ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ОЛИЙ ТАЪЛИМ ТИЗИМИ ПЕДАГОГ ВА РАҲБАР КАДРЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШНИ ТАШКИЛ ЭТИШ БОШ ИЛМИЙ - МЕТОДИК МАРКАЗИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

“КОМПЬЮТЕР ИНЖИНИРИНГИ”

йўналиши

“АХБОРОТ ХАВФСИЗЛИГИ”

МОДУЛИ БЎЙИЧА

Ў Қ У В –У С Л У Б И Й М А Ж М У А

ТОШКЕНТ - 2017

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ОЛИЙ ТАЪЛИМ ТИЗИМИ ПЕДАГОГ ВА РАҲБАР КАДРЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШНИ ТАШКИЛ ЭТИШ БОШ ИЛМИЙ - МЕТОДИК МАРКАЗИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

“АХБОРОТ ХАВФСИЗЛИГИ” модули бўйича

ЎҚУВ – УСЛУБИЙ МАЖМУА

ТОШКЕНТ - 2017

Мазкур ўқув-услубий мажмуа Олий ва ўрта махсус таълим вазирлигининг 2016 йил 6 апрелдаги 137-сонли буйруғи билан тасдиқланган ўқув режа ва дастур асосида тайёрланди.

Тузувчилар: ТАТУ “Ахборот хавфсизлиги” кафедраси ассистенти З.Т. Худойқулов

ТАТУ “Ахборот хавфсизлиги” кафедраси ассистенти Ш.Р. Ғуломов

ТАТУ “Ахборот хавфсизлиги” кафедраси ассистенти А.А. Абдурахмонов

Тақризчи: ТАТУ, АКТ бўйича маслаҳатчи проректори, Жанубий Кореялик мутахассис Ли Чул Су

Ўқув -услубий мажмуа Тошкент ахборот технологиялари университети Кенгашининг қарори билан нашрга тавсия қилинган (2016 йил 29 августдаги 1(661) - сонли баённома)

TO CURRICULUM FOR THE «COMPUTER ENGINEERING» COURSE OF PROFESSIONAL DEVELOPMENT AND RETRAINING ACADEMIC STAFF OF HIGHER EDUCATION

REVIEW

Typical training program of direction "Computer Engineering" is presented on pages 17 and contains 8 modules.A typical curriculum includes legal framework and legal university standards, modern educational technology and high pedagogical skills, use of information and communication technologies in pedagogical process, a foreign language, the basics of system analysis and application of the decision, the scientific practical work on the basis of special directions, new methods of creating education and process, creativity and competence of the teacher, the embedded system, new knowledge on information security and Linux.
The title and content of the curriculum of direction "Computer Engineering" corresponds to the typical curriculum specialty and educational standards, qualification requirements to a specialist.

The level of reflection in the standard curriculum of modern science, technology, culture teaching, as well as recommended by the author of the curriculum advanced technologies are presentedonthe qualification requirements for the preparation and improvement of professional skills of the teacher are sufficient.

The program includes the training of teachers of subjects in the field of education, training and skills development, quality and preparation of the general qualification requirements and training plans formed the basis of the teaching staff of higher education institutions in the sphere of modern education and innovative technologies.The best international practices of effective use of information and communication technologies in the educational process of the introduction of foreign language are intensive due to the level of development of their professional skills. The elevations of the regular activities of the scientific institutions of higher education are included in training and educational process of organization and management systems.

Vice rector of ICT, TUIT **Chul Soo Lee**

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГИК КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИДА "КОМПЬЮТЕР ИНЖИНИРИНГИ" ЙЎНАЛИШИ БЎЙИЧА ЎҚУВ ДАСТУРИГА ТАҚРИЗ

Ушбу ўқув дастурда"Компьютер инжиниринги" йўналиши бўйича назарий ва амалий билимлар кўрсатиб ўтилган.

Дастур мазмуни олий таълимнинг норматив-ҳуқуқий асослари ва қонунчилик нормалари, илғор таълим технологиялари ва педагогик маҳорат, таълим жараёнларида ахборот-коммуникация технологияларини қўллаш, амалий хорижий тил, тизимли таҳлил ва қарор қабул қилиш асослари, махсус фанлар негизида илмий ва амалий тадқиқотлар, технологик тараққиёт ва ўқув жараёнини ташкил этишнинг замонавий услублари бўйича сўнгги ютуқлар, педагогнинг касбий компетентлиги ва креативлиги, маълумотлар базасини бошқариш тизимлари, ахборот хавфсизлиги ва электрон тижорат бўйича янги билим, кўникма ва малакаларини шакллантиришни назарда тутади.

Дастур доирасида берилаётган мавзулар таълим соҳаси бўйича педагог кадрларни қайта тайёрлаш ва малакасини ошириш мазмуни, сифати ва уларнинг тайёргарлигига қўйиладиган умумий малака талаблари ва ўқув режалари асосида шакллантирилган бўлиб, бу орқали олий таълим муассасалари педагог кадрларининг соҳага оид замонавий таълим ва инновация технологиялари, илғор хорижий тажрибалардан самарали фойдаланиш, ахборот-коммуникация технологияларини ўқув жараёнига кенг татбиқ этиш, чет тилларини интенсив ўзлаштириш даражасини ошириш ҳисобига уларнинг касб маҳоратини, илмий фаолиятини мунтазам юксалтириш, олий таълим муассасаларида ўқув-тарбия жараёнларини ташкил этиш ва бошқаришни тизимли таҳлил қилиш, шунингдек, педагогик вазиятларда оптимал қарорлар қабул қилиш билан боғлиқ компетенцияларга эга бўлишлари таъминланади.

Қайта тайёрлаш ва малака ошириш йўналишининг ўзига хос хусусиятлари ҳамда долзарб масалаларидан келиб чиққан ҳолда дастурда тингловчиларнинг махсус фанлар доирасидаги билим, кўникма, малака ҳамда компетенцияларига қўйиладиган талаблар такомиллаштирилиши мумкин.

Умуман олганда, "Компьютер инжиниринги" йўналиши бўйичаяратилган ўқув дастур тингловчилар учун фойдали бўлиб ўқув жараёнида қуллаш учун тавсия этилади.

ТАТУ, "Ахборот технологиялари"
профессори, т.ф.д. Зайнидинов Х.Н.

МУНДАРИЖА

I. БЎЛИМ

ИШЧИ ДАСТУР

I. ИШЧИ ДАСТУР

Кириш

Дастур Ўзбекистон Республикаси Президентининг 2015 йил 12 июндаги “Олий таълим муассасаларининг раҳбар ва педагог кадрларини қайта тайёрлаш ва малакасини ошириш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида” ги ПФ-4732-сон Фармонидаги устувор йўналишлар мазмунидан келиб чиққан ҳолда тузилган бўлиб, у замонавий талаблар асосида қайта тайёрлаш ва малака ошириш жараёнларининг мазмунини такомиллаштириш ҳамда олий таълим муассасалари педагог кадрларининг касбий компетентлигини мунтазам ошириб боришни мақсад қилади. Дастур мазмуни олий таълимнинг норматив-ҳуқуқий асослари ва қонунчилик нормалари, илғор таълим технологиялари ва педагогик маҳорат, таълим жараёнларида ахборот-коммуникация технологияларини қўллаш, амалий хорижий тил, тизимли таҳлил ва қарор қабул қилиш асослари, махсус фанлар негизида илмий ва амалий тадқиқотлар, технологик тараққиёт ва ўқув жараёнини ташкил этишнинг замонавий услублари бўйича сўнгги ютуқлар, педагогнинг касбий компетентлиги ва креативлиги, глобал Интернет тармоғи, мультимедиа тизимлари ва масофадан ўқитиш усулларини ўзлаштириш бўйича янги билим, кўникма ва малакаларини шакллантиришни назарда тутади.

Ушбу дастурда ахборот хавфсизлигининг долзарблиги ва унинг криптографик ҳимояси, рухсатларни назоратлаш усуллари, дастурий маҳсулотлар хавфсизлигини тадбиқ этиш, ахборотнинг ҳуқуқий ва техник ҳимояси усуллари, SSL ва IPSec тармоқ протоколларини таҳлили, симсиз тармоқларда ахборот хавфсизлигини таъминлаш ва улардаги хавфсизлик протоколлари, зараркунанда дастурий воситаларнинг статик таҳлили ва Java дастурлаш тилида хавфсиз дастурларни ишлаб чиқиш баён этилган.

Модулнинг мақсади ва вазифалари

Ахборот хавфсизлиги **модулининг мақсад ва вазифалари:**

– тингловчиларга ахборот хавфсизлигини таъминлаш билан боғлиқ масалаларни ечишда ахборот-коммуникация тизимларида ахборотларни ҳимоялаш технологияларининг ўрни ва истиқболли йўналишлари профилига мос билим, кўникма ва малакани таълим стандартида талаб қилинган билимларни шакллантиришдир;

– ахборот хавфсизлиги тушунчаси, уни қўлланиш соҳаси ҳамда ахборот хавфсизлигини таъминлаш чора тадбирлари, усуллари ва воситаларини таҳлил қилиб улар асосида ахборотни ҳимоялаш қобилиятларини эгаллаш;

– ахборот-коммуникацион тизимларни самарали ҳимоялаш усул ва воситасини таҳлил қилишдан иборатдир.

Модул бўйича тингловчиларнинг билими, кўникмаси, малакаси ва компетенцияларига қўйиладиган талаблар

“Ахборот хавфсизлиги” курсини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида**:**

Тингловчи:

– ахборот ҳимояси, ҳимояланадиган объектлар, таҳдидлар ва уларга кутиладиган таъсирлар ***ҳақида тасаввурга эга бўлиши;***

Тингловчи:

– ахборот хавфсизлиги таъминотининг зарурий технология ва ҳимоя воситаларини танлаш;

– ахборот чиқиб кетадиган ташкилий ва техник каналларни аниқлаш;

– ташкилот хавфсизлик сиёсатини яратиш ***кўникмаларига эга бўлиши;***

Тингловчи:

– меъёрий ва фавқулодда вазиятларда ахборот хавфсизлиги тизимларини ташкилини;

– интеллектуал мулк ва муаллифлик ҳуқуқини, давлат фаолиятининг турли соҳаларида ахборотни ҳимоялаш принциплари ва усулларини;

– ахборот хавфсизлиги соҳасида асосий ҳуқуқий меъёрларни ***билиши ва улардан фойдалана олиши лозим.***

Модулни ташкил этиш ва ўтказиш бўйича тавсиялар

“Ахборот хавфсизлиги” курси маъруза ва амалий машғулотлар шаклида олиб борилади.

Курсни ўқитиш жараёнида таълимнинг замонавий методлари, педагогик технологиялар ва ахборот-коммуникация технологиялари қўлланилиши назарда тутилган:

– маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион ва электрон-дидактик технологиялардан;

– ўтказиладиган амалий машғулотларда техник воситалардан, экспресс-сўровлар, тест сўровлари, ақлий ҳужум, гуруҳли фикрлаш, кичик гуруҳлар билан ишлаш, коллоквиум ўтказиш ва бошқа интерактив таълим усулларини қўллаш назарда тутилади.

Модулнинг ўқув режадаги бошқа модуллар билан боғлиқлиги ва узвийлиги

“Ахборот хавфсизлиги” модули мазмуни ўқув режадаги “Операцион тизимлар” ва “Электрон ҳукумат” ўқув модуллари билан узвий боғланган ҳолда педагогларнинг ахборот хавфсизлиги бўйича касбий педагогик тайёргарлик даражасини оширишга хизмат қилади.

Модулнинг олий таълимдаги ўрни

Модулни ўзлаштириш орқали тингловчилар ахборот хавфсизлигидаги таҳдид ва ҳужумларни таҳлил қилиш, ахборотни шифрлаш ва дешифрлашни

ўрганиш, амалда қўллаш ва ахборотни ҳимояланганлигини баҳолашга доир касбий компетентликка эга бўладилар.

Модул бўйича соатлар тақсимоти

№	Модул мавзулари	Тингловчининг ўқув юкламаси, соат				
		Ҳаммаси	Аудитория ўқув юкламаси			Мустақил таълим
			Жами	жумладан		
				Назарий	Амалий машғулот	
1.	Ахборот хавфсизлигининг анъанавий тимсоллари. Ахборот хавфсизлиги сиёсати. Ҳимоя тизимини лойиҳалаш ва амалга ошириш босқичлари.	4	4	2	2	
2.	Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.	8	6	2	4	2
3.	Аутентификация ва идентификация усуллари. Рухсатларни назоратлаш. Тармоқлараро экран. Ҳужумларни аниқлаш тизимлари.	6	4	2	2	2
4.	Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.	6	6	2	4	
5.	Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар. Дастурий маҳсулотларни яратиш.	6	6	2	4	
	Жами:	**30**	**26**	**10**	**16**	**4**

НАЗАРИЙ МАШҒУЛОТЛАР МАЗМУНИ

1 - мавзу: Ахборот хавфсизлигининг анъанавий тимсоллари. Ахборот хавфсизлиги сиёсати. Ҳимоя тизимини лойиҳалаш ва амалга ошириш босқичлари.

Ахборот хавфсизлиги тушунчаси. Ахборот хавфсизлигида заифлик, таҳдид ва ҳужум тушунчалари. Ахборотни ташкил этувчилари. Ахборот бутунлиги, махфийлиги ва фойдаланувчанлиги. Идентификация. Аутентификация. Авторизация. Ахборотни ҳимоялаш усуллари. Ҳуқуқий ҳимоя. Ташкилий ҳимоя. Инжинер-техник ҳимоя. Дастурий ҳимоя. Апарат ҳимоя. Тармоқ хавфсизлиги. Операцион тизим хавфсизлиги. Дастурий маҳсулотлар хавфсизлиги.

2 - мавзу: Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.

Ахборотнинг криптографик ҳимояси. Ахборот бутунлигини ҳимоялаш. Ахборот махфийлигини ҳимоялаш. Шифрлаш алгоритмлари классификацияси. Симметрик шифрлаш усуллари. Ассиметрик шифрлаш усуллари. Хэш функциялар. Электрон рақамли имзо алгоритмлари. Калитларни бошқариш тизимлари.

3 – мавзу: Аутентификация ва идентификация усуллари. Рухсатларни назоратлаш. Тармоқлараро экран. Ҳужумларни аниқлаш тизимлари.

Идентификация. Аутентификация. Авториязация. Аутентификация усуллари. Пароллар асосида аутентификация. Смарт карталар асосида аутентификация. Биометрик хусусиятлар асосида аутентификация. Рухсатларни назоратлаш. Бошқариш моделлари. Тармоқлараро экран ва уларнинг турлари. Ҳужумларни аниқлаш тизимлари.

4 – мавзу: Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Паролларга асосланган аутентификацилаш протоколлари. Тасодифий сонлар ва вақт параметларига асосланган аутентификациялаш алгоритмлари. SSH протоколи ва унинг вазифаси. SFTP протоколи. Керберос протоколи. SKEY дастури. Диффи-Хелман калитларни алмашиниш протоколи. Нидхем-Шрёдер протоколи. Хавфсиз Command-shell. Port forwarding.

5 – мавзу: Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар. Дастурий маҳсулотларни яратиш.

Дастурий маҳсулотлар хавфсизлиги. Операцион тизим хавфсизлиги.

Дастурлаш тилларининг хавфсизлик таҳлили. Дастурий маҳсулотларга тегишли заифликлар ва таҳдидлар. Хотиранинг тўлиб тошиши (Buffer overflow). Ўртадан туриб ўзгартириш. Тезкор мурожат шарти таҳдиди. SQL инексия. Зараркунанда дастурларнинг таҳлили. Содда статик таҳлиллаш. Содда динамик таҳлиллаш.

АМАЛИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-амалий машғулот. Ахборот хавфсизлигининг анъанавий тимсоллари. Ахборот хавфсизлиги сиёсати. Ҳимоя тизимини лойиҳалаш ва амалга ошириш босқичлари.

Ахборот хавфсизлиги сиёсати. Ахборотнинг муҳандис техник усули. Техник ҳимоя воситалари. Ахборотнинг ташкилий ҳимояси. Ахборотнинг чиқиб кетиш каналлари. Ахборот хавфсизлиги бўйича халқаро стандартлар. Ташкилий таъминот.

2-амалий машғулот. Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари.

Содда симметрик шифрлаш усуллари. Цезар усули. Ўрин алмаштириш шифрлари. Ўрнига қўйиш шифрлари. Частотавий таҳлил усули. Замонавий шифрлаш алгоритмлари. DES шифрлаш стандарти. RSA очиқ калитли шифрлаш усули. Оқимли шифрлаш усуллари. A5/1 оқимли шифрлаш алгоритми.

3-амалий машғулот. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.

Тармоқлараро экран технологияси. Тармоқ ҳимоясида тармоқлараро экран воситаларидан фойдаланиш. Тармоқлараро экран турлари. Тармоқлараро экран воситаларини ўрнатиш ва созлаш. Янги қоидалар яратиш. Тизимни назоратлаш.

4-амалий машғулот. Аутентификация ва идентификация усуллари. Рухсатларни назоратлаш. Тармоқлараро экран. Ҳужумларни аниқлаш тизимлари.

TCP/IP протоколида мавжуд заифликлар. SSL тармоқ протоколи ва унинг вазифаси. Ўртага турган одам ҳужуми. SSL протоколини созлаш. X.509 сертификати.

5-амалий машғулот. Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Симсиз тармоқда мавжуд заифликлар. Симсиз тармоқда фойдаланилган хавфсизлик протоколлари. WEP протоколи. WPA ва WPA2 протоколлари. Симсиз тармоқлардан фойдаланишда бериладиган хавфсизлик тавсиялари.

6-амалий машғулот. Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Зараркунанда дастурий воситалар. Зараркунанда дастурларни таҳлиллаш. Статик таҳлил. Динамик таҳлил. Зараркунанда дастурлардан “қаторларни (strings)” аниқлаш. Қалбаки тармоқ. IDA Pro дастурида зараркунанда дастурларни юклаш. Дизассемберлаш. Тескари мухандислик инжиниринги.

7-Амалий машғулот.
Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар.

Дастурлар тилларининг хавфсизлик таҳлили. Java дастурлаш тилининг тузулиши ва имкониятлари. Java дастурлаш тилида мавжуд заифликлар. Java дастурлаш тилида хавфсиз дастурлаш кўникмалари. Компиляция. Транслятор. Интерпритатор. Бинар код. Java платформаси. Java хавфсизлик фреймворки. Имтиёзли кодлар.

8-Амалий машғулот.
Дастурий маҳсулотларни яратиш.

Замонавий операцион тизимлар. Ажратиш. Рухсатларни бошқариш. Хотира ҳимояси. Ишончли операцион тизим. Сегментлаш. Саҳифаларни рақамлаш. Ишончли жой. Локал хавфсизлик сиёсати. Пароллар сиёсати. Аудит сиёсати. Дастурий таъминотларни бошқариш ва чеклаш сиёсати. Windows операцион тизим тармоқлараро экрани.

ЎҚИТИШ ШАКЛЛАРИ

Мазкур модул бўйича қуйидаги ўқитиш шаклларидан фойдаланилади:

- маърузалар, амалий машғулотлар (маълумотлар ва технологияларни англаб олиш, ақлий қизиқишни ривожлантириш, назарий билимларни мустаҳкамлаш);
- давра суҳбатлари (кўрилаётган лойиҳа ечимлари бўйича таклиф бериш қобилиятини ошириш, эшитиш, идрок қилиш ва мантиқий хулосалар чиқариш);
- баҳс ва мунозаралар (лойиҳалар ечими бўйича далиллар ва асосли аргументларни тақдим қилиш, эшитиш ва муаммолар ечимини топиш қобилиятини ривожлантириш).

БАҲОЛАШ МЕЗОНИ

№	Баҳолаш турлари	Максимал балл	Изоҳ
1.	Кейс топшириқлари	2.5	1.2 балл
2.	Мустақил иш топшириқлари		0.5 балл
3.	Амалий топшириқлар		0.8 балл

II. БЎЛИМ

МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

II. МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

“SWOT-таҳлил” методи

Методнинг мақсади: мавжуд назарий билимлар ва амалий тажрибаларни таҳлил қилиш, таққослаш орқали муаммони ҳал этиш йўлларни топишга, билимларни мустаҳкамлаш, такрорлаш, баҳолашга, мустақил, танқидий фикрлашни, ностандарт тафаккурни шакллантиришга хизмат қилади.

Намуна: Ахборот хавфсизлигида фойдаланилган усулларнинг SWOT таҳлилини ушбу жадвалга туширинг.

S	Ахборотни ҳимоялаш усулларининг мавжудлиги	Ахборот хавфсизлигида кўплаб ҳимоя усуллари бўлиб, улар биргаликда фойдаланилади.
W	Ҳимоя усулларида заифликларни бўлиши	Бир ҳимоя усулда мавжуд камчилик бутун тизим хавфсиз-лигига таъсир этиши мумкин.
O	Ҳимоя усулларидан фойдаланган ҳолда олинган имкониятлар	Ахборотнинг тўлиқ хавфсизлиги таъминланади.
T	Тўсиқлар (ташқи)	Ахборотни йўқолишига сабаб бўлувчи атайин ёки билмасдан туриб амалга оширилган таҳдидларни мавжудлиги.

Хулосалаш» (Резюме, Веер) методи

Методнинг мақсади: Бу метод мураккаб, кўптармоқли, мумкин қадар, муаммоли характеридаги мавзуларни ўрганишга қаратилган. Методнинг моҳияти шундан иборатки, бунда мавзунинг турли тармоқлари бўйича бир хил ахборот берилади ва айни пайтда, уларнинг ҳар бири алоҳида аспектларда муҳокама этилади. Масалан, муаммо ижобий ва салбий томонлари, афзаллик, фазилат ва камчиликлари, фойда ва зарарлари бўйича ўрганилади. Бу интерфаол метод танқидий, таҳлилий, аниқ мантиқий фикрлашни муваффақиятли ривожлантиришга ҳамда ўқувчиларнинг мустақил ғоялари, фикрларини ёзма ва оғзаки шаклда тизимли баён этиш, ҳимоя қилишга имконият яратади. “Хулосалаш” методидан маъруза машғулотларида индивидуал ва жуфтликлардаги иш шаклида, амалий ва семинар машғулотларида кичик гуруҳлардаги иш шаклида мавзу юзасидан билимларни мустаҳкамлаш, таҳлили қилиш ва таққослаш мақсадида фойдаланиш мумкин.

Методни амалга ошириш тартиби:

тренер-ўқитувчи иштирокчиларни 5-6 кишидан иборат кичик гуруҳларга ажратади;

тренинг мақсади, шартлари ва тартиби билан иштирокчиларни таништиргач, ҳар бир гуруҳга умумий муаммони таҳлил қилиниши зарур бўлган қисмлари туширилган тарқатма материалларни тарқатади;

ҳар бир гуруҳ ўзига берилган муаммони атрофлича таҳлил қилиб, ўз мулоҳазаларини тавсия этилаётган схема бўйича тарқатмага ёзма баён қилади;

навбатдаги босқичда барча гуруҳлар ўз тақдимотларини ўтказадилар. Шундан сўнг, тренер томонидан таҳлиллар умумлаштирилади, зарурий ахборотлр билан тўлдирилади ва мавзу якунланади.

Намуна:

Ахборотни ҳимоялаш усуллари					
Ташкилий ҳимоя		**Ҳуқуқий ҳимоя**		**Криптографик ҳимоя**	
афзаллиги	камчилиги	афзаллиги	камчилиги	афзаллиги	камчилиги
Хулоса:					

“Ассесмент” методи

Методнинг мақсади: мазкур метод таълим олувчиларнинг билим даражасини баҳолаш, назорат қилиш, ўзлаштириш кўрсаткичи ва амалий кўникмаларини текширишга йўналтирилган. Мазкур техника орқали таълим олувчиларнинг билиш фаолияти турли йўналишлар (тест, амалий кўникмалар, муаммоли вазиятлар машқи, қиёсий таҳлил, симптомларни аниқлаш) бўйича ташҳис қилинади ва баҳоланади.

Методни амалга ошириш тартиби:

“Ассесмент” лардан маъруза машғулотларида талабаларнинг ёки қатнашчиларнинг мавжуд билим даражасини ўрганишда, янги маълумотларни баён қилишда, семинар, амалий машғулотларда эса мавзу ёки маълумотларни ўзлаштириш даражасини баҳолаш, шунингдек, ўз-ўзини баҳолаш мақсадида индивидуал шаклда фойдаланиш тавсия этилади. Шунингдек, ўқитувчининг ижодий ёндашуви ҳамда ўқув мақсадларидан келиб чиқиб, ассесментга қўшимча топшириқларни киритиш мумкин.

Намуна. Ҳар бир катакдаги тўғри жавоб 5 балл ёки 1-5 балгача баҳоланиши мумкин.

Тест

- 1. Ахборотни ташкил этувчи хусусиятлари сони ?
- A. 3
- B. 4
- C. 2

Қиёсий таҳлил

- Ҳимоя усулларининг қиёсий таҳлили ?

Тушунча таҳлили

- ЭРИ қисқармасини изоҳланг...

Амалий кўникма

- Хавфсизлик сиёсатини мақсади ?

“Тушунчалар таҳлили” методи

Методнинг мақсади: мазкур метод талабалар ёки қатнашчиларни мавзу буйича таянч тушунчаларни ўзлаштириш даражасини аниқлаш, ўз билимларини мустақил равишда текшириш, баҳолаш, шунингдек, янги мавзу буйича дастлабки билимлар даражасини ташҳис қилиш мақсадида қўлланилади.

Методни амалга ошириш тартиби:

- иштирокчилар машғулот қоидалари билан таништирилади;
- ўқувчиларга мавзуга ёки бобга тегишли бўлган сўзлар, тушунчалар номи туширилган тарқатмалар берилади (индивидуал ёки гуруҳли тартибда);
- ўқувчилар мазкур тушунчалар қандай маъно англатиши, қачон, қандай ҳолатларда қўлланилиши ҳақида ёзма маълумот берадилар;
- белгиланган вақт якунига етгач ўқитувчи берилган тушунчаларнинг тугри ва тулиқ изоҳини уқиб эшиттиради ёки слайд орқали намойиш этади;
- ҳар бир иштирокчи берилган тугри жавоблар билан узининг шахсий муносабатини таққослайди, фарқларини аниқлайди ва ўз билим даражасини текшириб, баҳолайди.

Намуна: “Модулдаги таянч тушунчалар таҳлили”

Тушунчалар	**Сизнингча бу тушунча қандай маънони англатади?**	**Қўшимча маълумот**
Заифлик	Тизимда мавжуд бўлган камчилик.	
Таҳдид	Мавжуд заифлик натижасида бўлиши мумкин бўлган, амалга ошмаган ҳужум.	
Вирус	Зарарли дастур.	
Шифрлаш	Бирор алгоритм асосида очиқ маълумотни тушунарсиз кўринишга ўтказиш жараёни.	
Калит	Маълумотни шифрлашда ва дешифрлашда фойдаланиладиган катталик.	
Хавфсизлик сиёсати	Хавфисизликни таъминлаш учун бажариладиган чора – тадбирлар йиғиндиси.	
Протокол	Бажарилиши керак бўлган ишларнинг кетма – кетлиги.	

Изоҳ: Иккинчи устунчага қатнашчилар томонидан фикр билдирилади. Мазкур тушунчалар ҳақида қўшимча маълумот глоссарийда келтирилган.

III. БЎЛИМ

НАЗАРИЙ МАТЕРИАЛЛАР

III. НАЗАРИЙ МАТЕРИАЛЛАР

1-мавзу: Ахборот хавфсизлигининг анъанавий тимсоллари. Ахборот хавфсизлиги сиёсати. Ҳимоя тизимини лойиҳалаш ва амалга ошириш босқичлари.

Режа:

1. Ахборот хавфсизлиги тушунчаси.
2. Ахборот ҳимояси.
3. Ахборот хавфсизлиги сиёсати.
4. Ахборотни ҳимоялаш усуллари.

Таянч иборалар: *ахборот, хавфсизлик, заифлик, таҳдид, ҳужум, бутунлик, фойдаланувчанлик, махфийлик, идентификация, аутентификация, авторизация, ҳуқуқий ҳимоя, ташкилий ҳимоя, инжинер-техник ҳимоя, дастурий ҳимоя, апарат ҳимоя, тармоқ хавфсизлиги, операцион тизим хавфсизлиги, дастурий маҳсулот хавфсизлиги.*

1.1.Ахборот хавфсизлиги тушунчаси

Умумжаҳон ахборот глобаллашуви жараёнлари ахборот-коммуникация технологияларини нафақат мамалакатлар иқтисодиёти ва бошқа соҳаларида жорий этиш, балки ахборот тизимлари хавфсизлигини таъминлашни ҳам тақазо этмоқда. Ахборот технологияларини ҳаётимизнинг ҳар бир жабҳасига кириб бориши, инсонларнинг ахборотга бўлган талабларини ортиши, ахборотни муҳимлик даражасини ортишига олиб келади. Бунинг натижасида эса, ахборотни қўлга киритишга қаратилган ҳатти-ҳаракатлар миқдори ортиб келмоқда. Бу эса ўз навбатида ҳар жабҳада ахборот хавфсизлигини таъминлаш долзарблигини билдиради.

Ахборот хавфсизлигининг анъанавий тимсоллари

Ахборот хавфсизлиги маълумотларни ҳимоялаш усуллари билан шуғулланади. Ахборот хавфсизлигида анаънавий тимсоллар сифатида 1.1-расмда кўрсатилган, Алиса, Боб ва Триди олинган бўлиб, Алиса ва Боб қонуний фойдаланувчилар ёки “яхши одамлар”, Триди эса бузғунчи ёки нияти бузуқ одам.

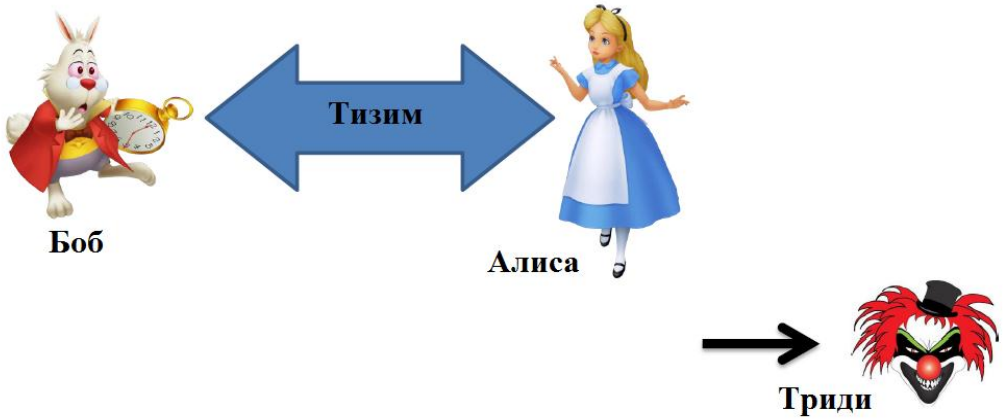
Хавфсизлик соҳалари. Ахборот хавфсизлигини таъминлаш барча соҳаларда амалга оширилиб, улар асосан қуйидагиларга бўлинади:

- Тармоқ хавфсизлиги;
- Web да хавфсизликни таъминлаш;

– Илова ва операцион тизим хавфсизлиги.

Ахборот хавфсизлиги муаммолари. Ахборот хавфсизлигида муаммолар тури кўп бўлиб, улар асосан қуйидаги сабабларга кўра келиб чиқади[1]:

– Кўп зарарли, хатоли дастурларни мавжудлиги;
– Нияти бузуқ фойдаланувчиларни мавжудлиги;
– Социал инжиниринг;
– Физик ҳимоя заифликлари ва ҳак.



1.1-расм. Ахборот хавфсизлиги тимсоллари

Ахборот хавфсизлигида муаммоларни ортишига асосан қуйидагилар мотивация бўлиши мумкин:

– Фойда;
– Терроризим;
– Ҳарбий соҳа ва ҳак.

Ахборот хавфсизлигида мавжуд муаммолар хавфлилик даражасига кўра: заифлик, таҳдид ва ҳужумга олиб келувчиларга бўлиши мумкин.

Заифлик – бу тизимда мавжуд бўлган хавфсизлик муаммоаси бўлиб, улар асосан тизимнинг яхши шакллантирилмаганлиги ёки созланмаганлиги сабабли келиб чиқади. Заифликлар тизимларда катта ёки кичик тарзда мавжуд бўлади.

Таҳдид – бу мавжуд бўлган заифлик натижасида бўлиши мумкин бўлган ҳужум тури бўлиб, улар асосан тизимни камчиликларини ўрганиш натижасида келиб чиқади.

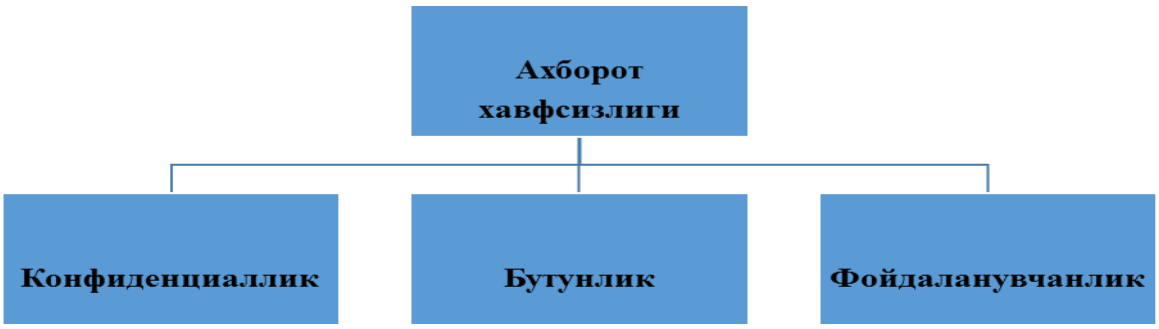
Ҳужум – бу мавжуд таҳдидни амалга оширилган кўриниши бўлиб, бунда кутилган таҳдид амалга оширилади.

[1] Stamp Mark. Information security: principles and practice. 1 – c.

1.2.Ахборот ҳимояси

Умумий ҳолда ахборот хавфсизлиги консепсияси учта ташкил этувчидан иборатлигини эътиборга олинса, ахборот хавфсизлигини таъминлаш дэганда маълумотнинг қуйидаги учта хусусиятини таъминлаш тушуниш мумкин.

Қуйида келтирилган 1.2 - расмда ушбу учта хусусиятни таъминлашда криптографик усулларнинг тутган ўрни келтирилган. Умумий ҳолда ахборот хавфсизилигини таъминлаш деганда ушбу учта хусусиятни таъминлаш тушунилиб, ҳар бир хусусият муҳимлиги ахборотнинг турига ва фойдаланилишига кўра ҳар хил бўлиши мумкин [1].



1.2 - расм. Ахборот хавфсизлиги хусусиятлари

Масалан, оммавий турдаги маълумот учун биринчи навбатда, фойдаланувчанлик ва бутунлик хусусиятларини таъминлаш муҳим бўлса, давлат сири даражасидаги маълумот учун унинг конфиденциялиги биринчи ўринда туради.

Конфиденциаллик (рухсатсиз ўқишнинг мумкин эмаслиги) хусусияти ахборотнинг рухсат этилмаган фойдаланувчилардан яшириш, маълумот маносини тушуниб олмаслик учун, уни тушунарсиз ҳолатда ўтказиш каби вазифаларни бажариш орқали бажарилади. Ахборотнинг ушбу хусусияти криптографик ҳимоя усулларидан бири саналган, шифрлаш усуллари асосида амалга оширилади. Шифрлаш усуллари ёрдамида очиқ маълумот яширинган кўринишдаги шифрматн ҳолатига айланади. Бу эса уни бузғунчи фойдаланишидан олдини олади.

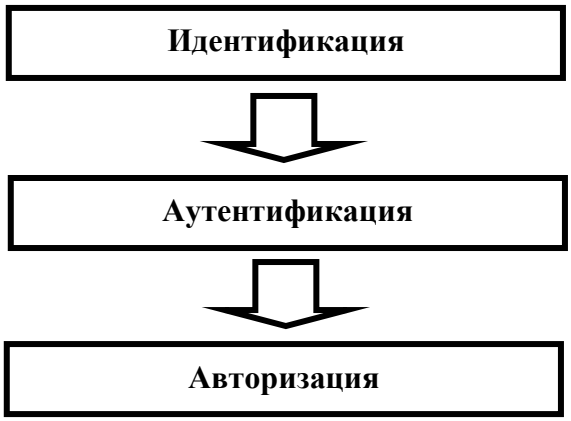
Бутунлик (рухсатсиз ёзишнинг мумкин эмаслиги) хусусияти асосида маълумотни узатиш давомида унга ўзгартириш киритилганлиги ёки киритилмаганлиги аниқланади. Ушбу хусусият бошқача қилиб айтилганда, маълумотни бузғунчи томонидан ўзгартирилган (алмаштирилган, ўчириб ташланган)лигини аниқлашни билдиради. Ахборотнинг ушбу хусусияти

[1] Stamp Mark. Information security: principles and practice. 2,3 – c.

криптографик ҳимоя усуллари асосида амалга оширилади. Ҳозирда криптографик хэш функциялар асосида маълумотнинг бутунлигини таъминлаш усуллари амалиётда кенг қўлланилади.

Фойдаланувчанлик хусусияти ахборотдан исталган вақт доирасида фойдаланиш имконияти мавжудлиги билан белгиланади. Ушбу хусусият очиқ турдаги маълумот учун дастлабки талаб этиладиган талабдир. Ушбу хусусиятни бузилишига олиб келувчи ҳужум усулларидан бири DOS (Denial of Service) ёки унинг шаклантирилган кўриниши DDOS (Distributed denial of Service) саналиб, ушбу ҳужум усули тизимни фойдаланувчанлик хусусиятини бузилишига олиб келади.

Ушбу учта хусусият ахборот ҳимоясининг асосий ташкил этувчилари саналиб, ахборотни ҳимоялаш дэганда асосан шу учта хусусиятни таъминлаш тушинилади. Аммо ушбу учта хусусият тўлиқ бажарилиши учун бир нечта бажарилиши мумкин бўлган ишлар талаб этилади. Бошқача қилиб айтганда ушбу учта хусусиятни бажаришдан олдин, қуйида келтирилган амалиётларни бажаришга тўғри келади (1.3-расм).



1.3-расм. Фойдаланишни бошқариш

Идентификация – бу фойдаланувчини тизимга ўзини танитиш жараёни бўлиб, унда фойдаланувчи номидан (логин), махсус шахсий карталардан ёки биометрик хусусиятларидан фойдаланиш мумкин.

Аутентификация – бу фойдаланувчиларни ҳақиқийлигини текшириш жараёни бўлиб, жараёни натижасида фойдаланувчи тизимдан фойдаланиш учун рухсат олади ёки олмайди.

Авторизация – бу фойдалувчига тизим томонидан берилган ҳуқуқлар тўплами бўлиб, фойдаланувчини тизим доирасида қилиши мумкин бўлган вазифаларини белгилайди.

1.3. Ахборот хавфсизлиги сиёсати

Ахборот хавфсизлиги сиёсати – ташкилот ўз фаолиятида риоя қиладиган ахборот хавфсизлиги соҳасидаги ҳужжатланган қоидалар, муолажалар, амалий усуллар ёки амал қилинадиган принциплар мажмуи саналиб, у асосида ташкилотда ахборот хавфсизлиги таъминланади.

Ахборот хавфсизлигининг сиёсатини ишлаб чиқишда, аввало ҳимоя қилинувчи объект ва унинг вазифалари аниқланади. Сўнгра душманнинг бу объектга қизиқиши даражаси, ҳужумнинг эҳтимолли турлари ва кўриладиган зарар баҳоланади. Ниҳоят, мавжуд қарши таъсир воситалари етарли ҳимояни таъминламайдиган объектнинг заиф жойлари аниқланади.

Самарали ҳимоя учун ҳар бир объект мумкин бўлган таҳдидлар ва хужум турлари, махсус инструментлар, қуроллар ва портловчи моддаларнинг ишлатилиши эҳтимоллиги нуқтаи назаридан баҳоланиши зарур. Таъкидлаш лозимки, нияти бузуқ одам учун энг қимматли объект унинг эътиборини тортади ва эҳтимолли нишон бўлиб хизмат қилади ва унга қарши асосий кучлар ишлатилади. Бунда, хавфсизлик сиёсатининг ишлаб чиқилишида ечими берилган объектнинг реал ҳимоясини таъминловчи масалалар ҳисобга олиниши лозим.

Қарши таъсир воситалари ҳимоянинг тўлиқ ва эшелонланган концепциясига мос келиши шарт. Бу дэгани, қарши таъсир воситаларини марказида ҳимояланувчи объект бўлган концентрик доираларда жойлаштириш лозим. Бу ҳолда душманнинг исталган объектга йўли ҳимоянинг эшелонланган тизимини кесиб ўтади. Мудофаанинг ҳар бир чэгараси шундай ташкил қилинадики, қўриқлаш ходимининг жавоб чораларини кўришига етарлича вақт мобайнида хужумчини ушлаб туриш имкони бўлсин.

Сўнгги босқичда қарши таъсир воситалари қабул қилинган ҳимоя концепциясига биноан бирлаштирилади. Бутун тизим ҳаёти циклининг бошланғич ва кутилувчи умумий нархини дастлабки баҳолаш амалга оширилади.

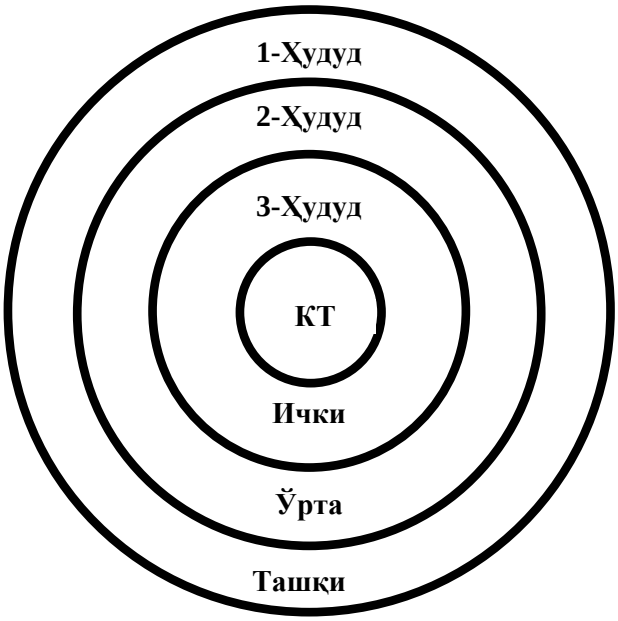
Агар бир бинонинг ичида турли ҳимоялаш талабларига эга бўлган объектлар жойлашган бўлса, бино отсекларга бўлинади. Шу тариқа умумий назоратланувчи макон ичида ички периметрлар ажратилади ва рухсатсиз фойдаланишдан ички ҳимоя воситалари яратилади. Периметр, одатда, физик тўсиқлар орқали аниқланиб, бу тўсиқлардан ўтиш электрон усул ёки қўриқлаш ходимлари томонидан бажарилувчи махсус муолажалар ёрдамида назоратланади.

Умумий чэгарага ёки периметрга эга бўлган бинолар гуруҳини ҳимоялашда нафақат алоҳида объект ёки бино, балки унинг жойланиш жойи

ҳам ҳисобга олиниши зарур. Кўп сонли бинолари бўлган ер участкалари хавфсизликни таъминлаш бўйича умумий ёки қисман мос келадиган талабларга эга бўлади, баъзи участкалар эса периметр бўйича тўсиққа ва ягона йўлакка эга. Умумий периметр ташкил этиб, ҳар бир бинодаги ҳимоя воситаларини камайтириш ва уларни фақат хужум қилиниши эхтимоли кўпроқ бўлган мухим объектларга ўрнатиш мумкин. Худди шу тариқа участкадаги хар бир иморат ёки объект хужумчини ушлаб қолиш имконияти нуқтаи назаридан бахоланади.

Юқоридаги келтирилган талаблар тахлили кўрсатадики, уларнинг барчаси ахборотни ишлаш ва узатиш қурилмаларидан хуқуқсиз фойдаланиш, ахборот элтувчиларини ўгирлаш ва саботаж имкониятини йўл қўймасликка олиб келади.

Бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага ўтиш йўлида жойлаштирган холда концентрик ҳалқа кўринишида ташкил этиш мақсадига мувофиқ хисобланади (1.4-расм).



1-ҳудуд. Компьютер тармоғи (КТ) хавфсизлигининг ташқи зонаси
Таъминланиши:
физик тусиқлар
периметр бўйлаб ўтиш жойлари
худудга кириш назоратининг ноавтоматик тизими
2-ҳудуд. КТ хавфсизлигининг ўртадаги зонаси
Таъминланиши:
эшиклари электрон ҳимояланган назорат пунктлари
видеокузатиш
бўм бўш зоналарни чиқариб ташлаш
3-ҳудуд. КТ хавфсизлигининг ички зонаси
Таъминлаш:
шахсий компьютерга фойдаланиш фақат назорат тизими орқали идентификациялашнинг биометрик тизими

1.4-расм. Бинодаги компьютер тизимининг хавфсизлик тизими

Ахборот хизмати бинолари ва хоналарига киришнинг назорати масаласига келсак, асосий чора-нафақат бино ва хоналарни, балки воситалар комплексини, уларнинг функционал вазифалари бўйича ажратиш ва

изоляциялаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тўлдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш химояланувчи объектнинг мухимлигини, воситаларга кетадиган харажатни ва назорат тизими ишончлилиги даражасини, ижтимоий жихатларни ва инсон нафси бузуқлигини олдиндан ўрганишга асосланади. Бармоқ, кафтлар, кўз тўр пардаси, қон томирлари излари ёки нутқни аниқлаш каби биометрик индентификациялаш ишлатилиши мумкин. Шартнома асосида техник воситаларга хизмат кўрсатувчи ходимларни объектга киритишнинг махсус режими кўзда тутилган. Бу шахслар идентификацияланганларидан сўнг объектга кузатувчи хамрохлигида киритилади. Ундан ташқари уларга аниқ келиш режими, маконий чэгараланиш, келиб-кетиш вақти, бажарадиган иш характери ўрнатилади.

Нихоят, бино периметри бўйича бостириб киришни аниқловчи турли датчиклар ёрдамида комплекс кузатиш ўрнатилади. Бу датчиклар объектни қўриқлашнинг марказий пости билан богланган ва бўлиши мумкин бўлган бостириб кириш нуқталарини, айниқса ишланмайдиган вақтларда, назорат қилади.

Вақти-вақти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошқа чиқиш йўлларининг физик химояланиш ишончлилигини текшириб туриш лозим.

Хар бир хонага ичидаги нарсанинг мухимлилигига боглиқ фойдаланиш тизимига эга бўлган зона сифатида қаралади. Кириш-чиқиш хуқуқи тизими шахс ёки объект мухимлигига боглиқ холда селекцияли ва даражалари бўйича рутбаланган бўлиши шарт. Кириш-чиқиш хуқуқи тизими марказлашган бўлиши мумкин (рухсатларни бошқариш, жадвал ва календар режаларининг режалаштирилиши, кириш-чиқиш хуқуқининг ёзма намуналари ва ҳ.).

Назорат тизимини вақти-вақти билан текшириб туриш ва уни доимо ишга лаёқатли холда сақлаш лозим. Буни ихтисослашган бўлинмалар ва назорат органлари таъминлайди.

Шахсий компьютер ва физикавий химоя воситалари каби ўлчамлари кичик асбоб-ускуналарни кўзда тутиш мумкин.

Юқорида келтирилганларга хулоса қилиб, компьютер тармоқларини химоялашда ахборот хавфсизлиги сиёсати қандай аниқланиши хусусида сўз юритамиз. Одатда кўп сонли фойдаланувчиларга эга бўлган корпоратив компьютер тармоқлари учун махсус “Хавфсизлик сиёсати” деб аталувчи,

тармоқда ишлашни маълум тартиб ва қоидаларга бўйсиндирувчи (регламентловчи) ҳужжат тузилади.

Сиёсат одатда икки қисмдан иборат бўлади: умумий принциплар ва ишлашнинг муайян қоидалари. Умумий принциплар Internetда хавфсизликка ёндашишни аниқласа, қоидалар нима рухсат этилишини ва нима рухсат этилмаслигини белгилайди. Қоидалар муайян муолажалар ва турли қўлланмалар билан тўлдирилиши мумкин.

Одатда хавфсизлик сиёсати тармоқ асосий сервисларидан (электрон почта, WWW ва ҳак.) фойдаланишни регламентлайди ҳамда тармоқдан фойдаланувчиларни улар қандай фойдаланиш ҳуқуқига эга эканликлари билан таништиради. Бу эса ўз навбатида фойдаланувчиларни аутентификациялаш муолажасини аниқлайди.

Бу ҳужжатга жиддий ёндашиш лозим. Ҳимоянинг бошқа барча стратегияси хавфсизлик сиёсатининг қатъий бажарилиши тахминига асосланган. Хавфсизлик сиёсати фойдаланувчилар томонидан кўпгина маломат орттирилишига сабаб бўлади, чунки унда фойдаланувчига маън этилган нарсалар очиқ-ойдин ёзилган. Аммо хавфсизлик сиёсати расмий ҳужжат, у бир томондан Internet тақдим этувчи сервисларда ишлаш зарурияти, иккинчи томондан мос мутахассис-профессионаллар тарафидан ифодаланган хавфсизлик талаблари асосида тузилади.

Автоматлаштирилган комплекс ҳимояланган ҳисобланади, қачонки барча амаллар объектлар, ресурслар ва муолажаларни бевосита ҳимоясини таъминловчи қатъий аниқланган қоидалар бўйича бажарилса (1.5-расм).

1.5-расм. Ахборот хавфсизлиги сиёсатини таъминлашнинг асосий қоидалари

Химояга қўйиладиган талабларнинг асосини тахдидлар рўйхати ташкил этади. Бундай талаблар ўз навбатида химоянинг зарурий вазифалари ва химоя воситаларини аниқлайди.

1.4. Ахборотни ҳимоялаш усуллари

Демак, компьютер тармоида ахборотни самарали химоясини таъминлаш учун химоя тизимини лойиҳалаш ва амалга ошириш уч босқичда амалга оширилиши керак:

- хавф-хатарни тахлиллаш;
- хавфсизлик сиёсатини амалга ошириш;
- хавфсизлик сиёсатини мададлаш.

Биринчи босқичда компьютер тармоининг заиф элементлари тахлилланади, тахдидлар аниқланади ва бахоланади, химоянинг оптимал воситалари танланади. Хавф-хатарни тахлиллаш хавфсизлик сиёсатини қабул қилиш билан тугалланади.

Иккинчи босқич - хавфсизлик сиёсатини амалга ошириш молиявий харажатларни хисоблаш ва масалаларни ечиш учун мос воситаларни танлаш билан бошланади. Бунда танланган воситалар ишлашининг ихтилофли эмаслиги, воситаларни етказиб берувчиларнинг обрўси, химоя механизмлари ва бериладиган кафолатлар хусусидаги тўла ахборот олиш имконияти каби омиллар хисобга олиниши зарур. Ундан ташқари, ахборот хавфсизлиги бўйича асосий қоидалар акс эттирилган принциплар хисобга олиниши керак.

Учинчи босқич - хавфсизлик сиёсатини мададлаш босқичи энг мухим дисобланади. Бу босқичда ўтказиладиган тадбирлар нияти бузуқ одамларнинг тармоққа бостириб киришини доимо назорат қилиб туришни, ахборот объектини х,имоялаш тизимидаги “раҳна”ларни аниқлашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш холларини ҳисобга олишни талаб этади. Тармоқ хавфсизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури бўйнида бўлади. У хавфсизликнинг муайян тизими бузилишининг барча холларига оператив муносабат билдириши, уларни тахлиллаши ва молиявий воситаларнинг максимал тежалишини хисобга олган холда химоянинг зарурий аппарат ва дастурий воситаларидан фойдаланиши шарт.

Ахборотни ҳимоялашда ҳозирда қатор ҳимоя усулларидан фойдаланилиб, умуммий ҳолда улар қуйидагиларга бўлинади:

- ахборотнинг ҳуқуқий ҳимояси;
- ахборотнинг инжинер – техник ҳимояси;
- ахборотнинг ташкилий ҳимояси;
- ахборотнинг дастурий ҳимояси;
- ахборотнинг апарат ва апарат-дастурий ҳимояси.

Ҳимоя усулларининг турланиши уларда фойдаланилган воситалар ва ёндошишларга асосланади. Ҳимоя усулларининг танлаш эса ўз навбатида ташкилотда ишлаб чиқилган ахборот хавфсизлиги сиёсатига кўра амалга

оширилади. Одатда ахборот хавфсизлигини таъминлашда барча ҳимоя усулларидан комплекс тарзда фойдаланиш орқали эришилади.

Назорат саволлари

1. Ахборот хавфсизлигини ташкил этувчилари.
2. Ахборот хавфсизлигида мавжуд муаммолар ва уларни сабаблари.
3. Ахборот хавфсизлигида заифлик тушунчаси.
4. Ахборот хавфсизлигида таҳдид тушунчаси.
5. Ахборот хавфсизлигида ҳужум тушунчаси.
6. Ахборот хавфсизлиги сиёсати.
7. Ахборотни ҳимоялаш усуллари.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.

2-мавзу. Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.

Режа:

1. Ахборотни ҳимоялашда криптографиянинг ўрни.
2. Симметрик шифрлаш алгоритмлари.
3. Ассиметрик шифрлаш алгоритмлари.
4. Хэш функциялар ва ЭРИ алгоритмлари.

Таянч иборалар: *криптология, криптография, криптотаҳлил, шифрлаш, дешифрлаш, хэш функция, калит, электрон рақамли имзо, симметрик шифрлаш, ассиметрик шифрлаш, очиқ калит, махфий калит, коллизия, бутунлик, махфийлик, оқимли шифрлаш, блокли шифрлаш, маълумотни аутентификациялаш тизимлари.*

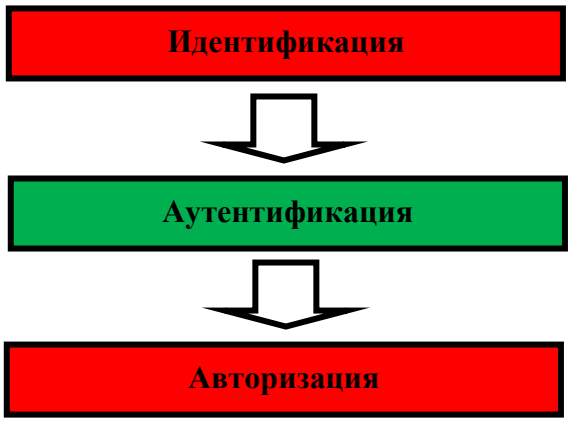
2.1. Ахборотни ҳимоялашда криптографиянинг ўрни

Электрон кўринишдаги маълумотларни ҳажмини ортиши, уни сақлаш билан боғлиқ бўлган муаммолар ҳажмини ҳам ортишига олиб келади. Ушбу муаммоларни ҳал қилишда мавжуд бўлган усуллар эса, кундан-кунга янгиланаверади. Шунга қармасдан ахборот хавфсизлигини таъминлашда қадимда ҳам фойдаланилаган ва ҳозирда ҳам фойдаланилаётган усуллардан бири бу – криптографик ҳимоя усулларидир. Криптографик ҳимоя усуллари ўзининг ишончлилиги, самарадорлиги ва фойдаланиш даражаси қамрови кенглиги билан бошқа усуллардан фарқ қилади. Ҳозирда ахборот хавфсизлигини таъминлашнинг ҳар бир жабҳасида криптографик усуллардан фойдаланилмоқда. Бу эса унинг муҳимлигидан дарак беради.

Умумий ҳолда ахборот хавфсизлиги консепсияси учта ташкил этувчидан иборатлигини эътиборга олсак, ахборот хавфсизлигини таъминлаш дэганда маълумотнинг қуйидаги учта хусусиятини таъминлаш тушуниш мумкин. Қуйида келтирилган 2.1- расмда ушбу учта хусусиятни таъминлашда криптографик усулларнинг тутган ўрни келтирилган.

2.1-расм. Ахборот хавфсизлиги хусусиятлари

Ушбу учта хусусият ахборот ҳимоясининг асосий ташкил этувчилари саналиб, ахборотни ҳимоялаш дэганда асосан шу учта хусусиятни таъминлаш тушинилади. Аммо ушбу учта хусусият тўлиқ бажарилиши учун бир нечта бажарилиши мумкин бўлган ишлар талаб этилади. Бошқача қилиб айтганда ушбу учта хусусиятни бажаришдан олдин, қуйида келтирилган амалиётларни бажаришга тўғри келади. 2.2-расмда келтирилган жараёнларда криптографик ҳимоя усулларидан фойдаланиш даражаси эса қуйидагича.



2.2-расм. Фойдаланишни бошқариш

Аутентификация жараёни фойдаланувчини тизимдан фойдаланиш учун уни ҳақиқийлигини текшириш саналиб, 2-расмда келтирилганидек, аутентификациялаш жараёни криптографик усуллардин фойдаланилган ҳолатда амалги оширилиб, бунда криптографик калит узутиш протоколлари, аутентификациялаш протоколлари, маълумотни аутентификациялаш кодлари ва ҳак. фойдаланилади. Ушбу жараёнда ҳам криптографик ҳимоя усуллари ўзининг бардошлиги, ишончлилиги билан ажралиб туради.

Криптография - ахборотларни аслидан ўзгартирилган ҳолатга акслантириш услубларини топиш ва такомиллаштириш билан шуғилланади. Дастлабки системалашган криптографик услублар эрамиз бошида, Юлий Цезарьнинг иш юритиш ёзишмаларида учрайди. У, бирор маълумотни маҳфий ҳолда, бирор кишига етказмоқчи бўлса, алфавитнинг биринчи ҳарфини алфавитнинг тўртинчи ҳарфи билан, иккинчисини бешинчиси билан ва ҳоказо шу тартибда алмаштириб матннинг асли ҳолатидан шифрланган матн ҳолатига ўтказган.

Ахборотларнинг мухофазаси масалалари билан криптология (*kryptos*- маҳфий, **logos**- илм) фани шуғилланади. Криптология мақсадлари ўзаро қарама-қарши бўлган икки йўналишга эга: – *криптография* ва *криптоанализ.*

Криптографиянинг очиқ маълумотларни шифрлаш масалаларини математик услублари билан шуғилланиши тўғрисида юқорида айтиб ўтилди.

