки таркибида бир хил қийматли байтлар кетма-кетлиги бўлган, узунлиги вирус жойлашишига етарли файлларга татбиқан фойдаланилди.

Юклама вируслар учун заҳарлаш босқичининг хусусиятлари улар киритилувчи объектлар – қайишқоқ ва қаттиқ дискларнинг юкланиш секторларининг сифати ва қаттиқ дискнинг бош юклама ёзуви (MBR) орқали аниқланади. Асосий муаммо-ушбу объект ўлчамларининг чегараланганлиги. Шу сабабли, вируслар ўзларининг қурбон жойида сиғмаган қисмини дискда сақлаши, ҳамда заҳарланган юкловчи оригинал кодини ташиши лозим.

Макровируслар учун заҳарлаш жараёни танланган хужжат-қурбонда вирус кодини сақлашдан иборат. Баъзи ахборотни ишлаш дастурлари учун буни амалга ошириш осон эмас, чунки хужжат файллари форматининг макропрограммаларни сақлаши кўзда тутилмаган бўлиши мумкин.

Деструктив функцияларни бажариш. Деструктив имкониятлари бўйича безиён, хавфсиз, хавфли ва жуда хавфли вируслар фарқланади.

Безиён вируслар - ўз-ўзидан тарқалиш механизми амалга оширилувчи вируслар. Улар тизимга зарар келтирмайди, фақат дискдаги бўш хотирани сарфлайди холос.

Хавфсиз вируслар – тизимда мавжудлиги турли таассурот (овоз, видео) билан боғлиқ вируслар, бўш хотирани камайтирсада, дастур ва маълумотларга зиён етказмайди.

Хавфли вируслар – компьютер ишлашида жиддий нуқсонларга сабаб бўлувчи вируслар. Натижада дастур ва маълумотлар бузилиши мумкин.

Жуда хавфли вируслар – дастур ва маълумотларни бузилишига ҳамда компьютер ишлашига зарур ахборотни ўчирилишига бевосита олиб келувчи, муолажалари олдиндан ишлаш алгоритмларига жойланган вируслар.

Бошқаришни вирус дастур – элтувчисига ўтказиш. Таъкидлаш лозимки, вируслар бузувчилар ва бузмайдиганларга бўлинади.

Бузувчи вируслар дастурлар заҳарланганида уларнинг ишга лаёқатлигини сақлаш хусусида қайғурмайдилар, шу сабабли уларга ушбу босқичнинг маъноси йўқ.

Бузмайдиган вируслар учун ушбу босқич хотирада дастурни коррект ишланиши шарт бўлган кўринишда тиклаш ва бошқаришни вирус дастур-элтувчисига ўтқазиш билан боғлиқ.

Зарар келтирувчи дастурларнинг бошқа хиллари. Вируслардан ташқари зарар келтирувчи дастурларнинг қуйидаги хиллари мавжуд:

- троян дастурлари;

- мантиқий бомбалар;

- масофадаги компьютерларни яширинча маъмурловчи хакер утилиталари;

- Internetдан ва бошқа конфиденциал ахборотдан фойдаланиш паролларини ўғриловчи дастурлар.

Улар орасида аниқ чегара йўқ: троян дастурлари таркибида вируслар бўлиши, вирусларга мантиқий бомбалар жойлаштирилиши мумкин ва ҳ.

Троян дастурлар ўзлари кўпаймайди ва тарқатилмайди. Ташқаридан троян дастурлар мутлақо беозор кўринади, ҳатто фойдали функцияларни тавсия этади. аммо фойдаланувчи бундай дастурни компьютерига юклаб, ишга туширса, дастур билдирмай зарар келтирувчи функцияларни бажариши мумкин. Кўпинча троян дастурлар вирусларни дастлабки тарқатишда, Internet орқали масофадаги компьютердан фойдаланишда, маълумотларни ўғрилашда ёки уларни йўқ қилишда ишлатилади.

Мантиқий бомба – маълум шароитларда зарар келтирувчи ҳаракатларни бажарувчи дастур ёки унинг алоҳида модуллари. Мантиқий бомба, масалан, маълум сана келганда ёки маълумотлар базасида ёзув пайдо бўлганида ёки йўқ бўлганида ва ҳ. ишга тушиши мумкин. Бундай бомба вирусларга, троян дастурларга ва оддий дастурларга жойлаштирилиши

мумкин.

Вируслар ва зарар келтирувчи дастурларни тарқатиш каналлари. Компьютерлар ва корпоратив тармоқларни ҳимояловчи самарадор тизимни яратиш учун қаердан хавф туғилишини аниқ тасаввур этиш лозим. Вируслар тарқалишнинг жуда хилма-хил каналларини топади. Бунинг устига эски усулларга янгиси қўшилади.

Тарқатишнинг классик (муттоз) усуллари. Файл вируслари дастур файллари билан биргаликда дискетлар ва дастурлар алмашишда, тармоқ каталогларидан, Web- ёки FTP – серверлардан дастурлар юкланишида тарқатилади. Юклама вируслар компьютерга фойдаланувчи заҳарланган дискетани дисководда қолдириб, сўнгра операцион тизимни қайта юклашида тушиб қолади. Юклама вирус компьютерга вирусларнинг бошқа хили орқали киритилиши мумкин. Макрокоманда вируслари MicroSoftWord, Excel, Access файллари каби офис хужжатларининг захарланган файллари алмашинишида тарқалади.

Агар заҳарланган компьютер локал тармоққа уланган бўлса вирус осонгина файл-сервер дискларига тушиб қолиши, у ердан каталоглар орқали тармоқнинг барча компьютерларига ўтиши мумкин. Шу тариқа вирус эпидемияси бошланади. Вирус тармоқда шу вирус тушиб қолган компьютер фойдаланувчиси хуқуқлари каби хуқуққа эга эканлигини тизим маъмури унутмаслиги лозим. Шунинг учун у фойдаланувчи фойдаланадиган барча каталогларга тушиб қолиши мумкин. Агар вирус тармоқ маъмури ишчи станциясига тушиб қолса оқибати жуда оғир бўлиши мумкин.

Электрон почта.

Ҳозирда Internet глобал тармоғи вирусларнинг асосий манбаи ҳисобланади. Вируслар билан заҳарланишларнинг аксарияти MicroSoftWord форматида хатлар алмашишда содир бўлади. Электрон почта макровирусларни тарқатиш канали вазифасини ўтайди, чунки ахборот билан бир қаторда кўпинча офис хужжатлари жўнатилади.

Вируслар билан заҳарлаш билмасдан ва ёмон ниятда амалга оширили-

ши мумкин. Масалан, макровирус билан заҳарланган муҳарриридан фойдаланувчи ўзи шубҳа қилмаган ҳолда, адресатларга заҳарланган хатларни жўнатиши мумкин. Иккинчи тарафдан нияти бузуқ одам атайин электрон почта орқали ҳарқандай хавфли дастурий кодни жўнатиши мумкин.

Троян Web-сайтлар. Фойдаланувчилар вирусни ёки троян дастурни Internet сайтларининг оддий кузатишда, троян Web-сайтни кўрганида олиши мумкин. Фойдаланувчи браузерларидаги хатоликлар кўпинча троян Web-сайтлари фаол компонентларининг фойдаланувчи компьютерларига зарар келтирувчи дастурларни киритишига сабаб бўлади. Троян сайтни кўришга таклифни фойдаланувчи оддий электрон хат орқали олиши мумкин.

Локал тармоқлар.

Локал тармоқлар ҳам тезликда заҳарланиш воситаси ҳисобланади. Агар ҳимоянинг зарурий чоралари кўрилмаса, заҳарланган ишчи станция локал тармоққа киришда сервердаги бир ёки бир неча хизматчи файлларни заҳарлайди. Бундай файллар сифатида Login.com хизматчи файлни, фирмада қўлланилувчи Excel-жадваллар ва стандарт хужжат-шаблонларни кўрсатиш мумкин. Фойдаланувчилар бу тармоққа киришида сервердан заҳарланган файлларни ишга туширади, натижада вирус фойдаланувчи компьютеридан фойдалана олади.

Зарар келтирувчи дастурларни тарқатишнинг бошқа каналлари.

Вирусларни тарқатиш каналларидан бири дастурий таъминотнинг қароқчи нусхалари ҳисобланади. Дискетлар ва CD-дисклардаги ноқунуний нусхаларда кўпинча турли-туман вируслар билан заҳарланган файллар бўлади. Вирусларни тарқатиш манбаларига электрон анжуманлар ва FTP ва BBS файл-серверлар ҳам тааллуқли.

Ўқув юртларида ва Internet-марказларида ўрнатилган ва умумфойдаланиш режимида ишловчи компьютерлар ҳам осонгина вирусларни тарқатиш манбаига айланиши мумкин. Агар бундай компьютерлардан бири навбатдаги фойдаланувчи дискетидан заҳарланган бўлса, шу компьютерда ишловчи бошқа фойдаланувчилар дискетлари ҳам заҳарланади.

Компьютер технологиясининг ривожланиши билан компьютер вируслари ҳам, ўзининг янги яшаш маконига мослашган ҳолда, такомиллашади. Ҳар қандай онда янги, олдин маълум бўлмаган ёки маълум бўлган, аммо янги компьютер асбоб-ускунасига мўлжалланган компьютер вируслари, троян дастурлари ва қуртлар пайдо бўлиши мумкин. Янги вируслар маълум бўлмаган ёки олдин мавжуд бўлмаган тарқатиш каналларидан ҳамда компьютер тизимларга татбиқ этишнинг янги технологияларидан фойдаланиши мумкин. Вирусдан заҳарланиш хавфини йўқотиш учун корпоратив тармоқнинг тизим маъмури, нафақат вирусга қарши усуллардан фойдаланиши, балки компьютер вируслари дунёсини доимо кузатиб бориши шарт.

Назорат саволлари:

1. Компьютер вируси ва зарар келтирувчи дастурлар тушунчаси.
2. Компьютер вирусларини қайси асосий аломатларига кўра туркумлаш мумкин?
3. Компьютер вирусини бажарилиш даври қандай босқичларни ўз ичига олади?
4. Зарар келтирувчи дастур турларини ва уларнинг ишлаш принципини тушунтириб беринг.
5. Компьютер вируслари ва зарар келтирувчи дастурларни тарқалиш каналларини тушунтириб беринг.

7.2. Вирусга қарши дастурлар

Компьютер вирусларини аниқлаш ва улардан ҳимояланиш учун махсус дастурларнинг бир неча хиллари ишлаб чиқилган бўлиб, бу дастурлар компьютер вирусларини аниқлаш ва йўқотишга имкон беради. Бундай дастурлар вирусга қарши дастурлар деб юритилади. Умуман, барча вирусга қарши дастурлар заҳарланган дастурларнинг ва юклама секторларнинг автоматик тарзда тикланишини таъминлайди.

Вирусларга қарши дастурлар фойдаланадиган вирусларни

аниқлашнинг асосий усуллари қуйидагилар:

- эталон билан таққослаш усули;

- эвристик тахлил;

- вирусга қарши мониторинг;

- ўзгаришларни аниқловчи усул;

- компьютернинг киритиш/чиқариш базавий тизимига (BIOSга) вирусга қарши воситаларни ўрнатиш ва ҳ.

Эталон билан таққослаш усули энг оддий усул бўлиб, маълум вирусларни қидиришда ниқоблардан фойдаланади. Вируснинг ниқоби-мана шу муайян вирусга хос коднинг қандайдир ўзгармас кетма-кетлигидир. Вирусга қарши дастур маълум вирус ниқобларини қидиришда текширилувчи файлларни кетма-кет кўриб чиқади (сканерлайди). Вирусга қарши сканерлар фақат ниқоб учун белгиланган, олдиндан маълум вирусларни топа олади. Оддий сканерлар компьютерни янги вирусларнинг суқилиб киришидан ҳимояламайди. Янги дастурни ёки юклама секторини заҳарлашда кодини тўла ўзгартира олувчи шифрланувчи ва полиморф вируслар учун ниқоб ажратиш мумкин эмас. Шу сабабли сканер уларни аниқламайди.

Эвристик таҳлил. Компьютер вируси кўпайиши учун хотирада нусхаланиш, секторга ёзилиш каби қандайдир муайян харакатларни амалга ошириши лозим. Эвристик таҳлиллагичда бундай ҳаракатларнинг рўйхати мавжуд. Эвристик таҳлиллагич дастурларни ва диск ва дискет юклама секторларини, уларда вирусга хос кодларни аниқлашга уринган ҳолда, текширади. Тахлиллагич заҳарланган файлни топиб, монитор экранига ахборот чиқаради ва шахсий ёки тизимли журналга ёзади. Эвристик тахлил олдин маълум бўлмаган вирусларни аниқлайди.

Вирусга қарши мониторинг. Ушбу усулнинг моҳияти шундан иборатки, компьютер хотирасида бошқа дастурлар томонидан бажарилувчи шубҳали ҳаракатларни мониторингловчи вирусга қарши дастур доимо бўлади. Вирусга қарши мониторинг барча ишга туширилувчи дастурларни, яратилувчи, очилувчи ва сақланувчи хужжатларни, Internet орқали олинган ёки

дискетдан ёки ҳар қандай компакт-дискдан нусҳаланган дастур ва ҳужжатларнинг файлларини текширишга имкон беради. Агар қандайдир дастур хавфли ҳаракат қилишга уринмоқчи бўлса, вирусга қарши монитор фойдаланувчига хабар беради.

Ўзгаришларни аниқловчи усул. Дискни тафтиш қилувчи деб аталувчи ушбу усулни амалга оширишда вирусга қарши дастур дискнинг хужумга дучор бўлиши мумкин бўлган барча соҳаларини олдиндан хотирлайди, сўнгра уларни вақти-вақти билан текширади. Вирус компьютерларни заҳарлаганида қаттиқ диск таркибини ўзгартиради: масалан, дастур ёки хужжат файлига ўзининг кодини қўшиб қўяди, Autoexec.bat файлига дастур-вирусни чақиришни қўшади, юклама секторни ўзгартиради, файл-йўлдош яратади. Диск соҳалари характеристикаларининг қийматлари солиштирилганида вирусга қарши дастур маълум ва ноъмалум вируслар томонидан қилинган ўзгаришларни аниқлаши мумкин.

Компьютерларнинг киритиш/чиқариш базавий тизимига (BIOSга) вирусга қарши воситаларни ўрнатиш. Компьютерларнинг тизимли платасига вируслардан ҳимоялашнинг оддий воситалари ўрнатилади. Бу воситалар қаттиқ дискларнинг бош юклама ёзувига ҳамда дисклар ва дискетларнинг юклама секторларига барча мурожаатларни назоратлашга имкон беради. Агар қандайдир дастур юклама секторлар таркибини ўзгартиришга уринса, ҳимоя ишга тушади ва фойдаланувчи огоҳлантирилади. Аммо бу ҳимоя жуда ҳам ишончли эмас.

Вирусга қарши дастур хиллари. Вирусга қарши дастурларнинг қуйидаги хиллари фарқланади:

- дастур-фаглар (вирусга қарши сканерлар);
- дастур-тафтишчилар (CRC-сканерлар);
- дастур-блокировка қилувчилар;
- дастур-иммунизаторлар.

Дастур-фаглар энг оммавий ва самарали вирусга қарши дастур ҳисобланади. Самарадорлиги ва оммавийлиги бўйича иккинчи ўринда дастур-

тафтишчилар туради. Одатда, бу иккала дастур хиллари битта вирусга қарши дастурга бирлаштирилади, натижада унинг қуввати анчагина ошади. Турли хил блокировка қилувчилар ва иммунизаторлар ҳам ишлатилади.

Дастур-фаглар (сканерлар) вирусларни аниқлашда эталон билан таққослаш усулидан, эвристик тахлиллашдан ва бошқалардан фойдаланади. Дастур-фаглар оператив хотира ва файлларни сканерлаш йўли билан муайян вирусга характерли бўлган ниқобни қидиради. Дастур-фаглар нафақат вируслар билан заҳарланган файлларни топади, балки уларни даволайди ҳам, яъни файлдан дастур-вирус баданини олиб ташлаб, файлни дастлабки холатига қайтаради. Дастур-фаглар аввал оператив хотирани сканерлайди, вирусларни аниқлайди ва уларни йўқотади, сўнгра файлларни даволашга киришади. Файллар ичида вирусларни катта сонини қидиришга ва йўқ қилишга аталган дастур-фаглар, яъни полифаглар ҳам мавжуд.

Дастур-фаглар иккита категорияга бўлинади: универсал ва ихтисослаштирилган сканерлар. Универсал сканерлар, сканер ишлаши мўлжалланган операцион тизим хилига боғлиқ бўлмаган ҳолда, вирусларнинг барча хилларини қидиришга ва зарарсизлантиришга мўлжалланган. Ихтисослаштирилган сканерлар вирусларнинг чегараланган сонини ёки уларнинг бир синфини, масалан макровирусларни зарарсизлантиришга аталган. Фақат макровирусларга мўлжалланган ихтисослаштирилган сканерлар MSWORD ва Excel муҳитларида хужжат алмашиниш тизимини ҳимоялашда энг қулай ва ишончли ечим ҳисобланади.

Дастур-фаглар сканерлашни "бир зумда" бажарувчи мониторинглашнинг резидент воситаларига ва фақат сўров бўйича тизимни текширишни таъминловчи резидент бўлмаган сканерларга ҳам бўлинади. Мониторинглашнинг резидент воситалари тизимни ишончлироқ ҳимоялашни таъминлайди, чунки улар вируслар пайдо бўлишига дарров реакция кўрсатади, резидент бўлмаган сканер эса вирусни аниқлаш қобилиятига фақат навбатдаги ишга туширилишида эга бўлади.

Дастур-фагларнинг афзаллиги сифатида уларнинг универсаллигини

кўрсатиш мумкин. Дастур-фагларнинг камчилиги сифатида вирусларни қидириш тазлигининг нисбатан катта эмаслигини ва вирусга қарши базаларнинг нисбатан катта ўлчамларини кўрсатиш мумкин. Ундан ташқари, янги вирусларнинг доим пайдо бўлиши сабабли дастур-фаглар тездан эскиради ва улар версияларининг мунтазам янгиланиши талаб этилади.

Дастур-тафтишчилар (CRC-сканерлар) вирусларни қидиришда ўзгаришларни аниқловчи усулдан фойдаланади. CRC-сканерлар дискдаги файллар/тизимли сектордагилар учун CRC-йиғиндини (циклик назорат кодини) ҳисоблашга асосланган. Бу CRC-йиғиндилар вирусга қарши маълумотлар баъзасида файллар узунлиги, саналар ва охирги модификацияси ва бошқа параметрлар хусусидаги қўшимча ахборотлар билан бир қаторда сақланади. CRC-сканерлар ишга туширилишида маълумотлар базасидаги маълумот билан реал ҳисобланган қийматларни таққослайди. Агар маълумотлар базасидаги ёзилган файл хусусидаги ахборот реал қийматларга мос келмаса, CRC-сканерлар файл ўзгартирилганлиги ёки вирус билан заҳарланганлиги хусусида хабар беради. Одатда холатларни таққослаш операцион тизим юкланишдан сўнг дарҳол ўтказилади.

CRC-сканерларнинг камчилиги сифатида уларнинг янги файллардаги вирусларни аниқлай олмаслигини кўрсатиш мумкин, чунки уларнинг маълумотлар базасида бу файллар хусусидаги ахборот мавжуд эмас.

Дастур-блокировка қилувчилар вирусга қарши мониторинглаш усулини амалга оширади. Вирусга қарши блокировка қилувчилар резидент дастурлар бўлиб, вирус хавфи вазиятларини тўхтатиб қолиб, у хусусида фойдаланувчига хабар беради. Вирус хавфи вазиятларига вирусларнинг кўпайиши онлардаги характерли чақириқлар киради. Блокировка қилувчиларнинг афзалликлари сифатида вируслар кўпайишининг илк босқичида уларни тўхтатиб қолишини кўрсатиш мумкин. Бу айниқса, кўпдан бери маълум вируснинг мунтазам пайдо бўлишида муҳим ҳисобланади. Аммо, улар файл ва дискларни даволамайди. Блокировка қилувчиларнинг камчилиги сифатида улар ҳимоясининг айланиб ўтиш йўлларининг мавжудлигини ва уларнинг "хира-

ликлигини" (масалан, улар бажарилувчи файлларнинг ҳарқандай нусхаланишига уриниш хусусида мунтазам огоҳлантиради) кўрсатиш мумкин. Таъкидлаш лозимки, компьютер аппарат компоненти сифатида яратилган вирусга қарши блокировка қилувчилар мавжуд.

Дастур-иммунизаторлар – файллар заҳарланишини олдини олувчи дастурлар икки хилга бўлинади: заҳарланиш хусусида хабар берувчи ва вируснинг қандайдир хили бўйича заҳарланишни блокировка қилувчи. Биринчи хил иммунизаторлар, одатда, файл охирига ёзилади ва файл ишга туширилганда ҳар марта унинг ўзгаришини текширади. Бундай иммунизаторлар битта жиддий камчиликка эга. Улар стелс-вирус билан захарланишни аниқлай олмайдилар. Шу сабабли бу хил иммунизаторлар ҳозирда ишлатилмайди.

Иккинчи хил иммунизаторлар тизимни вируснинг маълум тури билан заҳарланишдан ҳимоялайди. Бу иммунизатор дастур ёки дискни шундай модификациялайдики, бу модификациялаш уларнинг ишига таъсир этмайди, вирус эса уларни заҳарланган деб қабул қилади ва суқилиб кирмайди. Иммунизациялашнинг бу хили универсал бўлаолмайди, чунки файлларни барча маълум вируслардан иммунизациялаш мумкин эмас. Аммо бундай иммунизаторлар чала чора сифатида компьютерни янги ноъмалум вирусдан, у вирусга қарши сканерлар томонидан аниқланишига қадар, ишончли ҳимоялаши мумкин.

Вирусга қарши дастурнинг сифат мезонлари. Вирусга қарши дастурни бир неча мезонлар бўйича баҳолаш мумкин. Қуйида бу мезонлар муҳимлиги даражаси пасайиши тартибда келтирилган:

- ишончлилик ва ишлаш қулайлиги - фойдаланувчилардан махсус ҳаракатларни талаб этувчи техник муаммоларнинг йўқлиги; вирусга қарши дастурнинг ишончлилиги энг муҳим мезон ҳисобланади, чунки ҳатто энг яхши вирусга қарши дастур сканерлаш жараёнини охиригача олиб бора олмаса, у бефойда ҳисобланади;

- вирусларни барча тарқалган хилларини аниқлаш фазилати, ички

файл-хужжатлар/жадвалларни (MSOffice), жойлаштирилган ва архивланган файлларни сканерлаш, вирусга қарши дастурнинг асосий вазифаси-100% вирусларни аниқлаш ва уларни даволаш;

- барча оммавий платформалар (DOS, Windows 95/NT, NovellNetWare, OS/2, Alpha, Linux ва ҳ.) учун вирусга қарши дастур версияларининг мавжудлиги; сўров бўйича сканерлаш ва "бир зумда" сканерлаш режимларининг борлиги, тармоқни маъмурлаш имкониятли сервер версияларининг мавжудлиги. Вирусга қарши дастурнинг кўп платформалилиги муҳим мезон ҳисобланади, чунки муайян операцион тизимга мўлжалланган дастургина бу тизим функцияларидан тўла фойдаланиш мумкин. Файлларни "бир зумда" текшириш имконияти ҳам вирусга қарши дастурларнинг етарлича муҳим мезони ҳисобланади. Компьютерга келувчи файлларни ва қўйилувчи дискетларни бир лаҳзада ва мажбурий текшириш вирусдан заҳарланмасликка 100%-ли кафолат беради. Агар вирусга қарши дастурнинг сервер вариантида тармоқни маъмурлаш имконияти бўлса, унинг қиймати янада ошади;

- ишлаш тезлиги. Вирусга қарши дастурнинг ишлаш тезлиги ҳам унинг муҳим мезони ҳисобланади. Турли вирусга қарши дастурларда вирусни қидиришнинг ҳар хил алгоритмларидан фойдаланилади. Бир алгоритм тезкор ва сифатли бўлса, иккинчиси суст ва сифати паст бўлиши мумкин.

Ҳимоянинг профилактика чоралари.Ҳар бир компьютерда вируслар билан заҳарланган файллар ва дискларни ўз вақтида аниқлаш, аниқланган вирусларни тамомила йўқотиш вирус эпидемиясининг бошқа компьютерларга тарқалишининг олдини олади. Ҳар қандай вирусни аниқлашни ва йўқ қилишни кафолатловчи мутлоқ ишончли дастурлар мавжуд эмас. Компьютер вируслари билан курашишнинг муҳим усули ўз вақтидаги профилактика ҳисобланади.

Вирусдан заҳарланиш эҳтимоллигини жиддий камайтириш ва дисклардаги ахборотни ишончли сақланишини таъминлаш учун қуйидаги профилактика чораларини бажариш лозим:

- фақат қонуний, расмий йўл билан олинган дастурий таъминотдан

фойдаланиш;

- компьютерни замонавий вирусга қарши дастурлар билан таъминлаш ва улар версияларини доимо янгилаш;

- бошқа компьютерларда дискетда ёзилган ахборотни ўқишдан один бу дискетда вирус борлигини ўзининг компьютеридаги вирусга қарши дастур ёрдамида доимо текшириш;

- ахборотни иккилаш. Аввало дастурий таъминотнинг дистрибутив элтувчиларини сақлашга ва ишчи ахборотнинг сақланишига эътибор бериш;

- компьютер тармоқларидан олинувчи барча бажарилувчи файлларни назоратлашда вирусга қарши дастурдан фойдаланиш;

- компьютерни юклама вируслардан заҳарланишига йўл қўймаслик учун, операцион тизим ишга туширилганида ёки қайта юкланишида дисковод чўнтагида дискетани қолдирмаслик.

Вирусга қарши дастурларнинг ҳар бири ўзининг афзалликларига ва камчиликларига эга. Фақат вирусга қарши дастурларнинг бир неча хилини комплекс ишлатилиши мақбул натижага олиб келиши мумкин.

Қуйида вирусдан заҳарланиш профилактикасига, вирусларни аниқлаш ва йўқотишга мўлжалланган баъзи дастурий комплекслар тавсифланган.

AVP (Антивирус Касперского Personal) – Россиянинг вирусга қарши пакети. Пакет таркибига қуйидагилар киради:

- OfficeGuard – блокировка қилувчи, макровирусдан 100% ҳимояланишни таъминлайди;

- Inspector – тафтишчи, компьютердаги барча ўзгаришларни кузатади, вирус фаоллиги аниқланганида дискнинг асл нусхасини тиклашга ва зарар келтирувчи кодларни чиқариб ташлашга имкон беради;

- Monitor – вирусларни ушлаб қолувчи, компьютер хотирасида доимо ҳозир бўлиб, файллар ишга туширилганида, яратилишида ёки нусхаланишида уларни вирусга қарши текширади;

- Scanner – вирусга қарши модул, локал ва тармоқ дисклар таркибини кенг кўламли текшириш имконини беради. Сканерни қўл ёрдамида ёки бе-

рилган вақтда автоматик тарзда ишга тушириш мумкин;

- Dr.Web – Россиянинг вирусга қарши оммавий дастури, Windows 9x/NT/2000/XP учун мўлжалланган бўлиб, файлли, юклама, ва файл-юклама вирусларни қидиради ва зарарсизлантиради. Дастур таркибида резидент қоровул SpIDer Guard, Internet орқали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган.Dr.Web да ишлатилувчи алгоритмлар ҳақида маълум бўлган барча вирус хилларини аниқлашга имкон беради. Dr.Web дастурининг муҳим хусусияти – оддий сигнатурали қидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниқлаш имкониятидир;

- Symantec Antivirus – Symantec компаниясининг корпоратив фойдаланувчиларга таклиф этган вирусга қарши маҳсулоти набори.Symantec маҳсулотидан ишчи жойларининг умумий сони 100 ва ундан ортиқ бўлганида ва бўлмаганда битта Windows NT/2000/NetWare сервери мавжудлигида фойдаланиш мақсадга мувофиқ ҳисобланади. Ушбу пакетнинг башқалардан ажралиб турадиган хусусияти қуйидагилар:

- бошқаришнинг иерархик модели;

- янги вирус пайдо бўлишига реакция қилиш механизмининг мавжудлиги.

- AntiVir Personal Edition – вирусга қарши дастур AVP, Dr.Web ва ҳ.лар имкониятларидек имкониятларга эга. Дастур комплектига қуйидагилар киради:

- дискларни сканерловчи;

- резидент қурикчи;

- бошқариш дастури;

- режалаштирувчи.

Дастур Internet дан юкланувчи файлларни сканерлайди. Internet орқали янгиланишларни автоматик тарзда текшириш ва юклаш функцияси ҳам мавжуд. Дастур хотирани, юкланиш секторини текширишда ишлатилади ва

унда вируслар бўйича кенг кўламдаги маълумотнома мавжуд.

Назорат саволлари:

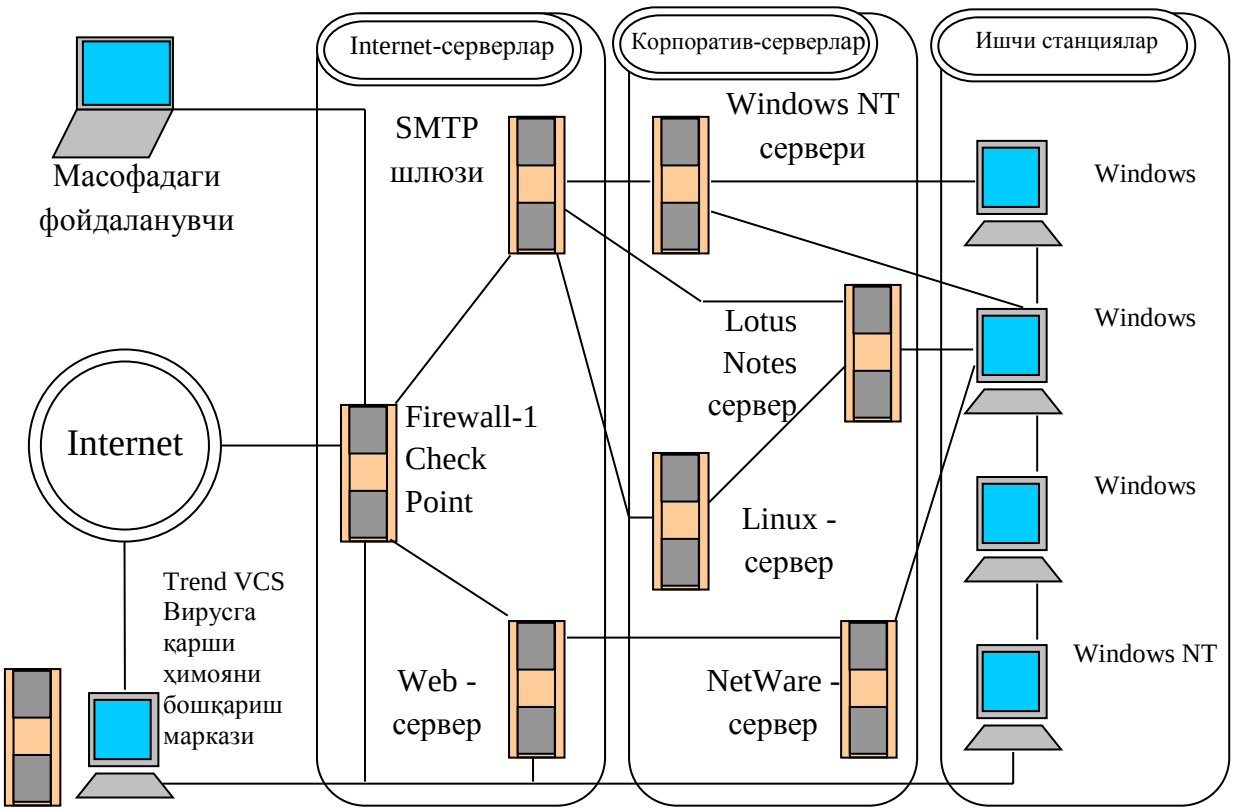
1. Компьютер вирусларини аниқлашнинг асосий усуллари нималардан иборат?
2. Вирусга қарши дастур турлари ва уларнинг ишлаш принципи.
3. Вирусга қарши дастурларнинг сифатини баҳоловчи мезонларни санаб беринг.
4. Вирусга қарши ҳимоянинг профилактика чораларини тушунтириб беринг.

7.3. Вирусга қарши ҳимоя тизимини қуриш

Ҳозирда ўртача компаниянинг корпоратив компьютер тармоғи таркибида ўнлаб ва юзлаб ишчи станциялари, ўнлаб серверлар, телекоммуникациянинг турли фаол ва пассив асбоб ускуналари мавжуд бўлган етарлича мураккаб структурага эга (7.2-расм).

Корпоратив тармоқдан фойдаланувчилар тармоққа вирусларнинг суқилиб кириш файллари билан доимо тўқнашадилар. Internet/intranet корпоратив тизимларига вирус хужумлари мунтазам бўлиб туради, фойдаланувчи ишчи станциясининг заҳарланган ахборот элтувчиси томонидан заҳарланиши эса одат тусини олган.

Корпоратив тармоқ вируслар ва бошқа зарар келтирувчи дастурлар хужумларига дучор бўлганида тармоқнинг вирусга қарши ҳимояси кўпинча вирусга қарши локал дастурий таъминот ёрдамида, сканерлаш ва қатор ишчи станцияларни даволаш билан тугайди ва ҳимоя таъминланади деб ҳисобланади. Аслида муаммонинг бундай локализациялаш минимал чора ҳисобланади ва корпоратив тармоқнинг кейинги барқарор ишлашини кафолатламайди. Бошқача айтганда, вирусга қарши локал ечимларнинг ишлатилиши корхонани вирусдан самарали ҳимоялаш учун зарурий, аммо етарли восита ҳисобланмайди.



7.2–расм. Корпоратив тармоқнинг намунавий архитектураси

Вирусга қарши ҳимоянинг самарали корпоратив тизими - "мижоз-сервер" технологияси бўйича амалга оширилган, тармоқдаги ҳар қандай шубҳали ҳаракатни сезгирлик билан фаҳмлаб олувчи, тескари боғланишли мосланувчан тизимдир. Бундай тизим корпоратив тармоқнинг ички структураси доирасида вирусларни ва бошқа ғаним дастурларнинг тарқалишига йўл қўймайди. Вирусга қарши ҳимоянинг самарали корпоратив тизими турли вирус хужумларини-маълумларини, ҳам номаълумларини, улар намоён бўлишининг дастлабки босқичида, аниқлайди ва бетарафлаштиради.

Албатта, турли вазиятлар бўлиши мумкин, масалан масофадан фойдаланувчининг заҳарланган компьютерининг корпоратив серверга уланишида ёки макровируслар бўлган WORD ёки Excel файлли дискетлардан иш жойларида фойдаланишда тармоқ заҳарланиши мумкин. Аммо, сифатли қурилган вирусга қарши ҳимоянинг корпоратив тизими учун бу жиддий эмас, чунки, биринчидан, заҳарланишнинг кўрсатилган ҳолатлар камдан-кам учрайди, иккинчидан, вируслар вақтида аниқланади ва бетарафлаштирилади.

Натижада уларнинг кўпайишига ва корпоратив тармоқ доирасида тарқалишига йўл қўйилмайди.

Уланадиган ишчи станциялари сони ошган сари корпоратив тармоқнинг хизмат кўрсатиш нархи оша боради. Корпоратив тармоқни вируслардан ҳимоялаш харажатлари корхона умумий харажатлари рўйхатида охирги бандини эгалламайди.

Ушбу харажатларни корпоратив тармоқни вирусга қарши ҳимоялашни вақтнинг реал масштабида марказлаштирилган бошқариш орқали оптималлаштириш ва камайтириш мумкин. Бундай ечим корхона тармоғи маъмурларига вирусни барча суқилиб кириш нуқталарини бошқаришнинг ягона консоли орқали кузатишга ва корпоратив тармоқдаги барча вирусга қарши воситаларни самарали бошқаришга имкон беради. Вирусга қарши ҳимояни марказлаштирилган бошқариш мақсади жуда оддий – вирусларнинг барча суқилиб кириш нуқталарини блокировка қилиш. Қуйидаги суқилиб киришларни ва захарланишларни кўрсатиш мумкин:

- ташувчи манбалардан (флоппи-дисклар, компакт-дисклар, Zip, Jazz, Floptical ва ҳ.) охирги заҳарланган файллардан фойдаланишда ишчи станцияларга вирусларнинг суқилиб кириши;

- Internetдан Web ёки FTP орқали олинган локал ишчи станциясида сақланган заҳарланган текин дастурий таъминот ёрдамида заҳарланиш;

- масофадаги ёки мобил фойдаланувчиларнинг заҳарланган ишчи станциялари корпоратив тармоққа уланганида вирусларнинг суқилиб кириши;

- корпоратив тармоққа уланган масофадаги сервердаги вируслар билан заҳарланиш.

- иловаларида макровируслар билан заҳарланган Excel ва Word файллар бўлган электрон почтанинг тарқалиши.

Вируслардан ва бошқа зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуриш қуйидаги босқичларни ўз ичига олади.

Биринчи босқичда ҳимояланувчи тармоқнинг ўзига хос хусусиятлари аниқланади ва бир неча вирусга қарши ҳимоя вариантлари танланади ва асо-

сланади. Бу босқичда қуйидагилар бажарилади:

- компьютер тизими ва вирусга қарши ҳимоя воситаларининг аудити;

- ахборот тизимини текшириш ва *картирлаш*;

- вирусларнинг суқилиб кириши билан боғлиқ тахдидларнинг амалга ошириш сценарийсини тахлиллаш.

Натижада вирусга қарши ҳимоянинг умумий ҳолати баҳоланади.

Иккинчи босқичда вирусга қарши хавфсизлик сиёсати ишлаб чиқилади. Бу босқичда қуйидагилар бажарилади:

- ахборот ресурсларини туркумлашнинг тури;

- вирусга қарши хавфсизликни таъминловчи кучларни яратиш- вакалатларни тақсимлаш;

- вирусга қарши хавфсизликни ташкилий-хуқуқий мададлаш;

- вирусга қарши хавфсизлик инструментларига талабларни аниқлаш;

- вирусга қарши хавфсизликни таъминлаш харажатларини ҳисоблаш.

Натижада корхонанинг вирусга қарши хавфсизлик сиёсати ишлаб чиқилади.

Учинчи босқичда дастурий воситалари, ахборот ресурсларини инвентаризациялаш ва мониторингини автоматлаштириш воситалари танланади. Вирусга қарши хавфсизликни таъминлаш бўйича ташкилий тадбирлар рўйхати ишлаб чиқилади.

Натижада корхонанинг вирусга қарши хавфсизлигини таъминловчи режа ишлаб чиқилади.

Тўртинчи босқичда вирусга қарши танланган ва тасдиқланган хавфсизлик режаси амалга оширилади. Бу босқичда вирусга қарши воситалар етказиб берилади, жорий этилади ва мададланади.

Натижада корпоратив вирусга қарши ҳимоялашнинг самарали тизими яратилишига имкон туғилади.

Назорат саволлари:

1. Вирусга қарши ҳимояга эга корпоратив тармоқнинг намунавий архитектурасини тушунтириб беринг.

2. Вирус ва зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуришда бажариладиган ҳимоялаш варианталарини танлашнинг моҳиятини тушунтириб беринг.

3. Вирус ва зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуришда бажариладиган вирусга қарши сиёсатни ишлаб чиқиш афзаллиги.

4. Вирус ва зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуришда бажариладиган ахборот коммуникация ресурсларини инвентаризациялаш ва мониторинглаш жараёнини ёритиб беринг.

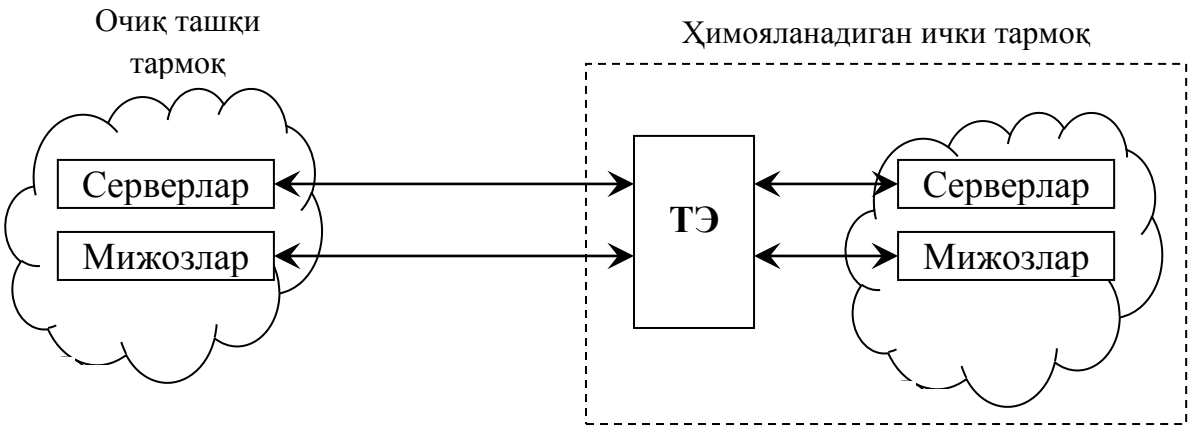
5. Вирус ва зарар келтирувчи дастурлардан ҳимояловчи корпоратив тизимни қуришда бажариладиган хавфизлик режасини амалга ошириш жараёнини тушунтириб беринг.

VIII боб. АХБОРОТНИ ҲИМОЯЛАШДА ТАРМОҚЛАРАРО ЭКРАНЛАРНИНГ ЎРНИ

8.1. Тармоқлараро экранларнинг ишлаш хусусиятлари

Тармоқлараро экран (ТЭ) - *брандмауэр* ёки *firewall системаси* деб ҳам аталувчи тармоқлараро ҳимоянинг ихтисослаштирилган комплекси. Тармоқлараро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чегара орқали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи қоидалар тўпламини амалга ошириш имконини беради. Одатда, бу чегара корхонанинг корпоратив (локал) тармоғи ва Internet глобал тармоқ орасида ўтказилади. Тармоқлараро экранлар гарчи корхона локал тармоғи уланган корпоратив интратармоғидан қилинувчи ҳужумлардан ҳимоялашда ишлатилишлари мумкин бўлсада, одатда улар корхона ички тармоғини Internet глобал тармоқдан суқилиб киришдан ҳимоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шарти ҳисобланади.

Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ ҳисобланувчи ташкилотнинг ҳимояланувчи тармоғи ва ташқи ғаним тармоқ орасида жойланиши лозим (8.1-расм).



8.1-расм. Тармоқлараро экранни улаш схемаси.

Бунда бу тармоқлар орасидаги барча алоқа фақат тармоқлараро экран орқали амалга оширилиши лозим. Ташкилий нуқтаи назаридан тармоқлараро экран ҳимояланувчи тармоқ таркибига киради.

Ички тармоқнинг кўпгина узелларини бирданига ҳимояловчи тармоқлараро экран қуйидаги иккита вазифани бажариши керак:

- ташқи (ҳимояланувчи тармоққа нисбатан) фойдаланувчиларнинг корпоратив тармоқнинг ички ресурсларидан фойдаланишини чегаралаш. Бундай фойдаланувчилар қаторига тармоқлараро экран ҳимояловчи маълумотлар базасининг серверидан фойдаланишга уринувчи шериклар, масофадаги фойдаланувчилар, хакерлар, ҳатто компаниянинг ходимлари киритилиши мумкин;

- ҳимояланувчи тармоқдан фойдаланувчиларнинг ташқи ресурслардан фойдаланишларини чегаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.

Ҳозирда ишлаб чиқарилаётган тармоқлараро экранларнинг тав-сифларига асосланган ҳолда, уларни қуйидаги асосий аломатлари бўйича туркумлаш мумкин:

OSI модели сатҳларида ишлаши бўйича:

- пакетли фильтр (экранловчи маршрутизатор – screening router);
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбиқий сатҳ шлюзи (application gateway);
- эксперт сатҳи шлюзи (stateful inspection firewall).

Ишлатиладиган технология бўйича:

- протокол ҳолатини назоратлаш (Stateful inspection);
- воситачилар модуллари асосида (proxy);

Бажарилиши бўйича:

- аппарат-дастурий;
- дастурий;

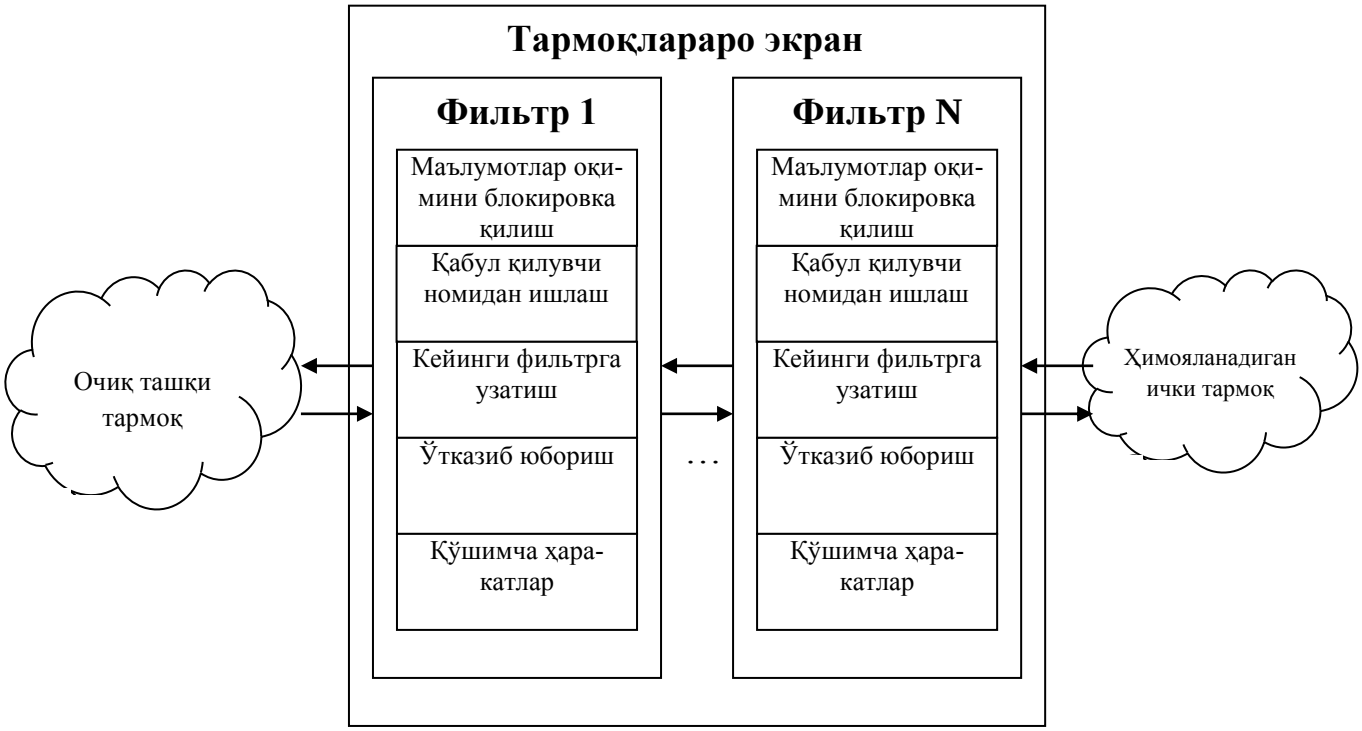
Уланиш схемаси бўйича;

- тармоқни умумий ҳимоялаш схемаси;

- тармоқ сегментлари ҳимояланувчи берк ва тармоқ сегментлари ҳимояланмайдиган очиқ схема;

- тармоқнинг берк ва очиқ сегментларини алоҳида ҳимояловчи схема.

Трафикларни фильтрлаш. Ахборот оқимларини фильтрлаш уларни экран орқали, баъзида қандайдир ўзгартиришлар билан, ўтказишдан иборат. Фильтрлаш қабул қилинган хавфсизлик сиёсатига мос келувчи, экранга олдиндан юкланган қоидалар асосида амалга оширилади. Шу сабабли тармоқлараро экранни ахборот оқимларини ишловчи фильтрлар кетма-кетлиги сифатида тасаввур этиш қулай (8.2-расм).



8.2-расм. Тармоқлараро экран тузилмаси.

Фильтрларнинг ҳар бири қуйидаги ҳаракатларни бажариш орқали фильтрлашнинг алоҳида қоидаларини изоҳлашга аталган:

1. Ахборотни изоҳланувчи қоидалардаги берилган мезонлар бўйича таҳлиллаш, масалан, қабул қилувчи ва жўнатувчи адреслари ёки ушбу ахборот аталган илова хили бўйича.

2. Изоҳланувчи қоидалар асосида қуйидаги ечимлардан бирини қабул

қилиш:

- маълумотларни ўтказмаслик;

- маълумотларни қабул қилувчи номидан ишлаш ва натижани жўнатувчига қайтариш;

- тахлиллашни давом эттириш учун маълумотларни кейинги фильтрга узатиш;

- кейинги фильтрларга эътибор қилмай маълумотларни узатиш.

Фильтрлаш қоидалари воситачилик функцияларига оид қўшимча, масалан маълумотларни ўзгартириш, ходисаларни қайдлаш ва ҳ. каби ҳаракатларни ҳам бериши мумкин. Мос ҳолда, фильтрлаш қоидалари қуйидагиларнинг амалга оширилишини таъминловчи шартлар рўйхатини аниқлайди:

- маълумотларни кейинги узатишга рухсат бериш ёки рухсат бермаслик;

- ҳимоялашнинг қўшимча функцияларини бажариш.

Ахборот оқимини тахлиллаш мезони сифатида қуйидаги параметрлардан фойдаланиш мумкин:

- таркибида тармоқ адреслари, идентификаторлар, интерфейслар адреси, портлар номери ва бошқа муҳим маълумотлар бўлган хабар пакетларининг хизматчи хошиялари;

- масалан, компьютер вируслари борлигига текширилувчи хабар пакетларининг бевосита таркиби;

- ахборот оқимининг ташқи характеристикалари, масалан, вақт ва частота характеристикалари маълумотлар ҳажми ва ҳ.

Ишлатилувчи тахлиллаш мезонлари фильтрлашни амалга оширувчи OSI моделининг сатҳларига боғлиқ. Умумий ҳолда, пакетни фильтрлашни амалга оширувчи OSI моделининг сатҳи қанчалик юқори бўлса, таъминланувчи ҳимоялаш даражаси ҳам шунчалик юқори бўлади.

Воситачилик функцияларининг бажарилиши. Тармоқлараро экран воситачилик функцияларини *экранловчи агентлар* ёки *воситачи дастурлар*

деб аталувчи махсус дастурлар ёрдамида бажаради. Бу дастурлар резидент дастурлар ҳисобланади ва ташқи ва ички тармоқ орасида хабарлар пакетини бевосита узатишни тақиқлайди.

Ташқи тармоқдан ички тармоқнинг ва аксинча фойдаланиш зарурияти туғилганда аввал тармоқлараро экран компьютерида ишловчи воситачи-дастур билан мантиқий уланиш ўрнатилиши лозим. Воситачи-дастур сўралган тармоқлараро алоқанинг жоизлигини текширади ва ижобий натижада ўзи суралган компьютер билан алоҳида уланиш ўрнатади. Сўнгра ташқи ва ички тармоқ компьютерлари орасида ахборот алмашиш, хабарлар оқимини фильтрлашни ҳамда бошқа ҳимоялаш функцияларини бажарувчи дастурий воситачи орқали амалга оширилади.

Таъкидлаш лозимки, тармоқлараро экран фильтрлаш функциясини воситачи-дастур иштирокисиз амалга ошириб, ташқи ва ички тармоқ орасида ўзаро алоқанинг шаффофлигини таъминлаши мумкин. Шу билан бирга воситачи дастурлар хабарлар оқимини фильтрлашни амалга оширмаслиги ҳам мумкин.

Умуман, воситачи-дастурлар, хабарлар оқимини шаффоф узатилишини блокировка қилган ҳолда, қуйидаги функцияларни бажариши мумкин:

- узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини текшириш;

- ички тармоқ ресурсларидан фойдаланишни чегаралаш;

- ташқи тармоқ ресурсларидан фойдаланишни чегаралаш;

- ташқи тармоқдан сўралувчи маълумотларни кэш хотирага сақлаш;

- хабарлар оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;

- фойдаланувчиларни идентификациялаш ва аутентификациялаш;

- ички тармоқ адресларини трансляциялаш;

- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, хамда қайдланган ахборотни тахлиллаш ва ҳисоботларни генерациялаш.

Узатилувчи ва қабул қилинувчи маълумотларнинг ҳақиқийлигини тек-

шириш нафақат электрон хабарларни, балки сохталаштирилиши мумкин бўлган миграцияланувчи дастурларни (Java, ActiveXControls) аутентификациялаш учун долзарб ҳисобланади. Хабар ва дастурларнинг ҳақиқийлигини текшириш уларнинг рақамли имзосини текширишдан иборатдир.

Ички тармоқ ресурсларидан фойдаланишни чегаралаш усуллари операцион тизим сатҳида мададланувчи чегаралаш усулларидан фарқ қилмайди.

*Ташқи тармоқ ресурсларидан фойдаланишни чегарлаш*да кўпинча қуйидаги ёндашишлардан бири ишлатилади:

- фақат ташқи тармоқдаги берилган адрес бўйича фойдаланишга рухсат бериш;

- янгиланувчи ножоиз адреслар руйхати бўйича суровларни фильтрлаш ва ўринсиз калит сўзлари бўйича ахборот ресурсларини қидиришни блокировка қилиш:

- маъмур томонидан ташқи тармоқнинг қонуний ресурсларини брандмауэрнинг дискли хотирасида тўплаш ва янгилаш ва ташқи тармоқдан фойдаланишни тўла тақиқлаш.

Ташқи тармоқдан сўралувчи *маълумотларни кэшлаш* махсус воситачилар ёрдамида мададланади. Ички тармоқ фойдаланувчилари ташқи тармоқ ресурсларидан фойдаланганларида барча ахборот, proxy-сервер деб аталувчи брандмауэр қаттиқ диски маконида тўпланади. Шу сабабли, агар навбатдаги сўровда керакли ахборот proxy-серверда бўлса, воситачи уни ташқи тармоққа мурожаатсиз тақдим этади. Бу фойдаланишни жиддий тезлаштиради. Маъмурга фақат proxy-сервер таркибини вақти-вақти билан янгилаб туриш вазифаси қолади.

Кэшлаш функцияси ташқи тармоқ ресурсларидан фойдаланишни чегаралашда муваффақиятли ишлатилиши мумкин. Бу ҳолда ташқи тармоқнинг барча қонуний ресурслари маъмур томонидан proxy-серверда тўпланади ва янгиланади. Ички тармоқ фойдаланувчиларига фақат proxy-сервернинг ахборот ресурсларидан фойдаланишга рухсат берилади, ташқи тармоқ ресурсларидан бевосита фойдаланиш эса ман қилинади.

Хабарлар оқимини фильтрлаш ва ўзгартириш воситачи томонидан қоидаларнинг берилган тўплами ёрдамида бажарилади. Бунда воситачи-дастурларнинг икки хили фарқланади:

- сервис турини аниқлаш учун хабарлар оқимини тахлиллашга мўлжалланган экранловчи агентлар, масалан, FTP, HTTP, Telnet;

- барча хабарлар оқимини ишловчи универсал экранловчи агентлар, масалан, компьютер вирусларини қидириб зарарсизлантиришга ёки маълумотларни шаффоф шифрлашга мўлжалланган агентлар.

Дастурий воситачи унга келувчи маълумотлар пакетини тахлиллайди ва агар қандайдир объект берилган мезонларга мос келмаса, воситачи унинг кейинги силжишини блокировка қилади ёки мос ўзгаришини, масалан, ошкор қилинган компьютер вирусларни зарарсизлантиришни бажаради. Пакетлар таркибини тахлиллашда экранловчи агентнинг ўтувчи файлли архивларни автоматик тарзда оча олиши муҳим ҳисобланади.

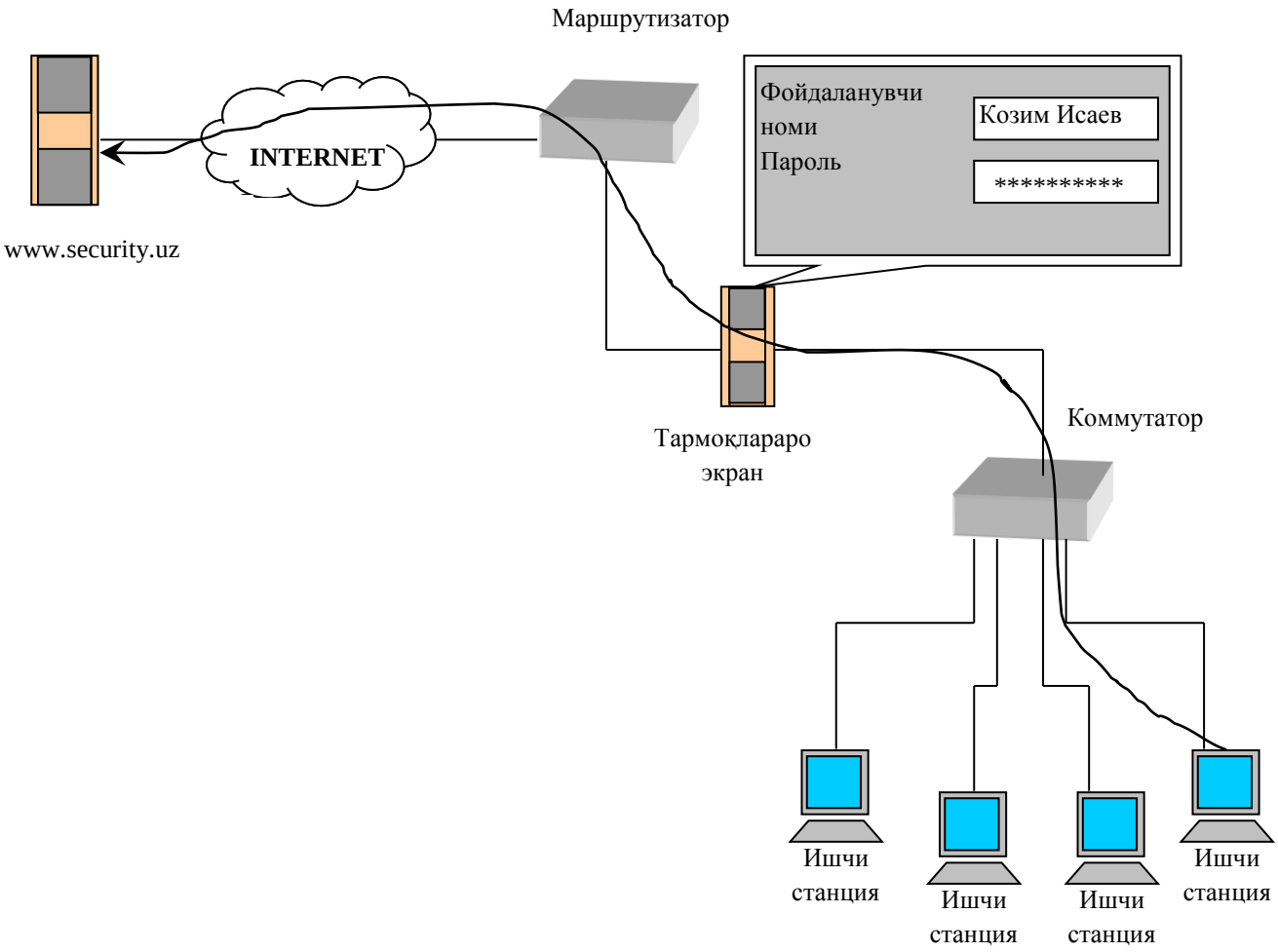
Фойдаланувчиларни идентификациялаш ва аутентификациялаш баъзида оддий идентификаторни (исм) ва паролни тақдим этиш билан амалга оширилади (8.3-расм). Аммо бу схема хавфсизлик нуқтаи назаридан заиф ҳисобланади, чунки паролни бегона шахс ушлаб қолиб ишлатиши мумкин. Internet тармоғидаги кўпгина можаролар қисман анъанавий кўп марта ишлатилувчи паролларнинг заифлигидан келиб чиққан.

Аутентификациялашнинг ишончлироқ усули – бир марта ишлатилувчи пароллардан фойдаланишдир. Бир мартали паролларни генерациялашда аппарат ва дастурий воситалардан фойдаланилади. Аппарат воситалари компьютернинг слотига ўрнатилувчи қурилма бўлиб, уни ишга тушириш учун фойдаланувчи қандайдир махфий ахборотни билиши зарур. Масалан, смарт-карта ёки фойдаланувчи токени ахборотни генерациялайди ва бу ахборотни хост анъанавий парол ўрнида ишлатади. Смарт-карта ёки токен хостнинг аппарат ва дастурий таъминоти билан бирга ишлаши сабабли, генерацияланувчи парол ҳар бир сеанс учун ноёб бўлади.

Ишончли орган, масалан калитларни тақсимлаш маркази томонидан

берилувчи рақамли сертификатларни ишлатиш ҳам қулай ва ишончли. Кўпгина воситачи дастурлар шундай ишлаб чиқиладики, фойдаланувчи фақат тармоқлараро экран билан ишлаш сеансининг бошида аутентификациялансин. Бундан кейин маъмур белгилаган вақт мобайнида ундан қўшимча аутентификацияланиш талаб этилмайди.

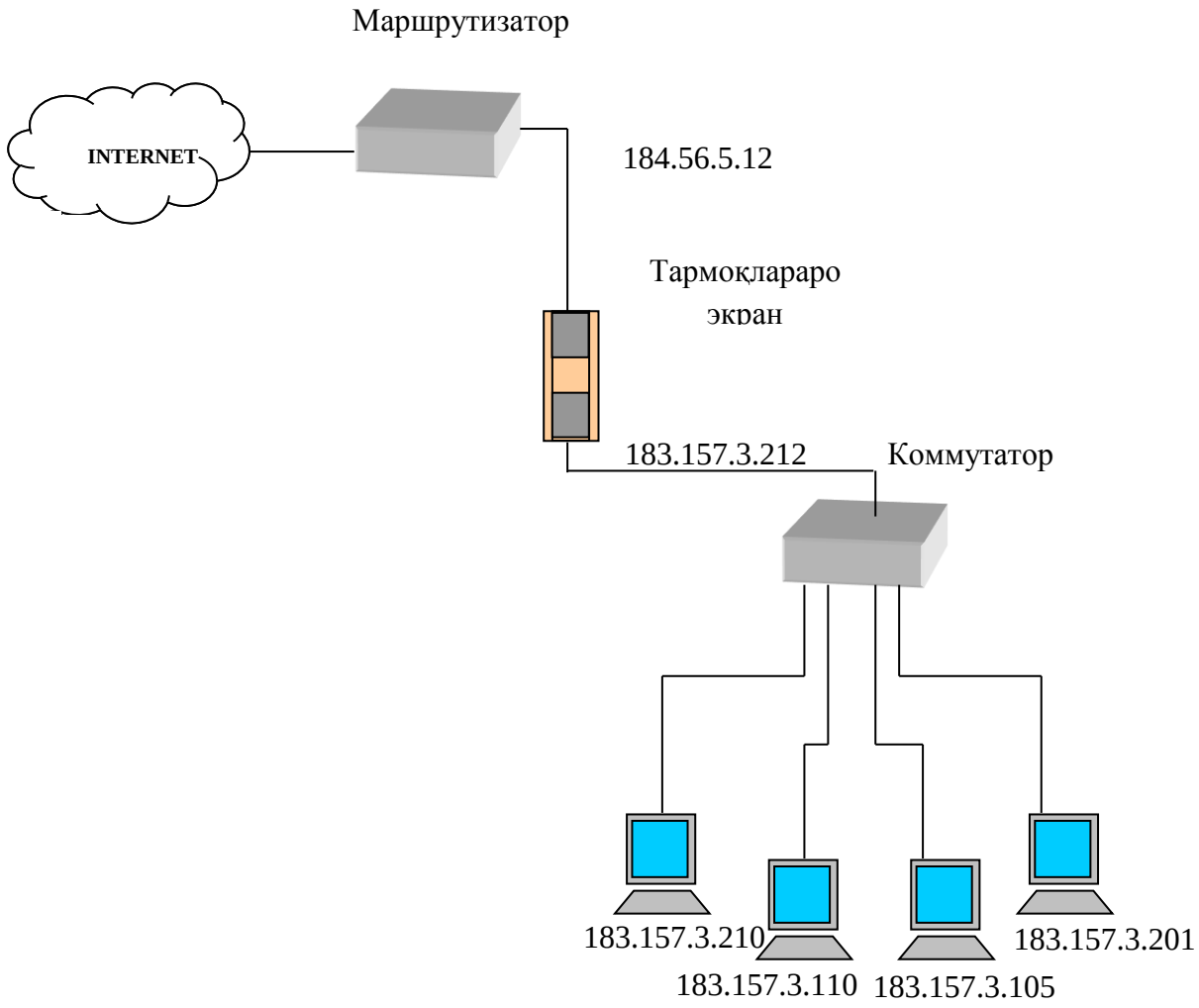
Тармоқлараро экранлар тармоқдан фойдаланишни бошқаришни марказлаштиришлари мумкин. Демак, улар кучайтирилган аутентификациялаш дастурлари ва қурилмаларини ўрнатишга муносиб жой ҳисобланади. Гарчи кучайтирилган аутентификация воситалари ҳар бир хостда ишлатилиши мумкин бўлсада, уларнинг тармоқлараро экранларда жойлаштириш қулай. Кучайтирилган аутентификациялаш чораларидан фойдаланувчи тармоқлараро экранлар бўлмаса, Telnet ёки FTP каби иловаларнинг аутентификацияланмаган трафиги тармоқнинг ички тизимларига тўғридан-тўғри ўтиши мумкин.



8.3–расм. Пароль бўйича фойдаланувчини аутентификациялаш схемаси

Қатор тармоқлараро экранлар аутентификациялашнинг кенг тарқалган усулларидан бири – Kerberosни мададлайди. Одатда, аксарият тижорат тармоқлараро экранлар аутентификациялашнинг турли схемаларини мададлайди. Бу эса тармоқ хавфсизлиги маъмурига ўзининг шароитига қараб энг мақбул схемани танлаш имконини беради.

Ички тармоқ адресларини трансляциялаш. Кўпгина хужумларни амалга оширишда нияти бузуқ одамга қурбонининг адресини билиш керак бўлади. Бу адресларни ҳамда бутун тармоқ топологиясини бекитиш учун тармоқлараро экранлар энг муҳим вазифани – ички тармоқ адресларини трансляциялашни бажаради (8.4-расм).



8.4–расм. Тармоқ адресларини трансляциялаш

Бу функция ички тармоқдан ташқи тармоққа узатилувчи барча пакетларга нисбатан бажарилади. Бундай пакетлар учун жўнатувчи компьютерларнинг IP-адреслари битта "ишончли" IP адресга автоматик тарзда ўзгартирилади.

Ички тармоқ адресларини трансляциялаш иккита усул-динамик ва статик усулларда амалга оширилиши мумкин. Динамик усулда адрес узелга тармоқлараро экранга мурожаат онида ажратилади. Уланиш тугалланганидан сўнг адрес бўшайди ва уни корпоратив тармоқнинг бошқа узели ишлатиши мумкин. Статик усулда узел адреси барча чиқувчи пакетлар узатиладиган тармоқлараро экраннинг битта адресига доимо боғланади. Тармоқлараро экраннинг IP-адреси ташқи тармоққа тушувчи ягона фаол IP-адресга айланади. Натижада, ички тармоқдан чиқувчи барча пакетлар тармоқлараро экрандан жўнатилган бўлади. Бу авторизацияланган ички тармоқ ва хавфли бўлиши мумкин бўлган ташқи тармоқ орасида тўғридан-тўғри алоқани истисно қилади.

Бундай ёндашишда ички тармоқ топологияси ташқи фойдаланувчилардан яширинган, демак, рухсатсиз фойдаланиш масаласи қийинлашади. Адресларни трансляциялаш тармоқ ичида ташқи тармоқ, масалан Internetдаги адреслаш билан келишилмаган адреслашнинг хусусий тизимига эга бўлишига имкон беради. Бу ички тармоқнинг адрес маконини кенгайтириш ва ташқи адрес танқислиги муаммосини самарали ечади.

Ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, ҳамда қайдланган ахборотни тахлиллаш ва ҳисоботларни генерациялаш тармоқлараро экранларнинг муҳим вазифалари ҳисобланади. Корпоратив тармоқни ҳимоялаш тизимининг жиддий элементи сифатида тармоқлараро экран барча ҳаракатларни рўйхатга олиш имкониятига эга. Бундай ҳаракатларга нафақат тармоқ пакетларини ўтказиб юбориш ёки блокировка қилиш, балки хавфсизлик маъмури томонидан фойдаланиш қоидасини ўзгартириш ва ҳ. ҳам тааллуқли. Бундай руйхатга олиш зарурият туғилганда (хавфсизлик можароси пайдо бўлганида ёки суд инстанцияларига ёки ички тергов учун далилларни

йиғишда) яратилувчи журналларга мурожаат этишга имкон беради.

Шубҳали ходисалар (alarm) хусусидаги сигналларни қайдлаш тизими тўғри созланганида тармоқлараро экран тармоқ хужумга дучор бўлганлиги ёки зондланганлиги тўғрисидаги батафсил ахборотни бериши мумкин. Тармоқдан фойдаланиш ва унинг зондланганлигининг исботи статистикасини йиғиш қатор сабабларга кўра муҳимдир. Аввало. тармоқлараро экраннинг зондланишга ва хужумларга бардошлигини аниқ билиш зарур ва тармоқлараро экранни ҳимоялаш тадбирларининг адекватлигини аниқлаш лозим. Ундан ташқари, тармоқдан фойдаланиш статистикаси тармоқ асбоб-ускуналарига ва дастурларига талабларни ифодалаш мақсадида хавф-хатарни тадқиқлаш ва тахлиллашда дастлабки маълумотлар сифатида муҳим ҳисобланади.

Кўпгина тармоқлараро экранлар статистикани қайдловчи, йиғувчи ва тахлилловчи қувватли тизимга эга. Мижоз ва сервер адреси, фойдаланувчилар идентификатори, сеанс вақтлари, уланиш вақтлари, узатилган ва қабул қилинган маълумотлар сони, маъмур ва фойдаланувчилар ҳаракатлари бўйича ҳисоб олиб борилиши мумкин. Ҳисоб тизимлари статистикани тахлиллашга имкон беради ва маъмурларга батафсил ҳисоботларни тақдим этади. Тармоқлараро экранлар махсус протоколлардан фойдаланиб, маълум ходисалар тўғрисида реал вақт режимида масофадан хабар беришни бажариши мумкин.

Рухсатсиз ҳаракатларни қилишга уринишларни аниқланишига бўладиган мажбурий реакция сифатида маъмурнинг хабари, яъни огоҳлантирувчи сигналларни бериш белгиланиши лозим. Хужум қилинганлиги аниқланганда огоҳлантирувчи сигналларни юборишга қодир бўлмаган тармоқлараро экранни тармоклараро ҳимоянинг самарали воситаси деб бўлмайди.

Назорат саволлари:

1. Тармоқлараро экран воситалари тушунчаси ва унинг вазифалари.
2. Тармоқлараро экранларнинг OSI модели сатҳлари бўйича туркумланиши.
3. Трафикларни фильтрлаш функциясининг ишлашини тушунтириб

беринг.

4. Тармоқ адресларини трансляциялаш қандай амалга оширилади?

5. Тармоқлараро экранларнинг воситачилик функцияларининг моҳияти нимадан иборат?

8.2. Тармоқлараро экранларнинг асосий компонентлари

Тармоқлараро экранлар тармоқлараро алоқа хавфсизлигини OSI моделининг турли сатҳларида мададлайди. Бунда эталон моделнинг турли сатҳларида бажариладиган ҳимоя функциялари бир-биридан жиддий фарқланади. Шу сабабли, тармоқлараро экранлар комплексини, ҳар бири OSI моделининг алоҳида сатҳига мўлжалланган, бўлинмайдиган экранлар мажмуи кўринишида тасаввур этиш мумкин.

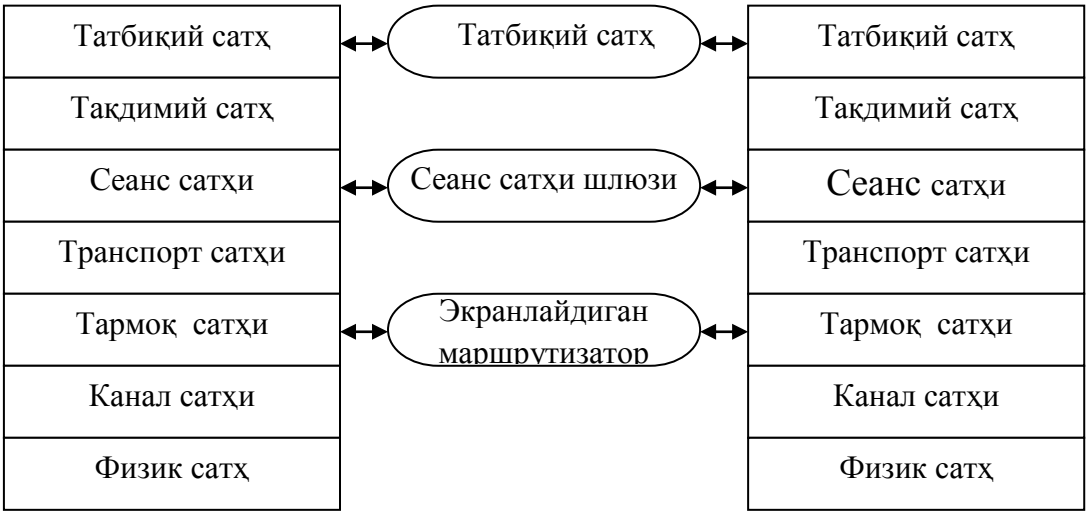
Экранлар комплекси кўпинча эталон моделнинг тармоқ, сеанс, татбиқий сатҳларида ишлайди. Мос ҳолда, қуйидаги бўлинмайдиган брандмауэрлар фарқланади (8.5-расм).

- экранловчи маршрутизатор;
- сеанс сатҳи шлюзи (экранловчи транспорт);
- татбиқий сатҳ шлюзи (экранловчи шлюз).

Тармоқларда ишлатиладиган протоколлар (TCP/IP, SPX/IPX) OSI эталон моделига батамом мос келмайди, шу сабабли санаб ўтилган экранлар хили функцияларини амалга оширишда эталон моделининг қўшни сатҳларини ҳам қамраб олишлари мумкин. Масалан, татбиқий экран хабарларнинг ташқи тармоққа узатилишида уларни автоматик тарзда шифрлашни, ҳамда қабул қилинувчи криптографик бекитилган маълумотларни автоматик тарзда расшифровка қилишни амалга ошириши мумкин. Бу ҳолда, бундай экран OSI моделининг нафақат татбиқий сатҳида, балки тақдимий сатҳида ҳам ишлайди.

Сеанс сатҳи шлюзи ишлашида OSI моделининг транспорт ва тармоқ сатҳларини қамраб олади. Экранловчи маршрутизатор хабарлар пакетини

тахлиллашда уларнинг нафақат тармоқ, балки транспорт сатҳи сарлавҳаларини ҳам текширади.



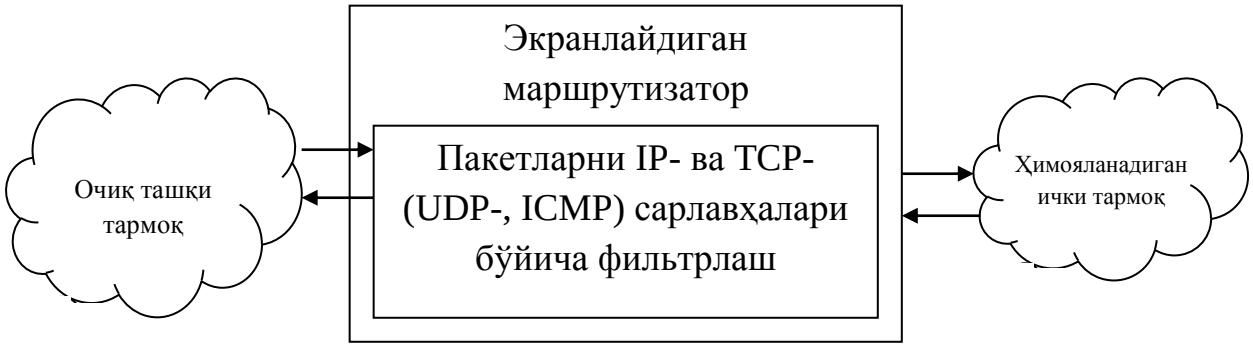
8.5-расм. OSI моделининг алоҳида сатҳларида ишлайдиган тармоқлараро экранлар тури

Юқорида келтирилган тармоқлараро экранларнинг хиллари ўзининг афзалликлари ва камчиликларига эга. Ишлатиладиган брандмауэрларнинг кўпчилиги ёки татбиқий шлюзлар, ёки экранловчи маршрутизаторлар бўлиб, тармоқлараро алоқанинг тўлиқ хавфсизлигини таъминламайди. Ишончли ҳимояни эса фақат ҳар бири экранловчи маршрутизатор, сеанс сатҳи шлюзи, ҳамда татбиқий шлюзни бирлаштирувчи тармоқлараро экранларнинг комплекси таъминлайди.

Экранловчи маршрутизатор (screeningrouter) (пакетли фильтр (packetfilter) деб ҳам аталади) хабарлар пакетини фильтрлашга аталган ва ички ва ташқи тармоқлар орасида шаффоф алоқани таъминлайди. У OSI моделининг тармоқ сатҳида ишлайди, аммо ўзининг айрим функцияларини бажаришида эталон моделининг транспорт сатҳини ҳам қамраб олиши мумкин.

Маълумотларни ўтказиш ёки бракка чиқариш хусусидаги қарор фильтрлашнинг берилган қоидаларига биноан ҳар бир пакет учун мустақил қабул қилинади. Қарор қабул қилишда тармоқ ва транспорт сатҳлари

пакетларининг сарлавҳалари тахлил этилади (8.6-расм).



8.6-расм. Пакетли фильтрнинг ишлаш схемаси

Ҳар бир пакетнинг IP- ва TCP/UDP – сарлавҳаларининг тахлилланувчи ҳошиялари сифатида қуйидагилар ишлатилиши мумкин:

- жўнатувчи адреси;
- қабул қилувчи адреси;
- пакет ҳили;
- пакетни фрагментлаш байроғи;
- манба порти номери;
- қабул қилувчи порт номери.

Биринчи тўртта параметр пакетнинг IP-сарлавҳасига, кейингилари эса TCP-ёки UDP сарлавҳасига тааллуқли. Жўнатувчи ва қабул қилувчи адреслари IP-адреслар ҳисобланади. Бу адреслар пакетларни шакллантиришда тўлдирилади ва уни тармоқ бўйича узатганда ўзгармайди.

Пакет хили ҳошиясида тармоқ сатҳига мос келувчи ICMP протокол коди ёки тахлилланувчи IP-пакет тааллуқли бўлган транспорт сатҳи протоколининг (TCP ёки UDP) коди бўлади.

Пакетни фрагментлаш байроғи IP-пакетлар фрагментлашининг борлиги ёки йўқлигини аниқлайди. Агар таҳлилланувчи пакет учун фрагментлаш байроғи ўрнатилган бўлса, мазкур пакет фрагментланган IP-пакетнинг қисм-пакети ҳисобланади.

Манба ва қабул қилувчи портлари номерлари TCP ёки UDP драйвер

томонидан ҳар бир жўнатилувчи хабар пакетларига қўшилади ва жўнатувчи иловасини, ҳамда ушбу пакет аталган иловани бир маънода идентификациялайди. Портлар номерлари бўйича фильтрлаш имконияти учун юқори сатҳ протоколларига порт номерларини ажратиш бўйича тармоқда қабул қилинган келишувни билиш лозим.

Ҳар бир пакет ишланишида экранловчи маршрутизатор берилган қоидалар жадвалини, пакетнинг тўлиқ ассоциациясига мос келувчи қоидани топгунича, кетма-кет кўриб чиқади. Бу ерда ассоциация деганда берилган пакет сарлавҳаларида кўрсатилган параметрлар мажмуи тушунилади. Агар экранловчи маршрутизатор жадвалдаги қоидаларнинг бирортасига ҳам мос келмайдиган пакетни олса, у, хавфсизлик нуқтаи назаридан, уни яроқсиз ҳолга чиқаради.

Пакетли фильтрлар аппарат ва дастурий амалга оширилиши мумкин. Пакетли фильтр сифатида оддий маршрутизатор, ҳамда кирувчи ва чиқувчи пакетларни фильтрлашга мослаштирилган, серверда ишловчи дастурдан фойдаланиш мумкин. Замонавий маршрутизаторлар ҳар бир порт билан бир неча ўнлаб қоидаларни боғлаши ва киришда, ҳам чиқишда пакетларни фильтрлаши мумкин.

Пакетли фильтрларнинг камчилиги сифатида қуйидагиларни кўрсатиш мумкин. Улар хавфсизликнинг юқори даражасини таъминламайди, чунки фақат пакет сарлавҳаларини текширади ва кўпгина керакли функцияларни мададламайди. Бу функцияларга, масалан, охирги узелларни аутентификациялаш, хабарлар пакетларини криптографик бекитиш, ҳамда уларнинг яхлитлигини ва ҳақиқийлигини текшириш киради. Пакетли фильтрлар дастлабки адресларни алмаштириб қўйиш ва хабарлар пакети таркибини рухсатсиз ўзгартириш каби кенг тарқалган тармоқ хужумларига заиф ҳисобланадилар. Бу хил брандмауэрларни "алдаш" қийин эмас - фильтрлашга рухсат берувчи қоидаларни қондирувчи пакет сарлавҳаларини шакллантириш кифоя.

Аммо, пакетли фильтрларнинг амалга оширилишининг соддалиги, юқори унумдорлиги, дастурий иловалар учун шаффофлиги ва нархининг

пастлиги, уларнинг ҳамма ерда тарқалишига ва тармоқ хавфсизлиги тизимининг мажбурий элементи каби ишлатилишига имкон яратди.

Сеанс сатҳи шлюзи, (*экранловчи транспорт* деб ҳам юритилади) виртуал уланишларни назоратлашга ва ташқи тармоқ билан ўзаро алоқа қилишда IP-адресларни трансляциялашга аталган. У OSI моделининг сеанс сатҳида ишлайди ва ишлаши жараёнида эталон моделнинг транспорт ва тармоқ сатҳларини ҳам қамраб олади. Сеанс сатҳи шлюзининг ҳимоялаш функциялари воситачилик функцияларига тааллуқли.

Виртуал уланишларнинг назорати алоқани квитирлашни кузатишдан ҳамда ўрнатилган виртуал каналлар бўйича ахборот узатилишининг назоратлашдан иборат. Алоқани квитирлашнинг назоратида сеанс сатҳида шлюз ички тармоқ ишчи станцияси ва ташқи тармоқ компьютери орасида виртуал уланишни кузатиб, сўралаётган алоқа сеансининг жоизлигини аниқлайди.

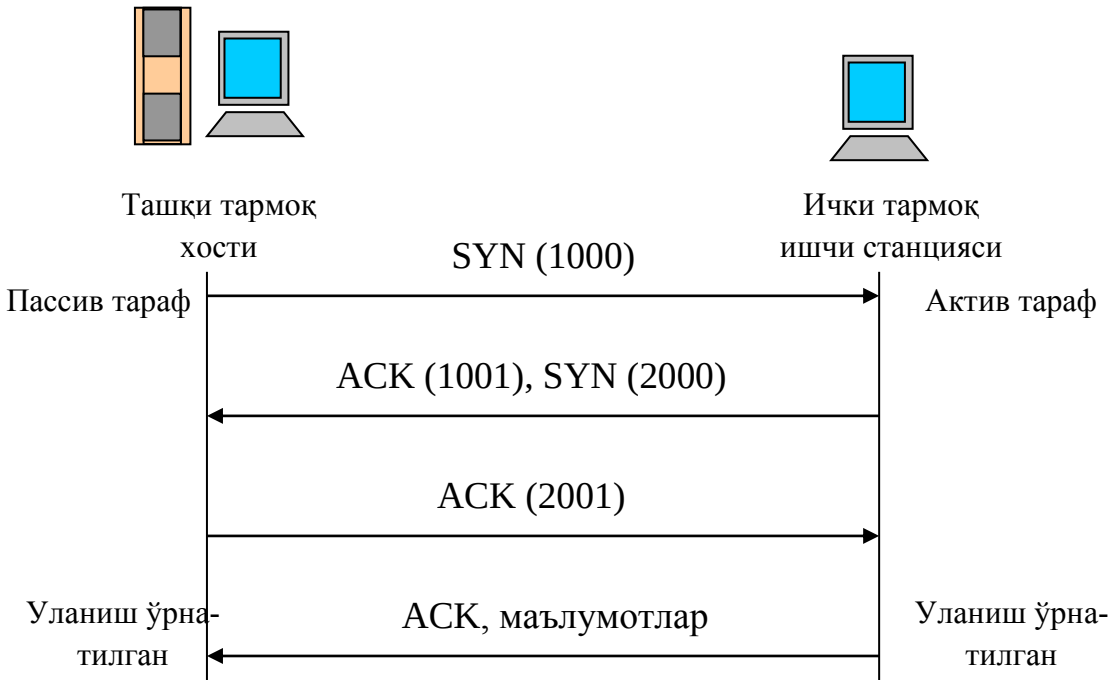
Бундай назорат TCP протоколининг сеанс сатҳи пакетларининг сарлавҳасидаги ахборотга асосланади. Аммо TCP-сарлавҳаларни тахлиллашда пакетли фильтр фақат манба ва қабул қилувчи портларининг номерини текширса, экранловчи транспорт алоқани квиртирлаш жараёнига тааллуқли бошқа ҳошияларни таҳлиллайди.