Криптоанализ эса шифирлаш услубини (калитини ёки алгоритмини)

билмаган ҳолда шифрланган маълумотни асли ҳолатини (мос келувчи очиқ маълумотни) топиш масалаларини ечиш билан шуғилланади.

Ҳозирги замон криптографияси қуйидаги тўртта бўлимни ўз ичига олади:

1) Симметрик криптотизимлар.
2) Очиқ калит алгоритмига асосланган криптотизимлар.
3) Электрон рақамли имзо криптотизимлари.
4) Криптотизимлар учун криптобардошли калитларни ишлаб чиқиш ва улардан фойдаланишни бошқариш.

Шифрлаш тизимлари фойдаланиладиган калитлар сонига кўра икки қисмга бўлинади: **симметрик** ва **асимметрик** - очиқ калитли.

Симметрик криптотизимларда шифрлаш учун ҳам ва дешифрлаш учун ҳам бир ҳил калитдан фойдаланилади.

Очиқ калитли криптотизимларда иккита калитдан фойдаланилади -– ўзаро математик боғлиқ бўлган очиқ ва ёпиқ калитлардан. Бунда маълумотлар ҳаммага маълум бўлган маълумот юборилаётган шахснинг очиқ калити билан шифрланади ва фақат маълумот юборилаётган шахснинг ўзигагина маълум бўлган ёпиқ калит билан дешифрланади.

Калитларни тақсимлаш ва бошқариш – криптобардошли калитларни ишлаб чиқиш (ёки яратиш), уларни муҳофазали сақлаш, ҳамда калитларни фойдаланувчилар орасида муҳофазаланган ҳолда тақсимлаш жараёнларини ўз ичига олади.

Электрон рақамли имзо - электрон матнга илова қилинадиган криптографик алмаштиришдан иборат бўлиб, шу электрон матн жўнатилган шахсга қабул қилинган электрон матннинг ва матинни рақамли имзоловчининг ҳақиқий ёки ноҳақиқий эканлигини аниқлаш имконини беради.

2.2. Симметрик шифрлаш алгоритмлари

Шифрлаш алгоритмлари асосларини очиқ маълумотни ифодаловчи алфавит белгиларини ёки белгилар бирикмаларини шифрмаълумотни ифодаловчи алфавит белгиларига ёки белгилар бирикмаларига акслантирувчи математик моделлар ташкил этилади. Шунинг учун ҳам шифрлаш алгоритмларини синфларга ажратишнинг бошланғич босқичи, улар негизидаги акслантириш турлари асосида амалга оширилади. Агар шифрлаш жараёнида очиқ маълумот алфавити белгилари шифр маълумот алфавити белгиларига алмаштирилса, бундай акслантиришга асосланган шифрлаш

алгоритми ўрнига қўйиш шифрлаш синфига киради. Агар шифрлаш жараёнида очиқ маълумот алфавити белгиларининг ўринлари алмаштирилса, бундай шифрлаш алгоритми ўрин алмаштириш шифрлаш синфига киради. Кўриниб турибдики, ўрин алмаштириш шифрлаш алгоритмларида очиқ маълумотни ташкил этувчи алфавит белгиларининг маъноси шифр маълумотда ҳам ўзгармасдан қолади. Аксинча, ўрнига қўйиш шифрлаш алгоритмларида шифрмаълумотни ташкил этувчи алфавит белгилари маъноси очиқ маълумотни ташкил этувчи алфавит белгиларининг маъноси билан бир хил бўлмайди. Шифрлаш жараёнида ўрнига қўйиш ва ўрин алмаштириш акслантиришларининг комбинацияларидан биргаликда фойдаланилса, бундай шифрлаш алгоритми композицион шифрлаш туркумига киради. Демак, шифрлаш алгоритмлари акслантириш турларига қараб *ўрнига қўйиш, ўрин алмаштириш ва композицион* шифрлаш синфига бўлинади.

Шифрлаш алгоритмларига қўйиладиган асосий талаблар қуйидагилардир:

– шифрланган ахборотни ўзгартириб қўйиш ёки шифрни бузиб очишга йўл қолдирмаслик;

– ахборот ҳимояси фақат калитнинг маълумлигига боғлиқ бўлиб, алгоритмнинг маълум ёки номаълумлигига боғлиқ бўлмаслик (О. Керкгофф қоидаси);

– дастлабки (шифрланадиган) ахборотни ёки калитни би¬роз ўзгартириш шифрланган матнни бутунлай ўзгартириб юбо¬риши лозим (К. Шеннон тамойили, “ўпирилиш” ҳодисаси);

– калит қийматлари соҳаси шундай катта бўлиши керакки, унда калит қийматларини бир бошдан кўриб чиқиш асосида шифрни бузиб очиш имкони бўлмаслиги лозим;

– алгоритм иқтисодий жиҳатдан тежамли ва етарли тез¬корликка эга бўлиши лозим;

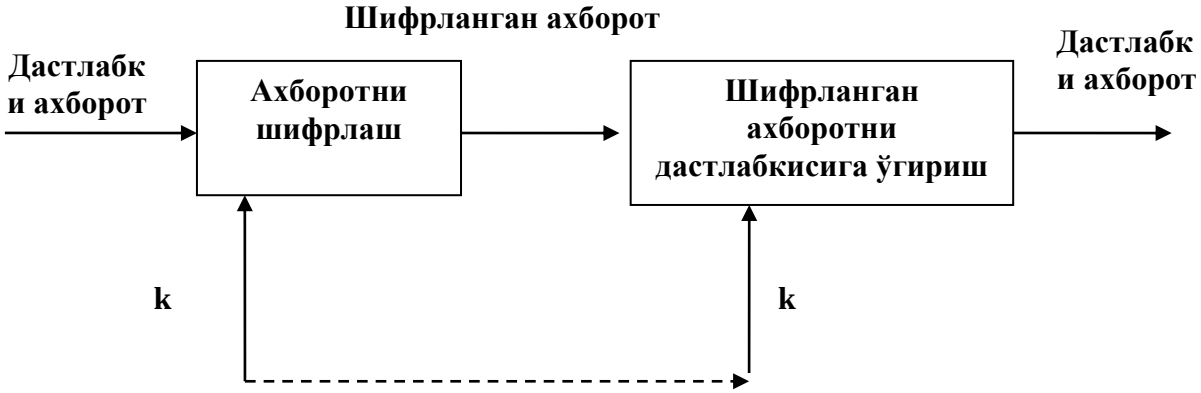
– шифрматнни бузиб очишга кетадиган сарф-ҳаражатлар ахборот баҳосидан юқори бўлиши лозим.

Шифрлаш алгоритмлари, калитлардан фойдаланиш турларига кўра, симметрик ва асимметрик синфларга бўлинади. Агар шифрлаш ва дешифрлаш жараёнлари бир хил калит билан амалга оширилса, бундай шифрлаш алгоритми симметрик шифрлаш алгоритми синфига киради. Агар шифрлаш жараёни бирор k_1 калит билан амалга оширилиб, дешифрлаш жараёни $k_2 \neq k_1$ бўлган k_2 калит билан амалга оширилиб, k_1 калитни билган ҳолда k_2 калитни топиш ечилиши мураккаб бўлган масала билан

боғлиқ бўлса, бундай шифрлаш алгоритми асимметрик шифрлаш алгоритми синфига таалуқли бўлади.

Симметрик шифрлаш алгоритмлари маълумотни шифрлашда ва дешифрлашда айнан бир хил калитдан фойдаланади. Бундай криптотизимда калит алоқанинг фақат иккала томони учун маълум, лекин икковларидан бошқа ҳеч кимга ошкора бўлмаслиги, яъни ўзгалардан мутлақо махфий бўлиши шарт. Бундай тизимнинг хавфсизлиги асосан ягона махфий калитнинг ҳимоя хоссаларига боғлиқ.

Криптотизимдан фойдаланишда матн муаллифи шифрлаш алгоритми ва шифрлаш калити воситасида аввало дастлабки матнни шифрланган матнга ўгиради. Матн муаллифи уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқарув тизимига ҳожат ҳам бўлмайди) уни сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса, сақлаб қўйилган ахборотнинг яхлитлигига ишонч ҳосил бўлади. Акс ҳолда ахборот бутунлиги бузилган бўлиб чиқади (2.3-расм). Бу ерда k – юборувчи ва қабул қилувчининг симметрик махфий калити.



2.3-расм. Симметрик криптотизимларда ахборот алмашиш

Агар шифрланган матн уни яратган кимсадан ўзга қонуний фойдаланувчига (олувчига) мўлжалланган бўлса, у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан унга аввалдан маълум бўлган шифрни очиш калити ва алгоритми воситасида дастлабки матнга ўгирилади.

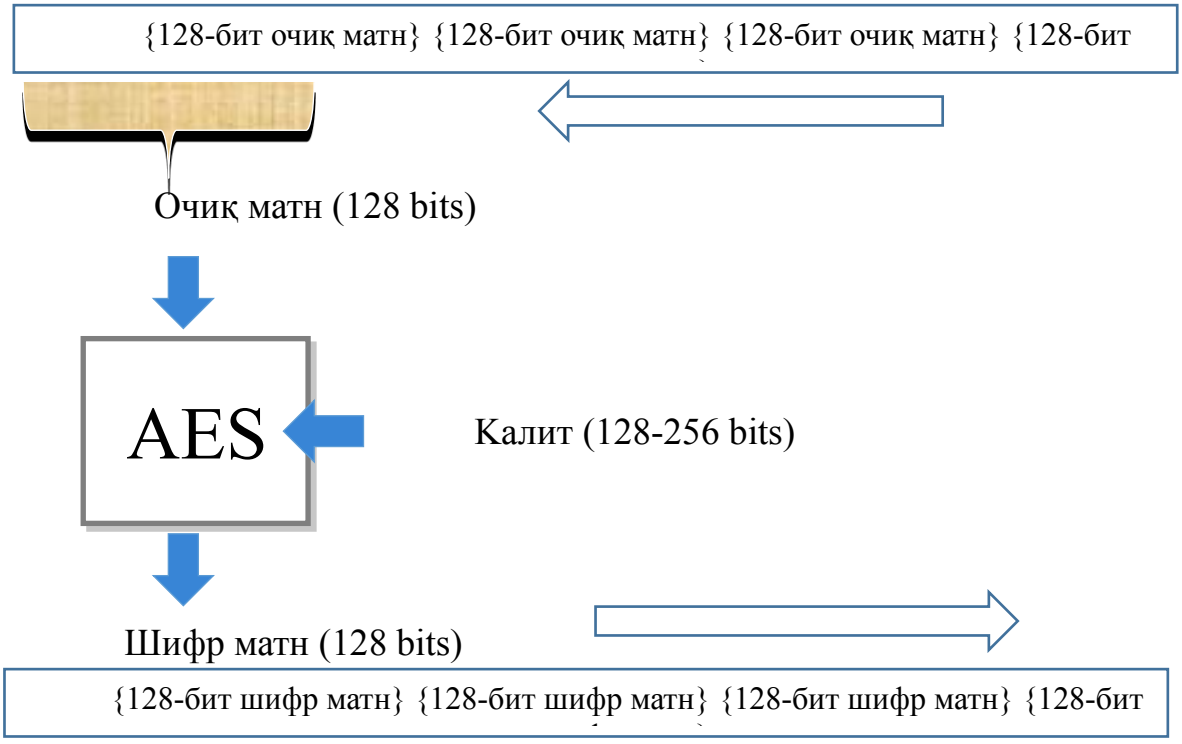
Симметрик криптотизимларда ахборот алмашиш уч босқичда юз беради:

– ахборот жўнатувчи уни олувчига махфий тарзда махфий калитни, яъни икковларидан ўзга ҳеч кимга маълум бўлмаган ўзаро махфий калитни топширади;

– жўнатувчи ўзаро махфий калит билан ахборотни шифрлаб уни олувчига жўнатади;

– қабул қилиб олувчи ахборотни олиб унинг шифрини ўзаро махфий калит билан очади. Умумун олганда иккала томон бу калитдан бир неча бор қайта фойдаланишлари мумкин.

Агар шифрлаш жараёни очиқ маълумот алфавити белгиларининг икки ва ундан ортиқ чекли сондаги бирикмаларини шифрмаълумот алфавити белгиларининг бирикмаларига акслантиришга асосланган бўлса, бундай шифрлаш алгоритми **блокли шифрлаш** синфига киради (2.4-расмда AES мисолида блокли шифрлаш алгоритми келтирилган).



2.4-расм. Блокли шифрлаш

Криптографияда блокли шифрлаш алгоритмлари кенг қўлланилиб, моҳият жихатдан қуйидагича. Масалан, очиқ матн 128-бит узунликка эга бўлган қисмларга ажратилади ва ҳар бир қисмлар устида алоҳида-алоҳида амаллар бажарилади. Кирувчи ушбу қисм устида махфий калит асосида амаллар бажарилади ва натижада 128-битли шифр матн олинади.

Блокли шифрлаш алгоритмлари яратилиш асосига кўра қуйидаги турларга бўлинади:

- Ўзгартириш-алмаштириш тармоқлари (Substitution-permutation networks);
- Фейстел тармоғига асосланган (Feistel ciphers);
- Лаи-Массей шифрлари (Lai-Massey ciphers);

Блокли шифрлаш алгоритмлари ишлаш режимлари. Симметрик шифрлаш алгоритмларида хавфсизлик нуқтаи-назаридан криптографик

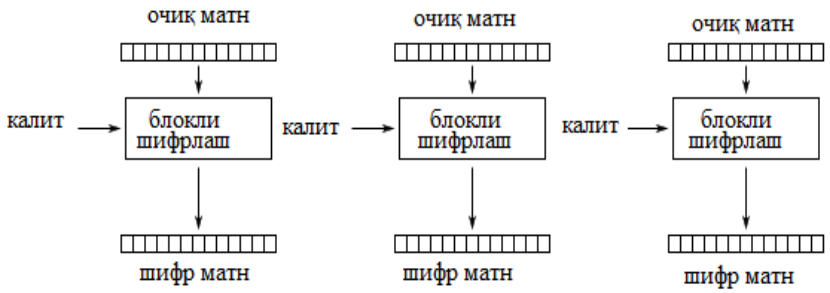
тизимлардан маълум кетма-кетликларга асосланиб фойдалиниш мавжуд. Бу тоифадаги алгоритмлар блокли шифрлаш алгоритимлари моделлари саналади.

Ушбу алгоритмларда амалга оширувчи вектор (initialization vector, IV) дан фойдаланилади. Амалга оширувчи вектор маълум битлар кетма-кетлигидан иборат бўлиб, очиқ матнга ёки калитга маълум алгоритм бўйича қўшилади. Бу катталик калитдан фарқли саналиб, одатда зарур бўлса ҳам сир сақланмайди. [1]

Ҳозирда қуйидаги моделлар кенг қўлланилади:

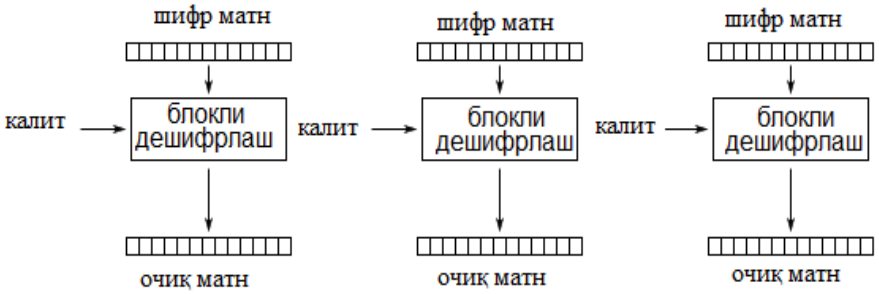
– Electronic codebook (ECB);
– Cipher-block chaining (CBC);
– Propagating cipher-block chaining (PCBC);
– Cipher feedback (CFB);
– Output feedback (OFB);
– Counter (CTR).

Electronic codebook (ECB). Дастлабки содда моделлардан бири бўлиб, очиқ мант блокларга бўлинади ва ҳар бир блок устида калит билан амаллар бажарилади (2.5, 2.6-расмлар).



Electronic codebook (ECB) модулда шифрлаш

2.5-расм. ECB модулда шифрлаш

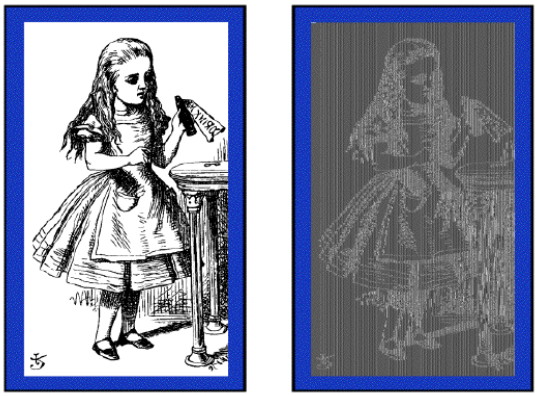


Electronic codebook (ECB) модулда дешифрлаш

2.6-расм. ECB модулда дешифрлаш

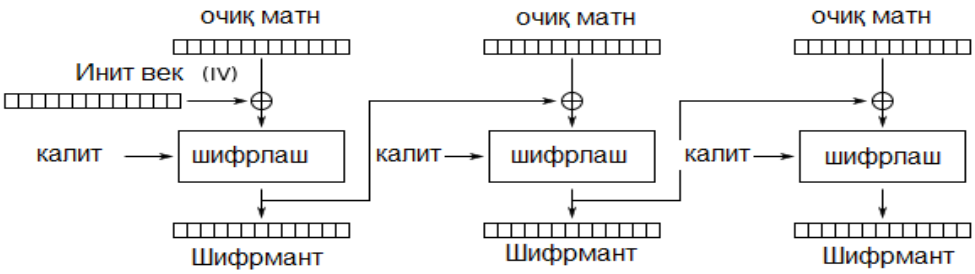
[1] Stamp Mark. Information security: principles and practice. 72 – c.

Ушбу моделнинг асосий камчилиги бир хил очиқ матн бир хил шифр матнга алмашади. Булардан ташқари бу модел матнни яшириш каби вазифаларни бажармайди. Шуларни ҳисобга олган ҳолда ўта махфий ахборотлар билан ишлашда ушбу моделдан фойдаланиш тавсия этилмайди (2.7 - расм). Дастурий томондан амалга оширишда параллел ҳисоблашларга асосланган ҳолда шифрлашни амалга ошириш имконияти мавжуд. [1]



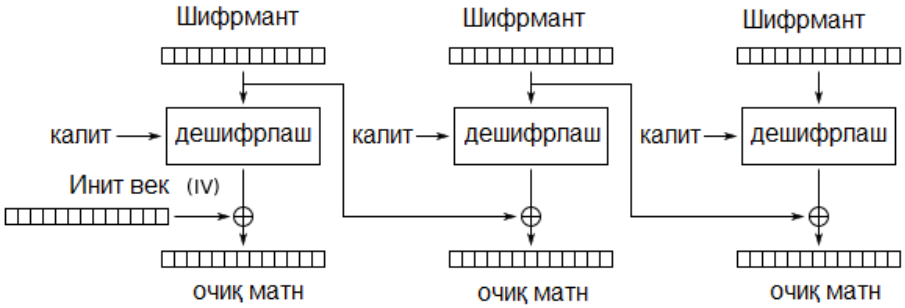
2.7-расм. ECB режимининг заифлиги

Cipher-block chaining (CBC). Ушбу модел 1976 йил IBM томонидан ишлаб чиқилган бўлиб, дастлаб очиқ матнга бошланғич вектор қўшилиб, натижа калит ёрдамида шифрланади (2.8,2.9 -расмлар).



2.8-расм. CBC моделда шифрлаш

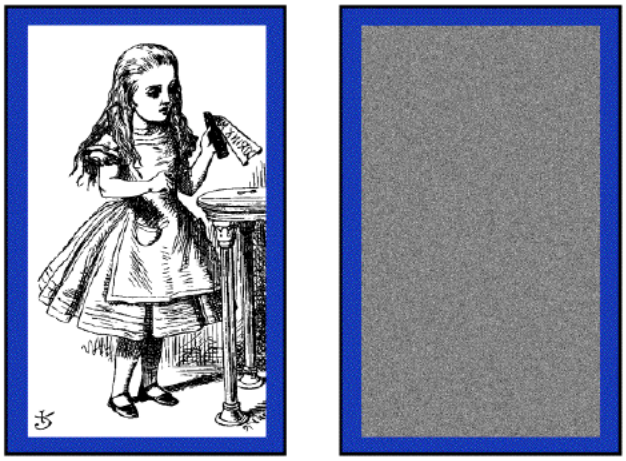
Дешифрлашда шифрматн калит ёрдамида дешифрланиб, бошланғич векторга қўшилади ва натижада очиқ матн олинади.



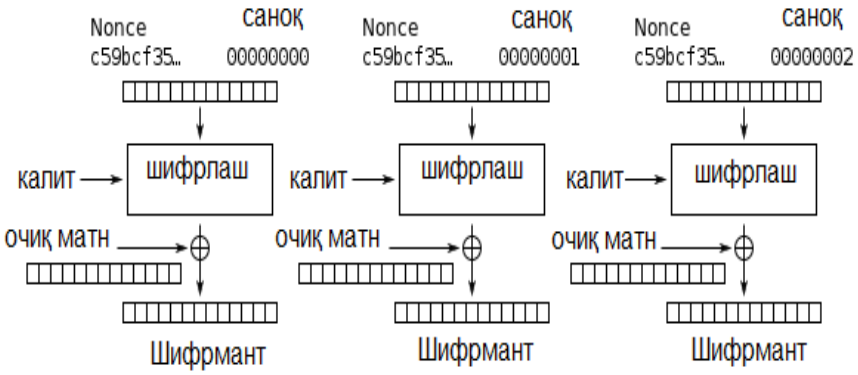
2.9-расм. CBC моделда дешифрлаш

[1] Stamp Mark. Information security: principles and practice. 73 – c.

Ушбу режимда шифрлашда бир хил маълумот блоклари ҳар хил шифрматн блокларига алмаштирилади. Бу эса шифрматнга қараб таҳлил қилиш усулини олдини олишга ёрдам беради (2.10 - расм). Камчилиги эса тизимни параллел тарзда амалги ошириш мумкин эмас, сабаби кейинги босқич натижаси олдинги босқич натижасига боғлиқ.[1]



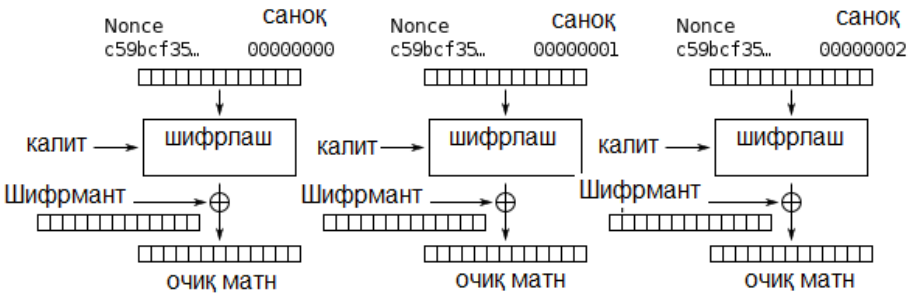
2.10 – расм. CBC режимининг афзаллиги



2.11-расм. CTR моделда шифрлаш

Counter (CTR). OFB модел каби ушбу моделда ҳам оқимли шифрлашда блокли мифрлашни амалга ошириш учун амалда фойдаланилади. Бу кейинги калит кетма-кетлиги санагич қийматини шифрлаш амали орқали амалга оширади. Санагич қиймати эса такрорланмайдиган алгоритм асосида ҳосил қилинади. Ушбу усул амалда кенг фойдаланилиб, криптобардошлиги билан ва параллел ҳисоблаш имконини бериши билан белгиланади (2.11,2.12-расмлар).

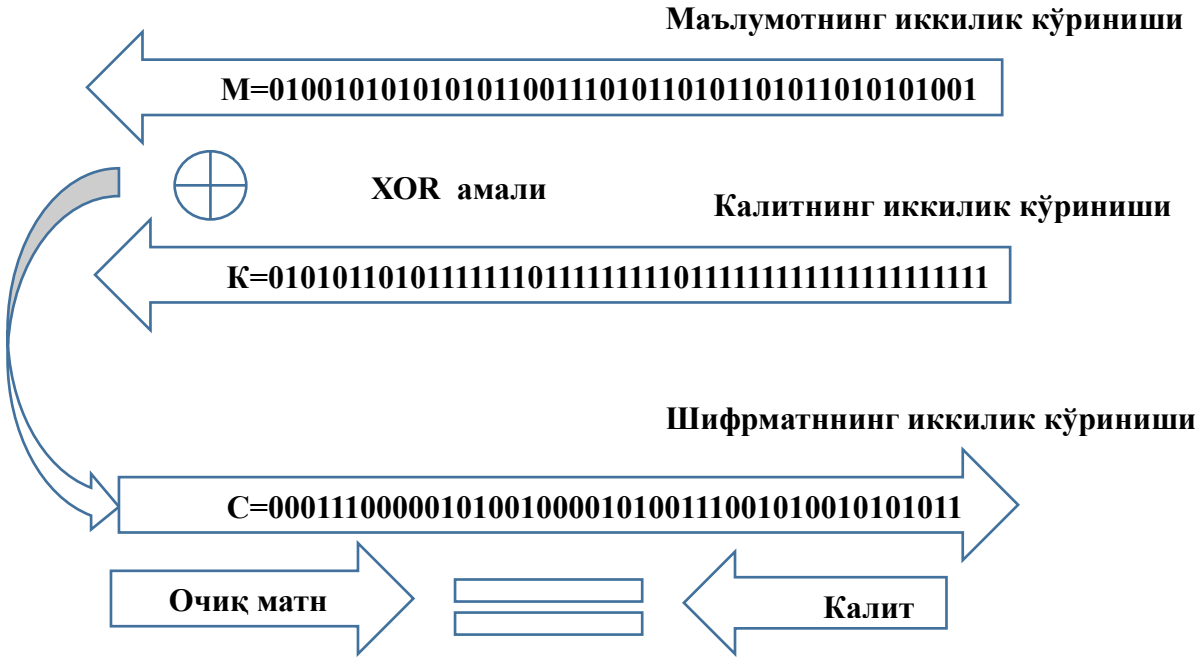
[1] Stamp Mark. Information security: principles and practice. 74 – c.



2.12-расм. CTR моделда дешифрлаш

Юқоридаги расмлардан кўриниб турибдики, баъзи шифрлаш режимларида ҳам шифрлаш ҳам дешифраш амаллари биргаликда амалга оширилса баъзида фақат шифрлаш амалидан фойдаланилади.

Симметрик оқимли шифрлаш алгоритмлари. Оқимли шифрлашда эса шифрлаш бирлиги бир бит ёки бир байт бўлади. Натижа одатда ундан олдин ўтган шифр оқимига боғлиқ бўлади. Бундай шифрлаш схемаси маълумотлар оқимини узатиш тизимларида қўлланилади, яъни бунда маълумотни узатиш ихтиёрий вақтда бошланиши ва тугатилиши мумкин.



2.13-расм. Оқимли шифрлаш тизими

Агар шифрлаш жараёни очиқ маълумотни ифодаловчи элементар (масалан: бит, ярим байт, беш бит, байт) белгиларни шифрмаълумотни ифодаловчи элементар белгиларга акслантириш асосида амалга оширилса, бундай шифрлаш алгоритми узлуксиз (оқимли) шифрлаш синфтуркумига киради. Ушбу тоифадаги шифрлаш алгоритмларининг умумий схемаси

қуйидагича (2.13-расм).[1]

Оқимли шифрлаш алгоритмлари олдин оммабоп саналган ва кичик имкониятга эга қурилмаларда хос бўлган. Оқимли шифрлаш алгоритмлари маълумот узунлигига тенг бўлган калит кетма-кетлигидан фойдаланганлиги сабабли ва ҳозирда компьютер техникаси имкониятини ортиши натижасида оқимли шифрлаш алгоритмлари ўрнини блокли шифрлаш алгоритмлари эгалламоқда.

Оқимли шифрлаш алгоритмларига мобил алоқа воситалари алоқа стандарти GSM (Global System for Mobile Communications) протоколида фойдаланилган A5 силжитиш регисторларига асосланган оқимли шифрлаш алгоритми, симсиз алоқа воситаларилариде мавжуд WEP протоколида фойдаланилган RC4 оқимли шифрлаш алгоритмларини мисол қилиб олишимиз мумкин.

2.3. Ассиметрик шифрлаш алгоритмлари

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очиқ калит ёрдамида шифрланса, махфий калит ёрдамида расшифровка қилинади. Асимметрик шифрлаш тизимларини очиқ калитли шифрлаш тизимлар деб хам 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 сохасидаги барча x учун $f_Z(x)$ функцияни осонгина олиш мумкин. Худди шу тариқа D_z алгоритми ёрдамида жоиз қийматлар сохасидаги барча y учун тескари функция $x=f^{-1}(y)$ ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар сохасидаги барча z ва деярли барча, y учун хатто E_z маълум бўлганида хам $f^{-1}(y)$ ни хисоблашлар ёрдамида топиб бўлмайди. Очиқ калит сифатида у 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 криптохимоясини соддалаштиради.

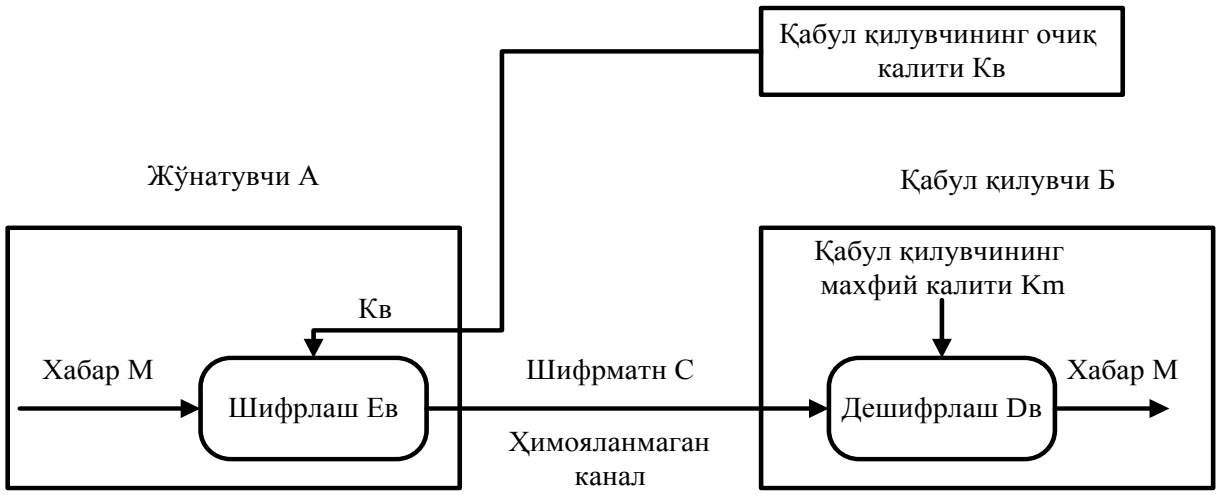
[1] Stamp Mark. Information security: principles and practice. 52 – c.

Асимметрик криптотизимларда ахборотни шифрлашда ва дешифрлашда турли калитлардан фойдаланилади:

- очиқ калит **К** ахборотни шифрлашда ишлатилади, махфий калит **к** дан хисоблаб чиқарилади;
- махфий калит **к**, 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 хар бирида бўлиши шарт.

Асимметрик шифрлашнинг умумлаштирилган схемаси 2.14-расмда келтирилган.



2.14-расм. Асимметрик шифрлашнинг умумлаштирилган схемаси

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_B абонент А га ва қолган абонентларга жўнатилади.

– А ва В абонентлар ўртасида ахборот алмашиш:

– абонент **А** абонент **В** нинг очиқ калити K_B ёрдамида ахборотни шифрлайди ва шифрматнни абонент В га жўнатади;

– абонент **В** ўзининг махфий калити k_B ёрдамида ахборотни дешифрлайди. Хеч ким (шу жумладан абонент А хам) ушбу ахборотни дешифрлай олмайди, чунки абонент В нинг махфий калити унда йўқ.

Асимметрик криптотизимда ахборотни химоялаш ахборот қабул

қилувчи калити k_B нинг махфийлигига асосланган.

Асимметрик криптотизимларнинг асосий хусусиятлари қуйидагилар:

1. Очиқ калитни ва шифр матнни химояланган канал орқали жўнатиш мумкин, яъни нияти бузуқ одамга улар маълум бўлиши мумкин.
2. Шифрлаш E_B:M → C ва расшифровка қилиш D_B: C → M алгоритмлари очиқ.

Амалда асимметрик шифрлаш алгоритмларининг яратиш учун бир томонлама функциялардан (муаммолардан) фойдаланиш тавсия этилади.

Ҳозирда очиқ калитли тизимларни яратиш учун қуйидаги муаммоларлар кенг фойдаланилади:

– катта сонни иккита туб кўпайтувчи шаклида ифодалаш;
– дискрет логарифмлаш муаммоси;
– эллиптик эгри чизиқларга асосланган.

Очиқ калитли криптотизимларни бир томонли функциялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида RSA, Эль-Гамал ва Мак-Элис тизимларини алохида тилга олиш ўринли. Хозирда 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).

RSA шифрлаш алгоритми ассиметрик шифрлаш алгоритмлари ичида яратилган дастлабки алгоритмлардан бири саналиб, катта сонни иккита туб сон кўпайтувчиси шаклида ёйиш муаммосига асосланган. Ҳозирги кунда ҳам ушбу алгоритмдан амалда камида 1024-бит калитдан фойдаланиш тавсия этилади.[1]

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 айтарлича ҳисоблаш ресурсларини талаб қилади.

2.4. Хэш функциялар ва ЭРИ алгоритмлари

Ахборотнинг криптографик ҳимоясининг асосий вазифаларидан бири бу – маълумот бутунлигини таъминлашдир. Маълумотни бутунлигини таъминлашда хэш функциялар деб аталувчи тизимлардан фойдаланилиб, ушбу тизимлар ахборотни узатиш давомида ўзгарганлигини текширишда фойдаланилади.

Ушбу тизимларнинг дастлабки вакилларига CRC (Cyclic Redundancy

[1] Stamp Mark. Information security: principles and practice. 95 – c.

Check) тизимларини мисол қилиб олиш мумкин. Ҳозирда ҳам кичик ҳисоблашлар талаб этиладиган қурилмаларда ва тизимларда айнан CRC тизимларидан кенг фойдаланилади. Масалан, WEP протоколида, тармоқ қурилмаларида ва ҳак.

Хэш функция деб ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ёки байт бирликларида) қийматга ўтказувчи функцияга айтилади. Хэш функциялар статистик тажрибаларни ўтказишда, мантиқий қурилмаларни текширишда, тез қидириб топиш алгоритмларини тузишда ва маълумотлар базасидаги маълумотларнинг тўлалигини текширишда қўлланилади.

Криптографияда хэш функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

– маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;
– маълумотнинг манбаини аутентификация қилиш учун.

Маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун ҳар бир маълумотнинг хэш қиймати (бу хэш қиймат маълумотни аутентификация қилиш коди ёки “имитовставка”-маълумот блоклари билан боғлиқ бўлган қўшимча киритилган белги дейилади) ҳисобланилади ва бу қиймат маълумот билан бирга сақланилади ёки узатилади. Маълумотни қабул қилган фойдаланувчи маълумотнинг хэш қийматини ҳисоблайди ва унинг назорат қиймати билан солиштиради. Агар таққослашда бу қийматлар мос келмаса, маълумот ўзгарганлигини билдиради.

Хэш функция деб, ихтиёрий узунликдаги M маълумотни фиксирланган узунликдаги h(M)=H қийматга акслантирувчи, осон ҳисобланадиган бир томонли функцияга айтилади.

Хэш қиймат бошқа номлар билан: “хэш код”, “свертка”, “дайджест”, “бармоқ излари” деб ҳам аталади.

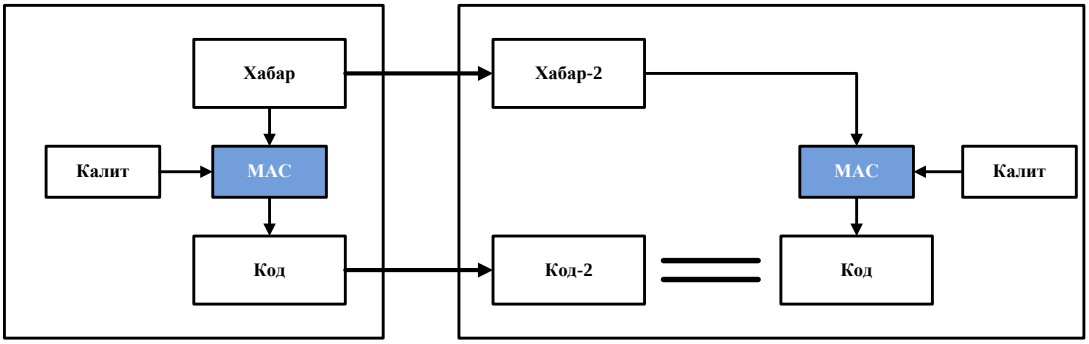
Хэш функцияга қуйидаги талаблар қўйилади:

1. Ихтиёрий узунликдаги матнга қўллаб бўлади.
2. Чиқишда тайинланган узунликдаги қийматни беради.
3. Ихтиёрий берилган x бўйича h(x) осон ҳисобланади.
4. Ихтиёрий берилган H бўйича h (x)= H тенгликдан x ни ҳисоблаб топиб бўлмайди. (Бир томонлилик хоссаси)
5. Олинган x ва y≠x матнлар учун h(x)≠ h(y) бўлади. (Коллизияга бардошлилик хоссаси).

Ҳозирда амалда хэш функциялар ўзи алоҳида фойдаланилмай, балки улар устида ишлаб чиқилган тизимлар кенг фойдаланилади. Ушбу

тизимларларга, электрон рақамли имзо алгоритмлари, маълумотларни аутентификациялаш тизимиларини олишимиз мумкин.

Маълумотни аутентификациялаш тизимлари (MAC) хэш функциялар бажарган маълумотни бутунлигини таъминлаш вазифаси устига қўшимча равишда, маълумотни аутентификациялаш вазифасини ҳам бажаради. Умумий ҳолда MAC тизимларининг ишлаши қуйидаги 2.15-расмда акс эттирилган.[1]



2.15-расм. MAC тизимлари

Ушбу тизимларда фақатгина икки томонга маълум бўлган махфий параметр “Калит” фойдаланилиб, ушбу параметр орқали фойдаланувчи маълумоти аутентификациядан ўтказилади. Ҳозирда MD5, SHA1, SHA2 хэш функцияларига асосланган MAC тизимларидан амалда кенг фойдаланилади.

Бундан ташқари маълумот манбаининг ҳақиқийлигини таъминлашда, маълумот муаллифини аниқлашда электрон рақамли имзо (ЭРИ) фойдаланилиб, уларнинг асосий вазифаси қуйидагилардан иборат:

- махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди;
- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;
- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Махсус ЭРИ алгоритмлари рақамли имзони ҳисоблаш ва имзони текшириш қисмларидан иборат. Рақамли имзони ҳисоблаш қисми имзо қўйувчининг махфий калити ва имзоланиши керак бўлган ҳужжатнинг хэш

[1] Stamp Mark. Information security: principles and practice. 136 – 138 – с.

қийматига боғлиқ бўлади. Имзони текшириш қисми имзо эгасининг очиқ калитига ва қабул қилиб олинган ҳужжатнинг хэш қийматига боғлиқ ҳолда амалга оширилади.

Электрон рақамли имзо алгоритмлари

Ҳар қандай ёзма хат ёки ҳужжатнинг охирида шу ҳужжатни тузувчиси ёки тузиш учун жавобгар бўлган шахснинг имзоси бўлиши табиий ҳолдир. Бундай ҳолат одатда қуйидаги иккита мақсаддан келиб чиқади. Биринчидан, маълумотни олган томон ўзида мавжуд имзо наъмунасига олинган маълумотдаги имзони солиштирган ҳолда шу маълумотнинг ҳақиқийлигига ишонч ҳосил қилади. Иккинчидан, шахсий имзо маълумот ҳужжатига юридик жиҳатдан муаллифликни кафолатлайди. Бундай кафолат еса савдо–сотиқ, ишончнома, мажбурият ва шу каби битимларда алоҳида муҳимдир.

Ҳужжатлардаги қўйилган шахсий имзоларни соҳталаштириш нисбатан мураккаб бўлиб, шахсий имзоларнинг муаллифларини ҳозирги замонавий илғор криминалистика услубларидан фойдаланиш орқали аниқлаш мумкин. Аммо Электрон рақамли имзо хусусиятлари бундан фарқли бўлиб, иккилик саноқ системаси хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ. Хотира битларининг маълум бир кетмакетлигидан иборат бўлган Электрон имзони кўчириб бирор жойга қўйиш ёки ўзгартириш компьютерлар асосидаги алоқа тизимларида мураккаблик туғдирмайди.

Бугунги юқори даражада ривожланган бутун дунё сиивилизациясида ҳужжатлар, жумладан маҳфий ҳужжатларнинг ҳам, Электрон кўринишда ишлатилиши ва алоқа тизимларида узатилиши кенг қўлланилиб борилаётганлиги Электрон ҳужжатлар ва Электрон имзоларнинг ҳақиқийлигини аниқлаш масалаларининг муҳимлигини келтириб чиқармоқда.

Очиқ калитли криптографик тизимлар қанчалик қулай ва криптобардошли бўлмасин, аутентификация масаласининг тўла ечилишига жавоб бера олмайди. Шунинг учун аутентификация услуби ва воситалари криптографик алгоритмлар билан биргаликда комплекс ҳолда қўлланилиши талаб этилади.

Қуйида иккита (А) ва (Б) фойдаланувчиларнинг алоқа муносабатларида аутентификация тизими рақиб томоннинг ўз мақсади йўлидаги қандай хатти-ҳаракатларидан ва криптотизим фойдаланувчиларининг фойдаланиш протоколини ўзаро бузилишлардан сақлаши кераклигини кўрсатувчи ҳолатлар кўриб чиқилади.

Рад этиш. Фойдаланувчи (А) фойдаланувчи (Б) га ҳақиқатан ҳам маълумот жўнатган бўлиб, узатилган маълумотни рад этиши мумкин.

Бундай қоида бузилишининг (тартибсизликнинг) олдини олиш мақсдида Электрон (рақамли) имзодан фойдаланилади.

Модификациялаш (ўзгартириш. Фойдаланувчи (Б) қабул қилиб олинган маълумотни ўзгартириб, шу ўзгартирилган маълумотни фойдаланувчи (А) юборди, деб таъкидлайди (даъво қилади).

Соҳталаштириш: Фойдаланувчи (Б)нинг ўзи маълумот тайёрлаб, бу соҳта маълумотни фойдаланувчи (А) юборди деб даъво қилади.

Фаол модификациялаш (ўзгартириш): (А) ва (Б) фойдаланувчиларнинг ўзаро алоқа тармоғига учинчи бир (В) фойдаланувчи ноқонуний тарзда боғланиб, уларнинг ўзаро узатаётган маълумотларини ўзгартирган ҳолда деярли узлуксиз узатиб туради.

Ниқоблаш (имитациялаш): Учинчи фодаланувчи (В) фойдаланувчи (Б)га фойдаланувчи (А) номидан маълумот жўнатади.

Юқорида санаб ўтилган: модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш каби алоқа тизими қоидаларининг бузилишини олдини олиш мақсадида рақамли сигнатурадан– рақамли имзо ва узатиладиган маълумотнинг бирор қисмини тўла ўз ичига олувчи рақамли шифрматндан иборат бўлган маълумотдан фойдаланилади.

Такрорлаш: Фойдаланувчи (В) фойдаланувчи (А) томонидан фойдаланувчи (Б)га жўнатилган маълумотни такроран (Б)га жўнатади. Бундай ноқонуний хатти–ҳаракат алоқа усулидан банклар тармоқларида Электирон ҳисоб–китоб тизимидан фойдаланишда ноқонунийлик билан ўзгалар пулларини талон-тарож қилишда фойдаланилади. Ана шундай ноқонуний усуллардан муҳофазаланиш учун қуйидаги чора - тадбирлари кўрилади.

- имитациялашга бардошлилик – имитабардошлилик;
- криптотизимга кираётган маълумотларни муҳофаза мақсадларидан келиб чиқиб тартиблаш.

Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди, яъни:

- махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди;
- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;
- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш

юритиши муносабатидаги кўплаб келишмовчиликларни бартараф етади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Кўп ҳолларда узтилаётган маълумотларни шифрлашга ҳожат бўлмай, уни Электрон рақамли имзо билан тасдиқлаш керак бўлади. Бундай ҳолатларда очиқ матн жўнатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жўнатилади. Маълумотни қабул қилиб олган томон жўнатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

1991 йилда АҚШ даги Стандартлар ва Технологиялар Миллий Институти DSA (Digital Signature Algorithm) рақамли имзо алгоритмининг стандартини DSS (Digital Signature Standart) биз юқорида келтирган Эл-Гамал ва RSA алгоритмлари асосида яратиб, фойдаланувчиларга таклиф етган.

Дастлаб таъкидланганидек, имзо хужжатнинг юридик мақомини кафолатлайди. Хозирги ривожланган жамиятда ахборот коммуникация тармоқларида Электрон маълумот алмашинувининг кенгайиб бориши маълумотларнинг маҳфийлигини, ҳақиқийлигини ва муаллифликни ўрнатиш масалаларини ечишни талаб етади. Масалан, алмашилган Электрон маълумотлар асосида у ёки бу ҳолатнинг ўзгариши, бу маълумотлар муаллифи манфатларига зид келиб, у электрон маълумот муаллифлигидан бош тортиши мумкин. Шундай ҳолатларнинг олдини олиш механизми маълумот муаллифини ўзигагина маълум бўлган бирор сонли параметр (махфий калит) билан боғлиқ ҳолда ҳосил қилинадиган сонлар кетма-кетлигида иборат бўлган Электрон рақамли имзо (ЭРИ) ҳисобланади.

ЭРИ ахборот коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани ечиш имконини беради:

– электрон ҳужжат манбаининг ҳақиқийлигини аниқлаш;

– электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;

– электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлайди.

Ҳар қандай ЭРИ алгоритми иккита қисмдан иборат бўлади.

– имзо қўйиш;

– имзони текшириш.

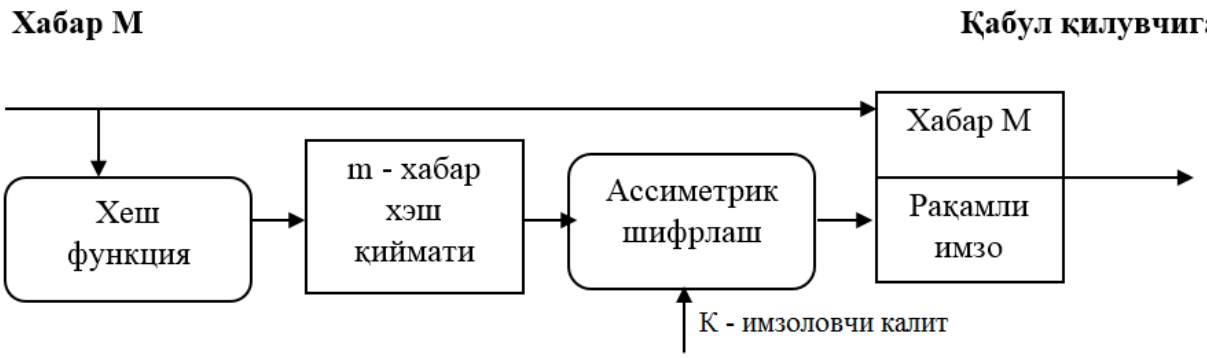
Рақамли имзони шакллантириш муолажаси. Ушбу муолажани тайёрлаш босқичида хабар жўнатувчи абонент A иккита калитни генерациялайди: маҳфий калит k_A ва очиқ калит K_A. Очиқ калит K_A унинг жуфти бўлган махфий калити k_A дан ҳисоблаш орқали олинади.

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 *h(M)* қийматини ҳисоблайди (16-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 (2.16-расм).

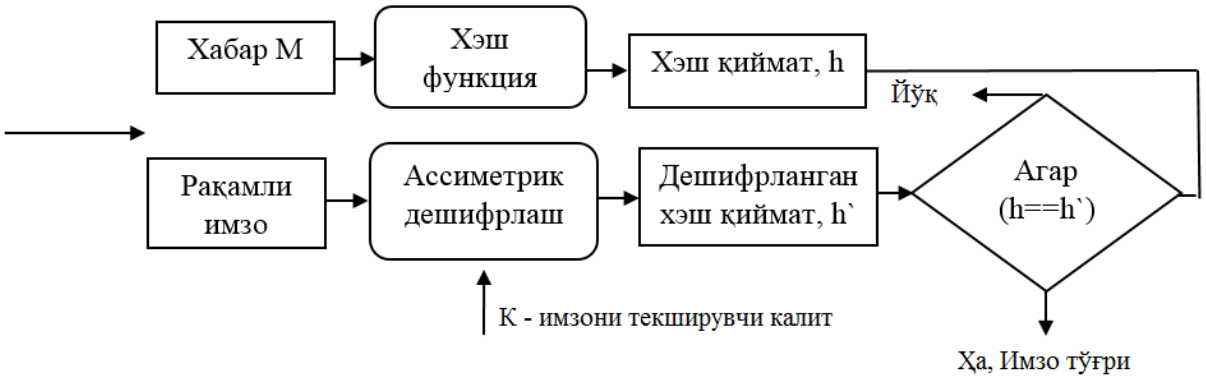


2.16–расм. Электрон рақамли имзони шакллантириш схемаси

Рақамли имзони текшириш муолажаси. Тармоқ абонентлари олинган хабар *"M"*нинг рақамли имзосини ушбу хабарни жўнатувчининг очик калити K_A ёрдамида текширишлари мумкин (2.17-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 хешфункция *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.



2.17 - расм. Электрон рақамли имзони текшириш схемаси

Имзо қўйиш муаллиф томонидан, фақат унга маълум бўлган махфий калит билан амалга оширилади. Имзонинг ҳақиқийлигини текшириш еса исталган шахс томонидан, имзо муаллифининг очиқ калити билан амалга оширилиши мумкин.

Электрон коммуникациялар ва Электрон хужжат алмашинуви ҳозирги кунда иш юзасидан бўладиган муносабатларнинг ажралмас қисми ҳисобланиб, ҳар қандай замонавий ташкилотни Электрон хужжатлар алмашинуви ва Интернетсиз тасаввур қилиш қийин.

Интернет тармоғидан Электрон хужжатлар алмашинуви асосида молиявий фаолият олиб боришда маълумотлар алмашинувини ҳимоя қилиш ва Электрон хужжатнинг юридик мақомини таъминлаш биринчи даражали аҳамият касб етади.

Электрон хужжатли маълумот алмашинуви жараёнида ЭРИни қўллаш ҳар хил турдаги тўлов тизимлари (пластик карточкалар), банк тизимлари ва савдо соҳаларининг молиявий фаолиятини бошқаришда Электрон хужжат алмашинуви тизимларининг ривожланиб бориши билан кенг тарқала бошлади.

Ҳозирда ЭРИ тизимини яратишнинг бир нечта йўналишлари мавжуд. Бу йўналишларни учта гуруҳга бўлиш мумкин:

1. очиқ калитли шифрлаш алгоритмларига асосланган;
2. симметрик шифрлаш алгоритмларига асосланган;
3. имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидир.

Калитларни бошқариш

Калитлар ҳақидаги маълумот дэганда ахборот-коммуникация криптотизимида мавжуд бўлган барча калитлар тўплами ва уларнинг муҳофазаси билан боғлиқ маълумотлар тушунилади. Агарда калитлар ҳақидаги маълумотларни етарли даражадаги ишончли муҳофазали

бошқаруви таъминланмаса, табиийки, рақиб томонга ахборот-коммуникация тизимидаги деярли иҳтиёрий маълумотни олиш учун тўла имконият туғилади.

Калитларни бошқариш жараёни қуйидаги учта муҳим бўлган:

- барча калитларнинг ўзаро боғлиқ ҳолда, яъни бир бутун ҳолда ишлаш жараёнини таъминлаш (калитлар генерацияси);
- калитлар тўпламининг мақсадли кенгайиб боришини таъминлаш (калитларларнинг тўпланиши);

калитларларни фойдаланувчилар доирасида тақсимлаш (калитларларнинг тақсимланиши) жараёнларига аҳамият беришни талаб этади.

Диффи – Хелман калитларни очиқ тақсимлаш протоколи. У. Диффи ва М.Е. Хеллманнинг калитларни очиқ тақсимлаш системаси очиқ калитли бошқа криптотизимлар каби маҳфий калитни маҳфий канал орқали узатилишининг ҳожати йўқлигини таъминлайди, аммо аутентификация масаласини ечмайди ва ўртадаги одам ҳужумига бардошсиз.[1]

Мисол:

ALICE	**EVIL EVE**	**BOB**
Alice ва Bob иккита g, p (p>g) сонни ҳосил қилади. p=11, g=7	Бузғунчига ҳам p=11, g=7 маълум.	Alice ва Bob иккита g, p (p>g) сонни ҳосил қилади. p=11, g=7
Alice ўзининг махфий калитини ҳосил қилади. X_A=6		Bob ўзининг махфий калитини ҳосил қилади. X_B=9
$Y_A=g^{X(A)}(modp)$ $Y_A=7^6 mod 11=4$		$Y_B=g^{X(B)}(modp)$ $Y_A=7^9 mod 11=8$
Alice Y_A=8 ни қабул қилади.	Бузғунчига ҳам Y_B =4, Y_A = 8 маълум.	Bob Y_B=4 ни қабул қилади.
Махфий калит = $_B{}^{X_A} modp$ Махфий калит = $8^6 mod 11$ = 3		Махфий калит = $_A{}^{X_B} modp$ Махфий калит = $4^9 mod 11$ = 3

Қуйида 2.1-жадвалда криптографик ҳимоя усуллари ва уларнинг ахборот хавфсизлигини таъминлашда тутган ўрни келтирилган.

2.1-жадвал

Криптографик ҳимоя усуллари ва уларнинг ахборот хавфсизлигини таъминлашда тутган ўрни

Алгоритмлар	**Махфийлик**	**Аутентификация**	**Яхлитлик**	**Калитлар бошқаруви**
Симметрик алгаритм	Ҳа	Йўқ	Йўқ	Ҳа

[1] Stamp Mark. Information security: principles and practice. 100 – 102 – с.

Носимметрик алгоритм	Ҳа	Йўқ	Йўқ	Ҳа
Электрон рақамли имзо алгоритми	Йўқ	Ҳа	Ҳа	Йўқ
Калит тарқатиш алгоритми	Ҳа	Йўқ	Йўқ	Ҳа
Бир томонлама хэш функциялар	Йўқ	Йўқ	Ҳа	Йўқ
Хабар аутентификация коди	Ҳа	Ҳа	Ҳа	Йўқ

Назорат саволлари

1. Ахборотнинг криптографик ҳимояси.
2. Криптография ва криптотаҳлил фанлари мақсади.
3. Криптографиянинг бўлимлари.
4. Симметрик шифрлаш тизимлари вазифалари.
5. Асимметрик шифрлаш тизимлари ва улардан фойданиш.
6. ЭРИ алгоритмлари вазифаси.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: издательство ТРИУМФ, 2003 -816 стр.
4. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. 2008.

3-мавзу. Аутентификация ва идентификация усуллари. Рухсатларни назоратлаш. Тармоқлараро экран. Ҳужумларни аниқлаш тизимлари.

Режа:

1. Аутентификация ва идентификация усуллари.
2. Рухсатларни назоратлаш.
3. Тармоқлараро экран.
4. Ҳужумларни аниқлаш тизимлари.

Таянч иборалар: *идентификация, аутентификация, авторизация, парол, биометрик хусусият, рухсатларни назоратлаш, мандатга асосланган модел, дискрецион модел, ролга асосланган модел, Белла-Ла-Пудула модели, тармоқлараро экран, ҳужусларни аниқлаш тизимлари, рухсатлар матрицаси.*

3.1. Аутентификация ва идентификация усуллари

Идентификация - жараёни фойдаланувчини тизимга танитиш жараёни бўлиб, унда одатда фойдаланувчи ўз исмидан (логин), смарт карталардан ва биометрик хусусиятларидан фойдаланиши мумкин.

Аутентификация жараёни - фойдаланувчи ёки маълумотни ҳақиқатда тўғри эканлигини текшириш жараёни бўлиб, одатда 3 турга бўлинади:[1]

- Бирор нарсани билиш асосида. Масалан:парол, PIN, савол-жавоб ва ҳ.к.
- Бирор нарсага эгалик қилиш асосида. Масалан: ID карта, хавфсизлик токенлари ва ҳ.к.
- Мавжуд ўзига хос факторлар асосида. Масалан: бармоқ изи, юз тузилиш, ДНК, овоз, ҳаракат ва ҳ.к.

Пароллар асосида аутентификациялаш. Парол асосида аутентификациялаш усули кенг тарқалган усуллардан бири саналиб қолмасдан, энг заиф усулдир. Парол асосида аутентификациялаш усулини заифликка олиб келувчи омиллар:

- мураккаб паролларни эсга қолиши қийин бўлганлиги сабабли фойдаланувчи томонидан содда пароллардан фойдаланиш;
- паролни унутиб қўйиш муаммоси;
- кўп тизимларда фойдаланувчи томонидан айнан бир хил паролдан фойдаланилиши;
- парол ўқиб олувчи ҳар хил дастурлар мавжудлиги ва ҳ.к.

[1] Stamp Mark. Information security: principles and practice. 230 - 233 – c.

Парол – аутентификациялашда кенг фойдаланилаётган катталик бўлиб, фойдаланишда катта қулайлик туғдиради. Аммо, бардошлиги жуда паст.

Криптографик калит – аутентификациялашда фойдаланилиб, бардошлиги жихатидан паролга қараганда бардошли.