Алоқа сеансига сўровнинг жоизлигини аниқлаш учун сеанс сатҳи шлюзи қуйидаги ҳаракатларни бажаради. Ишчи станция (мижоз) ташқи тармоқ билан боғланишни сўраганида, шлюз бу сўровни қабул қилиб унинг фильтрлашнинг базавий мезонларни қаноатлантиришини, масалан сервер мижоз ва у билан ассоциацияланган исмнинг IP-адресини аниқлай олишини текширади. Сўнгра шлюз, мижоз исмидан ҳаракат қилиб, ташқи тармоқ компьютери билан уланишни ўрнатади ва TCP протоколи бўйича квитирлаш жараёнининг бажарилишини кузатади.

Бу муолажа SYN (Синхронлаш) ва ACK (Тасдиқлаш) байроқлари орқали белгиланувчи TCP-пакетларни алмашишдан иборат (8.7-расм).

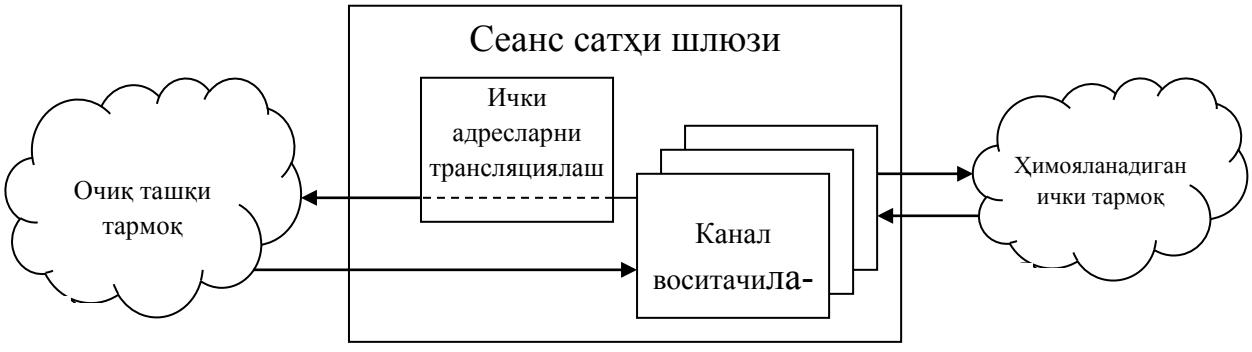
SYN байроқ билан белгиланган ва таркибида ихтиёрий сон, масалан 1000, бўлган TCP сеансининг биринчи пакети мижознинг сеанс очишга сўро-

ви ҳисобланади. Бу пакетни олган ташқи тармоқ компьютери жавоб тариқасида ACK байроқ билан белгиланган ва таркибида олинган пакетдагидан биттага катта (бизнинг ҳолда 1001) сон бўлган пакетни жўнатади. Шу тариқа, мижоздан SYN пакети олинганлиги тасдиқланади. Сўнгра, тескари муолажа амалга оширилади: ташқи тармоқ компьютери ҳам мижозга узатилувчи маълумотлар биринчи байтининг тартиб рақами билан (масалан, 2000) SYN пакетини жўнатади, мижоз эса уни олганлигини, таркибида 2001 сони бўлган пакетни узатиш орқали тасдиқлайди. Шу билан алоқани квиртирлаш жараёни тугалланади.



8.7–расм. TCP протоколи бўйича алоқани квитирлаш схемаси.

Сеанс сатҳи шлюзи (8.8-расм) учун сўралган сеанс жоиз ҳисобланади, қачонки алоқани квиртирлаш жараёни бажарилишида SYN ва ACK байроқлар, ҳамда TCP-пакетлари сарлавҳаларидаги сонлар ўзаро мантиқий боғланган бўлса.



Ички тармоқнинг ички станцияси ва ташқи тармоқнинг компьютери TCP сеансининг авторизацияланган қатнашчилари эканлиги ҳамда ушбу сеанснинг жоизлиги тасдиқланганидан сўнг шлюз уланишни ўрнатади. Бунда шлюз уланишларининг махсус жадвалига мос ахборотни (жўнатувчи ва қабул қилувчи адреслари, уланиш ҳолати, кетма-кетлик номери хусусидаги ахборот ва ҳ.) киритади.

Шу ондан бошлаб шлюз пакетларни нусхалайди ва иккала томонга йўналтириб, ўрнатилган виртуал канал бўйича ахборот узатилишини назорат қилади. Ушбу назорат жараёнида сеанс сатҳи шлюзи пакетларни фильтрламайди. Аммо у узатилувчи ахборот сонини назорат қилиши ва қандайдир чегарадан ошганида уланишни узиши мумкин. Бу эса, ўз навбатида, ахборотнинг рухсатсиз экспорт қилинишига тўсиқ бўлади. Виртуал уланишлар хусусидаги қайдлаш ахборотининг тўпланиши ҳам мумкин.

Сеанс сатҳи шлюзларида виртуал уланишларни назоратлашда *канал воситачилари* (ріреrгоху) деб юритилувчи махсус дастурлардан фойдаланилади. Бу воситачилар ички ва ташқи тармоқлар орасида виртуал каналларни ўрнатади, сўнгра TCP/IP иловалари генерациялаган пакетларнинг ушбу канал орқали узатилишини назоратлайди.

Канал воситачилари TCP/IPнинг муайян хизматларига мўлжалланган. Шу сабабли ишлаши муайян иловаларнинг воситачи-дастурларига асосланган татбиқий сатҳ шлюзлари имкониятларини кенгайтиришда сеанс сатҳ шлюзларидан фойдаланиш мумкин.

Сеанс сатҳи шлюзи ташқи тармоқ билан ўзаро алоқада тармоқ сатҳи ички адресларини (IP-адресларини) трансляциялашни ҳам таъминлайди. Ички адресларни трансляциялаш ички тармоқдан ташқи тармоққа жўнатилувчи барча пакетларга нисбатан бажарилади.

Амалга оширилиши нуқтаи назаридан сеанс сатҳи шлюзи етарлича оддий ва нисбатан ишончли дастур ҳисобланади. У экранловчи маршрутизаторни виртуал уланишларни назоратлаш ва ички IP-адресларни трансляциялаш функциялари билан тўлдиради.

Сеанс сатҳи шлюзининг камчиликлари – экранловчи маршрутизаторларнинг камчиликларига ўхшаш. Ушбу технологиянинг яна бир жиддий камчилиги маълумотлар ҳошиялари таркибини назоратлаш мумкин эмаслиги. Натижада, нияти бузуқ одамларга зарар келтирувчи дастурларни ҳимояланувчи тармоққа узатиш имконияти туғилади. Ундан ташқари, TCP-сессиясининг (TCPhijacking) ушлаб қолинишида нияти бузуқ одам хужумларини ҳатто рухсат берилган сессия доирасида амалга ошириши мумкин.

Амалда аксарият сеанс сатҳ шлюзлари мустақил маҳсулот бўлмай, татбиқий сатҳ шлюзлари билан комплектда тақдим этилади.

Татбиқий сатҳ шлюзи (*экранловчи шлюз* деб ҳам юритилади) OSI моделининг татбиқий сатҳида ишлаб, тақдимий сатҳни ҳам қамраб олади ва тармоқлараро алоқанинг энг ишончли ҳимоясини таъминлайди. Татбиқий сатҳ шлюзининг ҳимоялаш функциялари, сеанс сатҳи шлюзига ўхшаб, воситачилик функцияларига тааллуқли. Аммо, татбиқий сатҳ шлюзи сеанс сатҳи шлюзига қараганда ҳимоялашнинг анча кўп функцияларини бажариши мумкин:

- брандмауэр орқали уланишни ўрнатишга уринишда фойдаланувчиларни идентификациялаш ва аутентификациялаш;

- шлюз орқали узатилувчи ахборотнинг ҳақиқийлигини текшириш;

- ички ва ташқи тармоқ ресурсларидан фойдаланишни чеклаш;

- ахборот оқимини фильтрлаш ва ўзгартириш, масалан, вирусларни динамик тарзда қидириш ва ахборотни шаффоф шифрлаш;

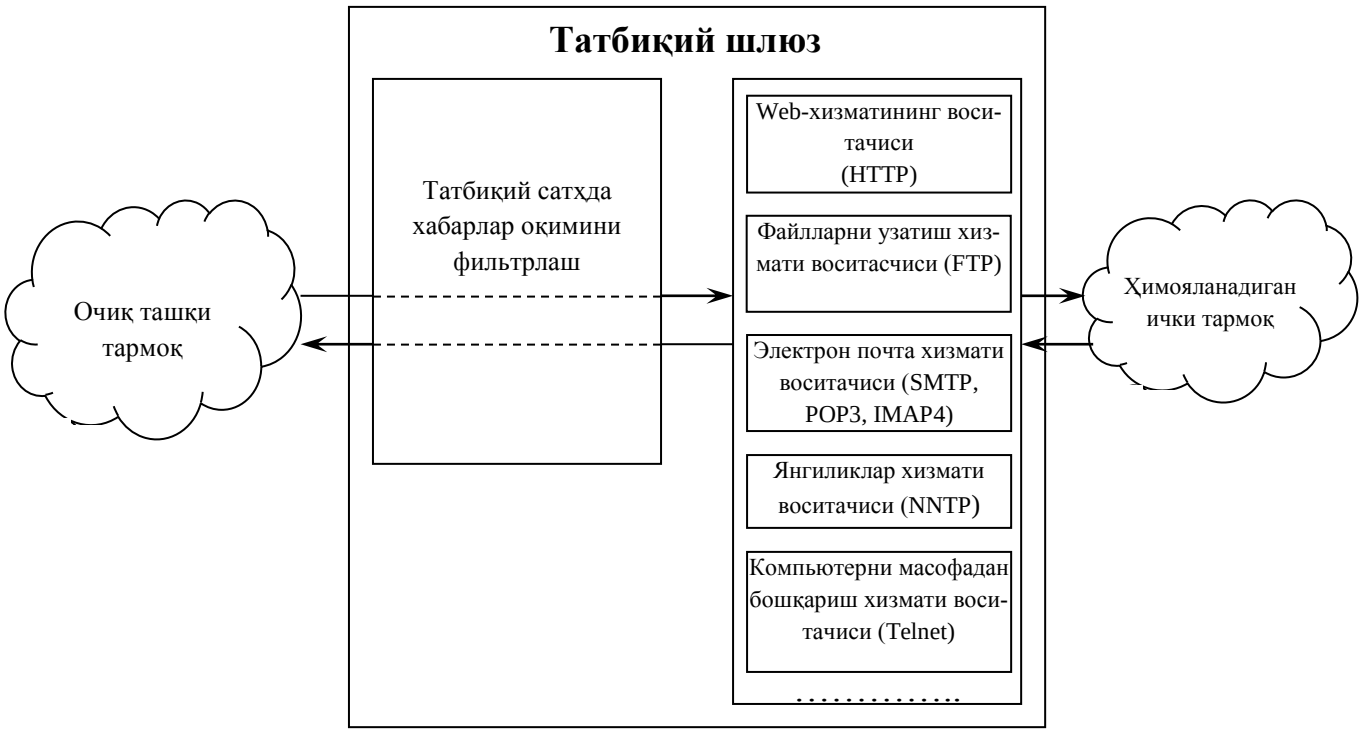
- ходисаларни қайдлаш, ходисаларга реакция кўрсатиш, ҳамда қайдланган ахборотни тахлиллаш ва хисоботларни генерациялаш;

- ташқи тармокдан сўралувчи маълумотларни кэшлаш.

Татбиқий сатҳ шлюзи функциялари воситачилик функцияларига тааал-

луқли бўлганлиги сабабли, бу шлюз универсал компьютер ҳисобланади ва бу компьютерда ҳар бир хизмат кўрсатилувчи татбиқий протокол (HTTP, FTP, SMTP, NNTP ва ҳ.) учун биттадан воситачи дастур (экранловчи агент) ишлатилади. TCP/IPнинг ҳар бир хизматининг воситачи дастури (applicationproxy) айнан шу хизматга тааллуқли хабарларни ишлашга ва ҳимоялаш функцияларини бажаришга мўлжалланган.

Татбиқий сатҳ шлюзи мос экранловчи агентлар ёрдамида кирувчи ва чиқувчи пакетларни ушлаб қолади, ахборотни нусхалайди ва қайта жўнатади, яъни ички ва ташқи тармоқлар орасидаги тўғридан-тўғри уланишни истисно қилган ҳолда, сервер-воситачи функциясини бажаради (8.9-расм).



8.9-расм. Татбиқий шлюзнинг ишлаш схемаси.

Татбиқий сатҳ шлюзи ишлатадиган воситачилар сеанс сатҳи шлюзларининг канал воситачиларидан жиддий фарқланади. Биринчидан, татбиқий сатҳ шлюзлари муайян иловалар (дастурий серверлар) билан боғланган, иккинчидан улар OSI моделининг татбиқий сатҳида хабарлар оқимини фильтрлашлари мумкин.

Татбиқий сатҳ шлюзлари воситачи сифатида мана шу мақсадлар учун

махсус ишлаб чиқилган TCP/IPнинг муайян хизматларининг дастурий серверлари – HTTP, FTP, SMTP, NNTP ва ҳ. – серверларидан фойдаланади. Бу дастурий серверлар брандмауэрларда резидент режимида ишлайди ва TCP/IPнинг мос хизматларига тааллуқли ҳимоялаш функцияларини амалга оширади. UDP трафигига UDP-пакетлар таркибининг махсус транслятори хизмат кўрсатади.

Ички тармоқ ишчи сервери ва ташқи тармоқ компьютери орасида иккита уланиш амалга оширилади: ишчи станциядан брандмауэргача ва брандмауэрдан белгиланган жойгача. Канал воситачиларидан фарқли ҳолда, татбиқий сатҳ шлюзининг воситачилари фақат ўзлари хизмат қилувчи иловалар генерациялаган пакетларни ўтказади. Масалан, HTTP хизматининг воситачи-дастури фақат шу хизмат генерациялаган трафикни ишлайди.

Агар қандайдир иловада ўзининг воситачиси бўлмаса, татбиқий сатҳдаги шлюз бундай иловани ишлай олмайди ва у блокировка қилинади. Масалан, агар татбиқий сатҳдаги шлюз фақат HTTP, FTP ва Telnet воситачи-дастурларидан фойдаланса, у фақат шу хизматларга тегишли пакетларни ишлайди ва қолган хизматларнинг пакетларини блокировка қилади.

Татбиқий сатҳ шлюзи воситачилари, канал воситачиларидан фарқли ҳолда, ишланувчи маълумотлар таркибини текширишни таъминлайди. Улар ўзлари хизмат кўрсатадиган татбиқий сатҳ протоколларидаги командаларнинг алоҳида хилларини ва хабарлардаги ахборотлани фильтрлашлари мумкин.

Татбиқий сатҳ шлюзини созлашда ва хабарларни фильтрлаш қоидаларини тавсифлашда қуйидаги параметрлардан фойдаланилади: сервис номи, ундан фойдаланишнинг жоиз вақт оралиғи, ушбу сервисга боғлиқ хабар таркибига чеклашлар, сервис ишлатадиган компьютерлар, фойдаланувчи идентификатори, аутентификациялаш схемалари ва ҳ.

Татбиқий сатҳ шлюзи қуйидаги афзалликларга эга:

- аксарият воситачилик функцияларини бажара олиши туфайли локал тармоқ ҳимоясининг юқори даражасини таъминлайди;

- иловалар сатҳида ҳимоялаш кўпгина қўшимча текширишларни амалга оширишга имкон беради, натижада дастурий таъминот камчиликларига асосланган муваффақиятли хужумлар ўтказиш эҳтимоллиги камаяди;

- татбиқий сатҳ шлюзининг ишга лаёқатлиги бузилса, бўлинувчи тармоқлар орасида пакетларнинг тўппа-тўғри ўтиши блокировка қилинади, натижада, рад қилиниши туфайли ҳимояланувчи тармоқнинг хавфсизлиги пасаймайди.

Татбиқий сатҳ шлюзининг камчиликларига қуйидагилар киради:

- нархининг нисбатан юқорилиги;

- брандмауэрнинг ўзи, ҳамда уни ўрнатиш ва конфигурациялаш муолажаси етарлича мураккаб;

- компьютер платформаси унумдорлигига ва ресурслари ҳажмига қуйиладиган талабларнинг юқорилиги;

- фойдаланувчилар учун шаффофликнинг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши.

Охирги камчиликка батафсил тухталамиз. Воситачилар сервер ва мижоз орасида пакетлар узатилишида оралиқ ролини бажаради. Аввал воситачи билан уланиш ўрнатилади, сўнгра воситачи адресат билан уланишни яратиш ёки яратмаслик хусусида қарор қабул қилади. Мос ҳолда татбиқий сатҳ шлюзи ишлаши жараёнида ҳар қандай рухсат этилган уланишни қайталайди. Натижада фойдаланувчилар учун шаффофлик йўқолади ва уланишга хизмат қилишга қўшимча ҳаражат сарфланади.

Татбиқий сатҳ шлюзининг фойдаланувчилар учун шаффофлигининг йўқлиги ва тармоқлараро алоқа ўрнатилишида ўтказиш қобилиятининг сусайиши каби жиддий камчиликларини бартараф этиш мақсадида пакетларни фильтрлашнинг янги технологияси ишлаб чиқилган. Бу технологияни баъзида *уланиш холатини назоратлашли фильтрлаш* (statefulinspection) ёки *эксперт сатҳидаги фильтрлаш* деб юритишади. Бундай фильтрлаш пакетлар ҳолатини кўп сатҳли таҳлиллашнинг махсус усуллари (SMLT) асосида амалга оширилади.

Ушбу гибрид технология тармоқ сатҳида пакетларни ушлаб қолиш ва ундан уланишни назорат қилишда ишлатилувчи татбиқий сатҳ ахборотини чиқариб олиш орқали уланиш ҳолатини кузатишга имкон беради.

Ишлаши асосини ушбу технология ташкил этувчи тармоқлараро экран *эксперт сатҳ брандмауэри* деб юритилади. Бундай брандмауэрлар ўзида экранловчи маршрутизаторлар ва татбиқий сатҳ шлюзлари элементларини уйғунлаштиради. Улар ҳар бир пакет таркибини берилган хавфсизлик сиёсатига мувофиқ баҳолайдилар.

Шундай қилиб эксперт сатҳидаги брандмауэрлар қуйидагиларни назоратлашга имкон беради:

- мавжуд қоидалар жадвали асосида ҳар бир узатилувчи пакетни;
- ҳолатлар жадвали асосида ҳар бир сессияни;
- ишлаб чиқилган воситачилар асосида ҳар бир иловани.

Эксперт сатҳ тармоқлараро экранларининг афзалликлари сифатида уларнинг фойдаланувчилар учун шаффофлигини, ахборот оқимини ишлашининг юқори тезкорлигини ҳамда улар орқали ўтувчи пакетларнинг IP-адресларини ўзгартирмаслигини кўрсатиш мумкин. Охирги афзаллик. IP-адресдан фойдаланувчи татбиқий сатҳнинг ҳар қандай протоколининг бундай брандмауэрлардан ҳеч қандай ўзгаришсиз ёки махсус дастурлашсиз бирга ишлай олишини англатади.

Бундай брандмауэрларнинг авторизацияланган мижоз ва ташқи тармоқ компьютери орасида тўғридан-тўғри уланишга йўл қўйиши, ҳимоянинг унчалик юқори бўлмаган даражасини таъминлайди. Шу сабабли амалда эксперт сатҳини фильтрлаш технологиясидан комплекс брандмауэрлар ишлаши самарадорлигини оширишда фойдаланилади. Эксперт сатҳнинг фильтрлаш технологиясини ишлатувчи комплекс брандмауэрларга мисол тариқасида FireWall-1 ва ON Guardларни кўрсатиш мумкин.

Назорат саволлари:

1. Экранловчи маршрутизаторларнинг ишлаш принципини тушунтириб берин.

2. Сеанс сатҳи шлюзининг функцияларини ёритиб беринг.

3. Татбиқий сатҳ шлюзи қандай тартибда ишлашини тушунтириб беринг.

4. Экранловчи маршрутизаторлар, сеанс сатҳи шлюзи ва татбиқий сатҳ шлюзи қўллайдиган функцияларнинг бир биридан фарқи нимада?

8.3. Тармоқлараро экранлар асосидаги тармоқ ҳимоясининг схемалари

Тармоқлараро алоқани самарали ҳимоялаш учун брандмауэр тизими тўғри ўрнатилиши ва конфигурацияланиши лозим. Ушбу жараён қуйидагиларни ўз ичига олади:

- тармоқлараро алоқа сиёсатини шакллантириш;
- брандмауэрни улаш схемасини танлаш ва параметрларини созлаш.

Тармоқлараро алоқа сиёсатини шакллантириш

Тармоқлараро алоқа сиёсатини шакллантиришда қуйидагиларни аниқлаш лозим:

- тармоқ сервисларидан фойдаланиш сиёсати;
- тармоқлараро экран ишлаши сиёсати.

Тармоқ сервисларидан фойдаланиш сиёсати ҳимояланувчи компьютер тармоғининг барча сервисларини тақдим этиш, ҳамда улардан фойдаланиш қоидаларини белгилайди. Ушбу сиёсат доирасида тармоқ экрани орқали тақдим этилувчи барча сервислар ва ҳар бир сервис учун мижозларнинг жоиз адреслари берилиши лозим. Ундан ташқари, фойдаланувчилар учун қачон ва қайси фойдаланувчилар қайси сервисдан ва қайси компьютерда фойдаланишларини тавсифловчи қоидалар кўрсатилиши лозим. Фойдаланиш усулларига чеклашлар ҳам берилади. Бу чеклашлар фойдаланувчиларнинг Internetнинг ман этилган сервисларидан айланма йўл орқали фойдаланишларига йўл қўймаслик учун зарур. Фойдаланувчилар ва компьютерларни аутентификациялаш қоидалари, ҳамда ташкилот локал тармоғи ташқарисидаги фойдаланувчиларнинг ишлаш шароитлари алоҳида белгиланиши лозим.

Тармоқлараро экран ишлаши сиёсатида тармоқлараро алоқани бошқаришнинг брандмауэр ишлаши асосидаги базавий принципи берилади. Бундай принципларнинг қуйидаги иккитасидан бири танланиши мумкин:

- ошкора рухсат этилмагани ман қилинган;
- ошкора ман этилмаганига рухсат берилган.

"Ошкора рухсат этилмагани ман қилинган" принципи танланганида тармоқлараро экран шундай созланадики, ҳарқандай рухсат этилмаган тармоқлараро алоқалар блокировка қилинади. Ушбу принцип ахборот хавфсизлигининг барча соҳаларида ишлатилувчи фойдаланишнинг мумтоз моделига мос келади. Бундай ёндашиш, имтиёзларни минималлаштириш принципини адекват амалга оширишга имкон бериши сабабли, хавфсизлик нуқтаи назаридан яхшироқ ҳисобланади. Моҳияти бўйича "ошкора рухсат этилмагани ман қилинган" принципи зарар келтириши фактини эътироф этишдир. Таъкидлаш лозимки, ушбу принципга асосан таърифланган фойдаланиш қоидалари фойдаланувчиларга маълум ноқулайликлар туғдириши мумкин.

"Ошкора ман этилмаганига рухсат берилган" принципи танланганида тармоқлараро экран шундай созланадики, фақат ошкора ман этилган тармоқлараро алоқалар блокировка қилинади. Бу ҳолда, фойдаланувчилар томонидан тармоқ сервисларидан фойдаланиш қулайлиги ошади, аммо тармоқлараро алоқа хавфсизлиги пасаяди. Фойдаланувчиларнинг тармоқлараро экранни четлаб ўтишларига имкон туғилади, масалан улар сиёсат ман қилмаган (ҳатто сиёсатда кўрсатилмаган) янги сервисларидан фойдаланишлари мумкин. Ушбу принцип амалга оширилишида ички тармоқ хакерларнинг хужумларидан камроқ ҳимояланган бўлади. Шу сабабли, тармоқлараро экранларни ишлаб чиқарувчилари одатда ушбу принципдан фойдаланмайдилар.

Тармоқлараро экран симметрик эмас. Унга ички тармоқнинг ташқи тармоқдан ва аксинча фойдаланишни чекловчи қоидалар алоҳида берилади. Умумий ҳолда, тармоқлараро экраннинг иши қуйидаги иккита гуруҳ функцияларни динамик тарзда бажаришга асосланган:

- у орқали ўтаётган ахборот оқимини фильтрлаш;

- тармоқлараро алоқа амалга оширилишида воситачилик.

Оддий тармоқлараро экранлар бу функцияларнинг бирини бажаришга мўлжалланган. Комплекс тармоқлараро экранлар ҳимоялашнинг кўрсатилган функцияларининг биргаликда бажарилишини таъминлайди.

Тармоқлараро экранларни улашнинг асосий схемалари. Корпоратив тармоқни глобал тармоқларга улаганда ҳимояланувчи тармоқнинг глобал тармоқдан ва глобал тармоқнинг ҳимояланувчи тармоқдан фойдаланишини чеклаш, ҳамда уланувчи тармоқдан глобал тармоқнинг масофадан рухсатсиз фойдаланишидан ҳимоялашни таъминлаш лозим. Бунда ташкилот ўзининг тармоғи ва унинг компонентлари хусусидаги ахборотни глобал тармоқ фойдаланувчиларидан бекитишга манфаатдор. Масофадаги фойдаланувчилар билан ишлаш ҳимояланувчи тармоқ ресурсларидан фойдаланишнинг қатъий чекланишини талаб этади.

Ташкилотдаги корпоратив тармоқ таркибида кўпинча ҳимояланишнинг турли сатҳли бирнеча сегментларга эга бўлиши эҳтиёжи туғилади:

- бемалол фойдаланилувчи сегментлар (масалан, реклама WWW-серверлари);

- фойдаланиш чегараланган сегментлар (масалан, ташкилотнинг масофадаги узеллари ходимларининг фойдаланиши учун);

- ёпиқ сегментлар (масалан, ташкилотнинг молия локал қисм тармоғи)

Тармоқлараро экранларни улашда турли схемалардан фойдаланиш мумкин. Бу схемалар ҳимояланувчи тармоқ ишлаши шароитига, ҳамда ишлатиладиган брандмауэрларнинг тармоқ интерфейслари сонига ва бошқа характеристикаларига боғлиқ. Тармоқлараро экранни улашнинг қуйидаги схемалари кенг тарқалган:

- экранловчи маршрутизатордан фойдаланилган ҳимоя схемалари;

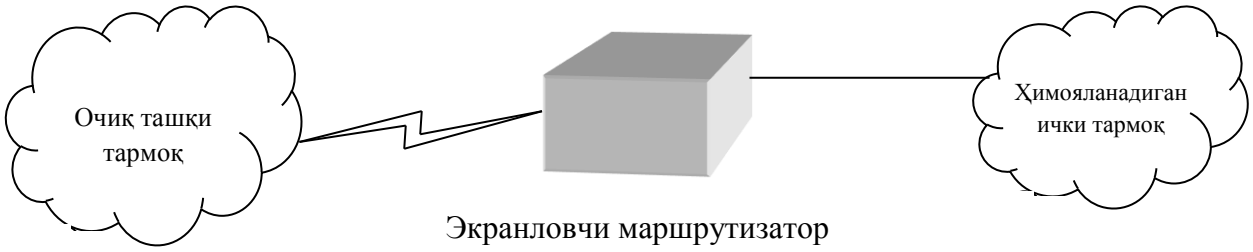
- локал тармоқни умумий ҳимоялаш схемалари;

- ҳимояланувчи ёпиқ ва ҳимояланмайдиган очиқ кисмтармоқли схемалар;

- ёпиқ ва очиқ қисм тармоқларни алоҳида ҳимояловчи схемалар.

Экранловчи маршрутизатордан фойдаланилган ҳимоя схемаси.

Пакетларни фильтрлашга асосланган тармоқлараро экран кенг тарқалган ва амалга оширилиши осон. У ҳимояланувчи тармоқ ва бўлиши мумкин бўлган ғаним очиқ тармоқ орасида жойлашган экранловчи маршрутизатордан иборат (8.10-расм).



8.10-расм. Тармоқлараро экран – экранловчи маршрутизатор

Экранловчи маршрутизатор (пакетли фильтр) кирувчи ва чиқувчи пакетларни уларнинг адреслари ва портлари асосида блокировка қилиш ва фильтрлаш учун конфигурацияланган.

Ҳимояланувчи тармоқдаги компьютерлар Internetдан тўғридан-тўғри фойдалана олади, Internetнинг улардан фойдаланишининг кўп қисми эса блокировка қилинади. Умуман, экранловчи маршрутизатор юқорида тавсифланган ҳимоялаш сиёсатидан исталганини амалга ошириши мумкин. Аммо, агар маршрутизатор пакетларни манба порти ва кириш йўли ва чиқиш йўли портлари номери бўйича фильтрламаса, "ошкора рухсат этилмагани ман қилинган" сиёсатини амалга ошириш қийинлашади.

Пакетларни фильтрлашга асосланган тармоқлараро экраннинг камчиликлари қуйидагилар:

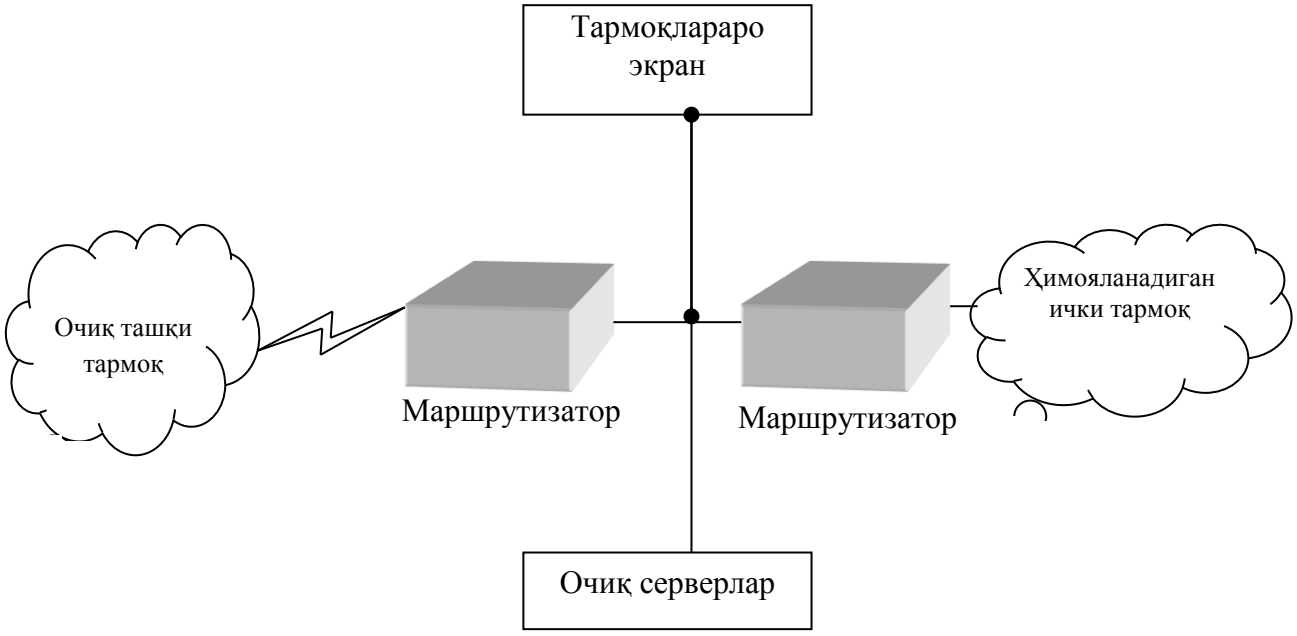
- фильтрлаш қоидаларининг мураккаблиги; баъзи ҳолларда бу қоидалар мажмуи бажарилмаслиги мумкин;

- фильтрлаш қоидаларини тўлиқ тестлаш мумкин эмаслиги; бу тармоқни тестланмаган хужумлардан ҳимояланмаслигига олиб келади;

- ходисаларни руйхатга олиш имкониятининг йўқлиги; натижада маъмурга машрутизаторнинг хужумга дуч келганлигини ва обрўсизлантирилганлигини аниқлаш қийинлашади.

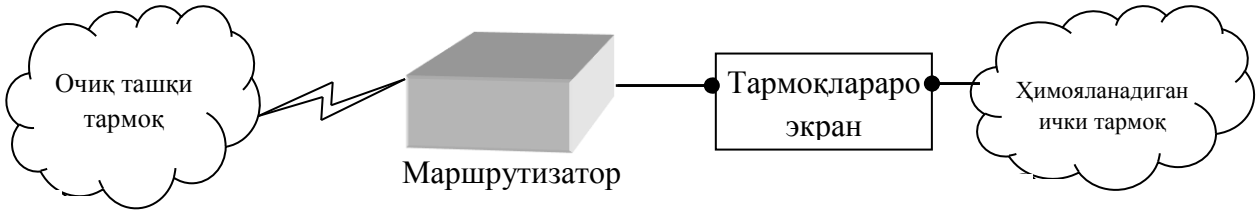
Локал тармоқни умумий ҳимоялаш схемалари. Битта тармоқ интерфейсли брандмауэрлардан фойдаланилган ҳимоялаш схемалари (8.11-расм) хавфсизлик ва конфигурациялашнинг қулайлиги нуқтаи назаридан самарасиз ҳисобланади. Улар ички ва ташқи тармоқларни физик ажратмайдилар, демак, тармоқлараро алоқанинг ишончли ҳимоясини таъминлай олмайдилар.

Локал тармоқни умумий ҳимоялаш схемаси энг оддий ечим бўлиб, унда брандмауэр локал тармоқни ташқи ғаним тармоқдан бутунлай экранлайди (8.12-расм). Маршрутизатор ва брандмауэр орасида фақат битта йўл бўлиб, бу йўл орқали бутун трафик ўтади. Брандмауэрнинг ушбу варианти "ошкора рухсат этилмагани ман қилинган" принципига асосланган ҳимоялаш сиёсатини амалга оширади. Одатда маршрутизатор шундай созланадики, брандмауэр ташқаридан кўринадиган ягона машина бўлади.



8.11- расм. Битта тармоқ интерфейсли firewall ёрдамида локал тармоқни ҳимоялаш

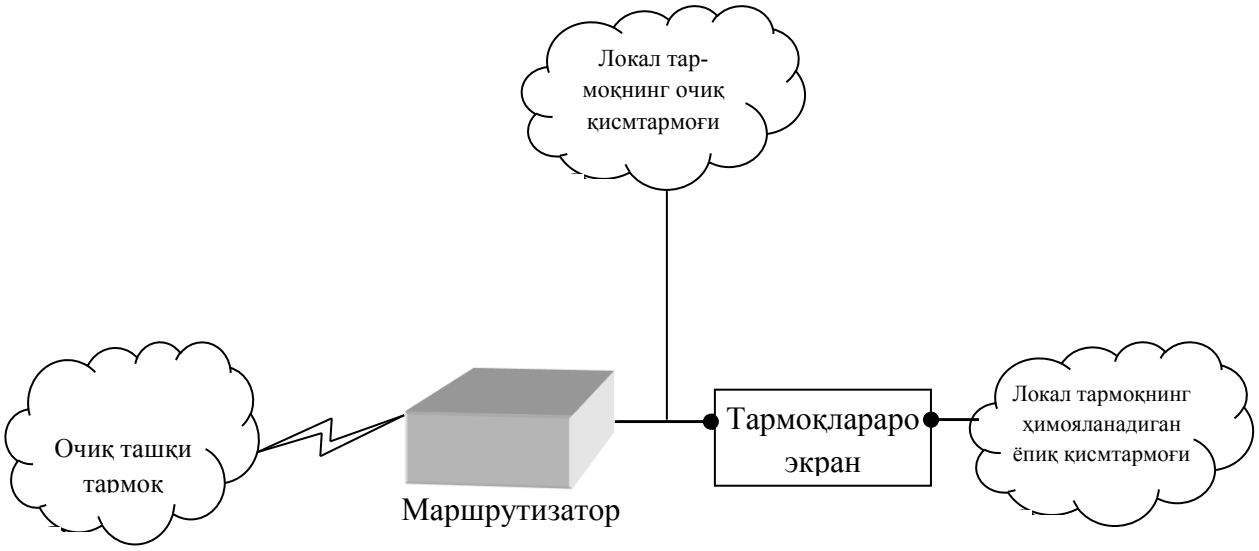
Локал тармоқ таркибидаги очиқ серверлар ҳам тармоқлараро экранлар томонидан ҳимояланади. Аммо, ташқи тармоқ фойдалана оладиган серверларни ҳимояланувчи локал тармоқларнинг бошқа ресурслари билан бирлаштириш тармоқлараро алоқа хавфсизлигини жиддий пасайтиради.



8.12-расм. Локал тармоқни умумий ҳимоялаш схемаси

Тармоқлараро экран фойдаланадиган хостга фойдаланувчиларни кучайтирилган аутентификациялаш учун дастур ўранатилиши мумкин.

Ҳимояланувчи ёпиқ ва ҳимояланмайдиган очиқ қисмтармоқли схемалар. Агар локал тармоқ таркибида умумфойдаланувчи очиқ серверлар бўлса уларни тармоқлараро экрандан олдин очиқ қисмтармоқ сифатида чиқариш мақсадга мувофиқ ҳисобланади (8.13-расм).



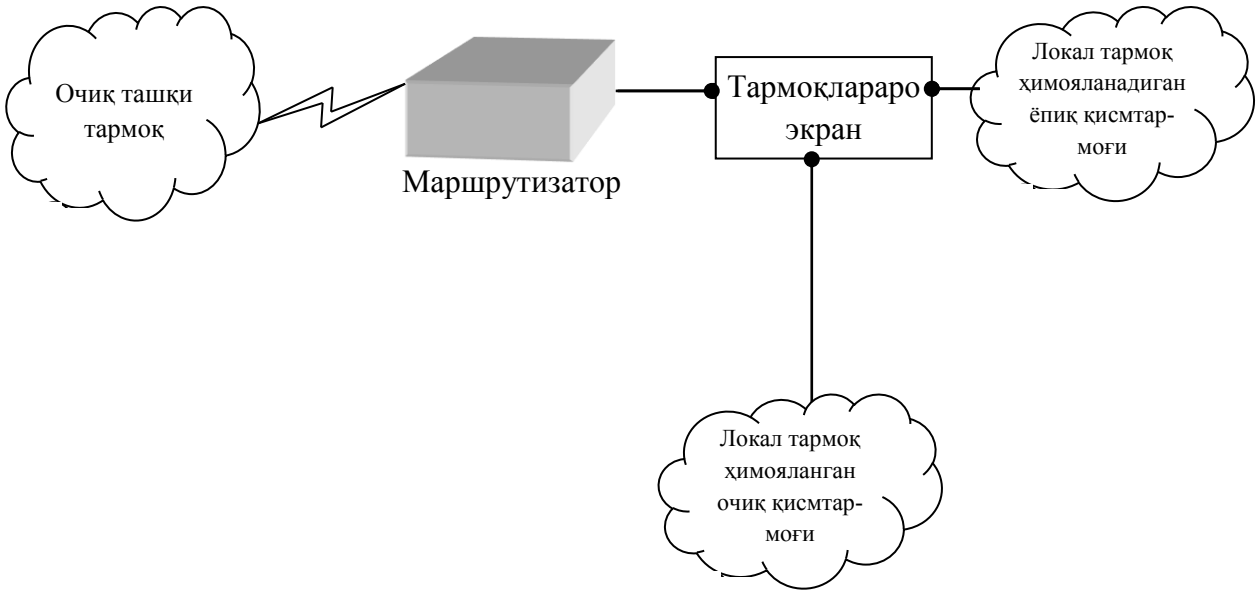
8.13-расм. Ҳимояланадиган ёпиқ ва ҳимояланмайдиган очиқ қисмтармоқли схема

Ушбу усул локал тармоқ ёпиқ қисмининг кучли ҳимояланишини, аммо тармоқлараро экрангача жойлашган очиқ серверларнинг пасайган ҳимояланишини таъминлайди.

Баъзи брандмауэрлар бу серверларни ўзида жойлаштиради. Аммо бу брандмауэрнинг хавфсизлиги ва компьютернинг юкланиши нуқтаи назаридан яхши ечим ҳисобланмайди. Ҳимояланувчи ёпиқ ва ҳимояланмайдиган

очиққисмтармоқли схемани очиқ қисмтармоқ хавфсизлигига қўйиладиган талабларнинг юқори бўлмаган ҳолларида ишлатилиши мақсадга мувофиқ ҳисобланади. Агар очиқ сервер хавфсизлигига юқори талаблар қўйилса, ёпиқ ва очиқ қисмтармоқларни алоҳида ҳимоялаш схемаларидан фойдаланиш зарур.

Ёпиқ ва очиққисм тармоқларни алоҳида ҳимояловчи схемалар. Бундай схемалар учта тармоқ интерфейсли битта брандмауэр (8.14-расм) ёки иккита тармоқ интерфейсли иккита брандмауэр (8.15-расм) асосида қурилиши

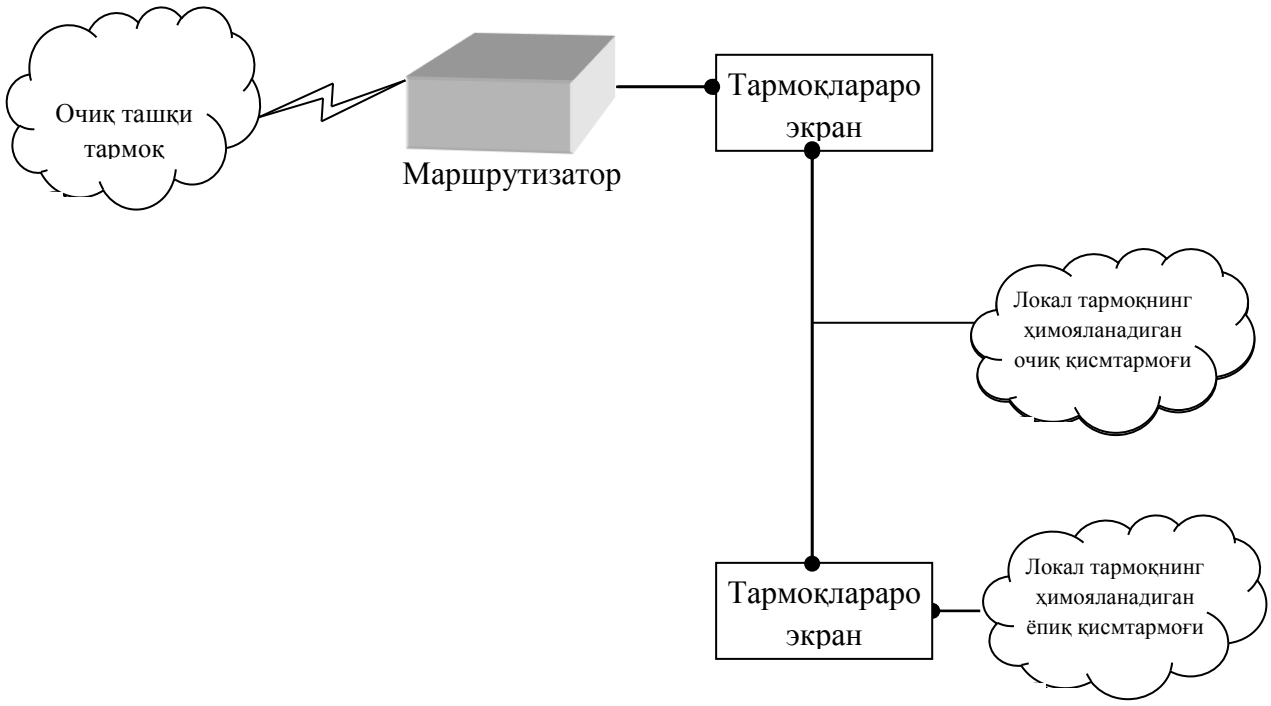


8.14 -расм. Учта тармоқ интерфейсли бир брандмауэр асосида ёпиқ ва очиқ қисмтармоқларни алоҳида ҳимоялаш схемаси

мумкин. Иккала ҳолда ҳам очиқ ва ёпиқ қисмтармоқлардан фақат тармоқлараро экран орқали фойдаланиш мумкин. Бунда очиқ қисмтармоқдан фойдаланиш ёпиққисмтармоқдан фойдаланишга имкон бермайди.

Иккита брандмауэрли схема тармоқлараро алоқа хавфсизлигининг юқори даражасини таъминлайди. Бунда ҳар бир брандмауэр ёпиқ тармоқни ҳимоялашнинг алоҳида эшелонини ҳосил қилади, ҳимояланувчи очиқ қисмтармоқ эса экранловчи қисмтармоқ сифатида иштирок этади. Одатда экранловчи қисмтармоқ шундай конфигурацияланадики, қисмтармоқ компьютеридан ғаним ташқи тармоқ ва локал тармоқнинг ёпиққисмтармоғи фойдалана олсин. Аммо ташқи тармоқ ва ёпиқ қисмтармоқ орасида тўғридан-

тўғри ахборот пакетларини алмашиш мумкин эмас. Экранловчи қисмтармоқли тизимга хужум қилишда, бўлмаганида ҳимоянинг иккита мустақил чизиғини босиб ўтишга тўғри келади. Бу эса жуда мураккаб масала ҳисобланади. Тармоқлараро экран ҳолатларини мониторинглаш воситалари бундай уринишни доимо аниқлаши ва тизим маъмури ўз вақтида рухсатсиз фойдаланишга қарши зарурий чоралар кўриши мумкин.



8.15-расм. Иккита тармоқ интерфейсли иккита брандмауэр асосида ёпиқ ва очиқ қисмтармоқларни алоҳида ҳимоялаш схемаси

Таъкидлаш лозимки, алоқанинг коммутацияланувчи линияси орқали уланувчи масофадаги фойдаланувчиларнинг иши ҳам ташкилотда ўтказилувчи хавфсизлик сиёсатига мувофиқ назорат қилиниши шарт. Бундай масаланинг намунавий ҳал этилиши – зарурий функционал имкониятларга эга бўлган масофадан фойдаланиш серверини (терминал серверни) ўрнатиш. Терминал сервер бир неча асинхрон портларга ва локал тармоқнинг битта интерфейсига эга бўлган тизим ҳисобланади. Асинхрон портлар ва локал тармоқ орасида ахборот алмашиш фақат ташқи фойдаланувчини аутентификациялашдан кейин амалга оширилади.

Терминал серверни улашни шундай амалга ошириш лозимки, унинг

иши фақат тармоқлараро экран орқали бажарилсин. Бу масофалаги фойдаланувчиларнинг ташкилот ахборот ресурслари билан ишлаш хавфсизлигининг керакли даражасини таъминлашга имкон беради.

Терминал серверни очиқ кисмтармоқ таркибига киритилганида бундай уланиш жоиз ҳисобланади. Терминал серверннг дастурий таъминоти коммутацияланувчи каналлар орқали алоқа сеансларини маъмурлаш ва назоратлаш имкониятини таъминлаши лозим. Замонавий терминал серверларни бошқариш модуллари серверннг ўзини хавфсизлигини таъминлаш ва мижозларнинг фойдаланишини чегаралаш бўйича етарлича ривожланган имкониятларга эга ва қуйидаги функцияларни бажаради:

- кетма-кет портлардан, PPP протоколи бўйича масофадан, ҳамда маъмур консолидан фойдаланишда локал паролни ишлатиш;

- локал тармоқнинг қандайдир машинасининг аутентификациялашга сўровидан фойдаланиш;

- аутентификациялашнинг ташқи воситаларидан фойдаланиш;

- терминал сервери портларидан фойдаланишни назоратловчи руйхатни ўрнатиш;

- терминал сервер орқали алоқа сеансларини протоколлаш.

Шахсий ва тақсимланган тармоқ экранлари. Охирги бир неча йил мобайнида корпоратив тармоқ тузилмасида маълум ўзгаришлар содир бўлди. Агар илгари бундай тармоқ чегараларини аниқ белгилаш мумкин бўлган бўлса, ҳозирда бу мумкин эмас. Яқиндаёқ бундай чегара барча маршрутизаторлар ёки бошқа қурилмалар (масалан, модемлар) орқали ўтар ва улар ёрдамида ташқи тармоқларга чиқилар эди. Аммо ҳозирда тармоқлараро экран орқали ҳимояланувчи тармоқнинг тўла ҳуқуқли эгаси – ҳимояланувчи периметр ташқарисидаги ходим ҳисобланади. Бундай ходимлар сирасига уйдаги ёки меҳнат сафаридаги ходимлар киради. Шубхасиз, уларга ҳам ҳимоя зарур. Аммо барча анъанавий тармоқлараро экранлар шундай қурилганки, ҳимояланувчи фойдаланувчилар ва ресурслар уларнинг ҳимоясида корпоратив ёки локал тармоқнинг ички томонида бўлишлари шарт. Бу эса мобил фойдала-

нувчилар учун мумкин эмас.

Бу муаммони ечиш учун қуйидаги ёндашишлар таклиф этилган:

- тақсимланган тармоқлараро экранлардан (distributed firewall) фойдаланиш;

- виртуал хусусий тармоқVPNлар имкониятидан фойдаланиш.

Тақсимланган тармоқлараро экран тармоқнинг алоҳида компьютерини ҳимояловчи марказдан бошқарилувчи тармоқ мини-экранлар мажмуидир.

Тақсимланган брандмауэрларнинг қатор функциялари (масалан марказдан бошқариш, хавфсизлик сиёсатини тарқатиш) шахсий фойдаланувчилар учун ортиқча бўлганлиги сабабли, тақсимланган брандмауэрлар модификацияланди. Янги ёндашиш *шахсий тармоқли экранлаш технологияси* номини олди. Бунда тармоқли экран ҳимояланувчи шахсий компьютерда ўрнатилади. Компьютернинг шахсий экрани (personal firewall) ёки тармоқли экранлаш тизими деб аталувчи бундай экран, бошқа барча тизимли ҳимоялаш воситаларига боғлиқ бўлмаган ҳолда бутун чиқувчи ва кирувчи трафикни назоратлайди. Алоҳида компьютерни экранлашда тармоқ сервисдан фойдаланувчанлик мададланади, аммо ташқи фаолликнинг юкланиши пасаяди. Натижада, шу тариқа ҳимояланувчи компьютер ички сервисларининг заифлиги пасаяди, чунки четки нияти бузуқ одам олдин, ҳимоялаш воситалари синчиклаб ва қатъий конфигурацияланган экранни босиб ўтиши лозим.

Тақсимланган тармоқлараро экраннинг шахсий экрандан асосий фарқи-тақсимланган тармоқлараро экранда марказдан бошқариш функциясининг борлиги. Агар шахсий тармоқли экранлар улар ўрнатилган компьютер орқали бошқарилса (уй шароитида қўлланишга жуда мос), тақсимланган тармоқлараро экранлар ташкилотнинг бош офисида ўрнатилган бошқаришнинг умумий консоли томонидан бошқарилиши мумкин.

Корпоратив тармоқ рухсатсиз фойдаланишдан ҳақиқатан ҳам ҳимояланган ҳисобланади, қачонки унинг Internetдан кириш нуқтасида ҳимоя воситалари ҳамда ташкилот локал тармоғи фрагментларини, корпоратив серверларини ва алоҳида компьютерлар хавфсизлигини таъминловчи ечимлар

мавжуд бўлса. Тақсимланган ёки шахсий тармоқлараро экран асосидаги ечимлар алоҳида компьютерлар, корпоратив серверлар ва ташкилот локал тармоқ фрагментлари хавфсизлигини таъминлашни аъло даражада бажаради.

Тақсимланган тармоқлараро экранлар, анъанавий тармоқлараро экранлардан фарқли равишда, қўшимча дастурий таъминот бўлиб, хусусан корпоратив серверларни, масалан Internet-серверларни ишончли ҳимоялаши мумкин. Корпоратив тармоқни ҳимоялашнинг оқилона ечими – ҳимоялаш воситасини у ҳимоя қилувчи сервери билан бир платформада жойлаштиришдир. 8.16-расмда корпоратив серверларни тақсимланган тармоқлараро экранлар ёрдамида ҳимоялаш схемаси келтирилган.

Анъанавий ва тақсимланган тармоқлараро экранлар қуйидаги кўрсаткичлари бўйича таққосланади.

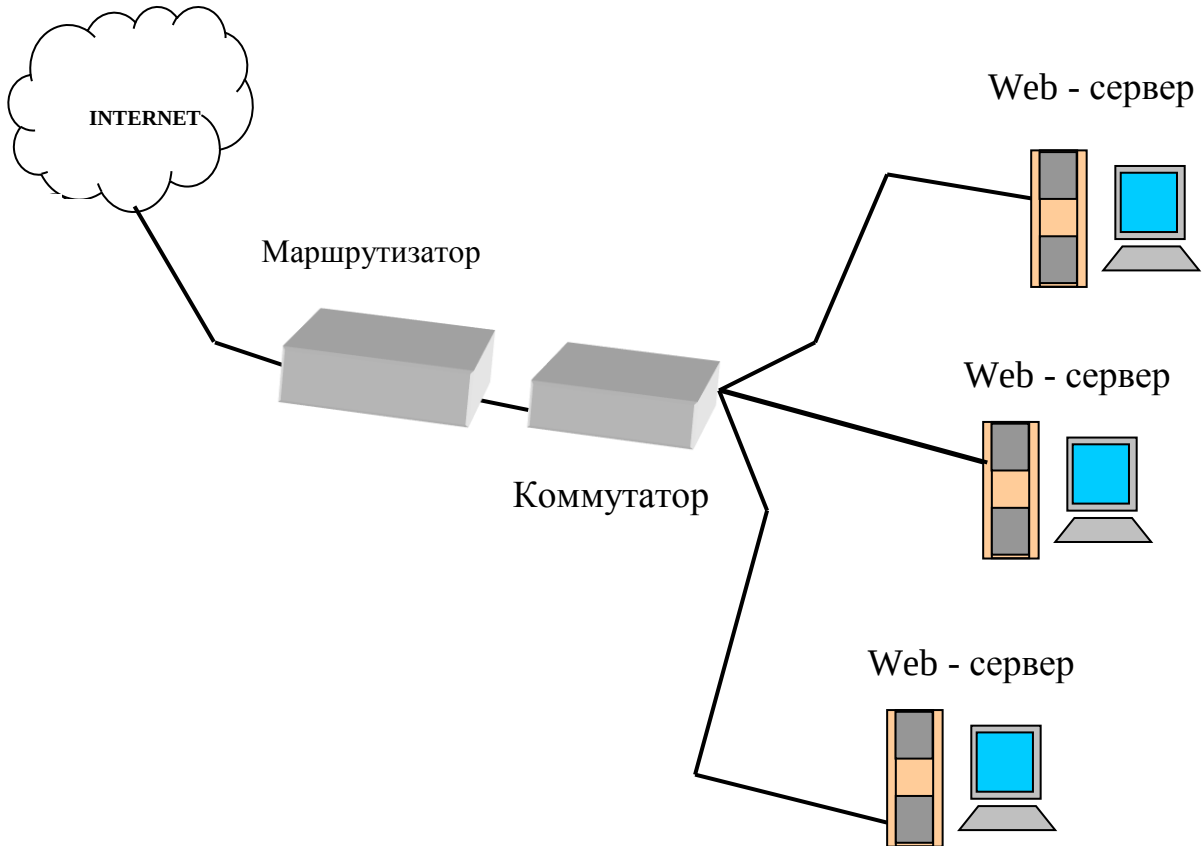
Самарадорлик. Анъанавий брандмауэр кўпинча тармоқ периметри бўйича жойлаштирилади, яъни у ҳимоянинг бир қатламини таъминлайди холос. Агар бу ягона қатлам бузилса, тизим ҳар қандай хужумга бардош бера олмайди. Тақсимланган брандмауэр операцион тизимнинг ядро сатҳида ишлайди ва барча кирувчи ва чиқувчи пакетларни текшириб корпоратив серверларни ишончли ҳимоялайди.

Ўрнатилишининг осонлиги. Анъанавий брандмауэр корпоратив тармоқ конфигурациясининг бўлими сифатида ўрнатилиши лозим. Тақсимланган брандмауэр дастурий таъминот бўлиб, саноқли дақиқаларда ўрнатилади ва олиб ташланади.

Бошқариш. Анъанавий брандмауэр тармоқ маъмури томонидан бошқарилади. Тақсимланган брандмауэр тармоқ маъмури ёки локал тармоқ фойдаланувчиси томонидан бошқарилиши мумкин.

Унумдорлик. Анъанавий брандмауэр тармоқлараро алмашишни таъминловчи қурилма бўлиб, унумдорлиги пакет/дақиқа бўйича белгиланган чеклашга эга. У бир-бири билан коммутацияланувчи маҳаллий тармоқ орқали боғланган ўсувчи сервер парклари учун тўғри келмайди. Тақсимланган брандмауэр қабул қилинган хавфсизлик сиёсатига зиён

етказмасдан сервер паркларини ўсишига имкон беради.



8.16 -расм. Тақсимланган тармоқлараро экранлар ёрдамида корпоратив серверларни ҳимоялаш

Нархи. Анъанавий брандмауэр, одатда функциялари белгиланган, нархи етарлича юқори тизим ҳисобланади. Брандмауэрнинг тақсимланган маҳсулотлари дастурий таъминот бўлиб, анъанавий тармоқлараро экранлар нархининг 1/5 ёки 1/10 гатенг.

Назорат саволлари:

1. Тармоқларни экранловчи маршрутизаторлар ёрдамида ҳимоялаш схемасини тушунтириб беринг.
2. Тармоқлараро экран ёрдамида локал тармоқни ҳимоялаш схемасини ёритиб беринг.
3. Ҳимояланадиган ёпиқ ва ҳимояланмайдиган очиқ қисмтармоқли схемани тушунтириб беринг.

4. Ёпиқ ва очиқ қисмтармоқларни тармоқлараро экранлар ёрдамида алоҳида ҳимоялаш схемасининг моҳияти.

5. Иккита тармоқлараро экран орқали очиқ ва ёпиқ қисмтармоқларни алоҳида ҳимоялаш схемасини тавсифлаб беринг.

6. Шахсий ва тақсимланган тармоқлараро экранлар, уларнинг камчилик ва афзалликлари.

IX боб. ОПЕРАЦИОН ТИЗИМ ҲИМОЯСИ

9.1. Операцион тизим хавфсизлигини таъминлаш муаммолари

Ҳимояланган операцион тизим тушунчаси. Ахборотни ҳимоялашнинг аксарият дастурий воситалари татбиқий дастурлардир. Уларни бажариш учун операцион тизим (ОТ) томонидан мададлаш талаб этилади. Операцион тизим ишлайдиган муҳит *ишончли ҳисоблаш базаси* деб юритилади. Ишончли ҳисоблаш базаси операцион тизимнинг, дастурларнинг, тармоқ ресурсларининг, физик ҳимоялаш воситаларининг, ҳатто ташкилий муолажаларнинг ахборот ҳимоясини таъминловчи элементларнинг тўлиқ тўпламини ўз ичига олади. Буларнинг ичида энг асосийси ҳимояланган операцион тизим ҳисобланади.

Операцион тизим *ҳимояланган* ҳисобланади, агар у таҳдидларнинг асосий синфидан ҳимояланиш воситаларига эга бўлса. Ҳимояланган операцион тизим таркибида фойдаланувчиларнинг ОТ ресурсларидан фойдаланишларини чекловчи воситалар, ҳамда операцион тизим билан ишлашни бошлаган фойдаланувчиларнинг ҳақиқийлигини текшириш воситалари бўлиши шарт. Ундан ташқари ҳимояланган ОТ операцион тизимни тасодифан ёки атайин ишдан чиқаришга қарши таъсир воситаларига эга бўлиши шарт.

Агар операцион тизим барча таҳдидлардан эмас, балки бир қанча тахдидлардангина ҳимояланишни кўзда тутса, бундай ОТ *қисман ҳимояланган* деб юритилади.

Ҳимояланган операцион тизимни яратишдаги ёндашишлар.

Ҳимояланган операцион тизимни яратишда иккита асосий ёндашиш мавжуд – фрагментли ва комплекс. *Фрагментли ёндашишда* аввало битта тахдиддан сўнгра бошқа тахдиддан ва ҳ. ҳимояланиш ташкил этилади.

Фрагментли ёндашиш қўлланилганда ОТ ҳимояси қисмтизими, одатда, турли ишлаб чиқарувчилар тақдим этган бошқа-бошқа дастурлар тўпламидан иборат бўлади. Ушбу дастурий воситалар бир бирига боғлиқ бўлмаган тарзда

ишлайди, яъни уларнинг ўзаро узвий боғланишини ташкил этиши мумкин эмас. Ундан ташқари бундай қисмтизимнинг баъзи элементлари нотўғри ишлаши мумкин. Натижада тизим ишончлилиги кескин пасаяди.

Комплекс ёндашишда ҳимоя функциялари операцион тизимга унинг архитектурасини лойиҳалаш босқичида киритилади ва унинг ажралмас қисми ҳисобланади. Комплекс ёндашиш асосида яратилган ҳимоя қисмтизимнинг алоҳида элментлари ахборотни ҳимоялашни ташкил этиш билан боғлиқ турли масалалар ечилганида бир бири билан узвий боғланган бўлади. Шу сабабли ҳимоя қисмтизимининг алоҳида компонентлари орасида ихтилоф бўлмайди. Комплекс ёндашиш асосида ҳимоя қисмтизимини шундай қуриш мумкинки, ҳатто ОТ ишдан чиққанда ҳам нияти бузуқ шахс тизимнинг ҳимоя функцияларини ўчира олмайди. Фрагментли ёндашишда ҳимоя қисмтизимини бундай ташкил этиш мумкин эмас. Одатда комплекс ёндашиш асосида яратилувчи операцион тизимни ҳимоялаш қисмтизими шундай лойиҳаланадики, унинг баъзи элементларини алмаштириш мумкин бўлсин.

Ҳимоялашнинг маъмурий чоралари.

Операцион тизимни ҳимоялашнинг дастурий-аппарат воситалари ҳимоянинг маъмурий чоралари билан тўлдирилиши шарт. Маъмур томонидан доимий малакали мададсиз, ҳатто ишончли дастурий-аппарат ҳимоя ҳам бузилиши мумкин.

Ҳимоянинг асосий маъмурий чоралари қуйидагилар.

1. *Операцион тизимнинг, айниқса унинг ҳимоялаш қисмтизимининг тўғри ишлашини доимий назоратлаш*. Агар операцион тизим энг муҳим ходисаларнинг махсус журналда автоматик тарзда қайд этилишини мададласа бундай назоратни ташкил этиш қулай ҳисобланади.

2. *Хавфсизликнинг адекват сиёсатини ташкил этиш ва мададлаш*. Операцион тизимда қабул қилинган хавфсизлик сиёсатининг адекват бўлмаслиги нияти бузуқ шахснинг тизим ресурсларидан рухсатсиз фойдаланишига ва операцион тизимнинг ишончли ишлашини пасайишига сабаб бўлиши мумкин. Операцион тизим хавфсизлиги сиёсати нияти

бузуқнинг операцион тизим хавфсизлигини енгишга уринишига, ҳамда ОТ конфигурациясининг ўзгаришига, татбиқий дастурларининг ўрнатилишига ва йўқотилишига оператив тарзда реакция билдириб операцион тизимга доимо тузатиш киритиши лозим.

3. Фойдаланувчиларни операцион тизим билан ишлаганда *хавфсизлик чораларига риоя қилишлари лозимлигини уқтириш* ва ушбу чораларга риоя қилинишини назоратлаш.

4. Операцион тизим дастурлари ва маълумотларининг *резерв нусхаларини мунтазам тарзда яратиш ва янгилаш*.

5. Операцион тизимнинг конфигурацион маълумотларидаги ва хавфсизлик сиёсатидаги ўзгаришларни доимо назоратлаш. Ушбу ўзгаришлар хусусидаги ахборотни операцион тизим хавфсизлигини енгган нияти бузуқ шахсга ўзининг рухсатсиз ҳаракатларини ниқоблашга қийинчилик туғдириш учун ноэлектрон ахборот элтувчиларида сақлаш мақсадга мувофиқ ҳисобланади.

Таъкидлаш лозимки, муайян операцион тизимда ахборотни ҳимоялашнинг яна бошқа маъмурий чоралари талаб этилиши мумкин.

Назорат саволлари:

1. Ҳимояланган операцион тизим тушунчаси.
2. Ҳимояланган операцион тизимни яратишдаги ёндашишларни тушунтириб беринг.
3. Ҳимоялашнинг маъмурий чоралари нималарни ўз ичига олади?

9.2. Операцион тизимни ҳимоялаш қисмтизимининг архитектураси

Операцион тизимни ҳимоялаш қисмтизимининг асосий функциялари. Операцион тизимни ҳимоялаш қисмтизими қуйидига асосий функцияларни бажаради:

Идентификация, аутентификация ва авторизация. Ҳимояланган операцион тизимда ҳар қандай фойдаланувчи (фойдаланувчи субъект) тизим

билан ишлашдан олдин идентификацияни, аутентификацияни ва авторизацияни ўтиши лозим.Фойдаланувчи субъектнинг идентификациясига биноан субъект операцион тизимга ўзи хусусидаги идентификацияловчи ахборотни (исми, ҳисоб рақами ва ҳ.) билдиради ва шу тариқа ўзини идентификациялайди.Фойдаланувчи субъектнинг аутентификациясига биноан субъект операцион тизимга идентификацияловчи ахборотдан ташқари унинг ҳақиқатдан ҳам фойдаланувчи субъект эканлигини тасдиқловчи *аутентификацияловчи ахборотни* тақдим этади.Фойдаланувчи субъектнинг авторизацияси муваффақиятли идентификациялаш ва аутентификациялаш муолажаларидан сўнг амалга оширилада. Субъектни авторизациялашда операцион тизим субъектнинг тизимда ишлашини бошланишига зарур ҳаракатларни бажаради.Субъектни авторизациялаш муолажаси операцион тизимни ҳимоялаш қисмтизимига тўғридан тўғри тааллуқли эмас. Авторизация жараёнида идентификацияланган ва аутентификацияланган фойдаланувчи субъектнинг тизимда ишлашини ташкил этиш билан боғлиқ техник масалалар ечилади.

Фойдаланишни чеклаш. Ҳар бир фойдаланувчи хавфсизликнинг жорий сиёсатига биноан рухсат этилган операцион тизим объектларидан фойдаланиши мумкин. Операцион тизим объектларидан фойдаланишни чеклаш жараёнининг асосий тушунчалари – фойдаланиш объекти, объектдан фойдаланиш усули ва фойдаланувчи субъект. Фойдаланиш объекти деганда, ускуна ресурслари (процессор, хотира сегментлари, принтер, дисклар ва ҳ.) ҳамда дастурий ресурслар (файллар, дастурлар ва ҳ.) тушунилади.Объектдан фойдаланиш усули деганда, объект учун белгиланган амал тушунилади. Масалан, процессор фақат командаларни бажаради, хотира сегментлари ёзилиши ва ўқилиши мумкин, магнит карталаридан ахборот фақат ўқилиши мумкин, файллар учун эса “ўқиш”, “ёзиш” ва “қўшиб қўйиш” (файл охирига ахборотни қўшиб қўйиш) каби амаллар белгиланиши мумкин.Фойдаланиш субъекти деганда объект устида амаллар бажарилишини (қандайдир фойдаланиш усули бўйича мурожаатни) бошлаб берувчи тушунилади.

Баъзида фойдаланиш субъектига тизимда бажарилувчи жараёнларни киритишади. Аммо мантиқан, номидан жараён бажарилувчи фойдаланувчини фойдаланиш субъекти деб ҳисоблаш керак.Операцион тизимда ҳаракатдаги фойдаланишни чеклаш қоидалари хавфсизликнинг жорий сиёсати аниқланганида тизим маъмури томонидан ўрнатилади.

Аудит. Операцион тизимга нисбатан аудитни қўллашда *хавфсизлик журнали* ёки *аудит журнали* деб юритилувчи махсус журналда ОТга хавф туғдирувчи ходисалар қайд этилади. Аудит журналини ўқиш хуқуқига эга фойдаланувчилар *аудиторлар* деб аталади. Операцион тизимга хавф туғдирувчи ходисаларга одатда қуйидагилар киритилади:

- тизимга кириш ёки ундан чиқиш;
- файллар устида амаллар бажариш (очиш, бекитиш, номини ўзгартириш, йўқ қилиш);
- масофадаги тизимга мурожаат;
- имтиёзларни ёки хавфсизликнинг бошқа атрибутларини алмаштириш (фойдаланиш режимини, фойдаланувчининг ишончлилик даражасини ва ҳ.).

Агар аудит журналида барча ходисалар қайд этилса, ахборот ҳажми тезда ўсиб боради. Бу эса қайд этилган ходисаларни самарали таҳлиллашга имкон бермайди. Шу сабабли фойдаланувчилар ва ходисаларга нисбатан танлов асосидаги қайдлашни кўзда тутиш лозим. Қандай ходисаларни қайдлаш, қандай ходисаларни қайдламаслик масаласини ечиш аудиторларга юкланади.Баъзи операцион тизимларда аудит қисмтизими қайдланган ходисалар хусусидаги ахборотни ёзиш билан бир қаторда ушбу ходисалар хусусида аудиторларга интерактив хабар бериш имконияти кўзда тутилган.

Хавфсизлик сиёсатини бошқариш. Ахборот хавфсизлиги сиёсати доимо адекват ҳолатда ушлаб турилиши шарт, яъни у ОТ ишлаши шароитининг ўзгаришига тезда реакция кўрсатиши лозим. Ахборот сиёсатини бошқариш маъмур томонидан, ОТга ўрнатилган тегишли воситалардан фойдаланилган ҳолда амалга оширилади.

Криптографик функциялар. Ахборотни ҳимоялашда криптографик воситалардан фойдаланмасдан амалга оширишни тасаввур қилиб бўлмайди. Операцион тизимда шифрлаш фойдаланувчилар паролини ҳамда тизим хавфсизлиги учун жиддий бўлган бошқа маълумотларни сақлаш ва алоқа канали орқали узатишда ишлатилади.

Тармоқ функциялар. Замонавий операцион тизимлар, одатда, алоҳида эмас, балки локал ва/ёки глобал компьютер тармоқлари таркибида ишлайди. Битта тармоқ таркибидаги компьютерларнинг операцион тизимлари турли масалаларни , хусусан, ахборотни ҳимоялашга бевосита дахлдор масалаларни ечишда ўзаро алоқада бўлади.

Ҳимояланиш стандартини қаноатлантирувчи ҳар қандай операцион тизим юқорида келтирилган барча функцияларни бажарувчи ҳимоя қисмтизимига эга бўлиши шарт.

Назорат саволлари:

1. Операцион тизимни ҳимоялаш қисмтизимининг асосий функцияларини аҳамияти нимада?
2. Операцион тизимда идентификация, аутентификация, авторизация ва фойдаланишларни чеклаш функцияларини тушунтириб беринг.
3. Операцион тизимда аудит ва хавфсизлик сиёсатини бошқариш функцияларини ёритиб беринг.
4. Операцион тизимда криптографик функциялар ва тармоқ функцияларининг аҳамиятини тавсифлаб беринг.

9.3. Ахборотни ҳимоялашда дастурий иловаларнинг қўлланилиши

Нияти бузуқнинг компьютердан рухсатсиз фойдаланиши нафақат ишланадиган электрон хужжатларнинг ўқилиши ва/ёки модификацияланиши, балки нияти бузуқ томонидан бошқарилувчи дастурий закладкани киритилиши имконияти билан хавфли. Ушбу дастурий закладка қуйидаги

ҳаракатларни амалга оширишга имкон беради:

- кейинчалик компьютерда сақланадиган ёки таҳрирланадиган электрон хужжатларни ўқиш ва/ёки модификациялаш;
- электрон хужжатларни ҳимоялашда ишлатилувчи турли муҳим ахборотни тутиб олиш;
- истило қилинган компьютердан локал тармоқнинг бошқа компьютерларини истило қилишда асос (плацдарм) сифатида фойдаланиш;
- компьютерда сақланадиган ахборотни йўқ қилиш ёки зарар келтирувчи дастурий таъминотни ишга тушириш йўли билан компьютерни ишдан чиқариш.

Компьютерни рухсатсиз фойдаланишдан ҳимоялаш ахборотни ҳимоялашнинг асосий муаммоларидан бири ҳисобланади. Шу сабабли, аксарият операцион тизимларга ва оммабоп дастурий пакетларга рухсатсиз фойдаланишдан ҳимоялашнинг турли қисмтизимлари ўрнатилган. Масалан, Windows оиласидаги операцион тизимга киришда фойдаланувчиларни аутентификациялашни бажариш. Аммо, рухсатсиз фойдаланишдан жиддий ҳимояланиш учун ўрнатиладиган воситаларнинг етишмаслиги шубҳа туғдирмайди. Шу сабабли, ҳимоялашнинг стандарт воситаларига қўшимча тарзда фойдаланишни чеклашнинг махсус воситаларидан фойдаланиш зарур. Бундай махсус воситаларни шартли равишда қуйидаги гуруҳларга ажратиш мумкин:

- ахборотни криптографик ҳимоялашнинг дастурий воситалари;
- тармоқни ҳимоялашнинг дастурий воситалари;
- VPNтармоқни қуришнинг дастурий воситалари;
- ҳимояланганликни тахлилловчи дастурий воситалар;
- антивируслар.

Ахборотни криптографик ҳимоялашнинг дастурий воситалари – мустақил ёки бошқа тизимлар таркибида ишловчи ва ахборот хавфсизлигини таъминлаш учун уни криптографик ўзгартирилишини таъминловчи маълумотларни ишлаш тизимининг дастурий ва техник элементлари мажмуи.

Қуйида ушбу дастурий воситаларга тааллуқли хорижий ва мамлакатимиз компанияларининг махсулотлари келтирилган.

M-506A-XP – MS Windows 2000/XP/2003/7 операцион тизим бошқарувида ишловчи локал ҳисоблаш тармоқларида ахборотни ҳимоялашга мўлжалланган дастурий-аппарат комплекс. M-506A-XP иккита асосий масалани ҳал этади: ахборотни рухсатсиз фойдаланишдан ҳимоялайди ва Россия стандарти ГОСТ28147-89га мувофиқ амалга оширилган маълумотларни криптографик ҳимоялашни бажаради.

Криптопровайдер КриптоПро CSP 3.6 – ахборотни криптографик ҳимоялашнинг сертификацияланган воситаси бўлиб, иккита асосий масалани хал этади: стандарт ва ҳамма жойда ишлатилувчи Microsoft фирмасининг ишончли Россия криптографиясили иловалардан фойдаланиш имконияти (корпоратив фойдаланувчилар учун) ва Microsoft фирмаси махсулотларидан фойдаланган ҳолда янги, ишончли ҳимояланган иловаларни яратиш имконияти (тизимли интеграторлар учун).

Ахборотни ҳимоялаш тизимининг Secret Disk оиласи шахсий компьютердан муайян фойдаланувчилар учун ҳимояланган ахборот элтувчиларини виртуал мантиқий дискларини ташкил этиш йўли билан ахборотни ҳимоялашга имкон беради. Фойдаланувчилар учун маълумотларни шифрлаш “шаффоф” режимида амалга оширилади, яъни ахборот ёзилишида автоматик тарзда шифрланади, ўқишда дешифровка қилинади.

Блок хост – ЭРИ – сертификацияланган криптоПроCSPдан фойдаланган ҳолда MS Windows платформасидаги шифрлаш ва электрон рақамли имзони яратиш тизими. MS Windows операцион тизимига ўрнатилган бошқа криптопровайдерлар билан ҳам ишлаш мададланади.

КриптоАРМ – криптографик воситалар билан ишлашнинг қулайлигини таъминловчи универсал дастурий таъминот. КриптоАРМ ахборотни ишончли ҳимоялашга ва Интернет тармоғи бўйича узатиладиган ва турли хил элтувчилардаги (дискетлардаги, флеш карталардаги, токенлардаги) электрон

маълумотларнинг муаллифлигини кафолатлашга мўлжалланган.

HIMFAYL – файлларни ҳимояланган сақлаш тизими шахсий компьютерда ёки ахборотни ташқи диск элтувчиларида сақланувчи папкалар ва файлларнинг махфийлигини (конфиденциаллигини), яхлитлигини таъминлаш ва уларни рухсатсиз фойдаланишдан ҳимоялаш учун мўлжалланган.

E-XAT – ҳимояланган электрон почта тизими фойдаланувчилар орасида электрон хабарларни ҳимояланган алмашишни ташкил этишга мўлжалланган. Ушбу тизим ахборотни криптографик ҳимоялаш воситаларидан ва ахборотни криптографик ҳимоялаш соҳасидаги давлат стандарти асосидаги электрон рақамли имзо (миллий криптопровайдер) воситаларидан фойдаланади. E-XAT тизими уйда ишлаш учун учта тилни мададлайди: ўзбек (лотин ва кириллица), рус (кириллица) ва инглиз (лотин).

Тармоқни ҳимоялашнинг дастурий воситалари. Аксарият хужумга уринишлар ташқаридан бўлиши сабабли тармоқ хавфсизлигига алоҳида эътибор бериш зарур. Тармоқлараро экран – маълум протоколларга мувофиқ кирувчи ва чиқувчи маълумотлар пакетини фильтрлаш вазифасини бажарувчи аппарат ёки дастурий воситалар комплекси. Қуйида муайян ташкилотлар учун тармоқлараро экран ишлашини созлаш ва тайёр вариантларини танлаш имконини берувчи дастурий маҳсулотлар келтирилган.

Trust Access – тақсимланган тармоқлараро экран Россиянинг “Ҳисоблаш техникаси воситалари. Тармоқлараро экранлар. Рухсатсиз фойдаланишдан ҳимоялаш. Ахборотни рухсатсиз фойдаланишдан ҳимоялаш кўрсаткичи” талабларига мувофиқ сертификатланган.

Security Studio Endpoint Protection – ўзида тармоқлараро экранни, хужумларни аниқлаш ва вирусга қарши воситаларни бирлаштиради. Тармоқ ресурсларидан хавфсиз фойдаланишни таъминлайди, спам ва турли хил ташқи таҳдидлардан ҳимоялайди.

UserGateProxy&Firewall – фойдаланувчиларнинг Интернетдан

фойдаланишларини, трафикни қайд этишни ва фильтрлашни, ресурсларни ташқи хужумлардан ҳимоялашни ташкил этишга мўлжалланган.

CISCO IDS/IPS – хужумларни қайтариш бўйича ечим. Унда анъанавий механизмлар билан бир қаторда тармоқ трафигидаги нонормалликларни ва тармоқ иловаларининг нормал ҳаракатидан четланишларини кузатувчи ноёб алгоритмлар ишлатилади.

DallasLock 8.0 – К – ахборотни ҳимоялаш маркази "Конфидент" томонидан ишлаб чиқилган автоматлаштирилган ишчи станцияларни ва серверларни рухсатсиз фойдаланишдан ҳимоялаш тизими.

Secret Net 6.5 (К - варианти) – ахборотни рухсатсиз фойдаданишдан ҳимоялаш тизими.

ПАК "Соболь" – рухсатсиз фойдаланишдан ҳимоялашни таъминловчи ишончли юклашнинг дастурий-аппарат модули. Локал тармоқ таркибидаги алоҳида компьютерни ҳамда ишчи станция/серверларни ҳимоялашни таъминлаши мумкин.

СЗИ "Блокхост-сеть" – ахборот ресурсларини рухсатсиз фойдаланишдан кўп функцияли ҳимоялашга мўлжалланган. Windows оиласидаги операцион тизим бошқарувидаги тизимларда ишлайди.

ПАК "Блокхост-МДЗ" – компьютерни юклаш босқичида ахборот ресурсларини рухсатсиз фойдаланишдан ҳимоялайди. Қаттиқ дискдаги ахборотнинг сақланишини таъминлайди.

VPN тармоқни қуришнинг дастурий воситалари. Ушбу дастурий комплекслар виртуал хусусий тармоқларни қуришга, уларни кузатишга, шифрланган канал бўйича маълумотларни хавфсиз узатиш учун туннелларни яратишга ҳамда талаблар ва шартларга мувофиқ виртуал тармоқни ўзгартириш имкониятига хизмат қилади. Қуйида виртуал хусусий тармоқни қуриш учун дастурий маҳсулотлар келтирилган.

Шифрлашнинг аппарат-дастурий комплекси "Континент"-3.5 – TCP/IP протоколларини ишлатувчи умумфойдаланувчи глобал тармоқлар асосида виртуал хусусий тармоқларни қуриш воситаси ҳисобланади.

Комплекс VPNнинг таркибий қисмлари орасида очиқ алоқа канали бўйича узатилувчи ахборотни криптографик ҳимоялашни таъминлайди. Комплекс узатиладиган ва қабул қилинадиган пакетларни турли мезонлар (адреслаш, ўлчаш, кенгайтириш ва ҳ.) бўйича фильтрлашни амалга оширади. Бу эса тармоқни ишончли ҳимоялашни таъминлайди.

VipNeTCustom – дастурий ва дастурий - аппарат маҳсулотлар қатори ҳисобланиб, йирик тармоқларда ахборотни ҳимоялашни ташкил этиш имкониятига эга ва ахборотни ҳимоялашнинг қуйидаги иккита масаласига мўлжалланган:

- бошқариш марказларига эга виртуал хусусий тармоқни ташкил этиш йўли билан алоқанинг умумфойдаланувчи ва ажратилган каналлари бўйича фойдаланиш чекланган ахборотни узатувчи ҳимояланган муҳитни яратиш;
- электрон рақамли имзо механизмларидан фойдаланиш мақсадида очиқ калитлар инфраструктурасини ташкил этиш.

Ҳимояланганликни тахлилловчи дастурлар. Ҳимоя самарадорлигини назоратлаш ахборотдан рухсатсиз фойдаланиш ҳамда ахборотни ёки ахборотни ишлаш ва узатиш воситаларининг нормал ишлашининг бузилиши эвазига ахборотнинг техник каналлар бўйича сирқиб чиқишини ўз вақтида аниқлаш ва бартараф этиш мақсадида амалга оширилади. Ушбу вазифани “хавфсизлик сканерлари” деб аталувчи “ҳимояланганликни тахлиллаш воситалари” бажаради. Қуйида ҳимояланганликни тахлиллаш воситаларининг дастурий махсулотлари келтирилган.

XSpider 7.8 – заифликларни татбиқий ҳамда тизимли сатҳларда тездан самарали қидиришни амалга оширувчи тармоқ хавфсизлиги сканери. Ушбу сканер ҳар қандай кўламли тармоқларда хавфсизлик мақомини назоратлашнинг самарали тизимини барпо этади.

Тармоқ ревизори – рухсатсиз фойдаланишга уринишларни бартараф этишга мўлжалланган тармоқ сканери. Тармоқ ревизори TCP/IP стеки протоколларидан фойдаланувчи ўрнатилган тармоқ дастурий ва аппарат

таъминоти заифликларини аниқлаш учун ишлатилади.

Сканер ВС - ҳимояланганликни комплекс тахлиллаш тизими. Ушбу сканер операцион тизимли ва олдиндан ўрнатилган дастурий таъминотли юкловчи DVD ёки USB –тўплагич. Ўрнатилган дастурий таъминот ахборот тизими ҳимояланганлигини комплекс тахлиллашни ва тестлашни амалга оширади.