<table>
<tr><th colspan="2">Криптографик калит</th><th colspan="2">Парол</th></tr>
<tr><td colspan="2">Калит ўлчами 64 – бит
Калитлар сони 2^{64}
Калит тасодифий танланади
Таҳдидчи $2^{64}/2=2^{63}$ та калитни ҳисоблаши керак.</td><td colspan="2">• Парол ўлчами 8 та белгидан иборат ва 256 та белгилардан фойдаланиш мумкин;
• Жами пароллар сони $256^8=2^{64}$
• Пароллар тасодифий танланмайди;
• Таҳдидчи 2^{63} дан кам уриниш билан паролни топа олади (луғат бўйича ҳужум).</td></tr>
<tr><td colspan="2">Ёмон парол</td><td colspan="2">Яхши парол</td></tr>
<tr><td>–frank
–Fido
–password</td><td>–Pikachu
–102560
–AustinStamp</td><td>–jfIej,43j-EmmL+y
–09864376537263
–P0kem0N</td><td>–FSa7Yago
–0nceuP0nAt1m8
–PokeGCTall150</td></tr>
</table>

Паролларга асосланган аутентификациялаш тизимларида парол 3 марта нотўғри киритилган тақдирда тизим қулфланиши шарт. Пароллар одатда файлларда хешланган ҳолда сақланади. Аутентификация жараёни хэшланган парол орқали амалга оширилади. Бу ҳолда бузғунчи файлни қўлга киритлан тақдирда ҳам паролга эмас балки унинг хэш қийматига эга бўлади.

Луғатга асосланган таҳдид. Бу таҳдид тури паролга асосланган аутентификациялаш тизимлари учун мос бўлиб, заиф пароллардан ёки умумий бўлган пароллардан фойдаланилган тақдирда катта фойда беради. Бунинг учун бузғунчи интернет тармоғидан кенг фойдаланилган пароллар рўйхатини (луғатини) кўчириб олади ва уларни тизимга бирин-кетин қўйиш орқали текшириб кўради.

Пароллар хэшланган тақдирда ҳам луғатга асосланган таҳдид ўринли бўлиб, заиф парол фойдаланилган вақтда катта самара беради.

Паролларни сақлашда одатда “туз (solt), s”дан кенг фойдаланади. Бунинг учун фойдаланувчи тасодифий катталик “туз”ни танлайди ва паролга қўшиб, унинг y=h(p,s) хэш қийматини ҳисоблайди ва пароллар файлига (y, s) шаклида ёзиб қўяди. Бу ерда “туз” махфий саналмайди аммо, бузғунчи ҳар бир фойдаланувчи учун уни алоҳида ҳисоблаши талаб этилади.[1]

Паролларни аниқлаш: математик ҳисоблаш. Фараз қилайлик парол 8 та белгидан иборат бўлиб, у 128 белгидан иборат бўлган алифбодан олинган. Бунда мавжуд пароллар сони $128^8=2^{56}$. Пароллар файлига жами бўлиб, 2^{10} та паролдан иборат бўлиб, таҳдидчи 2^{20} та кенг тарқалган паролдан

[1,2] Stamp Mark. Information security: principles and practice. 237 – с.

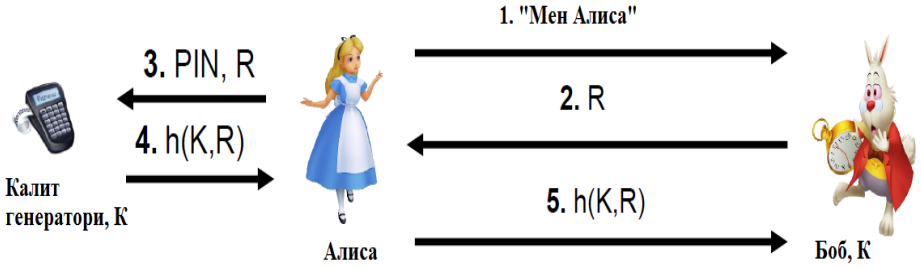
иборат бўлган луғатдан фойдаланади. Агар паролни луғатда бўлиш эҳтимоллиги ¼ га тенг деб олинса:[1]

- луғатдан фойдаланилмаган ҳолда, камида $2^{56}/2=2^{55}$ уринишни амалга ошириши шарт;
- “туз”дан фойдаланилган ҳолда эса ¼ (2^{19})+3/4 (2^{55}) =$2^{54.6}$ га тенг бўлади;
- “туз”дан фойдаланилмаган ҳолда, 2^{20} га тенг бўлади.

Амалда паролларни бузишга Password Cracker, Password Portal, L0phtCrack and LC4(Windows), John the Ripper(Unix) воситалардан фойдаланилмоқда.

ID карталар асосида аутентификациялаш усули пароллар асосида аутентификациялаш усулига қараганда бардошли саналиб, фойдаланувчи томонидан йўқотилиб қўйиш муаммоси мавжуд. Бу усулда асосан машинанинг пултини, парол генератори, смарт карта ва ҳак.

Калит генераторларига асосланган аутентификациялаш тизими қуйидагича:[2]



3.1 – расм. Калит генератори орқали аутентификациялаш

Мавжуд ўзига хос хусусиятлар ёки биометрик параметрлар асосида аутентификациялаш усули бардошли саналиб, юқоридаги усулларда мавжуд камчиликлар бартараф этилган. Камчилик сифатида эса фойдаланилган қурилма нархи ёки жараён вақтини узоқлигини келтириш мумкин.

Ананавий аутентификациялаш усуллари (пароль асосида ва нимагадир эгалик қилиш асосида) фойдаланишда қулай бўлишига қарамасдан қатор камчиликларга эга:

– фойдаланувчи пароли одатда содда ва фойдаланувчи хотирасида сақланиши осон бўлиш учун қисқа фразалардан фойдаланади, бу эса ушбу тизимнинг заифлигини англатади;

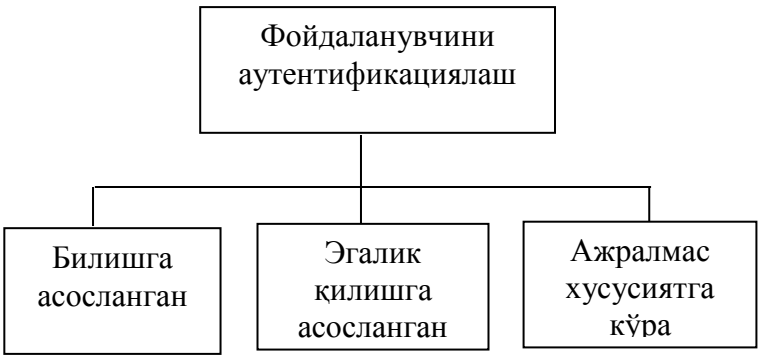
– паролларни эсдан чиқариб қўйиш муаммоси;

– аутентификациялаш токенларини (смарт карталар ва ҳ.) йўқотиб қўйиш муаммоси ва ҳ.

Ушбу муаммоларни бартараф этиш учун учинчи йўналиш, *биометрик* параметрларга асосланган аутентификациялаш усулларидан фойдаланилади.

[3] Stamp Mark. Information security: principles and practice. 252 – c.

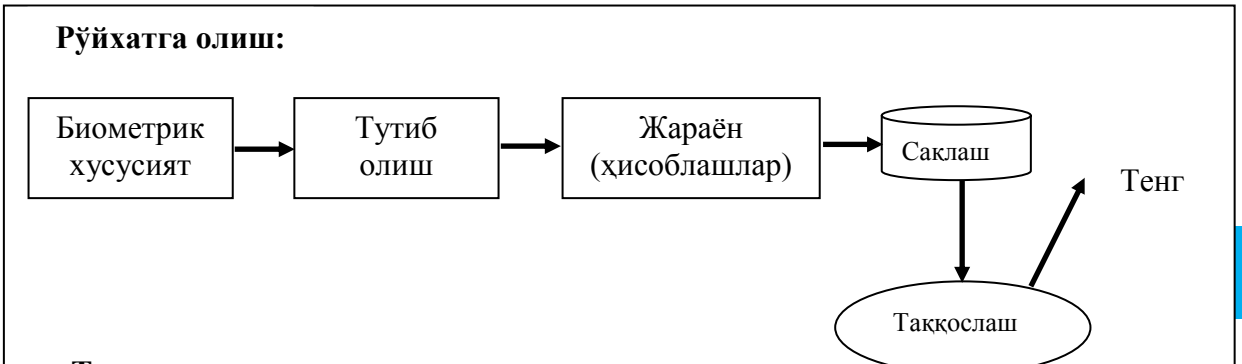
Биометрик параметрларга асосланган аутентификациялаш усуллари ўзининг ишончлилик, ўғирлаб бўлмаслик, кўчириб бўлмаслик, фойдаланишда қулайлик ва ҳ. хусусиятлари билан ажралиб туради (3.2-расм).



3.2-расм. Аутентификациялаш усуллари

Биометрик параметрларда унутиш, йўқотиб қўйиш, нусха кўчириш, сохталаштириш ва бошқа фойдаланувчи томонидан ишлатиб бўлмаслиги каби муаммоларнинг йўқлиги билан ажралиб туради.

Умумий кўриниши:		**Парол, махфийлик**	**Токен**	**Биометрик параметрлар**
Аутентификациялаш асоси:		Яширинлик ёки ноаниқлик асосида	Эгалик қилиш асосида	Ягоналик ва шахсийлик
Хавфсизлик ҳимояси		Маҳкам ёдда сақлаш	Доим ёнда олиб юриш	Қалбакилаш-тириш мураккаб
Мисол	**Ананавий**	Комбинацион қулф	Металл қулф	Ҳайдовчилик гувоҳномаси
	Рақамли	ШК пароли	Машина пульти	Бармоқ изи
Хавфсизлик томонидан камчилиги		Фойдаланиш даврида махфийлик камая боради	Токен йўқотилган ҳолатда катта хавф олиб келиши мумкин	ID алмаштиришни мураккаблиги



3.3-расм. Биометрик аутентификациялаш тизимларининг умумий ишлаш технологияси

Биометрик параметрлар турлари. Биометрик параметрларни турларга ажратгандан кўра, биометрик параметрлар орқали қабул қилинаётган сигналлар турига қараб ажратиш афзал ва улар қуйидагилар:[1]

– турғун биометрик сигналлар (бармоқ изи, юз тузилиш, қўл шакли, кўз қорачиғи ва ҳ.к);

– ўзгарувчан биометрик сигналлар (овоз, ҳаракат, клавиатурада ёзиш тезлиги).

Бундан ташқари биометрик параметрлар шахсга боғлиқ ҳолда физиологик (бармоқ изи, юз тузилиш, қўл шакли, кўз қорачиғи ва ҳ.) ва хатти-ҳаракатига (ҳаракат, клавиатурада ёзиш тезлиги) асосланган ва комбинацион (овоз) параметрларга бўлинади.

Биометрик аутентификациялаш усуллари қандай биометрик хусусиятларга асосланганлигига кўра қуйидаги турларга бўлинади:

– бармоқ изига;
– юзни таниб олишга;
– кўз қорачиғига;
– шахс имзосига;
– овозга;
– қўл геометриясига;
– ДНК таҳлилига;
– қўл қон томирларига;
– қулоқ шаклига;
– компьютер клавиатурасида ёзиш хусусиятига;
– ҳаракатга асосланган ва ҳ.

Биометрик хатоликлар. Ёлғон маълумотни қабул қилиниш даражаси ва ёлғонни мос келиш даражаси (False Accept Rate (FAR) and False Match

[1] Stamp Mark. Information security: principles and practice. 242 – 243 – c.

Rate (MAR)): ушбу катталик, киритилган маълумот билан маълумотлар базасидаги маълумотлар мос келмаган ҳолда тизимни муваффақиятли текширувни амалга ошириш даражасини кўрсатади. Бошқа сўз билан айтганда, нотўғри уринишлар фоизини кўрсатади. Ушбу хатолик миқдори катта бўлган тизимларда одатда, рухсат этилмаган фойдаланувчиларни тизимдан фойдаланишига йўл қўйилмайди.[1]

Тўғри маълумотни инкор этилиш даражаси ёки ёлғондан мос келмаслик даражаси(False Reject Rate (FRR) or False Non-Match Rate (FNMR)): ушбу катталик тўғри киритилган маълумотни тизим ёлғон маълумот деб қабул қилиши ва бунинг натижасида муваффақиятсиз текшурувни амалга оширилишига айтилади. Бошқа сўз билан айтганда, ушбу катталик тўғри маълумотларни рад этилиш даражасини кўрсатади.[2]

Ушбу юқорида номлари келтирилган усуллар қанчалик бардошли саналмасин, ушбу усуллар асосида ишлаб чиқилган тизим бардошлилиги фақат буларга боғлиқ бўлмайди. Одатда ушбу параметрлар ҳақиқий фойдаланувчи томонидан эмас, бузғунчи томонидан ҳам киритилиши мумкин. Ушбу ҳолатда ананавий аутентификациялаш усулида ўзига яраша муаммо келиб чиқади. Ушбу муамммони олдини олиш мақсадида ҳозирда кенг тарқалган *икки факторли аутентификациялаш* усулидан фойдаланилади. [3]

Ушбу усулда одатий аутентификациялаш усулидан ўтган фойдаланувчи юқоридаги усуллардан бири асосида иккинчи марта аутентификациядан ўтказилади. Ушбу усул парол асосида аутентификациялаш усулида иштирок этаётган ҳақиқий фойдаланувчи ёки компьютер эканлигини аниқласа, хавфсизлик токенларига асосланган усулда эса токен эгаси ҳақиқийлигини текширади. Биометрик аутентификациялаш усулларида эса фойдаланувчини ҳақиқийлиги ва тириклигини текширишда фойдаланилади.

Умумий ҳолда икки факторли аутентификациялаш усули оддий аутентификациялаш усулига қўшимча хавфсизлик параметрини қўшади. Икки факторли аутентификациялаш усули унда фойдаланилган қурилма турига қараб икки турга: уланган(connected) ва уланмаган (unconnected) бўлинади.

Уланган қурилмаларга асосланган икки факторли аутентификациялаш усулида тўғридан-тўғри боғланган қурилма орқали маълумот қабул қилинади. Масалан, USB ёки Bluetooth асосида уланган қурилмалар.

[1,2] Stamp Mark. Information security: principles and practice. 244 – с.
[3] Stamp Mark. Information security: principles and practice. 252 – с.

Уланмаган қурилмаларга асосланган икки факторли аутентификациялаш усулида фойдаланувчи қурилма ва аутентификация тизими орасида жойлашади.

Қуйида икки факторли аутентификациялаш усулари келтирилган:

– бир мартали парол ҳосил қилиб берувчи қурилмаларга асосланган;
– бир мартали парол ҳосил қилиб берувчи дастурий воситага асосланган;
– терминал (компьютер, мобил телефон ва ҳ.к.) хусусиятига асосланган;
– TAN (Transaction Authentication Number) рўйхатига асосланган;
– SMS токенларга асосланган;
– смарткарталар ва чип ўқувчи қурилмаларга асосланган;
– махсус хотирага эга USB асосланган;
– биометрик хусусиятларга асосланган ва ҳ.к.

3.2. Рухсатларни назоратлаш

Авторизация жараёни бу – фойдаланувчига тизим томонидан берилган фойдаланиш даражаси.

Тўқ сариқ китоб. Компьютер тизимлари хавфсизлигини аниқлаш критериялари (Trusted Computer System Evaluation Criteria ёки Orange book) 1983 йилда чоп этилган бўлиб, ҳозирги кунги, 2005 йилда қабул қилинган ISO/IEC 15408 нинг аналогидир. Ушбу критерия зарур ёки махфий ахборотларни сақлаш, қидириш, компьютер тизимларини танлаш, классификациялаш учун фойдаланилади.

Асосий мақсади ва воситаси. Хавфсизлик сиёсати компьютер тизими учун батафсил бўлиши, юқори даражада аниқланганлиги ва тегишли бўлиши шарт. Икки асосий хавфсизлик сиёсати мавжуд: мандатга асосланган хавфсизлик сиёсати ва дискрецион хавфсизлик сиёсати. Мандатга асосланган хавфсизлик сиёсатида махфий маълумотлардан фойдаланишда ндивидуал ёндошишга асосланади. Ҳар бир фойдаланувчига берилган рухсатлар ташкилотдани хавфсизлик сиёсатидан келиб чиқади. Дискерцион хавфсизлик сиёсатида эса рухсатни чеклашда ва бошқаришда қоидалар тўпламидан фойдаланилади. Бу қоидалар фақат бирор керакли бўлган маълумотни олишга қаратилган бўлади. Бошқа сўз билан айтганда ҳар бир маълумот учун фойдаланувчининг рухсатлари турлича бўлиши мумкин.

Хавфсизлик сиёсатидан бўлак, индивидуал жавобгарлик мавжуд бўлиб, улар асосан учта талабдан иборат:

– аутентификация;
– авторизация;
– аудит.

Тўқ сариқ китоб хавфсиз тизим, ишончли тизим, хавфсизлик сиёсати,

кафолатланганлик даражаси, ҳисобдорлик, ишончли ҳисоблаш базалари, мулоқот мониторинги, хавфсизлик ядроси, хавфсизлик переметри каби терминлардан иборат.

Ушбу критерия 4 та: D, C, B ва A бўлимлардан иборат бўлиб, хавфсизлик даражаси A да энг юқори. C, B ва A бўлимлар қисм бўлимлардан иборат.

D – Энг кичик хавфсизлик талабига эга бўлим.

C – Дискрецион ҳимоя. C1 – махфийликни дискрецион таъминоти бўлиб, фойдаланувчи, маълумотларни бўлимга ажратиш ва дискерцион рухсатларни бошқаришдан иборат бўлади. C2 – рухсатларни бошқариш. Дискрецион рухсатларни бошқаришнинг юқори аниқ бўлиши, индивидуал фойдаланувчи қайд ёзуви, тизимга рухсатларни бошқариш журнали, ресурсларни изоциялаш.

B – Мандатга асосланган ҳимоя. B1 – метахавфсизликдан фойдаланилган ҳолда ҳимоя. B2 – Тизимлашган ҳимоя. B3 – Хавфсизлик домени.

A – синалган ҳимоя. A1 – синалган дизайн ва юқори A1 қисмларидан иборат.

Умумий критериялар (Common Criteria for Information Technology Security Evaluation, Common Criteria**).** Компьютер хавфсизлиги бўйича халқаро стандарт. Ушбу стандарт асосий икки талабдан иборат: функционал ва ишонч талабларидан иборат.

Функционал талаблар хавфсизлик мақсадига кўра гуруҳланади. Уммумий ҳолда 11 та функционал синф (3 гуруҳда), 66 оила ва 135 та компонентдан иборат.

1. Биринчи гуруҳ хавфсизликнинг элементар хизматларини аниқлайди.
1. FAU – аудит, хавфсизлик.
2. FIA – идентификация, аутентификация.
3. FRU – ресурслардан иборат.
2. Элементар хавфсизлик хизматларидан хизматларни ишлаб чиқиш.
1. FCO – алоқа (жунатувчи-қабул қилувчи орасидаги хавфсиз алоқа).
2. FRP – ғайирилик.
3. FDP – фойдаланувчи маълумотларини ҳимоялаш.
4. FPT – объектни хавфсизлигини баҳолаш функцияси ҳимояси.
3. Учинчи гуруҳ объектни баҳолаш инфратузилмалари билан алоқадор.
1. FCS – криптографик ҳимоя.
2. FMT – хавфсизликни бошқариш.
3. FTA – объектни баҳолашга рухсат.
4. FTP – ишончли канал.

Хавфсизлик кафолати талаблари 10 та синф, 44 та оила ва 93 та

компонентдан иборат.

1. Биринчи гуруҳ талаблардан ташкил топган.

1. APE – ҳимоя профилини баҳолаш.

2. AES – хавфсизлик вазифаларини баҳолаш.

2. Иккинчи гуруҳ объектни аттестациялашнинг ҳаётий циклидан иборат.

1. ADV – объектни лойихалаш ва қуриш.

2. ALC – ҳаётий циклни қўллаб қувватлаш.

3. ACM – конфгурацияни бошқариш.

4. AGD – фойдаланувчи ва администраторга.

5. ATE – тестлаш.

6. AVA – заифликларни баҳолаш.

7. ADO – эксплутация ва этказиб беришга талаблар.

8. AMA – ишонч-талабларини қўллаб қувватлаш.

Авторизациялаш технологиялари. Авторизациялашда қатор технологиялардан фойдаланилиб, уларнинг асосийлари қуйидагилар.

Мандатга асосланган рухсатларни бошқариш (Mandatory Access Control (MAC)). Бу технологияга асосан объект ёки субъектнинг хавфсизлик байроғига асосан бошқарилади. Хавфсизлик байроғи хавфсизлик даражасини белгилайди. Қуйидаги 3.1 (а,б)-жадвалда хавфсизликни ҳарбий ва савдо соҳасида даражаланиши келтирилган.

3.1 (а)-жадвал

Ҳарбий соҳада

Классификация	**Изоҳ**
Классификайцияланмаган.	Ахборот махфий ёки классисификацияланган эмас.
Махфий аммо классификацияланмаган.	Ахборот очиқ бўлса, унга зиён этиши мумкин.
Конфиденциал	Фақат ички фойдаланиш учун очиқ.
Махфий	Ахборот миллий хавфсизликка жиддий таъсир этиши мумкин.
Топ махфий.	Ахборот миллий хавфсизликга ўта жиддий таъсир этиши мумкин.

3.1 (б)-жадвал

Савдо соҳасида

Классификация	**Изоҳ**
Очиқ	Ҳамма учун очиқ маълумот
Махфий	Маълумот бизнесга таъсир этиши мумкин.
Шахсий	Бир шахсга тегишли маълумотлар.
Конфиденциал	Бу турдаги маълумотлар очилса ташкилотга жиддий

	таъсир этади.

Бу технологияга асосланган хавфсизликни бошқариш модели бу – Белла-Ла-Падула моделидир.[1]

Дискрецион рухсатларни бошқариш. Мандатга асосланган рухсатларни бошқариш тизими ҳарбий соҳада кенг фойдаланилсада, дискерцион рухсатларни бошқариш тизими ўзининг содда фойдаланилиши билан ажралиб туради. Бунга кўра объект эгаси қайси субъектни нима иш қилишини белгилар беради. Бу усул мандатга асосланган усулга қараганда жуда хавфсизи саналмасада, операцион тизимларда кенг фойдаланилади. Бунда асосан бошқариш матрицасидан фойдаланилади. [2]

3.2-жадвал

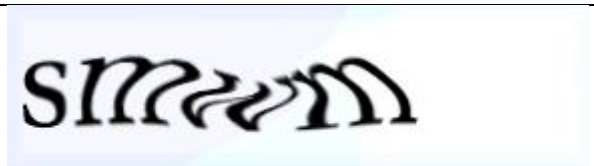
Рухсатлар матрицаси

	File 1	**File 2**	**File 3**	**Program 1**
Ann	Own, read, write	Read, write		Execute
Bob	Read		Read, write	
Karl		Read		Execute, read

Ролларга асосланган рухсатларни бошқариш. Бу усулга кўра рухсатлар субъектларнинг ролларига асосланиб берилади. Бу бир кўринишда гуруҳларга ажратишга ўхшаши мумкин аммо ундан фарқли равишда бир фойдаланувчи бир нечта гуруҳларга тегишли бўлиши мумкин. Аммо умумий ҳолда, фойдаланувчи ягона ролга эга бўлади.

Капча. Капча (инглизча: CAPTCHA — Completely Automated Public Turing test to tell Computers and Humans Apart) - компьютер ёки инсон еканлигини аниқлашнинг очиқ автоматлашган Туринг тести деб аталиб, масофадаги фойдаланувчини инсон ёки компьютер эканлигини аниқлашда фойдаланилади. Бу термин 2000 йилда пайдо бўлган бўлиб, 2013 йилга келиб кунига ўртача 320 млн. капча киритилган (3.4-расм).[3]

а) содда капча



б) мураккаб капча

3.4-расм. Капча

Ушбу тизимнинг асосий камчилиги бу ҳар доим ҳам капча ёркин ифодаланмайди. Гоҳида уни ҳаттоки инсон ҳам аниқлай олмайди.

[1,2] Stamp Mark. Information security: principles and practice. 271, 276 – c.
[3] Stamp Mark. Information security: principles and practice. 285-286 – c.

3.3. Тармоқлараро экран

Тармоқлараро экран (ТЭ) - *брандмауэр* ёки *firewall системаси* деб хам аталувчи тармоқлараро химоянинг ихтисослаштирилган комплекси. Тармоқлараро экран умумий тармоқни икки ёки ундан кўп қисмларга ажратиш ва маълумот пакетларини чэгара орқали умумий тармоқнинг бир қисмидан иккинчисига ўтиш шартларини белгиловчи қоидалар тўпламини амалга ошириш имконини беради. Одатда, бу чэгара корхонанинг корпоратив (локал) тармоги ва Internet глобал тармоқ орасида ўтказилади. Тармоқлараро экранлар гарчи корхона локал тармоги уланган корпоратив интратармогидан қилинувчи хужумлардан химоялашда ишлатилишлари мумкин бўлсада, одатда улар корхона ички тармогини Internet глобал тармоқдан суқилиб киришдан химоялайди. Аксарият тижорат ташкилотлари учун тармоқлараро экранларнинг ўрнатилиши ички тармоқ хавфсизлигини таъминлашнинг зарурий шарти хисобланади.[1]

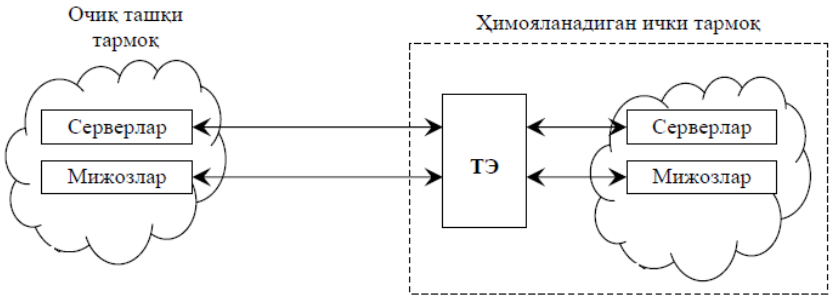
Рухсат этилмаган тармоқлараро фойдаланишга қарши таъсир кўрсатиш учун тармоқлараро экран ички тармоқ хисобланувчи ташкилотнинг химояланувчи тармоғи ва ташқи ғаним тармоқ орасида жойланиши лозим (3.5-расм). Бунда бу тармоқлар орасидаги барча алоқа фақат тармоқлараро экран орқали амалга оширилиши лозим. 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 чэгаралаш. 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 чэгаралаш. Бу масаланинг ечилиши, масалан, сервердан хизмат вазифалари талаб этмайдиган фойдаланишни тартибга солишга имкон беради.

[1] Stamp Mark. Information security: principles and practice. 288 – c.



3.5 – расм. Тармоқлараро экранни улаш схемаси

Тармоқлараро экранни классификациялашда стандарт мавжуд эмас. Шунга қарамасдан, уларни OSI моделининг қайси сатҳига ишлашига қараб қуйидаги турларга ажратиш мумкин:[1]

– пакет филтерлари – тармоқ сатҳида ишлайди;
– эксперт пакети филтерлари – транспорт саҳида ишлайди;
– илова проксилари – илова сатҳида.

Пакет филтерлари. Бу турдаги тармоқлараро экран тармоқ сатҳида пакетларни таҳлиллашга асосланган бўлиб, бунда калит маълумотлар сифатида: манба IP манзили, масофадиги IP манзил, манба порти, масофадаги порт, TCP байроқ битлари (SYN, ACK, RST ва ҳак.) параметрлар асосида амалга оширилади. Бу турдаги тармоқлараро экран асосан юқоридаги параметрлар асосида кирувчи ва чиқувчи трафикни таҳлиллайди.

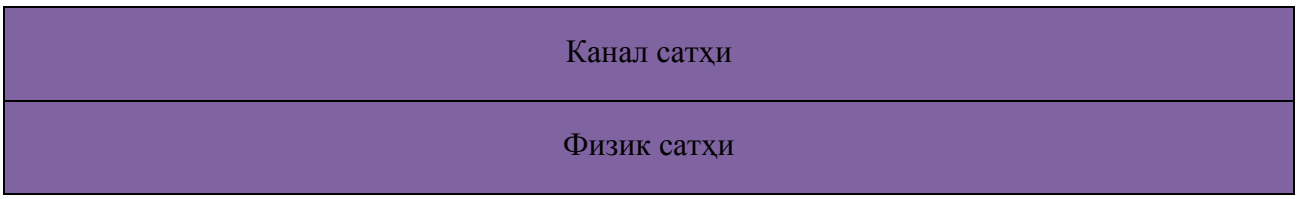
Бу турдаги тармоқлараро экран самарали бўлиб, фақат тармоқ сатҳида ишлайди ва сарлавҳа маълумотларни таҳлиллашда катта тезлик беради. Аммо, бу турдаги тармоқлараро экран қатор камчиликларга эга:

– ҳолатнинг турғунлиги мавжуд эмас, яъни ҳар бир пакет турлича бўлади;
– бу турдаги тармоқлараро экран TCP алоқани текширмайди;
– илова сатҳи маълумотларни, зарарли дастурларни ва ҳак. текширмайди.

Бу турдаги тармоқлараро экран “Рухсатларни назоратлаш рўйхати (ACL)” ёрдамида созланади (3.6,3.7 - расм).

Илова сатҳи
Транспорт сатҳи
Тармоқ сатҳи

[1] Stamp Mark. Information security: principles and practice. 288 – c.



3.6-расм. Пакет филтери

Ҳаракат	Манба IP	Масофадиги IP	Манба порт	Масофадаги порт	Протокол	Байроқ
Рухсат	Ички	Ташқи	Ихтиёрий	80	HTTP	Ихтиёрий
Рухсат	Ташқи	Ички	80	>1023	HTTP	ACK
Тақиқ	Барча	Барча	Барча	Барча	Барча	Барча

3.7-расм. Рухсатларни назоратлаш рўйхатига мисол

Юқоридаги қоидага асосан фақат Web учун кириш ва чиқиш мавжуд бўлиб, қолган ҳолларда ҳаракатлар чекланган.

Бу созланмадан бузғунчи қандай қилиб фойдаланиши мумкин ? Бунинг учун дастлаб бузғунчи тармоқлараро экраннинг қайси порти очиқ эканлиги аниқлаш керак. Бошқа сўз билан айтганда портларни сканерлашни амалга ошириши керак.

Очиқ порт аниқлангандан сўнг, у порт орқали зарарли маълумот юборилиши мумкин. Буни олдини олиш учун одатда, тармоқлараро экран мавжуд TCP боғланишларни хотирасида сақлаши керак ва натижада қабул қилинган боғланиш олдинги боғланиш билан бир хил еканлигини аниқлайди.

Эксперт пакети филтрлари. Бу турдаги тармоқлараро экран пакетни филтерлаш вазифасини бажарувчи тармоқлараро экранга мавжуд камчиликларни бартараф этади. Бу турга асосан текширув тармоқ ва транспорт сатҳида амалга оширилади. Камчилиги эса, текшириш вақтининг кўплиги ва илова сатҳи маълумотларини текшириш имкони йўқлигидир (3.8-расм.).[1]

3.8-расм. Эксперт пакети филтри

Илова проксилари. Бу турдаги тармоқлараро экран олдинги икки турга мавжуд камчиликларни ўзида бартараф этади ва илова сатҳида

[1,2] Stamp Mark. Information security: principles and practice. 290 - 293 – c.

ишлайди (3.9 - расм).[1]

3.9-расм. Илова проксилари

Бу тоиқадаги тармоқлараро экранда пакетлар тармоқ, транспорт ва илова сатҳларида текширилади. Илова сатҳи учун пакет “бузулиб” қайтадан “қурилади”.

Шахсий тармоқлараро экран. Бу дастурий воситалар юқоридаги уч турдан бирига тегишли бўлиб, одатда бир ҳостни ҳимоялаш учун фойдаланилади. Бу дастурий воситалар содда интерфейсга эга бўлиб, осон созланади.[2]

3.4. Ҳужумларни аниқлаш тизимлари

Ташкилотларда ҳимоялаш билан боғлиқ бўлган муаммоларни ечиш учун аксарият ҳолларда қисман ёндашишлардан фойдаланишади. Бу ёндашишлар, одатда, аввало фойдалана олувчи ресурсларнинг жорий даражаси орқали аниқланади. Ундан ташқари, хавфсизлик маъмурлари кўпинча ўзларига тушунарли бўлган хавфсизлик хавф-хатарларига реакция кўрсатишади. Аслида хавф-хатарлар жуда кўп бўлиши мумкин. Корпоратив ахборот тизимини фақат қатъий жорий назорати ва хавфсизликнинг умумий сиёсатини таъминловчи комплекс ёндашиш хавфсизлик хавф-хатарларини анчагина камайтириши мумкин.

Охирги вақтда турли компаниялар томонидан қатор ёндашишлар ишлаб чиқилдики, бу ёндашишлар нафақат мавжуд заифликларни аниқлашга, балки ўзгарган эски ёки пайдо бўлган янги заифликларни аниқлашга ва уларга мос химоялаш воситаларини қарши қўйишга имкон беради. Хусусан, ISS(Internet Security Systems) компанияси томонидан хавфсизликни адаптив бошқариш модели ANS (Adaptive Network Security) ишлаб чиқилди.

Хавфсизликка адаптив ёндашиш, тўғри лойиҳаланган ва яхши бошқарилувчи жараён ва воситалар ёрдамида хавфсизлик хавф-хатарларини реал вақт режимида назоратлаш, аниқлаш ва уларга реакция кўрсатишга имкон беради.

Тармоқнинг адаптив хавфсизлиги қуйидаги асосий учта элемент орқали

[1] Stamp Mark. Information security: principles and practice. 290 - 293 – c.

таъминланади:

– хавф-хатарларни бахолаш;
– ҳимояланишни тахлиллаш;
– ҳужумларни аниқлаш.

Хавф-хатарларни бахолаш. Хавф-хатарларни (келтирадиган зарарнинг жиддийлик даражаси бўйича), тармоқ қисм тизимларини (жиддийлик даражаси бўйича), тахдидларни (уларнинг амалга оширилиши эхтимоллиги бўйича) аниқлаш ва рутбалашдан иборат. Тармоқ конфигурацияси муттасил ўзгариши сабабли, хавф-хатарларни бахолаш жараёни хам узлуксиз ўтказилиши лозим. Корпоратив ахборот тизимининг химоялаш тизимини қуриш хавф-хатарларни бахолашдан бошланиши лозим.

Химояланишни тахлиллаш - тармоқнинг заиф жойларини қидириш. Тармоқ уланишлардан, узеллардан, хостлардан, ишчи станциялардан, иловалардан ва маълумот базаларидан таркиб топган. Буларнинг барчаси химояланишлар самарадорлигининг хамда ноъмалум заифликларининг аниқланишига мухтож. Ҳимояланишни тахлиллаш технологияси тармоқни тадқиқлаш, нозик жойларини топиш, бу маълумотларни умумлаштириш ва улар бўйича хисобот бериш имкониятига эга. Агар бу технологияни амалга оширувчи тизим адаптив компонентга хам эга бўлса, аниқланган заифликларни автоматик тарзда бартараф этиш мумкин. Ҳимояланишни тахлиллаш технологияси тармоқ хавфсизлиги сиёсатини, уни ташкилот ташқарисидан ёки ичкарисидан бузишга уринишлардан олдин, амалга оширишга имкон берувчи таъсирчан усул хисобланади.

Химояланишни тахлиллаш технологияси томонидан идентификацияланувчи муаммоларнинг баъзилари қуйидагилар:

– тизимлардаги "тешиклар" (back door) ва троян оти хилидаги дастур;
– кучсиз пароллар;
– химояланмаган тизимдан суқилиб киришга ва "хизмат қилишдан воз кечиш" хилидаги хужумларга таъсирчанлик;
– операцион тизимлардаги зарурий янгиланишларнинг йўқлиги;
– тармоқлараро экранларнинг, Web-серверларнинг ва маълумотлар базасининг нотўгри созланиши ва ҳ.

Хужумларни аниқлаш - корпоратив тармоқдаги шубҳали харакатларни бахолаш жараёни. Ҳужумларни аниқлаш операцион тизим ва иловаларни қайдлаш журналларини ёки реал вақтдаги трафикни тахлиллаш орқали амалга оширилади. Тармоқ узеллари ёки сегментларида жойлаштирилган ҳужумларни аниқлаш компонентлари турли ходисаларни, хусусан, маълум заифликлардан фойдаланувчи харакатларни хам бахолайди.

Тармоқ ахборотини тахлиллаш усуллари. Моҳияти бўйича, хужумларни аниқлаш жараёни корпоратив тармоқда бўлаётган шубҳали харакатларни бахолаш жараёнидир. Бошқача айтганда хужумларни аниқлаш-хисоблаш ёки тармоқ ресурсларига йўналтирилган шубҳали харакатларни идентификациялаш ва уларга реакция кўрсатиш жараёни. Ҳозирда хужумларни аниқлаш тизимида қуйидаги усуллар ишлатилади:

– статистик усул;
– эксперт тизимлари;
– нейрон тармоқлари.

Статистик усул. Статистик ёндашишнинг асосий афзаллиги — аллақачон ишлаб чиқилган ва ўзини танитган математик статистика аппаратини ишлатиш ва субъект ҳарактерига мослаш.

Аввал таҳлилланувчи тизимнинг барча субъектлари учун профиллар аниқланади. Ишлатиладиган профилларнинг эталондан ҳар қандай четланиши рухсат этилмаган фойдаланиш ҳисобланади. Статистик усуллар универсал ҳисобланади, чунки мумкин бўлган хужумларни ва улар фойдаланадиган заифликларни билиш талаб этилмайди. Аммо бу усуллардан фойдаланишда бир қанча муаммолар пайдо бўлади:

1. Статистик тизимлар ходисалар келиши тартибига сезувчанмаслар; баъзи ҳолларда бир ходисанинг ўзи, келиши тартибига кўра аномал ёки нормал фаолиятни характерлаши мумкин.

2. Аномал фаолиятни адекват идентификациялаш мақсадида хужумларни аниқлаш тизими томонидан кузатилувчи характеристикалар учун чэгаравий (бўсағавий) қийматларни бериш жуда қийин.

3. Статистик усуллар вақт ўтиши билан бузғунчилар томонидан шундай "ўрнатилиши" мумкинки, хужум ҳаракатлари нормал каби қабул қилинади.

Эксперт тизимлари. Эксперт тизими одам-эксперт билимларини қамраб олувчи қоидалар тўпламидан ташкил топган. Эксперт тизимидан фойдаланиш хужумларни аниқлашнинг кенг тарқалган усули бўлиб, хужумлар хусусидаги ахборот қоидалар кўринишида ифодаланади. Бу қоидалар ҳаракатлар кетма-кетлиги ёки сигнатуралар кўринишида ёзилиши мумкин. Бу қоидаларнинг ҳар бирининг бажарилишида рухсатсиз фаолият мавжудлиги хусусида қарор қабул қилинади. Бундай ёндашишнинг муҳим афзаллиги — ёлғон тревоганинг умуман бўлмаслиги.

Эксперт тизимининг маълумотлари базасида ҳозирда маълум бўлган аксарият хужумлар сценарияси бўлиши лозим. Эксперт тизимлари, долзарбликни сақлаш мақсадида, маълумотлар базасини муттасил янгилашни талаб этади. Гарчи эксперт тизимлари қайдлаш журналларидаги

маълумотларни кўздан кечиришга яхши имкониятни тавсия қилсада, сўралган янгиланиш эътиборсиз қолдирилиши ёки маъмур томонидан қўлда амалга оширилиши мумкин. Бу энг камида, эксперт тизими имкониятларининг бўшашига олиб келади.

Эксперт тизимларининг камчиликлари ичида энг асосийси - номаълум хужумларни акслантира олмаслиги. Бунда олдиндан маълум хужумнинг хатто озгина ўзгариши хужумларни аниқлаш тизимининг ишлашига жиддий тўсиқ бўлиши мумкин.

Нейрон тармоқлари. Ҳужумларни аниқлаш усулларининг аксарияти қоидалар ёки статистик ёндашиш асосида назоратланувчи мухитни тахлиллаш шаклларидан фойдаланади. Назоратланувчи мухит сифатида қайдлаш журналлари ёки тармоқ трафиги кўрилиши мумкин. Бундай тахлиллаш маъмур ёки хужумларни яниқлаш тизими томонидан яратилган, олдиндан аниқланган қоидалар тўпламига таянади.

Хужумни вақт бўйича ёки бир неча нияти бузуқ одамлар ўртасида хар қандай бўлиниши эксперт тизимлар ёрдамида аниқлашга қийинчилик тугдиради. Хужумлар ва улар усулларининг турли-туманлиги туфайли, эксперт тизимлари қоидаларининг маълумотлар базасининг хатто доимий янгиланиши хам хужумлар диапазонини аниқ идентификациялашни кафолатламайди.

Нейрон тармоқларидан фойдаланиш эксперт тизимларининг юқорида келтирилган муаммоларни бартараф этишнинг бир усули хисобланади. Эксперт тизимлари фойдаланувчига кўрилаётган характеристикалар қоидалар маълумотлари базасидагига мос келиши ёки мос келмаслиги хусусида аниқ жавоб бераолса, нейротармоқ ахборотни тахлиллайди ва маълумотларни аниқлашга ўрганган характеристикаларига мос келишини бахолаш имкониятини тақдим этади. Нейротармоқли ифодалашнинг мослик даражаси 100%га етиши мумкин, аммо танлаш хақиқийлиги тамоман қўйилган масала мисолларини тахлиллаш сифатига боглиқ.

Аввал предмет сохасининг олдиндан танлаб олинган мисолида нейротармоқни тўгри идентификациялашга "ўргатишади". Нейротармоқ реакцияси тахлилланади, қониқарли натижаларга эришиш мақсадида тизим созланади. Нейротармоқ хам вақт ўтиши билан, предмет сохаси билан боглиқ маълумотларни тахлиллашни ўтказишига қараб "тажриба орттиради".

Нейротармоқларнинг суиистеъмол қилинишни аниқлашдаги мухим афзаллиги, уларнинг атайин қилинадиган хужумлар характеристикаларини "ўрганиш" ва тармоқда олдин кузатилганига ўхшамаган элементларни идентификациялаш қобилиятидир.

Юқорида тавсифланган хужумларни аниқлаш усулларининг хар бири афзалликларга ва камчиликларга эга. Шу сабабли, хозирда тавсифланган усулларнинг фақат биттасидан фойдаланувчи тизимни учратиш қийин. Одатда, бу усуллар биргаликда ишлатилади.

Хужумларни аниқлаш тизимларининг туркумланиши. Хужумларни аниқлаш тизимлари IDS (Intrusion Detection System)да ишлатилувчи хужумларни аниқловчи механизмлар бир неча умумий усулларга асосланган. Таъкидлаш лозимки, бу усуллар бир-бирини инкор этмайди. Аксарият тизимларда бир неча усулларнинг комбинациясидан фойдаланилади.

Хужумларни аниқлаш тизимлари қуйидаги аломатлари бўйича туркумланиши мумкин:

– реакция кўрсатиш усули бўйича;
– хужумларни фош этиш усули бўйича;
– хужум хусусидаги ахборотни йигиш усули бўйича.

Реакция кўрсатиш усули бўйича пассив ва актив IDSлар фарқланади. Пассив IDS лар хужум фактларини қайдлайди, маълумотларни журнал файлига ёзади ва огохлантиришлар беради. Актив IDSлар, масалан, тармоқлараро экранни қайта конфигурациялаш ёки маршрутизатордан фойдаланиш руйхатини генерациялаш билан хужумга қарши харакат қилишга уринади.

Хужумларни фош этиш усули бўйича IDSларни қуйидаги иккита категорияга ажратиш қабул қилинган:[1]

– аномал ҳатти-ҳаракатни аниқлаш (anomaly-based);
– суиистеъмолликларни аниқлаш (misuse detection ёки signature- based).

Аномал ҳатти-ҳаракатни аниқлаш йўли билан хужумларни аниқлаш технологияси қуйидаги гипотезага асосланган. Фойдаланувчининг аномал ҳатти-ҳаракати (яъни хужуми ёки қандайдир ғаразли ҳаракати) — нормал ҳатти-ҳаракатдан четлашиш. Аномал ҳатти-ҳаракатга мисол тариқасида қисқа вақт оралиғида уланишларнинг катта сонини, марказий процессорнинг юқори юкланишини ва ҳ. кўрсатиш мумкин.

Агар фойдаланувчининг нормал ҳатти-ҳаракати профилини бир маънода тавсифлаш мумкин бўлганида, ҳар қандай ундан четланишларни аномал ҳатти-ҳаракат сифатида идентифкациялаш мумкин бўлар эди. Аммо, аномал ҳатти-ҳаракат ҳар доим ҳам хужум бўлавермайди. Масалан, тармоқ маъмури томонидан юборилган кўп сонли сўровларни хужумларни аниқлаш тизими "хизмат кўрсатишдан воз кечиш" хилидаги хужум сифатида идентификациялаши мумкин.

[1] Stamp Mark. Information security: principles and practice. 295 – c.

Ушбу технология асосидаги тизимдан фойдаланилганда иккита кескин ҳолат юз бериши мумкин:

– хужум бўлмаган аномал ҳатти-аракатни аниқлаш ва уни хужумлар
– синфига киритиш;
– аномал ҳатти-ҳаракат таърифига мос келмайдиган хужумларни ўтказиб юбориш. Бу ҳолат хужум бўлмаган аномал ҳатти ҳаракатни хужумлар синфига киритишга нисбатан хавфлироқ ҳисобланади.

Бу категория тизимларини созлашда ва эксплуатациясида маъмур қуйидаги қийинчиликларга дуч келади:

– фойдаланувчи профилини қуриш сермеҳнат масала бўлиб, маъмурдан катта дастлабки ишларни талаб этади.
– юқорида келтирилган иккита кескин ҳаракатлардан бирининг пайдо бўлиши эҳтимоллигини пасайтириш учун фойдаланувчи ҳатти-ҳаракатининг чэгаравий қийматларини аниқлаш зарур.

Аномал хатти-харакатларни аниқлаш технологияси хужумларнинг янги хилини аниқлашга мўлжалланган. Унинг кимчилиги - доимо "ўрганиш" зарурияти. Суиистеъмолликларни аниқлаш йўли билан хужумларни аниқлаш технологиясининг мохияти хужумларни сигнатура кўринишида тавсифлаш ва ушбу сигнатурани назоратланувчи маконда (тармоқ трафигида ёки қайдлаш журналида) қидиришдан иборат. Хужум сигнатураси сифатида аномал фаолиятни характерловчи харакатлар шаблони ёки символлар сатри ишлатилиши мумкин. Бу сигнатуралар вирусга қарши тизимларда ишлатилувчи маълумотлар базасига ўхшаш маълумотлар базасида сақланади. Таъкидлаш лозимки, вирусга қарши резидент мониторлар хужумларни аниқлаш тизимларининг хусусий холи хисобланади. Аммо бу йўналишлар бошидан параллел ривожланганлари сабабли, уларни ажратиш қабул қилинган. Ушбу хил тизимлар барча маълум хужумларни аниқласада, янги, ҳали маълум бўлмаган хужумларни аниқлай олмайди.

Бу тизимларни эксплуатациясида хам маъмурларга муаммоларни дуч келади. Биринчи муаммо - сигнатураларни тавсифлаш механизмларини, яъни хужумларни тавсифловчи тилларни яратиш. Иккинчи муаммо, биринчи муаммо билан боглиқ бўлиб, хужумларни шундай тавсифлаш лозимки, унинг барча модификацияларини қайдлаш имкони туғилсин.

Хужум хусусидаги ахборотни йиғиш усули бўйича туркумлаш энг оммавий хисобланади:

– тармоқ сатҳида хужумларни аниқлаш (network-based);
– хост сатхида хужумларни аниқлаш (host-based);
– илова сатхида хужумларни аниқлаш (application-based).

Тармоқ сатхида хужумларни аниқлаш тизимида тармоқдаги трафикни эшитиш орқали нияти бузуқ одамларнинг мумкин бўлган ҳаракатлари аниқланади. Хужумни қидириш "хостдан-хостгача" принципи бўйича амалга оширилади. Ушбу хилга тааллуқли тизимлар, одатда хужумлар сигнатурасидан ва "бир зумда" тахлиллашдан фойдаланиб, тармоқ трафигини тахлиллайди. "Бир зумда" тахлиллаш усулига биноан тармоқ трафиги реал ёки унга яқинроқ вақтда мониторингланади ва мос аниқлаш алгоритмларидан фойдаланилади. Кўпинча рухсатсиз фойдаланиш фаолиятини характерловчи трафикдаги маълум сатрларни қидириш механизмларидан фойдаланилади.

Хост сатхида хужумларни аниқлаш тизими маълум хостда нияти бузуқ одамларни мониторинглаш, детектирлаш ва харакатларига реакция кўрсатишга аталган. Тизим химояланган хостда жойлашиб, унга қарши йўналтирилган харакатларни текширади ва ошкор қилади. Бу тизимлар операцион тизим ёки иловаларнинг қайдлаш журналларини тахлиллайди. Қайдлаш журналларини тахлиллаш усулини амалга ошириш осон бўлсада, у қуйидаги камчиликларга эга:

– журналда қайд этилувчи маълумотлар хажмининг катталиги назоратланувчи тизим ишлаши тезлигига салбий таъсир кўрсатади;

– қайдлаш журналини тахлиллашни мутахассислар ёрдамисиз амалга ошириб бўлмайди;

– хозиргача журналларни сақлашнинг унификацияланган формати мавжуд эмас;

– қайдлаш журналларидаги ёзувни тахлиллаш реал вақтда амалга оширилмайди.

IDSнинг учинчи хили маълум иловадаги муаммоларни қидиришга асосланган.

Назорат саволлари

1. Идентификация.
2. Аутентификация.
3. Авторизация.
4. Аутентификация усуллари.
5. Пароллар асосида аутентификация.
6. Смарт карталар асосида аутентификация.
7. Биометрик хусусиятлар асосида аутентификация.
8. Рухсатларни назоратлаш.
9. Бошқариш моделлари.

10. Тармоқлараро экран ва уларнинг турлари.
11. Ҳужумларни аниқлаш тизимлари.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.
4. https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation
5. https://en.wikipedia.org/wiki/Common_Criteria

4-мавзу. Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Режа:

1. Содда аутентификациялаш протоколлари.
2. Симметрик ва ассиметрик шифрлашга асосланган протоколлар.
3. Secure Shell протоколи.

Таянч иборалар: *протокол, самарадорлик, мобиллик, аутенификация, сеанс калити, калит тақсимлаш, криптографик алгоритм, аутентификация сўрови, фойдаланувчи, шифрлаш, маълумот бутунлиги, тасодифий сон, парол, сертификат, арбитр, имзо қўйиш, имзони текшириш, такрорлаш таҳдид, параллел сеанс таҳдиди.*

4.1. Содда аутентификациялаш протоколлари

Икки ёки ундан ортиқ томонлар бажарадиган, бирор-бир масалани ечиш учун лойиҳалаштирилган ҳаракатлар кетма-кетлиги протокол ҳисобланиб, “ҳаракатлар кетма-кетлиги” сўзи протокол бошидан то охирига қадар кетма-кет бажарилишини билдиради. Ҳар бир ҳаракат навбатма-навбат бажарилади, шунингдек кейинги ҳаракатлар олдинги ҳаракатлар тугагандан кейингина бажарилишни бошлайди. “Икки ёки ундан ортиқ томонлар бажарадиган” сўзи протокол бажарилиши учун камида икки томоннинг иштироки кераклигини билдиради. Протоколни якка тартибда бажариб бўлмайди. Ниҳоят “бирор-бир масалани ечиш учун лойиҳалаштирилган” сўзи протокол қандайдир натижага олиб бориши кераклигини англатади.

Протоколга ўхшаш, аммо бирор-бир натижага олиб бормайдиган ҳаракатлар кетма-кетлиги – бу протокол эмас, аксинча бекорга кетказилган вақт ҳисобланади.

Протоколлар қуйидаги ҳусусиятларга эга бўлиши керак:

– амаллар бошидан охиригача тартибга эга, яъни ҳеч бир амал ундан олдингиси тугамагунча бошланмаслиги керак;

– протоколнинг ҳар бир иштирокчиси протоколга бўйсуниши шарт;

– ҳар бир амал айнан аниқланган бўлиб, икки хил маъно касб этмаслиги керак, ҳар бир вазиятдан аниқ чиқиш йўли бўлиши керак;

– протокол учун битта иштирокчининг бўлиши етарли эмас (икки ёки ундан ортиқ бўлиши керак);

– протоколнинг барча иштирокчилари аввалдан бажариладиган амаллар кетма-кетлиги билан таниш ва уни бажаришга рози бўлишлари керак;

– томонлар бирор бир аниқ вазифани бажарадилар – бу мақсадсиз амаллар

бўлмаслиги керак.

– протокол тўлиқ бўлиши лозим – унда аниқ ҳаракатлар келтирилиши керак.

Ҳар кунлик ҳаётимизда формал бўлмаган протоколлар деярли ҳамма жойда ишлатилади: масалан, телефон орқали торт буюриш, сайловларда овоз бериш ва ҳ.з. Одамлар бу протоколлар ҳақида унча ўйлашмайди. Улар узоқ вақт мобайнида эволюциялашган, улардан қандай фойдаланишни ҳамма билади ва улар ишончли ишлайди.

Протоколлар ишлашини намойиш қилиш учун бир-нечта иштирокчилар ёрдамидан фойдаланамиз (4.1-жадвал).

4.1-жадвал

Протокол иштирокчилари

Иштирокчилар	**Фаолияти**	**Белгиланиши**
Алиса	Барча протоколларнинг биринчи иштирокчиси	**A**
Боб	Барча протоколларнинг иккинчи иштирокчиси	**B**
Кэрол	Уч ва тўрт томонли протоколлар иштирокчиси	**K**
Дейв	Тўрт томонли протоколлар иштирокчиси	**D**
Трент	Ишончли воситачи	**T**
Ева	Пассив бузғунчи	**E**
Мэллори	Ёмон ниятли актив бузғунчи	**M**

Криптографик протокол криптоалгоритмдан ва шифрлаш калитларидан фойдаланишни белгилаб берадиган қоидалар ва процедуралар тўпламидир. Томонлар бир-бирига ишониб дўст бўлиши мумкин ёки аксинча бир-бирига ишонмаслиги, яъни бузғунчи бўлиши мумкин. Криптографик протокол таркибига маълум бир криптографик алгоритм киради, аммо протоколлар фақатгина махфийликни таъминлаш учун мўлжалланмаган. Протоколларда криптографияни ишлатишдан мақсад фирибгарлик ва ноқонуний эшитишни аниқлаш ёки унга йўл қўймаслик.

Умумий қоида шундай:

Протоколда келтирилгандан ташқари кўпроқ нарса билиш ёки ўзгартириш мумкин эмас.

Баъзи протоколларда иштирокчилардан бири иккинчисини алдаши мумкин. Бошқа протоколларда эса бузғунчи протоколни бузиши ёки ундаги

махфий маълумотни билиб олиши мумкин.

Криптографик протоколлар (КП) қуйидаги бир неча иштирокчилардан таркиб топган тақсимланган алгоритмдир:

– одамлар;
– компьютер дастурлари;
– компьютерлар ва ҳисоблаш комплекслари;
– маълумотлар базаси;
– алоқа тармоқлари;
– аутентификация воситалари;
– ва бошқалар.

КПнинг ҳар бир иштирокчиси маълум алгоритмлар кетма-кетлигига мос равишда иш бажаради. Ҳар бир иштирокчи томонидан бажариладиган амал қуйидагича бўлиши мумкин:

– бошқа иштирокчига (ёки иштирокчилар гуруҳига) *хабарни юбориш;*
– бошқа иштирокчидан *хабар қабул қилиш;*
– *ички амал,* яъни иштирокчилар амалга оширадиган баъзи ҳисоблаш ишлари.

КП иштирокчилари 3 синфга бўлинади:

1. *Одатдаги (қонуний) иштирокчилар* (**A, B** ва ҳакозо белгилар кўринишида ифодаланади, индекслар билан ҳам келиши мумкин).

2. *Ишончли воситачи* (**T** белгиси кўринишида ифодаланади, индекс билан ҳам келиши мумкин).

3. Қуйидаги икки синфга бўлинувчи *бузғунчилар:*

a) *Пассив бузғунчилар* (**E** белгиси кўринишида ифодаланади, индекс билан ҳам келиши мумкин).

Пассив бузғунчи бошқа иштирокчиларга юборган хабарни ушлаб олиши, ўғирлаши ва таҳлил қилиши мумкин.

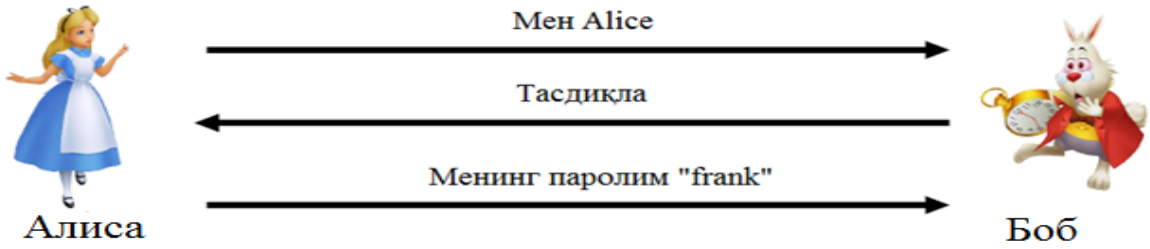
b) *Актив бузғунчилар* (**M** белгиси кўринишида ифодаланади, индекс билан ҳам келиши мумкин).

Актив бузғунчи қуйидаги амалларни бажариши мумкин:

– бошқа иштирокчиларга юборилган хабарни ушлаб олиши ва таҳлил қилиши;
– юборилган хабарни ўзгартириши ёки ўчириши;
– янги хабарни ҳосил қилиб, бошқа иштирокчиларга юбориши;
– ўзини бошқа иштирокчи қилиб кўрсатиши (бундай актив бузғунчиларни *фирибгар* деб номлашади).