Антивируслар. Ҳозирда кичик компаниялар ҳамда корпорациялар томонидан ишлаб чиқиладиган ва мададланадиган вирусга қарши дастурий маҳсулотларнинг етарлича катта сони мавжуд. Уларнинг орасида вирусга қарши комплекс дастурларни алоҳида ажратиш мумкинки, бу дастурлар компьютерда ўрнатилган дастурий таъминотни тўлиқ назоратлайди. Қуйида бундай дастурий маҳсулотларнинг баъзилари келтирилган.

Dr.Web – Россиянинг вирусга қарши оммавий дастури. Дастур таркибида резидент қуриқчи SpIDerGuard, Internet орқали вирус базаларини янгилашнинг автоматик тизими ва автоматик текшириш жадвалини режалаштирувчи мавжуд. Почта файлларини текшириш амалга оширилган. Dr. Web дастурининг муҳим хусусияти – оддий сигнатурали қидириш натижа бермайдиган мураккаб шифрланган ва полиморф вирусларни аниқлаш имкониятидир.

Касперский лабораторияси – ахборот хавфсизлиги соҳасидаги илдам қадамлар билан ривожланаётган компаниялардан бири. Компания вирусга қарши тадқиқотлар, хавфли иловаларга қарши таъсирлар, трафикни фильтрлаш ва ҳакозоларни ўз ичига олувчи жуда жиддий IT-тахдидлар билан узлуксиз курашиш йилларида тўпланган бой тажрибага эга. Касперский лабораторияси барча категорияли клиентларнинг эҳтиёжларини ҳисобга олувчи вирусдан, спамдан, хакер хужумидан ишончли ҳимоялашни таъминловчи кенг кўламли ечимларни тақдим этади.

“Eset” компанияси – вирусга қарши дастур таъминотини ҳалқаро ишлаб чиқарувчиси, кибержиноятчиликдан ва компьютер тахдидларидан ҳимоялаш соҳасидаги эксперт. Компания дунёнинг 180 мамлакатида

вакилларига эга. Ушбу компания маълум ва номаълум зарар келтирувчи дастурларни детектирлаш ва хавфсизлантиришга имкон берувчи тахдидларни аниқлашнинг эвристик усулларини яратиш соҳасининг ташаббускори ҳисобланади. Eset Nod 32 – Россияда вирусга қарши ечимлар оммабоплиги бўйича иккинчи ўринда туради, ҳар бир учинчи компьютер унинг ҳимоясида.

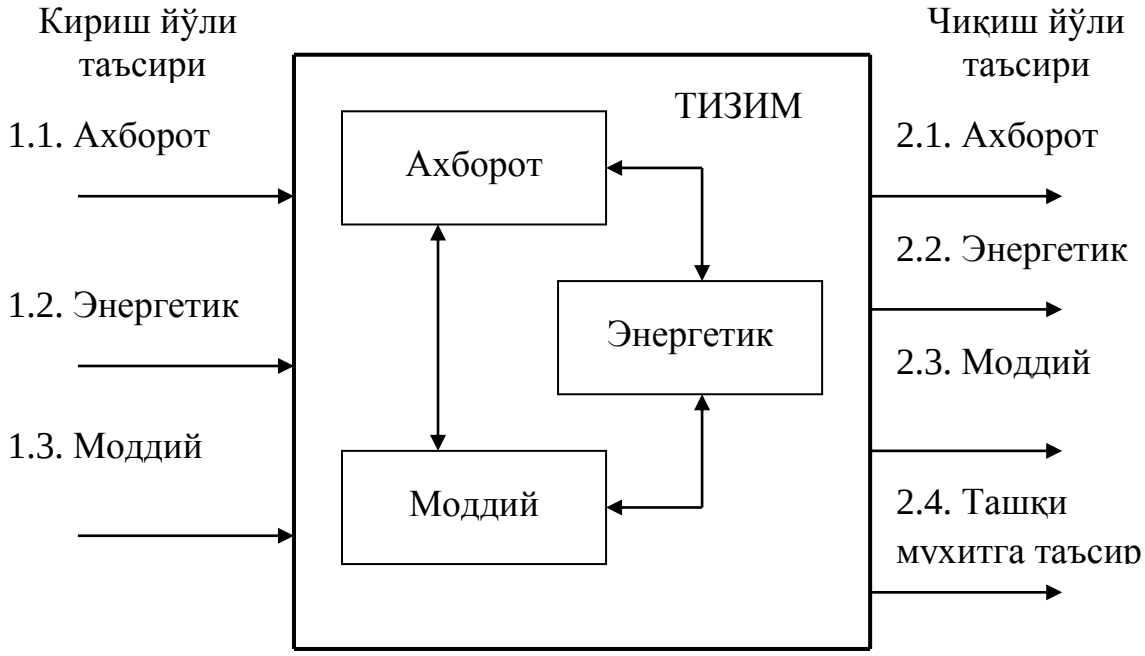
Назорат саволлари:

1. Ахборотни ҳимоялашда қўлланиладиган дастурий воситаларнинг шартли равишда қандай гуруҳларга ажратиш мумкин?
2. Ахборотни криптографик ҳимоялашнинг дастурий воситаларини ишлаш принципини тушунтиринг.
3. Тармоқни ҳимоялашнинг дастурий воситаларини тавсифлаб беринг.
4. VPN тармоқларни қуриш дастурий воситаларини ишлаш принципини тушунтириб беринг.
5. Ҳимояланганликни таҳлилловчи дастурий иловаларнинг аҳамияти.
6. Антивирус воситаларининг операцион тизимларни ҳимоялашда тутган ўрни.

X боб. АХБОРОТНИ СИРҚИБ ЧИҚИШ КАНАЛЛАРИ

10.1. Ахборот сирқиб чиқадиган техник каналлар ва уларнинг туркумланиши

Ахборотнинг техник канал бўйича сирқиб чиқиши нуқтаи назаридан объект модели ўзаро ва ташқи мухит билан боғланган ахборот, энергетик, моддий тизимларни ўз ичига олади (10.1-расм).



10.1-расм. Объект модели

Ахборот тизими энергетик тизим билан ва у орқали ташқи мухит билан ўзаро таъсирда бўлади. Энергетик тизим орқали ахборот сирқиб чиқадиган канал шаклланиши мумкин. Объектнинг энергетик тизимининг ташқи мухитга таъсири натижасида ниқобни очувчи акустик майдон яратилади. Энергетик тизим моддий тизим билан хам ўзаро таъсирда бўлади ва натижада, тебранма (механик) майдон шаклланади. Тебранма майдон ахборот тизими сигналини модуляция қилиши мумкин. Ҳар бир тизим ўзининг элементларига, боғланишларининг ички структурасига, ўзгарувчи параметрлари сонига хамда ташқи мухит орқали ўзаро таъсирига боғлиқ чеклашларга эга. Объектларнинг ишлаши уларнинг хақиқий мақсад ва вазифаларини кузатишдан

бекитади. Хар бир тизимда ахборот сирқиб чиқадиган техник каналлар мавжуд.

Ахборот сирқиб чиқадиган техник каналлар деганда техник воситаларнинг ишлаш жараёнида пайдо бўлувчи турли табиатли қўшимча нурланиш хисобига ахборотнинг бехосдан узатилиши тушунилади. Ахборот сирқиб чиқадиган техник каналнинг структураси 10.2 – расмда келтирилган.

10.2-расм. Ахборот сирқиб чиқадиган техник канал структураси

Канал кириш йўлига дастлабки сигнал кўринишидаги ахборот қабул қилинади.

Дастлабки сигнал – ахборот манбаидан олинадиган ахборот элтувчисидир. Қуйидаги *сигнал манбаларини* кўрсатиш мумкин:

- электромагнит ва акустик тўлқинларини қайтарувчи кузатув объекти;
- ўзидан оптик ва радио диапазонларидаги электромагнит тўлқинларини тарқатувчи кузатув объекти;
- функционал алоқа каналининг узатувчи қурилмаси;
- яширинча ўрнатилган қурилма;
- хавфли сигнал манбаи;
- ахборот билан модуляцияланган акустик тўлқинлар манбаи.

Канал кириш йўлига манбадан ахборот сигнали манба тилида (харф, рақам, матн, символлар, белгилар, товуш сигналлари ва ҳ. кўринишида) қабул қилинганлиги сабабли узатувчи қурилма ахборотнинг ушбу ифодаланиш шаклини тарқалиш мухитига мос ахборот элтувчисига ёзишни

таъминловчи шаклга ўзгартиради.

Узатиш муҳити - элтувчи кўчиб юрувчи фазонинг қисми. У элтувчининг кўчиб юриши шартларини белгиловчи физик параметрлар набори орқали характерланади. Тарқалиш муҳитини тавсифлашда қуйидаги асосий параметрларни ҳисобга олиш зарур:

- субъектлар ва моддий жисмлар учун физик тўсиқлар;
- масофа бирлигидаги сигналнинг сусайиш ўлчови;
- частота характеристикалари;
- сигнал учун халаллар кўриниши ва қуввати.

Қабул қилувчи қурилма қуйидаги вазифаларни бажаради:

- қабул қилувчига керакли ахборот элтувчисини танлаш;
- қабул қилинган сигналнни ахборотни олишни таъминловчи қийматигача кучайтириш;
- элтувчидан ахборотни олиш;
- ахборотни қабул қилувчига (инсонга, техник қурилмага) тушунарли сигнал шаклига ўзгартириш ва сигналнни хатосиз ўзлаштирилишига етарли қийматгача кучайтириш.

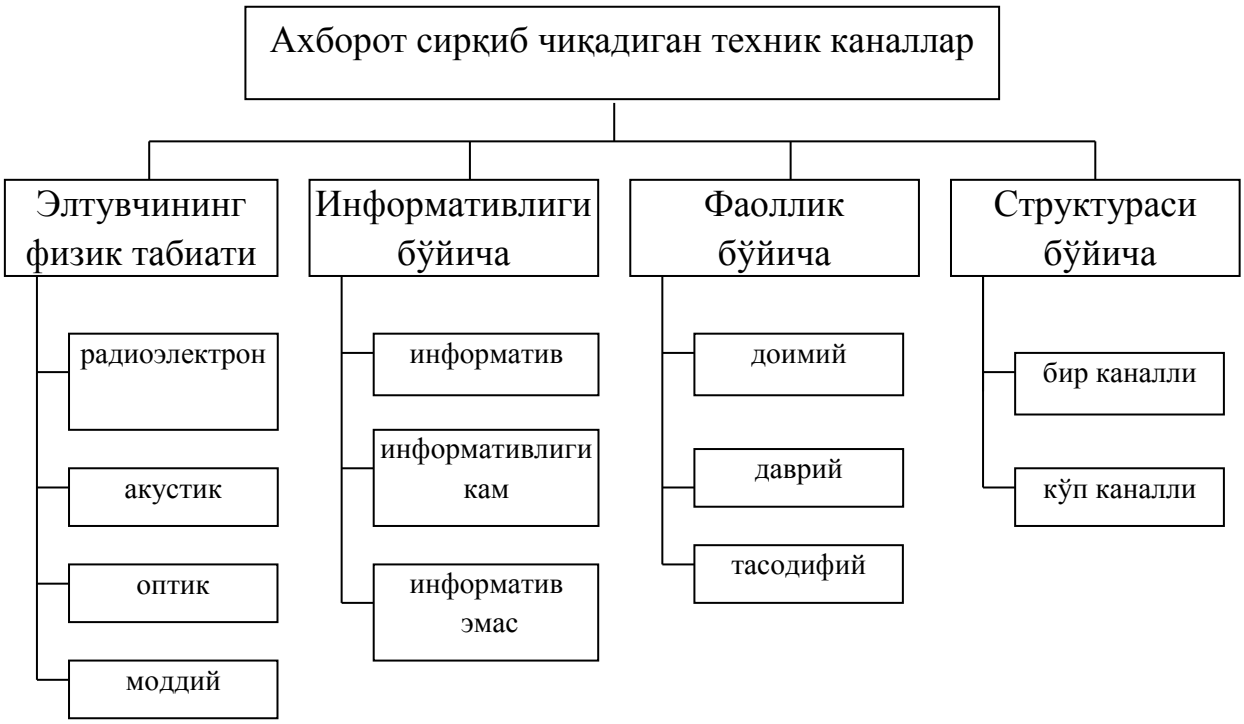
Ахборот сирқиб чиқадиган техник каналларнинг туркумланиши 10.3-расмда келтирилган.

Ахборот элтувчининг физик табиати бўйича қуйидаги ахборот сирқиб чиқадиган техник каналлар фарқланади:

- радиоэлектрон;
- акустик;
- оптик;
- моддий.

Ахборот сирқиб чиқадиган радиоэлектрон каналда элтувчи сифатида радиодиапазондаги электрик, магнит ва электромагнит майдонлар, хамда металл ўтказувчилар бўйича тарқалувчи электр токи (электронлар оқими) ишлатилади. Радиоэлектрон каналнинг частоталар диапазони қуйидагича:

- паст частотали 10-1 км (30-300 КГц);
- ўрта частотали 1 км-100 м (300 КГц-3МГц);
- юқори частотали 100-10 м (3-30 МГц);
- ультра юқори частотали 10-1м (30-300 МГц);
- ўта юқори частотали 10-1см (3-30 ГГц).



10.3-расм. Ахборот сирқиб чиқадиган техник каналларнинг туркумланиши

Акустик каналда ахборот элтувчиси сифатида мухитда тарқалувчи акустик тўлқинлар ишлатилади. Акустик каналнинг частоталар диапазони қуйидагича:

- инфратовуш 1500-75 м (1-20Гц);
- пастки товуш 150-5м(1-300Гц);
- товуш 5-0,2м (300-16000Гц);
- ультратовуш -16000 Гцдан 4 МГц гача.

Оптик каналдаги ахборот элтувчиси – электромагнит майдон (фотонлар). Оптик диапазон қуйидагиларга бўлинади:

- узоқ инфрақизил қисм. Диапазон 100-10мкм (3-300ТГц);
- ўрта ва яқин инфрақизил қисм. Диапазон 10-0,76 мкм (30-400 ТГц);

- кўринадиган диапазон (кўк-яшил-қизил). Диапазон 0,76-0,4 мкм (400-750 ТГц).

Моддий каналда ахборотнинг сирқиб чиқиши химояланувчи ахборотли элтувчиларнинг назоратланувчи зона ташқарисига рухсатсиз тарқалиши хисобига рўй беради. Элтувчи сифатида кўпинча хужжатлар қўл ёзмаси ва ишлатилган нусхалаш қоғозлари ишлатилади.

Информативлиги бўйича ахборот сирқиб чиқадиган каналлар информатив, информативлиги кам ва информатив эмасларга бўлинади. Канал информативлиги канал бўйича узатилувчи ахборот қиймати орқали бахоланади.

Фаоллик вақти бўйича каналлар доимий, даврий ва тасодифийларга бўлинади. Доимий каналда ахборот сирқиб чиқиши етарлича мунтазам характерга эга. Тасодифий каналларга ахборот сирқиб чиқиши тасодифий, бир марталик характерга эга бўлган каналлар тегишли.

Ахборот сирқиб чиқадиган каналларнинг амалга оширилиши натижасида қуйидаги хавфлар пайдо бўлиши мумкин:

- акустик ахборотнинг сирқиб чиқиши хавфи;
- тасвирий ахборотнинг сирқиб чиқиши хавфи;
- ахборотнинг қўшимча электроманит нурланишлар ва наводкалар бўйича сирқиб чиқиши хавфи.

Структуралари бўйича ахборот сирқиб чиқадиган каналлар бир канали ва кўп каналли бўлиши мумкин. Кўп каналлиларда ахборот сирқиб чиқиши бир қанча кетма-кет ёки параллел каналлар бўйича бўлади.

Назорат саволлари:

1. Ахборот сирқиб чиқадиган техник каналлар тушунчаси.
2. Ахборот сирқиб чиқадиган техник канал структурасини тушунтириб беринг.
3. Ахборот сирқиб чиқадиган техник каналларнинг туркумланиши.

10.2. Ахборот сирқиб чиқадиган техник каналларни аниқлаш

усуллари ва воситалари

Электромагнит нурланиш индикаторлари қўшимча электромагнит нурланишларни аниқлаш ва назоратлаш учун ишлатилади. Индикаторнинг соддалаштирилган схемаси 10.4-расмда келтирилган.

10.4-расм. Электромагнит нурланиш индикаторининг схемаси

Асбоб фазонинг маълум нуқтасидаги электромагнит нурланишларни қайдлайди. Агар ушбу нурланишларнинг сатҳи бўсағa нурланишдан ошиб кетса товуш ёки нур ёрдамида ишловчи огоҳлантирувчи қурилма ишга тушади. Демак, ушбу жойда яширинча ўрнатилган радио қурилмаси (радиозакладка) мавжуд.

Индикаторнинг ишлаш принципи қуйидагича. Индикатор схемасида ташқи сигналлар фонида тест акустик сигналини ажратишга имкон берувчи паст частота кучайтиргичи ва радиокарнай мавжуд. Тест акустик сигнал билан модуляцияланган нурланишни индикатор антеннаси қабул қилади ва кучайтирилгандан сўнг радиокарнайга узатилади. Радиозакладка микрофони билан индикатор радиокарнайи орасида хуштакни эслатувчи товуш сигнали кўринишида намоён бўлувчи мусбат тескари боғланиш ўрнатилади. Бу акустик тескари боғланиш ёки "акустик боғланиш" режими деб аталади.

Электромагнит майдон индикаторлари қуйидаги кўрсаткичлари билан характерланади:

- частотанинг ишчи диапазони;

- сезувчанлик;
- закладкани топиш радиуси;
- таъминот манбаи хили;
- закладкани қидириш режимида автоном ишлаш вақти;
- индикация хили.

Замонавий индикатор D-008 нинг кўриниши 10.5 - расмда келтирилган. Асбоб ишлашининг иккита режими мавжуд:

- радионурлантирувчи закладкани қидиришга мўлжалланган майдонни аниқлаш;
- яширинча тингловчи қурилмаларни қидиришга мўлжалланган симли линияларни тахлиллаш.

Ушбу асбоб модуляция хилига боғлиқ бўлмаган ҳолда закладкаларни аниқлайди. Аниқлаш радиуси нурланиш қувватига, закладка ишлаши частотасига, текширилувчи хонадаги электромагнит аҳволга боғлиқ. Закладка қуввати 5 мВт бўлганида аниқлаш радиуси тахминан 1м га тенг бўлади.

10.5-расм. D-008 индикатори

Акустик тескари боғланиш режими қурилманинг локал электромагнит майдон таъсирида янглиш ишлашини бартараф этиш ва ўзига хос товуш сигнали бўйича закладкани аниқлаш имкониятини беради. Қурилма 50-1500 мГц частота диапазонида ишлайди.

Радиочастотомерлар электромагнит нурланишнинг частота бўйича бўсағанинг ошиб кетишини қайдлайди. Закладкани қидириш хонани режа асосида радиочастотомер билан айланиш йўли орқали амалга оширилади ва закладка бўлиши мумкин бўлган жой текширилаётган хонанинг маълум

нуқтасидаги сигналнинг максимал сатҳи бўйича аниқланади. Нурланиш аниқланганда дисплейда олинган сигнал частотаси кўрсатилади, товуш ёки ёруғлик орқали хабар берилади.

Радиочастотомерларнинг баъзи хиллари ахборотни юқори частотада линия орқали узатувчи закладкаларни аниқлашда қўлланилади. Нияти бузуқнинг техник воситасининг узатиш частотаси 40-600 КГц (баъзида 7 МГц гача) диапазонда бўлади.

РИЧ-3 частотомернинг (10.6-расм) ишлаш принципи радиосигналларни кенг полосали детектирлашга асосланган. Бу эса ихтиёрий модуляцияли радиоузатувчи қурилмаларни аниқлаш имкониятини беради.

Асбоб иккита режимда ишлайди:қидириш ва қўриқлаш.

Қидириш режими радиомикрофонлар, телефон радиотрансляторлар, радиостетоскоплар, яширин видеокамералар ўрнатилган жойларни аниқлашда ишлатилади. Ундан ташқари радиостанциялар ва радиотелефонларни рухсатсиз ишга туширилганлигини аниқлайди.

10.6-расм. РИЧ-3 частотомери

Қўриқлаш режими бегона радионурланиш манбасини пайдо бўлиш онини қайдлашга ва тревога сигналини узатишга имкон беради.

РИЧ-3 асбоби частота ўлчанишининг юқори аниқлигида (0,002%), частотанинг 100-3000 МГц диапазонида ишлайди.

Сканерловчи приемниклар транспортда ташиладиган ва қўлда олиб юриладиганларга бўлинади. Майдон индикатори ва радиочастотомерларга

ўхшаб, сканерловчи приемниклар ахборот сирқиб чиқувчи каналларни аниқлашда қўлланилиши мумкин.

10.7-расмда Winradio сканерловчи приемникнинг ташқи кўриниши келтирилган. Ушбу приемник компьютернинг 16-битли слотига ўрнатиладиган карта кўринишида ясалган (10.8-расм), бу эса унинг кетма - кет портлар орқали уланадиганларига нисбатан имкониятларини орттиради.

Winradio 1000 модели 500 кГц дан 1300 мГц гача частоталарда ишлайди ва турли модуляцияли сигнални қабул қилиши мумкин. Дастурий бошқариш сичқонча ва клавиатура ёрдамида қурилма ресурсларини оператив бошқаришга имкон беради. Бошқариш панели монитор экранида акслантирилади. Тезлиги – 50 канал/с, частота бўйича ўзгартириш қадами 1 кГц дан то 1 мГц гача.

10.7-расм. Winradio сканерлайдиганқабул қилувчи қурилма

10.8-расм. Winradio сканерловчи приемникнинг компьютерга ўрнатиш

Winradio Communication фирмаси радиоприемниклари комплекти таркибига бошқаришнинг қуйидаги дастурий воситалари киради:

- базавий дастурий таъминот;
- қўшимча дастурий таъминот;
- сканерлаш режимини амалга оширишига имкон берувчи дастурий таъминот.

Базавий дастурий таъминот приемник ишлашини бошқарувчи асосий бошқариш дастури бўлиб, қуйидаги масалаларни ҳал этади: приемникни иш частотасига ва ишлаш режимига ўрнатиш, сканерлаш параметрларини белгилаш ва натижаларини акслантириш, иш натижалари бўйича маълумотлар базасини шакллантириш.

Қўшимча дастурий таъминот приемникнинг функционал имкониятларини кенгайтиришга имкон беради:

- Digital Suite дастури сигналнинг вақт ва частота характеристикаларини тахлиллашга, турли стандартлардаги сигналларини ишлашга, ҳамда аудио - сигналларини WAV – форматда қаттиқ дискга ёзишга имкон беради. Сигналларни тахлиллаш ва ишлаш муолажаларини амалга оширишда компьютернинг стандарт товуш картасидан фойдаланилади.
- Datebase дастури ихтисослаштирилган маълумотлар базасининг шаклланишини таъминлайди. Дастур таркибига бутун дунё бўйича уч юз мингдан ортиқ қайдланган частоталарини, манзил мамлакати, географик координатлари кўрсатилган радиостанциялар хусусидаги ахборотли маълумотлар базаси киради.

Сканерлашнинг кўпгина алгоритмлари мавжудки, уларнинг асосий вазифалари қуйидагилар:

- агар қабул қилинадиган сигнал сатҳи берилган бўсағадан ошса сканерлаш тўхтатилади. Оператор товуш ёки нур орқали огоҳлантирилади.
- сигнал аниқланганда сканерлаш тўхтатилади ва сигнал йўқолганида сканерлаш қайтадан бошланади;
- сигнални тахлиллаш вақтида сканерлаш тўхтатиб турилади ва сканерлаш режими ишга туширилганда давом эттирилади;
- қўл ёрдамида сканерлаш – приёмникни созлаш оператор ёрдамида

амалга оширилади.

Қўшимча дастурий таъминот частоталари маълум радиозакладкаларни қидиришда ишлатилади. Бунда баъзи сканерловчи приемникларда модуляциянинг берилган хили ва устивор каналлар бўйича сканерлаш кўзда тутилган.

Юқорида айтиб ўтилганидек, шахсий компьютерларнинг аниқлаш қурилмалари билан комплексда ишлатилиши сигналларни аниқлаш ва тахлиллаш бўйича имкониятларни жиддий кенгайтиради. "Сканерловчи приемник + шахсий компьютер" комплекти автоматлаштирилган қидирув комплексининг оддий мисоли ҳисобланади. Янада мураккаб тизимлар ҳам шахсий компьютер ва сканерловчи приемник асосида қурилади, аммо улар комплекснинг тезкорлигини ҳамда функционал имкониятларини кенгайтирувчи қўшимча блокларга эга.

Шахсий компьютерлар асосида қурилган автоматлаштирилган қидирув комплекси ишлашини "Нелк" фирмасининг "КРОНА" ва "КРОНА Про" комплекслари мисолида кўрамиз.

"КРОНА" комплекси(10.9-расм) қуйидаги муолажаларни бажаришга мўлжалланган:

- ҳозирги кунда маълум барча ниқоблаш воситаларидан фойдаланувчи радиозакладкаларни аниқлаш ва локализациялаш. 3 ГГц гача диапазонда ишлайди (қўшимча конвертор билан 18 ГГц гача). Маълумотларни узатувчи рақамли каналларни ва ахборотни радиоканал бўйича узатувчи яширин видеокамераларни автоматик тарзда аниқлаш имкониятига эга. Мавжуд дастурий таъминот радиозакладкаларни юқори даражада ишончлиликда аниқлашга имкон беради;
- ҳимояланувчи объектдаги электромагнит аҳволни муттасил мониторинглаш. Дастурий таъминот янги ёки маълум сигналлар параметрларини қидириш ва баҳолаш, частота диапазонини назоратлаш, қайд этилган частоталарни назоратлаш ва ҳ. масалаларини ечишга имкон беради.

"КРОНА Про" комплекси кўп каналли комплекс бўлиб радионурланувчи воситаларни аниқлашда ва радиомониторингни амалга

оширишда қўлланилади. Назорат диапазони 10..3000 МГц (қўшимча конвертор билан 18000 МГц гача). Ушбу комплекс яширин радиоузатувчи радиокамераларни, маълумотларни узатувчи рақамли каналларни автоматик тарзда аниқлайди. Ўрнатилган жойни топиш аниқлиги 10 см гача, автоном таъминот 2 соатгача. Комплекс ахборотни рухсатсиз олувчи воситаларни аниқлаш имкониятига эга.

10.9-расм. "КРОНА" русумли автоматлаштирилган қидирув комплекси

Юқорида кўрилган автоматлаштирилган қидирув комплекслари стандарт компьютерларда ва оддий кўчмас сканерловчи приемниклар асосида қурилган. Махсус қидирув дастурий – аппарат воситалар алоҳида гуруҳга ажратилади. Масалан, РК855-S, ScanbockSelectPlus, OSCOROSC-5000 Deluxe (10.10-расм). Улар радиозакладкаларни автоматик тарзда қидиришга мўлжалланган. Комплекслар таркибида махсус сканерловчи приемник, микропроцессор ва тест акустик сигнал генератори ёки товушсиз корелятор мавжуд. Бундай комплексларнинг асосий характеристикаси - унумдорлик, яъни аниқланган сигнални радиозакладка сигналлари синфига таалуқли эканлигига сарфланган вақтни инобатга олган ҳолда радиодиапазонни тахлиллаш тезлиги.

10.10-расм. OSCOR OSC-5000 DeLuxe русумли махсус автоматлаштирилган қидирув комплекси

Назорат саволлари:

1. Электромагнит нурланиш индикаторининг ишлаш схемасини тушунтириб беринг.
2. Радиочастотомерларнинг ишлаш режимларини тушунтириб беринг.
3. Сканерловчи қурилмаларнинг ахборот сирқиб чиқишидан ҳимоялашдаги аҳамияти.
4. Шахсий компьютерлар асосида қурилган автоматлаштирилган қидирув комплекси.

10.3. Объектларни инженер химоялаш ва техник қўриқлаш

Ахборот манбаларини физик химоялаш тизими нияти бузуқнинг химояланувчи ахборот манбаларига суқилиб киришини олдини олувчи ҳамда табиий офатдан, аввало ёнғиндан, огохлантирувчи воситаларни ўз ичига олади.

Инженер конструкциялар тахдид манбаларини ахборот манбалари томон харакати (тарқалиши) йўлида ушлаб қолувчи тўсиқларни яратади. Аммо ахборотни ҳимоялашни таъминлаш учун тахдидларни нияти бузуқнинг ва табиий офатнинг ҳимояланувчи ахборотли манбага таъсиридан олдин нейтраллаш зарур. Бунинг учун тахдид *нейтраллаш воситалари* томонидан аниқланиши ва олди олиниши зарур. Бу масалалар *ахборот манбаларини*

техник қўриқлаш воситалари томонидан ҳал этилади.

Ахборотга таҳдидларнинг турлари ва рўй бериши вақтининг ноаниқлиги, ахборотни ҳимояловчи воситаларининг кўп сонлилиги ва турли – туманлиги, фавқулот вазиятлардаги вақтнинг танқислиги *ахборотни физик ҳимоялаш воситаларини бошқаришга* юқори талаблар қўяди.

Бошқариш қўйидагиларни таъминлаши лозим:

- ахборотни ҳимоялашнинг умумий принципларини амалга ошириш;
- ахборотни физик ҳимоялаш тизимини ва уни сирқиб чиқишидан ҳимоялаш тизимини ягона доирада ишлашини мувофиқлаштириш;
- ахборотни ҳимоялаш бўйича оператив қарор қабул қилиш;
- ҳимоя чораларининг самарадорлигини назоратлаш.

Физик ҳимоялаш тизимини бошқариш бўйича меъёрий хужжатлар ахборотни ҳимоялаш бўйича йўриқномаларда ўз аксини топган. Аммо йўриқномаларда барча вазиятларни ҳисобга олиш мумкин эмас. Физик ҳимоялаш тизимининг воситалари вақт танқислиги шароитида нотипик вазиятлар содир бўлганида тўғри хулоса қабул қилинишини таъминлаши лозим.

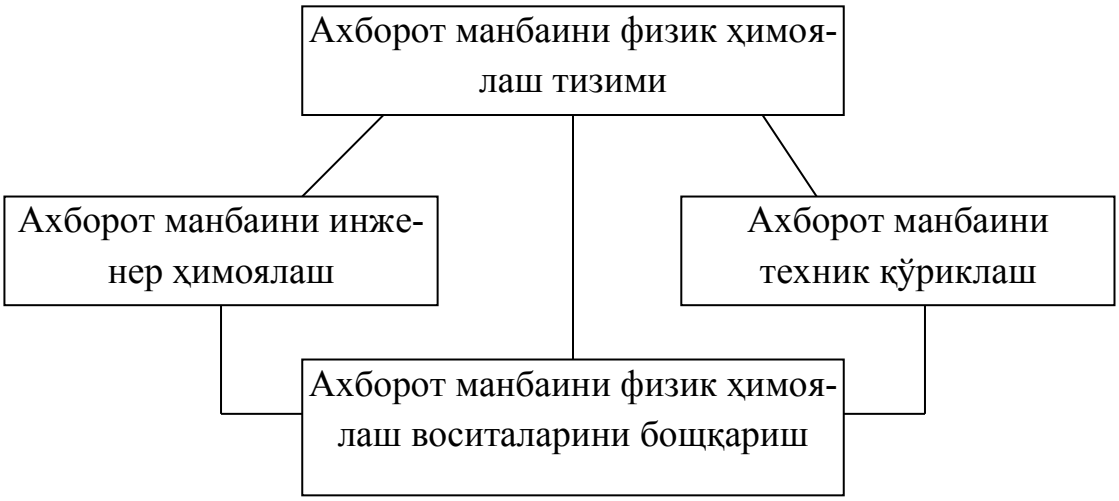
Ахборотни химоялаш унинг самарадорлигини назоратламасдан амалга ошириш мумкин бўлмаганлиги сабабли, бошқариш тизимининг мухим вазифаси химоялаш бўйича чораларни турли хил назоратлашни ташкил этиш ва амалга оширишдир.

Физик химоялаш тизимининг таркиби турли – туман: оддий қулфли ёғоч эшикдан то қўриқлашнинг автоматлаштирилган тизимигача. Физик химоялаш тизимнинг умумлаштирилган схемаси 10.11-расмда келтирилган.

Объектларни инженер ҳимоялаш ва техник қўриқлаш зарурияти статистика орқали тасдиқланади, яъни суқилиб киришларнинг 50% дан кўпроғи ходимлар ва мижозлар томонидан эркин фойдаланиладиган объектларга амалга оширилса, фақат 5 % кучли қўриқлаш режимли объектларга амалга оширилади.

Нияти бузуқларнинг суқилиб киришлари яширинча, инструмент ёрда-

мида ёки портлатиш орқали инженер конструкцияларини механик бузиш билан амалга оширилиши мумкин. Баъзи холларда суқилиб киришлар қоровулларни нейтраллаш билан харбий хужум кўринишида амалга оширилади.



10.11-расм. Ахборот манбаини физик ҳимоялаш тизимининг структураси

Ахборотни инженер химоялашни қуйидагилар таъминлайди:

- нияти бузуқнинг ва табиий офатнинг ахборот манбаларига (ёки қимматбаҳо нарсаларга) қараб ҳаракат қилиши мумкин бўлган йўлдаги табиий ва сунъий тўсиқлар;
- фойдаланишни назоратловчи ва бошқарувчи тизимларнинг тўсувчи қурилмалари.

Табиий тўсиқларга ташкилот худудида ёки ёнидаги юриш қийин бўлган жойлар (зовурлар, жарлар, қоялар, дарёлар, қуюқ ўрмон ва чангалзор) тааллуқли бўлиб, улардан чегаралар мустахкамлигини кучайтиришда фойдаланиш мақсадга мувофиқ ҳисобланади.

Сунъий тўсиқлар одамлар томонидан яратилиб, табиий тўсиқлардан конструкцияси ва нияти бузуқ таъсирига барқарорлиги билан жиддий фарқланади. Уларга турли деворлар, қаватлараро поллар, шиплар, бино дера-

залари ва ҳ. тааллуқли.

Барқарорлиги энг паст тўсиқларга биноларнинг эшиклари ва деразалари, айниқса бинонинг биринчи ва охирги қаватларидаги эшиклар ва деразалар тааллуқли. Эшиклар (дарвозалар)нинг мустаҳкамлиги уларнинг қалинлигига, ишлатилган материал хилига ва конструкциясига ҳамда қулфларнинг ишончлигига боғлиқ.

Деразалар механик таъсирга бардош ойна ва металл панжаралар ёрдамида мустахкамланади.

Ҳимоянинг охирги чегараларини металл шкафлар, сейфлар ташкил этади. Шу сабабли уларнинг механик мустахкамлигига юқори талаблар қўйилади.

Металл шкафлар махфийлик грифи юқори бўлмаган ҳужжатларни, қимматбаҳо нарсаларни, катта бўлмаган пул маблағини сақлашга мўлжалланган. Шкафларнинг ишончлилиги фақат металнинг пишиқлигига ва қулфларнинг махфийлигига боғлиқ.

Муҳим ҳужжатларни, нарсаларни, катта пул маблағини сақлаш учун *сейфлар* ишлатилади. Сейфларга деворлари орасидаги бўшлиққа турли материаллар, масалан бетон бирикмалари билан тўлдирилган икки қаватли металл шкафлар тааллуқли.

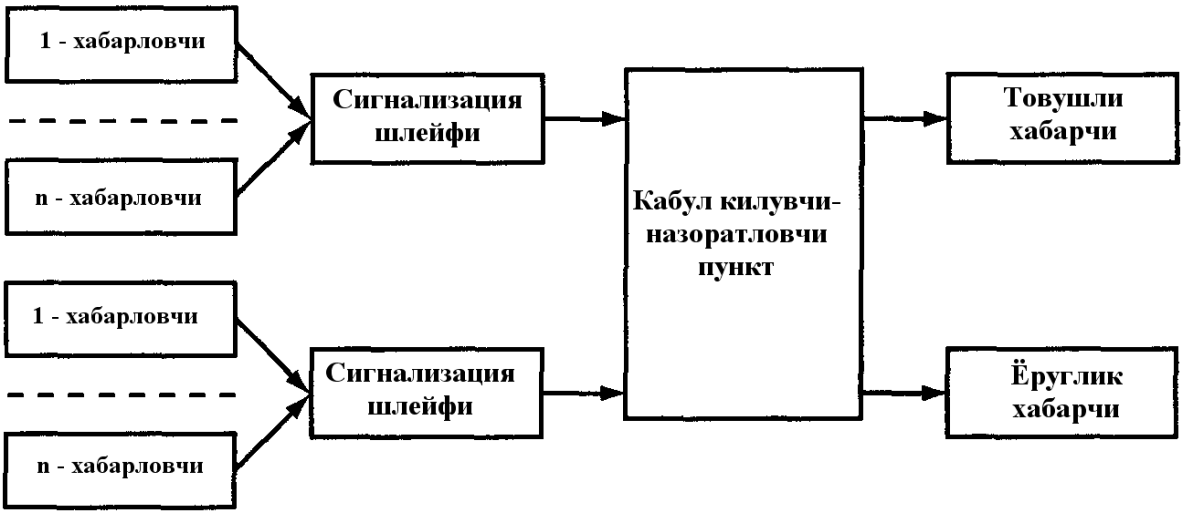
Нияти бузуқларнинг ғовларни ва механик тўсиқларни енгишга уринишларини ҳамда ёнғинни аниқлаш учун турли физик принципларда қурилган *объектларни қўриқловчи техник воситалардан* фойдаланилади.

10.12 - расмда объектларни қўриқловчи техник воситалар комплексининг намунавий структураси келтирилган. Қўриқлайдиган *хабарловчи* (датчик) техник қурилма бўлиб, у унга нияти бузуқ томонидан механик куч ва майдон таъсир қилганида тревога сигналини шакллантиради. Самарали универсал датчикларни яратиш мумкин бўлмаганлиги сабабли, нияти бузуқнинг алоҳида аломатларини ва ёнғинни сезувчи датчик турларининг катта сони яратилган. Турли хил датчиклардан олинган маълумотлардан биргаликда фойдаланиш хатоликларни камайтиришга имкон беради.

Сигнализация шлейфи электр занжирни ҳосил қилиб, датчиклар ва қабул қилувчи - назоратловчи асбобларнинг электр боғланишини таъминлайди. Уловчи симларни тежаш мақсадида датчиклар гуруҳларга бирлаштирилади, шлейфлар эса қабул қилувчи - назоратловчи асбоб билан уланади. Масалан, қўриқловчи ва ёнғин датчиклари тревога сигналларини битта шлейф орқали узатади.

Шлейфлар қанча кўп бўлса, датчикларнинг ўрнатилиш жойларининг локализацияланганлиги шунчалик аниқ бўлади ва нияти бузуқнинг суқилиб кириш жойи аниқроқ аниқланади. Ундан ташқари қўриқлаш ва ёнғин сигнализациялари учун алоҳида шлейфлар бўлиши мақсадга мувофиқ ҳисобланади. Бу ҳолда ёнғиндан қўриқлашнинг сигнализация воситаларини иш вақтида ўчириб қўйиш мумкин.

Қабул қилувчи – назоратловчи пункт датчиклардан келадиган сигналларни қабул қилиш ва ишлашга, қўриқлаш ходимларини товуш ва ёруғлик сигнали ёрдамида тревога сигналлари келганлиги, датчиклар ва шлейфлар ишлашидаги носозликлар хусусида хабардор қилишга мўлжалланган.



10.12-расм. Объектларни қўрикловчи техник воситалар комплексининг намунавий структураси

Ҳозирда *телевизион кузатув тизими* кенг қўлланилмоқда. Бу тизим

таркибига тунги вақтда қўриқланувчи ҳудудда керакли ёритилганлик даражасини таъминловчи навбатчи ёритувчи воситалари ҳам киради. Кузатиш тизими қўриқланувчи худуд ва нияти бузуқларнинг ҳаракатини масофадан визуал назоратлашга имкон беради. Ундан ташқари замонавий кузатув воситаларининг имкониятлари нияти бузуқнинг назоратланувчи зоналарга суқилиб киришини аниқлаш ва қўриқлаш масалаларини ҳал этаолади.

Автоном қўриқлаш тизимининг эксплуатацияси катта сарф - харажатларни талаб этади. Шу сабабли марказлаштирилган қўриқлаш тизимлари кенг қўлланилади. Ушбу тизимда нияти бузуқларни нейтраллаштириш масаласи бир неча ташкилотлар учун умумий ҳисобланади.

Марказлаштирилган қўриқлашга мисол тариқасида омонат банк филиалларини, кичик фирмаларни, хусусий уйларни, дала ҳовлиларни, хонадонларни қўриқлашни кўрсатиш мумкин. Худудий ёнма – ён, масалан битта бинода жойлашган фирмалар қўриқлашнинг умумий бўлинмасига эга бўлишлари мумкин. Самарали марказлаштирилган қўриқлашни ички ишлар вазирлигининг қўриқлаш хизмати бўлинмаси таъминлайди.

Тревога сигнали келиши билан оператор буйруғи бўйича қўриқлаш объектига қуролланган ходимлар гуруҳи жўнатилади. Қўриқлаш гуруҳининг объектга етиб келиш вақти қатъий белгиланган (5-7 минут). Аммо марказлаштирилган қўриқлаш тизимининг реакция вақти автоном қўриқлаш тизимига қараганда катта, айниқса агар қўриқланувчи объект мобил қўриқлаш гуруҳининг машинаси турган жойдан узоқда бўлса. Ундан ташқари ушбу вақт баъзи ҳолларда ножоиз катталаши мумкин. Бунга мисол тариқасида радиоалоқанинг бузилишини, йўллардаги “тирбандлик”ни, тасодифий йўл - транспорт ҳодисаларини ва ҳ. кўрсатиш мумкин. Аммо, марказлаштирилган қўриқлаш тизими тахдидларни, айниқса қуролли хужумларни нейтраллашда катта имкониятларга эга.

Назорат учун саволлар:

1. Ахборот манбаларини физик ҳимоялаш тизими тушунчаси.

2. Объектларни инженер ҳимоялаш ва техник қуриқлаш тизими таркиби.

3. Объектларни қуриқловчи техник воситалар комплексининг намунавий структуралари.