Бу бўлимда содда аутентификация протоколларини қуриш ҳақида тўхталиб ўтилади. Бунда содда аутентификация тизимларидан тортиб

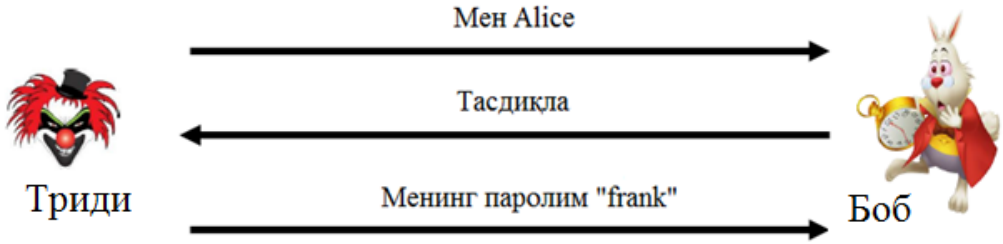
хавфсиз протоколларга қараб борилади.[1]



4.1-расм. Содда аутентификациялаш усули

Бу усул ягона компьютерда фойдаланилганда қулай бўлиб, тармоқда фойдаланишда хавфли. Бундан ташқари Бобда ҳам Алисанинг пароли бўлиши керак. Бу аутентификациялаш усулида қуйидаги таҳдид бўлиши мумкин.

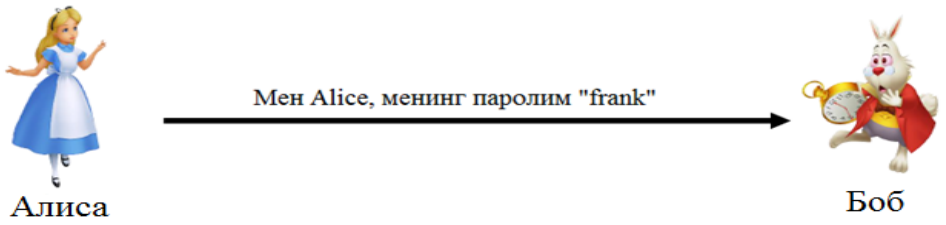
4.2 – расм.



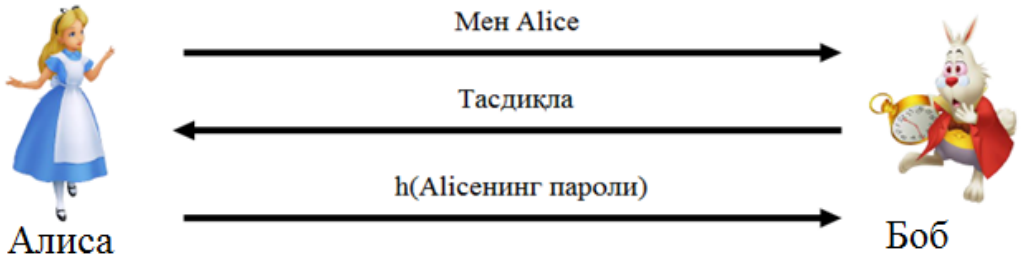
4.3-расм. Қайта юбориш ҳужуми

Юқоридаги протоколни янада самаралироқ тарзда ифодалаш мумкин. Аммо бунда ҳам юқоридаги таҳдид мавжуд (4.4, 4.5 - расмлар). 4.5-расмда парол хешланган ҳолда бўлса ҳам, қайта юбориш таҳдидига бардошсиз.[2]

[1] Stamp Mark. Information security: principles and practice. 318 – с.
[2] Stamp Mark. Information security: principles and practice. 319 – с.

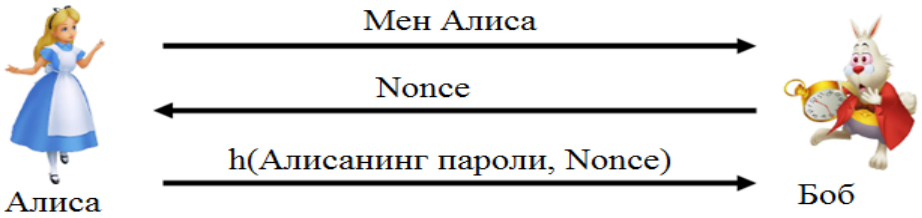


4.4 – расм.



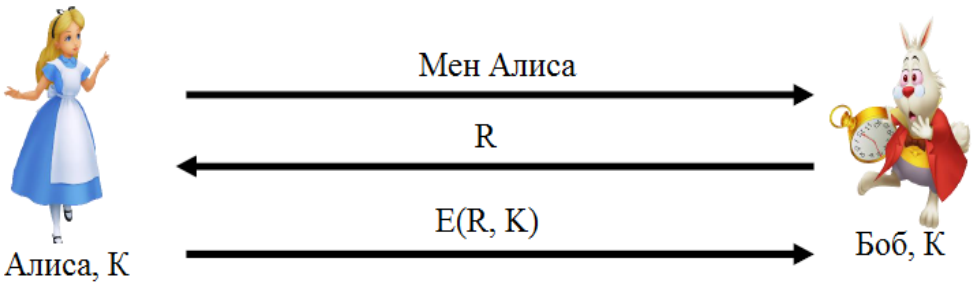
4.5 – расм.

Аутентификациялашда одатда “савол-жавоб” усулидан кенг фойдаланилади (4.6 – расм).



4.6 – расм.

Аутентификацилашда симметрик шифрлаш усулларидан фойдалиниш кенг тарқалган. Бу ҳолда ҳар икки томон бир хил калитда эга бўлиши талаб этилади. [1]



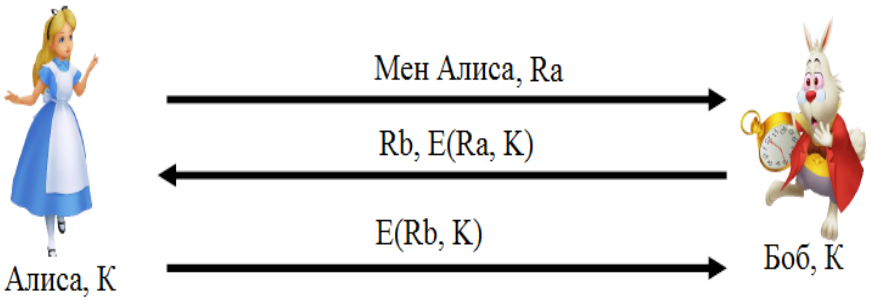
4.7 – расм. Симметрик шифрлаш асосида аутентификация

Бу ерда бир томонлама аутентификация амалга оширилган. Алиса эса Бобни ҳақиқийлигини аниқлай олмайди. Бу муаммо қуйидаги расмда бартараф этилган (4.8 - расм). Аммо бу аутентификация протоколида Алиса ғараз ниятли фойдаланувчи ҳам бўлиши мумкин.

[1] Stamp Mark. Information security: principles and practice. 321 – с.

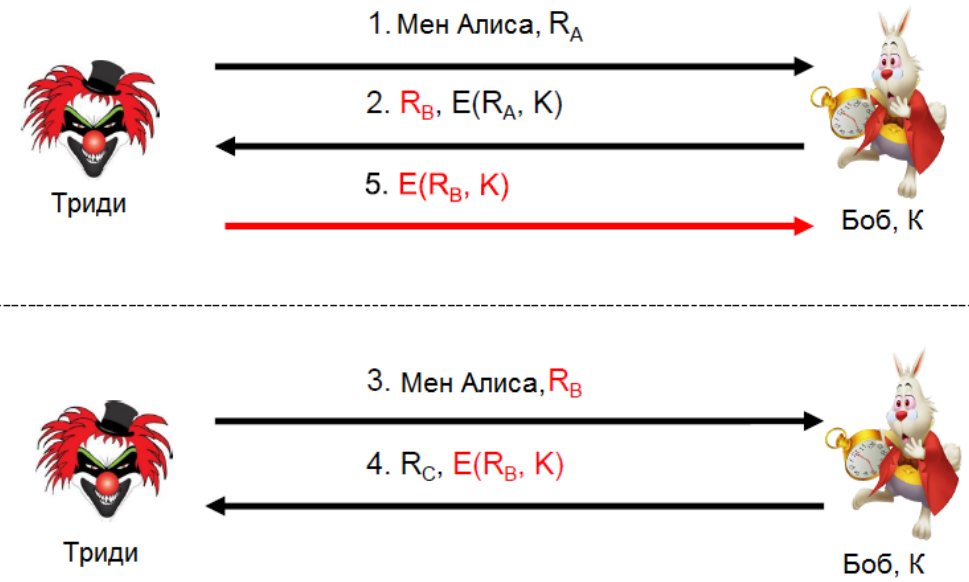
4.8 – расм. Икки томонлама аутентификация

4.8 – расмда келтирилган аутентификация усулини қуйидаги тартибда бартараф этса бўлади (4.9 - расм).



4.9 – расм. Икки томонлама аутентификация

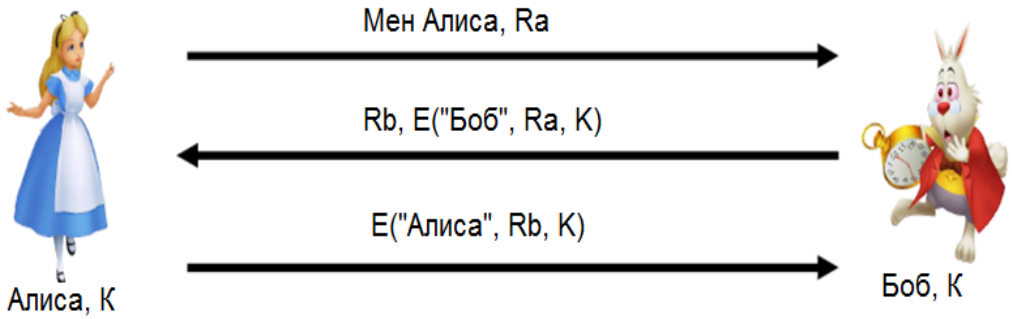
Юқоридаги аутентификациялаш усули бир қараганда хавфсиз кўрилсада, амалда параллел сеанс ҳужумига бардошсиз (4.10 - расм). [1]



4.10 – расм. Пареллел сеанс асосида таҳдид

Юқоридаги таҳдиддан келиб чиқиб шуни айтиш мумкинки, бир томонлама аутентификациялаш усулларидан икки томонлама аутентификациялашда фойдаланиш хавфли экан. Бу қуйидагича бартараф этиш мумкин (4.11 - расм).

[1] Stamp Mark. Information security: principles and practice. 322 – с.

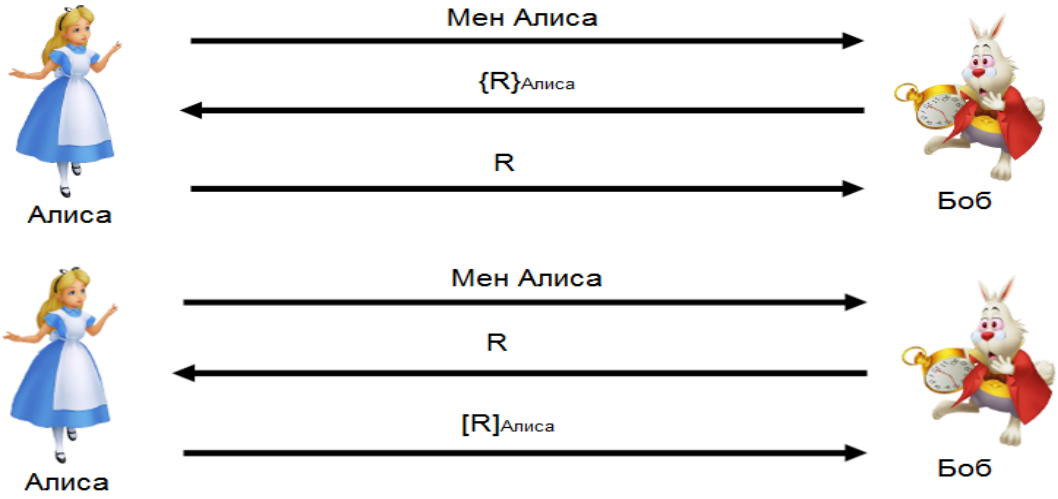


4.11 – расм. Икки томонлама аутентификациялаш

4.2. Симметрик ва ассиметрик шифрлашга асосланган протоколлар

Очиқ калитли шифрлаш алгоритмларидан фойдаланилган протоколларда, қуйидагича белгилашлар киритиб олинади: $\{M\}_{Алиса}$ – Алисанинг очиқ калитидан фойдаланиб шифрлаш, $[M]_{Алиса}$ – Алисанинг махфий калити билан имзолаш. [1]

Очиқ калитли шифрлаш тизими ва ЭРИ алгоритмларидан фойдаланиб, осонлик билан аутентификациялашни амалга ошириш мумкин.



4.12 – расм. Очиқ калитли шифрлаш асосида аутентификациялаш

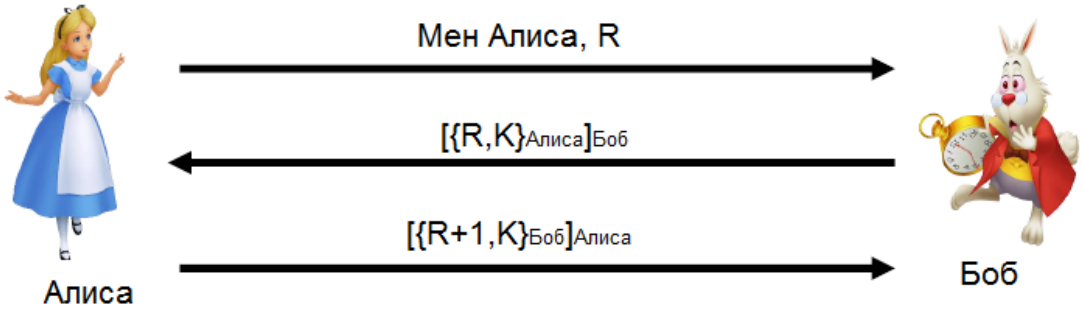
Аутентификациялашда одатда сеанс калити деб аталган калит мавжуд бўлиб, у аутентификация жараёнидан сўнг олинади ва бир сеанс давомида фойдаланилади. Қуйида ассиметик шифрлаш усулидан фойдаланилган ҳолда сеанс калитини узатиш протоколи келтирилган. Самарали саналсада, икки томонлама аутентификацияни амалга оширилмаган.

[1] Stamp Mark. Information security: principles and practice. 323 – c.

4.13 – расм. Сеанс калитини узатиш

Қуйидаги протоколда икки томонлама аутентификациялаш ва сеанс калити махфий калити хавфсиз тарзда узатилган.[1]

4.14 – расм. Сеанс калитини узатиш



4.15 – расм. Сеанс калитини узатиш

Нидхем-Шрёдер протоколи

Рожер Нидхем ва Михаэл Шрёдерлар томонидан яратилган бу протоколда арбитр ва симметрик криптотизимдан фойдаланилади:[2]

1. А - фойдаланувчи ишончли томонга (W) ўзининг исмини, В-фойдаланувчининг исмини ва ўзининг тасодифий сонини узатади.

$A \rightarrow W : A, B, R_A$.

2. З - ишончли томон сеанс калитни генерация қилади. Бу сеанс калитни ва А - фойдаланувчининг исмини В - фойдаланувчи билан умумий

[1] Stamp Mark. Information security: principles and practice. 325 –с.

[2] Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши”. 362 – с.

бўлган калит орқали шифрлайди. Сўнгра А -фойдаланувчи ва ўзи учун умумий бўлган калит ёрдамида А - фойдаланувчининг тасодифий сони, В-фойдаланувчининг исми, калит ва шифрматнни шифрлайди. Ниҳоят у шифрланган маълумотни А -фойдаланувчига узатади:

$W \to B : E_A(R_A, B, k, E_B(k, A))$.

3. А - фойдаланувчи маълумотни дешифрлаб, k -калитни олади. У R_A ва 1 - босқичда узатилган R_A ни солиштиради. Сўнгра А - фойдаланувчи ишончли томон шифрлаган маълумотни В -фойдаланувчига узатади:

$A \to B : E_B(k, A)$.

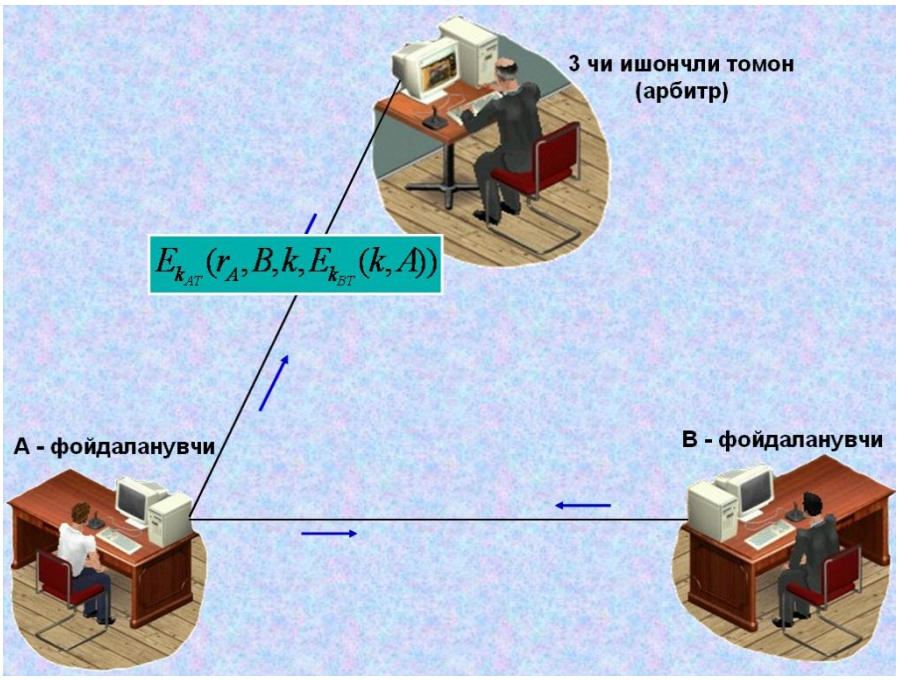
4. В - фойдаланувчи бу маълумотни дешифрлайди ва k - калитни олади. Сўнгра у тасодифий R_B - сонини генерация қилади. Бу тасодифий сонни k -калит ёрдамида шифрлайди ва А -фойдаланувчига узатади:

$B \to A : E_k(R_B)$.

5. А - фойдаланувчи k - калит ёрдамида маълумотни дешифрлайди. А-фойдаланувчи тасодифий $R_B - 1$ - сонини генерация қилади. Бу сонни k -калит ёрдамида шифрлаб қайта В -фойдаланувчига узатади:

$A \to B : E_k(R_B - 1)$.

6. В - фойдаланувчи маълумотни дешифрлаб, $R_B - 1$ - сонини текширади ва ҳақиқатдан А - фойдаланувчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.



4.16 – расм. Уч томонлама аутентификация

Бу протоколда R_A, R_B ва $R_B - 1$ - сонларидан такроран фойдаланилади. Агар криптоаналитик аввал фойдаланилган k -калитни қўлга киритса, 3 -

босқичда А -фойдаланувчи номидан В -фойдаланувчига маълумот узатиши мумкин.

Керберос протоколи

Kerberos протоколи **Нидхем-Шрёдер** протоколининг модификацион варианти ҳисобланади. А - фойдаланувчи В - фойдаланувчи билан маълумот алмашиши учун уларга сеанс калити қуйидагича амалга оширилади: [1]

1. А - фойдаланувчи арбитрга ўзининг исми ва В - фойдаланувчининг исмидан ташкил топган маълумотни узатади:

$$\text{A} \rightarrow \text{W}: \ A, B$$

2. Арбитр иккита маълумотни ҳосил қилади, биринчиси вақт белгиси, ҳаётий вақт L, тасодифий сеанс калит ва А - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва В - фойдаланувчи учун умумий бўлган калит билан шифрлайди, иккинчиси вақт белгиси, ҳаётий вақт, тасодифий сеанс калит ва В - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва А -фойдаланувчи учун умумий бўлган калит билан шифрлайди. У иккала шифрматнни А -фойдаланувчига узатади:

$$\text{W} \rightarrow \text{A}: \ E_A(t, L, k, B), E_B(t, L, k, A) \ .$$

3. А - фойдаланувчи ўзининг калити билан биринчи шифрматнни дешифрлайди. У ўзининг исми ва вақт меткасини бирлаштириб, k - сеанс калит билан шифрлайди. Бу шифрматнни ва арбитрдан қабул қилган иккинчи шифрматнни В - фойдаланувчига узатади:

$$\text{A} \rightarrow \text{B}: \ E_k(A, t), E_B(t, L, k, A) \ .$$

4. В - фойдаланувчи ўзининг калити ёрдамида иккинчи шифрматнни дешифрлайди ва сеанс калитига эга бўлади. Бу сеанс калит ёрдамида биринчи шифрматнни дешифрлайди. Натижада ҳосил бўлган А - фойдаланувчининг исми ва вақт белгиси аввалгиси билан мос бўлса, В - фойдаланувчи А - фойдаланувчини идентификация қилади. Энди А - фойдаланувчи уни идентификация қилиши учун вақт белгисига 1 рақамини қўшиб сеанс калит билан шифрлайди. Ҳосил бўлган шифрматнни А - фойдаланувчига узатади:

$$\text{B} \rightarrow \text{A}: \ E_k(t+1).$$

Агар ҳар бир фойдаланувчининг соатлари арбитрнинг соати билан синхрон равишда ишласа Бу протокол яхши натижа беради.

SKEY дастури

[1] Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши”. 366 – с.

Маълумотнинг хавфсизлигини таъминлаш учун SKEY (маълумотнинг ҳақиқийлигини текширувчи) дастуридан фойдаланиш мумкин. Бу дастур қуйидагича амалга оширилади.

А – фойдаланувчи аутентификация масаласини ҳал қилиш учун тасодифийR сонини киритади. Компьютер $f(R)$, $f(f(R))$, $f(f(f(R)))$, ... қийматларини ҳисоблайди. Бу қийматларни мос холда $x_1, x_2, x_3 \ldots x_{100}$ деб белгилаймиз. А фойдаланувчи бу рўйхатни қоғозга ёзиб олади ва беркитади. Бундан ташқари, компьютер x_{101} қийматни шифрланмаган холда сақлайди.

А – фойдаланувчи системага биринчи марта кириши учун ўз исмини ва x_{101} қийматини киритади. Компьютер $f(x_{100})$нинг қийматини ҳисоблайди ва x_{101} билан солиштиради. Агар қийматлар тенг бўлса, хақиқатдан ҳам А – фойдаланувчи эканлигини тасдиқлайди. Сўнгра компютер маълумотлар базасидаги x_{101} қийматни x_{100}билан алмаштириб қўяди. А – фойдаланувчи эса x_{100} нинг қийматини ўз рўйхатидан ўчиради.

Кейинчалик А – фойдаланувчи ҳар сафар системага киришида охирги ўчирилмаган сонни киритади, масалан i. Компютер $f(x_i)$ қийматни ҳисоблайди ва маълумотлар базасида сақланаётган x_{i+1} сон билан солиштиради. SKEY дастурида ҳар бир сон бир марта иштирок этади. Бундай холатда эса криптоаналитик ҳеч қандай фойдали маълумотга эга бўла олмайди.

4.3. Secure Shell протоколи

SSH протоколи алоқа тармоғида, масофадан туриб амал бажариш, икки тармоқ фойдаланувчиси орасида хавфсиз канал ҳосил қилиш учун фойдаланиладиган криптографик тармоқ протоколидир. Ушбу алгоритм хавфсиз тармоқ орқали махфий алоқани ташкил этиш учун фойдаланилади ва бунда SSH клиент ва SSH сервер орасида хавфсиз канал ҳосил қилинади. Ушбу протоколнинг икки SSH-1 ва SSH-2 вариантлари мавжуд. [1]

Ушбу протокол Unix ёхуд LINUX системаларига ресурсларга мурожаатни амалга оширишда фойдаланиладиган асосий ютилиталардан саналиб, WINDOWS операцион тизими фойдаланувчилари учун ҳам мослаштирилган. Ушбу протокол Telnet ёки бошқа хавфсиз бўлмаган протоколлар (Bekreley rsh, rexec, rlogin) ўрнини босиш мақсадида ишлаб чиқилган. Ушбу протоколда шифрлашдан фойдаланиш орқали маълумотнинг бутунлиги ва конфиденциаллигини таъминлаш амалга оширилган (Лекин, Эдвард Сновден томонидан базида NSA (National Security Agency) томонидан

[1] Stamp Mark. Information security: principles and practice. 352 – c.

SSHни дешифрлаш орқали маълумотдан яширинча фойдаланилган деб ҳам айтилган).

SSH протоколи қуйидаги имкониятларни беради:

– хавфсиз логин билан боғланишни;
– хавфсиз маълумот алмашишни очиқ (ишончсиз) канал орқали амалга оширишни таъминлайди.

SSH протоколлари қуйидагиларга асосланади:

– очиқ калитли шифрлаш алгоритмларига ёки
– рақамли сертификатларга ёки
– паролларга.

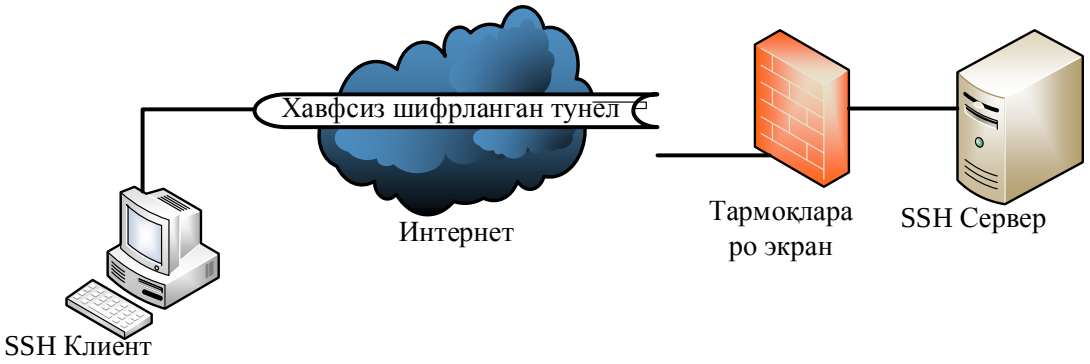
Ушбу протоколнинг икки турдаги варианти, пуллик ва бупул турлари мавжуд.

SSH вазифалари:

– хавфсиз буйруқ-ойнаси (command-shell);
– хавфсиз файл трансфери;
– Port forwarding.

Хавфсиз Command-shell. Command shell тизими Linux, Unix, Windows операцион тизимларда мавжуд бўлиб, асосан дастурий воситаларни юклашда ва бошқа буйруқларни бажаришда фойдаланилади. Хавфсиз command-shell иловаси масофадан туриб, буйруқларни бажаришда, файлларни таҳрир қилишда, каталог таркибини кўришда ва маълумот базасини бошқаришда фойдаланилиши мумкин. Ушбу тизимдан тармоқ администратори масофадан туриб, ўз вазифаларини бажаришда, хизматларни бошқаришда ва бошқа амалларни бажаришда фойдаланиши мумкин. Бунда барча буйруқлар хавфсиз канал орқали юборилади.

Port forwarding. SSH нинг ушбу имконияти, TCP/IP хизмати орқали амалга оширилувчи, e-mail, истемолчи маълумоти базаси ва ҳак. иловалардан хавфсиз канал орқали фойдаланиш учун замин яратади. Ушбу хизмат баъзида тунеллаш каби хизматни амалга ошириб, TCP/IP иловаларини хавфсиз канал орқали амалга оширади. Port forwarding хизмати ўрнатилгандан сўнг, ҳимояланган канал орқали бир томондан (фойдаланувчи қисм) иккинчи томонга (сервер томонга) маълумот жўнатилади. Бунда ҳосил қилинган ягона ҳимояланган канал орқали кўплаб иловалар маълумотлари юборилиши мумкин. Баъзи иловаларни бошқаришда буйруқлар ойнасини ўзи етарли саналмайди, график интерфейс орқали бошқариш таълаб этилади. Ушбу ҳолда SSH ушбу хизмати орқали масофадаги илова билан криптографик ҳимояланган канал ҳосил қилинади. Бунга мисол қилиб, Virtual Network Client (VNC) ни мисол қилиб олиш мумкин.



4.17 – расм. SSH протоколи

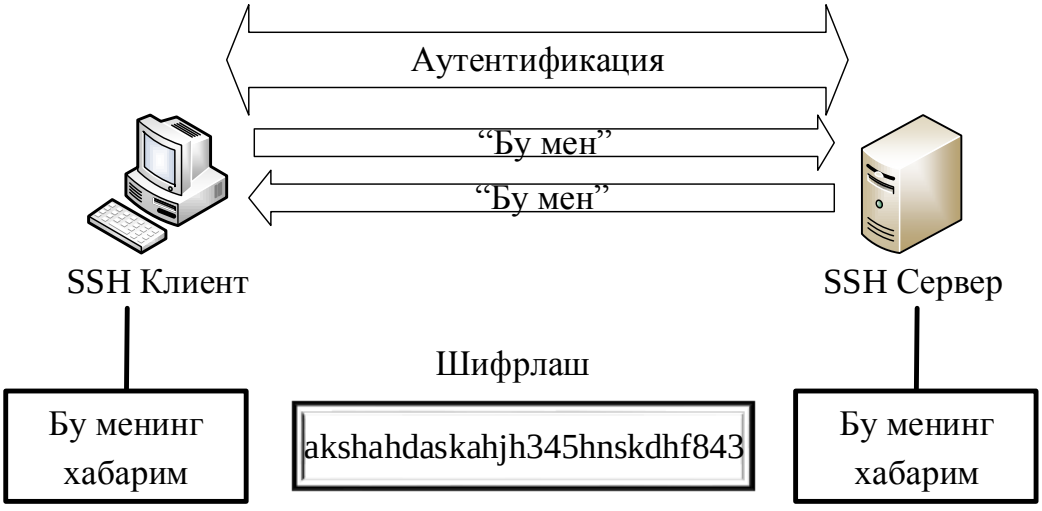
Хавфсиз файл трансфери. Secure File Transfer Protocol (SFTP) протоколи SSH протоколи асосида ишлаб чиқилган бўлиб, бунда FTP протоколида мавжуд кўплаб заифликлар олди олинган.

Биринчидан SFTP фойдаланувчи логин/паролини ва юборилаётган маълумотини шифрлаб жўнатади.

Иккинчидан ушбу протокол SSH нинг порти (22 порт) орқали ишлайди. Бундан ташқари FTP протоколида мавжуд бўлган Network Address Translations (NAT) муаммоси учрамайди.

SSH нинг протокол асоси

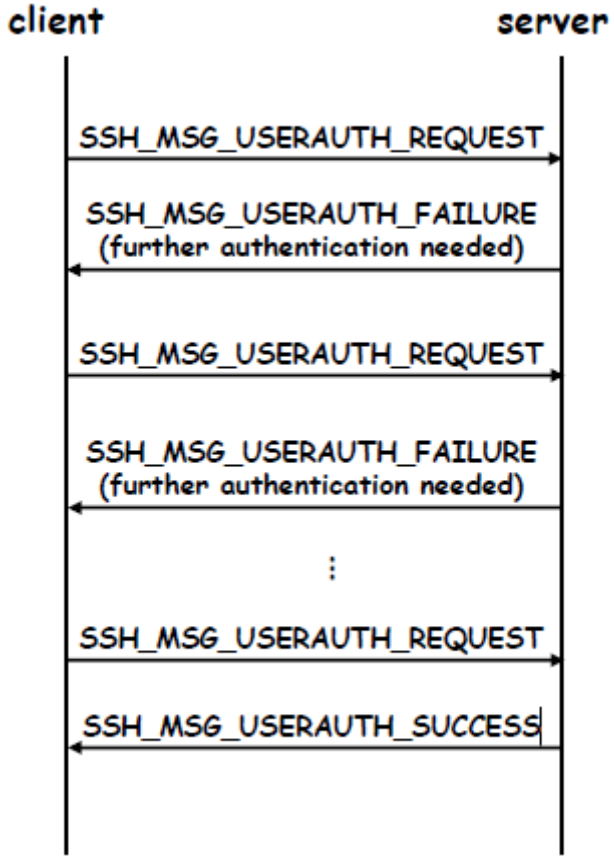
- Фойдаланувчи аутентификацияси (User authentication);
- Ҳостга асосланган аутентификациясилаш (Host authentication);
- Маълумотни шифрлаш;
- Маълумот бутунлиги.



4.18 – расм. SSH аутентификация имконитялари

Фойдаланувчи аутентификацияси (User authentication). Фойдаланувчини ҳақиқийлигини таъминлашда SSH тизими қуйидаги турдаги аутентификациялаш воситаларидан фойдаланилади:

– парол асосида;
– очиқ калитли шифрлаш алгоритмларига асосланган аутентификациялаш усуллари;
– Керберос, NTLM ва бошқалар.



USERAUTH_REQUEST
Фойдаланувчи номи
Хизмат номи
Метод номи
USERAUTH_FAILURE
Фойдаланилаётган аутентификациялаш методлари номлари
байроқ ҳолати
True: дастлабки аутентификация мувофақиятли аммо яхшироқ аутентияикафлаш зарур
False: олдинги аутентификациялаш муофақиятсиз
USERAUTH_SUCCESS
Аутентификация тугади ва сервер хизмат сўровини кутишни бошлайди

Парол асосида аутентификациялаш. Ушбу усул бошқа аутентификациялаш усулларига қараганда кўп учраб, бунда парол ва логини асосида фойдаланувчи ҳақиқийлиги таъминланади. Баъзи протоколлар, FTP, Telnet протоколлари логин ва паролни каналда очиқ ҳолатда юборади. Бу эса бузғунчига тармоқни тинглаш ва уларни қўлга киритиш имконини беради. Бундан фарқли равишда SSH протоколида логин ва парол тармоқда шифрланган ҳолатда юборилади.

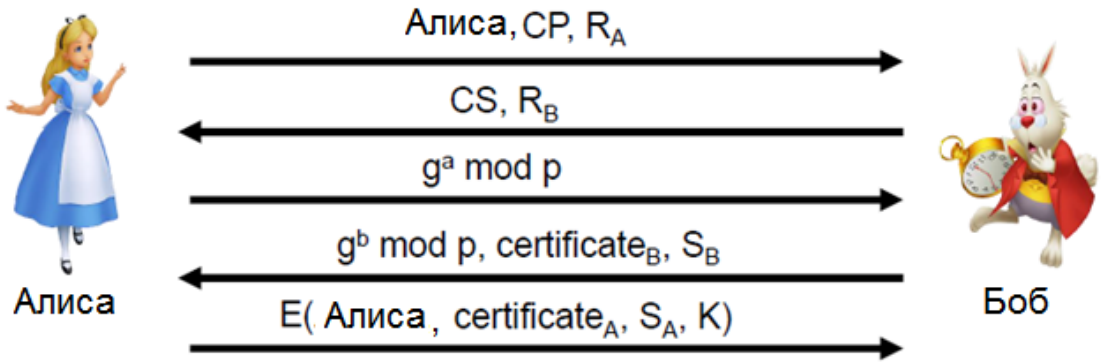
SSH_MSG_USERAUTH_REQUEST
– Фойдаланувчи исми
– Хизмат номи
– Парол
– FALSE (байроқ ҳолати FALSE)
– Парол

Ушбу сўровга сервер қуйидагича жавоб бериши мумкин:

SSH_MSG_USERAUTH_FAILURE,
SSH_MSG_USERAUTH_SUCCESS, ёки
SSH_MSG_USERAUTH_PASSWD_CHANGEREQ

Очиқ калитли шифрлаш алгоритмларига асосланган аутентификациялаш усуллари. Ушбу усул SSH тизимида кенг фойдаланиладиган аутентификациялаш усулларидан биридир. Бунда калит узунлиги 1024 битдан 2048 бит оралиғида бўлади. Ушбу усулда фойдаланувчи очиқ калитлари серверда сақланади. Бундан ташқари фойдаланувчи махфий калитга мос паролга эга бўлиб, бузғунчи махфий калитни билганда ҳам паролсиз тизимни бошқара олмайди.

Қуйида сертификатларга асосланган соддалаштирилган SSH протоколи келтирилган:[1]



4.19 – расм. Содда SSH протоколи

Бу ерда:
CP=”crypto proposed” ва CS = “crypto selected”.
H=h (Алиса, Боб, CP, CS, R_A, R_B, g^amodp, g^bmodp, g^{ab}modp).
S_B= $[H]_{Боб}$;
S_A= [H, Алиса, certificate$_A$] $_{Алиса}$;
K= g^{ab}modp.

SSH да MIM хужуми

[1] Stamp Mark. Information security: principles and practice. 352 – 353 – с.

4.20 – расм. SSH протоколи ўртага турган одам ҳужуми

Алиса қуйидагини ҳисоблайди:

H_a=h (Алиса, Боб, CP, CS, R_A, R_B, g^amodp, g^tmodp, g^{at}modp).

Аммо Боб қуйидагига имзо чекади:

H_b=h (Алиса, Боб, CP, CS, R_A, R_B, g^tmodp, g^bmodp, g^{tb}modp).

Ҳост асосланган аутентификациялаш (Host authentication).

Ушбу усулда фойдаланувчи ҳостига асосланган ҳолда аутентификациялаш амалга оширилади. Агар бир нечта фойдаланувчилар бир машинада бўлса у ҳолда улар учун ягона ҳост калити мавжуд бўлиб, аутентификациялаш айнан шу калитга асосланган ҳолда амалга оширилади. Ушбу ҳолда фойдаланувчи ўзининг шахсий калити ва шахсини таъминлаш учун сертификатини юборади. Сервер эса очиқ калитни айнан шу фойдаланувчига тегишли ёки тегишли эмаслигини ва имзони ҳақиқийлигини текширади.

SSH_MSG_USERAUTH_REQUEST

- Фойдаланувчи исми;
- Хизмат номи;
- “hostbased”;
- Очиқ калитли алгоритм номи;
- Мижоз ҳости учун сертификат ва очиқ калит;
- Мижоз ҳости номи;
- Мижоз ҳостида фойдаланувчи исми;
- Имзо (сессия рақами, ва ҳак).

Маълумотни шифрлаш.

Юборилаётган маълумот бошқалар тушуна олмаслиги учун шифрлаш алгоритмлари ёрдамида шифрланади. Бунда SSH протоколи блокли шифрлаш алгоритмлари саналган (DES, 3DES, Blowfish, AES, ва Twofish) лардан фойдаланади. Маълумот алмашинишдан олдин икки томон орасида фойдаланиланиши керак бўлган крипографик алгоритмлар келишиб олинади. Аутентификация жараёнидан сўнг, умумий калит танланиб, ушбу калит

асосида фойдаланувичилар маълумотни шифрлаб юборишади.

Маълумот бутунлиги.

Маълумот узатилиш жараёнида бузғунчи томонидан маълумотни йўқ қилинишга уриниш ёки маълумотни ўзгартириш ҳолатлари кузатилади. Ушбу ҳолатларни олдини олиш ва текшириш учун SSH тизимларида маълумот бутунлигини таъминлаш алгоритмлари фойдаланилади. SSH1 протоколида маълумотни бутунлигини текширишда оддий 32 битли CRC маълумотни текшириш тизимидан фойдаланилган бўлса, SSH2 тизимида эса MAC (Message Authentication Code) тизимларидан фойдаланилган.

SSH протоколида қуйидаги криптографик алгоритмлардан фойдаланилган:

– TCP ўрнига SCTP протоколи қўлланилган;
– ECDSA ЭРИ алгоритми;
– ECDH калит алмашиниш протоколи;
– UMAC тизими, маълумотни бутунлигини текшириш учун (HMAC ўрнига).

Назорат саволлари

1. Криптографик протокол ва уларга қўйиладиган талаблар.
2. Содда аутентификациялаш усуллари.
3. Симметрик шифрлашга асосланган аутентификациялаш протоколи.
4. Ассиметрик шифрлашга асосланган аутентификациялаш протоколи.
5. Керберос протоколи.
6. SKEY дастури.
7. SSH протоколи.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Ахмедова О.П., Хасанов Х.П., Назарова М.Ҳ., Нуритдинов О.Д.. Криптографик протоколлар. Тошкент, 2012 – 187 бет.
3. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.

5-мавзу. Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар. Дастурий маҳсулотларни яратиш. III

Режа:

1. Дастурий маҳсулотлар хавфсизлиги муаммолари
2. Дастурий маҳсулотларда мавжуд заифликлар.
3. Зараркунанда дастурларнинг таҳлили

Таянч иборалар: *хавфсизлик, таҳдид, дастурий таъминот, инексия, заифлик, хотиранинг тўлиб – тошиши, ахборотни оқиб чиқиши, манзил, хотира, стек, авария, буфер, қуйи хотира манзили, юқори хотира манзили, хотира бўшлиқлари, ўртадан туриб ўзгартириш, оқим, сўров, хэш қиймат, таҳлил, статик таҳлил, динамик таҳлил.*

5.1. Дастурий маҳсулотлар хавфсизлиги муаммолари

Дастурий маҳсулотлар хавфсизлиги ҳозирги кунда келиб, криптография, рухсатларни назоратлаш ва хавфсизлик протоколлари каби муҳим саналади. Бунга сабаб, ахборотларнинг вертуал хавфсизлиги дастури воситалар орқали амалга оширилади. Бундан келиб чиқадики, агар дастурий восита таҳдидга учраган тақдирда, хавфсизлик механизми ҳам барбод бўлади.

Барча дастурий воситаларда заифликлар мавжуд бўлиб, уларнинг муҳимлик даражалари турличадир. Масалан, қиймати 165 мил. $ ни ташкил этган NASA Mars Lander, Марс сайёраси юзасига қўниш вақтида ҳалокатга учраган. Бунган сабаб эса, оддий Инглиз ва метр узунлик ўлчовлари орасидаги фарқ саналган. Бундан ташқари, Денвер халқаро айропортидаги юкларни ушлаш тизимида фойдаланилган дастурий воситадаги камчилик натижасида, 11 ой давомида кунига 1 мил.$ дан зарар кўрилган. [1]

Дастурий воситаларда хавфсизлик муаммоларини мавжудлиги бир нечта омиллар билан белгиланади:

– дастурий воситаларнинг кўплаб дастурчилар томонидан ёзилиши (комплекслилик);
– дастурий маҳсулотлар яратилишида инсон иштироки;
– дастурчининг малакаси юқори эмаслиги;
– дастурлаш тилларининг хавфсиз эмаслиги.

Яратиладиган дастурий воситалар ўзида миллионлаб кодларни ташкил этиб, қуйида буларга аниқ мисоллар келтирилган.[2]

[1,2] Stamp Mark. Information security: principles and practice. 404 – с.

Тизим	Дастурдаги кодлар узунлиги
Netscape	17 мил.
Space Shuttle	10 мил.
Linuxkernel 2.6.0	5 мил.
Windows XP	40 мил.
Mac OS X 10.4	86 мил.
Boeing 777	7 мил.

Таҳлиллар натижаси шуни кўрсатадики ҳар 10 000 қатор кодда, 5 та баг мавжуд бўлар экан. Бошқача қилиб айтилганда ўртача 3кбайт .exe файлда 50 тага яқин баг бўлади.

Дастурий воситалардаги мавжуд таҳдидлар одатда дастурлаш тиллари имкониятлари билан белгиланади. Масалан, нисбатан қуйи дастурлаш тиллари дастурчидан юқори малакани талаб этгани боис, уларда кўплаб хавфсизлик муаммолари пайдо бўлади. Масалан, C#, Java дастурлаш тиллари C ёки C++ дастурлаш тилларига нисбатан хавфсиздир. Сабаби бу дастурлаш тилларида кўплаб муаммолар автоматик равишда, компиляция жараёнида аниқланади.

5.2. Дастурий маҳсулотларда мавжуд заифликлар

Одатда зарарли дастурий воситалар икки турга бўланади:

– дастурлардаги заифликлар (атайин қилинмаган);
– зараркунанда дастурлар (атайин қилинган).

Биринчи турга асосан, дастурчи томонидан йўл қўйилган хатолик натижасида келиб чиққкан зарарли дастурлар мисол бўлса, иккинчи турга бузғунчилик мақсадида ёзилган махсус дастурий маҳсулотлар (вируслар) мисол бўлади.

Қуйида ҳозирда дастурий воситаларда дастурчилар томонидан йўл қўйиладиган таҳдид ва камчиликлар билан танишиб чиқилади.

Хотиранинг тўлиб тошиши (Buffer overflow). Амалда кўп учрайдиган дастурлаш тилларидаги камчиликлар одатда, тақиқланган форматдаги ёки ҳажмдаги маълумотлар киритилиши натижасида келиб чиқади. Бу турдаги таҳдидлар ичида кенг тарқалгани бу – хотиранинг тўлиб тошиш таҳдиди саналади. [1]

Масалан, веб сайтда фойдаланувчидан маълумотлар киритилиши талаб этилса (исми, фамиляси, йили, ва ҳак.), фойдаланувчи томонидан киритилган

[1] Stamp Mark. Information security: principles and practice. 407 – c.

“исм” майдонидаги маълумот сервердаги N та белги ҳажмига эга соҳага ёзилади. Агар киритилган маълумот узунлиги N дан катта бўлган ҳолда, хотиранинг тўлиб тошиши ҳодисаси юзага келади.

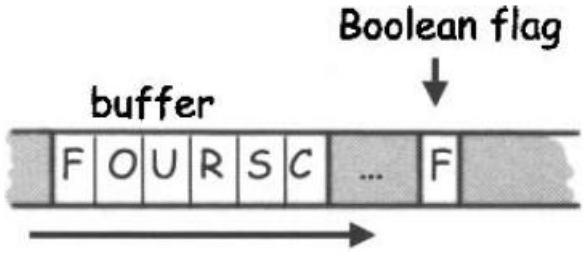
Агар бузғунчи томонидан “керакли” маълумот киритилса, бу ўз навбатида компьютерни бузулишига олиб келади.

Қуйида С дастурлаш тилида ёзилган код келтирилган бўлиб, агар бу код компиляция қилинса хотиранинг тўлиб тошиши ҳодисаси келиб чиқади.

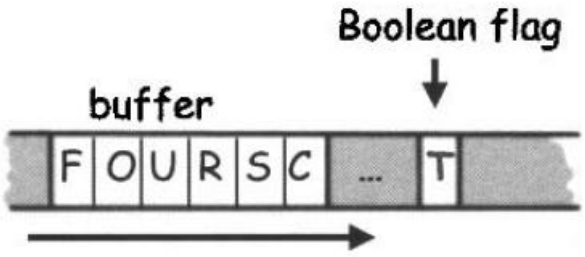
```
int main()
   {
   int buffer [10];
     buffer [20] =37;
     }
```

Сабаби 10 байт ўлчамдаги хотиранинг 20 байтига маълумот ёзилмоқда. Бу эса хотиранинг рухсат этилмаган манзилига мурожаатни келтириб чиқаради.

Агар дастурий маҳсулот аутентификацияни таъминлаш мақсадида яратилган бўлиб, аутентификация натижаси бир бит билан ифодаланади. Агар хотиранинг тўлиб тошиши натижасида ушбу бит бузғунчи томонидан муофақиятли ўзгартирилса Триди ўзини Алиса деб таништириш имкониятига эга бўлади. Бу ҳолат қуйидаги 5.1-расмда келтирилган. Бу ерда F аутентификациядан мувафақиятли ўтилмаганлигини билдиради. Агар Триди F (0 ни) майдон қийматини T (1 га) ўзгартирса, дастурий таъминот Тридини Алиса сифатида танийди ва унга ресурсларидан фойдаланиш имкониятини яратади (5.2 - расм).

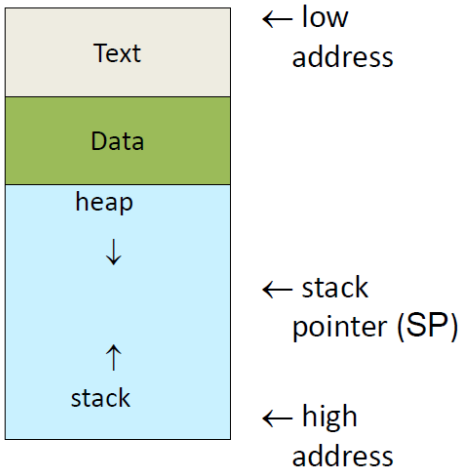


5.1 – расм. Хотира ва мантиқий байроқ



5.2 – расм. Содда хотирани тўлиб тошиши

Хотирани тўлиб тошиш ҳодисасини чиқурроқ ўрганишдан олдин замонавий компьютернинг хотира тузилиши билан танишилиб чиқилади. Компьютер хотирасининг соддалашган кўриниши қуйидаги 5.3 – расмда келтирилган.



5.3 – расм. Хотиранинг тузилиши

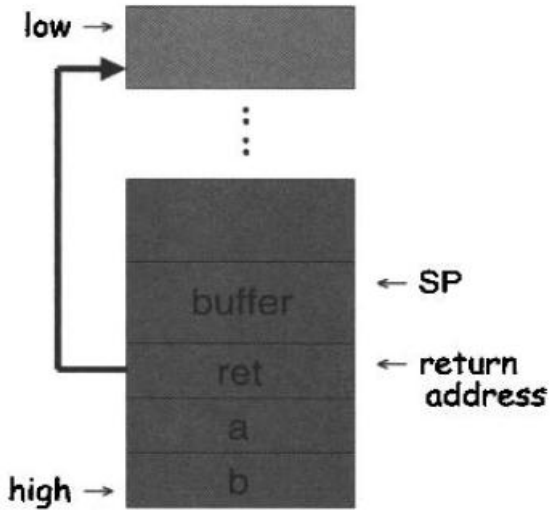
Бу ерда *text* мадонида кодлар сақланиб, *data* соҳасида статик катталиклар сақланади. *Help* соҳаси динамик маълумотларга тегишли бўлиб, *stack* ни процессор учун «кераксиз қоғоз» вазифасини ўтайди. Масалан, динамик локал ўзгарувчилар, функция параметлари, функцияларнинг қайтриш манзиллари каби маълумотлар stack да сақланади. *Stack pointer* ёки *SP* эса stackни энг юқорисини кўрсатади. Расмда stackни қуйидан юқорига чиқиши ҳолати билан ифодаланган.

Stackни аварияга учратиш. Stackни аварияга учраш ҳодисаси асосан хотирани тўлиб тошиши натижасида келиб чиқади. Бу турдаги таҳдидда Триди функцияларни чақирилиши давомида stackни текширади. Функцияни чақириш давомида stackдан фойдаланиш тартиби қуйидаги кодда келтирилган.[1]

```
void func(int a, int b)
{
    char buffer[10];
}
void main()
{
    func(1, 2);
    }
```

[1] Stamp Mark. Information security: principles and practice. 408 – c.

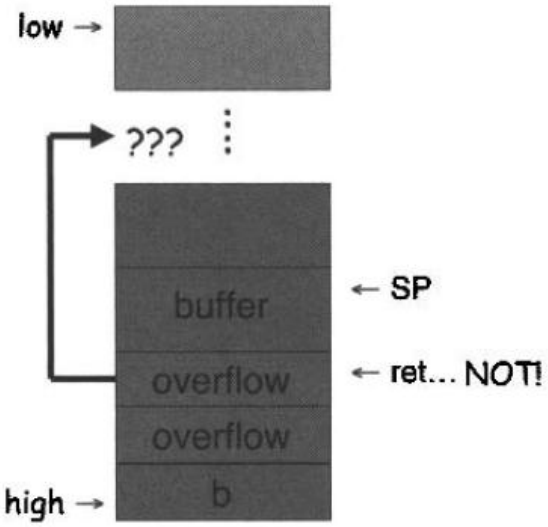
Қачонки *func* функцияси чақирилганда функциянинг параметрлари stack да итариб чиқарилади (5.4 – расм).



5.4 – расм. Stackга мисол

Бу ерда stack функцияни бажарилиши давомида *buffer* массивини яратиш учун фойдаланилмоқда. Бундан ташқари stack функцияни қайтарувчи, функция бажарилиб бўлинганидан кейин ўтиши керак бўлган манзилини ҳам ўзида сақлайди. Расмда кўрсатилгани каби *buffer* қайтувчи манзилдан (ret) дан юқорида жойлашган, яъни, қайтарулувчи манзилдан сўнг *buffer* stackда юкланади. Натижада, агар хотирани тўлиб тошиши юзага келса, у ҳолда хотиранинг *ret* соҳаси қайтадан ёзилади. Бу таҳдид натижасида олиниши мумкин бўлган, реал натижа.

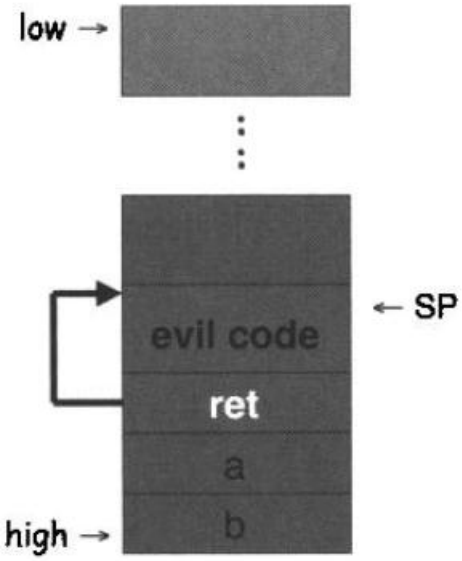
Агар Триди томонидан хотира тўлдирилса ва қайтарувчи манзил тасодифий битлар билан тўлдирилса, у ҳолда дастур мавжуд бўлмаган манзилга сакрайди ва тизим аврияга учрайди (5.5-расм).



5.5 – расм. Хотиранинг тўлиб тошиш муаммоси

Бу ҳолда дастур ишини тўхтатгандан Триди хурсанд бўлиши аниқ.

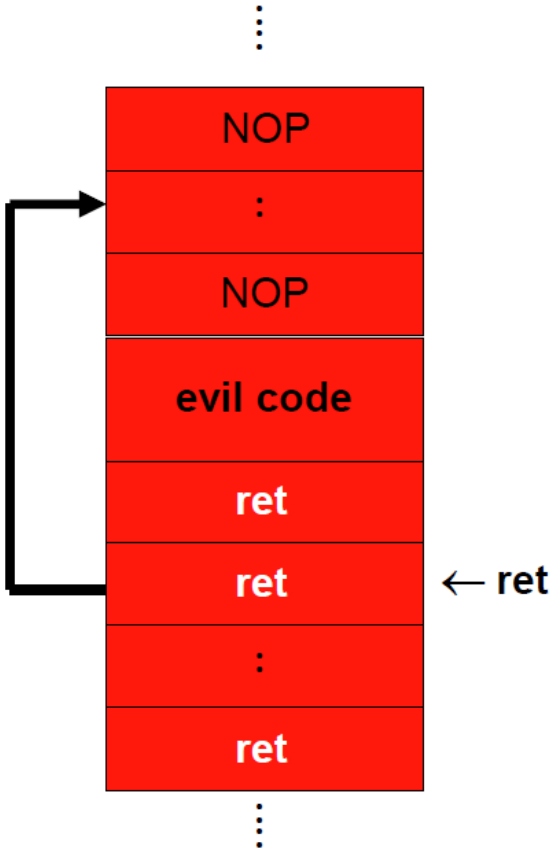
Агар Триди янада ақллироқ бўлса ва буферни тасодифий битлар билан эмас, балки муҳим хотира манзили билан тўлдирса ва бу хотира манзилига бирор зарарли дастур бўлса, у ҳолда жиддийроқ муаммо бўлиши аниқ (5.6 - расм).



5.6 – расм. Зарарли кодни юклаш

Бу ҳолда Триди қуйидаги икки муаммога дуч келиши мумкин. Биринчиси, Триди зараркунанда дустурни хотиранинг қайси манзилига ёзилганини билмайди. Иккинчиси эса, stackда функцияни қайтувчи манзилини аниқ билмайди.

Қуйидаги икки содда хийла натижасида, хотирани тўлиб тошиш жараёнини тезлаштириш мумкин. Биринчиси бу, зараркунанда дастур кодини хотира бўшлиқлари билан (NOP) тўлдириш бўлса, иккинчиси эса, исталган такрорланувчи қайтувчи манзилни қўйишдир (5.7 - расм).



5.7 – расм. Хотирани NOP билан тўлдириш

Бу таҳдид одатда кўплаб, дастурий маҳсулот учун керакли бўлган сериал калитларни бузишда кенг фойдаланилади.

Stackни авария ҳолатидан сақлаш. Стекни авариядан учрашидан ҳимоялашнинг кўплаб усуллар мавжуд бўлиб, улардан бири бу – дастурлаш нуқтаи – назаридан ёндошишдир, яъни киришда маълумот ўлчамини текшириш. Бу имкониятлар C# ва Java дастурлаш тилларида компилятор томонидан бажарилади. [1]

Бошқа бир усул эса, хотирани тўлганини аниқлаш ва автоматик равишда хабар беришдир. Бу ҳолда тизим код стекда юкланишдан олдин уни тўхтатади. Бундан ташқари, функцияни қайтувчи манзилини тасодифий равишда хотирага ёзиш усули мавжуд бўлиб, бунда Триди функцияни қайтувчи манзилини аниқ билмайди.

Ўртадан туриб ўзгартириш. C дастурлаш тилида *strcpy(buffer, input)* функцияси мавжуд бўлиб, у *input* маълумотни *buffer* га кўчириб ёзишни бажаради. Бу ҳолда хотирани тўлиб тошишидан сақлаш учун, *input* маълумотни ўлчамини текшириш талаб этилади. Бу ҳимоя усули фақат ўлчамни текшириб, маълумот таркибини текширмайди. Бу ҳолда *ўртадан*

[1] Stamp Mark. Information security: principles and practice. 415 – c.

туриб ўзгартириш таҳдиди бўлиши мумкин.[1]

Бунга қуйидагича мисол келтириш мумкин. Масалан, фойдаланувчи Веб саҳифадан туриб маълумотларни киритди ва у қуйидаги сўров шаклида ифодаланди:

```
http
://www.things.com/orders/final&custID=112&num=55A&qty=20&price=10&
shipping=5&total=205
```

Сервер томонидан бу маълумот қуйидагича таҳлилланади: фойдаланувчининг ID рақами 112 га тенг фойдаланувчи ҳар бирининг нархи 10 $ дан бўлган 55 тартиб рақамли маҳсулотдан 20 та сотиб олди ва 5 $ етказиб бериш нархи билан жами 205 $ доллар тўловни амалга оширган. Бу сўров сервер томонидан текширилганида ҳеч қандай хатолик топилмади.