Фойдаланилган ва тавсия этиладиган адабиётлар

1. Борисов М.А., Романов О.А. Основы организационно-правовой защиты информации. Изд. 4-е-М: Ленанд, 2015.
2. Шаньгин В.Ф. Информационная безопасность. М: ДМК Пресс, 2014.
3. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студ. Учреждений выс. Образования/ - М.: Издательский центр «Академия», 2014.
4. Мельников Д.А. Информационная безопасность открытых систем: учебник / -М.: Флинта: Наука, 2013.
5. Stamp, Mark. Information security: principles and practice / Mark Stamp/ -2nd ed. ISBN 978-0-4-470-62639-9(hardback)/ QA76.9.A25S69, USA, 2011.
6. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы 4 издание - Питер-2010. 944с.
7. Hacking exposed. Web Applications 3. Joel Scambray, Vincent Liu, Caleb Sima. 2010 y.
8. P.Y.A. Ryan, S.A. Schneider, M.H. Goldsmith, G. Lowe and A.W. Roscoe. The Modelling and Analysis of Security Protocols: the CSP Approach. The original version is in print December 2010 with Pearson Education.
9. Hacking exposed. Network Security Secret &solutions. Stuart McClure, Joel Scambray, Jeorge Kurtz. 2009 y.
10. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. Учебное пособие. Допущено УМО. М.: Изд. центр «Академия», 2009. – 272 с.
11. Сергей Панасенко. Алгоритмы шифрования. Специальный справочник. Санкт-Петебург 2009. 576с.
12. Ганиев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т.,

“Алоқачи” 2008.

13. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на Си. – М.: Издательство ТРИУМФ, 2008 г.

14. А.А. Варфоломеев. Основы информационной безопасности. Москва 2008. 412с.

15. Е.И. Духан, Н. И. Синадский, Д. А. Хорьков. Применение программно-аппаратных средств защиты компьютерной информации. Екатеринбург УГТУ–УПИ 2008

16. Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А. С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. Защита информации в компьютерных сетях. Практический курс. Екатеринбург УГТУ–УПИ 2008. 248с.

17. Rafail Ostrovskiy, Roberto de Prisco, Ivan Visconti. Security and Cryptography for networks. Springer-Verlag Berlin Heidelberg 2008.

18. Johnny Long, Timothy Mullen, Ryan Russel, Scott Pinzon. Stealing the network. How to own a shadow. 2007.

19. William Stallings. Cryptography and Network Security Principles and Practices, Fourth Edition. USA, 2006.

20. Ю.В. Романец, П.А. Тимофеев. Защита информации в компьютерных системах и сетях. Санкт-Петербург 2006 г.

21. Торокин А.А. Инженерно–техническая зашита информации: учеб. пособие для студентов, обучаюшихся по специальностям в обл. информ. безопасности / А.А.Торокин – М: Гелиос АРВ, 2005-960с.

22. Бузов Г.А. и др. Защита от утечки информации по техническим каналам. – М.: - Телеком, 2005.

23. С.С.Қосимов. Ахборот технологиялари. Ўқув қўлланма. — Тошкент. “Алоқачи”, 2006.

24. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения. Петербург, 2005. — 432 с.

25. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты ин-

формации: Учебное пособие для вузов. –М.: Горячая линия – Телеком, 2005. – 229 с. : ил.

26. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защиты информации в сети – анализ технологий и синтез решений – М.: ДМК Пресс, 2004.

27. Д. Ю. Гамаюнов, А.И. Качалин. Обнаружение атак на основе анализа переходов состояний распределённой системы. Москва, 2004.

28. Горбатов В. С, Полянская О. Ю. Основы технологии PKI. М.: Горячая линия-Телеком, 2004. - 248 с

29. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров.-Москва. 2004.

30. С.К.Ғаниев, М.М. Каримов. Ҳисоблаш системалари ва тармоқларида информация ҳимояси. Олий ўқув юрт.талаб. учун ўқув қўлланма.-Тошкент Давлат техника университети, 2003.

31. А.М. Астахов. Аудит безопасности информационных систем. //Конфидент.-2003.-№1,2.

32. А. Соколов, О. Степанюк. Защита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002.

33. ISO/IEC 27001:2005 – “Ахборот технологиялари. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқариш тизимлари. Талаблар”.

34. ISO/IEC 27002:2005 – “Ахборот технологияси. Хавфсизликни таъминлаш методлари. Ахборот хавфсизлигини бошқаришнинг амалий қоидалари.

35. O‘zDStISO/IEC 27005:2013 – “Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборотхавфсизлиги рискларини бошқариш”

36. O‘zDStISO/IEC 27006:2013 – “Ахборот технологияси. Хавфсизликни таъминлаш усуллари. Ахборот хавфсизлигини бошқариш тизимларининг аудити ва уларни сертификатлаштириш органларига қўйиладиган талаблар”

37. ISO/IEC 15408-1-2005 – “Ахборот технологияси. Хавфсизликни

таъминлаш методлари ва воситалари. Ахборот технологиялари хавфсизлигини баҳолаш мезонлари”

38. O‘z DSt 1092:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари”

39. O‘z DSt 1105:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми”

40. O‘z DSt 1106:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси”

41. O‘z DSt 1204:2009 – “Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Криптографик модулларга хавфсизлик талаблари”

42. RH 45-215:2009 - Раҳбарий ҳужжат. Маълумотлар узатиш тармоғида ахборот хавфсизлигини таъминлаш тўғрисида Низом.

43. RH 45-185:2011-Раҳбарий ҳужжат.Давлат ҳокимияти ва бошқарув органларининг ахборот хавфсизлигини таъминлаш дастурини ишлаб чиқиш тартиби.

44. RH 45-193:2007 -Раҳбарий ҳужжат. Давлат органлари сайтларини жойлаштириш учун провайдерлар серверлари ва техник майдонларнинг ахборот хавфсизлигини таъминлаш даражасини аниқлаш тартиби.

45. TSt 45-010:2010 – Тармоқ стандарти. Алоқа ва ахборотлаштириш соҳасида ахборот хавфсизлиги. Атамалар ва таърифлар.

ИЛОВАЛАР

1 - илова

RSA шифрлаш алгоритмининг дастурий амалга оширилиши.

Алгоритм модуль арифметикасининг даражага кўтариш амалидан фойдаланишга асосланган. Алгоритмни қуйидаги қадамлар кетма-кетлиги кўринишида ифодалаш мумкин.

1-қадам. Иккита 200дан катта бўлган туб сон p ва q танланади.

2-қадам. Калитнинг очиқ ташкил этувчиси n ҳосил қилинади

$$n=p*q.$$

3-қадам. Қуйидаги формула бўйича Эйлер функцияси ҳисобланади:

$$f(p,q)=(p-1)(q-1).$$

Листинг (C++ дастурлаш тилида).

```
printf("Ikkitatubsonnikiriting\t: ");
scanf("%d%d",&p,&q);
n = p*q;
phi=(p-1)*(q-1);
printf("\n\tF(n)\t= %d",phi);
do
{
printf("\n\nKiritishe\t: ");
scanf("%d",&e);
```

Эйлер функцияси n билан ўзаро туб, 1 дан n гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига эга бўлмаган сонлар тушунилади.

4-қадам.f(p,q) қиймати билан ўзаро туб бўлган катта туб сон *d* танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи e сони аниқланади

$$e \cdot d = 1 (modf(p,q)).$$

Бу шартга биноан $e \cdot d$ кўпайтманинг *f(p,q)* функцияга бўлишдан қолган қолдиқ 1га тенг. е сони очиқ калитнинг иккинчи ташкил этувчиси сифатида қабул қилинади. Махфий калит сифатида *d* ва *n* сонлари ишлатилади.

Листинг (C++ дастурлаш тилида).

```
while(FLAG==1);
d = 1;
do
{
s = (d*e)%phi;
d++;
}while(s!=1);
d = d-1;
```

6-қадам. Дастлабки ахборотунинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги *L* бит узунликдаги блокларга ажратилади, бу ерда $L–L \geq \log_2(n+1)$ шартини қаноатлантирувчи энг кичик бутун сон. Ҳар бир блок [0, *n*-1] оралиққа тааллуқли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот *X*(*i*), i=$\overline{1, I}$ сонларнинг кетма-кетлиги орқали ифодаланади. *I* нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи *Y*(*i*) сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e (\mathrm{mod} n).$$

Листинг (C++ дастурлаш тилида).

```
voidencrypt()
{
inti;
C = 1;
for(i=0;i<e;i++)
C=C*M%n;
```

```
C = C%n;
printf("\n\tShifrlanganso'z: %d",C);
}
```

Ахборотни расшифровка қилишда қуйидаги муносабатдан фойдаланилади:

$$X(i) = (Y(i))^d \,(\mathrm{mod} n).$$

Листинг (C++ дастурлаш тилида).

```
voiddecrypt()
{
inti;
M = 1;
for(i=0;i<d;i++)
M=M*C%n;
M = M%n;
printf("\n\tDeshifrlanganso'z : %d",M);
}
```

DES шифрлаш алгоритмининг дастурий амалга оширилиши.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади. Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

Расшифровка жараёни шифрлаш жараёнига инверс бўлиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.

Ҳозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроқсиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу шахсий

компьютерларнинг замонавий ривожи учун жуда кам;

- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яъни алгоритмда микропроцессорларда бажарилишида кўп вақт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).

DES алгоритмининг дастурий коди:

```
# include <stdio.h>
# include <fstream.h>
# include <string.h>
# include <iostream.h>
//Калит киритиш жараёни
int key[64]={
0,0,0,1,0,0,1,1,
0,0,1,1,0,1,0,0,
0,1,0,1,0,1,1,1,
0,1,1,1,1,0,0,1,
1,0,0,1,1,0,1,1,
1,0,1,1,1,1,0,0,
1,1,0,1,1,1,1,1,
1,1,1,1,0,0,0,1
};
//Блокларга ажратиш жараёни
class Des
{
 public:
  int keyi[16][48],
  total[64],
  left[32],
```

- right[32],
- ck[28],
- dk[28],
- expansion[48],
- z[48],
- xor1[48],
- sub[32],
- p[32],
- xor2[32],
- temp[64],
- pc1[56],
- ip[64],
- inv[8][8];
- char final[1000];
- void IP();
- void PermChoice1();
- void PermChoice2();
- void Expansion();
- void inverse();
- void xor_two();
- void xor_oneE(int);
- void xor_oneD(int);
- void substitution();
- void permutation();
- void keygen();
- char * Encrypt(char *);
- char * Decrypt(char *);
- };
- //Бошланғич IP ўзгартириш

```
void Des::IP() //Initial Permutation
{
int k=58,i;
for(i=0;i<32;i++)
{
ip[i]=total[k-1];
if(k-8>0)  k=k-8;
else       k=k+58;
}
k=57;
for( i=32;i<64;i++)
{
ip[i]=total[k-1];
if(k-8>0)   k=k-8;
else        k=k+58;
}
}
void Des::PermChoice1() //Permutation Choice-1
{
int k=57,i;
for(i=0;i<28;i++)
{
pc1[i]=key[k-1];
if(k-8>0)    k=k-8;
else         k=k+57;
}
k=63;
for( i=28;i<52;i++)
{
```

```
pc1[i]=key[k-1];
if(k-8>0)    k=k-8;
else         k=k+55;
}
k=28;
for(i=52;i<56;i++)
{
pc1[i]=key[k-1];
k=k-8;
}
}
void Des::Expansion() //Expansion Function applied on `right' half
{
int exp[8][6],i,j,k;
for( i=0;i<8;i++)
{
for( j=0;j<6;j++)
{
if((j!=0)||(j!=5))
{
k=4*i+j;
exp[i][j]=right[k-1];
}
if(j==0)
{
k=4*i;
exp[i][j]=right[k-1];
}
if(j==5)
```

- {
- k=4*i+j;
- exp[i][j]=right[k-1];
- }
- }
- }
- exp[0][0]=right[31];
- exp[7][5]=right[0];
- k=0;
- for(i=0;i<8;i++)
- for(j=0;j<6;j++)
- expansion[k++]=exp[i][j];
- }
- void Des::PermChoice2()
- {
- int per[56],i,k;
- for(i=0;i<28;i++) per[i]=ck[i];
- for(k=0,i=28;i<56;i++) per[i]=dk[k++];
- z[0]=per[13];z[1]=per[16];z[2]=per[10];z[3]=per[23];z[4]=per[0];z[5]=per[4];z[6]=per[2];z[7]=per[27];
- z[8]=per[14];z[9]=per[5];z[10]=per[20];z[11]=per[9];z[12]=per[22];z[13]=per[18];z[14]=per[11];z[15]=per[3];
- z[16]=per[25];z[17]=per[7];z[18]=per[15];z[19]=per[6];z[20]=per[26];z[21]=per[19];z[22]=per[12];z[23]=per[1];
- z[24]=per[40];z[25]=per[51];z[26]=per[30];z[27]=per[36];z[28]=per[46];z[29]=per[54];z[30]=per[29];z[31]=per[39];
- z[32]=per[50];z[33]=per[46];z[34]=per[32];z[35]=per[47];z[36]=per[43];z[37]=per[48];z[38]=per[38];z[39]=per[55];
- z[40]=per[33];z[41]=per[52];z[42]=per[45];z[43]=per[41];z[44]=per[

49];z[45]=per[35];z[46]=per[28];z[47]=per[31];

- }
- void Des::xor_oneE(int round) //for Encrypt
- {
- int i;
- for(i=0;i<48;i++)
- xor1[i]=expansion[i]^keyi[round-1][i];
- }
- void Des::xor_oneD(int round) //for Decrypt
- {
- int i;
- for(i=0;i<48;i++)
- xor1[i]=expansion[i]^keyi[16-round][i];
- }
- void Des::substitution()
- {
- int s1[4][16]={
- 14,4,13,1,2,15,11,8,3,10,6,12,5,9,0,7,
- 0,15,7,4,14,2,13,1,10,6,12,11,9,5,3,8,
- 4,1,14,8,13,6,2,11,15,12,9,7,3,10,5,0,
- 15,12,8,2,4,9,1,7,5,11,3,14,10,0,6,13
- };
- int s2[4][16]={
- 15,1,8,14,6,11,3,4,9,7,2,13,12,0,5,10,
- 3,13,4,7,15,2,8,14,12,0,1,10,6,9,11,5,
- 0,14,7,11,10,4,13,1,5,8,12,6,9,3,2,15,
- 13,8,10,1,3,15,4,2,11,6,7,12,0,5,14,9
- };
- int s3[4][16]={

- 10,0,9,14,6,3,15,5,1,13,12,7,11,4,2,8,
- 13,7,0,9,3,4,6,10,2,8,5,14,12,11,15,1,
- 13,6,4,9,8,15,3,0,11,1,2,12,5,10,14,7,
- 1,10,13,0,6,9,8,7,4,15,14,3,11,5,2,12
- };
- int s4[4][16]={
- 7,13,14,3,0,6,9,10,1,2,8,5,11,12,4,15,
- 13,8,11,5,6,15,0,3,4,7,2,12,1,10,14,9,
- 10,6,9,0,12,11,7,13,15,1,3,14,5,2,8,4,
- 3,15,0,6,10,1,13,8,9,4,5,11,12,7,2,14
- };
- int s5[4][16]={
- 2,12,4,1,7,10,11,6,8,5,3,15,13,0,14,9,
- 14,11,2,12,4,7,13,1,5,0,15,10,3,9,8,6,
- 4,2,1,11,10,13,7,8,15,9,12,5,6,3,0,14,
- 11,8,12,7,1,14,2,13,6,15,0,9,10,4,5,3
- };
- int s6[4][16]={
- 12,1,10,15,9,2,6,8,0,13,3,4,14,7,5,11,
- 10,15,4,2,7,12,9,5,6,1,13,14,0,11,3,8,
- 9,14,15,5,2,8,12,3,7,0,4,10,1,13,11,6,
- 4,3,2,12,9,5,15,10,11,14,1,7,6,0,8,13
- };
- int s7[4][16]={
- 4,11,2,14,15,0,8,13,3,12,9,7,5,10,6,1,
- 13,0,11,7,4,9,1,10,14,3,5,12,2,15,8,6,
- 1,4,11,13,12,3,7,14,10,15,6,8,0,5,9,2,
- 6,11,13,8,1,4,10,7,9,5,0,15,14,2,3,12
- };

```
int s8[4][16]={
13,2,8,4,6,15,11,1,10,9,3,14,5,0,12,7,
1,15,13,8,10,3,7,4,12,5,6,11,0,14,9,2,
7,11,4,1,9,12,14,2,0,6,10,13,15,3,5,8,
2,1,14,7,4,10,8,13,15,12,9,0,3,5,6,11
};
int a[8][6],k=0,i,j,p,q,count=0,g=0,v;
for(i=0;i<8;i++)
{
for(j=0;j<6;j++)
{
a[i][j]=xor1[k++];
}
}
for( i=0;i<8;i++)
{
p=1;q=0;
k=(a[i][0]*2)+(a[i][5]*1);
j=4;
while(j>0)
{
q=q+(a[i][j]*p);
p=p*2;
j--;
}
count=i+1;
switch(count)
{
case 1:         v=s1[k][q];  break;
```

```
case 2:     v=s2[k][q];  break;
case 3:     v=s3[k][q];  break;
case 4:     v=s4[k][q];  break;
case 5:     v=s5[k][q];  break;
case 6:     v=s6[k][q];  break;
case 7:     v=s7[k][q];  break;
case 8:     v=s8[k][q];  break;
}
int d,i=3,a[4];
while(v>0)
{
d=v%2;
a[i--]=d;
v=v/2;
}
while(i>=0)
{
a[i--]=0;
}
for(i=0;i<4;i++)
sub[g++]=a[i];
}
}
void Des::permutation()
{
p[0]=sub[15];p[1]=sub[6];p[2]=sub[19];p[3]=sub[20];p[4]=sub[28];p[
5]=sub[11];p[6]=sub[27];p[7]=sub[16];
p[8]=sub[0];p[9]=sub[14];p[10]=sub[22];p[11]=sub[25];p[12]=sub[4];
p[13]=sub[17];p[14]=sub[30];p[15]=sub[9];
```

- p[16]=sub[1];p[17]=sub[7];p[18]=sub[23];p[19]=sub[13];p[20]=sub[31];p[21]=sub[26];p[22]=sub[2];p[23]=sub[8];
- p[24]=sub[18];p[25]=sub[12];p[26]=sub[29];p[27]=sub[5];p[28]=sub[21];p[29]=sub[10];p[30]=sub[3];p[31]=sub[24];
- }
- void Des::xor_two()
- {
- int i;
- for(i=0;i<32;i++)
- {
- xor2[i]=left[i]^p[i];
- }
- }
- void Des::inverse()
- {
- int p=40,q=8,k1,k2,i,j;
- for(i=0;i<8;i++)
- {
- k1=p;k2=q;
- for(j=0;j<8;j++)
- {
- if(j%2==0)
- {
- inv[i][j]=temp[k1-1];
- k1=k1+8;
- }
- else if(j%2!=0)
- {
- inv[i][j]=temp[k2-1];

- k2=k2+8;
- }
- }
- p=p-1;q=q-1;
- }
- }
- char * Des::Encrypt(char *Text1)
- {
- int i,a1,j,nB,m,iB,k,K,B[8],n,t,d,round;
- char *Text=new char[1000];
- strcpy(Text,Text1);
- i=strlen(Text);
- int mc=0;
- a1=i%8;
- if(a1!=0) for(j=0;j<8-a1;j++,i++) Text[i]=' '; Text[i]='\0';
- keygen();
- for(iB=0,nB=0,m=0;m<(strlen(Text)/8);m++) //Repeat for TextLenth/8 times.
- {
- for(iB=0,i=0;i<8;i++,nB++)
- {
- n=(int)Text[nB];
- for(K=7;n>=1;K--)
- {
- B[K]=n%2; //Converting 8-Bytes to 64-bit Binary Format
- n/=2;
- } for(;K>=0;K--) B[K]=0;
- for(K=0;K<8;K++,iB++) total[iB]=B[K]; //Now `total' contains the 64-Bit binary format of 8-Bytes

- }
- IP(); //Performing initial permutation on `total[64]'
- for(i=0;i<64;i++) total[i]=ip[i]; //Store values of ip[64] into total[64]
- for(i=0;i<32;i++) left[i]=total[i]; // +--> left[32]
- // total[64]--|
- for(;i<64;i++) right[i-32]=total[i];// +--> right[32]
- for(round=1;round<=16;round++)
- {
- Expansion(); //Performing expansion on `right[32]' to get `expansion[48]'
- xor_oneE(round); //Performing XOR operation on expansion[48],z[48] to get xor1[48]
- substitution();//Perform substitution on xor1[48] to get sub[32]
- permutation(); //Performing Permutation on sub[32] to get p[32]
- xor_two(); //Performing XOR operation on left[32],p[32] to get xor2[32]
- for(i=0;i<32;i++) left[i]=right[i]; //Dumping right[32] into left[32]
- for(i=0;i<32;i++) right[i]=xor2[i]; //Dumping xor2[32] into right[32]
- }
- for(i=0;i<32;i++) temp[i]=right[i]; // Dumping -->[swap32bit]
- for(;i<64;i++) temp[i]=left[i-32]; // left[32],right[32] into temp[64]
- inverse(); //Inversing the bits of temp[64] to get inv[8][8]
- /* Obtaining the Cypher-Text into final[1000]*/
- k=128; d=0;
- for(i=0;i<8;i++)
- {
- for(j=0;j<8;j++)
- {
- d=d+inv[i][j]*k;

- k=k/2;
- }
- final[mc++]=(char)d;
- k=128; d=0;
- }
- } //for loop ends here
- final[mc]='\0';
- return(final);
- }
- char * Des::Decrypt(char *Text1)
- {
- int i,a1,j,nB,m,iB,k,K,B[8],n,t,d,round;
- char *Text=new char[1000];
- unsigned char ch;
- strcpy(Text,Text1);
- i=strlen(Text);
- keygen();
- int mc=0;
- for(iB=0,nB=0,m=0;m<(strlen(Text)/8);m++) //Repeat for TextLenth/8 times.
- {
- for(iB=0,i=0;i<8;i++,nB++)
- {
- ch=Text[nB];
- n=(int)ch;//(int)Text[nB];
- for(K=7;n>=1;K--)
- {
- B[K]=n%2; //Converting 8-Bytes to 64-bit Binary Format
- n/=2;

- } for(;K>=0;K--) B[K]=0;
- for(K=0;K<8;K++,iB++) total[iB]=B[K]; //Now `total' contains the 64-Bit binary format of 8-Bytes
- }
- IP(); //Performing initial permutation on `total[64]'
- for(i=0;i<64;i++) total[i]=ip[i]; //Store values of ip[64] into total[64]
- for(i=0;i<32;i++) left[i]=total[i]; // +--> left[32]
- // total[64]--|
- for(;i<64;i++) right[i-32]=total[i];// +--> right[32]
- for(round=1;round<=16;round++)
- {
- Expansion(); //Performing expansion on `right[32]' to get `expansion[48]'
- xor_oneD(round);
- substitution();//Perform substitution on xor1[48] to get sub[32]
- permutation(); //Performing Permutation on sub[32] to get p[32]
- xor_two(); //Performing XOR operation on left[32],p[32] to get xor2[32]
- for(i=0;i<32;i++) left[i]=right[i]; //Dumping right[32] into left[32]
- for(i=0;i<32;i++) right[i]=xor2[i]; //Dumping xor2[32] into right[32]
- } //rounds end here
- for(i=0;i<32;i++) temp[i]=right[i]; // Dumping -->[swap32bit]
- for(;i<64;i++) temp[i]=left[i-32]; // left[32],right[32] into temp[64]
- inverse(); //Inversing the bits of temp[64] to get inv[8][8]
- /* Obtaining the Cypher-Text into final[1000]*/
- k=128; d=0;
- for(i=0;i<8;i++)
- {
- for(j=0;j<8;j++)

```
{
d=d+inv[i][j]*k;
k=k/2;
}
final[mc++]=(char)d;
k=128;   d=0;
}
} //for loop ends here
final[mc]='\0';
char *final1=new char[1000];
for(i=0,j=strlen(Text);i<strlen(Text);i++,j++)
final1[i]=final[j]; final1[i]='\0';
return(final);
}
int main()
{
Des d1,d2;
char *str=new char[1000];
char *str1=new char[1000];
 //strcpy(str,"PHOENIX it & ece solutions.");
cout<<"Enter a string : ";
gets(str);
str1=d1.Encrypt(str);
cout<<"\ni/p Text: "<<str<<endl;
cout<<"\nCypher  : "<<str1<<endl;
//        ofstream fout("out2_fil.txt"); fout<<str1; fout.close();
cout<<"\no/p Text: "<<d2.Decrypt(str1)<<endl;
return 0;
}
```

```
// Калит генерацияси жараёни
void Des::keygen()
{
PermChoice1();
int i,j,k=0;
for(i=0;i<28;i++)
{
ck[i]=pc1[i];
}
for(i=28;i<56;i++)
{
dk[k]=pc1[i];
k++;
}
int noshift=0,round;
for(round=1;round<=16;round++)
{
if(round==1||round==2||round==9||round==16)
noshift=1;
else
noshift=2;
while(noshift>0)
{
int t;
t=ck[0];
for(i=0;i<28;i++)
ck[i]=ck[i+1];
ck[27]=t;
t=dk[0];
```

```
for(i=0;i<28;i++)
dk[i]=dk[i+1];
dk[27]=t;
noshift--;
}
PermChoice2();
for(i=0;i<48;i++)
keyi[round-1][i]=z[i];
}
}
```

Паролли аутентификациялаш алгоритмининг дастурий амалга оширилиши.

Оддий аутентификацияни ташкил этиш схемалари нафақат паролларни узатиш, балки уларни сақлаш ва текшириш турлари билан ажралиб туради. Энг кенг тарқалган усул – фойдаланувчилар паролини тизимли файлларда очиқ ҳолда сақлаш усулидир. Бунда файлларга ўқиш ва ёзишдан ҳимоялаш атрибутлари ўрнатилади (масалан, операцион тизимдан фойдаланишни назоратлаш руйхатидаги мос имтиёзларни тавсифлаш ёрдамида). Тизим фойдаланувчи киритган паролни пароллар файлида сақланаётган ёзув билан солиштиради. Бу усулда шифрлаш ёки бир томонлама функциялар каби криптографик механизмлар ишлатилмайди. Ушбу усулнинг камчилиги – нияти бузуқ одамнинг тизимда маъмур имтиёзларидан, шу билан бирга тизим файлларидан, жумладан парол файлларидан фойдаланиш имкониятидир.

Аутентификациялаш алгоритмининг дастурий коди(C++ дастурлаш тилида).

Фойдаланувчини аутентификациядан ўтказиш функцияси:

```
void Auth()
{
    cout<<"Authentification process";
```

```
        ifstream Passfile("password.txt", ios::in);
        Passfile>>inpass;
        ifstream Userfile("username.txt", ios::in);
        Userfile>>inuser;
        system("cls");
        cout<<"USERNAME: ";
        cin>>user;
        cout<<"PASSWORD: ";
        cin>>pass;
        Userfile.close();
        Passfile.close();
        if(user==inuser&&pass==inpass)
        {
                cout<<"\nHit enter to continue to members area";
                        getch();
                //Nimadir sh qisin
                main();
        }
        else
        {
                cout<<"nope";
                getch();
                main();
        }
}
```

Фойдаланувчини руйхатдан ўтказиш функцияси:

```
void Registration()
{
        string tempuser, temppassword;
        cout<<"Enter Username: ";
```

```
        cin>>tempuser;
        cout<<"\nEnter password: ";
        cin>>temppassword;
        ofstream Userfile("username.txt", ios::out);
        Userfile<<tempuser;
        Userfile.close();
        ofstream Passfile("password.txt", ios::out);
        Passfile<<temppassword;
        Passfile.close();
        cout<<"Account hass been added";
        getch();
        main();
}
```

2-илова

Атамаларнинг рус, ўзбек ва инглиз тилларидаги изоҳли луғати

Авторизация- представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Авторизация –тизимда фойдаланувчига, унинг ижобий аутенфикациясига асосан, маълум фойдаланиш хукукларини такдим этиш.

Authorization -View user specific access rights on the basis of a positive result in its authentication system.

Авторское право - совокупность правовых норм (раздел гражданского права), которые регулируют отношения, возникающие в связи с созданием и использованием произведений науки, литературы и искусства.

Муаллифлик ҳуқуқи – фан, адабиёт ва санъат асарларини яратиш, фойдаланиш ва ҳуқуқий ҳимоялашда вужудга келадиган муносабатларни тартибга солувчи ҳуқуқий нормалар мажмуи.

Copyright - the body of law (Civil Law Section), which regulate the relations arising in connection with the creation and use of scientific, literary and artistic works (copyright).

Администратор защиты- субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Ҳимоя маъмури – автоматлаштирилган тизимни ахборотдан рухсатсиз фойдаланишдан ҳимоялашга жавобгар фойдаланиш субъекти.

Security administrator-access entity responsible for the protection of the automated system from unauthorized access to information.

Акустическая защищенность выделенного помещения - уровень акустической защищенности выделенного помещения, достигнутый в ре-

зультате проведения акустической защиты.

Ажратилган хонанинг акустик ҳимояланганлиги – акустик ҳимоянинг ўтказилиши натижасида эришилган ажратилган хонанинг акустик ҳимояланганлиги даражаси.

Acoustic protection dedicated premises - level of acoustic protection dedicated space made as a result of acoustic protection.

Акустическая информация - информация, носителем которой являются акустические сигналы.

Акустик ахборот – элтувчиси акустик сигналлар бўлган ахборот.

Acoustic information - information that is held by acoustic signals.

Алгоритм - упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Алгоритм – амалларнинг чекланган сони ёрдамида масала ечимини белгиловчи буйруқларнинг чекланган тўплами.

Algorithm - an ordered finite set of clearly defined rules for solving a finite number of steps.

Алгоритм блочного шифрования - алгоритм зашифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков текста открытого, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины.

Шифрлашнинг блокли алгоритми - шифрлаш алгоритми булиб, калитнинг хар бир муайян кийматида белгиланган узунликдаги очик матн блоклари тўплами устида битта кайтарилувчи акслантиришни амалга оширади. Белгиланган узунликдаги матн блокларини оддий алмаштириш алгаритми хисобланади.

Block encryption algorithm – encryption algorithm that implements a fixed

value for each key one reversible mapping of open block s of text with a fixed length. Algorithm is simple replacement of text blocks of fixed length.

Алгоритм поточного шифрования - алгоритм зашифрования, реализующий при каждом фиксированном значении ключа последовательность обратимых отображений (вообще говоря, различных), действующую на последовательность блоков текста открытого.

Окимли шифрлаш алгаритми- шифрлаш алгоритми булиб, калит-нинг хар бир муайян кийматида очик матн блоклари кетма-кетлигига таъсир этувчи кайтарилувчи (умуман, турли) акслантириш кетма-кетлигини амалга оширади.

Stream encryption algorithm - encryption algorithm that implements, for each fixed sequence of reversible key mappings (in general, different), acting on a sequence of blocks of text open.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию зашифрования.

Шифрлаш алгоритми- шифрлаш функциясини амалга оширувчи криптографик алгоритм.

Encryption algorithm - a cryptographic algorithm that implements the encryption function.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Криптографик алгоритм – криптографик функцияларнинг бирини хисоблашни амалга оширувчи алгоритм

Cryptographic algorithm - тhe algorithm that implements the computation of one of the cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный

к алгоритму зашифрования и реализующий функцию расшифрования.

Расшифровкалаш алгоритми – расшифровкалаш функциясини амалга оширувчи ва шифрлаш алгоритмига тескари алгоритм

Decryption algorithm – a cryptographic algorithm, the inverse of the algorithm encryption and decryption function implements.

Алгоритм формирования подписи цифровой - составная часть схемы подписи цифровой. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, ключ секретный, а также открытые параметры схемы подписи цифровой. Результатом работы алгоритма является подпись цифровая. В некоторых разновидностях схемы подписи цифровой при формировании подписи используется протокол.

Ракамли имзони шакллантириш алгоритми – ракамли имзо схемасининг таркибий кисми. Кириш йулига имзоланувчи хабар, махфий калит, хамда ракамли имзо схемасининг очик параметрлари берилувчи алгоритм. (умуман рандомизацияланган алгоритм). Алгоритм ишининг натижаси ракамли имзо хисобланади. Ракамли имзо схемасининг баьзи турларида имзони шакллантиришда протокол ишлатилади.

The algorithm for generating a digital signature - part of a digital signature scheme. Algorithm (generally randomized) whose input is fed to sign a message, secret key and public parameters of digital signature schemes. The result of the algorithm is a digital signature. In some species, the digital signature scheme used to generate the signature protocol.

Алгоритм хеширования - в криптографии — алгоритм, реализующий хеш-функцию криптографическую. В математике и программировании — алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале — от всех). Обычно, а. х. преобразует строки произвольной длины в строки

фиксированной длины.

Хешлаш алгоритми – криптографияда – криптографик хеш-функцияни амалга оширувчи алгоритм. Математик ва дастурлашда – одатда, сатр узунлигини камайтирувчи символлар сатрини узгартирувчи алгоритм. Чикиш йули сатрининг хар бир символининг киймати кириш йули символларининг катта сонига (идеалда – барчасига) мураккаб тарзда боглик. Одатда хешлаш алгоритми ихтиёрий узунликдаги сатрни белгилаган узунликдаги сатрга ўзгартиради.

Hashing algorithm - cryptography - an algorithm that implements a cryptographic hash function. In mathematics and programming - algorithm for transforming character strings, usually reduces the length of the string, and such that the value of each character of the output string depends in a complex way on a large number of input symbols (ideally - all). Typically, a. x. converts strings of arbitrary length to fixed-length strings.

Анализ трафика -1. заключение о состоянии информации на основе наблюдения за потоками трафика (наличие, отсутствие, объем, направление и частота. 2. Анализ совокупности сообщений шифрованных, передаваемых по системе связи, не приводящий к дешифрованию, но позволяющий противнику и/или нарушителю получить косвенную информацию о передаваемых сообщениях открытых и в целом о функционировании наблюдаемой системы связи. А. т. использует особенности оформления сообщений шифрованных, их длину, время передачи, данные об отправителе и получателе и т. п.

Трафик тахлили- 1. Трафик окимини кузатиш (борлиги, йуклиги хажми, йуналиши ва частотаси) асосида ахборат холати хусусида хулоса килиш. 2. Дешифрланишга сабаб бўлмайдиган, аммо ғанимга ёки бузғунчига узатилаётган очик матн ва умуман, кузатилаётган алока тизимининг ишлаши хусусидаги билвосита ахборотни олишига имкон берувчи алока тизими оркали узатилувчи шифрланган хабарлар мажмуининг тахлили. Трафик тахлили

шифрланган хабарларнинг расмийлаштириш хусусиятларидан, уларнинг узунлиги, узатилиш вакти узатувчи ва кабул килувчи хусусидаги маьлумотлардан фойдаланади.

Traffic Analysis -1 . Report on the state information based on observation of traffic flows (presence , absence, amount , direction and frequency . 2 . Analysis of all encrypted messages sent over the communication system does not lead to decrypt , but allowing the opponent and / or the offender obtain indirect information about the transmitted Post and generally observed on the functioning of the communication system . A. that uses features of registration messages encrypted , and their length , the transmission time , the data sender and recipient , etc.

Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.

Тармок тахлиллагичлари (сниффер) – тармоқ трафигини «тинглаш» ни ва тармок трафигидан автоматик тарзда фойдаланувчилар исмини, паролларни, кредит карталар номерини, шу каби бошка ахборотни ажратиб олишни амалга оширувчи дастурлар.

Network analyzers (sniffer) - Programs, asking for "listening" network traffic and automatically selects the network traffic of user names, passwords, credit card numbers, other similar information.

Анонимность - понятие, родственное. Выражает предоставляемую участникам (протокола) возможность выполнять какое-либо действие анонимно, т. е. не идентифицируя себя. При этом, однако, участник обязан доказать свое право на выполнение этого действия. Анонимность бывает абсолютной и отзываемой.

Анонимлик - Кузатолмаслик тушунчасига ухшаш. Иштирокчига (протокол иштирокчисига) кандайдир харакатни аноним тарзда, яьни ўзини

идентификацияламасдан, бажарилишини ифодалайди. Бунда, аммо, иштирокчи ушбу харакатни бажаришга хақли эканлигини исботлаши лозим. Анонимлик абсолют ва чакирилувчи бўлиши мумкин.

Anonymity - a concept related. Expresses provided to participants (protocol) to perform any act anonymously, without identifying themselves. In this case, however, the participant must prove their right to perform this action. Anonymity is absolute and recalls.

Антибот - программное обеспечение для автоматического обнаружения и удаления программ-роботов, программ-шпионов (Spyware), несанкционированно установленного рекламного ПО (Adware) и других видов вредоносного ПО.

Антивот – робот-дастурларни, айғоқчи дастурни (spyware), рухсатсиз ўрнатилган реклама дастурий таъминотни (Adware) ва бошка зарар келтирувчи дастурий таъминот турларини автоматик тарзда аникловчи ва йук килувчи дастурий таъминот.

Security Code Software for automatic detection and removal of software robots, spyware (Spyware), illegally installed adware (Adware) and other types of malicious software .

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. еще - программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.

Антивирус – вирусларни аниқловчи ёки аниқловчи ва йўқ қилувчи дастур.

Яна – вируслардан химоялашга, захарланган дастурий модуллар ва тизимли маконларни аниклашга, хамда захарланган обектларнинг дастлабки холатини тиклашга мулжалланган дастур.

Antivirus- a program that detects and detects and removes viruses. If the virus is not removed, it is possible, the infected program is destroyed. still - a program designed to protect against viruses, detection of infected software modules and system areas, as well as the original, infected objects.

Аппаратные средства защиты - механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации.

Ҳимоянинг аппарат воситалари – ахборотни рухсатсиз фойдаланишдан модификацияланишидан, нусхалашдан, ўғриланишидан ҳимоялашга мўлжалланган механик, электромеханик, электрон, оптик, лазер, радио, радиотехник, радиолокацион ва бошқа қурилмалар, тизимлар ва иншоатлар.

Hardware protection - mechanical, electromechanical, electronic, optical, laser, radio, radar and other devices, systems and structures designed to protect the information from unauthorized access, copying, modification or theft.

Аппаратура технической разведки - совокупность технических устройств обнаружения, приема, регистрации, измерения и анализа, предназначенная для получения разведывательной информации.

Техник разведка аппаратураси – разведка ахборотини олишга мўлжалланган аниқлаш, қабул қилиш, қайдлаш, ўлчаш ва таҳлиллаш техник қурилмалари мажмуи.

Equipment and technical intelligence - a set of technical detection devices, receiving, recording, measurement and analysis, designed for intelligence.

Асимметричный шифр - шифр, в котором ключ шифрования не совпадает с ключом дешифрирования.

Асимметрик шифр – бундай шифрда шифрлаш калити дешифрлаш калитига мос келмайди.

Asymmetric cipher - a cipher in which the encryption key does not match the decryption key.

Атака - нарушение безопасности информационной системы, позволяющее захватчику управлять операционной средой.

Хужум – босқинчининг операцион муҳитини бошқаришга имкон берувчи ахборот тизими хавфсизлигининг бузилиши.

Attack - breach of security of information system, which allows the invader to manage operating environment.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Хизмат килишдан воз кечишга ундайдиган хужум – тизим бузилишига сабаб булувчи хужум, яьни шундай шароитлар тугдирадики, конуний фойдаланувчи тизим такдим этган ресурслардан фойдалана олмайди ёки фойдаланиш анчагина кийинлашади.

Denial-of-Service attack (DoS attack)- Attack to cause failure of the system, that is to create the conditions under which legitimate users can not get access to the resources provided by the system, or that access will be significantly hampered.

Аттестация - оценка на соответствие определенным требованиям. С точки зрения защиты аттестации подлежат субьекты, пользователи или бъекты, помещения, технические средства, программы, алгоритмы на предмет соответствия требованиям защиты информации по соответствующим классам безопасности.

Аттестация- маълум талабларга мослигининг бахоси. Химоя нуктаи назаридан, мос хавфсизлик синфлари буйича ахборотни химоялаш талабларига мослигини аниклаш мақсадида субъектлар, фойдаланувчилар ёки объектлар, бинолар, техник воситалар, дастурлар, алгоритмлар аттестация килинади.

Attestation- assessment for compliance with certain requirements. From a security standpoint subject to certification facilities, premises, facilities, programs, algorithms, to ensure compliance with the protection of information security in the appropriate classes.

Аудит (безопасности) — ведение контроля защищенности путем регистрации (фиксации в файле аудита) заранее определенного множества событий, характеризующих потенциально опасные действия в системе компьютерной, влияющие на ее безопасность

Хавфсизлик аудити – компьютер тизими хавфсизлигига таъсир этувчи, бўлиши мумкин бўлган хавфли харакатларни характерловчи, олдиндан аникланган ходисалар тўпламини рўйхатга олиш(аудит файлида кайдлаш) йули билан химояланишни назоратлаш.

Security audit – maintain security control by registering (fixation in the audit file) a predetermined set of events that characterize the potentially dangerous actions in the computer affecting its security.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Аутентификатор– фойдаланувчининг фарқли аломатини ифодаловчи аутентификация воситаси. Кўшимча код сўзлари, биометрик маълумотлар ва фойдаланувчининг бошка фарқли аломатлари аутентификация воситалари бўлиши мумкин.

Authenticator - authentication means representing the hallmark of the user. Means of user.

Аутентификация - проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Аутентификация – одатда тизим ресурсларидан фойдаланишга рухсат етиш хусусида қарор қабул қилиш учун фойдаланувчининг (хакикийлигини), курилманинг ёки тизимнинг бошка ташкил этувчисининг идентификациясини текшириш; сақланувчи ва узатилувчи маълумотларнинг рухсатсиз модификацияланганлигини аниклаш учун текшириш.

Authentication - checking user authentication (authentication), device or other component in the system, usually to make a decision about granting access to system resources; checking the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификация биометрическая — способ аутентификации абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.

Биометрик аутенфикация – абонентни (фойдаланувчини) унинг биометрик характеристикаси (бармок излари, панжа геометрияси, юзи, овози, кўз пардасининг тўри ва х.) асосидаги аутентификациялаш усули. Ушбу усулнинг афзаллиги – биометрик характеристикаларни фойдаланувчидан ажратиб булмаслиги. Уларни эсдан чикаришнинг, йўқотишнинг ёки бошка фойдаланувчига беришнинг иложи йук.

Biometric Authentication - Authentication Method subscriber (user), based on its verification of biometrics (fingerprints, hand geometry, face, voice, retina pattern, etc.). The advantages of this method is the inseparability of the biometric characteristics of the user: they can not be forgotten, lost or transferred to another user.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Икки факторли аутентификация – фойдаланувчиларни иккита турли факторлар асосида аутентификациялаш, одатда, фойдаланувчи биладиган нарса ва эгалик киладиган нарса (масалан, пароль ва физик идентификатори) асосида.