Аммо Триди бу кўровни қуйидаги сўров билан алмаштирса,нима ҳодиса рўй беради ?

```
http
://www.things.com/orders/final&custID=112&num=55A&qty=20&price=10&
shipping=5&total=25
```

Бу сўров ҳам олдингиси каби сервер томонидан текширишдан муофаққиятли ўтади, аммо унинг маноси тамомила бошқа !!!

Тезкор мурожат шарти таҳдиди (Race condition ёки race hazard). Бу дастурий маҳсулотнинг ёки электрон тизимнинг ўзини тутиш ҳолати бўлиб, чиқиш қиймати бошқариб бўлмас бошқа ҳодисалар кетма-кетлиги ёки вақтига боғлиқ бўлади. Дастурлашда бу ҳолда хатолик юзага келиб, иккита сигнал биринчи чиқиш учун ҳаракат қилади. Бу ҳодиса асосан, дастурлашда параллел ҳисоблашда (thread) юзага келади. [2]

Қуйида иккита оқим томонидан ўз қийматини бирга ошириш учун бажарган тезкор мурожати келтирилган. Агар тизим тўғри ишлаганда қуйидаги натижа олиниши шарт эди.

Thread 1	Thread 2		Integer value
			0
read value		←	0
increase value			0
write back		→	1
	read value	←	1
	increase value		1

1 Stamp Mark. Information security: principles and practice. 418 – c.
[2] Stamp Mark. Information security: principles and practice. 419 – c.

	write back	→	2

Аммо, тезкор мурожаат натижасида қуйидаги ҳолат келиб чиқди:

Thread 1	Thread 2		Integer value
			0
read value		←	0
	read value	←	0
increase value			0
	increase value		0
write back		→	1
	write back	→	1

Бу таҳдид мавжуд дастурий маҳсулотларда time-of-check-to-time-of-use (TOCTTOU) заифлиги мавжуд бўлади.

Одатда бу таҳдидларни олдини олишда дастурлаш тилларида глобал ўзгарувчини қулфлаб қўйиш усулларидан фойдаланилади.

SQL инексия (SQL injection). SQL инексия таҳдиди маълумотлар базасига тегишли бўлган таҳдид бўлиб, SQL сўровларга тақиқланган белгиларни киритиш ва бунинг натижасида маълумотлар базасида бошқа натижа олишга қаратилган. Бу таҳдид тури энг кўп учрайдиган таҳдид тури бўлиб, унинг ҳажми йилдан – йилга ортиб бормоқда.

Бу таҳдид асосан тақиқланган белгиларни текширмаслик натижасида келиб чиқади. Қуйида ушбу заифликни ўз ичига олган SQL сўрови келтирилган:

```
statement = "SELECT * FROM users WHERE name = '" +
userName + "';"
```

Бу сўровга асосан айнан керакли фойдаланувчи номи маълумотлар базасидан қидирилмоқда. Агар бу сўров бузғунчи томонидан userName ўрнига ' OR '1'='1 киритилса, қуйидиги сўров ҳосил бўлади:

```
SELECT * FROM users WHERE name = '' OR '1'='1';
```

Натижада маълумотлар базасидан барча фойдаланувчилар тўғрисидаги маълумотлар чиқарилади. Бу ерда қуйидаги тақиқланган белгилар бирикмасидан ҳам фойдаланиш мумкин.

```
' OR '1'='1' --
```

```
' OR '1'='1' ({
' OR '1'='1' /*
```

Бу таҳдидларни олдини олишда кирувчи сўров махсус белгиларга текширилиши керак. Аммо, бу сўровларни кундан-кунга янги турлари келиб чиқмоқда.

5.3. Зараркунанда дастурларнинг таҳлили

Дастурий воситалар билан учраб турадиган таҳдидларнинг иккинчиси бу – атайин ёзилган зарарли дастурий воситалардир. Бундай дастурий воситалар малакали дастурчилар томонидан ёзилган бўлиб, улар аниқ мақсадга қаратилган бўлади. Бу тоифадаги дастурларни аниқлашда ва таҳлиллашда одатда статик ва динамик таҳлиллаш усулларидан кенг фойдаланилади.

Ҳар бир таҳлиллаш ўз навбатида содда ва мураккаб таҳлиллашларга бўлинади.

Содда статик таҳлиллаш. Зараркунанда дастурий воситаларнининг *содда статистик* таҳлили дейилганда улар ҳақида дастлабки маълумотларни олишдан иборат бўлган таҳлил тушунилади. Бу таҳлил натижасида зараркунанда дастурларнинг (ЗД) кодларнинг тузулиши, дастурий томондан тузулиши, қайси библотекалардан фойдаланганлиги ва ҳ.к. лар ҳақида маълумот олиш мумкин.[1]

ЗДларни дастлабки таҳлил қилишда антивирус воситалари кенг фойдаланилади. Одатда икки турдаги, *файл сигнатурасига* асосланган (масалан, Касперский) ва *эвристикага* асосланган (масалан, ESET NOD32)антивирус воситаларидан кенг фойдаланилади. Сигнатурага асосланган антивирус дастурлар ЗД ларни ўзининг базасида мавжуд ёки мавжуд емаслигини текширади. Бу эса ЗД топишда ҳар доим ҳам катта фойда бермайди. Эвристикага асосланган антивирус воситалари сигнатурага асосланган антивирусларга қараганда анча кенг имкониятга эга бўлиб, ЗД ларни топишда кенг фойдаланилади.

Амалда ЗД статистик таҳлил ўтказишда улар бир нечта антивирус воситалари ёрдамида текширилади ва улардан олинган натижалар таҳлил этилади. Ушбу вазифани бажаришда http://www.virustotal.com/ онлайн ЗД таҳлили воситаси кенг фойдаланилади. Ушбу онлайн таҳлиллаш воситаси нафақат ЗД бир нечта антивирус воситалари ёрдамида тестлайди, балки уларнинг дастурий томондан тузулишини ва улар ҳақида қўшимча маълумотларни беради.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 42 – с.

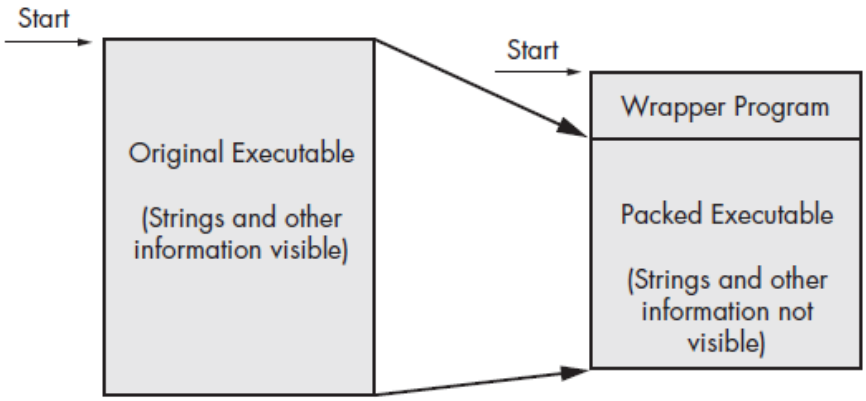
ЗД статистик таҳлил қилишда қуйидаги усуллардан фойдаланилади:

ХЭШ қиймат асосида таҳлиллаш. Хэш функциялаш ЗД аниқлаш учун керакли бўладиган дастлабки таҳлиллаш усулларидан бири бўлиб, унга асосан ихтиёрий хэш қийматни ҳисоблаб берувчи алгоритмлар асосида (масалан, MD5, SHA1)ЗД хэш қиймати ҳисобланади. Ушбу олинган хэш қиймат асосида қуйидагиларни аниқлаш мумкин:

- Хэш қийматни дастурнинг (масалан, таҳлилланувчи ЗД) ёрлиқи сифатида фойдаланиш;
- Олинган хэш қийматни бошқа ЗД таҳлилловчи дастурлар учун юбориш;
- Олинган хэш қийматни онлайн тарзда қидириш ва ЗД рўйхатида мавжуд/ мавжуд эмаслигини аниқлаш.

ЗД лардан "қаторларни (strings)" аниқлаш. Ҳар бир дастурий восита яратилишида маълум кетма-кетмаликлан иборат бўлган матн шаклидаги маълумотлардан фойдаланилади. Масалан, "GDI32.DLL", "99.124.22.1", "Mail system DLL is invalid.!Send Mail failed to send message" ва ҳак. Албатта, яратилган дастурий воситалар якунида улар .exe, .dll файл шаклларида ассембланади. Бошқа сўз билан айтганда, бу кенгайтмадаги файллар ўн олтилик (hex)саноқ системасида ифодаланади (0x42, 0x41, 0x44→ BAD).Белгиларни 16 лик саноқ тизимига ўтказишда одатда ASCII (8-бит)ва Unicode (16-бит)кодлаш стандартларидан фойдаланилади. Ушбу стандартларда ҳар бир келган белгилар кетма-кетлиги охири 0x00 билан тугайди. Бунинг маноси эса сўзнинг тугуганлигини англатади. [1]

Сиқилган ЗД. Одатда ЗД воситалар статистик таҳлилларга бардошли бўлиши учун улар сиқилади. Қуйида ҳақиқий ва сиқилган ҳолатдаги файл кўриниши келтирилган.



5.8-расм. Сиқилган ва ҳақиқий файл кўриниши

Portable Executable (PE)файл формати. Ушбу файл формати таркибига юкланувчи, кутубхона файл кенгайтмалари киради (масалан, .cpl, .exe, .dll,

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 44 – c.

.ocx, .sys, .scr, .drv, .efi, .fon) ва улар Windows ОТ учун фойдаланилади. ЗД ларда кутубҳона файлларидан асосан импорт (import)қилиш орқали асосий дастурга боғланади. Ушбу боғланиш уч турда амалга оширилиши мумкин: статик, динамик ва юкланганда.

Статик турдаги боғланишларда кўра кутубхона файллари тўлиқ кўчирилиб асосий дастур ичига ташланади. Бу турдаги боғланишлар асосан UNIXва LinuxОТ да кенг фойдаланилади. Бунда асосий дастур коди ва кутубхонага тегишли кодларни ажратиш қийин бўлади.

Юкланганда талаб этиладиган боғланишлар асосан ЗД яратишга кенг фойдаланилиб, унга асосан фақат функция чақирилган пайтда боғланиш амалга оширилади.

Кўплаб Windows ОТлари бошқа дастурларга ўз ресурсларидан фойдаланишга рухсат беради. PE файллар ўзида ҳар бир кутубхона ва кутубхонадаги функциялар ҳақидаги маълумотни сақлайди.

Кўплаб мавжуд DLL (Dynamic-link library) файллар ўзида кўплаб функцияларни сақлайди. Қуйида WINDOWS ОТ га тегишли DLL файллар ва уларнинг вазифаси келтирилган:

DLL	Тавсифи
Kernel32.dll	Ушбу DLL файл кенг тарқалган бўлиб асосан ўзак функциялардан ташкил топган, масалан, хотирани, файлларни ва қурилмани бошқариш ва унга эгалик қилиш (http://www.geoffchappell.com/studies/windows/win32/kernel32/api/)
Advapi32.dll	Ушбу DLL файл WINDOWS ОТ нинг кенгайтирилган имкониятларини бошқаришда, масалан, хизматларни ва регисторларни бошқаришда фойдаланилади (http://www.geoffchappell.com/studies/windows/win32/advapi32/api/etw/index.htm?tx=14).
User32.dll	Ушбу DLL файл фойдаланувчи интерфейсини ташкил этувчиларни, масалан, тугмалар, скрол барслар, фойдаланувчи ҳаракатларига жавоб берувчи вазифаларни бажарувчи функциялардан иборат.
Gdi32.dll	Ушбу DLL файл график ҳолатни намойиш этиш ва бошқариш учун керакли бўлган функциялардан иборат.
Ntdll.dll	Ушбу DLL файл WINDOWS ОТ ўзагининг фойдаланувчи режимидаги кўринишини ифодаловчи функциялардан иборат. Ушбу вазифаларни одатда Kernel32.dll ва Advapi32.dll кутубхонасини чақириш орқали бажаради, масалан, жараёнларни бошқариш, вазифаларни яшириш ва ҳак.
WSock32.dll ва Ws2_32.dll	Ушбу DLL файллар тармоққа тегишли бўлиб, тармоққа тегишли бўлган вазифаларни бажараридиган функциялардан иборат.
Wininet.dll	Ушбу DLL файл тармоқнинг юқори вазифаларини бажарувчи

	функциялардан иборат бўлиб, тармоқ протоколлари, FTP, HTTP, ва NTP ларни назоратлайди.

PE файл сарлавҳаси ва бўлимлари. PE файллари сарлавҳаси уларни импорт қилганда қараганда кўпроқ маълумотларни ўзида сақлайди. PE файллар бир нечта бўлимлардар иборат бўлиб, бу бўлимлар ва уларда сақланадиган маълумотлар қуйидагилар:

.text	Ушбу бўлим CPU да юкланувчи кодлардан иборат.
.rdata	Дастурда мавжуд глобал эълон қилинган фақат ўқиш ҳуқуқига эга маълумотлардан ташкил топган.
.data	Дастур орқали бошқариладиган глобал маълумотларни сақлайди.
.idata	Баъзида мавжуд бўлади ва ўзида импорт қилинадиган функция маълмотларини сақлайди. Ушбу бўлим мавжуд бўлмаса, ушбу ҳолда маълумотлар .rdata бўлимида сақланади.
.edata	Баъзида мавжуд бўлади ва ўзида экспорт қилинадиган функция маълмотларини сақлайди. Ушбу бўлим мавжуд бўлмаса, ушбу ҳолда маълумотлар .rdata бўлимида сақланади.
.pdata	64-битли тизимларда мавжуд бўлади ва хатоликларни тузатиш маълумотларини сақлайди.
.rsrc	Функцияларни бажаришда керакли бўлган ресурсларни ўзида сақлайди.
.reloc	Кутубхона файлларини қайта жойлаштириш учун керакли бўлган маълумотларни сақлайди.

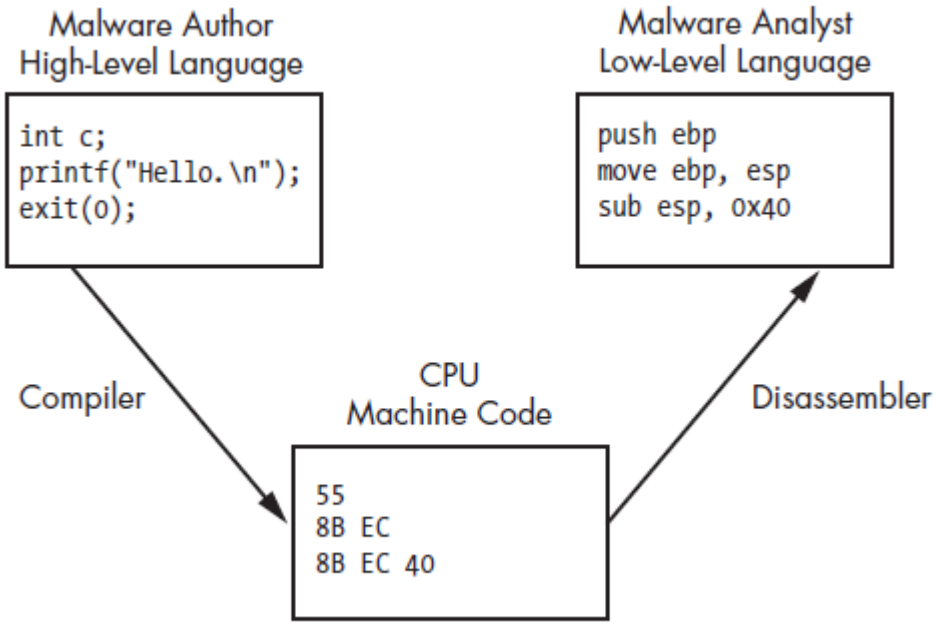
PE сарлавҳаси ЗД таҳлил қилишда керак бўладиган кўплаб муҳим маълумотларга эга. Улар қуйидаги жадвалга келтирилган:

Imports	ЗД фойдаланилган кутубхона файллари
Exports	Кутубхона ичидаги бошқа кутубхона/ дастур орқали чақирилган функциялар
Time Date Stamp	Дастур компиляция қилинган вақти
Sections	Файлдаги бўлим номи, унинг хотирадаги ва дискдаги ўлчами
Subsystem	Дастурни буйруқлар сатри шаклида ёки фойдаланувчи интерфейси шаклида ишлашини кўрсатади
Resources	Файлда мавжуд иконкалар, менюлар, қаторлар ва бошқа малумотлар.

Мураккаб статик таҳлил. Содда статик ва динамик таҳлиллаш усуллари фойдаланишда қулай саналсада, зараркунандан дастурлар ҳақида тўлиқ маълумот олишга имкон бермайди. Шунинг учун амалда бу усулларнинг кенгайтирилган шакли кенг фойдаланилади. Мураккаб статик таҳлилнинг моҳияти тескари инжинерлик хоссасидан фойдаланган ҳолда, ЗД ни дисассембрлаш амали орқали таҳлил қилишга асосланган. Лабаратория

ишининг назарий қисмида x86 архитектураси ва унда дизассемблаш амали билан танишилиб чиқилади. [1]

ЗД яратишда юқорида дастурлаш тилидан фойдаланилади ва машина кодини ҳосил қилишда компиляторлардан фойдаланилади. Дизассемблашда машина кодидан ассемблер код ҳосил қилинади ва уни таҳлиллаш орқали ЗД ҳақида хулоса чиқарилади. Қуйида ушбу жараён келтирилган:



5.9-расм.

5.9 - расмда келтирилган соддалаштирилган модел қуйида келтирилган олти турли даражалардан иборат:

Қурилма (Hardware). Қурилма даражаси физик сатҳ бўлиб, электрик схемалардан иборат ва бу қурилмаларда мантиқий амаллар, XOR, AND, OR ва NOT бажарилади. Сабаби, физик жихоз ёки қурилмани дастурий томондан бошқариш жуда қийин.

Микрокодлар (Microcode). Микрокодлар сатҳи прошивка (firmware) сатҳи деб ҳам аталади. Микрокодлар маълум аниқланган жихозларги мўлжалланган бўлади. Уларнинг асосий вазифаси юқори машина тилида ёзилганкодларни қурилмага мослаштириб бериш.

Машина коди (Machine code)**.** Машина коди ўн олтилик саноқ тизимида ёзилган рақамлардан иборат бўлиб, процессорни нима иш бажаришини белгилайди. Машина коди юқори дастурлаш тилида ёзилган кодларни компиляция қилиш жараёнида ҳосил қилинади.

Қуйи даражали дастурлаш тиллари (Low-level languages). Қуйи

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 65 – c.

даражали дастурлаш тиллари инсон ўқий оладиган компьютер архитектураси кетма-кетлиги ҳолати бўлиб, кенг тарқалган қуйи даражали дастурлаш тили бу – ассемблер тилидир. ЗДларни машина коди орқали таҳлил этиш инсон учун мураккаб саналгинлиги сабабли, ассемблер тилида ёзилган кодларни таҳлил этиш орқали ЗД ҳақидамаълумотлар олинади.

Юқори даражали дастурлаш тиллари (High-level languages). Кўплаб дастурчилар юқори даражали дастурлаш тилларидан фойдаланган ҳолда ўз иловаларини яратадилар. Юқори даражали дастурлаш тиллари машина тилидан узоқ бўлиб, инсон тушиниши учун анча осондир. Юқори дастурлаш тилларига C,C++ ва бошқаларни олиш мумкин. Бу дастурлаш тилида ёзилган кодлар компиляторлар орқали машина кодига айлантирилади.

Изоҳлаш тиллари (Interpreted languages). Изоҳлаш тиллари энг юқори даражали тиллар ҳисобланади. Кўплаб дастурчилар айнан шу тиллардан, C#, Perl, .Net ва Javaфойдаланадилар. Бу тиллардан ёзилган кодлар машина тилига компиляция этилмайди, балки байткодларда ўтказилади. Байткодлар дастурий кодларни оралиқ ифодаланиши бўлиб, интерпритаторлар орқали машина кодига айлантирилади.

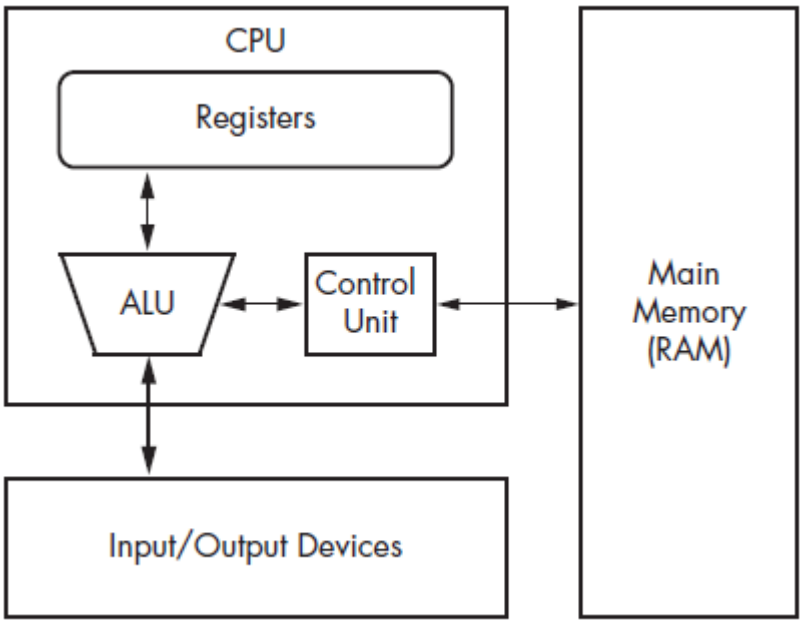
ЗД доимий хотирада машина тилининг бинар шаклида сақланади. 4.1-расмда келтирилган схемага асосан, ЗД дизассембрланганда, бинар ҳолатдаги ЗД кодини чиқишда ассемблер тилига ўтказиш амалга оширилади.

Ассемблер тили бир нечта тиллар тўплами бўлиб, ҳар бир тил айнан бир микропроцессор (x86, x64, SPARC, PowerPC, MIPS, ва ARM) учун мўлжалланган бўлади.

Ҳозирда кенг тарқалган шахсий компьютерлардаги архитектура бу x86 бўлиб, кейинчалик яратилган AMD64 ёки Intel 64 архитектуралари ҳам x86 ни қўллаб қувватлайди. Шунинг учун аксарият, яратувчилар x86 архитектурасига асосланган ЗД дастурларни яратадилар.

x86 архитектураси. Амалда фойдаланилаётган кўплаб архитектуралар (шу жумладан x86 ҳам) Жон Фон Нейман архитектурасидан келиб чиққан (10-расм).[1]

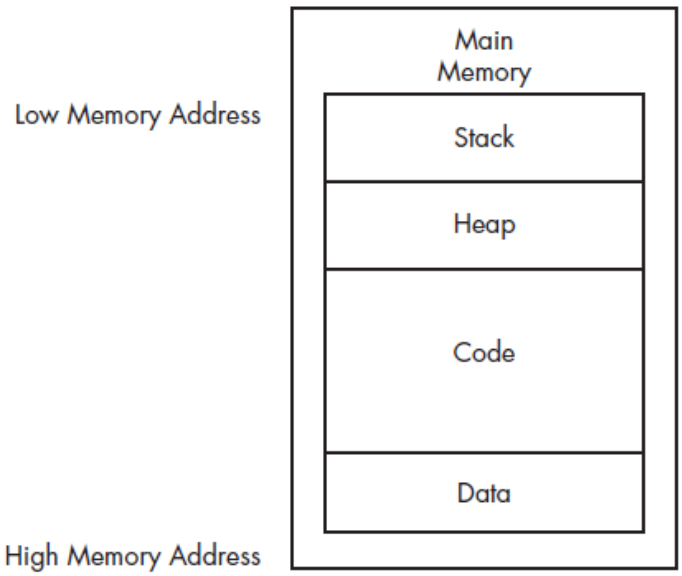
[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 68 – c.



5.10-расм. Жон Фон Нейман архитектураси

Юқоридаги расмда келтирилганидек, CPU бир нечта ташкил этувчилардан иборат. Бошқарув бирлашмаси (Control Unit) регистрлардан фойдаланган ҳолда RAM дан кўрсатмаларни олади. Регистрларда бажарилиши керак бўлган кўрсатмалар манзили сақланади. Регистрлан CPUнинг асосий маълумот сақловчи қисми бўлиб, вақти тежаш учун CPU нинг RAM га мурожаат этишини камайтиради. Арифметик мантиқий бирлашма (Arithmetic logic unit, ALU) RAM дан олинган кўрсатмаларни регистрларга ёки хотирага жойлаштиришда фойдаланилади.

Асосий хотира. Асосий хотира (main memory, RAM) битта дастур доирасида қуйидаги тўрт бўлимга бўлинади:



5.11-расм. Асосий хотира

Маълумот (Data). Асосий хотиранинг бу бўлимида дастур дастлабки юкланишида талаб этилаётган катталиклар сақланади. Бу катталиклар кўп ҳолларда статик катталиклар деб аталиши ёки дастурнинг ихтиёрий қисмидан чақирилувчи глобал катталиклар деб аталиши ҳам мумкин.

Код (Code). Код CPU томонидан дастур вазифасини бажариш учун керакли бўлган кўрсатмаларни ўз ичига олади. Код дастур бажарилишини ва дастур вазифаси ташкил этилишини бошқаради.

Уюм (Heap). Уюм дастур бажарилиши давомида динамик хотира вазифасида, янги қийматни ҳосил қилишда, жойлаштиришда, керак бўлмаган қийматларни ўчириб ташлашда фойдаланилади.

Стек (Stack). Стеклар функциялардаги локал ўзгарувчилар ва параметрлар учун фойдаланилади ва дастур оқимини бошқаришда ёрдам беради.

Юқоридаги расмда келтирилган расмдаги бўлимлар тартиби хусусий бўлиб, хотира бўйлаб турли ҳолларда жойлишиши мумкин.

Кўрсатмалар (Instructions). Кўрсатмалар ассемблер тилининг қурувчи блокларидир. X86 ассемблер тилида, кўрсатмалар *mnemonic* ва *operand* лардан қурилади. Қуйидаги 5.12 – расмда *mnemonic* сўз шаклиди ифодаланган кўрсатмани *mov* орқали, яъни маълумотни кўчиришни тасвирлаган. *Operand*лар маълумотни кўрсатишда регисторлар ёки маълумотлардан фойдаланади.[1]

Mnemonic	Destination operand	Source operand
mov	ecx	0x42

5.12 - расм. Кўрсатмалар формати

Амалий кодлар ва тескари тартиб (Opcodes and Endianness). CPU да кўрсатмаларни юборишда амалий кодлардан фойдаланган ҳолда ассемблер коди машина кодига ўтказилади. Дизассембрлашда амалий кодлар инсон тушинадиган тилга (ассемблер тилига) ўзгартирилади. Қуйидаги 5.13 - расмда *B9 42 00 00 00* амалий кодни ассемблер тилида *mov ecx, 0x42* шаклида ўтказилганлиги кўрсатилган. Бунда *0xB9* коди мос ҳолда *mov ecx* га ва *0x42000000* коди эса *0x42* га айлантирилган.

Instruction	mov ecx,	0x42
Opcodes	B9	42 00 00 00

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 69 – c.

5.13 - расм.

x86 архитектурасида, 0x42000000 кодини ассемблер кодига ўтказишда *тескари тартибдан* фойдаланилади, яъни кетма-кетлик байтлаб тескари томондан ўқилади ва 0x42 қиймати олинади.

Operandлар. Операндлар кўрсатмалар орқали маълумотларни танитишда фойдаланилади. Уч турдаги операндлар бўлиши мумкин:

1. *Бевосита операндлар.* Бу турдаги операндлар қатий белгиланган катталиклар билан ифодаланади, масалан, 0x42.
2. *Регистор операндлар* регистор қиймати билан белгиланади, масалан, *есх.*
3. *Хотира манзиллари операндлари.* Бу турдаги операндлар кўрсатилган хотира адресидаги қиймат орқали ифодаланади. Хусусий ҳолда қийматлар, регистор ва қавс ичида ёзилган кетма-кетликлар орқали ифойдаланади, масалан, [eax].

Регисторлар. Регисторлар CPUдаги кичик ҳажмдаги маълумот сақловчи қурилмалар бўлиб, унда маълумотни ёзиш ва сақлаш жуду тез амалга оширилади. Қуйида x86 архитектурасида мавжуд кенг тарқалган регисторлар турлари келтирилган:

1. *Умумий регисторлар* CPU томонидан бажарилиш давомида фойдаланилади.
2. *Сегмент регисторлар* хотира бўлимларини аниқлашда фойдаланилади.
3. *Ҳолат байроқлари* CPU ни бирор амал бажаришида қарор қабул қилиши учун керак бўлади.
4. *Йўриқнома кўрсаткичлари* кейинги бажарилиши керак бўлган йўриқномани сақлаш учун фойдаланилади.

Қуйидаги жадвалда юқорида келтирилган регистор турлари ва унга мисоллар келтирилаган:

Умумий регисторлар	*Сегмент регисторлар*	*Ҳолат байроқлари*	*Йўриқнома кўрсаткичлари*
EAX EBX ECX EDX EBP ESP ESI	CS SS DS ES FS GS	EFLAGS	EIP

x86 архитектурасида барча регисторлар 32 бит ўлчамга эга.

Ҳолат байроқлари регистор ҳолатларини кўрсатади. Ҳар бир амал бажарилишида ҳар бир байроққа 1 ёки 0 қийматлари ўрнатилади. Қуйидаги

ҳолат байроқлари ЗД таҳлилига жуда зарур бўлади:

ZF. Бу байроқ *zero flag* деб номланиб, амал нолга тенг бўлган ҳолда ўрнатилади. Акс ҳолда тозаланиб ташланади.

CF. Бу байроқ *carry flag* деб номланиб, амал натижасидаги қиймат кейинги қийматга қараганда жуда катта ва жуда кичик бўлган ҳолларда ўрнатилади. Акс ҳолда тозаланиб ташланади.

SF. Бу байроқ *sign flag* деб номланиб, амал натижаси манфий бўлганда ўнатилади. Натижа мусбат бўлганда тозаланиб ташланади.

TF. Бу байроқ *trap flag* деб номланиб, у дебаг қилишда фойдаланилади. x86 процессор ушбу байроқ ўрнатилган ҳолда юкланади.

Содда кўрсатмалар. Жуда кенг фойдаланиладиган кўрсатмалардан бири бу *mov* бўлиб, маълумотни бир жойдан бошқа бир жойга кўчиришни амалга оширади. Бошқа сўз билан айтганда бу кўрсатма хотирадан ўқиш ва ёзиш учун фойдаланилади. Бу кўрсатманинг умумий кўриниши *mov destination, source* тарзида. Қуйидаги жадвалда *mov* билан боғлиқ бўлган кўрсатмаларга мисоллар келтирилган.

Кўрсатмалар	Изоҳ
mov eax, ebx	EBX қийматини EAX регистрга кўчириш.
mov eax, 0x42	EAX регистрга 0x42 қийматини кўчириш.
mov eax, [0x4037C4]	0x4037C4 хотира адресида жойлашган 4 байт маълумотни EAX регистрига кўчириш.
mov eax, [ebx]	EBX регистри хотира жойлашувидан 4 байт маълумотни EAX регистрига кўчириш.
mov eax, [ebx+esi*4]	ebx+esi*4 тенглик натижасида жойлашган хотира манзилида жойлашган 4 байт маълумотни EAX регистрга кўчириш.

Mov амалига ўхшаш бўлган амал *lea (load effective address)* бўлиб, умумий кўриниши *lea destination, source* шаклда бўлади. Бу кўрсаткич хотира манзилини масофадаги манзилга қўйишда фойдаланилади. Масалан, *lea eax, [ebx+8]* . *ebx+8* қиймати жойлашган манзилни *eax* регистрига сақлайди.

Арифметик амаллар. x86 ассемблаш тили кўплаб содда арифметик амалларни қўллаб қуватлайди. [1]

Кўрсатмалар	Изоҳ
sub eax, 0x10	EAX регистр қийматидан 0x10 ни олиб ташлаш.
add eax, ebx	EBX қийматига EAX қийматини қўшиш ва EAX га ўзлаштириш.
inc edx	EDX регистр қийматини 1 га ошириш.
dec ecx	ECX регистр қийматини 1 га камайтириш.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 74 – c.

mul 0x50	EAX регистор қиймати 0x50 га кўпайтирилади. 64 битли натижа EDX:EAX регисторларига сақланади. 32 битли катта қисми EDX га ва кичик 32 битли қисм EAX га сақланади.
div 0x75	EDX:EAX 64 битли регистор қийматлари 0x75 га бўлинади ва натижа EAX га ва қолдиқ EDX га сақланади.
xor eax, eax	EAX регистор қийматини тозалаш
or eax, 0x7575	EAX регистори қийматига 0x7575 ни мантиқий қўшиш амалида қўшиш
shl eax, 2	EAX регистор қийматини 2 бит чапга силжитиш.
shr eax, 2	EAX регистор қийматини 2 бит ўнга силжитиш.
ror bl, 2	Bl регистор қийматини ўнга циклик 2 бит айлантириш.
rol bl, 2	Bl регистор қийматини чапга циклик 2 бит айлантириш.
nop	Ҳеч қандай амални бажармайди. Кейинги кўрсатмага ўтилади.

Стек. Асосий хотиранинг қисми, стекда функцияга тегишли бўлган ўзгарувчилар ва параметрлар сақланади. Стекда амалга ошириладиган кўрсатмалар, *push, pop, call, leave, enter ва ret* бўлиши мумкин.

Push кўрсаткичи стекдаги регисторни жойлашувини қуйи хотира қисмига, яъни тезроқ бажариш учун ўзгартиради.

Pop кўрсаткичи стекдаги регисторни жойлашувини юқори хотира қисмига, яъни кейинроқ бажариш учун ўзгартиради.

Call кўрсаткичи кейинги стекни чақириш учун фойдаланилади.

Leave кўрсаткичи ESP қийматини EBP га ўрнатади ва кейин EBP ни юқори хотира қисмига ўтказади, яъни, *mov(ebp, esp); pop(ebp);*

Enter кўрсаткичи қуйидаги кўрсаткичлар кетма-кетлигига тенг: *push ebp; mov ebp, esp.*

Шартлар. Барча тилларда бўлгани каби ассемблаш тилида ҳам шартлар мавжуд бўлиб, асосан иккита *test* ва *cmp* кўрсаткичидан кенг фойдаланилади. *Test* кўрсаткичи *and* кўрсаткичига ўхшаш бўлиб, бундан ташқари операндлар кўрсаткич томонидан ўзгартирилмайди. *Test* кўрсаткичи фақат байроқни ўрнатиш учун фойдаланилади. Одатда *test* кўрсаткичидан сўнг ZF байроғи ўрнатилади. *Test* кўрсаткичи бир операнд доирасида операнд қийматини *NULL* тенглигини текширишда фойдаланилади. Масалан, *test eax,eax* кўрсаткичи *eax AND eax* кўрсаткичига тенг бўлиб, натижага кўра ZF байроқ ўрнатилади.

Cmp кўрсаткичи иккинчи кенг фойдаланиладиган шартли белги бўлиб, вазифаси жихатидан *sub* кўрсаткичига тенгдир. Бу кўрсаткич ҳам операндга таъсир қилмай фақт байроқ ҳолатини ўзгартириш учун ишлатилади. Бу шарт натижасида ZF ва CF байроқлар ўрнатилиши мумкин. Қуйидаги жадвалда *cmp* кўрсаткичи билан боғлиқ бўлган мисоллар берилган:

cmp dst, src	ZF	CF
dst = src	1	0
dst < src	0	1
dst > src	0	0

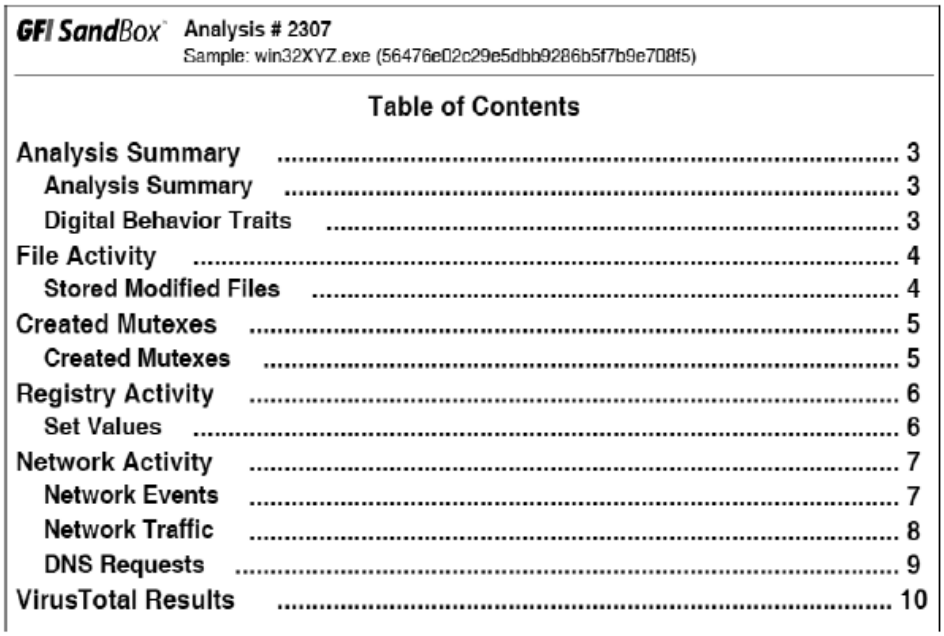
Сакрашлар. Келтирилган шартлар бажарилгандан сўнг бирор амални бажаришга тўғри келади. Бажарилиши керак бўлган юклашда *сакраш (jump)* амалга оширилади. Сакрашлар ассемблер тилида *jmp* кўрсаткичи орқали амалга оширилади. Бу кўрсаткичнинг умумий кўриниши қуйидагича: *jmp location.* Бу шартсиз ўтиш амали саналади. Ассемблаш тилида *if* шарти ўтиш оператори мавжуд эмас. Шартли ўтишларни амалга оширишда ҳолат байроқларидан фойдаланилади. Бу ҳолда ҳолат байроғига қараб кейинги босқичга ўтиш ёки сакраш амалги оширилиши бажарилади. Ассемблер тилида 30 дан ортиқ шартли ўтиш ҳолатларидан фойдаланилади. Қуйидаги жадвалда буларга мисоллар келтирилган.

Кўрсаткичлар	Изоҳ
jz loc	ZF = 1 бўлганда белгиланган соҳага сакраш
jnz loc	ZF = 0 бўлганда белгиланган соҳага сакраш
je loc	Jz билан бир хил фақат кўп ҳолларда cmp кўрсаткичидан кейин ишлатилади. Масофадаги операнд жорий операндга тенг бўлса сакраш ҳосил бўлади.
jne loc	Jz билан бир хил фақат кўп ҳолларда cmp кўрсаткичидан кейин ишлатилади. Масофадаги операнд жорий операндга тенг бўлмаган ҳолда сакраш ҳосил бўлади.
jg loc	Масофадаги операнд жорий операндан катта бўлган ҳолда *cmp* кўрсаткичидан кейин фойдаланилади.
jge loc	Масофадаги операнд жорий операндан катта ёки тенг бўлган ҳолда *cmp* кўрсаткичидан кейин фойдаланилади.
ja loc	Jg билан бир хил фақат unsigned таққослашларда фойдаланилади.
jae loc	Jge билан бир хил фақат unsigned таққослашларда фойдаланилади.
jl loc	Масофадаги операнд жорий операндан кичик бўлган ҳолда *cmp* кўрсаткичидан кейин фойдаланилади.
jle loc	Масофадаги операнд жорий операндан кичик ёки тенг бўлган ҳолда *cmp* кўрсаткичидан кейин фойдаланилади.
jb loc	Jl билан бир хил фақат unsigned таққослашларда фойдаланилади.
jbe loc	Jle билан бир хил фақат unsigned таққослашларда фойдаланилади.
jo loc	OF = 1 бўлса олдинги кўрсатмага ўтилади.
js loc	SF = 1 бўлса амалга оширилади.
jecxz loc	ECX = 0 бўлса белгиланган соҳага сакрайди.

Динамик таҳлиллаш. Зараркунанда дастурий воситаларнининг *содда динамик таҳлили* одатда содда статик таҳлил иш бермаган ҳолда фойдаланилиб, таҳлил зараркунанда дастурий восита бевосита юклангандан сўнг амалга оширилади. Бу усул орқали ЗДларнинг вазифалари тўлиқ аниқланади. Қуйида содда динамик таҳлиллаш технологиялари билан танишиб чиқилади.

Sandboxes. Ушбу дастурий воситалар содда динамик таҳлиллаш кенг фойдаланилиб, у ҳост ОТ билан ҳимояланган соҳани ҳосил қилади ва ЗД ушбу соҳада юклайди. Бу турдаги воситаларга Norman SandBox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, ва Comodo Instant Malware Analysis **(**open source**)** ларни олиш мумкин. Амалда Norman SandBox ва GFI Sandboxлардан кенг фойдаланилади.[1]

Изоҳ. Амалда кенг фойдаланилаётган sandboxes дастурлар пуллик саналади. Умумий ҳолда барча sandboxes дастурий воситалари бир хил ишлаш алгоритмига эга. Яъни, ЗД ҳимояланган соҳада юкланади ва ОТ белгиланган соҳаларидаги ўзгаришларга асосан таҳлил натижалари шакллантирилади. Қуйида GFI Sandboxда олинган PDF туридаги таҳлил натижаси келтирилган.



GFI SandBox Analysis # 2307
Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

5.14-расм. GFI Sandboxнинг win32XYZ.exe ЗД учун содда таҳлил натижаси

5.14-расмда кўрсатилганидек, GFI Sandboxнинг таҳлилари олтита бўлимга кўра олинган:

1. *Analysis Summary бўлими.* Бу бўлида ЗД статик таҳлил натижаси ва

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 40 – с.

динамик таҳлил натижаларининг юқори даражали маълумотлари келтирилади;

2. *File Activity бўлими.* Бу бўлимда ЗД томонидан ўчирилган, очилган, яратилган ва фойдаланилган барча файллар рўйхати келтирилади;

3. *Created Mutexes бўлими*. Бу бўлимда ЗД томонидан яратилган ресурслар рўйхати келтирилади;

4. *Registry Activity бўлими.* Бу бўлимда регистрда мавжуд бўлган ўзгаришлар келтирилади;

5. *Network Activity бўлими.* Бу бўлимда ЗД томонидан тармоқдан фойдаланиш даражаси ва ҳолати келтирилади;

6. *VirusTotal Results бўлими.* Бу бўлимда ЗД VirusTotal орқали сканерлаш натижаси келтирилади.

Sandbox камчиликлари. Кўплаб Sandbox дастурий воситалари бин нечта катта камчиликларга эга. Масалан, Sandboxларда ЗД фақат юклаш орқали таҳлилланади (буйруқлар сатрида буни амалга ошириш имокнияти мавжуд эмас). Агар ЗД буйруқлар сатридан юкланишни сўраса бу ҳолда Sandbox дастурлар бу ЗД юклай олмайди.

Бундан ташқари қуйидаги камчиликлар кузатилади:

– ЗД тез-тез вертуал машина юкланганини аниқлайди ва бу ҳолда ЗД юкланишдан ўзини тўхтатиши ёки ўзини бошқача тутиши мумкин. Бу барча Sandboxлар учун мос эмас;

– баъзи ЗД юкланишда ОТ махсус файл ва регистор маълумотларини талаб этади. Бу маълумотлар ўз навбатида Sandboxда мавжуд бўлмайди;

– агар ЗДлар *dll* файл кенгайтмасида бўлса, улар юкланувчи ЗДлар (.exe кенгайтмали) дек тўлиқ Sandboxга юкланмайди;

– Sandbox муҳити ЗД учун мос бўлмаслиги мумкин. Масалан, Windows XP га мос бўлган ЗД, Windows 7 учун мос бўлмаслиги мумкин;

– Sandboxлар ЗД ларни вазифасини аниқласада, аслида нима қилаётганинини айтмайди.

ЗД юклаш (running malware). Содда динамик таҳлиллаш технологиялари ЗД юкланмаган ҳолда уларни таҳлиллай олишмайди. ЗДларнинг аксарияти *.exe* ва *.dll* файл кенгайтмаларида бўлишларини ҳисобга олиб, қуйида бу икки турдаги файлларни юклаш усулларини қараб чиқилади. *.exe* кенгайтмали файл юкланишга осон бўлиб, одатда сичқонча тугмачасини икки марта босиш орқали ёки буйруқлар сатридан фойдаланган ҳолда юкланади.

.dll кенгайтмали файллар нисбатан хийлакор бўлиб, windows ОТ буни қандақҳй қилиб автоматик юклашни билмайди.

Барча турдаги замонавий Windows ОТлари *rundll32.exe* файлига эга бўлиб, бу файл ўзида *DLL* ларни юклаш имкониятини сақлайди. Ушбу файл орқали ЗД юклаш тартиби қуйидагича:

C:\>rundll32.exe DLLname, Export arguments

Бу ерда *Export* қиймати олинган *DLL* файл ичидан експорт қилиниши керак бўлган функция номи. Статик таҳлиллаш усулида фойдаланилган дастурий воситалар PEview ёки PE Explorer орқали *DLL* файл ичидаги функция номи аниқланади. Масалан, *rip.dll* деб номланувчи файл ўзида *Install* ва *Uninstall* деб номланувчи функцияларни олади. Бу ҳолда юқоридаги тартиб қуйидагича бўлиши мумкин:

C:\>rundll32.exe rip.dll, Install

Баъзи ҳолларда DLL шаклидаги ЗДлар хизмат каби ўрнатилишни талаб этади.

C:\>rundll32 ipr32x.dll,InstallService ServiceName

C:\>net start ServiceName

Бу ердаги *ServiceName* DLL файл таркибидан олинади. net start буйруғи эса хизматни Windows ОТ амалга ошириш учун керак бўлади.

Мураккаб динамик таҳлиллар. Debugger бирор дастурни тестлаш ёки юклаш учун фойдаланилган қурилма ёки дастурий таъминот. Debugger ёзилган дастурий кодда хатолик мавжуд бўлганда ва хатоликни айнан қайерда эканлигини аниқлаш учун фойдаланилади. Debugger дастурий кодни юклагандан сўнг, уни қадамба-қадам таҳлилаш имконини беради. [1]

Код сатҳи ва ассемблер сатҳида Debuggerлаш. Кўплаб дастурчилар дастурий воситаларини код сатҳида debugging қилиш орқали таҳлил этадилар. Бунда дастур қайси кодда ёзилган бўлса, debugging ҳам шу дастурлаш тили коди доирасида амалга оширилади.

Ассемблер сатҳида debuggerлаш қуйи сатҳда debuggerлаш деб ҳам аталиб, код сатҳидаги каби кетма-кетликларни амалга ошириш имкониятига эга бўлинади. Бунда компиляция қилинган файлларни debuggerлаш амалга оширилади.

Ўзак сатҳи ва фойдаланувчи сатҳи debuggerлари. Фойдаланувчи сатҳида debuggerлаш код сатҳида debuggerлаш каби амалга оширилади. Бу сатҳда debuggerланганда дастур ОТ ажратилган ҳолда амалга оширилади (маълум чекланишлар билан).

Ўзак сатҳида debuggerланганда дастур ҳеч қандай чекланишсиз юкланади. Бунда дастурда breakpoint қўйилса, бошқа ҳеч қандан дастур юкланмайди. Шунинг учун ўзак сатҳида debuggerлаш бирмунча мураккаб.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 168 – c.

Debuggerлаш учун кўплаб дастурий воситалар фойдаланилиб, улар фойдаланувчи ёки ўзак сатҳида юклашни қўллаб-қувватлайди. WinDbg дастурий ҳар иккала сатҳни қўллаб қувватласа, OllyDbg эса фақат фойдаланувчи сатҳини қўллаб-қувватлайди. IDA Pro дастури ҳам бу debuggerлаш имкониятини қўллаб қувватласада, имкониятлари юқоридаги икки дастурдаги каби эмас.

Бир қадамли debuggerлаш. Бу усулда debug қилинганда ҳар бир қатор учун тўхталиб ўтилади. Бу усулда таҳлиллаш яхши натижа берсада, жуда кўп вақт олади.

Батафсил ва сакраб ўтишли debuggerлаш. Бу усулда кўра фойдаланувчи талабига кўра функция ичидаги қаторлар таҳлилланади ёки функциядан кейинги жойлашган қаторга ўтилади.

Назорат саволлари

1. Дастурий маҳсулотлар хавфсизлиги.
2. Дастурий маҳсулотларда заифликларни келиб чиқиши.
3. Дастурий маҳсулотларда мавжуд таҳдидлар.
4. Хотиранинг тўлиб тошиш таҳдиди.
5. SQL инекция.
6. Зараркунанда дастурий воситаларнинг таҳлиллаш усуллари.
7. Статик таҳлиллаш.
8. Динамик таҳлиллаш.

Фойдаланилаган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Michael Sikorski, Andrew Honig. Practical malware analysis. 2012.

IV. БЎЛИМ

АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

IV. АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

1 – амалий машғулот. Ахборот хавфсизлигининг анъанавий тимсоллари. Ахборот хавфсизлиги сиёсати. Ҳимоя тизимини лойиҳалаш ва амалга ошириш босқичлари.

Ишнинг мақсади: Ахборотнинг ҳуқуқий ва муҳандис-техник ҳимоясини таъминлаш воситалари.

Масаланинг қўйилиши: берилган ташкилот учун инжинер-техник ҳимоя ишлаб чиқилсин.

Ишни бажариш учун намуна

Ахборотни техник чиқиб кетиш каналлари. Маълумот майдон ёки модда орқали узатилади. Бу акустик тўлқин (товуш), ёки электромагнит нурланиш, ёки матн ёзилган бир варақ қоғоздир. Бироқ, на узатилган енергия, на фойдаланилган модда ўз-ўзича ҳеч қандай қийматга эга емас, улар фақат маълумот ташувчи ҳисобланади холос. Физик табиатига кўра қуйидагилар маълумот ташувчи воситалар ҳисобланади: ёруғлик нури; товуш тўлқинлари; електромагнит тўлқинлар; материал ва моддалар. Табиатда маълумотларни ташиш учун булардан бошқалари мавжуд емас. Ўз манфаатларига қараб инсонлар у ёки бу физик майдондан фойдаланиб ўзаро маълумот узатишнинг бирор тизимини яратадилар. Бундай тизимларни алоқа тизими деб номлаш қабул қилинган. Ихтиёрий алоқа тизими (маълумот узатиш тизими) маълумотлар манбаи, узатгич, маълумот узатиш канали, қабул қилгич ва қабул қилиб олувчи ҳақидаги маълумотдан ташкил топади. Бу тизимлар кундалик ҳаётда бирор мақсад учун фойдаланилади ва маълумот узатишнинг расмий воситаси ҳисобланади. Унинг фаолияти ишончлиликни, аниқлиликни ва маълумот узатиш хавфсизлигини таъминлаш мақсадида назорат қилинади. Бу еса рақобатчиларнинг тизимга рухсациз киришни олдини олади. Бироқ, маълум шароитлар мавжудки, унда бир жойдан бошқасига маълумот узатиш тизими обект ва манбанинг хоҳишига боғлиқ бўлмайди. Бундай ҳолларда, албатта, бундай канал ўзини очиқча намоён қилмаслиги керак. Маълумотлар узатиш канали сингари бундай канал маълумот чиқиб кетиш канали деб аталади. У ҳам сигнал манбаи, уни тарқатувчи физик муҳит ва ёвуз ниятли шахслар (бузғунчилар) томонидаги қабул қилувчи қурилмалардан ташкил топади. Қуйидаги 1.1-расмда маълумот чиқиб кетиш каналининг тузилиши келтирилган.

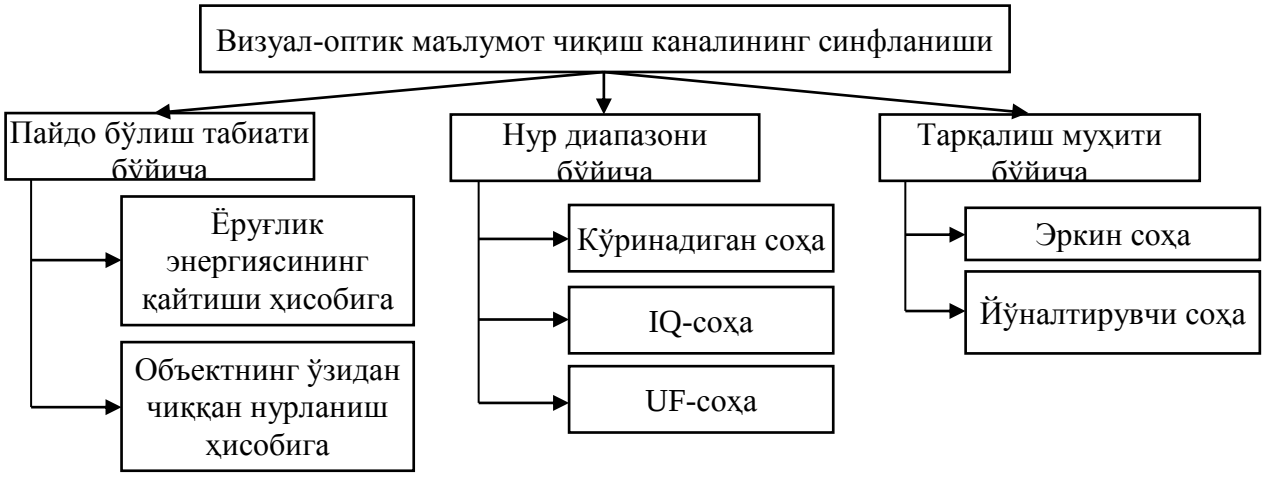
1.1-расм. Маълумотнинг чиқиб кетиш каналлари

Маълумотлар чиқиб кетиш канали деб конфиденсиал маълумотлар манбасидан ёвуз ниятли шахсгача бўлган физик йўл тушунилади. Бу йўл орқали маълумот чиқиб кетиши ёки сақланаётган маълумотга рухсациз кириш мумкин. Маълумотлар чиқиб кетиш каналининг вужудга келиши (пайдо бўлиши, ўрнатиш) учун маълум фазовий, енергетик ва вақтдаги шароит ҳамда ёвуз ниятли шахсда уларга мос маълумотларни қабул қилиш ва қайд қилиш воситалари мавжуд бўлиши керак. Физик хусусиятларини инобатга олган ҳолда маълумотлар чиқиб кетиш каналининг пайдо бўлишини қуйидаги гуруҳларга ажратиш мумкин:

– визуал-оптик;
– акустик;
– електромагнит (магнит ва електрик майдонни ўз ичига олади);
– материал-буюмли (қоғоз, фото, магнитли ташувчилар, турли кўринишдаги қаттиқ, суюқ, газ ҳолатидаги саноат чиқиндилари).

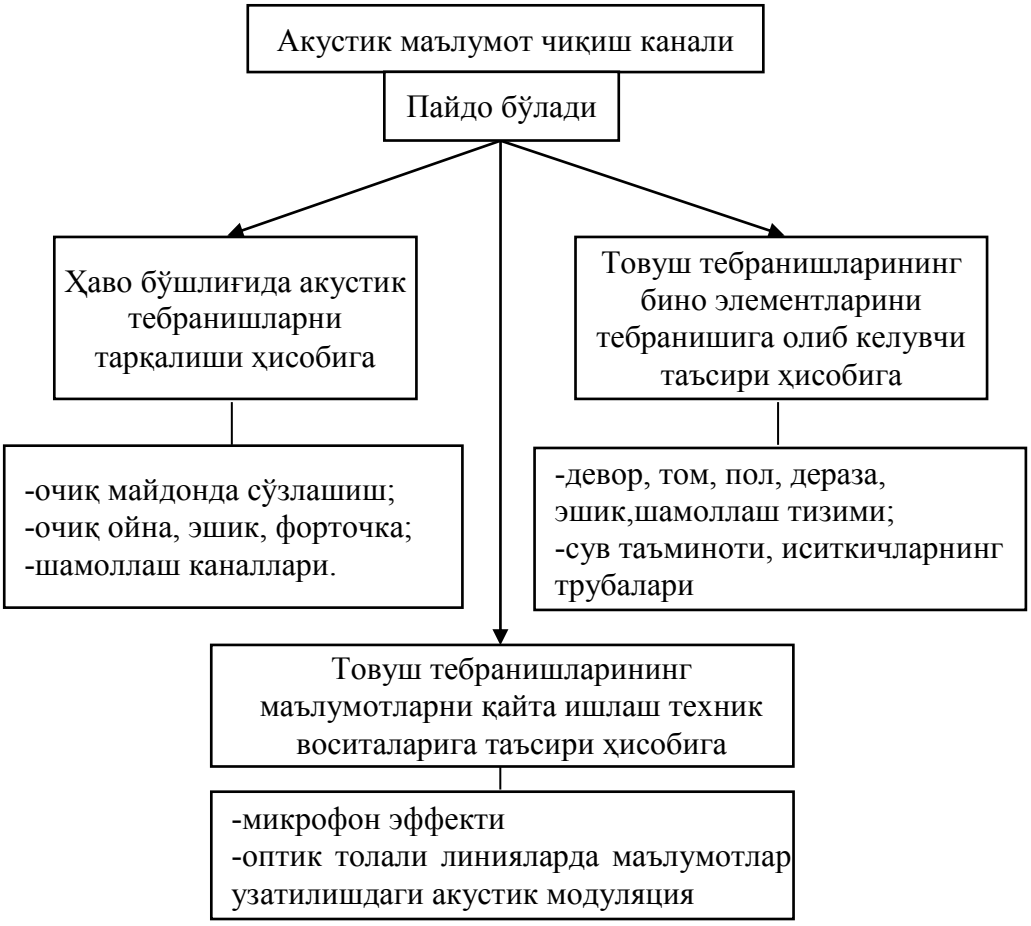
Визуал-оптик каналлар – бу бевосита ёки узоқдан (жумладан телевизион) кузатишдир.

Маълумот ташувчи бўлиб, конфиденциал маълумот манбаси чиқарадиган ёки ундан қайтувчи кўринадиган, инфрақизил ва ултрабинафша диапазондаги ёруғлик хизмат қилади.



1.2-расм. Визуал-оптик маълумот чиқиш каналининг синфланиши

Акустик каналлар. Инсон учун маълумотларни ешитиш қобилияти кўришдан кейин иккинчи ўринда туради. Шу сабабли маълумот чиқиб кетиши каналининг енг кўп тарқалгани акустик канал ҳисобланади. Акустик каналда маълумот ташувчиларга ултра (20000 Гц дан юқори), ешитиш ва инфратовуш диапазондаги тўлқинлар киради. Инсон ешитадиган товуш частотаси 16 дан 20000 Гц гача ва инсон гапиргандаги 100 дан 6000 Гц гача бўлади.



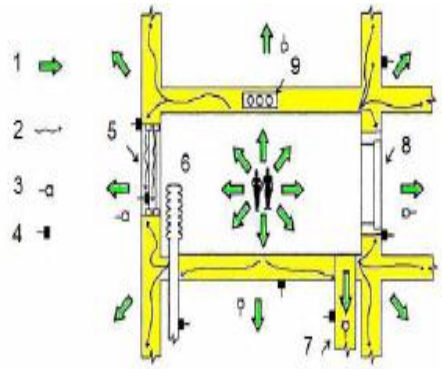
1.3-расм. Акустик маълумот чиқиш канали

Ҳавода акустик тўлқин тарқалганда ҳаво зарралари тебранади ва бунинг натижасида биридан-бирига енергия узатилади. Агар товуш йўлида тўсиқ бўлмаса, у ҳамма томонга бирдай тарқалади.

Агар товуш тўлқинлари йўлида девор, ойна, ешик, том ва каби бошқа тўсиқлар бўлса, товуш тўлқини уларга маълум даражада босим беради ҳамда уларни ҳам тебрантиради. Товуш тўлқинларининг бундай таъсири акустик маълумот чиқиб кетиши каналининг пайдо бўлишига асосий сабаб бўлади. Муҳитга қараб товуш тўлқинларининг тарқалиши фарқ қилади. Бу товушнинг ҳаво бўшлиғида тўғри тарқалиши, қаттиқ муҳитда (таркибий товуш) тарқалишидир. Бундан ташқари, товушнинг бино ва иморатларга

босим билан таъсири қилиши уларнинг тебранишига сабаб бўлади.

Қуйидаги расмда акустик ва вибрацион тебранишлар орқали маълумотлар чиқиб кетиш каналларининг чизмаси келтирилган бўлиб, унда акустик тебраниш ва товушларнинг қаттиқ муҳитда, метал буюмларда ва бинонинг бошқа елементларида тарқалиши тасвирланган.

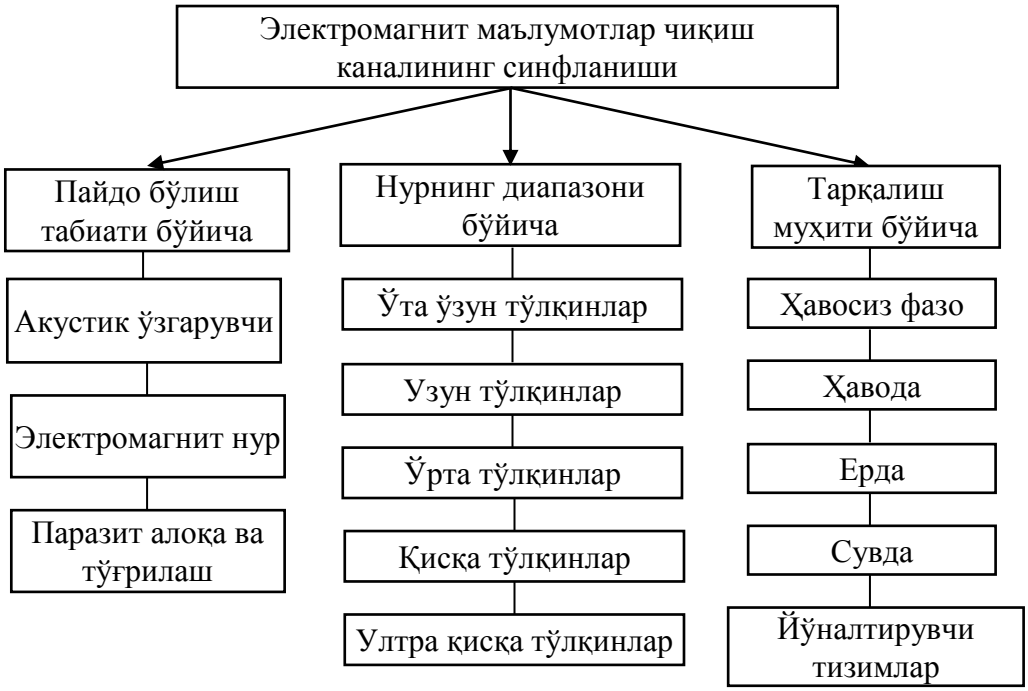


1. Акустик тебранишларнинг тарқалиши
2. Вибрацион тебранишларнинг тарқалиши
3. Эшитиш микрофони
4. Эшитиш вибродатчиги
5. Дераза
6. Иситгич батареялари
7. Ҳаво тозалагич
8. Эшик
9. Кабеллар учун жой

1.4-расм. Акустик ва вибрацион тебранишлар орқали маълумотлар чиқиши

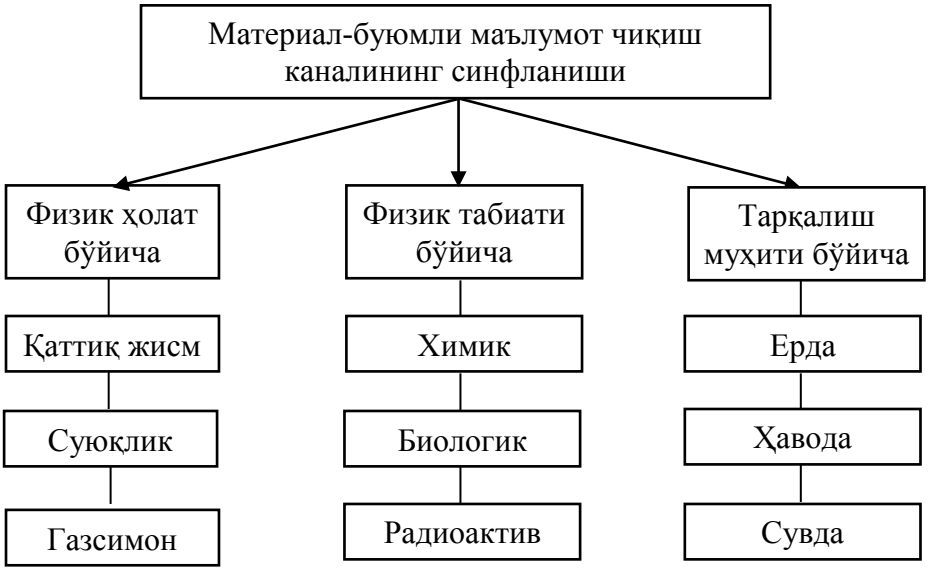
Электромагнит каналлар. Бундай ҳолларда маълумот ташувчи, ўта узун тўлқин узунлигидан (10000 м – частотаси 30 Гц дан кичик) суб миллиметрлигача (1-0,1 мм – частотаси 300дан 3000 ГГц гача) бўлган диапазондаги електромагнит тўлқинлар ҳисобланади. Бу кўринишдаги ҳар бир електромагнит тўлқин тарқалишнинг фазо ва узоқлиги бўйича ўзига хос хусусиятига эга.

Масалан, узун тўлқинлар жуда узоқ масофаларга, миллиметрлилар еса аксинча, фақат тўғри йўналишда бир ва бир неча ўн километрга тарқалади. Бундан ташқари, турли телефон ва алоқа симлари ҳамда кабеллари ўз атрофида магнит ва електр майдонини ҳосил қилади. Яқин масофада булар ҳам маълумотларнинг чиқиб кетиши елементларига киради.



1.5-расм. Электромагнит маълумотлар чиқиши каналининг синфланиши

Материал-буюмли маълумот чиқиб кетиши каналига қаттиқ, суюқ ва газсимон ёки корпускуляр (радиоактив елементлар) кўринишдаги моддалар киради. Булар, жуда кўп ҳолларда, саноатнинг турли чиқиндилари, сифациз моллар, хомаки материаллар ва бошқалар бўлиши мумкин. Шундай екан ҳар бир конфиденциал маълумот манбаи у ёки бу даражадаги маълумот чиқиб кетиши каналига эга бўлиши мумкин.

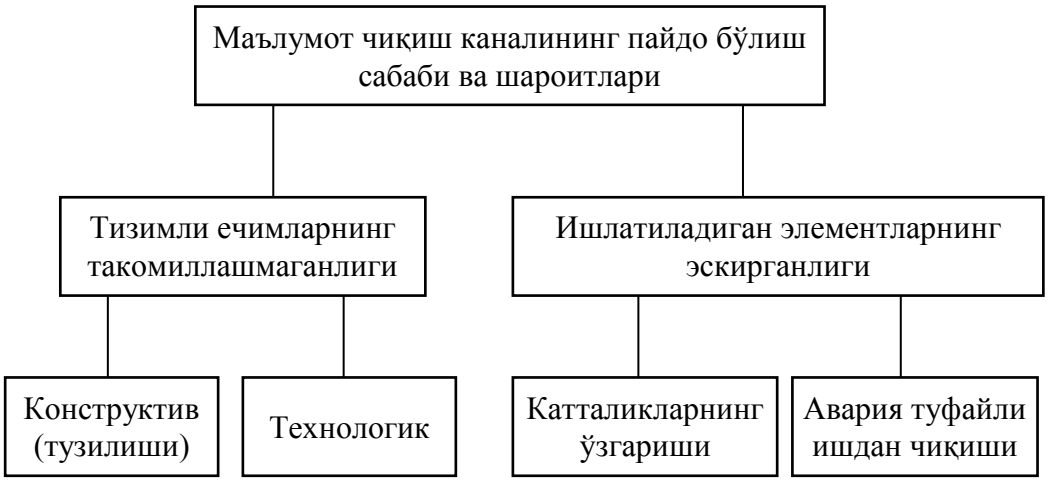


1.6-расм. Материал-буюмли маълумот чиқиш каналлари

Ишлаб чиқаришда, илмий фаолиятларда ва ахборотни автоматик қайта ишлашда турли техник таъминот воситаларидан кенг фойдаланиш деб ном олган маълумотлар чиқиб кетиши техник каналлари гуруҳининг пайдо бўлишига олиб келди. Уларда маълумотларни ташувчи бўлиб, турли хил тоифадаги ёндош електромагнит нурланишлар ва наводкалар (ЁЕМНН): акустик-ўзгартириладиган, нурланувчан ҳамда зарарли алоқа ва наводкалар ҳисобланади. ЁЕМНН ихтиёрий електрон қурилмага, тизимларга, табиий хусусиятларга эга бўлган маҳсулотларга ҳосдир. Хавфли нурланишга асос бўлувчи физик ҳодисалар турли хил тавсифларга эга. Шунинг билан бирга, бундай нурланиш ҳисобига бўладиган умумий кўринишидаги маълумотлар чиқиб кетишини, ҳимояланадиган маълумотларнинг бирор «қўшимча» алоқа тизими орқали узатилиши деб қараш мумкин. Шуни таъкидлаш жоизки, техник восита ва тизимлар нафақат қайта ишланадиган ахборотлардан иборат бўлган сигналларни фазога тарқатади, балки ўзининг микрофон ёки

антеннаси ёрдамида акустик ёки магнит (электромагнит) нурланишларни қабул ҳам қилади, уларни електр сигналига айлантиради ва ўз алоқа линияси орқали, одатда назорациз, жўнатади. Бу еса маълумот чиқиб кетиши хавфини янада орттиради.

Алоҳида техник воситалар ўз таркибида «микрофон» ва «антенна» каби қурилмалардан ташқари юқори частотали ёки импулсли генераторларга ҳам эга бўлади. Уларнинг нурланиши конфиденциал маълумотларга эга бўлган турли сигналларга мослаштирилган бўлиши мумкин. Хавфли «микрофон эффекти» (зарарли електр сигналларининг пайдо бўлиши) айрим телефон қурилмаларида, ҳатто телефон трубкаси қўйилган ҳолда бўлишига қарамасдан ҳам пайдо бўлади. Электромагнит нурланишлар товуш чиқарувчи ва товуш кучайтирувчи қурилмаларнинг радиочастоталарида ўз-ўзидан пайдо бўлишида ҳам ҳосил бўлиши мумкин.



1.7-расм. Маълумот чиқиш каналининг пайдо бўлиш сабаби

ЁЕМНН нинг пайдо бўлиш манбасининг шароити ва сабабининг таҳлили шуни кўрсатадики, унинг пайдо бўлишига маълум тоифадаги техник воситаларнинг ишлаш схемасини такомиллашмаганлигини, елементларнинг ишлатилиши натижасида ескирганлигини ва шу кабилар асос бўлади.

Инжинер-техник ҳимоя усуллари. Техник канал бўйича маълумотлар чиқиб кетишидан ҳимоялашда, одатда қуйидаги амалларнинг бажарилиши талаб этилади:

1. Мумкин бўлган маълумотлар чиқиб кетиши каналларини ўз вақтида аниқлаш.

2. Назорат зонаси (ҳудуди, кабинети) чэгарасида маълумот чиқиб кетиши каналининг енергетик тавсифларини аниқлаш.

3. Ёвуз ниятли шахслар томонидан канални назорат қилиш воситаларининг имкониятларини баҳолаш.

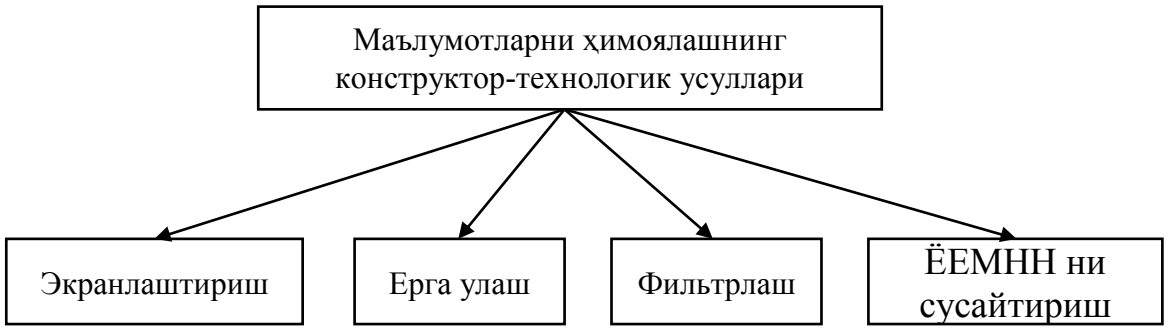
4. Ташкилий, ташкилий-техник ёки техник чора ва воситалар ёрдамида маълумот чиқиб кетиши каналларининг енергетикасини йўқ қилиш ёки заифлаштириш.

Техник тадбирларни конфиденциал сўзлашувларни махсус ҳимояланган воситалардан фойдаланиш ҳисобига ўтказиш мумкин.

Товушни ўтказмайдиган қилиш билан ҳимоялашнинг самарадорлигини аниқлаш учун шовқин ўлчагичлар ишлатилади. Шовқин ўлчагич – товуш босими тебранишларини товуш босими даражасига мос кўрсаткичларга айлантирувчи ўлчов асбобидир. Одам товушини акустик ҳимоя қилиш соҳасида аналогли шовқин ўлчагичлардан фойдаланилади. Аниқлик даражаси бўйича шовқин ўлчагичлар тўрт синфга ажратилади. Нолинчи синфдаги шовқин ўлчагичлар лабораториядаги ўлчашларда, биринчиси – табиий шароитдаги ўлчашларда, иккинчиси – умумий мақсадлардаги ўлчашларда, учинчиси – йўналтирилган ўлчашларда ишлатилади. Амалиётда акустик каналнинг ҳимояланганлик даражасини баҳолаш учун шовқин ўлчагичларнинг иккинчи синфи, кам ҳолларда биринчи синфидан фойдаланилади.

Электромагнит каналлардан маълумотлар чиқиб кетишини ҳимоялаш учун умумий ҳимоялаш усуллари ва айнан шу турдаги каналга мўлжалланган махсус ҳимоялаш усуллари қўлланилади. Бундан ташқари, ҳимоя чораларини конструктор-технологик ечимлар ва експлуатацион (фойдаланиш) синфларига ажратиш мумкин. Конструктор-технологик ечимларда маълумотларнинг чиқиб кетиши ехтимоли мавжуд бўлган каналларнинг пайдо бўлиши бартараф етилади. Эксплуатацион ҳимояда ишлаб чиқариш ва меҳнат фаолияти шароитида турли хил техник воситаларни қўллаш орқали чиқиб кетиш каналлари тўсилади.

Қурилма ва унинг елементларини ерга улаш ҳамда сиртларини металл пуркаб қоплаш йўналтирилган сигналларни ерга ўтказиб юбориш, алоҳида занжирлар орасидаги зарарли алоқаларни сусайтиришнинг ишончли воситасидир. Турли мақсадларга мўлжалланган филтрлар пайдо бўлган ёки тарқаладиган сигналларни камайтириш ёки сусайтиришга ҳамда ахборотларни қайта ишлаш қурилмаларининг манба тизимини ҳимоя қилиш учун хизмат қилади.



1.8-расм. Маълумотларни ҳимоялашнинг конструктор-технологик усуллари

Физик воситалар маълумотлар ва ҳисоблаш тизими елементлари ҳимоясининг биринчи чизиғи ҳисобланади. Шунинг учун ҳам бундай тизим ва қурилмаларнинг физик бутлигини таъминлаш маълумотлар ҳимоясининг зарурий шарти ҳисобланади. Ривожланган хорижий давлатларда ҳимоянинг физик воситалари қўлла нишига ва такомиллашувига катта еътибор қаратилмоқда.

Физик ҳимоя воситаларининг асосий вазифалари:

1. Ҳудудни қўриқлаш.
2. Асбоб-ускуналар ва маълумот ташувчиларни қўриқлаш.
3. Ички хоналарни қўриқлаш ва уларни кузатиш.
4. Назорат зоналарига назоратли ўтишни жорий қилиш.
5. Наводка ва нурланишларнинг таъсирини йўқотиш.
6. Визуал кузатувларга тўсқинлик қилиш.
7. Ёнғинга қарши ҳимоя.
8. Бузғунчи шахсларнинг ҳаракатини блокировка қилиш.

Ташкилотлардаги маълумотларни електрон қайта ишлаш марказлари кучли електромагнит нур манбаи бўлган объектлардан узоқда жойлашган бўлиши ва атрофи девор билан ўралиши керак. Назорат зонасини кузатиш телевизион, радиолокацион, лазерли, оптик, акустик ва бошқа умумий пултга уланган тизим орқали амалга оширилиши мумкин.

Обектлар хавфсизлигини таъминлаш тизимларининг умумий тузилиши қуйидаги расмда келтирилган. Аниқ ҳолатлар учун схеманинг айрим елементлари бўлмаслиги ёки айрим елементлар қўшилиши мумкин.

Одатда, обектнинг хавфсизлигини таъминлаш қуйидаги тамойилларга асосланади: обектга бўлган хавф-хатарни аниқлаш ва баҳолаш; адекват (мос) ҳимоя чораларини ишлаб чиқиш ва уларни қўллаш.

Обектни периметри бўйича қўриқлашни ташкил етишда унинг ички ҳудуди (қўриқланадиган майдон) шартли равишда: аниқлаш, кузатиш, тўхтатиб қолиш, нишонга олиш каби бир неча функсионал зоналарга бўлиб, ҳар бир зонада ўзига хос техник воситалар жойлашиши керак.

Юқори частотали електромагнит нурланишнинг асосий манбаи монитор ҳисобланади. Компютер мониторидан чиқаётган тасвирни бир неча юз метрдан қабул қилиш мумкин. Маълумотларни тўлиқ чиқиб кетишини олдини олиш учун шовқин генераторларидан фойдаланиш лозим. Маълумотларни чиқиб кетишдан ҳимояланишнинг бошқа усулларидан бири

плазмали ёки суюқ кристалли мониторлардан фойдаланиш ҳисобланади.

Бинони тўлиқ екранлашнинг яна бир ишончли усулларидан бири хоналарни алюмин, темир ёки махсус пластмасса листлар орқали (қалинлиги 1 мм дан кичкина бўлмаган) қоплаш ва ерга улаб қўйиш ҳисобланади. Ойналарга бундай ҳолатларда ячайкали филтрлар-алюминий сим тўрлар (катаклар катталиги 1 см дан ката бўлмаган) қўйилиши тавсия етилади.

Принтер паст частотали електромагнит нурланишнинг манбаи яъни масофақа узоқлигига қараб нурлари тез сўнади. Шунчалик кичик булса ҳам бу нурланиш анча хавфли ҳисобланади. Бу билан курашиш анча қийин, яъни уни ташкил етувчи жуда кучлимагнит тўлқинлар бўлиб, улар ўта қийин екранланади ва шовқинланади. Шунинг учун юқори шовқин сигналлари билан жуда кучли шовқинлантириш лозим ёки лазерли ҳамда пурковчи принтерлар ва термопечат қилувчи воситалардан фойдаланиш лозим.

Компютерларда махсус жўнатувчи-узатувчи воситалар ёки радиомаёқлардан фойдаланиш жуда хавфли ҳисобланади. Шунинг учун қимматли ахборотларни ҳар қандай компютер ва ривожланаётган давлатларнинг сохталаштирилган компютерларида қайта ишлаш тавсия етилмайди Агар компютер устахонаг жўнатилаётган бўлса аввал унда ахборотлар қолмаганига текшириб чиқиш талаб етилади

Ташқи кабеллар ва ўтказгичлардан електромагнит нурланишлар унчалик ката емас, аммо шуни ҳисобга олиш лозимки кабеллар бино ташқарисига чиқиб кетувчи кабеллар билан кесишмаслиги керак.

Қурилмаларни ерга улашларини монтаж қилиш назорат қилинаётган ҳудуд ичида амалга оширилиши керак. Ҳеч қачон ерга улаш симлари бошқа ўтказгичлар билан кесишиб қолишига йўл қўймаслик керак. Барча “ташқи дунё” билан алоқалар електрик тугунлар орқали амалга оширилиши лозим.

Назорат саволлари

1. Ахборотнинг техник каналдан чиқиб кетиш усуллари.
2. Ахборотнинг техник ҳимояси.
3. Ахборотнинг муҳандис техник ҳимояси.
4. Ихтиёрий ташкилот олиниб, унинг учун муҳандис – техник ҳимоя ишлаб чиқилсин.

Фойдаланилган адабиётлар

1. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.

2. https://en.wikipedia.org/wiki/ISO/IEC_27001:2005
3. http://ictnews.uz/api/news/78

2 – амалий машғулот.Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.

Ишнинг мақсади: Шифрлаш алгоритмлари асосида ахборотни махфийлигини таъминлаш**.**

Масаланинг қўйилиши: ўрганилган шифрлаш усуллари асосида берилган топшириқлар бажарилсин.

Ишни бажариш учун намуна

Симметрик шифрлаш усуллари фойдаланилган алмаштириш турига кўра ўрин алмаштириш ва ўрнига қўйиш усулларига бўлинади. Ўрин алмашиниш шифрларига очиқ матн белгилари махфий калит билан бирор алгоритм бўйича тартиби ўзгартирилади. Ўрнига қўйиш усулларида эса очиқ матн белгилари бошқа алфавит белгиларига алмаштирилади.

Содда ўрин алмаштириш усуллари

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.

Ўрин алмаштириш шифри оддий шифрлаш ҳисобланиб, бу усулда қатор ва устундан фойдаланилади. Чунки шифрлаш жадвал асосида амалга оширилади. Бу ерда калит (К) сифатида жадвалнинг устун ва қатори хизмат қилади. Матн (T_0) символларининг ўлчамига қараб NxM жадвали тузилади ва очиқ матнни (T_0) устун бўйича жойлаштирилиб чиқилади, қатор бўйича ўқилиб шифрланган матнга (T_1) эга бўлинади ва блокларга бўлинади.

Масалан, «Ахборот хавфсизлиги жадвали» матни шифрлансин.

T_0=Ахборот хавфсизлиги жадвали;

К = 5х5; В=5;

А	О	Ф	И	Д
Х	Т	С	Г	В
Б	Х	И	И	А
О	А	З	Ж	Л
Р	В	Л	А	И

T_1=АОФИД_ХТСГВ_БХИИА_ОАЗЖЛ_РВЛАИ

Усулнинг криптотурғунлиги блок узунлигига (матрица ўлчамига) 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.

Йўналишли ўрин алмаштириш синфидаги шифрларнинг қўлланилиши амалда кўп тарқалган. Бундай шифрлаш алгоритмлари бирор геометрик шаклга асосланган бўлади. Очиқ маълумот блоклари геометрик шаклга бирор траектория (узлуксиз из) бўйича жойлаштирилади. Шифрмаълумот эса бошқа траектория бўйича ҳосил қилинади. Геометрик шакл сифатида (*n* x *m*) ўлчамли жадвал олиб, унинг биринчи сатри бошидан бошлаб очиқ маълумот белгиларини чапдан ўнгга кетма-кет жойлаштириб, сатр тугагач иккинчи сатрга, очиқ маълумот белгиларини ўнгдан чапга кетма-кет жойлаштириб, бу сатр тамом бўлгач, кейинги сатрга олдингисига тескари йўналишда жойлаштирилади ва ҳоказо. Охирида тўлмай қолган сатр ячейкалари очиқ маълумот алфавитидан фарқли бўлган белгилар билан тўлдирилади. Сўнгра, очиқ маълумотни жойлаштириш тартибидан фарқли бўлган бирор йўналиш танлаб олиниб, шу йўналиш асосида шифрмаълумот ҳосил қилинади. Шифрмаълумот ҳосил қилиш йўналиши калит вазифасини бажаради. Мисол сифатида "*йўналишли ўрин алмаштириш шифрлаш алгоритми*" жумласини шифрлашни (4x10) –ўлчамли жадвал асосида қўйидагича амалга ошириш мумкин:

1	2	3	4	5	6	7	8	9	10
Й	*ў*	*н*	*а*	*л*	*и*	*ш*	*л*	*и*	*ў*
и	*т*	*ш*	*а*	*м*	*л*	*а*	*н*	*и*	*р*
р	*и*	*ш*	*ш*	*и*	*ф*	*р*	*л*	*а*	*ш*
...	*и*	*м*	*т*	*и*	*р*	*о*	*г*	*л*	*а*

Бу жадвал устунлари кетма-кетликларини аралаштирган ҳолда (бундай аралаштиришларнинг умумий сони 10!=3628800 та бўлади), масалан, 72968411035 тартиб (калит) билан "*шароўтиииалилфрлнлгааштйир.ўршаншимлмии*" шифрмаълумотни ҳосил қилинади. Шифрмаълумотни ҳосил қилиш жараёнини жадвалнинг сатрлари ўринларини ёки ҳар бир устунлари сатрларини алоҳида алмаштиришлар билан яна ҳам мураккаблаштириш мумкин. Сатрлар, устунлар ва алоҳида олинган сатр устунларини ёки алоҳида олинган устун сатрларини шифрлаш жараёни босқичларида ўзгартириб туриш билан яна ҳам мураккаб бўлган шифрлаш алгоритмларини ҳосил қилиш мумкин.

Содда ўрнига қўйиш усуллари

Шифрлаш алгоритмлари очиқ маълумот алфавити белгиларини шифрмаълумот белгиларига акслантиришдан иборат эканлиги такидланди. Акслантиришлар функциялари (калит деб аталувчи номаълум) параметрга

боғлиқ ҳолда: жадвал ва аналитик ифода кўринишларида берилиши мумкин. Ўрнига қўйиш шифрлаш алгоритмларининг дастлабки намуналари бўлган тарихий шифрлаш алгоритмларининг деярли ҳаммаси жадвал кўринишида ифодаланади. Ўрнига қўйиш шифрлаш алгоритмларининг умумий хусусиятини ҳисобга олиб, бу синфдаги алгоритмларни жадвал кўринишда қуйидагича ифодалаш мумкин:

Очиқ маълумот алфавити (кириллча белгилар)	А	Б	...	...	Я
Шифрмаълумот алфавити (иккилик саноқ системаси белгилари)	$x_0^0 x_1^0 x_2^0 x_3^0 x_4^0$	$x_0^1 x_1^1 x_2^1 x_3^1 x_4^1$	...	...	$x_0^{31} x_1^{31} x_2^{31} x_3^{31} x_4^{31}$

Кириллча алфавит белгилари сони 32 та, шу 32 та ҳар хил белгиларни битлар билан ифодалаш учун беш бит кифоя, яъни $2^5 = 32$. Келтирилган жадвалдан фойдаланиб, кириллча алфавитда ифодаланган очиқ малумот белгиларини уларга мос келувчи иккилик саноқ системасидаги беш битлик белгиларга алмаштириб шифрмаълумот ҳосил қилинади, яъни $x_i^j \in \{0;1\}$. Агарда, келтирилган жадвалда очиқ маълумот алфавити белгиларига шифрмаълумот алфавитининг қандай беш битлик белгилари мос қўйилганлиги номаълум бўлса, бу жадвал калит бўлиб, шифрмаълумотдан очиқ маълумотни тиклаш масаласи мураккаблашади. Бундай шифрлаш жараёнини ифодаловчи алгоритмнинг калитларининг умумий сони 32! бўлиб, ушбу $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Стирлинг формуласига кўра қуйидагича

$$32! = \left(\frac{32}{2{,}7}\right)^{32} \sqrt{2 \cdot 3{,}14 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} = 2^{96} \cdot 2^3 \cdot \sqrt{2} > 2^{99}$$

ҳисобланади. Бундай ҳолат эса калитни билмаган ҳолда дешифлаш жараёнини амалга оширишни жиддий мураккаблаштиради.

Аффин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аниқланади: *E(x)=ax+b (modm)*, бу ерда a, b - бутун сонлар бўлиб, калитлар ҳисобланади, 0≤a, b<m. *m* – алфавит узунлиги.

Дешифрлаш жараёни қуйидаги формула асосида амалга оширилади: $D(E(x)) = a^{-1}(E(x) - b) modm$. Бу ерда a^{-1} modm бўйича a га тескари бўлган сон.

Лотин алфавити фойдаланилганда у қуйидагича рақамланади:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Шифрлаш. Ушбу усулда маълумотларни шифрлаш учун “ATTACK AT DAWN” очиқ матни олиниб, калит сифатида a=3 ва b=4 олинди. Алфавит узунлиги m=26 га тенг. Бу ҳолда шифрлаш функцифсининг умумий кўриниши қуйидагича бўлади:$y = E(x) = (3x + 4)mod26$. Юқоридаги жадвалга асосланиб қуйидагини олиш мумкин:

Хабар	A	T	T	A	C	K	A	T	D	A	W	N
	0	19	19	0	2	10	0	19	3	0	22	13

Шифрлашнинг умумий кўриниши эса қуйидагича бўлади:

Хабар	A	T	T	A	C	K	A	T	D	A	W	N
x	0	19	19	0	2	10	0	19	3	0	22	13
3x+4	4	61	61	4	10	34	4	61	13	4	70	43
(3x+4)mod26	4	9	9	4	10	8	4	9	13	4	18	17
Шифр матн	E	J	J	E	K	I	E	J	N	E	S	R

Дешифрлаш жараёни. Дешифрлаш формуласи $D(y) = a^{-1}(y - b)modm$ га тенг бўлиб, $a^{-1} = 9$, b=4 ва m=26 га тенг бўлади.

Шифр матн	E	J	J	E	K	I	E	J	N	E	S	R
	4	9	9	4	10	8	4	9	13	4	18	17

Дешифрлашнинг умумий кўриниши эса :

Шифрматн	E	J	J	E	K	I	E	J	N	E	S	R
y	4	9	9	4	10	8	4	9	13	4	18	17
9(y-4)	0	45	45	0	54	36	0	45	81	0	126	117
9(y-4)mod26	0	19	19	0	2	10	0	19	3	0	22	13
Хабар	A	T	T	A	C	K	A	T	D	A	W	N

Частотавий таҳлил усули

Частотавий, яъни статистик характеристикалар усулида симметрик ёки носимметрик криптотизим криптотаҳлилчиси шифрматндаги белгилар, ҳарфлар, сўзларнинг такрорланишлари сонини (частоталарини) ҳисоблаб, очиқ матн қайси тилда ёзилганини аниқлайди. Сўнгра эса, шифрматн шифр

белгилари параметрларини очиқ матн қайси тилда ёзилган бўлса, шу тилнинг параметрлари билан солиштиради. Масалан, инглиз тилида **E** ҳарфи частотаси юқори, шифрматнда **L** ҳарфи частотаси юқори. Шифрматндаги **L** ҳарфини **E** ҳарфи билан алмаштирилади, яъни шифрматн ва очиқ матн ёзилган тил частоталарини камайиш тартибида ёзиб, тартиби тўғри келган белгилар ўзаро алмаштирилади. Кейин шифрматн биграмма, триграмма ва **k**-граммаларининг такрорланишлар сонини топиб, очиқ матн ёзилган тил биграмма, триграмма ва **k**-граммалари билан мос ҳолда алмаштиради. Биграмма, триграмма, **k**-грамма дэганда, матнда иккита, учта ва **k**-та белгининг кетма-кет келиши тушунилади. Масалан, инглиз тилида **th**, **in**, **is**, **er**, **he**, **en**, биграммалари, рус тилида **ст**, **но**, **ен**, **то**, **на** биграммалари, **сто, ено, нов, тов, ова** триграммалари кўп учрайди. Қуйидаги жадвалда инглиз тили ҳарфларининг пайдо бўлишининг нисбий частотаси келтирилган (40 000 та сўз ичида).[1]

Ҳарф	Сони		Ҳарф	Частотаси
E	21912		E	12.02
T	16587		T	9.10
A	14810		A	8.12
O	14003		O	7.68
I	13318		I	7.31
N	12666		N	6.95
S	11450		S	6.28
R	10977		R	6.02
H	10795		H	5.92
D	7874		D	4.32
L	7253		L	3.98
U	5246		U	2.88
C	4943		C	2.71
M	4761		M	2.61
F	4200		F	2.30
Y	3853		Y	2.11
W	3819		W	2.09
G	3693		G	2.03
P	3316		P	1.82
B	2715		B	1.49
V	2019		V	1.11
K	1257		K	0.69
X	315		X	0.17
Q	205		Q	0.11
J	188		J	0.10

[1] Stamp Mark. Information security: principles and practice. 24 – c.

Z	128		Z	0.07

Юқорида айтиб ўтилган принциплар ҳозирги кунда кенг тарқалган паролларни танлаш бўйича дастурларда қўлланилади. Паролларни танлаш бўйича дастур аввало эҳтимоллиги катта бўлган паролларни танлайди. эҳтимоллиги кичик бўлган паролларни кейинга олиб қўяди.

A5/1 оқимли шифрлаш алгоритми

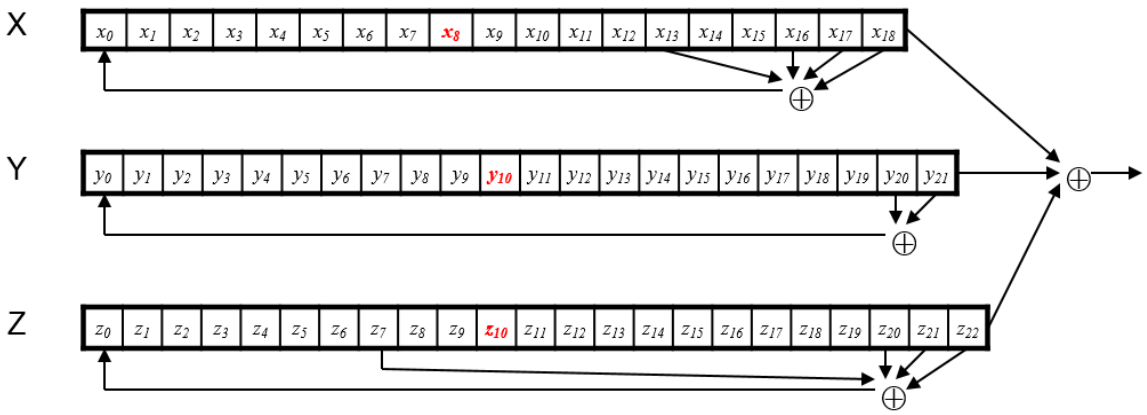
A5/1 шифрлаш алгоритмида дастлабки калитнинг узунлиги 64 битни ташкил этиб, у қуйидиги учта регистрга қиймат қилиб берилади:[1]

- ✓ X: 19 bit (x_0,x_1,x_2, ...,x_{18})
- ✓ Y: 22 bit (y_0,y_1,y_2, ...,y_{21})
- ✓ Z: 23 bit (z_0,z_1,z_2, ...,z_{22})

Ҳар бир қадамда: m = maj(x_8, y_{10}, z_{10}) ҳисобланади

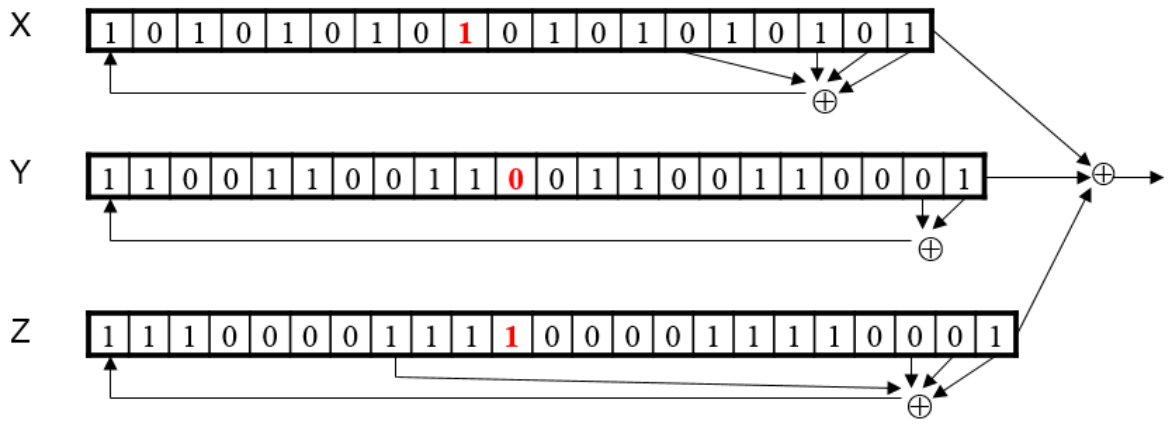
- ○ **масалан**: maj(0,1,0) = 0 ва maj(1,1,0) = 1
- ✓ агар $x_8 = m$ га тенг бўлса, у ҳолда X регистор қийматлари
- ○ $t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$
- ○ $x_i = x_{i-1}$ for i = 18,17,…,1 va $x_0 = t$
- ✓ агар $y_{10} = m$ га тенг бўлса, у ҳолда Y регистор қийматлари
- ○ $t = y_{20} \oplus y_{21}$
- ○ $y_i = y_{i-1}$ for i = 21,20,…,1 and $y_0 = t$
- ✓ агар $z_{10} = m$ га тенг бўлса, у ҳолда Z регистор қийматлари
- ○ $t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$
- ○ $z_i = z_{i-1}$ for i = 22,21,…,1 and $z_0 = t$
- ✓ **натижавий калит кетма-кетлиги** $x_{18} \oplus y_{21} \oplus z_{22}$ га тенг бўлади.

Бу амаллар қуйидаги расмда ифодаланган:



[1] Stamp Mark. Information security: principles and practice. 53 – c.

Масалан қуйидаги кўрсатилган ҳол учун:



$m = \text{maj}(x_8, y_{10}, z_{10}) = \text{maj}(\mathbf{1},\mathbf{0},\mathbf{1}) = \mathbf{1}$ га тенг бўлади. Натижада X регистор силжийди, Y регистор силжимайди ва Z регистор силжийди. Ўнг томондаги битлар XOR амал бўйича қўшилади ва $0 \oplus 1 \oplus 0 = 1$ қиймат олинади.

Ушбу усулда бир циклда бир бит калит ҳосил қилинади.

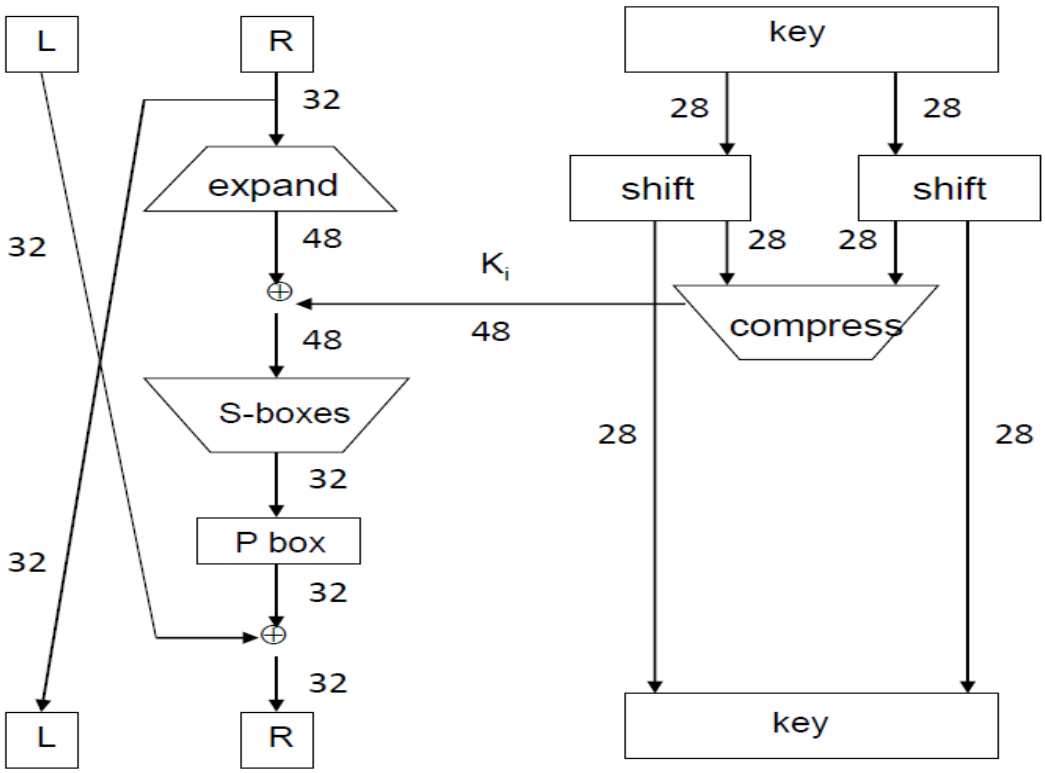
DES шифрлаш алгоритми

DES стандарт шифрлаш алгоритми Америка Қўшма Штатлари (АҚШ) “Миллий Стандартлар Бюроси” томонидан 1977 йилда эълон қилинган. 1980 йилда АҚШнинг “Стандартлар ва Технологиялар Миллий Институти” бу алгоритмни давлат ва савдо-сотиқ молияси соҳасидаги маҳфий бўлмаган, аммо муҳим бўлган маълумотларни руҳсат этилмаган жисмоний ва юридик шаҳслардан муҳофаза қилинишида шифрлаш алгоритми сифатида қўллаш стандарти деб қабул қилди. [1]

DES алгоритмида: дастлабки 56 битли калитдан раунд калитларини ҳосил қилишнинг мураккаб эмаслиги, раунд асосий акслантиришларининг аппарат-техник ва дастурий таъминот кўринишларида қўлланилишини таъминлашнинг қулайлиги, ҳамда, улар криптографик ҳоссаларининг самарадорлиги – криптобардошлилигининг юқорилиги, бу алгоритмнинг асосий хусусиятларини белгилайди.

Шифрлаш жараёни 64 битли очиқ маълумот блокларини алгоритмда берилган *IP* –жадвал бўйича ўрин алмаштириш, унинг натижасини дастлабки 56 битли калитдан алгоритмда келтирилган жадваллар билан битларнинг ўринларини алмаштириш, циклик суриш ва баъзи битларни йўқотиш акслантиришларидан фойдаланиб ҳосил қилинадиган 48 битли раунд калитлари ҳамда асосий акслантиришлари билан 16 марта шифрлаш, шифрлаш натижаси блоки битларини берилган IP^{-1} –жадвал бўйича ўринларини алмаштиришдан иборат (2.1-расм).

[1] Stamp Mark. Information security: principles and practice. 58 – с.



2.1-расм. DES алгоритмининг 1 раунди

DES шифрлаш алгоритмида фойдаланилган муҳим хавфсизлик хусусиятларидан бири бу S – жадвалдир. Бу жадвалда кирувчи қиймат 6 битни ташкил этиб, чиқишда 4 битга ўзгаради. DES алгоритми содда криптографик ўзгартиришлардан иборат бўлиб, шифрлашда ва дешифрлашда катта тезликга эга.

DES алгоритмида фойдаланилган E кенгайтириш жадвали

- Киришда 32 бит

```
 0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
```

- Чиқишда 48 бит

```
31  0  1  2  3  4  3  4  5  6  7  8
 7  8  9 10 11 12 11 12 13 14 15 16
15 16 17 18 19 20 19 20 21 22 23 24
23 24 25 26 27 28 27 28 29 30 31  0
```

DES да фойдаланилган S жадваллар

Кирувчи 6 бит маълумот , 101011

(0,5) (1,2,3,4)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Чиқишда, 1001

P жадвал:

- Киришда 32 бит

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

- Чиқишда 32 бит

15	6	19	20	28	11	27	16	0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8	18	12	29	5	21	10	3	24

RSA алгоритми

1976 йилда Диффи ва Хеллман ўзларининг «Криптологияда янги йўналиш» илмий ишларида бир томонли функция сифатида $y = g^a \bmod n$ ифода билан аниқланган дискрет даражага кўтариш функциясини таклиф қилиб, $a = \log_g y \bmod n$ ифодадаги дискрет логарифмни ҳисоблашнинг амалий жиҳатдан мураккаблигига асосланган эди. 1978 йилда эса, Массачусетс технология институтининг олимлари: Р.Л. Ривест, А. Шамир, Л. Адлман, ўзларининг илмий мақоласида биринчи бўлиб маҳфий услубли ва ҳақиқатан ҳам бир томонли бўлган функцияни таклиф этдилар. Бу мақола «Рақамли имзоларни қуриш услублари ва очиқ калитли криптосистемалар» деб аталиб, кўпроқ аутентификация масалаларига қаратилган. ҳозирги кунда, бу юқорида номлари келтирилган олимлар таклиф этган функцияни, шу олимларнинг шарафига RSA бир томонли функцияси дейилади. Бу функция мураккаб бўлмай, унинг аниқланиши учун, элементар сонлар назарясидан баъзи маълумотлар керак бўлади.[1]

Мисол: Учта ҳарфдан иборат бўлган “CAB” маълумотини шифрлаймиз.

Биз қулайлик учун кичик туб сонлардан фойдаланамиз Амалда эса мумкин қадар катта туб сонлар билан иш кўрилади.

1. Туб бўлган p=3 ва q=11 сонларини танлаб оламиз.

[1] Stamp Mark. Information security: principles and practice. 95 – c.

2. Ушбу $n=pq=3*11=33$ сонини аниқлаймиз.

Сўнгра, $\varphi(33)=(p-1)(q-1)=2\cdot 10=20$ сонини топамиз, ҳамда бу сон билан 1 дан фарқли бирор умумий бўлувчига эга бўлмаган e сонини, мисол учун $e=3$ сонини, оламиз.

3. Юқорида келтирилган (24) шартни қаноатлантирувчи d сонини $3d=1 \pmod{20}$ тенгликдан топамиз. Бу сон $d=7$

4. Шифрланиши керак бўлган «CAB» маълумотини ташкил этувчи ҳарфларни: A→1, B→2, C→3 мосликлар билан сонли кўринишга ўтказиб олиб, бу маълумотни мусбат бутун сонларнинг, кетма-кетлигидан иборат деб қараймиз. У ҳолда маълумот (3,1,2)кўринишда бўлади ва уни {e;n}={3;33} очиқ калит билан $f_z(x)=x^3 \pmod{33}$ бир томонли функция билан шифрлаймиз:

x=3 да ШМ1=(3^3)(mod33)=27,

x=1 да ШМ2=(1^3) (mod33)=1,

x=2 да ШМ3=(2^3) (mod33)=8.

5. Бу олинган шифрланган (27,1,8) маълумотни маҳфий {$d;n$}={7;33} калит билан $f_z^{-1}(y)=y^7 \pmod{33}$ ифода орқали дешифрлаймиз:

y=9 да ОМ1=(27^7) (mod33)=3,

y=1 да ОМ2=(1^7) (mod33)=1,

y=29 да ОМ3=(8^7) (mod33)=2.

Шундай қилиб, криптотизимиларда RSA алгоритмининг қўлланиши қуйидагича: ҳар бир фойдаланувчи иккита етарли даражада катта бўлмаган p ва q туб сонларни танлайдилар ва юқорида келтирилган алгоритм бўйича d ва e туб сонларини ҳам танлаб олади. Бунда $n=pq$ бўлиб, {$e;n$} очиқ калитни {$d;n$}эса маҳфий калитни ташкил этади. Очиқ калит очиқ маълумотлар китобига киритилади. Очиқ калит билан шифрланган шифрматнни шу калит билан дешифрлаш имконияти йўқ бўлиб, дешифрлашнинг маҳфий калити фақат шифр маълумотининг хақиқий эгасига маълум.

Топшириқ

1. A5/1 шифрлаш алгоритмида қуйидаги қийматлар билан 5 бит кетма – кетлик ҳосил қилинг:

$X = (x_0, x_1, ..., x_{18}) = (1010101010101010101)$

$Y = (y_0, y_1, \cdot\cdot, y_{21}) = (1100110011001100110011)$

$Z = \{z_0, z_1, ..., z_{22}) = (11100001111000011110000)$

2. Цезар усулида қуйидиги шифрни очинг ва калитни аниқланг:

CSYEVIXIVQMREXIH

3. Қуйида берилган шифрматнни частоталар усули бўйича таҳлил қилинг ва очиқ матнни топинг:

GBSXUCGSZQGKGSQPKQKGLSKASPCGBGBKGUKGCEUKUZKGG
BSQEICACGKGCEUERWKLKUPKQQGCIICUAEUVSHQKGCEUPCG
BCGQOEVSHUNSUGKUZCGQSNLSHEHIEEDCUOGEPKHZGBSNKC
UGSUKUASERLSKASCUGBSLKACRCACUZSSZEUSBEXHKRGSHW
KLKUSQSKCHQTXKZHEUQBKZAENNSUASZFENFCUOCUEKBXG
BSWKLKUSQSKNFKQQKZEHGEGBSXUCGSZQGKGSQKUZBCQAEI
ISKOXSZSICVSHSZGEGBSQSAHSGKHMERQGKGSKREHNKIHSLI
MGEKHSASUGKNSHCAKUNSQQKOSPBCISGBCQHSLIMQGKGSZG
BKGCGQSSNSZXQSISQQGEAEUGCUXSGBSSJCQGCUOZCLIENKG
CAUSOEGCKGCEUQCGAEUGKCUSZUEGBHSKGEHBCUGERPKHE
HKHNSZKGGKAD

Назорат саволлари

1. Ўрин алмаштириш ва ўрнига қўйиш шифрлари.
2. Модул арифметрикаси.
3. DES шифрлаш алгоритми хусусиятлари.
4. RSA алгоритми.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.

3 – амалий машғулот. Ахборотни ҳимоялашда криптографиянинг ўрни. Симметрик блокли шифрлаш алгоритмлари. Очиқ калитли шифрлаш алгоритмлари. Хэш функциялар ва ЭРИ алгоритмлари. Электрон рақамли имзо алгоритмлари.

Ишнинг мақсади: Тармоқлараро экран қурилмасини ўрнатиш ва уни созлаш**.**

Масаланинг қўйилиши: Фойдаланувчи шахсий компьютерида тармоқдан бўлиши мумкин таҳдидларни олдини олиш учун шахсий тармоқлараро экран воситасини ўрнатиши ва созлаши лозим.

Ишни бажариш учун намуна

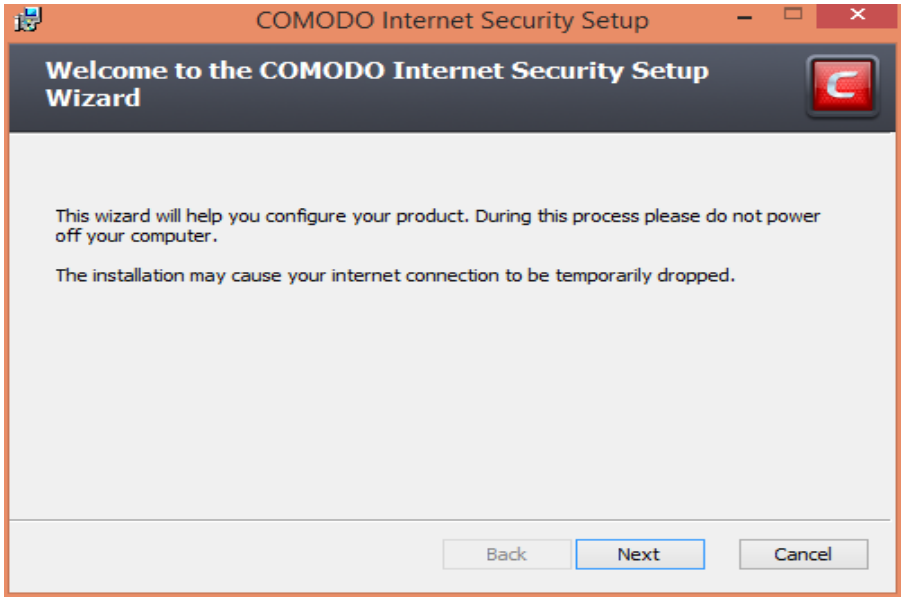
Ушбу амалий ишда шахсий тармоқлараро экранлар турига кирувчи COMODO Internet Security Firewall дастурий воситаси олиниб, уни ўрнатиш ва созлаш амалга оширилади.

Ушбу дастурий воситани ўрнатиш учун тизимдан қуйидаги ресурслар талаб этилади:

– Windows 7 (32-bit ва 64-bit версиялар) ёки Windows XP (32-bit ва 64-bit версиялар);
– Internet Explorer 5.1 ёки ундан юқори версияси;
– 128 MB оператив хотира (RAM);
– 210 MB қаттиқ дискдан жой.

Ушбу дастурий воситани http://www.personalfirewall.comodo.com) манзилидан олишингиз мумкин.

Дастурий воситани кўчириб олганингиздан сўнг, COMODO Internet Security 8.2.0.4508_x32 файл устида икки марта босинг. Шундан сўнг ҳосил бўлган ойнадан керакли танлов танланади.

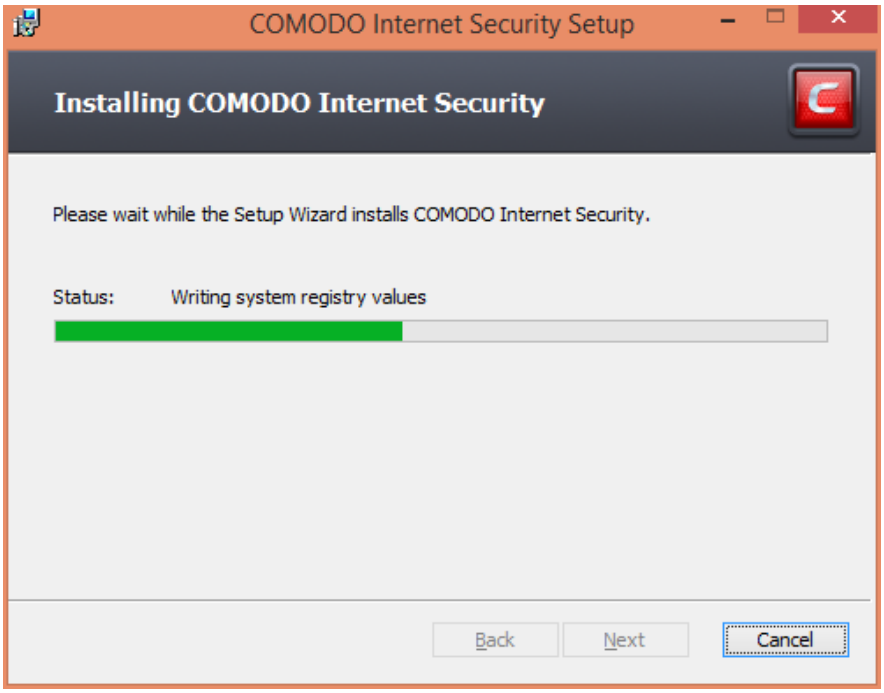


3.1 – расм. Ўрнатиш тилини танлаш

Шундан сўнг, тизим томонидан таклиф этилган келишувга ўз

розилигингизни билдирасиз. Шундан сўнг дастурни ўрнатиш жараёни юкланади.