Two-factor authentication- user authentication based on two different factors are usually based on what the user knows, and what he owns (eg password-based and physical identifier).

Аутентификация многофакторная — реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов.

Куп факторли аутентификация- бир неча мустақил факторлар асосида фойдаланувчини идентификациялаш орқали фойдаланиш назоратини амалга ошириш.

Multifactor Authentication - implementing access control, which is a user identification based on several independent factors.

Аутентичность — 1. подлинность. 2. свойство гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким субъектам, как пользователи, процессы, системы и информация.

Аслига тўғрилик- 1. Хақиқийлик 2. Субъект ёки ресурснинг сўралганига мувофиқлиги кафолатланувчи хусусият. Аслига тўғрилик фойдаланувчилар, жараёнлар, тизимлар ва ахборот каби субьектларга қўлланилади.

Authenticity - 1. Authenticity. 2. Feature ensures that the subject or resource identical stated. Authenticity applies to entities such as people, processes, systems and information.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

Маълумотлар базаси - татбиқий дастурларга боғлиқ бўлмаган холда маълумотларни тавсифлашни, сақлаш ва манипуляциялашнинг умумий принципларини кўзда тутувчи маълум қоидалар бўйича ташкил этилган маълумотар мажмуи.

Database - a set of data organized according to certain rules, general principles providing descriptions, storing and manipulating data, regardless of the application.

Банк данных - автоматизированная информационная система централизованного хранения и коллективного использования данных.

Маълумотлар банки- маълумотларни марказлашган сақлаш ва коллектив фойдаланишнинг автоматлаштирилган ахборот тизими.

Databank - automated information system for centralized storage and sharing of data.

Безопасная операционная система - операционная система, эффективно управляющая аппаратными и программными средствами с целью обеспечения уровня защиты, соответствующего содержанию данных и ресурсов, контролируемых этой системой.

Хавфсиз операцион тизим – маълумотлар ва ресурслар мазмунига мос ҳимоялаш даражасини таъминлаш мақсадида аппарат ва дастурий воситаларни самарали бошқарувчи операцион тизим.

Secure operating system - an operating system that effectively manages the hardware and software to provide the level of protection corresponding to the content data and resources controlled by the system.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Хавфсизлик - таъсири натижасида номақбул холатларга олиб келувчи атайин ёки тасодифан, ички ва ташқи беқарорловчи факторларга қарши тизимнинг тура олиш хусусияти. Яна маълумотлар файлларининг ва дастурларнинг ишлатилиши, кўриб чиқилиши ва авторизацияланмаган шахслар (жумладан тизим ходими), компъютерлар ёки дастурлар томонидан модификацияланиши мумкин бўлмаган холат.

Security - property system to withstand external or internal factors destabilizing effect of which may be undesirable its state or behavior. Also, a state in which data files and programs may not be used, viewed and modified by unauthorized persons (including staff system) computers or programs.

Безопасность автоматизированной информационной системы - совокупность мер управления и контроля, защищающая APIS от отказа в обслуживании и несанкционированного (умышленного или случайного) раскрытия, модификации или разрушения АИС и данных.

Автоматлаштирилган ахборот тизим хавфсизлиги – автоматлаштирилган ахборот тизимини хизматдан воз кечишидан ва

рухсатсиз (атайин ёки тасодифан) фош этилишидан модификацияланишдан ёки унинг ва маълумотларнинг бузилишидан ҳимояловчи бошқариш ва назорат чоралари мажмуи.

Automated information system security – a set of measures of management and control, protecting APIS denial of service and unauthorized (intentional or accidental) disclosure, modification or destruction of AIS data.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение, еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность /конфиденциальность/, целостность и доступность.

Ахборот хавфсизлиги - ахборот холати бўлиб, унга биноан ахборотга тасодифан ёки атайин рухсатсиз таъсир этишга ёки унинг олинишига йўл қўйилмайди. Яна - ахборотни техник воситалар ёрдамида ишланишида унинг махфийлик (конфиденциаллик), яхлитлик ва фойдаланувчанлик каби характеристикаларининг (хусусиятларининг) сақланишини таъминловчи ахборотнинг ҳимояланиш сатҳи холати.

Information security - state information , which prevents accidental or intentional tampering or unauthorized information to receive it, also - state -level data protection during processing technologies to support the preservation of its qualitative characteristics (properties) as privacy / confidentiality / integrity and availability.

Безопасность информационная - способность системы противостоять случайным или преднамеренным, внутренним или внешним информационным воздействиям, следствием которых могут быть ее нежелательное состояние или поведение.

Ахборот хавфсизлиги – таъсири натижасида номақбул ҳолатларга

олиб келувчи атайин ёки тасодифан, ички ва ташқи информацион таъсирларга қарши тизимнинг тура олиш хусусияти.

Safety information - the system's ability to resist accidental or intentional, internal or external information influences, that could result in an undesirable state or her behavior.

Безопасность информационно - коммуникационных технологий (безопасность ИТТ) — все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно-телекоммуникационных технологий.

Ахборот - коммуникация технологиялар хавфсизлиги (АТТ хавсизлиги) – ахборот - телекоммуникация технологияларининг конфиренциаллигини, яхлитлигини, фойдаланувчанлигини, бош тортмаслигини, ҳисобот беришини, аслига тўғрилигини ва ишончлигини аниқлаш, уларга эришиш ва мададлаш билан боғлиқ барча жихатлар.

ICT security – communication technology (ICT security) - All aspects related to the definition, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and telecommunication technologies.

Безопасность сетевая — меры, предохраняющие сеть информационную от доступа несанкционированного, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

Тармоқ хавфсизлиги - ахборот тармоғини рухсатсиз фойдаланишдан, меъёрий ишлашига тасодифан ёки атайин аралашишдан ёки тармоқ компонентларини бузишга уринишдан эхтиёт қилувчи чоралар. Асбоб-ускуналарни, дастурий - таъминотни, маълумотларни ҳимоялашни ўз ичига

олади.

Network Security - measures that protect the network information from un-authorized access, accidental or intentional interference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.

Безотказность - способность системы выполнять возложенные на нее функции в требуемый момент времени в задаваемых условиях.

Бузилмаслик – тизимнинг унга юклатилган вазифаларини исталган вақт онида, берилган шароитда бажариш қобилияти.

Reliability - The ability of the system to fulfill its function in the desired time in the given conditions.

Биометрические данные - средства аутентификации, представляющие собой такие личные отличительные признаки пользователя как тембр голоса, форма кисти руки, отпечатки пальцев и т.д., оригиналы которых в цифровом виде хранятся в памяти компьютера.

Биометрик маълумотлар – аутентификация воситаси бўлиб, фойдаланувчининг бармоқ излари, қўл панжасининг геометрик шакли, юз шакли, ва ўлчамлари, овоз хусусиятлари, кўз ёй ва тўр пардасининг шакли каби шахсий, фарқли аломатлари. Асл нусхалари рақам кўринишида компъютер хотирасида сақланади.

Biometric data - authentication, which are personal features such as user tone of voice, the shape of the hand, fingerprints, etc., The originals of which are stored digitally in a computer memory.

Бот — (сокр. от робот) Специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. При обсуждении компьютерных программ термин употребляется в основном в применении к

Интернету.

Бот - (“робот” сўзининг қисқартирилгани). Оддий фойдаланувчи интерфейси орқали автоматик тарзда ва / ёки берилган жадвал бўйича қандайдир харакатларни бажарувчи махсус дастур. Компъютер дастурлари муҳокама қилинганида бот атамаси асосан Интернетга қўллаш билан ишлатилади.

Bot – 1. (Short for robot) Special program will be executed automatically and / or on the schedule any action through the same interface as a normal user. In the discussion, the term computer program is used mainly in the application to the Internet.

Ботнет — компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами. Обычно используются для координации сетевых атак на компьютеры — рассылки спама, хищения личных данных пользователей, перебора паролей на удалённой системе, атак на отказ в обслуживании и т.п. (от англ. слов robot и network).

Ботнет - ишга тушурилган ботларга эга бир қанча сонли хостлардан ташкил топган компъъютер тармоғи. Одатда компъютерларга бўладиган тармоқ хужумларини (оламни тарқатиш, фойдаланувчиларнинг шахсий маълумотларини ўғрилаш, масофадаги тизимда паролларни саралаш, хизмат қилишдан воз кечишга ундаш хужумлари ва ҳ.к.) мувофиқлаштириш учун ишлатилади. (инглизча robot ва network сўзларидан олинган.)

Botnet - computer network consisting of a number of hosts running bots. Usually used to coordinate attacks on network computers - spam, identity theft users of brute force on the remote system attacks denial of service, etc. (from the English. words robot and network).

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля за ним аппаратно-программными средствами. еще - является защитным ба-

рьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

Брандмауэр – аппарат-дастурий воситалар ёрдамида тармоқдан фойдаланишни марказлаштириш ва уни назоратлаш йўли билан тармоқни бошқа тизимлардан ва тармоқлардан келадиган хавфсизликка тахдидлардан ҳимоялаш усули. Яна - бир неча компонентлардан (масалан, брандмауэр дастурий таъминоти ишлайдиган маршрутизатор ёки шлюздан) ташкил топган химоя тўсиғи ҳисобланади.

Firewall - a method of protecting the network from security threats from other systems and networks by centralizing network access and control of hardware and software. Also, is a protective barrier, consisting of several components (such as a router or gateway that is running firewall software).

Брандмауэр с фильрацией пакетов - является маршрутизатором или компьютером, на котором работает программное обеспечение, сконфигурированное таким образом, чтобы отбраковывать определенные виды входящих и исходящих пакетов

Пакетларни фильтрловчи брандмауэр – кирувчи ва чиқувчи пакетларни маълум хилларини бракка чиқариш мақсадида конфигурацияланган дастурий таъминот ишлайдиган маршрутизатор ёки компьютер.

Packet-filtering firewall – a router or computer on which the software is running, configured so as to reject certain types of incoming and outgoing packets.

Брандмауэр экспертного уровня - проверяет содержимое принимаемых пакетов на трех уровнях модели OSI - сетевом, сеансовом и прикладном. Для выполнения этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизованных пакетов.

Эксперт сатҳидаги брандмауэр- олинадиган пакетларни ISO

моделининг учта сатхида тармоқ, сеанс ва татбиқий сатҳларда текширади. Ушбу вазифани бажаришда пакетларни фильтрлашнинг махсус алгоритмлари ишлатилади. Улар ёрдамида ҳар бир пакет авторизатцияланган пакетларнинг маълум шаблонлари билан таққосланади.

Stateful inspecthion firewall - checks the contents of the packets received on the three levels of the model OSI - network, session and application. To perform this task, use special packet filtering algorithms by which each packet is compared with the known pattern of authorized packets.

Верификация - процесс сравнения двух уровней спецификации средств вычислительной техники или их комплексов на надлежащее соответствие. Еще - в программировании доказательство правильности программ. Различают два подхода к верификации: статические и конструктивные методы.

Верификация – ҳисоблаш воситалари ёки уларнинг комплекси спецификасининг икки сатҳини тегишли мосликка таққослаш жараёни. Янадастурлашда – дастур тўғрилигининг тасдиғи. Верификацияга иккита ёндашиш фарқланади: статик ва конструктив усуллар.

Verification - the process of comparing two levels of specification of computer equipment or systems for proper alignment. Also - programming proof of the correctness of programs. There are two approaches to verification: static and constructive methods.

Взламывание пароля — техника (способ) тайно получать доступ к системе (сети) информационной, в которой нападающая сторона с помощью вскрывателя паролей пробует угадать (подобрать) или украсть пароли.

Паролни бузиб очиш - ахборот тизимидан (тармоғидан) яширинча фойдаланиш техникаси (усули) бўлиб, ҳужум қилувчи тараф паролларни фош қилувчи ёрдамида паролларни аниқлашга (танлашга) ёки ўғрилашга уриниб кўради.

Cracking password - tech (method) secretly to access the system (network) information, in which the attacker using opener tries to guess passwords (pick) or steal passwords.

Виды механизмов защиты —некоторыми видами механизмов защиты являются: шифрование, аспекты административного управления ключами, механизмы цифровой подписи, механизмы управления доступом, механизмы целостности данных, механизмы обмена информацией аутентификации, механизмы заполнения трафика, механизм управления маршрутизацией, механизм нотаризации, физическая или персональная защита, надежное аппаратное/программное обеспечение.

Ҳимоя механизмлари турлари - ҳимоя механизмларининг баъзи турлари - шифрлаш, калитларни маъмурий бошқариш жиҳатлари, рақамли имзо механизмлари, фойдаланишни бошқариш механизмлари, маълумотлар яхлитлиги механизмлари, аугентификация ахборотини алмашиш механизмлари, трафикни тўлдириш механизмлари, маршрутлашни бошқариш механизми, нотаризация механизми, физик ёки шахсий ҳимоя, ишончли аппарат (дастурий таъминот).

Types of protection mechanisms- some kinds of protection mechanisms are: encryption, key management aspects of administrative, digital signature mechanisms, access control mechanisms, mechanisms for data integrity, information exchange mechanisms authentication mechanisms fill traffic routing control mechanism, the mechanism of notarization, physical or personal protection, reliable hardware / software.

Вирус - небольшая программа, которая вставляет саму себя в другие программы при выполнении. еще - программа, способная самопроизвольно создавать свои копии и модифицирующая другие программы, записанные в файлах или системных областях, для последующего получения управления и воспроизводства новой копии.

Вирус - ўзини бошқа дастурлар бажарилаётганида уларга киритувчи унчалик катта бўлмаган дастур. Яна - нусхаларини беихтиёр яратиш ва кейинчалик янги нусхасини бошқариш ва қайта яратишга эришиш мақсадида файллардаги ва тизимли соҳалардаги бошқа дастурларни модификациялаш имкониятига эга дастур.

Virus - a small program that inserts itself into other programs when executed. Still - a program which can spontaneously create their copies and modifies other programs stored in files or system areas for subsequent management and reproduction of a new copy.

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

Юклама вирус - қаттиқ ва/ёки қайишқоқ дискларнинг юклама қисмини захарловчи вирус.

Boot virus - a virus that infects the boot of the hard and / or floppy disks.

Вирус невидимка - вирус, использующий специальные алгоритмы, маскирующие его присутствие на диске (в некоторых случаях в оперативной памяти).

Кўринмас вирус – дискда (баъзида асосий хотирада) эканлигини ниқобловчи махсус алгоритмдан фойдаланувчи вирус.

Stealth virus-a virus that uses special algorithms, masking its presence on the disk (in some cases in RAM).

Вирусы полиморфные (зашифрованные) — вирусы, предпринимающие специальные меры для затруднения их поиска и анализа. Не имеют сигнатур, то есть не содержат ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения.

Полиморф (шифрланган) вируслар - қидиришларини ва

тахлиллашларини қийинлаштириш учун махсус чораларни кўрувчи вируслар. Сигнатураларга эга эмаслар, яъни коднинг бирорта ҳам доимий қисмига эга эмаслар. Аксарият ҳолда битта полиморф вируснинг иккита намунаси бирорта ҳам мосликка эга бўлмайди.

Polymorphic viruses (encrypted) - viruses take special measures to obstruct their search and analysis. Do not have a signature, not contain any permanent part of the code. In most cases, two samples of the same polymorphic virus does not have any overlap.

Восстанавливаемость - свойство загружаемого модуля, состоящее в возможности защиты его в процессе выполнения от модификации как им самим, так и любым другим модулем. Программа восстановления может заменить такой модуль новым экземпляром, не повлияв при этом ни на порядок обработки, ни на конечный результат.

Тикланувчанлик – юкланувчи модулнинг бажарилиши жараёнида модификацияланишидан ўзи ёки ихтиёрий бошқа модул томонидан ҳимоялаш мумкинлиги ҳусусияти. Тиклаш дастури бундай модулни, ишлаш тартибига, якуний натижага таъсир этмасдан, янги нусха билан алмаштириши мумкин.

Recoverability (refreshable) – loadable module property of being able to protect it during the execution of the modification of both themselves and any other module. The recovery program can replace a module with a new instance, without affecting neither an order processing or the end result.

Вскрыватель паролей — программа компьютерная, которая осуществляет подбор или похищение паролей.

Паролларни фош қилувчи - паролларни танлашни ёки ўғрилашни амалга оширувчи компьютер дастури.

Password cracker - computer program that carries out the selection or stealing passwords.

Вторжение — доступ неправомочный или проникновение любого рода (физическое или информационное) в компьютеры, системы информационные и сети непосредственно или опосредованно через корреспондирующие сети или системы.

Бостириб кириш - ноқонуний фойдаланиш ёки компьютерга, ахборот тизими ва тармоғига бевосита ёки билвосита, тармоқ ёки тизим орқали ихтиёрий хил (физик ёки ахборот) кириш.

Intrusion - Unauthorized access or penetration of any kind (physical or informational) in computers, information systems and networks, or indirectly through offsetting network or system.

Вычислительная сеть (компьютерная сеть) - система взаимосвязанных между собой компьютеров, а также технического и программного обеспечения для их взаимодействия.

Ҳисоблаш тармоғи (компьютер тармоғи) – бир-бирлари билан ўзаро боғланган компъютерлар тизими, ҳамда уларнинг ўзаро харакатлари учун техник ва дастурий таъминот.

Area network (computer network) - a system of interconnected computers, as well as hardware and software for their interaction.

Гаммирование - процесс наложения по определенному закону гаммы шифра на открытые данные.

Гаммалаш – очиқ маълумотларга маълум қонуният бўйича гамма шифрини сингдириш жараёни.

Gamming - the process of applying for a specific law on the open range of the cipher data.

Гарантия защиты - наличие сертификата соответствия для технического средства обработки информации или аттестата на объект информатики, подтверждающих, что безопасность обрабатываемой информации соответ-

ствует требованиям стандартов и других нормативных документов.

Ҳимоянинг кафиллиги – ишланадиган ахборот хавфсизлигининг стандартлар ва бошқа меъёрий хужжатлар талабларига мослигини тасдиқловчи ахборотни ишловчи техник воситаларга мослик сертификатининг ёки информатика объектига аттестатнинг мавжудлиги.

Security accredidation - a certificate of conformity to the technical means of information processing or certificate for Informatics to confirming that the security of information processed complies with the standards and other normative documents.

Генератор - составная часть транслятора, выполняющая генерацию машинных команд.

Генератор – машиналар командаларини генерацияловчи трансляторнинг таркибий қисми.

Generator - part of the translator performs the generation of machine instructions.

Генератор ключей — техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

Калитлар генератори- калит (криптотизим калити), калит кетма-кетлиги, иницилизация векторлари ва ҳ. сифатида ишлатилувчи сон массивлари ёки бошқа маълумотларни ишлаб чиқаришга мўлжалланган техник қурилма ёки дастур.

Key generator- technical device or program designed to generate arrays of numbers or other data to be used as keys (cryptographic) key sequence, initialization vectors, and so on.

Генератор последовательностей псевдослучайных — техническое

устройство или программа для выработки последовательностей псевдослучайных.

Псевдотасодифий кетма-кетликлар генератори - псевдотасодифий кетма-кетликларни ишлаб чиқарувчи техник қурилма ёки дастур.

Pseudorandom generator - technical device or a program for generating pseudo-random sequences.

Генератор случайных паролей – программно - аппаратное средство, представляющее собой генератор случайных чисел, используемых в качестве паролей.

Тасодифий пароллар генератори - пароллар сифатида ишлатилувчи тасодифий сонлар генераторидан иборат дастурий-аппарат восита.

Randompassword generator – tools of software and hardware agent representing a random number generator to be used as passwords**.**

Генератор случайных чисел – программа или устройство, предназначенные для выработки последовательности псевдослучайных чисел по заданному закону распределения.

Тасодифий сонлар генератори - берилган тақсимланиш қонунияти бўйича псевдотасодифий кетма-кетликни шакллантириш учун мўлжалланган дастур ёки қурилма.

Random number generator - program or device designed to generate a sequence of pseudorandom numbers from a given distribution law.

Государственная тайна - сведения, охраняемые государством, разглашение которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для ее обороноспособности, государственной безопасности, экономических и политических интересов. К государственной тайне относится секретная информация с грифами «особой важности» и «со-

вершенно секретно».

Давлат сири - давлат томонидан муҳофаза қилинувчи, фош қилиниши давлатнинг ҳарбий-иқтисодий потенциалининг сифатий ҳолатига салбий таъсир этувчи ёки унинг мудофаа имконияти, давлат хавфсизлиги, иқтисодий ва сиёсий манфаатлари учун бошқа оғир оқибатларга олиб келиши мумкин бўлган маълумотлар. Давлат сирига "жуда муҳим" ва "мутлақо манфий" грифли ахборот тааллуқли.

State secret - information protected by the state, the disclosure of which could have a negative impact on the qualitative state of military-economic potential of the country or cause other serious consequences for its defense, national security, economic and political interests. To state secret is secret information classified "special importance" and "top secret".

Готовность системы - мера способности системы выполнять свои функции при нахождении в рабочем состоянии. Количественно готовность можно оценивать с помощью коэффициента готовности.

Тизимнинг тайёрлиги – тизимнинг ишлаш холатида ўз вазифаларини бажариш қобилиятининг ўлчови. Микдоран, тайёрликни тайёрлик коэффициенти ёрдамида баҳолаш мумкин.

System availability - measure the system's ability to perform its functions when in working condition. Readiness can be assessed quantitatively by the coefficient of readiness.

Данные - информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека либо автоматическими средствами.

Маълумотлар – одам иштироки билан ёки автоматик тарзда узатишга, изоҳлашга ёки ишлашга яроқли, формаллашган кўринишда ифодаланган ахборот.

Data - information presented in a formalized manner suitable for communi-

cation, interpretation or processing involving human or automated means.

Данные идентификационные — совокупность уникальных идентификационных данных, соответствующая конкретному участнику, позволяющая осуществить однозначную его идентификацию в системе.

Идентификация маълумотлари - тизимда бир маъноли идентификацияланишга имкон берувчи, муайян қатнашчига тегишли ноёб идентификация маълумотлари мажмуи.

Data identification - a set of unique identification data corresponding to a specific party, it allows an unambiguous identification of the system.

Дезинформация - сознательное искажение передаваемых сведений с целью ложного представления у лиц, использующих эти сведения; передача ложной информации.

Дезинформация – фойдаланувчи шахсларда ёлғон тасаввурни шакллантириш мақсадида уларга узатилувчи хабарни атайин бузиб кўрсатиш; ёлғон ахборотни узатиш.

Misinformation - deliberate distortion of transmitted data with the purpose of the false representations in individuals using this information; transmission of false information.

Длина (размер) ключа — длина слова в определённом алфавите, представляющего ключ. Длина ключа бинарного измеряется в битах.

Калит узунлиги (ўлчови) - калитни ифодаловчи маълум алфавитдаги сўз узунлиги. Иккили калит узунлиги битларда ўлчанади.

Key length - word length in a certain alphabet, representing the key. The key length is measured in binary bits.

Доверие — основа для уверенности в том, что продукт или система технологий информационных отвечают целям безопасности.

Ишонч - ахборот технологиялари маҳсулоти ёки тизимининг хавфсизлик мақсадларига жавоб беришига ишониш учун асос.

Assurance - basis for confidence that the product or system information technology meet the security objectives.

Доверительность - свойство соответствия безопасности некоторым критериям.

Ишончлилик – хавфсизликнинг қандайдир мезонларга мослик хусусияти.

Trusted funcionality – property according security with some critiries

Документ конфиденциальный —документ ограниченного доступа на любом носителе, содержащий информацию конфиденциальную.

Махфий ҳужжат - махфий ахборотли ихтиёрий элтувчидан фойдаланиш чекланган ҳужжат

Confidential document - document restricted in any medium, containing confidential information.

Документированная информация — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Ҳужжатланган ахборот - реквизитлари идентификацияланишига имкон берувчи, материал элтувчида қайдланган ахборот

Documented information - fixed in a tangible medium with requisites allowing its identification.

Домен безопасности - ограниченная группа объектов и субъектов безопасности, к которым применяется одна методика безопасности со стороны одного и того же администратора безопасности.

Хавфсизлик домени – хавфсизликнинг битта маъмури томонидан

хавфсизликнинг бир хил усули қўлланиладиган хавфсизлик субъектлари ва объектларининг чекланган гурухи.

Secyrity domain - limited group of objects and subjects of security, to which the one method of security from the same security administrator.

Достоверность - свойство информации быть правильно воспринятой; вероятность отсутствия ошибок.

Ишончлилик – ахборотниниг тўғри ўзлаштирилиш хусусияти; хатолик йўқлигининг эҳтимоллиги.

Validity - property information to be correctly perceived; the probability of no errors.

Доступ - предоставление данных системе обработки данных или получение их из нее путем выполнения операций поиска, чтения и (или) записи данных.

Фойдаланиш - маълумотларни ишлаш тизимига маълумотларни тақдим этиш ёки ундан қидириш, ўқиш ва/ёки ёзиш амалларини бажариш йўли билан маълумотларни олиш.

Access - providing data processing system or getting them out of it by doing a search, read and (or) data record.

Доступ к информации - процесс ознакомления с информацией, ее документирование, модификация или уничтожение, осуществляемые с использованием штатных технических средств.

Ахборотдан фойдаланиш – штатга оид техник воситалардан фойдаланиб ахборот билан танишиш, уни хужжатлаш, нусхалаш, модификациялаш ёки йўқ қилиш жараёни.

Access to information - the process of reviewing the information, documenting, modification or destruction, implemented by the staff of technical means. still - familiar with the information, information processing, in particular, copying,

modification or destruction of information.

Доступ к конфиденциальной информации — санкционированное полномочным должностным лицом ознакомление конкретного лица с информацией, содержащей сведения конфиденциального характера.

Конфиденциаль ахборотдан фойдаланиш - муайян шахсга таркибида конфиденциаль характерли маълумот бўлган ахборот билан танишишга ваколатли мансабдор шахснинг рухсати

Access to confidential information - authorized official introduction of a particular person with the information containing confidential information.

Доступ несанкционированный к информации — получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Ахборотдан рухсатсиз фойдаланиш - манфаатдор субъект томонидан ўрнатилган ҳуқуқий ҳужжатларни ёки мулкдор, ахборот эгаси томонидан ҳимояланувчи ахборотдан фойдаланиш ҳуқуқлари ёки қоидаларини бузиб ҳимояланувчи ахборотга эга бўлиши.

Unauthorized access to information - preparation of protected information interested entity in violation of the legal instruments or by the owner, the owner of the information or rights of access to protected information.

Доступ ограниченный — доступ к ресурсу информационному, разрешаемый установленными для данного ресурса правилами доступа только определенному кругу лиц, обладающих соответствующими полномочиями.

Чекланган фойдаланиш - ахборот ресурсидан, ушбу ресурсга фақат мос ваколатларга эга шахсларнинг маълум доирасига ўрнатилган фойдаланиш қоидалари бўйича рухсатли фойдаланиш.

Restricted access - access to the resources of the information allowed by the established rules for the resource access only certain persons with appropriate authority.

Доступность — свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Фойдалувчанлик - авторизацияланган мантиқий обьект сўрови бўйича мантиқий объектнинг тайёрлик ва фойдаланувчанлик ҳолатида бўлиши хусусияти

Availability - property of an object in a state of readiness and usage upon request authorized entity.

Живучесть - свойство системы оставаться работоспособной в условиях внешних воздействий.

Яшовчанлик – тизимнинг ташқи таъсирлар шароитида ишга лаёқатли қолиши хусусияти.

Viability - property of the system to remain operational under external influences.

Журнал восстановления - журнал, обеспечивающий возможность восстановления базы данных или файла. Содержит информацию о всех изменениях в Б.Д. (файле) с того момента, когда было установлено, что данные достоверны и была сделана последняя резервная копия.

Тиклаш журнали –маълумотлар базаси ёки файлни тиклаш имкониятини таъминловчи журнал. Унда маълумотлар базасидаги (файлдаги) маълумотларнинг хақиқийлиги аниқланган ва охирги резерв нусха олинган ондан бошлаб, барча ўзгаришлар хусусида ахборот мавжуд.

Recovery log - magazine, providing the ability to restore a database or file. Contains information about all the changes in DB (file) from the moment when it was found that the data is reliable and has been made the last backup.

Заверение - регистрация данных у доверенного третьего лица для дальнейшей уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Ишонтириш – мазмуни, маълумотлар манбаи, етказиш вақти каби характеристикаларнинг тўғрилигига бундан буён ишониш учун маълумотларни ишончли учинчи шахсда қайдлаш.

Notalization - registration data from a trusted third party for further confidence in the correctness of such properties as the source of data, the time of delivery.

Заполнение трафика — генерация фиктивных сеансов обмена данными, фиктивных блоков данных и/или фиктивных данных в составе блоков данных.

Трафикни тўлдириш – маълумотлар алмашишнинг сохта сеансларини, маълумотларнинг сохта блокларини ва/ёки маълумотлар блоклари таркибида сохта маълумотларни генерациялаш.

Filling traffic - generate dummy data exchange session, dummy data units and / or the dummy data comprising data blocks.

Запрос идентификации - запрос, заданный ведущей станцией ведомой станции для ее идентификации или определения ее состояния.

Идентификация сўрови – бошқарувчи станциянинг бошқарилувчи станцияга уни идентификациялаш ёки холатини аниқлаш учун берган сўрови.

request identification - query specified slave master station to identify it or determine its status.

Заражение - в вычислительной технике процесс создания вирусом своей копии, связанный с изменением кодов программ, системных областей или

системных таблиц.

Захарлаш – ҳисоблаш техникасида вируснинг дастур, тизимли зона ёки тизимли жадвалларнинг ўзгариши билан боғлиқ ўзининг нусхасини яратиш жараёни.

Infection - in computing the process of creating copies of its virus associated with changes in program codes, system areas or system tables.

Зарегистрированный пользователь - пользователь, имеющий приоритетный номер в данной системе коллективного пользования.

Руйхатга олинган фойдаланувчи – берилган коллектив фойдаланувчи тизимда устувор номерли фойдаланувчи.

Authorized user - a user with a priority number in the system of collective use.

Защита - средство для ограничения доступа или использования всей или части вычислительной системы; юридические, организационные и технические, в том числе программные, меры предотвращения несанкционированного доступа к аппаратуре, программам и данным.

Ҳимоялаш - ҳисоблаш тизимидан ёки унинг қисмидан фойдаланишни чеклаш воситаси; аппаратурадан, дастурдан ва маълумотлардан рухсатсиз фойдаланишни бартараф этувчи ташкилий ва техник, жумладан, дастурий чоралар.

Protection, security, lock out - means for restriction of access or use of all or part of the computing system; legal, organizational and technical, including program, measures of prevention of unauthorized access to the equipment, programs and data.

Защита антивирусная — комплекс организационных, правовых, технических и технологических мер, применяемых для обеспечения защиты средств вычислительной техники и системы автоматизированной от

воздействия вирусов программных.

Вирусга қарши ҳимоя - ҳисоблаш техникаси ва автоматлаштирилган тизим воситаларини дастурий вирус таъсиридан ҳимоялашни таъминлашда ишлатилувчи ташкилий, хуқуқий, техник ва технологик чоралар комплекси.

Protection anti-virus — the complex of the organizational, legal, technical and technological measures applied to ensuring protection of computer aids and system of automated from influence of viruses program.

Защита информации - включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности. На практике под этим понимается поддержание целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

Ахборотни ҳимоялаш –ахборот хавфсизлигини таъминлашга йўналтирилган тадбирлар комплекси. Амалда ахборотни ҳимоялаш деганда маълумотларни киритиш, сақлаш, ишлаш ва узатишда унинг яхлитлигини, фойдаланувчанлигини ва, агар керак бўлса, ахборот ва ресурсларнинг конфиденциаллигини мададлаш тушунилади.

Information protection - includes a complex of the actions aimed at providing information security. In practice is understood as maintenance of integrity, availability and if it is necessary, confidentiality of information and the resources used for input, storage, and processing and data transmission.

Защита информации криптографическая — защита информации с помощью ее криптографического преобразования.

Ахборотни криптографик ҳимоялаш - ахборотни криптографик ўзгартириш ёрдамида ҳимоялаш.

Cryptographic protection of information - information security by means of its cryptographic transformation.

Защита информации организационная — защита информации, осуществляемая путем принятия административных мер.

Ахборотни ташкилий ҳимоялаш- маъмурий чораларни қўллаш йўли билан амалга оширилувчи ахборот ҳимояси.

Information security organizational — the Information security which is carried out by acceptance of administrative measures.

Защита информации от разглашения — защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Ахборотни фош қилинишдан ҳимоялаш - ҳимояланувчи ахборотни, ушбу ахборотдан фойдаланиш хуқуқига эга бўлмаган манфаатдор субектларга (истеъмолчиларга) рухсатсиз етказишни бартараф этишга йўналтирилган ахборот ҳимояси.

Information security from disclosure — the information security directed on prevention of unauthorized finishing of protected information to interested subjects (consumers), not having right of access to this information.

Защита информации от технических разведок - деятельность, направленная на предотвращение или существенное снижение возможностей технических разведок по получению разведывательной информации путем разработки и реализации системы защиты.

Ахборотни техник разведкадан ҳимоялаш – ҳимоялаш тизимини ишлаб чикиш ва амалга ошириш йўли билан техник разведканинг ахборот олиш имкониятларини бартараф қилишга ёки жиддий камайтиришга йўналтирилган фаолият.

Information security from technical investigations - the activity directed on prevention or essential decrease in opportunities of technical investigations on obtaining prospecting information by development and realization of system of

protection.

Защита информации от утечки — защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами.

Ахборотни сирқиб чикишидан ҳимоялаш - ҳимояланувчи ахборотнинг фош қилиниши ва ундан рухсатсиз фойдаланиш натижасида, назоратсиз тарқалишини бартараф этишга, ҳамда (ажнабий) разведка ва бошқа манфаатдор субъектлар томонидан ўзлаштирилишини истисно қилишга (қийинлаштиришга) йўналтирилган ахборот ҳимояси.

Information security from leak — the information security directed on prevention of uncontrollable distribution of protected information as a result of its disclosure and unauthorized access to it, and also on an exception (difficulty) of obtaining protected information (foreign) investigations and other interested subjects.

Защита от несанкционированного доступа - предотвращение или существенное затруднение несанкционированного доступа к программам и данным путем использования аппаратных, программных и криптографических методов и средств защиты, а также проведение организационных мероприятий. Наиболее распространенным программным методом защиты является система паролей.

Рухсатсиз фойдаланишдан ҳимоялаш – аппарат-дастурий ва криптографик усуллар ва воситалар ёрдамида, ҳамда ташкилий тадбирларни ўтказиб дастурлардан ва маълумотлардан рухсатсиз фойдаланишни бартараф этиш ёки жиддий қийинлаштириш. Ҳимоялишнинг энг кенг тарқалган дастурий усули пароллар тизими ҳисобланади.

Protection from unauthorized access - prevention or essential difficulty of unauthorized access to programs and this way of use of hardware, program and cryptographic methods and means of protection, and also carrying out organizational actions. The most widespread program method of protection is the system of passwords.

Злоумышленник - лицо или организация, заинтересованные в получении несанкционированного доступа к программам или данным, предпринимающие попытку такого доступа или совершившие его.

Нияти бузуқ – дастурлардан ёки маълумотлардан рухсатсиз фойдаланишдан манфаатдор, бундай фойдаланишга уринган ёки амалга оширган шахс ёки ташкилот.

Intruder - the person or the organization interested in receiving unauthorized access to programs or data, making an attempt of such access or made it.

Идентификатор - средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

Идентификатор – субъект ёки объектнинг фарқланувчи аломатидан иборат фойдаланишнинг идентификация воситаси. Фойдаланувчилар учун асосий идентификация воситаси парол ҳисобланади.

Identifier - means of identification of the access, representing a distinctive sign of the subject or object of access. The main means of identification of access for users is the password.

Идентификатор доступа- уникальный признак субъекта или объекта доступа.

Фойдаланиш идентификатори – фойдаланувчи субъект ёки объектнинг ноёб аломати.

Access identifier - unique sign of the subject or object of access.

Идентификатор пользователя– символическое имя, присваиваемое отдельному лицу или группе лиц и разрешающее использование ресурсов вычислительной системы.

Фойдаланувчи идентификатори – ҳисоблаш тизими ресурсларидан фойдаланиш учун алоҳида шахсга ёки шахслар гурухига бериладиган рамзий исм.

User identifier, userid – symbol the check name appropriated to the individual or a group of persons and allowing use of resources of the computing system.

Идентификация- присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Идентификация – фойдаланиш субъектлари ва обектларига идентификатор бериш ва/ёки тақдим этилган идентификаторни берилганлари рўйҳати билан таққослаш.

Identification -assignment to subjects and objects of access of the identifier and/or comparison of the shown identifier with the list of the appropriated identifiers.

Избирательное управление доступом- метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит.

Фойдаланишни танлаб бошқариш – фойдаланувчини, жараённи ва/ёки у тегишли гуруҳни идентификациялашга ва танишга асосланган тизим субъектларининг объектлардан фойдаланишни бошқариш усули.

Discretionary access control (DAC) - method of control over access of subjects of system to. To the objects, based on identification and an identification of the user, process and/or group to which it belongs.

Имитация — атака активная на протокол криптографический, целью которой является навязывание противником и/или нарушителем одной из сторон сообщения от имени другой стороны, которое не будет отвергнуто при приеме.

Имитация –қабул қилинишида рад этилмайдиган, душман ва/ёки бузғунчи томонидан тарафларнинг бири хабарини тарафларнинг иккинчиси номидан мажбуран қабул қилдириш мақсадида криптографик протоколга фаол хужум.

Imitation — attack active on the protocol cryptographic which purpose is imposing by the opponent and/or the violator of one of the message parties on behalf of other party which won't be rejected at reception.

Имитовставка - отрезок информации фиксированной длины, полученный по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Имитовставка – Имитоҳимояни таъминлаш мақсадида очиқ маълумотлардан ва калитдан маълум қоида бўйича олинган ва шифрланган маълумотларга қўшилган ахборотнинг белгиланган узунликдаги бўлаги.

Massage authentication code - piece of information of the fixed length, received by a certain rule from open data and a key and added to the ciphered data for providing imitation protection.

Имитозащита - защита системы шифрованной связи от навязывания ложных данных.

Имитоҳимоя – шифрланган алоқа тизимини ёлғон маълумотларнинг мажбуран киритилишидан ҳимоялаш.

Integrity protection, protection from imitation - protection of system of encoded communication against imposing of false data.

Имитостойкость — свойство системы криптографической (протокола криптографического), характеризующее способность противостоять атакам активным со стороны противника и/или нарушителя, целью которых является навязывание ложного сообщения, подмена передаваемого сообщения или изменение хранимых данных.

Имитобардошлик – криптографик мақсади ёлғон хабарни мажбуран киритиш, узатилувчи хабарни алмаштириш ёки сақланувчи маълумотларни ўзгартириш бўлган душман ёки/ва бузғунчи томонидан қилинадиган фаол хужумларга қарши тура олиш қобилияти орқали характерланувчи хусусияти.

imitation resistance — property of system cryptographic (the protocol cryptographic), characterizing ability to resist to attacks active from the opponent and/or the violator which purpose is imposing of the untrue report, substitution of the transferred message or change of stored data.

Инженерия социальная — обход системы информационной безопасности с помощью информации, получаемой из контактов с обслуживающим персоналом и пользователям путем введения их в заблуждение различными уловками, обмана и т.д.

Ижтимоий инженерия – хизматчи ходимлар ва фойдаланувчилар билан мулоқотда турли найранглар ва алдашлар йўли билан олинган ахборотдан фойдаланиб ахборот хавфсизлиги тизимини четлаб ўтиш.

Social engeneering — round system of information security with using information obtained from contacts with serves staff and users by introducing them in delusion different tricks, deception, etc.

Инсайдер — член группы людей, имеющей доступ к закрытой информации, принадлежащей этой группе. Как правило, является ключевым персонажем в инциденте, связанным с утечкой информации. С этой точки зрения различают следующие типы инсайдеров: халатные, манипулируеммые, обиженные, нелояльные, подрабатывающие, внедренные

и т.п.

Инсайдер – гурухга тегишли яширин ахборотдан фойдаланиш хуқуқига эга гурух аъзоси. Одатда, ахборот сирқиб чиқиш билан боғлиқ можарода муҳим шахс ҳисобланади.Шу нуқтаи назардан инсайдерларнинг қуйидаги хиллари фарқланади: бепарволар: манипуляцияланувчилар, ранжиганлар, қўшимча пул ишловчилар ва х.

Insider — the member of group of the people having access to the classified information, belonging this group. As a rule, is the key character in the incident, connected with information leakage. From this point of view distinguish the following types of insiders: negligent, manipulated, offended, disloyal, earning additionally, introduced, etc.

Информационная надежность–1.способность алгоритма или программы правильно выполнять свои функции при различных ошибках в исходных данных. 2.способность информационной системы обеспечивать целостность хранящихся вней данных.

Ахборот ишончлилиги – 1. дастлабки маълумотлардаги турли хатоликларда алгоритм ёки дастурнинг ўз вазифасини тўғри бажариш қобилияти. 2. ахборот тизимининг унда сақланаётган маълумотлар яхлитлигини таъминлаш қобилияти.

Information reliability –1.Abilityofalgorithm or the program it is correct to carry out the functions at various mistakes in basic data. 2. Ability of information system to provide integrity of the data which were stored in it.

Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Ахборот тизими – хужжатларнинг (хужжатлар массивининг) ва ахборот технологияларини, хусусан ахборот жараёнларини амалга оширувчи

хисоблаш техникаси ва алоқа воситаларидан фойдаланиб ташкилий тартибга солинган мажмуи.

Information system - organizationally ordered set of documents (document files) and information technologies, including with use of computer aids and the communications, realizing information processes.

Информационная технология - система технических средств и способов обработки информации.

Ахборот технологияси – ахборотни ишлаш усуллари ва техник воситалари тизими.

Information technology - system of technical means and ways of information processing.

Инфраструктура ключей открытых — подсистема системы ключевой шифрсистемы асимметричной. Предназначена для обеспечения (с помощью сертификатов ключей) доверия пользователей законных к подлинности ключей, соответствия ключей пользователям и оговоренным условиям их применения.

Очиқ калитлар инфраструктураси –асимметрик шифртизим калитлари тизимининг қисмтизими. Қонуний фойдаланувчиларнинг калитларнинг хақиқийлигига, калитларнинг фойдаланувчиларга ва улар олдиндан келишилган ишлатиш шартларига мослигига ишонишларини (калитлар сертификатлари ёрдамида) таъминлашга мўлжалланган.