3.2 – расм. Дастур шартларини қабул қилиш

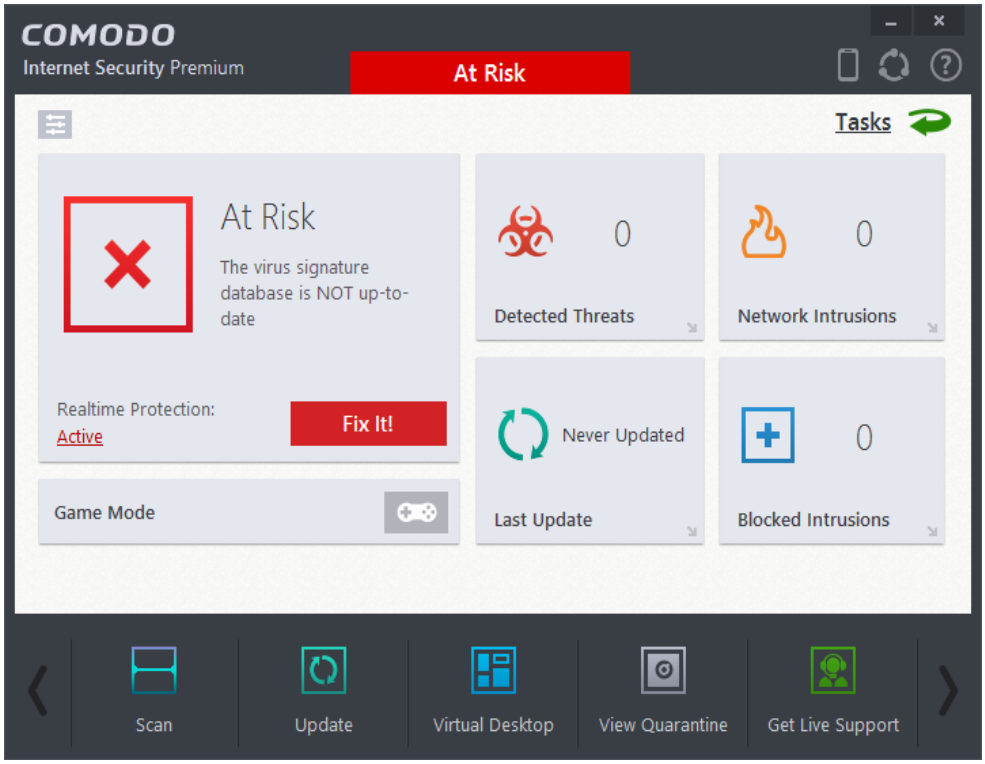


3.3 – расм. Дастурни ўрнатиш

Дастур ўрнатилгандан сўнг қуйидаги ойна ҳосил бўлади ва бу ойнадан керакли бандни танланг (масалан, I am at Home).

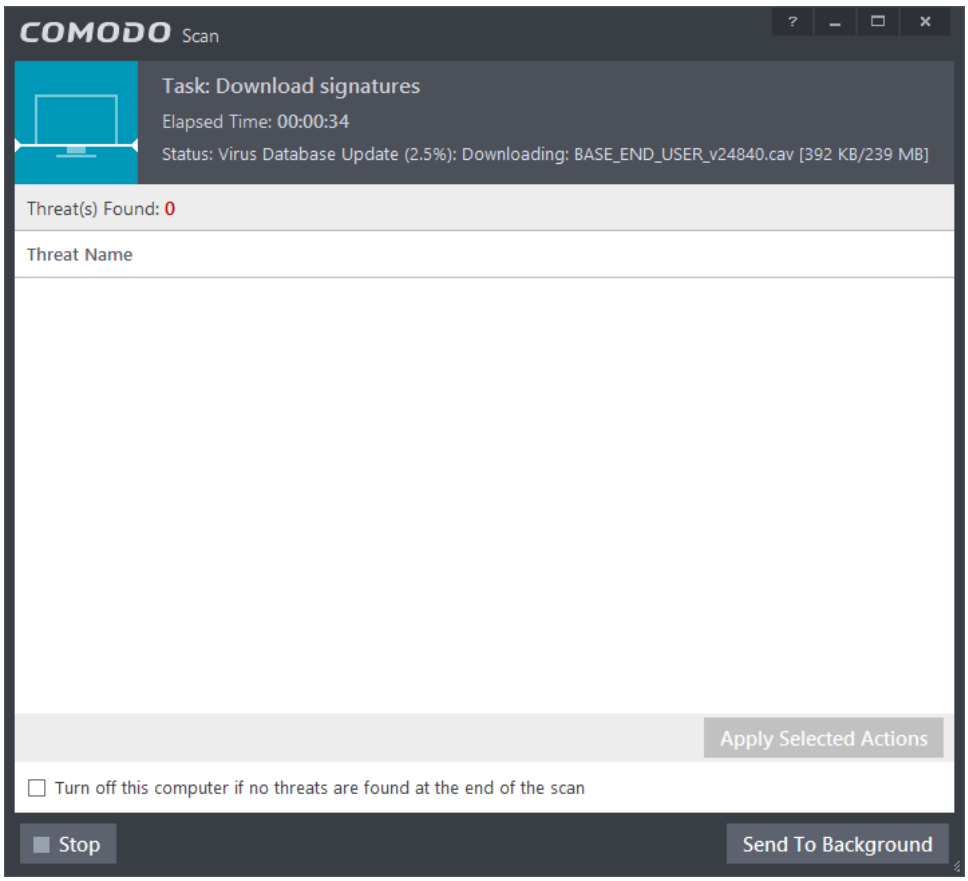
3.4 – расм. Керакли тармоқни танлаш

Шундан сўнг, дастурнинг асосий ойнаси ҳосил бўлади (5 -расм). Дастур янги ўрнатилгандан сўнг, интернер тармоғидан ўз базасини янгилайди. Шундан сўнг ўз ишини бошлайди. Агар дастур ўз базасини янгиламаган бўлса расмда кўрсатилгани каби “At Risk” кўрсаткичи пайдо бўлади.



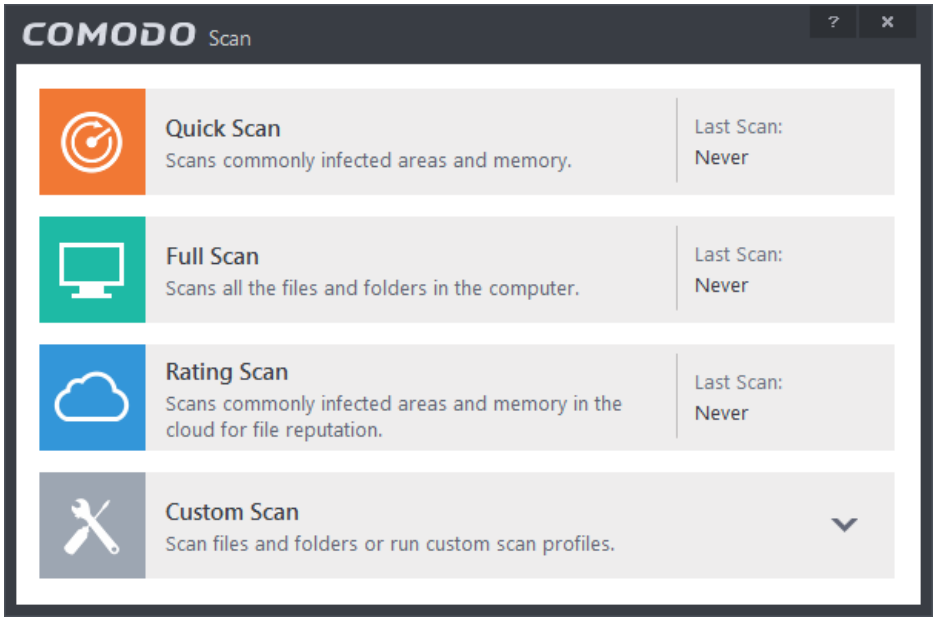
3.5 – расм. Дастурнинг асосий ойнаси

Дастурни янгилаш учун Update банди танланади ва базани юклаб олгунга қадар кутиш тавсия этилади (3.6 – расм.).



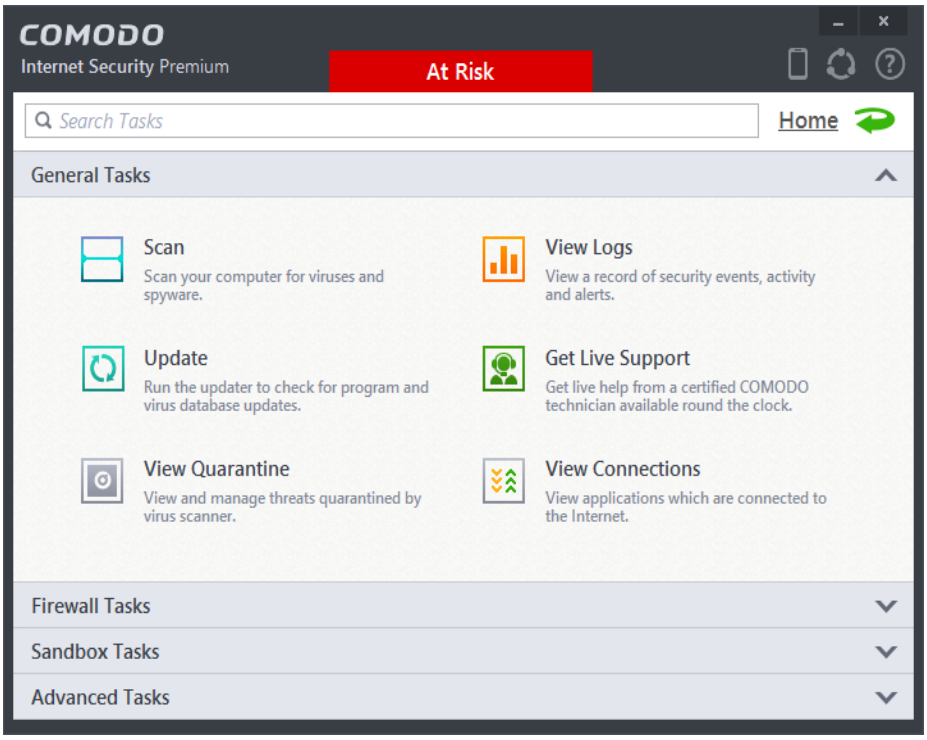
3.6 – расм. Дастурни базасини янгилаш

Тизимни текшириш учун Scan бандига ўтилади ва керакли текшириш тури танланади.



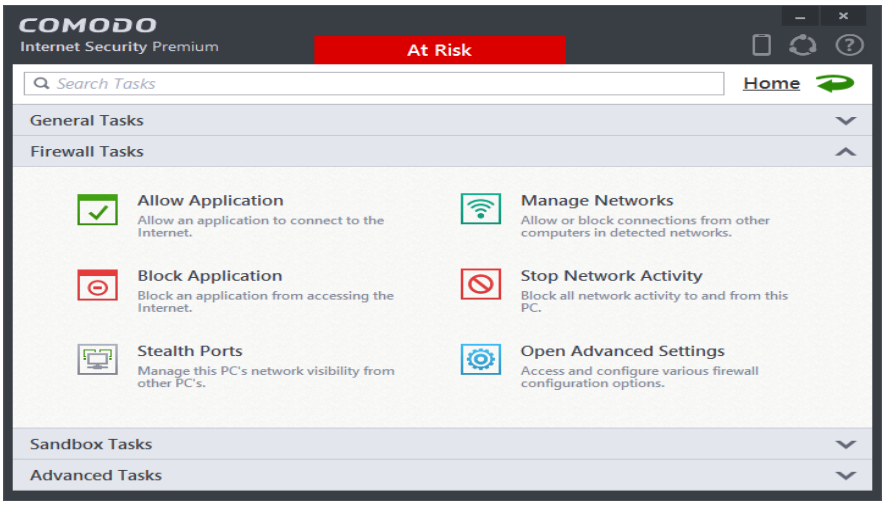
3.7 – расм. Текшириш турини танлаш

Дастурнинг асосий созланишларини амалга ошириш учун, дастурнинг асосий онасида “Tasks” банди танланади. Бу ойнада бир қанча бандлар мавжуд бўлиб, улар умумий созланишлар - “General tasks”, Тармоқлараро экран созланмалари – “Firewall Tasks”, сандбох созланмалари – “Sandbox Tasks”, кенгайтирилган созланмалар – “Advanced Tasks”. Ҳар бир бандлар ўз номига хос вазифаларни бажариб, ушбу амалий ишида тармоқлараро экранни созлаш билан яқиндан танишиб чиқилади.



3.8 – расм. Дастурнинг асосий созланишлар ойнаси

Тармоқлараро экранни бошқаришнинг ойнаси қўриниши 3.9 – расмда келтирилгани каби бўлиб, у қуйидаги бандлардан иборат:



3.9 – расм. Тармоқларро экран вазифалари

– Интернет тармоғига рухсат берилган иловалар (Allow application);
– Интернет тармоғи орқали бошқариш чекланган иловалар (Block

Application);

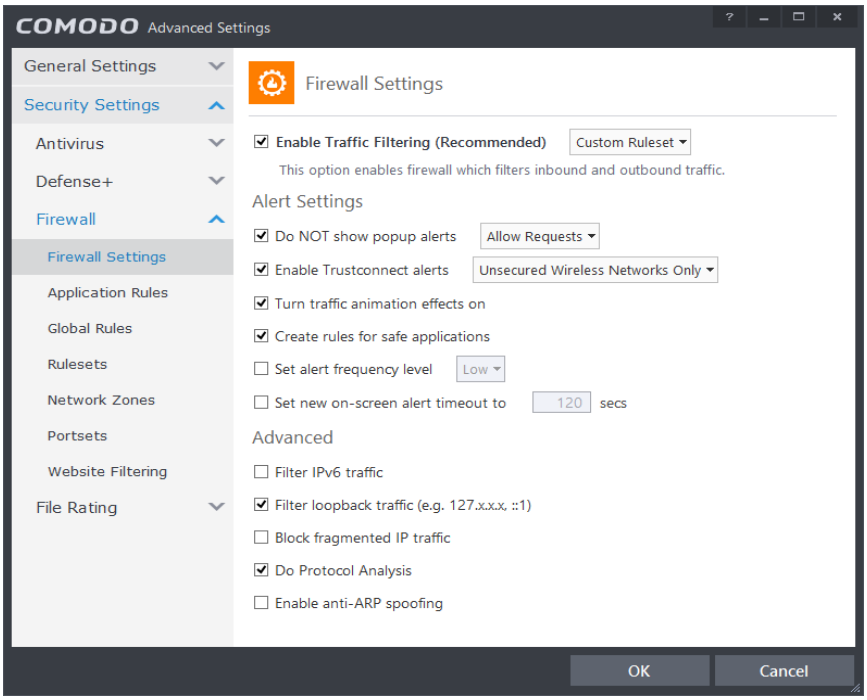
– тармоқни бошқариш (Manage Network);

– тармоқни қулфлаб қўйиш (Stop Network Activity);

– компьютерни тармоқда бошқа компьютерларга турли кўринишда кўрсатиш (Steals Ports);

– кенгайтирилган созланишлар (Open Advanced Settings).

Ушбу саҳифада энг муҳим саналган бандлардан бири бу – кенгайтирилган бандлардир. Ушбу бандниг умумий кўриниши 3.10 – расмда кўрсатилган.



3.10 – расм. Тармоқлараро экран ойнаси

Ушбу ойнада тармоқлараро экранни созлашнинг кенг имкониятлари келтирилган бўлиб, бу банд орқали янги қоидаларни яратиш, қоидалар гуруҳини яратиш, иловалар учун қоидалар яратиш, веб сайтларни филтерлаш, файларни назоратлаш каби бир қатор ишларни амалга ошириш мумкин.

Топшириқ

1. Юқорида келтирилган маълумотлар асосида тармоқлараро экранни ўрнатинг ва маълумотлар базасини янгиланг.

2. Антивирус созланмаларини ўрнатинг ва анитивирус учун базани янгиланг.

3. Турли иловаларни блоклаш орқали ишламаётганига ишонч ҳосил қилинг.

4. Кенгайтирилган созланиш ойнасидан фойдаланилган ҳолда, турли

қоидалар яратинг ва уларни ишлаганига ишонч ҳосил қилинг.

5. Тармоқлараро экран ишлаш вақтидаги ҳодисаларни қайд этганини Лог файлдан фойдаланиб аниқланг.

6. Барча натижаларни ҳисоботда акс эттиринг.

Назорат саволлари

1. Тармоқлараро экранни вазифаси.
2. Шахсий тармоқлараро экран вазифаси.
3. Тармоқлараро экран турлари.
4. Тармоқлараро экранда янги қоидалар яратиш.

Фойдаланилаган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.

2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.

3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.

4 – амалий машғулот. Аутентификация ва идентификация усуллари. Рухсатларни назоратлаш. Тармоқлараро экран. Ҳужумларни аниқлаш тизимлари.

Ишнинг мақсади: SSL ва IPSec тармоқ протоколларининг таҳлили ва улардан фойдаланиш.

Масаланинг қўйилиши: SSL протоколларида хавфсизлик таҳлили амалга оширилсин.

Ишни бажариш учун намуна

SSL тармоқ протоколи. Transport Layer Security (TLS) дастлаб яратилган Secure Sockets Layer (SSL) протоколининг давомчиси саналиб, компьютер тармоғида алоқа хавфсизлигини таъминлаш учун яратилган ва бир нечта криптографик протоколлар ва алгоритмлардан ташкил топган. Ушбу протоколда X.509 сертификатидан фойдаланилган бўлиб, томонларни аутентификациялашда ассиметрик шифрлаш алгоритмларидан фойдаланилади.

X.509 сертификати. Криптографияда X.509 стандарти очиқ калитли инфратузилмалар (public key infrastructure (PKI)) ва имтиёзга асосланган бошқариш инфратузилмалари (Privilege Management Infrastructure (PMI)) учун мўлжалланган.

Ушбу X.509 v3 сертификатининг тузулиши қуйидагича:

- **Certificate;**
- **Version** (версия);
- **Serial Number** (сериал рақами);
- **Algorithm ID** (алгоритм ID си);
- **Issuer** (сертификат берувчи ташкилот, эмитент);
- **Validity** (амал қилиш муддати);
- **Not Before;**
- **Not After;**
- **Subject** (сертификат олувчи ташкилот, истемолчи);
- **Subject Public Key Info** (истемолчи очиқ калит маълумоти);
- **Public Key Algorithm** (очиқ калит алгоритми);
- **Subject Public Key** (очиқ калит);
- **Issuer Unique Identifier (optional)** (эмитентнинг такрорланмас идентификатори);
- **Subject Unique Identifier (optional)** (истемолчининг такрорланмас идентификатори);
- **Extensions (optional)** (кенгайтирилган имкониятлари);

– **Certificate Signature Algorithm** (сертификатда фойдаланилган ЭРИ алгоритми);

– **Certificate Signature** (сертификат қўйилган имзо).

TLS/SSL протоколида фойдаланилган рақамли сертификатларни яратувчи, учинчи ишончли томон сифатида қатнашган ташкилотларнинг 2015 йил бошидаги кўрсаткичи қуйида кўрсатилган (4.1-жадвал):

4.1-жадвал

Рақамли сертификатларни яратувчи ташкилотлар

Ўрин	Ташкилот	Фойдаланилиши	Бозордаги улуши
1.	Comodo	6.6%	33.6%
2.	Symantec Group	6.5%	33.2%
3.	Go Daddy Group	2.6%	13.2%
4.	GlobalSign	2.2%	11.3%
5.	DigiCert	0.6%	2.9%

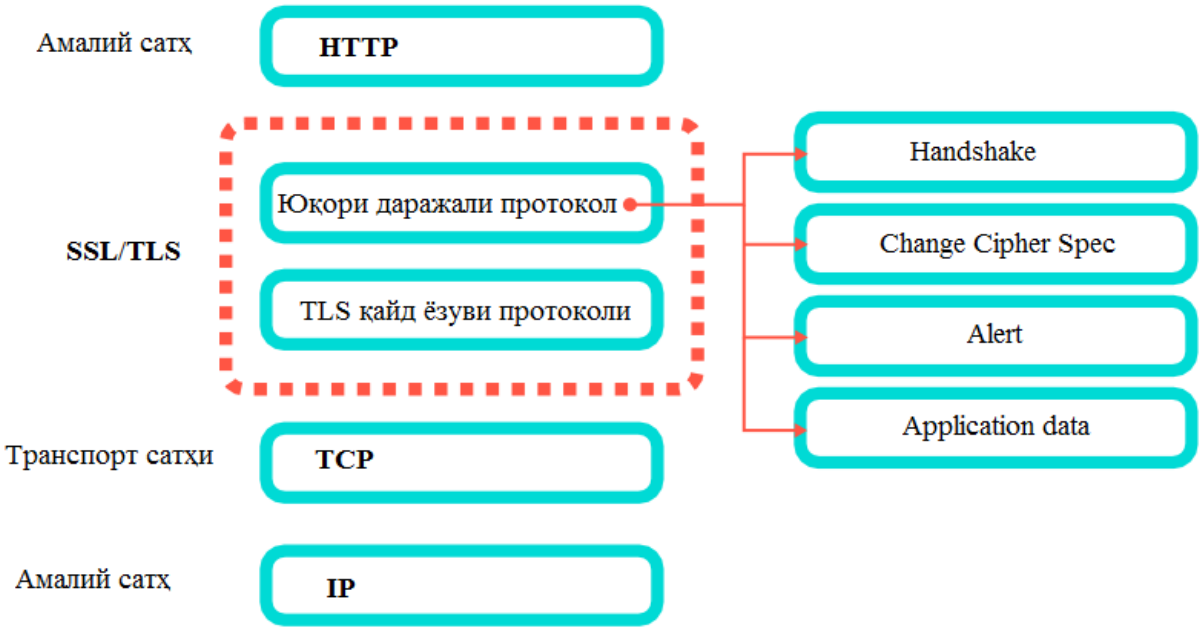
Ҳозирда юқорида номлари келтирилган SSL/TLS протоколверсиялари амалда фойдаланилмоқда ва қуйидаги жадвалда уларнинг web саҳифаларда фойдаланиш кўрсаткичлари ва уларнинг хавфсизлик хусусияти келтирилган (4.2-жадвал).

4.2-жадвал

SSL/TLS протоколларнинг хавфсизлиги таҳлили

Протокол версияси	Web саҳифаларда қўллаб қуватланиши	Хавфсизлик кўрсаткичи
SSL 2.0	14.4% (−0.5%)	Хавфсиз эмас
SSL 3.0	47.3% (−3.1%)	Хавфсиз эмас
TLS 1.0	99.7% (±0.0%)	Алгоритм турига боғлиқ
TLS 1.1	51.5% (+1.6%)	Алгоритм турига боғлиқ
TLS 1.2	54.5% (+1.8%)	Алгоритм турига боғлиқ

Қуйидаги, 4.1-расмда SSL/TLS тармоқ протоколининг тармоқ сатҳларида жойлашуви келтирилган.



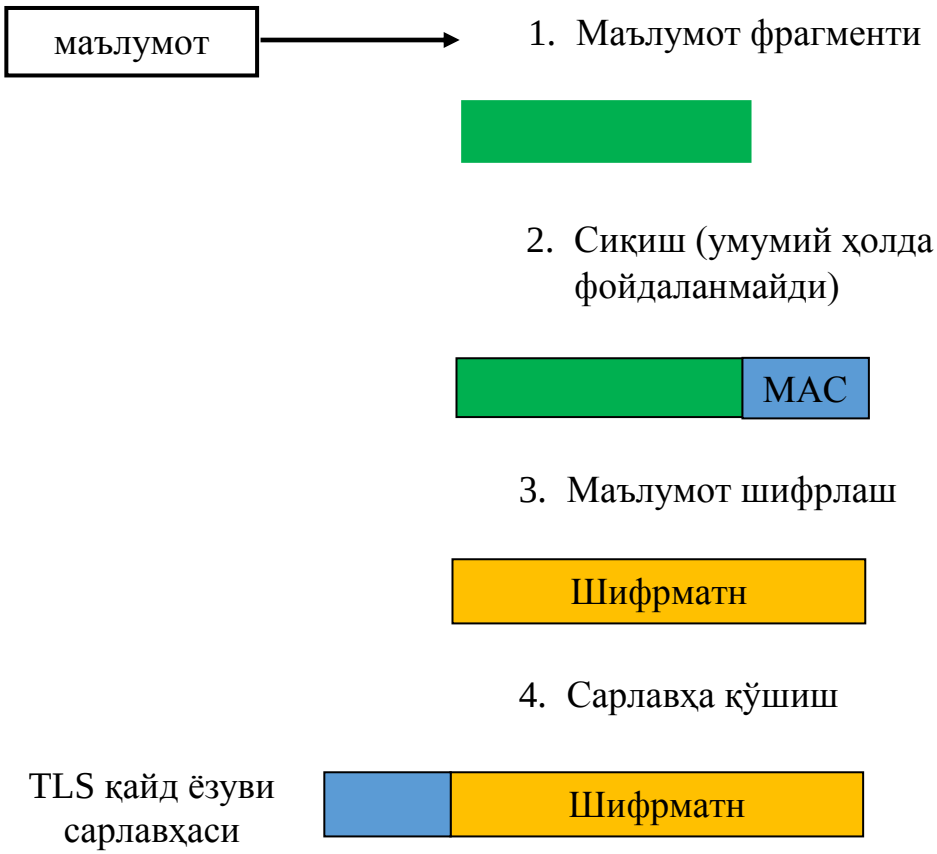
4.1-расм. SSL/TLS протоколи

SSL/TLS сатҳининг қуйи ташкил этувчи протоколи (TLS қайд ёзуви протоколи), дастлабки маълумотни фрагментларга ажратиш, созланишга кўра фрагмент маълумотни сиқиш, сиқилган маълумотга унинг MAC қийматини қўшиш, ҳосил бўлган маълумот жуфтини шифрлаш алгоритми ёрдамида шифрлаш ва унга TLS қайд ёзуви сарлавҳасини қўшиш амалларидан ҳосил бўлади (4.2-расм).

*Юқори даражали протокол.*Ушбу протокол TLS қайд ёзуви протоколи устида жойлаштирилган бўлиб, у тўртта протоколдан иборат. Ҳар бир протокол ўзининг махсус вазифасига эга бўлиб, улар алоҳида ёки биргаликда ҳам фойдаланилиши мумкин.

*Handshake протоколи.*Ушбу протокол ҳар икки томонда бир-бирини аутентификациялаш, фойдаланиладиган криптографик алгоритмларни келишиш ва бошқа боғланиш параметларини алмашиш имконини беради. Ушбу протокол клиент ва сервер орасида алмашинувчи тўртта хабарлар мажмуасидан иборат. Ҳар бир хабарлар мажмуаси алоҳида пакет бўлиб юборилади.

*ChangeCipherSpec Protocol:*ушбу протокол асосида алоқа канали ҳимояланади.



4.2-расм. TLS/SSL қайд ёзуви протоколи

*Alert Protocol:*ушбу хабар бериш протоколи, барча протокол натижаларини эълон қилишда фойдаланилади.

*Application Data Protocol:*ушбу протокол илова сатҳидан маълумотни олиб, уни махфий канал орқали юборишни таъминлайди.

TLS қайд ёзуви формати. Ушбу формат учта майдондан иборат бўлиб, унинг асосида юқори даражали протокол қурилади (4.6-жадвал).

– Byte 0:TLS қайд ёзуви тури.
– Bytes 1-2:TLS протокол версияси (major/minor).
– Bytes 3-4: қайд ёзувидаги маълумот узунлиги (ўзидан ташқари). Максимал қиймати 16384 бит ёки 16 Кбит.

4.3-жадвал

TLS қайд ёзуви формати

TLS қайд ёзуви тури	Версияси		Маълумот узунлиги		юқори даражали протокол
	major	minor	(bits 15..8)	(bits 7..0)	

TLS қайд ёзуви тури қуйидаги 4.4-жадвалда кенлтирилган

4.4-жадвал

Hex	**Dec**	**Тури**
0x14	20	ChangeCipherSpec
0x15	21	Alert
0x16	22	Handshake
0x17	23	Application
0x18	24	Heartbeat

Протокол версияси эса 4.5-жадвалда келтирилиб ўтилган.

4.5-жадвал

Hex	**Dec**	**Протокол версияси**
0x0300	3,0	SSL 3.0
0x0301	3,1	TLS 1.0
0x0302	3,2	TLS 1.1
0x0303	3,3	TLS 1.2

*Handshake протокол формати.*Ушбу протокол TLSпротоколида асосий протоколларда бири саналиб, бу протокол орқали хавфсизлик параметрлари узатилади. Ушбу протокол орқали ўнбир турдаги хабар узатилаши мумкин (4.6-жадвал).

4.6-жадвал

Handshake протокол формати

Byte +0	Byte +1	Byte +2	Byte +3
22			
Версия		Узунлик	
Минор	Мажор	(bits 15..8)	(bits 7..0)
Хабар тури	Handshake маълумоти узунлиги		
	(bits 23..16)	(bits 15..8)	(bits 7..0)
Handshake маълумоти			

*Handshake маълумоти узунлиги.*Ушбу майдон узунлиги 3 байт бўлиб, фақат Handshake маълумоти узунлигини билдиради, сарлавҳани ўз ичига олмаган ҳолда. Битта TLS ёзишмасида бир нечта Handshake маълумоти бўлиши мумкин. Handshake протоколида хабар тури қуйидагича бўлиши мумкин (4.7-жадвал).

4.7-жадвал

Handshake протоколида хабар тури

Хабар тури		
Dec	**Hex**	**Тасниф**
0	0x00	HelloRequest
1	0x01	ClientHello
2	0x02	ServerHello
4	0x04	NewSessionTicke
11	0x0b	Certificate
12	0x0c	ServerKeyExchange
13	0x0d	CertificateRequest
14	0x0e	ServerHelloDone
15	0x0f	CertificateVerify
16	0x10	ClientKeyExchange
20	0x14	Finished

*ChangeCipherSpec протокол формати.*Ушбу протокол битта хабардан иборат бўлиб, пакетнинг шифрланганлигини билдиради. TLS протоколи бутун TLS қайд ёзуви маълумотини инкапсуциялайди.

*Alert протоколи.*Handshaking ва application туридаги протокол ўз ишини нормал ҳолатда тугатмаган ҳолда Alert протоколи орқали хабар берилади. Шунга қарамасдан, ушбу хабар ҳар бир турлаги протокол билан биргаликда юборилади. Агар ушбу хабар маълумоти “fatal error” бўлса, у ҳолда сессия зудлик билан ёпилади. Агар хабар маълумоти “warning” бўлса, у ҳолда масофадаги фойдаланувчи талабига кўра сессияни тугатиш ёки тугатмаслик танланади.

Byte +0	Byte +1	Byte +2	Byte +3
21			
Версияси		Узунлиги	
Мажор	Минор	0	2
Даража	Тасниф		

4.3-расм. Alert протоколи формати

*Даража.*Ушбу майдон Alert ни даражасини кўрсатади. Юқорида айтиб ўтилганидек, икки турдаги Alert мавжуд (4.8-жадвал).

4.8-жадвал

Коди	**Даража тури**	**Боғланиш ҳолати**
1	**warning**	Боғланиш ёки хавфсизлик ўзгарувчан бўлиши мумкин.
2	**fatal**	Боғланиш ёки хавфсизлик хавфли бўлиши мумкин, тиклиб бўлмас хатолик юз берган.

Агар жараён нормал ҳолатда ўз ишини тугатган тақдирда ҳам, бирор бир даража тури қайтарилади. Жараённинг қандай тугаганлиги эса тасниф асосида аниқланади. Қуйида тасниф жадвали келтирилган (4.9-жадвал).

4.9-жадвал

Жараён таснифи

Коди	Тасниф	Даража	Коди	Тасниф	Даража
0	Close notify	warning/fatal	49	Access denied	fatal
10	Unexpected message	fatal	50	Decode error	fatal
20	Bad record MAC	fatal	51	Decrypt error	warning/fatal
21	Decryption failed	fatal	60	Export restriction	fatal
22	Record overflow	fatal	70	Protocol version	Fatal
30	Decompression failure	fatal	71	Insufficient security	Fatal
40	Handshake failure	fatal	80	Internal error	Fatal
41	No certificate	warning/fatal	90	User canceled	fatal
42	Bad certificate	warning/fatal	100	No renegotiation	warning
43	Unsupported certificate	warning/fatal	110	Unsupported extension	warning
44	Certificate revoked	warning/fatal	111	Certificate unobtainable	warning
45	Certificate expired	warning/fatal	112	Unrecognized name	warning/fatal
46	Certificate unknown	warning/fatal	113	Bad certificate status response	Fatal
47	Illegal parameter	fatal	114	Bad certificate hash value	Fatal
48	Unknown CA (Certificate authority)	fatal	115	Unknown PSK identity (used in TLS-PSK and TLS-SRP)	Fatal

*ApplicationData протоколи.*Ушбу протокол маълумотни шифрлаб жўнатувчи протокол саналиб, маълумот ва унинг MAC қиймати биргаликда шифрланиб юборилади (4.4-расм).

Byte +0	**Byte +1**	**Byte +2**	**Byte +3**
23			
Версияси		**Узунлиги**	
Мажор	**Минор**	**16 кб гача**	
Маълумот			**MAC қиймати**

4.4-расм. ApplicationData протоколи

Назорат саволлари

1. X.509 сертификати.
2. SSL протоколи тарихи.
3. SSL протоколида хавфсизлик усуллари.
4. SSL протоколида ўртага турган одам таҳдиди.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. https://ru.wikipedia.org/wiki/SSL

5– амалий машғулот. Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Ишнинг мақсади: Симсиз тармоқ протоколларида ахборот хавфсизлигини таъминлаш.

Масаланинг қўйилиши: Локал симсиз тармоқларда (WI-FI роутер) хавфсизлик созланмаларини амалга оширилсин.

Ишни бажариш учун намуна

Симсиз тармоқлар одамларга симли уланишсиз ўзаро боғланишларига имкон беради. Бу силжиш эркинлигини ва уй, шахар қисмларидаги ёки дунёнинг олис бурчакларидаги иловалардан фойдаланиш имконини таъминлайди. Симсиз тармоқлар одамларга ўзларига қулай ва хохлаган жойларида электрон почтани олишларига ёки Web-сахифаларни кўздан кечиришларига имкон беради.

Симсиз тармоқларнинг турли хиллари мавжуд, аммо уларнинг энг мухим хусусияти боғланишнинг компьютер қурилмалари орасида амалга оширилишидир. Компьютер қурилмаларига шахсий рақамли ёрдамчилар (Personal digital assistance, PDA), ноутбуклар, шахсий компьютерлар, серверлар ва принтерлар тааллуқли. Одатда уяли телефонларни компьютер қурилмалари қаторига киритишмайди, аммо энг янги телефонлар ва хатто наушниклар маълум хисоблаш имкониятларига ва тармоқ адаптерларига эга. Яқин орада электрон қурилмаларнинг аксарияти симсиз тармоқларга уланиш имкониятини таъминлайди.

Боғланиш таъминланадиган физик худуд ўлчамларига боғлиқ холда симсиз тармоқларнинг қуйидаги категориялари фарқланади:

- симсиз шахсий тармоқ (Wireless personal-area network, PAN);
- симсиз локал тармоқ (Wireless local-area network, LAN);
- симсиз регионал тармоқ (Wireless metropolitan-area network, MAN):
- симсиз глобал тармоқ (Wireless Wide-area network, WAN).

5.1-жадвал

Симсиз тармоқ усуллари

Тармоқ тури	**Таъсир доираси**	**Амалда фойдала нилиши**	**Мавжуд стандартлар**	**Қўлланиш соҳаси**
Шахсий симсиз тармоқлар	Фойдаланувчидан бевосита яқинликда	Ўртача	Bluetooth,IEEE 802.15,IRDA	Ташқи қурилмалар кабеллари нинг ўрнида
Локал симсиз тармоқлар	Бинолар ёки офислар орасида	Юқори	IEEE 802.11, Wi-Fi ва HiperLAN	Симли тармоқларни мобил кенгайти риш
Регионал симсиз тармоқлар	Шаҳарлар орасида	Юқори	IEEE 802.16, ва WIMAX	Бинолар ва корхоналар ва Internet орасида белгиланган симсиз боғланиш
Глобал симсиз тармоқлар	Бутун дунё бўйича	Паст	CDPD, 2G, 2.5G, 3G, 4G	Бутун дунё бўйича интернетдан фойдаланишда

WI-FI технологиясида фойдаланилган криптографик протоколлар

Симсиз локал тармоқларда фойдланилган WI-FIтехнологиясида қуйидаги криптографик протоколлардан фойдаланилган:

– Wired Equivalent Privacy (WEP);
– Wi-Fi Protected Access (WPA) ва унинг иккинчи варианти.

Wired Equivalent Privacy (WEP) хавфсизлик алгоритми IEEE 802.11 симсиз тармоқлари учун фойдаланилиб, IEEE 802.11 стандарти 1999 йил сентябр ойидақабуд қилинган бўлиб, симсиз тармоқларда (wireless LAN) маълумотни бутунлигини, аутентификация ва тўлиқлигини таъминлашда фойдаланилади.

Ушбу протоколдп 10 ёки 26 та ўн олтилик тизимдаги калитдан фойдаланилади, ва бу калит дастлаб роутерни созлашда фойдалинилган парол билан бир хил бўлади.

Ушбу протоколда қуйидаги хавфсизлик амалиётларидан фойдаланилган:

– Аутентификациялаш;

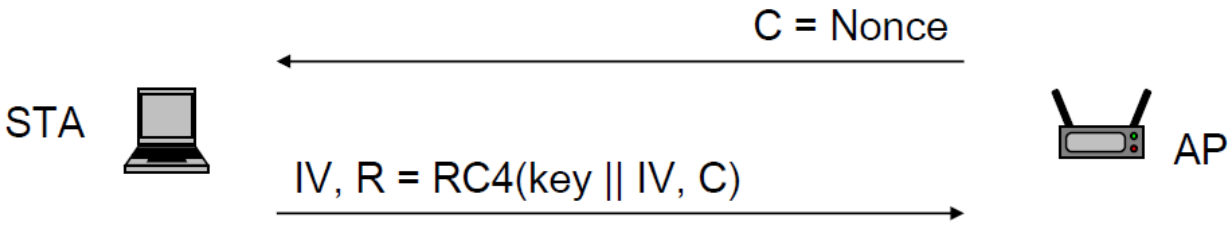
– Маълумотни бутунлигини таъминлаш;
– Маълумот махфийлагини таъминлаш.

*WEP да аутентификациялаш.*Ушбу протоколда икки турдаги аутентификациялашдан фойдаланилади.

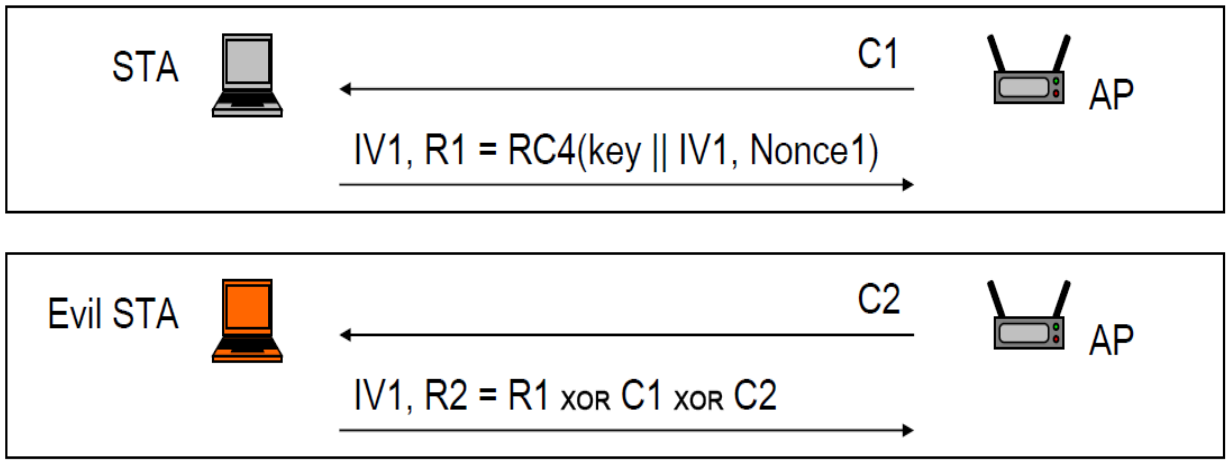
– Open System authentication;
– Shared Key authentication.

Биринчи усулда аутентификациялаш амалга оширилмай ихтиёрий фойдаланувчи серверга боғланиши мумкин. Маълумот WEP калити асосида шифрланади. Фойдаланувчи серверга боғланаши учун клиент тўғри калитга эга бўлиши керак.

Shared Key асосида аутентификациялаш усули 5.1 - расмда келтирилган бўлиб, 5.2 – расмда ушбу аутентификацияни синдириш усули келтирилган.[1]



5.1 – расм. Shared Key аутентификациялаш усули



5.2 – расм. Shared Key аутентификация усулини синдириш

R2=R1 XOR C1 XOR C2 = (keystream(key || IV1) XOR C1) XOR C1 XOR C2 = keystream(key || IV1) XOR (C1 XOR C1) XOR C2 = keystream(key || IV1) XOR C2 = қониқарли жавоб.

*Маълумот махфийлагини таъминлаш***.**WEP протоколи икки хил узунликдаги калитлардан фойдаланганлиги сабабли, улар мос ҳолда WEP-40 WEP-104 деб аталади. WEP-40вариантида 40 битли (10 та ўн олтилик белги)

[1] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures.

калитдан фойдаланиб, 24 битли бошланғич вектордан (IV) фойдаланилади. WEP-104вариантида 104 битли (26 та ўн олтилик белги) калитдан фойдаланиб, 24 битли бошланғич вектордан фойдаланилади. Шифрлаш RC4 алгоритми асосида амалга оширилади (5.3-расм).

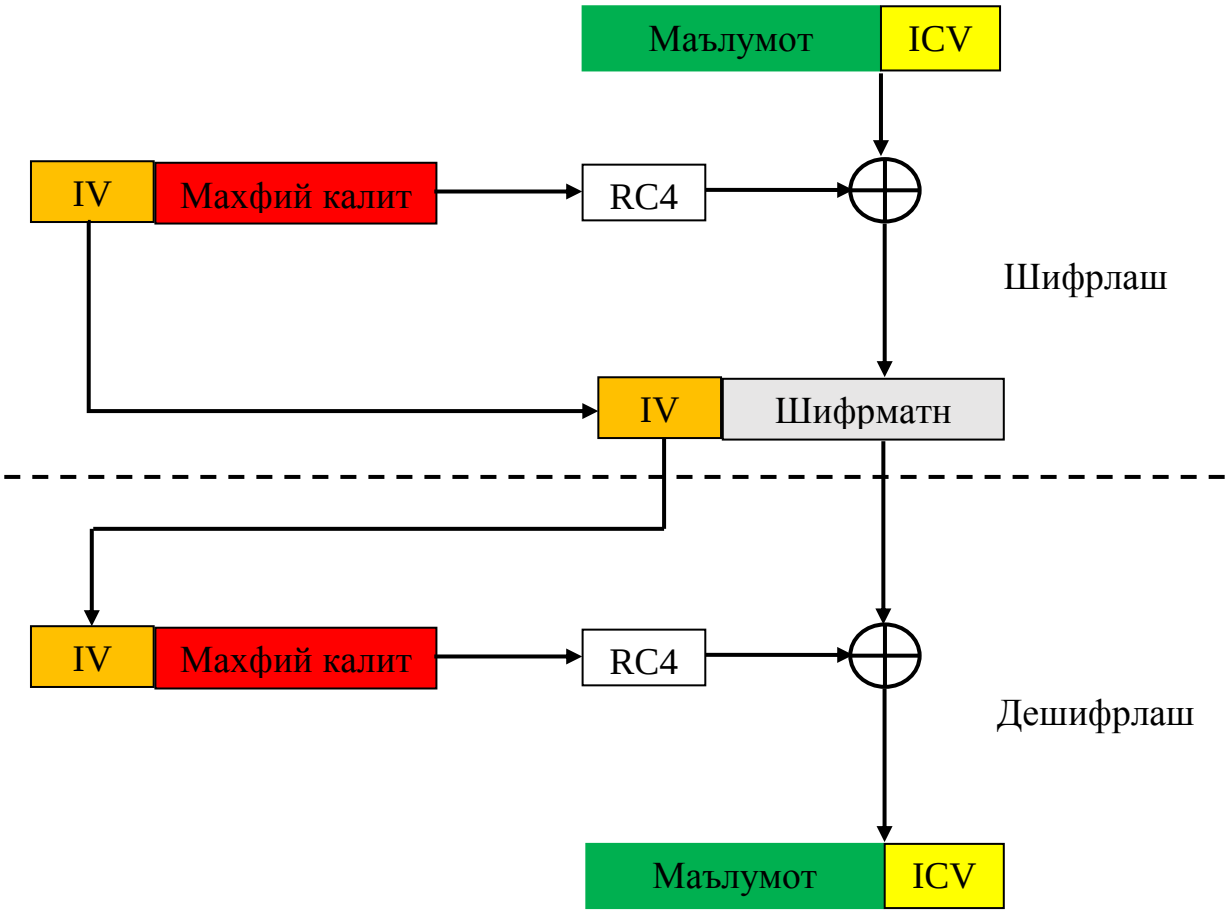
Иккинчи усулда WEP протоколида аутентификациялаш учун оддий савол-жавоб тизимидан фойдаланилган. Жараён кетма-кетлиги қуйидагича:

1. Клиент серверга (бошқарув нуқтасига) аутентификациялаш сўровини юборади.
2. Сервер фойдаланувчига тасодифий сонни юборади(r, 128 битдан катта бўлган) .
3. Фойдаланувчи ушбу сонни умумий калит (бошқарув нуқтаси пароли) билан шифрлаб юборади ($e_K(r)$).
4. Шифрматнни очиш натижасига қараб, аутентификациялашдан ўтилади ёки йўқ.

*Маълумотни бутунлигини таъминлаш.*WEP протоколида маълумот бутунлигини таъминлашда CRC-32 функциясидан фойдаланилади.

WEP протокол заифликлари. Ушбу протокол амалда фойдалниш даражаси пасайишига қуйидаги заифликлари орқали келиб чиққан ҳужумлар сабабчи бўлган.[1]

[1] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures.



5.3-расм. WEP протоколида шифрлаш

Бу ерда: IV – бошланғич вектор, ICV – маълумотнинг CRC қиймати.

1. Сервер (бошқарув нуқтасига) фойдаланувчини аутентификацияламайди.
2. Шифрлашда ва аутентификациялашда битта калитдан фойдаланилади.
3. Аутентификациялаш давомида сессия калитидан фойдаланилмайди.
4. Протокол хабарни такрорлаш ҳужумидан ҳимояланмаган.
5. Фойдаланилган IVқайта фойдаланилади ва қиймати жуду ҳам кичик:
6. 24 бит узунлик, 16.777.216 мумкин бўлган калитлар.
7. Қарийиб 17 миллион хабардан сўнг IVтакрорланади.
8. Аган тизим 11 Mbps тезликдан фойдаланса, секундига 700 та пакет юборади ва бир IV қиймати қарийиб 7 соат учун етарли бўлади.
9. Одатда барча курилмаларда IVнолдан бошланади.
10. Баъзи заиф калитлардан фойдаланиш орқали RC4 тасодифий саналмаган калитларни ишлаб чиқаради.
11. Юқоридаги сабабга кўра, амалда RC4 орқали ҳосил қилинган калитнинг дастлабки 256 байти олинмайди. Аммо WEP бундай эмас.

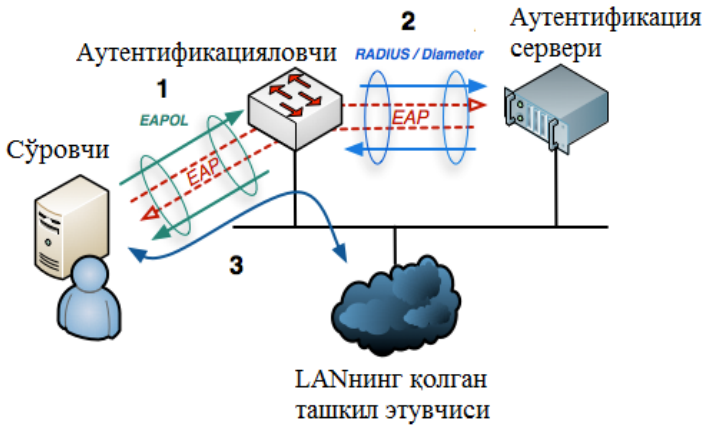
Юқорида келтирилган сабабларга кўра, амалда WEP протоколидан фойдаланиш тавсия этилмайди.

WPA протоколи. 2003 йилда Wi-Fi AllianceWEP протоколи Wi-Fi Protected Access (WPA) билан алмаштирлганин элъон қилди. 2004 йилда WPA ва WPA2 протоколини ўз ичига олган 802.11i стандарти ишлаб чиқилди. Ушбу ишлаб чиқилган протоколлар WEP протоколига қараганда хавфсиздир. Қурилмалар ушбу протоколлардан фойдаланиш учун уларни аппарат томондан янгилаш шарт.

WPA протоколи WEP протоколида мавжуд заифликларни бартараф этиш учун ишлаб чиқилган бўлиб, унда Temporal Key Integrity Protocol (TKIP) протоколидан фойдаланилади. WEP протоколида 40 битли ёки 104 битли калитлардан фойдаланилган бўлса, WPA протоколида ҳар бир пакет учун алоҳида ҳосил қилинган калитлардан фойдаланилади. WEP протоколи заиф деб топилгандан сўнг, вақтинчалик қурилмаларни янгилашга қадар фойдаланиш учун бардошли протокол керак эди. TKIPпротоколи WEPпротоколи асосида қурилган бўлиб, WEP протоколи қурилмалари учун мосдир.

Маълумотни бутунлигини таъминлаш алгоритмлари сифатида фойдаланилган CRC тизимлари ўрнига эса “Michael” деб номланувчи маълумотни бутунлигини текуширувчи алгоритмдан фойдаланилган. MAC тизимлари юқоридаги икки тизимларга қараганда бардошли саналсада, қурилмалардан юқори имкониятларни талаб этади. “Michael” тизими MAC қараганда тезкор ва CRC мавжуд камчиликларни ўзида бартараф этган.

Аутентификациялаш. WPAпротоколида 802.1X аутентификациялаш моделидан фойдаланилади.



5.4-расм. 802.1X аутентификациялаш модели

*Маълумот махфийлиги.*TKIP протоколида шифрлаш алгоритми сифатида RC4 оқимли шифрлаш алгоритмидан фойдаланилган. TKIP протоколида фойдаланилган калитлар мажмуаси қуйидагилар.

5.2-жадвал

WPA проктоколида фойдаланилган калитлар

Фойдаланувчи аутентификацияланади.
Аутентификация сервери “Masterkey” ни ҳосил қилади.
“Master key” билан “Key Encryption Keys”лар шифрланади.
“Key Encryption Keys” билан “Temporal key”шифрланади.
“Temporal key” фойдаланувчи маълумотини шифрлашда ишлатилади.

“Temporal key” калитлар тўплами икки калитдан, улар 128-битли шифрлаш калити ва 64-битли Michael функцияси калитидан иборат.

Маълумотни шифрлашда RC4 оқимли шифрлаш алгоритмидан фойдаланилган бўлиб, WEP протоколидан фарқли равишда ҳар бир пакет учун алоҳида такрорланмас калитлардан фойдаланади.

WPA2 протоколи IEEE 802.11i-2004 ёки 802.11i стандартида асосида ишлаб чиқилган ва WEP, WPA (TKIP) протоколидан тамоман фарқ қилади. Ушбу протокол ишлаши учун янгидан ишлаб чиқилган қурилма асосида ишлайди. Ушбу протоколнинг тўлиқ номи CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) деб номалиниб, унда блокли шифрлаш алгоритми саналган AES-128 шифрлаш алгоритмидан фойдаланилади.

Ушбу протоколнинг TKIP протоколидан асосий фарқи, 48-битли PN (Packet Number) майдони фойдаланилган бўлиб, унинг асосий мақсади ҳар бир пакет учун алоҳида ҳисобланиб, пакетни қайта юбориш ҳужумига қарши фойдаланилади.

5.3-жадвал

WI-FI симсиз алоқа тармоқлари усуллари таҳлили

Хусусият	**Статик WEP**	**Динамик WEP**	**WPA**	**WPA 2**
Идентификациялаш	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер	Фойдаланувчи, компьютер
Аутентификациялаш	Умумий калит	EAP	EAP ёки умумий калит	EAP ёки умумий калит
Бутунлик	CRC-32	CRC-32	64-битли MIC	CBC режими асосида MIC
Махфийлик	Статик калит	Сессия калити	TKIP асосида калит	CCMP (AES)
Калитларни тақсимлаш	Бир томонлама	Pair-wise Master Key (PMK)	PMK	PMK
Бошланғич вектор	24-бит	24-бит	56-бит	48-бит (PN)
Алгоритм	RC4	RC4	RC4	AES
Калит узунлиги	64/128	64/128	128	128, 192, 256
Талаб этиладиган структура	Йўқ	RADIUS	RADIUS	RADIUS

Назорат саволлари

1. Симсиз тармоқ турлари.
2. WEP протоколи ва унда мавжуд заифликлар.
3. WI – FI стандартида хавфсизлик созланмаларини ўрнатиш.
4. WEP протоколида фойдаланилган криптографик алгоритмлар.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.
3. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures. School of Multimedia, Hannam University, Daejeon, Korea. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.
4. http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

6 – амалий машғулот. Содда аутентификациялаш протоколлари. Симметрик ва ассиметрик шифрлашга асосланган протоколлар. SSH протоколи.

Ишдан мақсад: Зараркунанда дастурий воситаларнинг таҳлилини амалга ошириш.

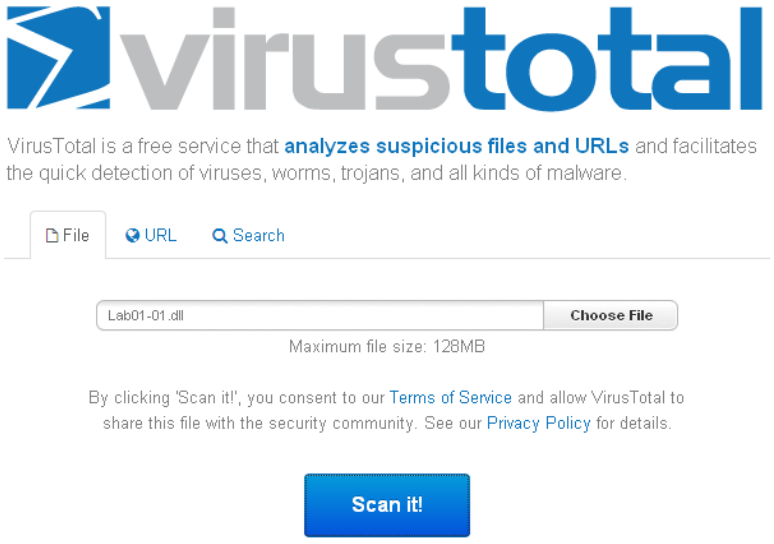
Масаланинг қўйилиши: Берилган зараркунанда дастурларни таҳлиллаш воситалари асосида таҳлил этинг.

Ишни бажариш учун намуна

Зараркунанда дастурий воситаларни таҳлил этганда одатда статик ва динамик таҳлиллаш усулларидан кенг фойдаланилади.

Ҳар бир таҳлиллаш ўз навбатида содда ва мураккаб таҳлиллашларга бўлинади.

Содда статик таҳлил воситалари. Амалда ЗД статистик таҳлил ўтказишда улар бир нечта антивирус воситалари ёрдамида текширилади ва улардан олинган натижалар таҳлил этилади. Ушбу вазифани бажаришда http://www.virustotal.com/ онлайн ЗД таҳлили воситаси кенг фойдаланилади. Ушбу онлайн таҳлиллаш воситаси нафақат ЗД бир нечта антивирус воситалари ёрдамида тестлайди, балки уларнинг дастурий томондан тузулишини ва улар ҳақида қўшимча маълумотларни беради (6.1 -расм).[1]



6.1 -расм. **http://www.VirusTotal.com/**ойнаси

ЗД лардан "қаторларни (strings)" аниқлаш. Ҳар бир дастурий восита яратилишида маълум кетма-кетмаликлан иборат бўлган матн шаклидаги маълумотлардан фойдаланилади. Масалан, "GDI32.DLL", "99.124.22.1", "Mail system DLL is invalid.!Send Mail failed to send message" ва ҳак. Албатта, яратилган дастурий воситалар якунида улар .exe, .dll файл шаклларида

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 10 – с.

ассембланади. Бошқа сўз билан айтганда, бу кенгайтмадаги файллар ўн олтилик (hex)саноқ системасида ифодаланади (0x42, 0x41, 0x44→ BAD).Белгиларни 16 лик саноқ тизимига ўтказишда одатда ASCII (8-бит)ва Unicode (16-бит)кодлаш стандартларидан фойдаланилади. Ушбу стандартларда ҳар бир келган белгилар кетма-кетлиги охири 0x00 билан тугайди. Бунинг маноси эса сўзнинг тугуганлигини англатади.

Ҳозирда ассемрланган файллардан қаторларни топишда “strings” дастуридан (https://technet.microsoft.com/en-us/sysinternals/bb897439) кенг фойдаланилади. Қуйида ассемрланган файллардан топилган қаторлар келтирилган.

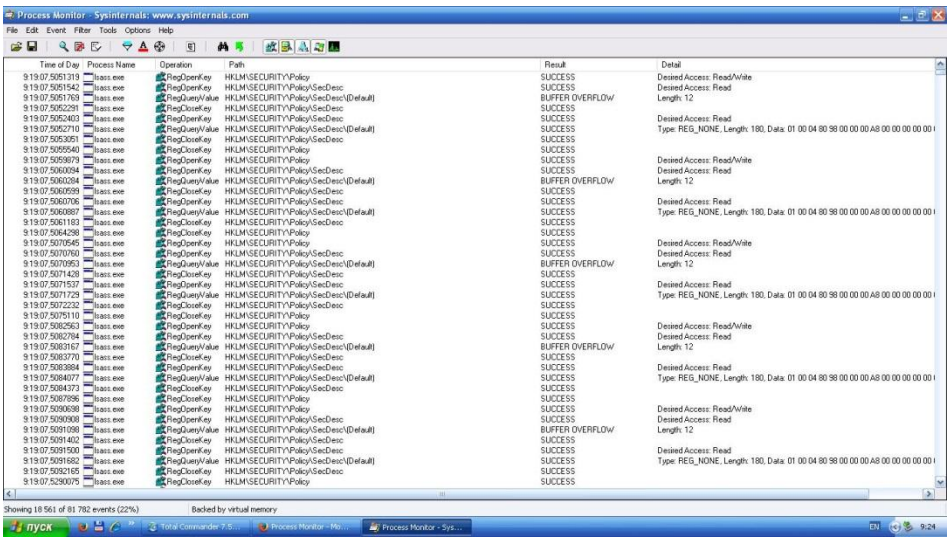
```
C:>strings bp6.ex_
VP3
VW3
t$@
D$4
99.124.22.1 ❹
e-@
GetLayout ❶
GDI32.DLL ❸
SetLayout ❷
M}C
Mail system DLL is invalid.!Send Mail failed to send message. ❺
```

6.2-расм. Strings дастурида таҳлиллаш

Содда динамик таҳлил воситалари. Process Monitor (PM) дастури Windows ОТ учун мўлжалланган, кенгайтирилган кузатиш воситаси бўлиб, мавжуд регисторларни, файл тизимларини, тармоқ, жараён ва ҳаракат оқимларини (thread activity)кузатиш имкониятини беради.[1]

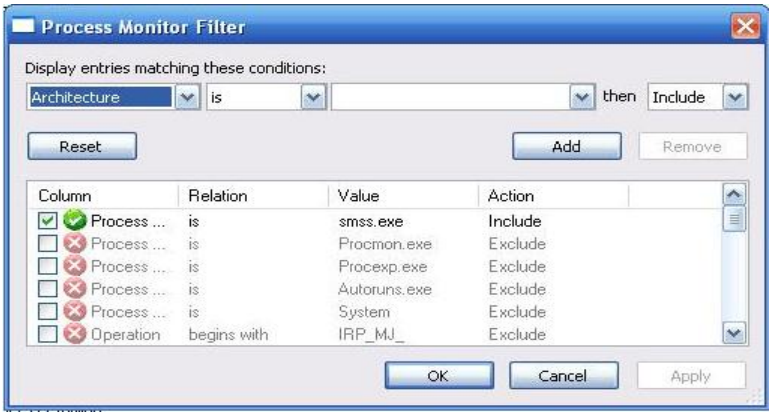
Бу дастурий восита орқали ҳодисалар кетма-кетлигини, вақтини, жараёнлар номини, жараён амалга ошираётган амални, ҳодиса юз берган манзилни ва ҳодиса натижасини билиш мумкин.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 43 – с.