Public Key Infrastructure (PKI) — subsystem of system key cipher system of asymmetric. It is intended for providing (by means of certificates of keys) trust of users of lawful keys to authenticity, compliance of keys to users and the stipulated conditions of their application.

Инцидент — зафиксированный случай попытки получения несанкционированного доступа или проведения атаки на компьютерную

систему.

Можаро – рухсатсиз фойдаланиш хуқуқига эга бўлишга ёки компъютер тизимига хужум ўтказишга уринишнинг қайд этилган холи.

Incident— the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.

Искажение - отклонение значений параметров сигнала данных от установленных требований.еще - изменение содержимого сообщения, передаваемого по линии связи.

Бузилиш – маълумотлар сигнали параметрлари қийматларининг ўрнатилган талаблардан четланиши. Яна -алоқа линияси бўйича узатилувчи хабар таркибининг ўзгариши.

Distortion - deviation of values of parameters of a signal of data from the established requirements. Still - change of contents of the message transferred on the communication lines.

Канал передачи данных — физическая среда, по которой передается информация из одного устройства в другое.

Маълумотларни узатувчи канал - физик муҳит, у орқали ахборот бир қурилмадан иккинчисига узатилади.

Data transmission channel — the physical environment on which information from one device is transferred to another.

Канал проникновения — физический путь от злоумышленника к источнику конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

Кириб олиш канали - нияти бузуқдан то конфиденциаль ахборот манбаигача бўлган йўл. У орқали ҳимояланувчи маълумотлардан рухсатсиз фойдаланиш мумкин.

Insecurity channel — actual path from the malefactor to a source of

confidential information by means of which unauthorized access to protected data is possible.

Канал утечки информации — физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможно несанкционированное получение охраняемых сведений (совокупность источника коммерческой тайны, физической среды и средства промышленного шпионажа).

Ахборот сирқиб чиқарувчи канал - кўрикланувчи маълумотлардан (тижорат сири, физик муҳит ва саноат айғоқчилик воситалари мажмуи) рухсатсиз фойдаланишга имкон берувчи конфиденциаль ахборот манбаидан то нияти бузуқгача бўлган физик йўл.

Information leakage channel — actual path from a source of confidential information to the malefactor, on which probably unauthorized obtaining protected data (set of a source of a trade secret, the physical environment and means of industrial espionage).

Киберпреступность — действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информации в корыстных или хулиганских целях.

Кибержиноятилик - ғаразли ёки хулиганлик мақсадларда ҳимоялашнинг компьютер тизимларини бузиб очишга, ахборотни ўғрилашга ёки бузишга йўналтирилган алоҳида шахсларнинг ёки гуруҳнинг ҳаракатлари.

Cyber cryme — actions of individuals or the groups, directed on breaking of systems of computer protection, on plunder or information destruction in the mercenary or hooligan purposes.

Кибертерроризм — действия по дезорганизации компьютерных систем, создающие опасность гибели людей, значительного имущественного

ущерба либо иных общественно опасных последствий.

Кибертерроризм - инсонлар ҳалокати, айтарлича моддий зарар хавфини ва бошқа жамиятга хавфли оқибатларни туғдирувчи компьютер тизимларини чалғитиш бўйича ҳаракатлар.

Cyber terrorism — actions on disorganization of the computer systems creating danger of death of people, significant property damage or other socially dangerous consequences.

Ключ открытый — несекретный ключ шифрсистемы асимметричной.

Очиқ калит –ассиметрик шифртизимнинг махфий бўлмаган калити.

Public key — unclassified key the asymmetric cryptosystem.

Ключ разовый — ключ, однократно используемый для шифрования в цикле (жизненном ключей). Обычно не подлежит хранению и является элементом ключа составного.

Бир мартали калит - циклда (калитларнинг ҳаёт циклида) шифрлаш учун бир марта ишлатилувчи калит. Одатда сақланмайдиган ва таркибий калит элементи ҳисобланади.

Once-only key — the key which is once used for enciphering in a cycle (vital keys). Usually isn't subject to storage and is an element of a key compound.

Ключ расшифрования — ключ, используемый при расшифровании.

Дешифрлаш калити - дешифрлашда ишлатилувчи калит.

Decryption key — the key used for decryption.

Ключ сеансовый — ключ, специально сгенерированный для одного сеанса связи между двумя участниками (протокола).

Сеанс калити - иккита қатнашчилар (протокол қатнашчилари) орасидаги битта алоқа сеанси учун махсус генерацияланган калит.

Session key — the key which has been specially generated for one

communication session between two participants (protocol).

Ключ секретный — ключ, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной шифрсистемы симметричной или к использованию некоторых функций данной шифрсистемы асимметричной.

Махфий калит - маълум симметрик шифртизим калитларидан ёки маълум асимметрик шифртизимнинг баъзи функцияларидан фойдаланиш ҳуқуқига эга бўлмаган шахслардан махфий саналувчи калит.

Secret key — the key kept in a secret from persons, not having the admission to keys given symmetric cryptosystem or to use of some functions given the asymmetric cryptosystem.

Код – 1. Представление символа двоичным кодом. 2. Криптографический прием, в котором используется произвольная таблица или кодировочная книга для преобразования текста в закодированную форму.

Код - 1. Символни иккилик код орқали ифодалаш. 2. Матнни кодланган шаклга ўзгартиришда ихтиёрий жадвалдан ёки кодлаш китобидан фойдаланувчи криптографик усул.

Code -1.Symbol representation by a binary code. 2. Cryptographic reception in which any table or the quoted book for transformation of the text to the coded form is used.

Код аутентификации — вид алгоритма кодирования имитозащищающего информации. Как правило, к. а. сопоставляет сообщению его код аутентичности сообщения. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения.

Аутентификация коди – ахборотни имитоҳимояловчи кодлаш алгоритмининг тури. Одатда, аутентификация коди хабарни унинг аслига тўғри коди билан таққослайди. Ахборотнинг ҳақиқийлиги хусусида қарор қабул қилиш алгоритми хабарнинг аслига тўғри коди қийматини текширишга

асосланган.

Authentication code — type of algorithm of coding imitation secure information. As a rule, authentication code compares to the message its code of authenticity of the message. The algorithm of decision-making on authenticity of information is based on check of value of a code of authenticity of the message.

Код аутентичности сообщения — в протоколах аутентификации сообщений с доверяющими друг другу участниками — специальный набор символов, добавляемый к сообщению и предназначенный для обеспечения его целостности и аутентификации источника данных.

Хабарнинг аслига тўғрилиги коди - бир-бирига ишонувчи иштирокчилар томонидан хабарларни аутентификациялаш протоколларида хабарга қўшиладиган ва унинг яхлитлигини ва маълумотлар манбаининг аутентификациясини таъминлашга мўлжалланган символларнинг махсус набори.

Message authentication code, seal, integrity check value — in protocols of authentication of messages with participants trusting each other — the special character set added to the message and intended for ensuring its integrity and authentication of data source.

Компрометация - утеря критичной информации либо получение ее неавторизованными для этого субъектами (лицами, программами, процессами и т.д.)

Обрўсизлантириш –жиддий ахборотни йўқотиш ёки уни авторизацияланмаган субъектлар (шахслар, дастурлар жараёнлар ва ҳ.) томонидан ўзлаштирилиши.

Compromising - loss of critical information or receiving it the subjects not authorized for this purpose (persons, programs, processes, etc.)

Контроль доступа - определение и ограничение доступа пользовате

лей, программ или процессов к устройствам, программам и данным вычислительной системы.

Фойдаланиш назорати –фойдаланувчиларнинг, дастурларнинг ёки жараёнларнинг ҳисоблаш тизимлари қурилмаларидан, дастурларидан ва маълумотларидан фойдаланишларини аниқлаш ва чеклаш.

Access control - definition and restriction of access of users, programs or processes to devices, programs and data of the computing system.

Концепция защиты информации - система взглядов и общих технических требований по защите информации.

Ахборотни ҳимоялаш концепцияси –ахборотни ҳимоялаш бўйича қарашлар ва умумий техник талаблар тизими.

The concept of information security - frame of reference and the general technical requirements on information security.

Криптографическая система - совокупность технических и /или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

Криптографик тизим –ахборотни криптографик ўзгартиришни ва калитларни тақсимлаш жараёнини бошқаришни таъминловчи техник ва/ёки дастурий воситалар, ташкилий усуллар мажмуи

Cryptographic system, Cryptosystem - set technical and/or software, the organizational methods providing cryptographic transformation of information and management process of distribution of keys.

Лицензия - разрешение на право продажи или предоставления услуг.

Лицензия –сотиш ёки хизмат кўрсатиш ҳуқуқига рухсатнома.

License - permission to the right of sale or service.

Лицензия в области защиты информации - разрешение на право проведения тех или иных работ в области защиты информации, оформленное лицензионным соглашением /договором/.

Ахборот ҳимояси соҳасидаги лицензия –ахборот хавфсизлиги соҳасида у ёки бу ишларни бажариш ҳуқуқига лицензион битим (шартнома) билан расмийлаштирилган рухсатнома.

License information security - permission to the right of carrying out these or those works in the field of the information security, issued by the license agreement/contract/.

Ложная информация - информация, ошибочно отражающая характеристики и признаки, а также информация о не существующем реальном объекте.

Ёлғон ахборот –характеристикаларни ва аломатларни нотўғри акслантирувчи ахборот ҳамда реал мавжуд бўлмаган объект ҳусусидаги ахборот.

False information - information which is mistakenly reflecting characteristics and signs, and also information on object not existing really.

Макровирусы — программы на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и так далее).

Макровируслар - қандайдир маълумотларни ишлаш тизимига (матн редакторига, электрон жадвалларга ва ҳ.) ўрнатилган тиллардаги (макротиллардаги) дастурлар.

Macro viruses — programs in the languages (macrolanguages) which have been built in some systems of data processing (text editors, spreadsheets and so on).

Мандат - разновидность указателя, определяющего путь доступа к

объекту и разрешенные над ним операции.

Мандат – объектдан фойдаланиш ва унинг устида рухсат этилган амалларни бажариш йўлини аниқловчи кўрсаткич тури.

Mandate - kind of the index defining a way of access to object and operations allowed over it.

Мандатное управление доступом - концепция (модель) доступа субъектов к информационным ресурсам по грифу секретности, разрешенной к пользованию информации, определяемому меткой секретности /конфиденциальности/.

Фойдаланишни мандатли бошқариш –- махфийлик (конфиденциаллик) белгиси орқали аниқланувчи махфийлик грифи буйича ахборотдан фойдаланишга рухсат этилган субъектларнинг ахборот ресурсларидан фойдаланиш концепцияси (модели).

Mandate management access - the concept (model) of access of subjects to information resources on the security classification of information allowed for using determined by a tag of privacy/confidentiality/.

Маскарад - попытка получить доступ к системе, объекту или выполнение других действий субъектом, не обладающим полномочиями на соответствующее действие и выдающим себя за другого, которому эти действия разрешены.

Маскарад – тегишли ҳаракатларни амалга оширишга ваколатлари бўлмаган субьектнинг ўзини бошқа ваколатли шахс деб кўрсатиб, у шахс номидан ҳаракатларнинг имкониятларига ва имтиёзларига эга бўлишга уриниши.

Masquerade - attempt to get access to system, object or performance of other actions by the subject which isn't possessing powers on the corresponding action and giving out for another to which these actions are allowed.

Матрица доступа - таблица, отображающая правила доступа субъектов к информационным ресурсам, данные о которых хранятся в диспетчере доступа. Еще- таблица, отображающая правила разграничения доступа.

Фойдаланиш матрицаси – хусусидаги маълумотлар фойдаланиш диспетчерида сақланувчи ахборот, ахборот ресурсларидан субъектларнинг фойдаланиш қоидаларини акс эттирувчи жадвал; Яна - фойдаланишни чеклаш қоидаларини акс эттирувчи жадвал.

Access matrix – the table displaying rules of access of subjects to information resources, given about which are stored in the dispatcher of access. Also, the table displaying rules of differentiation of access.

Матрица полномочий - таблица, элементы которой определяют права (полномочия, привилегии) определенного объекта относительно защищаемых данных.

Ваколатлар матрицаси –элементлари муайян объектнинг ҳимояланувчи маълумотларга нисбатан ҳуқуқларини (ваколатларини, имтиёзларини) белгиловчи жадвал.

Privilege matrix - the table, which elements define the rights (powers, privileges) a certain object from nositelno protected data.

Менеджмент риска — полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

Хавф-хатар менеджменти — ахборот-телекоммуникация технология ресурсларига таъсир этиши мумкин булган хавфли ходисалар окибатларини идентификациялашнинг, назоратлашнинг, бартараф этишнинг ёки камайтиришнинг тўлик жараёни.

Risk management — full process of identification, control, elimination or reduction of consequences of dangerous events which can have impact on re-

sources of information and telecommunication technologies.

Модель нарушителя правил доступа - абстрактное описание нарушителя правил доступа к информационному ресурсу. Примерами моделей нарушителя правил доступа являются такие программы как троянский конь, логическая бомба, компьютерный вирус и другие.

Фойдаланиш қоидаларини бузувчининг модели – ахборот ресурсидан фойдаланиш қоидаларини бузувчининг абстракт тавсифи. Ахборот ресурсидан фойдаланиш қоидаларини бузувчининг модели сифатида троян дастурини, мантиқий бомбани, компьютер вирусини ва ҳ. кўрсатиш мумкин.

Model intruder access rules - abstract the description of the breaker of rules of access to information resource. Examples of models of the breaker of rules of access are such programs as the Trojan horse, a logical bomb, a computer virus and others.

Модификация информации - изменение содержания или объема информации на ее носителях при обработке техническими средствами.

Ахборотни модификациялаш – ахборотни техник воситаларида ишлашда унинг мазмунини ёки хажмини ўзгартириш.

Modification of information - to change the content or the amount of information on the processing of technical means.

Мониторинг безопасности информации — постоянное наблюдение за процессом обеспечения безопасности информации в системе информационной с целью установить его соответствие требованиям безопасности информации.

Ахборот хавфсизлиги мониторинги - ахборот хавфсизлиги талабларига мослигини аниқлаш мақсадида ахборот тизимидаги ахборот хавфсизлигини таъминлаш жараёнини муттасил кузатиш.

Information security monitoring - constant monitoring of the process information security in the system information to determine its compliance with information security.

Наблюдаемость - возможность для ответственных за защиту информации лиц восстанавливать ход нарушения или попытки нарушения безопасности информационной системы.

Кузатувчанлик - ахборотни ҳимоясига жавобгар шахслар учун ахборот тизими хавфсизлигини бузиш жараёнини ёки бузишга уринишларни тиклаш имконияти.

Observability - an opportunity for those responsible for data protection officials to restore the course of violations or attempted violations of information system security.

Надежность - характеристика способности функционального узла, устройства, системы выполнять при определенных условиях требуемые функции в течение определенного периода времени.

Ишончлилик–берилган вақт оралиғида функциональ узелнинг, қурилманинг, тизимнинг маълум шароитларда ўзига топширилган вазифаларни бажариш қобилиятининг характеристикаси.

Reliability - the ability of the functional characteristics of node devices, the system under certain circumstances to carry out the desired function during a certain period of time.

Нападающий — субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Хужумчи - ҳаракати кўрилаётган компьютер тизимида ахборот хавфсизлигини бузадиган субъект.

Attacker - a subject whose actions violate the information security in a under consideration computer system.

Нарушение полномочий - попытка пользователя или программы выполнить неразрешенную операцию.

Ваколатларнинг бузилиши –фойдаланувчининг ёки дастурнинг рухсат этилмаган амални бажаришга уриниши.

Privilege violation - user or program attempts to perform an unauthorized operation.

Нарушение системы безопасности — успешное поражение средства управления безопасностью, которое завершается проникновением в систему.

Хавфсизлик тизимининг бузилиши - тизимга суқилиб кириш билан тугалланадиган хавфсизликни бошқариш воситаларининг шикастланиши.

Security system violation - the successful defeat security controls, which concludes with penetration into the system.

Нарушение целостности - искажение содержимого записей файла или базы данных. Происходит вследствие машинных сбоев, программных ошибок, а также ошибочных действий пользователей.

Яхлитликнинг бузилиши - файл ёки маълумотлар базасидаги ёзувларнинг бузилиши. Машинанинг янглишиши, дастурий хатоликлар ҳамда фойдаланувчиларнинг нотўғри ҳаракатлари натижасида рўй беради.

Integrity violation - the distortion of the contents of the recorded files or database. Thid is due to machine failures, software errors and erroneous actions of users.

Нарушение целостности информации - утрата информации, при ее обработке техническими средствами, свойства целостности в результате ее несанкционированной модификации или несанкционированного уничтожения.

Ахборот яхлитлигининг бузилиши –ахборотнинг, уни техник

воситалари ёрдамида ишланишида йўқотилиши? рухсатсиз модификацияланиши ёки йўқ қилиниши натижасида яхлитлик хусусиятининг йўқолиши.

Information integrity violation - the loss of information when it is processed by technical means, the integrity of the property as a result of its unauthorized modification or unauthorized destruction.

Нарушитель - субъект, действия которого нарушают безопасность информации в рассматриваемой компьютерной системе.

Бузғунчи – ҳаракатлари кўрилаётган компьютер тизимида ахборот хавфсизлигини бузадиган субъект.

Attacker - a subject whose actions violate the information security in a computer system under consideration.

Обработка данных - систематическое выполнение операций над данными.

Маълумотларни ишлаш – маълумотлар устида амалларнинг мунтазам бажарилиши.

Data processing - manipulation of data by a computer.

Ошибка в данных - ошибочное представление одного или нескольких исходных данных может стать причиной аварийного завершения программы либо оказаться необнаруженной, но результаты нормально завершившейся программы будут при этом неверными.

Маълумотлардаги хатолик - бир ёки бир неча дастлабки маълумотларнинг хато ифодаланиши дастурнинг авариялиги тугалланишига сабаб бўлиши мумкин ёки хатолик аниқланмаслиги мумкин? аммо тугалланган дастур натижаси нотўғри бўлади.

Data error - presentation errors of one or more source data might become cause of accident program crash or be undetected, but the results normally com-

plete the program will under this infidels.

Пакетная фильтрация — процесс пропускания или блокирования пакетов в сети на основе значений адресов отправителя и получателя, портов или протоколов. П.ф., как правило, является частью программного обеспечении firewall, защищающего локальную сеть от нежелательных вторжений.

Пакетли фильтрация - жўнатувчи ва қабул қилувчи адреслари, портлар ёки протоколлар қийматлари асосида тармоқдаги пакетларни ўтказиш ёки блокироққа қилиш жараёни. Пакетли фильтрлаш, одатда, локал тармоқни номақбул суқилиб киришлардан ҳимояловчи тармоқлараро экран дастурий таъминотининг қисми ҳисобланади.

Packet Filtering - missing process or blocking process packets in a network based on the values and destination addresses, ports, or protocols. P.f, as a rule, is a piece of software protection firewall, protecting the local network from unwanted intrusions.

Пароль одноразовый — пароль, действительный только для одного сеанса или транзакции. Наряду с многофакторной аутентификацией п.о. уменьшает риск подключения к системе с незащищенной рабочей станции.

Бир мартали пароль - фақат битта сеанс ёки транзакция учун ҳақиқий пароль. Бир мартали пароль, кўп факторли аутентификациялаш билан бирга, ҳимояланмаган ишчи станцияли тизимга уланиш хавф-хатарини камайтиради.

One-Time Password (OTP) - is a password that is valid for only one login session or transaction, on a computer system or other digital device.

Пароль — уникалная последовательноеть символов, которую необходимо ввести по запросу компьютера, чтобы исключить доступ к системе, программе или данным.

Пароль –тизимдан, дастурдан ёки маълумотлардан фойдаланишга рухсат олиш учун компьютер сўрови бўйича киритиладиган символларнинг ноёб кетма-кетлиги**.**

Password - a password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.

Перестановка - криптографическая операция, связанная с изменением порядка следования отдельных битов или символов в блоке данных.

Жойини ўзгартириш – маълумотлар блокида алоҳида битлар ёки символларнинг жойлашиш тартибини ўзгартириш билан боғлиқ криптографик амал.

Permutation - cryptographic operations, connected to the change in the order of the individual bits or symbols in the data block.

Подделка информации - умышленная несанкционированная модификация информации при ее обработке техническими средствами с целью получения определенных выгод (преимуществ) перед конкурентом или нанесения ему ущерба.

Ахборотни соҳталаш – ахборотнинг техник воситаларда ишланишида рақибнинг олдида муайян фойда (афзаллик) олиш мақсадида ахборотни атайин рухсатсиз модификациялаш.

Fake information (Forgery) - intentional unauthorized modification of data when it is processed by technical means to obtain certain benefits (benefits) to a competitor or suffering damage.

Подотчетность — возможность проверки; имеет две стороны: во-первых, любое состояние системы можно вернуть в исходное для выяснения того, как система в нем оказалась; во-вторых, имеющийся порядок проведения аудита безопасности позволяет гарантировать, что система удовлетворяет всем заявленным требованиям.

Ҳисобдорлик - текшириш имконияти. Иккита жиҳатга эга. Биринчидан, тизимнинг ҳар қандай ҳолатини, ушбу ҳолатга қай тарзда тушиб қолганини аниқлаш учун, дастлабки ҳолатига қайтариш. Иккинчидан, хавфсизлик аудитини ўтказишнинг мавжуд тартиби тизимнинг барча билдирилган талабларни қониқтиришини кафолатлашга имкон беради.

Auditability - ability to test; has two aspects: firstly, any state of the system can be reset to determine how the system was in it; Second, the existing procedures for auditing the security helps ensure that your system meets all the stated requirements.

Подпись цифровая — представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого ключа секретного, известного только подписывающему субъекту. Предполагается, что п. ц. должна быть легко проверяемой без получения доступа к ключу секретному.

Рақамли имзо - хабарга ёки ҳужжатга ва фақат имзо чекувчи субъектга маълум қандайдир махфий калитга боғлиқ қандайдир алфавитдаги қатордан (масалан рақамли қатордан) иборат. Рақамли имзонинг, махфий калитдан фойдаланмасдан осонгина текширилиши лозимлиги фараз қилинади.

Digital signature - is a string in some alphabet (eg, digital), depending on the message or document and from a secret key known only to the signatory subject. It is assumed that digital signatur should be easily verified without access to the secret key.

Подпись электронная — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электрон имзо - бошқа электрон шаклдаги ахборотга (имзоланувчи

ахборотга) бирлаштирилган ёки бошқа тарзда шундай ахборот билан боғланган ва ахборотни имзоловчи шахсни аниқлашда ишлатиладиган электрон шаклдаги ахборот.

Electronic signature - information in electronic form which is attached to the other information in electronic form (signed information) or otherwise relating to such information and is used to determine the person signing the information.

Подстановка - криптографическая операция, связанная с замещением блока другим и использующая определенный код.

Ўрнига қўйиш –блокни ўрнига бошқасини қўйиш ва муайян коддан фойдаланиш билан боғлиқ криптографик амал.

Substitution - cryptographic operations associated with the replacement unit and the other using a specific code.

Подтверждение подлинности - механизм, направленный на подтверждение подлинности и предусматривающий обмен информацией.

Ҳақиқийликнинг тасдиғи –хақиқийликни тасдиқлашга йўналтирилган ва ахборот алмашишни кўзда тутувчи механизм.

Authentication exchange - mechanism aimed at providing authentication and exchange of information**.**

Политика безопасности (информации в организации) — совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Хавфсизлик сиёсати (ташкилотдаги ахборот хавфсизлиги сиёсати) - ташкилот ўз фаолиятида риоя қиладиган ахборот хавфсизлиги соҳасидаги ҳужжатланган қоидалар, муолажалар, амалий усуллар ёки амал қилинадиган принциплар мажмуи.

Security policy - set of documented policies, procedures, practical methods

or guidelines in the field of information security used by the organization in its activities.

Полномочия - право пользователя (терминала, программы, системы) осуществлять те или иные процедуры над защищенными данными.

Ваколатлар –ҳимояланган маълумотлар устида у ёки бу муолажани бажариши бўйича фойдаланувчининг (терминалнинг, дастурнинг, тизимнинг) ҳуқуқи.

Privileges - the right of the user (terminal program, system) to implement certain procedures over the protected data.

Полномочное управление доступом - разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении субъектов обращаться к информации такого уровня конфиденциальности.

Фойдаланишни ваколатли бошқариш - объектлар таркибидаги ахборотнинг конфиденциаллигини характерловчи белгига ва субъектларнинг бундай конфиденциаллик даражасига эга ахборотга мурожаат этишларига расмий рухсатга асосланган субъектларнинг объектлардан фойдаланишларини чеклаш.

Plenipotentiary access control - access control subjects to objects based on the characterized Tagged confidentiality of the information contained in the objects, and the authorization of subjects to access information of such a level of confidentiality.

Предоставление права на доступ - выдача разрешения (санкции) на использование определенных программ и данных.

Фойдаланиш ҳуқуқини тақдим этиш – муайян дастурлар ва маълумотлардан фойдаланишга рухсат (санкция) бериш.

Authorization - authorization (approval) to use certain programs and

data.

Проникновение - успешное преодоление механизмов защиты системы.

Суқилиб кириш - тизимнинг ҳимоя механизмларидан муваффаққиятли ўтиши.

Penetration - successful resolution mechanisms to protect the system.

Протокол - совокунность правил, определящих алгоритм взаимодействия устройств, программ, систем обработки данных, процессов или пользователей.

Протокол - қурилмалар, дастурлар, маълумотларларни ишлаш тизимлари, жараёнлар ёки фойдаланувчиларнинг ўзаро ҳаракати алгоритмини белгиловчи қоидалар мажмуи.

Protocol - a set of rules that define the algorithm of interaction devices, software, data processing systems, processes or users.

Профиль защиты - документ, описывающий задачи обеспечения защиты информации в терминах функциональных требований и требований гарантированности.

Ҳимоя профили – ахборотни ҳимоялаш масаласини функциональ талаблар ва кафолатланиш талаблари атамаларида тавсифланган хужжат.

Protection Profile - document describing the task of ensuring the protection of information in terms of the functional requirements and the requirements of the warranty.

Разглашение информации — несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Ахборотнинг ошкор қилиниши - ахборотни, ушбу ахборотдан фойдаланиш ҳуқуқига эга бўлмаган истеъмолчиларга рухсатсиз етказиш.

Disclosure of information - unauthorized bringing protected information to consumers who do not have access to this information.

Разграничение доступа - совокупность методов, средств и мероприятий, обеспечивающих защиту данных от несанкционированного доступа пользователей.

Фойдаланишни чеклаш - маълумотларни фойдаланувчиларнинг рухсатсиз фойдаланишларидан ҳимоялашни таъминловчи усуллар, воситалар ва тадбирлар мажмуи.

Access control - a set of methods, tools and measures to ensure the protection of data from unauthorized users.

Разделение привилегий - принцип открытия механизма защиты данных, при котором для доступа к ним необходимо указать не один, а два пароля (например, двумя лицами).

Имтиёзларнинг бўлиниши - маълумотлардан фойдаланиш учун битта эмас, балки иккита паролни кўрсатиш (масалан, иккита шахс паролини) лозим бўлган маълумотларни ҳимоялаш механизмини очиш принципи.

Privilege sharing - the principle of the opening mechanism of protection of data in which to access them you must specify not one, but two passwords (for example, two persons).

Распределенная атака на отказ в обслуживания - входит в число наиболее опасных по последствием классов компьютерных атак, направленных на нарушение доступности информационных ресурсов. Позволяет генерировать больший график, кроме того, её трудно заблокировать, так как поведение различных атакующих компьютеров может отличаться.

Хизмат қилишдан воз кечишга ундайдиган тақсимланган хужумлар - ахборот ресурсларининг фойдаланувчанлигини бузишга

йўналтирилган, оқибати бўйича ўта хавфли компьютер хужумлари синфига мансуб. Узайтирилган трафикни генерациялашга имкон беради, ундан ташқари, уни блокировка қилиш қийин, чунки турли компьютерларнинг хужумлари турлича бўлади.

Distributed Denial of Service (DDoS) - among the most dangerous consequence of classes on cyber attacks aimed at the violation of the availability of information resources. Allows you to generate a larger graph, in addition, it is difficult to block, since the behavior of the various attacking computers may differ. -

Резидентный - постоянно присутствующий в оперативной памяти.

Резидент - асосий хотирада доимо мавжуд.

Resident - constantly present in memory.

Сервер-посредник - брандмауэр, в котором для преобразования IP-адресов всех авторизованных клиентов в IP-адреса, ассоциированные с брандмауэром, используется процесс, называемый трансляцией адресов (address translation).

Сервер-воситачи - брандмауэр бўлиб, унда барча авторизацияланган мижозларнинг IP-адресларини брандмауэр билан ассоцияланган IP-адресларга ўзгартириш учун адресларни трансляциялаш (adress translation) деб аталувчи жараёндан фойдаланилади.

Proxy server - firewall, in which to convert the IP-addresses of all authorized clients in IP-addresses associated with a firewall, use a process called NAT (address translation).

Система обнаружения вторжения — программное или аппаратное средство, предназначенное для выявления фактов несанкционированного доступа в компьютерную систему или сеть.

Бостириб киришларни аниқлаш тизими - компьютер тизимидан ёки тармоғидан рухсатсиз фойдаланиш фактини аниқлашга мўлжалланган

дастурий ёки аппарат восита.

Intrusion Detection System (IDS) - software or hardware designed to detect cases of unauthorized access to a computer system or network.

Скремблер - кодирующее устройство, используемое в цифровом канале, которое выдает случайную последовательность бит.

Скремблер - рақамли каналда ишлатилувчи, битларнинг кетма-кетлигини шакллантирувчи кодловчи қурилма.

Scrambler - encoder used in the digital channel, which provides a random sequence of bits.

Сниффинг — вид сетевой атаки, также называется «пассивное прослушивание сети».

Сниффинг - тармоқ хужуми тури, "тармоқни яширинча эшитиш" деб ҳам аталади.

Sniffing - type of network attack also called "sniffing".

Спамминг - посылка большого числа одинаковых сообщений в различные группы UNINET.

Спамминг - UNINETнинг турли гуруҳларига катта сонли бир хил хабарларни жўнатиш.

Spamming - sending a large number of identical messages to different groups UNINET.

Стеганография - отрасль науки, изучающая математические методы сокрытия конфиденциальной информации в открытых информационных массивах.

Стеганография - очиқ ахборот массивларида конфиденциаль ахборотни яширишнинг математик усулларини ўрганувчи фан соҳаси.

Steganography - a branch of science that studies the mathematical methods

of hiding confidential information in open information arrays.

Стойкость криптографическая — фундаментальное понятие криптографии — свойство криптосистемы (криптопротокола), характеризующее её (его) способность противостоять атакам противника и/или нарушителя, как правило, имеющим целью получить ключ секретный или сообщение открытое.

Криптографик бардошлилик - криптографиянинг фундаментал тушунчаси - криптотизимнинг (криптопротоколнинг), одатда, мақсади махфий калитга ёки очиқ хабарга эга бўлиш бўлган душманнинг ва/ёки бузғунчининг ҳужумларига қарши тура олиши қобилиятини характерловчи хусусияти.

Cryptographic resistance - the basic concept of cryptography - property cryptosystem, which characterizes her (his) ability to withstand enemy attacks and / or the offender, as a rule, have to obtain the secret key or open a message.

Стратегия защиты - формальное определение критериев, особенно оперативных, которыми следует руководствоваться при обеспечении защиты системы от известных угроз.

Ҳимоялаш стратегияси - тизимнинг маълум тахдидлардан ҳимоялашни тьаъминлашда амал қилиниши лозим бўлган мезонларни, айниқса, оператив мезонларни расмий тавсифи.

Security strategy - a formal definition of the criteria, particularly operation-al, to be followed while protecting the system against known threats.

Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Ахборотни ҳимоялаш техникаси - ахборотни ҳимоялашни таъминлашга мўлжалланган ахборотни ҳимоялаш воситалари, ахборотни

ҳимоялаш самарадорлигини назоратлаш воситалари, бошқариш тизимлари ва воситалари.

Security technique - protection of information, tools for monitoring the effectiveness of information security, instrumentation and control systems designed to protect information.

Техническая защита информации - деятельность, направленная на обеспечение безопасности информации инженерно-техническими мерами.

Ахборотни техник ҳимоялаш - инженер-техник чоралар ёрдамида ахборот хавфсизлигини таъминлашга йўналтирилган фаолият

Technical protection of information - activities aimed at ensuring of information security engineering and technical measures.

Техническая разведка - получение сведений путем сбора и анализа информации техническими средствами.

Техник разведка - техник воситалар ёрдамида ахборотни йиғиш ва тахлиллаш йўли билан маълумотларни олиш.

Technical intelligence - obtain information through the collection and analysis of information by technical means.

Тип доступа - сущность права доступа к определенному устройству, программе, файлу и т.д. (обычно read, write, execute, append, modify, delete).

Фойдаланиш тури - маълум қурилмадан, дастурдан, файлдан ва ҳ. фойдаланиш ҳуқуқининг маъноси (одатда read, write, execute, append, modify, delete).

Access type - essence of the right of access to a particular device, programs, files, etc. (usually read, write, execute, append, modify, delete).

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность

нарушения безопасности информации.

Тахдид (ахборот хавфсизлигига тахдид) - ахборот хавфсизлигини бузувчи потенциаль ёки реал мавжуд хавфни туғдирувчи шароитлар ва омиллар мажмуи.

Threat - set of conditions and factors that create potential or actual violations of the existing danger of information security.

Управление доступом - определение и ограничение доступа пользователей, программ и процессов к данным, программам и устройствам вычислительной системы.

Фойдаланишни бошқариш - фойдаланувчиларнинг, дастурларнинг ва жараёнларнинг маълумотлардан, ҳисоблаш техникаси дастурлари ва қурилмаларидан фойдаланишларини белгилаш ва чеклаш.

Access control - definition and limitation of access users, programs, and processes the data, programs, and devices of a computer system.

Утечка информации - неконтролируемое распространение информации, которое привело к ее несанкционированному получению.

Ахборотни сирқиб чиқиши - ахборотни рухсатсиз олинишига сабаб бўлган унинг назоратсиз тарқалиши.

Information loss - uncontrolled dissemination of information that led to the elevation of its.

Фальсификация - использование различных технологий для обхода систем управления доступом на основе IP-адресов с помощью маскирования под другую систему, используя ее IP-адрес.

Сохталаштириш - бошқа тизим IP-адресидан фойдаланиб, унга ўхшаб ниқобланиш ёрдамида IP-адреслар асосида фойдаланишни бошқариш тизимини четлаб ўтиш учун турли технологиялардан фойдаланиш.

Spoofing - the use of different technologies to bypass access control sys-

tems, IP-based addresses using masking under another system using its IP-address.

Фишинг — технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт и т.д.

Фишинг - фойдаланиш пароли, банк ва идентификация карталари маълумотлари ва ҳ. каби шахсий конфиденциаль маълумотларни ўғрилашдан иборат интернет-фирибгарлик технологияси.

Phishing - Internet-fraud technique, is used for stealing personal confidential data such as passwords, bank and identification cards, etc.

Фрод - обман; мошенничество, жульничество; подделка. Вид интернет-мошенничества, при котором мошенник самыми разными способами незаконно получает какую-то часть денег или услуг, относящихся к какому-либо сервису.

Фрод - алдаш, фирибгарлик, ғирромлик, қалбаки. Интернет-фирибгарлик тури бўлиб, фирибгар турли усуллар ёрдамида пулнинг ёки қандайдир серверга тегишли хизмат қисмига ноқонуний эга бўлади.

Fraud - deception; fraud scam; fake. Kind of Internet fraud in which the scammer in many ways unlawfully obtains some of the money or services relating to any service.

Хакер - пользователь, который пытается вносить изменения в системное программное обеспечение, зачастую не имея на это право. Хакером можно назвать программиста, который создает более или менее полезные вспомогательные программы, обычно плохо документированные и иногда вызывающие нежелательные побочные результаты.

Хакер - тизимли дастурий таъминотга, кўпинча ноқонуний ўзгартиришлар киритишга уринувчи фойдаланувчи. Одатда ёмон ҳужжатланган ва баъзида ножоиз қўшимча натижалар туғдирувчи озми-

кўпми фойдали ёрдамчи дастурлар яратувчи дастурчини хакер деб аташ мумкин.

Hacker - a user who is trying to make changes to system software, often without that right. Can be called a hacker programmer who creates a more or less useful utility programs are usually poorly documented and sometimes cause unwanted side effects.

Хеш-функция - функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины

Хеш-функция - чекли алфавитдаги узунлиги чекли кириш йўли сўзини берилган, одатда, қатъий узунликдаги, сўзга акслантириш функцияси.

Hash function - function mapping input word of finite length over a finite alphabet in a given word, usually a fixed length.

Целостность информации - способность средства вычислительной техники или системы автоматизированной обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Ахборот яхлитлиги - тасодифан ва/ёки атайин бузилиш ҳолларида ҳисоблаш техникаси воситаларининг ёки автоматлаштирилган тизимнинг ахборотини ўзгартирмаслигини таъминловчи хусусияти.

Information Integrity - the ability of computers and automated systems to provide consistent information in a casual and / or intentional distortion (destruction).

Ценность информации - свойство информации, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности человека.

Ахборот қиммати –ахборотнинг инсоннинг мақсадли фаолиятининг турли соҳаларида амалий фойдаланишга яроқлиги орқали аниқланувчи

хусусияти.

Information value - property information, determine its applicability to practical use in various fields of purposeful human activity.

Червь - программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе. В отличие от вирусов червь обычно не искажает файлы данных и программы. Обычно червь выполняется, оставаясь необнаруженным, и затем самоуничтожается.

Қурт –кўпинча ёмон ниятда тизимга киритиладиган ва ахборотнинг ишлаш жараёнини тўхтатувчи дастур. Вируслардан фарқланган ҳолда қурт одатда маълумотлар файлини ва дастурни бузмайди. Қурт яширинча бажарилади ва ўз-ўзини йўқотади.

Worm - programs implemented in the system, often malicious, and interrupting the flow of processing information in the system. Unlike viruses worm usually does not distort the data files and programs. Typically, the worm is executed, undetected, and then deletes itself.

Червь сетевой - разновидность программы вредоносной, самостоятельно распространяющейся через локальные и глобальные компьютерные сети.

Тармоқ қуртлари – локаль ва глобал компьютер тармоқлари орқали мустақил равишда тарқалиш хусусиятига эга бўлган зарарли дастур тури.

Network worm - a kind of malicious program, self-propagating through local and global computer networks.

Шлюз прикладного уровня - исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне модели OSI. Связанные с приложениями программы-посредники перенаправляют через шлюз информацию, генерируемую конкретными сервисами TCP/IP.

Илова сатҳи шлюзи - авторизациядан ўтган мижоз ва ташқи хост ўртасидаги тўғридан тўғри ўзаро алоқа амалга ошишига йўл қўймайди. Шлюз OSI моделининг илова сатҳида кирувчи ва чиқувчи тармоқ пакетларининг барчасини фильтрлайди. Иловалар билан боғлиқ дастур-воситачилар TCP/IP аниқ хизматлари генерациялайдиган ахборотни шлюз орқали узатилишини таъминлайди.

Application-level gateway - eliminates the direct interaction between an authorized client and the external host. Gateway filters all incoming and outgoing packets at the application layer model OSI. Application-related program intermediary redirect gateway information generated by a particular service TCP/IP.

Шлюз сеансового уровня - исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Он принимает запрос доверенного клиента на определенные услуги и, после проверки допустимости запрошенного сеанса, устанавливает соединение с внешним хостом. После этого шлюз просто копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Сеанс сатҳи шлюзи - авторизациядан ўтган мижоз ва ташқи хост ўртасидаги тўғридан тўғри ўзаро алоқа амалга ошишига йўл қўймайди. Шлюз ишончли мижоздан сўров қабул қилади ва сўралган сеансга рухсатнин жоизлиги текширилганидан сўнг ташқи хост билан алоқани ўрнатади. Шундан сўнг иккала шлюз йўналишда тармоқ пакетларини фильтрламасдан нусҳа олади.

Circuit-level gateway - eliminates the direct interaction between an authorized client and the external host. It takes a trusted client request for certain services and, after validation of the requested session, establishes the connection with the external host. After this, the gateway simply copies the packets in both directions, not realizing their filtration.

Шпионское программное обеспечение — вид вредоносного программного обеспечения, осуществляющего деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Хуфия дастурий таъминот – фойдаланувчиларни рухсатисиз компьютер конфигурациялари, фойдаланувчилар фаолияти ва ҳар қандай бошқа конфиденциал ахборотни йиғиш бўйича фаолият олиб борадиган зарарли дастурий таъминот тури.

Spyware - type of malicious software, carrying out activities to collect information about your computer configuration, user activity, and any other confidential information without the consent of the user.

Экспертиза системы защиты информации - оценка соответствия представленных проектных материалов по защите информации (на объекте) поставленной цели, требованиям стандартов и других нормативных документов.

Ахборотни ҳимоялаш тизимининг экспертизаси - ахборотни ҳимоялаш бўйича тақдим этилган лойиҳа материалларининг қўйилган мақсад стандартлар талабларига ва бошқа меъерий хужжатларга мослигини баҳолаш.

Expert operation of the system of protection to information - conformity assessment submitted project materials for the protection of information (on-site) goal, the standards and other regulatory documents.

Эксплойт — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на компьютерную систему.

Эксплойт – компьютер тизимига хужум уюштириш учун

қўлланиладиган ва дастурий таъминот заифликларидан фойдаланувчи компьютер дастури, дастурий код фрагменти ёки буйруқлар кетма-кетлиги.

Exploit - computer program code snippet or a sequence of commands that use vulnerabilities in software and used for an attack on a computer system.

Эффективность - свойство объекта удовлетворять требованиям к услуге с заданными количественными характеристиками**.**

Самарадорлилик – берилган миқдорий характеристикалари билан хизмат кўрсатишга бўлган талабларни қондирувчи объектнинг хусусияти.

Efficiency - object property to satisfy the requirements of the service with the given quantitative characteristics.

Ядро защиты - технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Ҳимоя ядроси –фойдаланиш дистпетчери концепциясини амалга оширувчи ҳимоялаш воситалари комплексининг техник дастурий ва микродастурий элементлари.

Security kernel - hardware, software and micro-program elements of remedies tools protection implementing the concept of Access Manager.