6.3-расм. ProcMon дастури кўриниши

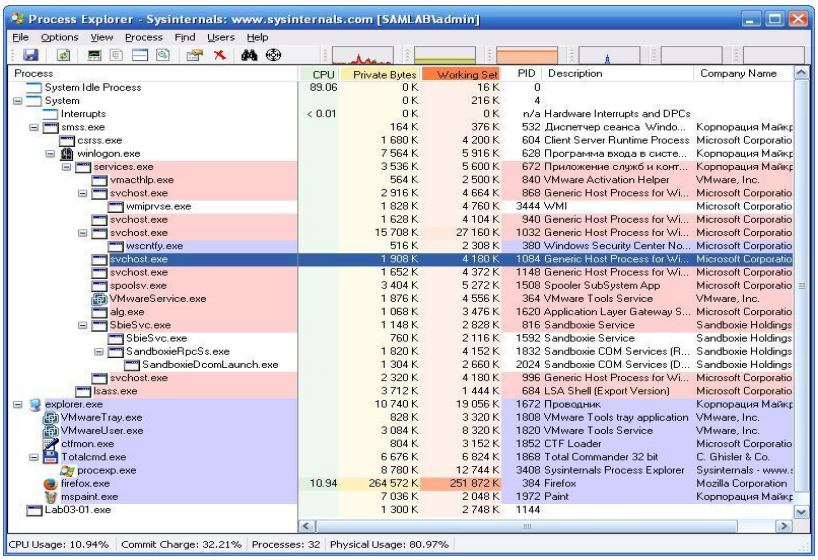
Ушбу дастурдан фойдаланган ҳолда барча жараёнларни кузатиш мураккаб, яъни ҳодисалар жуда ҳам кўп ва улар ичидан кераклисини аниқлаш мушкул. Керакли маълумотларни ажратиб олиш учун уларни филтерлаш амалга оширилади. Бу амални Process Monitor дастурида амалга ошириш учун *“Filter→Filter”* бандига ўтилади.



6.4-расм. Фильтр менюси

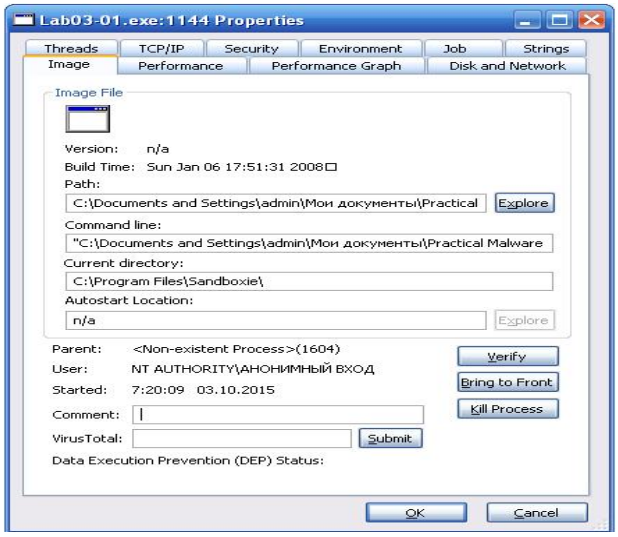
Process Explorer ёрдамида жараёнларни кузатиш. Ушбу дастурий восита Windows томонидан ишлаб чиқилган бўлиб, динамик таҳлиллашда кенг қўлланилади. Бу дастурий восита орқали актив жараёнлар рўйхатини, жараёнлар орқали юкланган DLL файллар рўйхатини, жараёнларнинг хусусиятларини ва тизим ҳақида умумий маълумотларни олиш мумкин. Бундан ташқари жараёнларни тугатиш, юклаш каби амалларни бажариш мумкин. Дастур ойнасида жараёнлар шажара шаклида берилади. Ойнада 7 устун бўлиб, Process устида жараён номи, PID устида жараён идентификация номери, CPU устида фойдаланиш кўрсаткичи, Description, Company name, Working set, Private bytes устунларидан иборат. Одатий ҳолда дастур ойнасида хизматлар пушти рангда, жараёнлар кўк рангда, янги жараёнлар

яшил рангда, тугатилган жараёнлар қизил рангда тасвирланади.Яшил ва қизил ранглар вақтинчалик саналади. ЗД таҳлиллашда бу дастур орқали янги жараённи ҳосил бўлиши ўзгараши орқали билиш мумкин.[1]



6.5-расм. Process Explorer дастурий воситаси кўриниши

Танланган жараённинг устида сичқонча тугмасини икки марта босиш орқали жараён ҳақида тўлиқ маълумотга эга бўлиш мумкин.



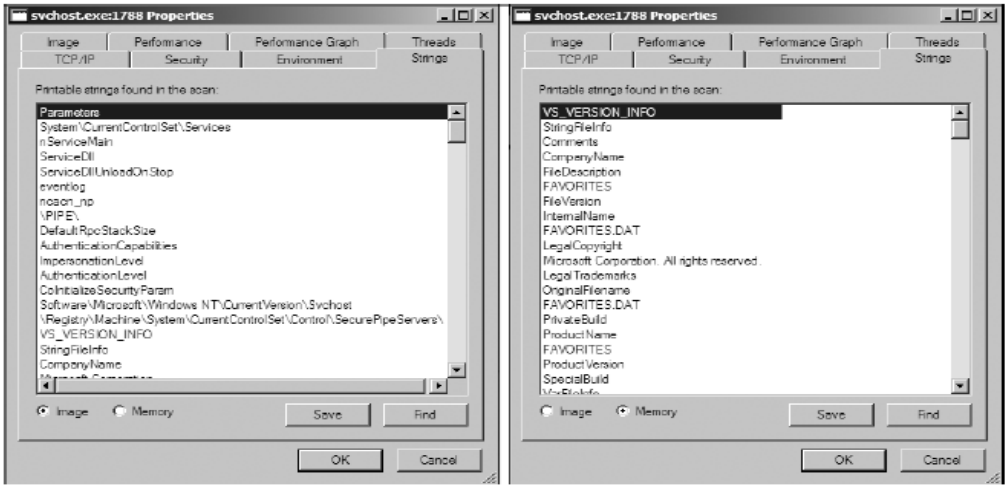
6.6-расм. Process Explorer дастурий воситаси хусусиятлар ойнаси

*Verify (текшириш) танлови.*Process Explorer дастурининг муҳим хусусиятларини бири бу – *текшириш* танлови бўлиб, бу орқали жараённи ҳақиқий ёки алмаштирилган эканлигини аниқлаш мумкин. Бунинг учун дастурнинг*Image* бандидан *Verify* тугмасини босиш талаб эталади. ЗД одатда ўзларини бошқа жараён кўринишида кўрсатишга ҳаракат қиладилар. Дастурнинг бу имконияти эса бу ўзгаришни аниқлаш имконини беради.

Қаторларни солиштириш. Process Explorer дастурининг яни бир муҳим

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 47 – c.

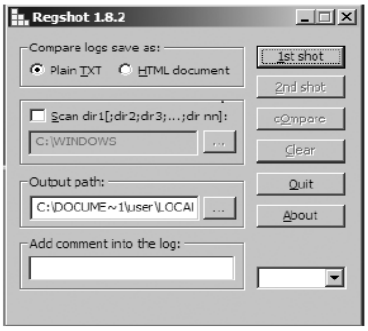
хусусиятларидан бири бу – жараёнларни ўзгартирилишини аниқлашдир. Одатда кўплаб ЗД лар ўзини бошқа жараён орқасига яширади. Жараённинг дискдага шакли ва унинг хотирага юкланган шакли орасида фарқ юзага келади. ЗД дискдаги шаклини эмас, хотирадаги қийматини ўзгартиради, яъни, ўзини функцияларини жойлаштиради.



6.7-расм. Қаторларни солиштириш

Regshot дастури орқали регистор ҳолати ўзгаришини аниқлаш. Бу дастурий восита регисторнинг икки ҳолатини бир-бири билан солиштириш учун фойдаланилади.[1]

Дастурдан фойдаланиш учун дастлаб регисторларнинг жорий ҳолати олинади (*1st shot*тугмасини босиш орқали). Шундан сўнг ЗД юкланади ва ОТ маълум ўзгаришлар бўлиши кузатилади ва дастур бу ўзгаришларни ёзиб олиши учун *2nd shot*тугмаси босилади. Шундан сўнг олинган икки ҳолат *compare*тугмасини босиш орқали солиштирилади (6.8-расм).

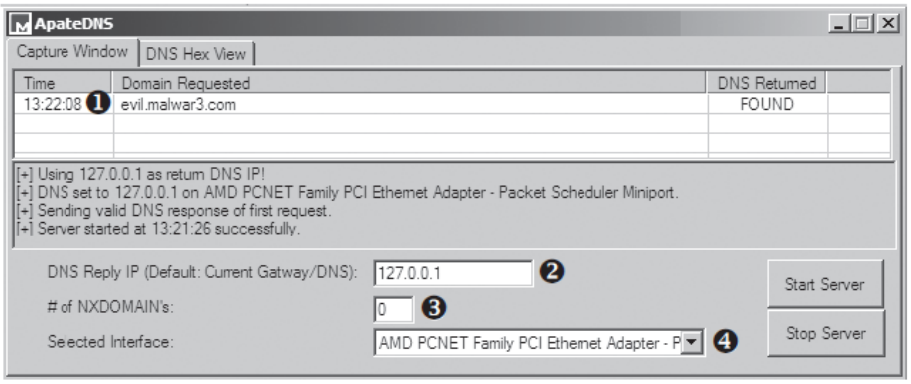


6.8-расм. Regshot дастури

Қалбаки тармоқ. Баъзи ЗД ларни тармоқда қайерда улунишини аниқлашда қалбаки тармоқлардан кенг фойдаланилади, яъни, ЗД ҳақиқий тармоқда уланиш ўрнига қалбаки яратилган тармоққа уланади. Бунинг натижасида ЗДнинг тармоқдаги фаолиятини кузатиш имконияти яратилади.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 57 – с.

*ApateDNS дастури.*Ушбу дастурий восита орқали ЗД лар томонидан берилган DNSсўровларни кузатиш имкони мавжуд (6.9-расм). [1]



6.9-расм. ApateDNS дастури кўриниши

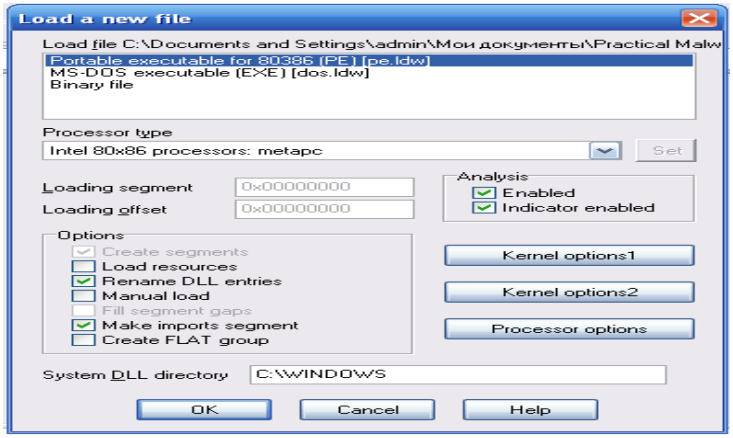
Бу дастурий восита фойдаланувчи ШКнинг IP манзили ва 53 порти орқали кузатувни амалга ошириб, қабул қилинган DNS сўровга жавоб қайтаради ва қабул қилинган сўровни фойдаланувчига ўн олтилик саноқ тизимида ва ASCII стандартида намойиш этади.

Бу дастурий воситадан фойдаланиш учун, расмда кўрсатилган 2 бандда, DNS сўровни қабул қилувчи манзилни кўрсатиш, 4 бандда мос тармоқ интерфейсини танлаш ва шундан сўнг серверни юклаш тугмасини босиш талаб этилади. Шундан сўнг ЗД томонидан юборилган DNS сўровга жавоб фойдаланувчига намойиш этилади.

Мураккаб статик таҳлил воситалари. Буни амалга оширишда IDA Pro дастуридан фойдаланилади. Бу дастурий восита орқали Portable Executable (PE), Common Object File Format (COFF),Executable and Linking Format (ELF) туридаги файлларни дизассемблаш мумкин.

IDA Pro дастурида ЗД ларни юклаш.Ушбу дастурий воситада таҳлилланувчи дастурни юклаш учун жихозлар панелидан “Load a new file or database” бандини танланади ва қуйидаги ойна ҳосил бўлади. Бунда IDAProдастури юкланган дастурни форматини ва процессор архитектурасини кўрсатади.[2]

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 51 – с.
[2] Michael Sikorski, Andrew Honig. Practical malware analysis. 88 – с.



6.10 – расм.

Ушбу дастурий восита икки муҳитга, график ва текст муҳитига эга. Ушбу дастурнинг график муҳитида таҳлилланувчи дастурий восита блок схема ва ранглар асосида тасвирланади. Текс муҳитида эса хотира манзили ва унда жойлашган ассемблер код тасвирланади.

График муҳитда кодлар олдида манзилни чиқариш учун “Option→General→” бандига ўтилади ва “Line Prefix” белгиланади.

IDA Pro дастури муҳитида қуйидаги ойналар мавжуд:

1. ***Functions window.*** Фойдаланилган функциялар рўйхатини ўз ичига олади. Бу ойнада (F, L, S, ва ҳак) устунлар мавжуд бўлиб, *L* кўрсаткичи кутубхона функцияси эканлигини билдиради.
2. ***Names window.*** Ҳар манзилни номлар билан аталади, функциялар, қаторлар, код номлари, маълумот номлари.
3. ***Strings window.*** Барча қаторларни кўрсатади.
4. ***Imports window.*** Файл учун импорт қилинган кутубхоналар рўйхати.
5. ***Exports window.*** Файл учун экспорт қилинган кутубхоналар рўйхати. Ушбу ойна DLL функцияларни таҳлил қилишда жуда муҳимдир.
6. ***Structures window.*** Барча мавжуд маълумот структураларини рўйхати.

Ушбу дастурда маълум ишларни бажарганда турли ўзгаришлар юзага келади. Дастлабки ҳолда қайтиш учун эса “Windows→Reset Desktop” банди танланади.

Қуйидаги ассемблер кодда боғланишлар келтирилган бўлиб, уларнинг асосий учта тири бор:

– *Sub links.* Улар функциялар, printf ва sub_4010A0 га ўхшаш, юклаш учун ишлатилади;

– *Loc links.*Сакраш керак бўлган функцияларни, loc_40107E ва loc_401097 га ўхшаш, юклаш учун фойдаланилади;

– *Offset links.* Хотирага қўйилиши керак бўлган боғланишлар.

```
00401075        jnz     short ❶loc_40107E
00401077        mov     [ebp+var_10], 1
0040107E loc_40107E:                    ; CODE XREF: ❶❷sub_401040+35j
0040107E        cmp     [ebp+var_C], 0
00401082        jnz     short ❶loc_401097
00401084        mov     eax, [ebp+var_4]
00401087        mov     [esp+18h+var_14], eax
0040108B        mov     [esp+18h+var_18], offset ❶aPrintNumberD ; "Print Number= %d\n"
00401092        call    ❶printf
00401097        call    ❶sub_4010A0
```

6.11-расм.

Юқоридаги 6.11-расмда 1 нуқталарда сичқонча тугмаси икки марта босилса, унда керакли манизилга ўтилади. 2 нуқтада *Cross-references* кўрсатилган бўлиб, улар кўрсатилган0x401075 манзилга ўтиш кераклигини билдиради.

Манзилга сакраш. Вертуал хотира манзилига сакраш учун оддий G тугмаси босилади ва керакли бўлган манзил ёки sub_401730 ёки printf ҳолатда киритилади. Бундан ташқари кенгайтирилган ҳолда *Jump→Jump to File Offset* банди танланиши мумкин.

Дастурнинг *Search* ойнаси орқали керакли кодни, текстни, байтлар кетма-кетлигини қидириш мумкин.

Cross-references *лардан* фойдаланиш. Ушбу катталиклар IDA Pro дастурида *xref* номи билан таниқли бўлиб, қайси қатор ёки функция фойдаланилаётганлигини кўрсатади. Агар қайсидир функция ҳақида маълумот керак бўлса, Cross-references дан фойдаланган ҳолда буни соддалик билан амалга ошириш мумкин.

*Код Cross-references.*Қуйидаги кодда Код Cross-references тасвирланган бўлиб, 1 қисмда sub_401000 функция main функциясида 0x3 манзилида чақирилмоқда. 2 ҳолатдаги Cross-referencesда эса кўрсатилган манзилга ўтиш айтилган (6.12-расм).

```
00401000        sub_401000      proc near       ; ❶CODE XREF: _main+3p
00401000        push    ebp
00401001        mov     ebp, esp
00401003    loc_401003:                         ; ❷CODE XREF: sub_401000+19j
00401003        mov     eax, 1
```

6.12-расм

Берилган ассемблер кодида бирор бир функцияни неча маратоба чақирилганлигини аниқлаш учун, функция номи устида X тугмаси босилади.

Ушбу дастурий восита орқали функцияларда иштирок этган ўзгарувчилар ва параметрларни аниқлаш имконияти мавжуд. Локал ўзгарувчилар var_ олд қўшимчаси билан берилади. Параметрлар эса arg_ олд

қўшимчаси билан берилади.

IDA Pro дастури ассемблер кодларда фойдаланилган 16 олтилик саноқ тизимидаги катталикларни турли саноқ тизимларида ифодалаш имконига эга. Бунинг учун ассемблер коддан 16 тизимидаги қийматни топинг ва унинг устига сичқончани ўнг тугмасини босинг. Ҳосил бўлган ойнадан сиз қийматни турли саноқ тизимларидаги кўринишини кўришингиз мумкин. Бу имконият маълум қаторларни ва катталикларни аниқлашда кенг фойдаланилади.

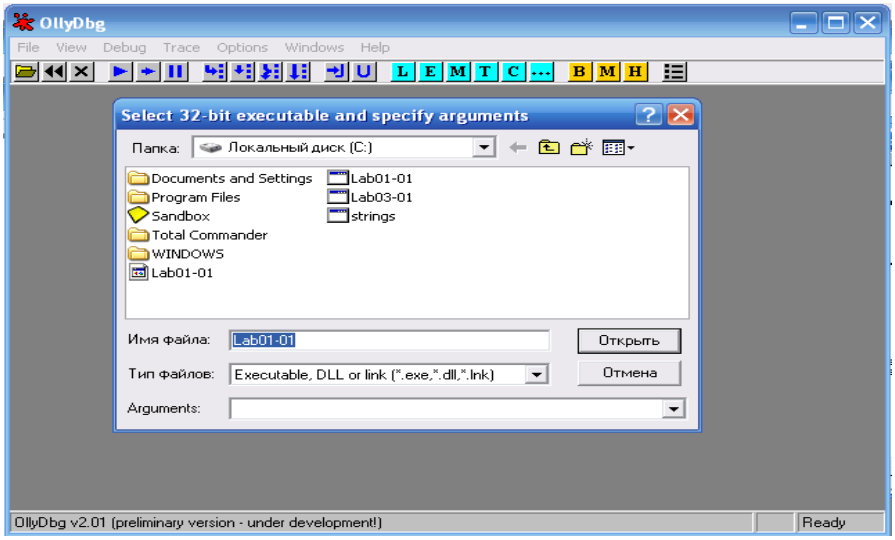
Ушбу дастурий воситада кодлар турлича рангларда ифодаланади:

– оч кўк рангда кутубхона кодлари ифодаланади;
– қизил рангда компилятор ҳосил қилган кодлар ифодаланади;
– тўқ кўк рангда фойдаланувчи ёзган кодлар ифодаланади.

Бундан келиб чиқадаки ЗД таҳлил этганда тўқ кўк рангдаги кодларга кўпроқ этибор қаратиш керак бўлади.

Мураккаб динамик таҳлил. Мураккаб динамик таҳлил OllDbgv2.01 debugger дастурида амалга оширилади. Ушбу дастур x86 архитектурасидаги debuggerлаш учун фойдаланилиб, бу дастурда ЗД юклаш ёки ШК хотирасида юкланган ЗД ни debug қилиш мумкин. Ушбу дастурий восита ЗДларнинг динамик таҳлилида кенг фойдаланилади. Ушбу дастур ЗД таҳлиллаш учун ишлатишга қадар, дастурларни бузиш учун (крек қилиш) фойдаланилган.[1]

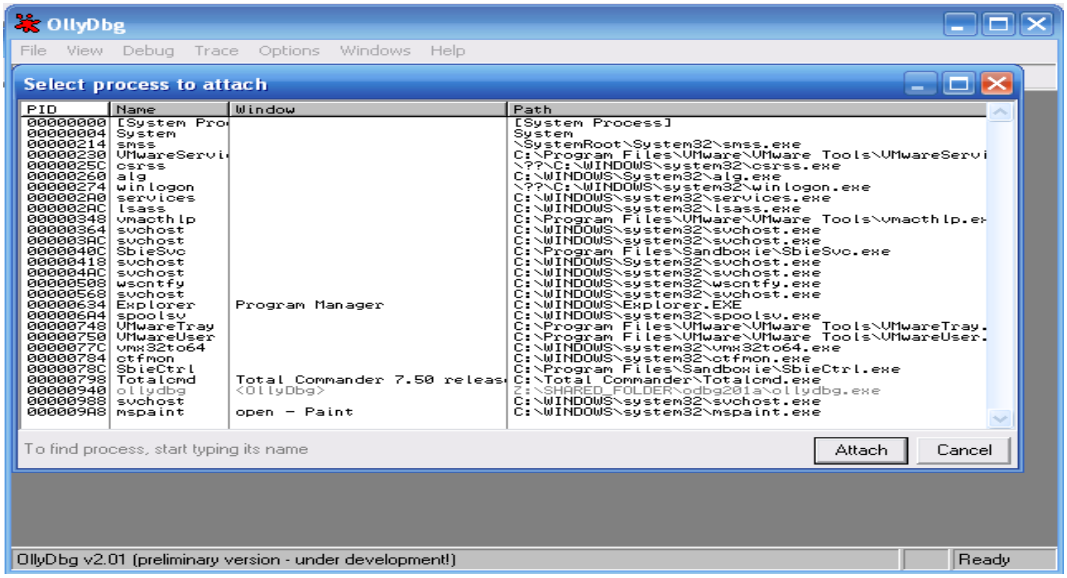
ЗД юклаш. Ушбу дастурда ЗД икки усулда юклаш мумкин. Биринчиси ЗД ни файлдан юклаш ва иккинчиси компьютер хотирасида юкланган ЗД тутиб олиш орқали debug қилади.



6.13 – расм. Янги ЗД юклаш (File→Open)

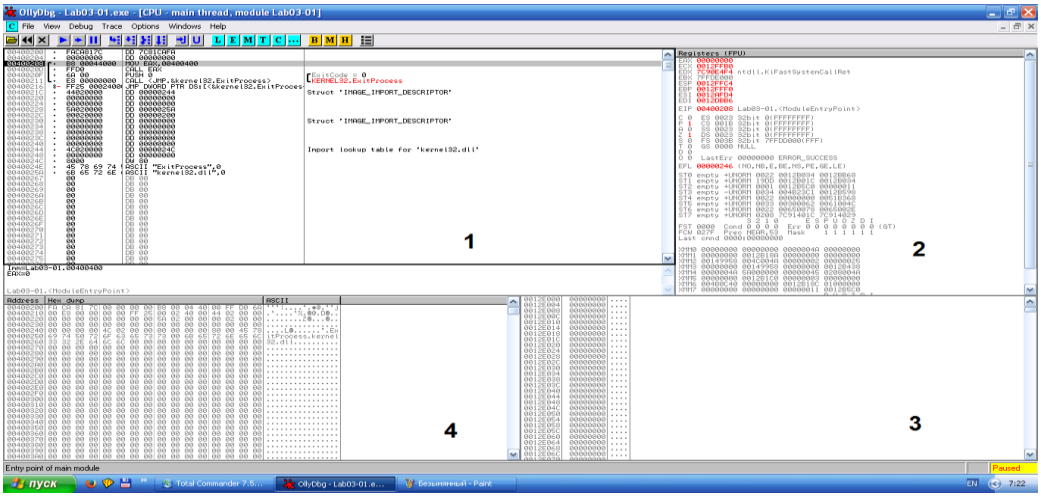
Изоҳ: arguments банди орқали ЗД қатор орқали кирувчи аргументларни киритиш мумкин.

[1] Michael Sikorski, Andrew Honig. Practical malware analysis. 180 – с.



6.14 – расм. Жараёнда юкланган ЗД тутиш (File→Attach)

Ушбу дастурий воситанинг интерфейси қуйидаги ойналардан иборат:



6.15 – расм. OllyDbg дастури интерфейси

Disassembler window 1. Бу ойнадebugger дастурининг ассемблер кодидан иборат. Ассемблер кўрсатмани ёки маълумотни ўзгартириш учун ушбу ойна устида *пробел* тугмасини босиш талаб этилади.

Registers window 2. Ушбу ойнада debugger дастурида регистрларнинг жорий ҳолатини кўрсатади. Дастур debuggerлаш қилиш жараёнида ушбу регистрлар қийматлари ўзгариб боради. Ўзгаришни рангдаги ўзгаришлардан билиш мумкин. Регистор қийматини ўзгартириш учун тегишли регистор устида сичқончанинг ўнг тугмаси босилади ва “Modify” банди танланади.

Stack window 3. Ушбу ойнада debug қилинаётган оқим хотирасида стекнинг жорий ҳолатини кўрсатади. Бу ойнада берилган оқимнинг юқори

стеки намойиш этилади.

Memory dump window 4. Ушбу ойнада хотирадаги маълумотлар намойиш этилади. Ушбу ойнада CTRL-G тугмаларини босиш орқали керакли хотира маълумоти олинади.

Хотира харитаси. Хотира харитаси ойнаси (View→Memory map) debuggerланадиган дастур томонидан жойлаштирилган барча хотира блокларини кўрсатади. Қуйида блокнот дастурининг хотира харитаси келтирилган (6.16 – расм).

Memory map

Address	Size	Owner	Section	Contains	Type	Access
00010000	00001000				Priv	RW
00020000	00001000				Priv	RW
0012C000	00001000				Priv	RW Gua
0012D000	00003000			stack of main thread	Priv	RW Gua
00130000	00003000				Map	R
00140000	00004000				Priv	RW
00240000	00006000				Priv	RW
00250000	00003000				Map	RW
00260000	00016000				Map	R
00280000	0003D000				Map	R
002C0000	00041000				Map	R
00310000	00006000				Map	R
00320000	00004000				Priv	RW
00330000	00003000				Map	R
00400000	00001000	nc		PE header	Imag	R
00401000	0000A000	nc	.text	code	Imag	R
0040B000	00003000	nc	.rdata	imports	Imag	R
0040E000	00002000	nc	.data	data	Imag	R
71AA0000	00001000	WS2HELP		PE header	Imag	R
71AA1000	00004000	WS2HELP	.text	code,imports,exports	Imag	R
71AA5000	00001000	WS2HELP	.data	data	Imag	R
71AA6000	00001000	WS2HELP	.rsrc	resources	Imag	R
71AA7000	00001000	WS2HELP	.reloc	relocations	Imag	R
71AB0000	00001000	WS2_32		PE header	Imag	R
71AB1000	00013000	WS2_32	.text	code,imports,exports	Imag	R
71AC4000	00001000	WS2_32	.data	data	Imag	R
71AC5000	00001000	WS2_32	.rsrc	resources	Imag	R
71AC6000	00001000	WS2_32	.reloc	relocations	Imag	R
77C10000	00001000	msvcrt		PE header	Imag	R
77C11000	0004C000	msvcrt	.text	code,imports,exports	Imag	R
77C5D000	00007000	msvcrt	.data	data	Imag	R
77C64000	00001000	msvcrt	.rsrc	resources	Imag	R
77C65000	00003000	msvcrt	.reloc	relocations	Imag	R

6.16 – расм. nc.exeдастури хотира харитаси

Оқим ва стекларни кўриш. ЗД кўплаб оқимлар фойдаланилиши мумкин. Таҳлилланувчи дастурда оқимларни кўриш учун View→Threads бандидан фойдаланилади. Бу ойна оқимларнинг хотира манзили ва уларнинг мавжуд ҳолатини кўрсатади (актив, пауза ҳолати ёки жараён вақтинчалик тўхтатилган). Агар оқим биттадан кўп бўлган тақдирда, уларга вақтинчалик тўхтатиб тури, кераклисини ишлатиш мумкин. Ҳар бир оқимни ўзига тегишли стеки бўлади. 6.16 – расмда main оқими стеки “stack of main thread” ёрлиғи билан номланган.

Кодни юклаш. OllyDbg дастурида ЗД debug қилиш учун юклаш қуйидаги усуллардан фойдаланилади.

Функция	**Меню**	**Тугмалар бирикмаси**	**Ёрлиқ кўриниши**
Run	Debug→Run	F9	
Pause		F12	
Run thread	Debug→Run thread	F11	

Single-step/step-into	Debug→Step Into	F7	
Step-over	Debug→Step Over	F8	
Run until return	Debug→Execute till Return	Ctrl-F9	
Run until user code		Alt-F9	

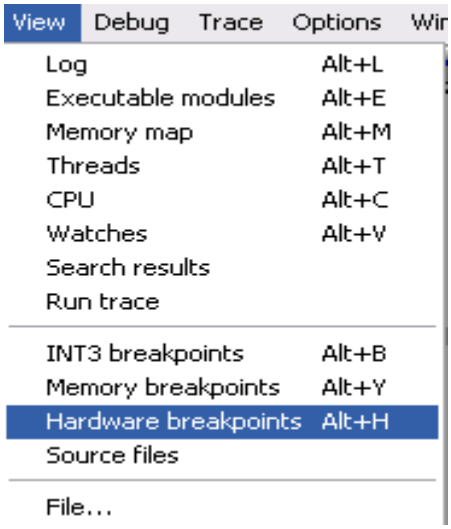
Кенг фойдаланиладиган Run ва Pause танловлари, дастурни ишини бошлаш ва тўхтатиш учун фойдаланилади.

Execute till User Code танлови ЗД таҳлиллашда кенг фойдаланилади.

Тўхтатиш нуқтаси. Бу нуқта таҳлилловчи томонидан ўрнатилади. Дастур шу нуқтага келгинда тўхтайди ва таҳлилловчини буйруғини кутади. OllyDbg дастурида бир нечта, дастур тўхтатиш нуқтаси, қурилма тўхтатиш нуқтаси,шартли тўхтатиш нуқталари ва хотира тўхтатиш нуқталаридан фойдаланиш мумкин.

Тўхтатиш нуқтасини қўйиш ва олиб ташлаш учун F2 тугмасидан фойдаланилади. Барча тўхтатиш нуқталарини кўриш учун қуйидаги расмда келтирилган тартиб танланади ёки уларнинг қисқа тугмалар 

дан бирини танлаш орқали амалга оширилади.



6.17 – расм.

Дастур тўхтатиш нуқтаси. strings дастури ЗДдаги қаторларни кўриш имконини беради. ЗД яратувчилари эса бу таҳлилга қарши қаторларни маълум станлартларга кодлаш усулидан фойдаланишади ва қаторлар тушуниб бўлмас ҳолга ўтказилади. ЗД юкланганда кодланган қатор хотирага юклангандан сўнг, String_Decoder функциялари орқали декодерланади ва керакли очиқ қатор олинади (6.18 - расм). Ушбу тўхтатиш нуқтаси усули декодурлаш функцияси мавжуд ҳолларда катта самара беради. Бу ҳолда тўхтатиш String_Decoder чақирилгандан сўнг қўйилади ва керакли очиқ қатор олинади.

```
push offset "4NNpTNHLKIXoPm7iBhUAjvRKNaUVBlr"
call String_Decoder
...
push offset "ugKLdNlLT6emldCeZi72mUjieuBqdfZ"
call String_Decoder
...
```

6.18 – расм.

Шартли тўхтатиш нуқтаси. Бу ҳолда дастур тўхталиши маълум шарт бажарилган ҳолда тўхтайди. Бу усул таҳлиллаш вақтини тежаш мақсадида кенг фойдаланилади. Бу турдаги тўхтатишдан қуйидагича фойдаланиш мумкин:

– Debuggerлаш ойнасида сичқончанинг ўнг тугмаси босилади ва қуйидаги кетма-кетлик танланади: Breakpoint→Conditional;

– керакли шарт киритилади ва OKтугмаси босилади, масалан, [ESP+8]>100;

– Play тугмасини босиш орқали шарт бажарилиши кутилади.

Қурилма тўхтатиш нуқтаси. Бу усулда қурилма регисторларидан фойдаланилади. Бу усул жуда ҳам тез амалга оширилади. Бу усул камчиллиги бир вақтнинг ўзида тўртта тўхтатиш нуқтасини қўйиш мумкин. Бу усулда тўхтатиш нуқтасини қўйиш учун Breakpoint→Hardware, on Executionкетма-кетлиги танланади.

***Хотира тўхтатиш нуқтаси*.** Бу усулда тўхтатишлар хотирада амалга оширилади. Тўхтатиш нуқтаси сифатида хотира адреси олинади ва хотира манзили кетма-кетлигида ҳаракатлантирилади. OllyDbg дастури хотира тўхтатиш нуқтаси усулини ёзиш (write), ўқиш (read) ва амалга ошириш (execute) ҳолатлари учун қўллаш имконини беради. Бу усулдан фойдаланиш учун сичқончанинг ўнг тугмаси босилиб, Breakpoint→Memory, on Access кетма – кетлиги танланади.

Бу усул асосан дастурда DLL файл юкланиши вақтини аниқлаш учун ишлатилади. Бунинг учун қуйидаги кетма-кетлик амалга оширилади:

– Хотира харитасига ўтиб, керакли DLL устида сичқончанинг ўнг тугмаси босилади (.text бўлимида);

– *Set Memory Breakpoint on Access* бандини танланг;

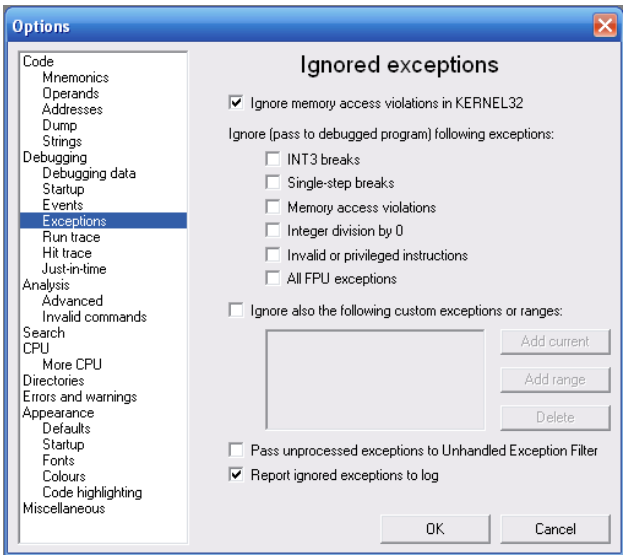
– F9 босилади ва қайтадан юклаш амалга оширилади.

Бу усулда .text бўлимида DLL юклангандан сўнг тўхтатилади.

Хатоликлар таҳлили. Debuggerлаш жараёни вақтида турли истисно ҳолатлар бўлиши мумкин. Бу ҳолда OllyDbg дастури debuggerлашни тўхтатади ва истисно ҳолатга кўрсатади. Бу ҳолда фойдаланувчи қуйидагилардан бирини танлаш талаб этилади:

– Shift-F7 босиш ва истисно ҳолат ичига ўтиш;
– Shift-F8 босиш ва истисно ҳолатдан кейинги ҳолатга ўтиш;
– Shift-F9 босиш ва истиснони тутиш ҳолатини ёқиш.

OllyDbg дастурида ЗД таҳлиллашда одатда барча истисно ҳолатларни ўчириб қўйиш тавсия этилади. Бу амалга ошириш учун Options→Exceptions бандига ўтилади:



6.19 – расм. Exception менюси

Ўзгартириш. OllyDbg дастури дастурда юкланган маълумотларни, регистор қийматларини ўзгартириш имконини беради. Бунинг учун Disassembler window ойнасидан Edit→Binary Edit банди танланади.

Топшириқ

1. Юқорида кўрсатилган кўрсалмалар асосида Lab01-02.exe, Lab01-03.exe ва Lab01-04.exe ЗД ларни юқорида номи келтирилган статик таҳлиллаш воситалари ва **http://www.VirusTotal.com/**воситаси асосида таҳлил этилсин.
2. Яратилган ЗД яратилган куни.
3. Қайси кутубхонага тегишли қандай файллар импорт қилинган ва улар вазифаси.
4. ЗД тармоқ хусусиятларига қандай тасир қилади.
5. Ушбу ЗД мақсадини аниқлашга ҳаракат қилинг.
6. Lab03-01.exe зараркунанда дустурини юкланг ва қуйидагиларни бажаринг:
7. Дастлаб procmon, process explorer, regshot, ApadeDNS дастурларини юкланг;
8. Шундан сўнг ЗД юкланг. Маълум вақт ўтгандан сўнг юкланган динамик таҳлиллаш воситалари ҳолатини кузатинг. Бундан ташқари статик таҳлиллаш воситаларидан фойдаланган ҳолда қўшимча маълумотларни

олинг.

9. Олинган натижалар асосида ЗД га тавсиф беринг.
10. IDA Pro дастурида Lab05-01.dll файлини таҳлил қилинг ва қуйидаги саволларга жавоб беринг:
11. DllMain манзилини аниқланг;
12. Imports ойнасидан фойдаланган ҳолда gethostbyname функциясини импорт қилинган манзилини аниқланг;
13. Gethostbyname нечта функция томонидан чақиртирилган;
14. 0x10001757 манзилда gethostbyname чақирилганлигини аниқланг ва қайси манзилга DNS сўрови юборилганлигини аниқланг;
15. 0x10001656 манзилда IDA Pro томонидан нечта локал ўзгарувчилар аниқланди.

Назорат саволлари

1. Статик таҳлиллаш усулларининг камчиликлари.
2. Динамик таҳлиллашнинг афзалликлари.
3. PE файлларни юклаш усуллари.
4. Тескари муҳандислик инжинерияси.
5. Қаторлар бўйича таҳлиллаш.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Michael Sikorski, Andrew Honig. Practical malware analysis. 2012.

7– амалий машғулот.Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар. Дастурий маҳсулотларни яратиш.

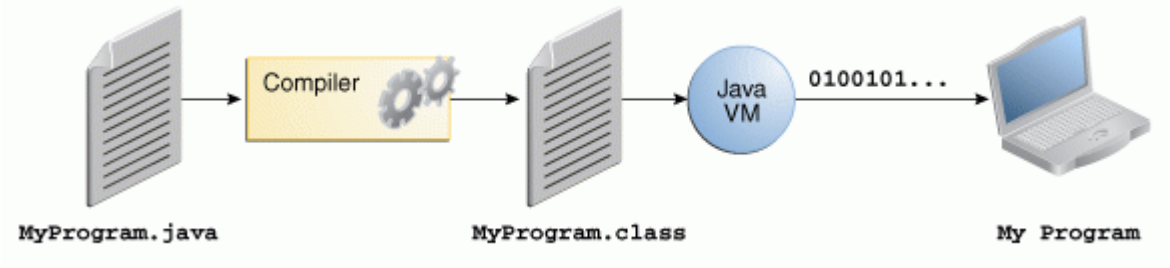
Ишдан мақсад: Java дастурлаш тилида хавфсиз дастурий таъминотларни яратиш кўникмаларини эгаллаш.

Масаланинг қўйилиши: Java дастурлаш тилида берилган вазифани амалга оширувчи хавфсиз дастурий таъминотлар яратилсин.

Ишни бажариш учун намуна

Изоҳлаш тиллари энг юқори даражали тиллар ҳисобланади. Кўплаб дастурчилар айнан шу тиллардан, C#, Perl, .Net ва Javaф ойдаланадилар. Бу тиллардан ёзилган кодлар машина тилига компиляция этилмайди, балки байткодларда ўтказилади. Байткодлар дастурий кодларни оралиқ ифодаланиши бўлиб, интерпритаторлар орқали машина кодига айлантирилади.

Java дастурлаш тилида барча дастлабки кодлар аввал .java кенгайтма билан тугайдиган очиқ текс файлда ёзилади. Ушбу файлдаги код интерпритатор орқали .class кенгайтмали файлга ўтказилади. Ушбу файл процессорда табий бўлган кодлардан эмас, балки Java Вертуал машинасининг (Java VM) тили байткодлардан иборат бўлади. Шундан сўнг жавани ишга тушурувчи курилма сизнинг илова – дастурингизни Java вертуал машинасида ишга туширади (7.1 - расм).



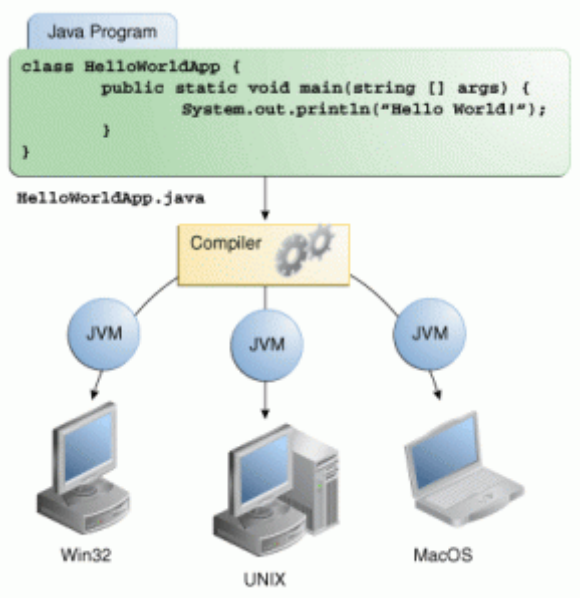
7.1 – расм. Дастурий таъминотни юклашнинг умумий кўриниши

Қуйида Java дастурлаш тилида ёзилган содда дастурий код келтирилган:

```
* HelloWorld.java
 */
public class HelloWorld
{
            public static void main(String[] args) {
```

```
            System.out.println("Hello World!");
        }
}
```

Ҳосил бўлган .class файлни турли операцион тизимларда юклаш имкони бўлганлиги учун, Java дастурлаш тили кўп платформали тил ҳисобланади:



7.2 – расм. Javани кўп платформаларда фойдаланилиши

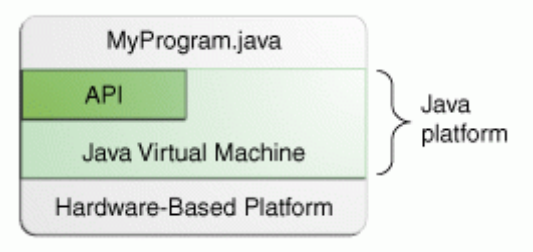
Java платформаси. Платформа бу – ускунавий ёки дастурий таъминот муҳити бўлиб, унда дастур ишга туширилади. Платформа сифатида кўп ҳолларда Microsoft Windows, Linux, Solaris OS ва Mac OS лар тушинилади. Java платформаси эса, бошқа кўпчилик платформалардан фақат дастурий таъминотдан иборатлиги билан ажралиб туради ва бошқа қурилмавий платформаларда ишлай олади.

Java платформаси икки таркибий қисмдан иборат:

– Java вертуал машинаси;
– Java дастурлаш илова интерфейси.

Java вертуал машинаси Java платформаси учун асос саналиб, турли қурилмавий платформаларда осон кўчиб ўта олади.

”API” кўплаб қулайликларни таъминлаш имкониятига эга дастурий пакетлар тўплами. Дастурчи ушбу пакетлардан фойдаланилган ҳолда ўзининг дастурий таъминотини яратади.



7.3 – расм. API ва Java вертуал машинаси дастурни асос қурилмадан ажратиб туради

Бу тизим ўз навбатида жараённи секинлашишига сабаб бўлади. Аммо ҳозирда вертуал машиналар соҳасидаги ривожланишлар буларни камайтиради.

Java хавфсизлик фреймворки. Стандарт Java платформаси (компилятор, байткод текширувчиси, реал вақт тизими) қуйидаги қоидалар асосида лойихалаштирилган:[1]

– класс азоларини бошқаришда (private, protected, ва public калит сўзлар орқали) қатий риоя этади;

– дастур ўзбошимчалик билан хотира манзилларига сакрамайди (кўрсатикичлар мавжуд эмас);

– *final* деб эълон қилинган катталиклар ўзгартирилмайди;

– ўзгрувчиларни эълон қилинмасдан олдин фойдаланиш мумкин эмас;

– масивларни бошқаришда дастлаб уларни чегаралари текширилади;

– бир турдаги объэктлар ўзбошимчалик билан бошқа турга ўтказилиши мумкин эмас.

Бундан ташқари бошқаришни назоратлашда махсус усуллардан фойдаланади.

Имтиёзли кодлар. Javaнинг рухсатни бошқариш тизими ресурслардан рухсат этилмаган тарзда фойдаланишни ҳимоялайди. Бунинг содда усули эса уларга имтиёзлар бериш. Фақат ресурсдан фойдаланиш имкониятига эга фойдаланувчигина (дастур) ундан фойдаланиш мумкин. Имтиёзга эга бўлмаган дастур эса тизим томонидан блокланади. Имтиёзга эга блоклар ўз навбатида тизимни хавфсиз ишлашига, рухсат этилмаган амалларни бажарамасликка катта ёрдам беради. Ҳар бир имтиёзга эга кодлар ўзи билан тизимга таваккалчиликни олиб келиши мумкин. Шуннинг учун имтиёзга эга кодлардан имкони борича камроқ фойдаланиш тавсия этилади.

Имтиёзга эга кодларда хатолик бўлганда, бу катта хавфсизлик муаммосини олиб келиши мумкин. Шунинг учун имтиёзга эга кодлардан тизимда фойдаланишдан олдин, улар аудитланиши шарт. Шунинг учун

[1] ESA Board for Software Standardisation and Control. Java coding Standards.

имтиёзга эга кодлар ичидаги ҳар бир ўзгарувчи текширилиши шарт. Бунга мисол қилиб қуйидаги кодни киритиш мумкин:

```
public static String getProp(final String name)
{
     return (String) AccessController.doPrivileged(new
     PrivilegedAction()
     {
     public Object run()
     {
     // 'name' is tainted, beware!
     Return System.getProperty(name);
     } // end method
} // end constructor
     }
```

Юқоридаги мисолда public тоифасидаги метод берилган бўлиб, name имтиёз текширилмасдан туриб берилмоқда. Бу эса ўз навбатида ихтиёрий фойдаланувчи томонидан бажарилиши мумкинлигини билдиради.

Бундан ташқари қуйидагилар тавсия этилади:

– *final public static* бўлмаган типлардан фойдаланишни чеклаш;

– имкони борича методлар кўламини камайтириш (имкони борича камроқ public мақомига эга ўзгарувчи ва методлардан фойдаланиш);

– махфий маълумотларга эга бўлган ички ўзгарувчан объектларга ҳеч қачон цилка қайтармаслик;

– ҳеч қачон тўридан-тўғри фойдаланувчи тақдим этган ўзгарувчан объектларни сақламанг;

– фойдаланувчи кутубхоналардан фойдаланишдан олдин, уларни текшириш талаб этилади;

– махфий маълумотларни асосий хотирадан тазалаб ташланг;

– махфий маълумотларни сақлашда (паролларни, шифрлаш калитлари) ўзгурвчан катталиклардан фойдаланинг. Масалан, паролларни сақлашда String ўрнига StringBuffer объектларидан фойдаланиш тавсия этилади;

Топшириқ

1. Ихтиёрий Java дастурлаш тилида ёзилган кодни компиляцилаш имкониятига эга дастурий маҳсулотни ўрнатинг (масалан, Eclipse, NetBeans, IDEA ва ҳак.).

2. Қуйидаги дастурий кодни киритинг ва методларни чақириш билан танишинг.

```
/* CallingMethodsInSameClass.java
```

```
 *
public class CallingMethodsInSameClass
{
      public static void main(String[] args) {
            printOne();
            printOne();
            printTwo();
      }
      public static void printOne() {
            System.out.println("Hello World");
      }
      public static void printTwo() {
            printOne();
            printOne();
      }
}
```

3. Қуйидаги жадвалдан фойдаланган ҳолда методларни бошқариш усулларидан фойдаланишни ўрганинг. Уларни тўғрилигини мисоллар асосида исботланг.

Имтиёз	Class	Package	Subclass
Public	Y	Y	Y
Protected	Y	Y	Y
Private	Y	N	N

4. String ва StringBuffer типидаги катталиклар фойдаланишни ўз ичига олган дастурий таъминотни яратинг.

Назорат саволлари

1. Юқори ва қуйи дастурлаш тиллари.
2. Java дастурлаш тилининг имкониятлари.
3. Java дастурлаш тилида хавфсиз дастурий таъминотни яратиш.

Фойдаланилган адабиётлар

1. ESA Board for Software Standardisation and Control. Java coding Standards. 2005.
2. Stamp Mark. Information security: principles and practice. USA, 2011.

8– амалий машғулот. Дастурий маҳсулотлар хавфсизлиги. Дастурий маҳсулотларда мавжуд заифликлар. Дастурий маҳсулотларни яратиш.

Ишдан мақсад: Хавфсиз операцион тизим тушунчаси ва Windows 7 операцион тизимида хавфсизлик созланмаларини ўрнатиш.

Масаланинг қўйилиши: Windows 7 операцион тизими учун берилган топшириқ асосида хавфсизлик созланмаси ўрнатилсин.

Ишни бажариш учун намуна

Операцион тизимни катта ҳажмдаги дастурлар мажмунинг комплекси деб қараш мумкин. Замонавий операцион тизимлар кўп вазифали ва кўп фойдаланувчили амаллар учун лойихаланади. Бинобарин, ОТ камида *ажратишни, хотира ҳимояси* ва *рухсатларни назоратлашни* қўллаб қувватлаши шарт. Қуйида уларнинг ҳар бири билан алоҳида танишиб чиқилади.[1]

Ажратиш. Замонавий ОТ ларнинг фундаментал хавфсизлик чораси сифатида одатда ажратиш қаралади. ОТ фойдаланувчиларни ва жараёнларни бир – биридан ажратиши шарт. Ажратишлар турли кўринишларда бўлиши мумкин:

– Физик ажратиш. Бу турдаги ажратишда фойдаланувчилар қурилма билан ажратилади. Бу кучли ажратиш тури бўлиб, амалда уни амалга ошириш мураккаб;

– Вақтинчалик ажратиш. Бирор керакли вақтда жараёнлар бир – биридан ажратилади. Бу турдаги ажратишда кўплаб муаммолар мавжуд ва шунинг учун самарадорлик йўқотилади.

– Мантиқий ажратиш. Масалан, ҳар бир жараён ўзининг мантиқий “қумли қутисига” (sandbox) бажарилади. Жараёни ўзининг қумли қутиси ичига ҳикмрон ва еркин бўлади. Аммо, ўз қутисидан ташқарида у ҳеч нарса эмас.

– Криптографик ажратиш. Криптография одатда маълумотни ташқарида тушунарсиз тарзда ифодалаш учун ишлатилади.

Албатта, амалда бу ажратиш усулларининг комбинациясидан фойдаланилади.

Хотира ҳимояси. ОТ яна бир муҳим вазифаларидан бири бу – хотира ҳимосини таъминлашдир. Бу ўз ичига ОТ ўзи фойдаланган хотирасини фойдаланувчининг жараёнларидан ажратишни олади. Бу одатда “тўсиқ”, “тўсиқ манзил” билан амалга оширилади. Тўсиқ манзил бу шундай манзилки фойдаланувчи ва унинг жараёнлари бу манзилда кесишмайди. Бу манзилнинг

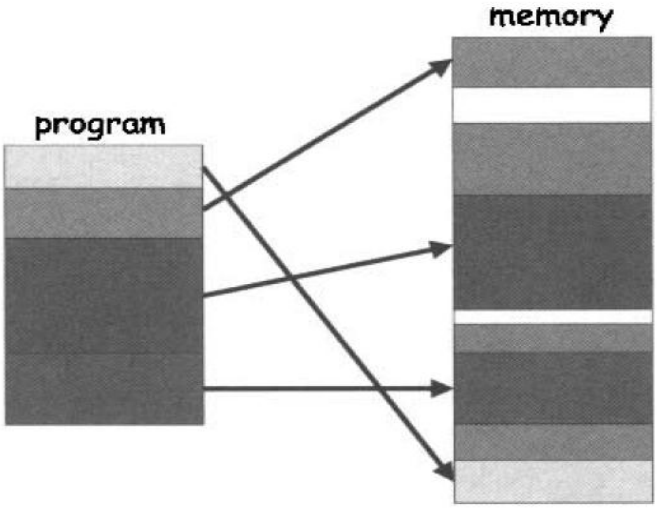
[1] Stamp Mark. Information security: principles and practice. 492 – с.

бир томонида ОТ ўз жараёнларини амалга оширади, бошқа томонида эса фойдаланувчи ўз жараёнларини бажаради.

Тўсиқ манзил статик, яъни ўзгармас бўлиши ёки динамик ўзгурувчан бўлиши мумкин. Динамик тўсиқда тўсиқ регисторидан фойдаланилиб, у ўзида жорий тўсиқ манзилини сақлайди.

Хотира ҳимоясида одатда *сегментлаш* ва *саҳифаларни рақамлаш* усулларидан фойдаланилади.

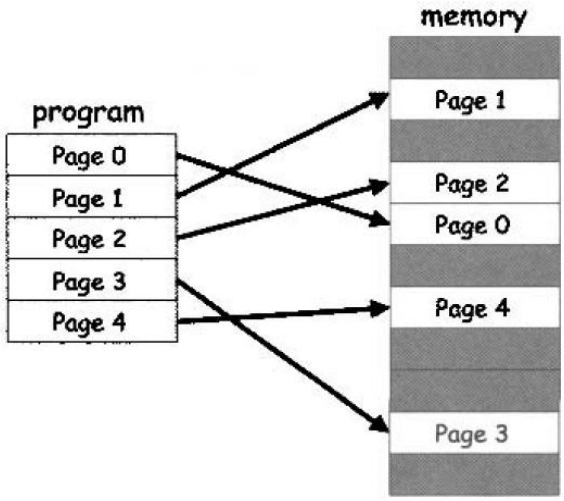
Сегментлаш 8.1–расмда келтирилган бўлиб, хотира мантиқий бўлимларга бўлинган, масалан, индивидуал жараён ва маълумотлар бир бўлимда. Ҳар бир сегментга мос рухсатларни бошқариш амалга оширилади. Сегментлашнинг афзаллиги шундан иборатки сегмент хотиранинг ихтиёрий жойида бўлиши мумкин. Бу жараёнда албатта, ОТ сегментни сакраш манзилини ўзида қайд этиши шарт. Бу одатда <segment, offset> жуфтлигида сақланади. Бу ерда offset сегментнинг бошланиш манзили.



8.1 – расм. Сегментлаш

Сегментлашнинг бир камчилиги бу сегментларнинг турли ўлчамлигидир. Натижада ОТ бирор элементни сегментга жойлаштиришдан олдин, сегментни ўлчамини билиши зарур.

Саҳифаларни рақамлаш усули сегментлашга ўхшаш бўлиб, фарқли томони ҳар бир сегментнинг ўлчами белгиланган бўлади (8.2 - расм).



8.2 – расм. Саҳифани рақамлаш

Белгиланган саҳифани чақириш <page, offset> кўринишида амалга оширилади. Саҳифани рақамлаш усулининг афзаллиги шундаки бунда фрагмент ҳосил бўлмайди, яъни ўзгурувчан ўлчам бўлмайди. Камчилиги эса, ҳар бир саҳифада мантиқий бўлимнинг йўқлиги ва натижада саҳифани бошқариш қийинлигидир.

Рухсатларни бошқариш

ОТ рухсатларни бошқаришда енг муҳим энг муҳим ўрин тутади. Шунинг учун, агар ОТ қаратилган таҳдид муофаққиятли амалга оширилса, ихтиёрий юқори даражада қурилган ҳимоя йўққа чиқарилади.

Ишончли ОТ

Тизим ишончли деб аталади, агар биз хавфсизликка таянсак. Бошқача қилиб, агар ишончли тизим кутилган хавфсизликни таъминлашда аврияга учраса, у ҳолда тизим хавфсизлиги синдирилган деб аталади.[1]

Бу таҳлилдан, ишончлилик ва хавфсизлик орасида фарқ мавжудлигини аниқлаш мумкин. Ишонч бирор бар нарсага таянади, яъни сиз ишонасиз ёки ишонмайсиз.

Хавфсизлик эса, бирор бир механизмнинг самарадорлиги ҳақидаги қарордир. Шуни эсда тутиш керакки хавфсизлик ишонга таянади.

Агар барча ОТ ажратишни, рухсатларни бошқаришни ва хотира ҳимоясини амалга оширса, унда ишончли ОТ нима қилади ? Ишончли ОТ ўз навбатида юқоридаги жараёнларни хавфсиз амалга ошириши билан характерланади.

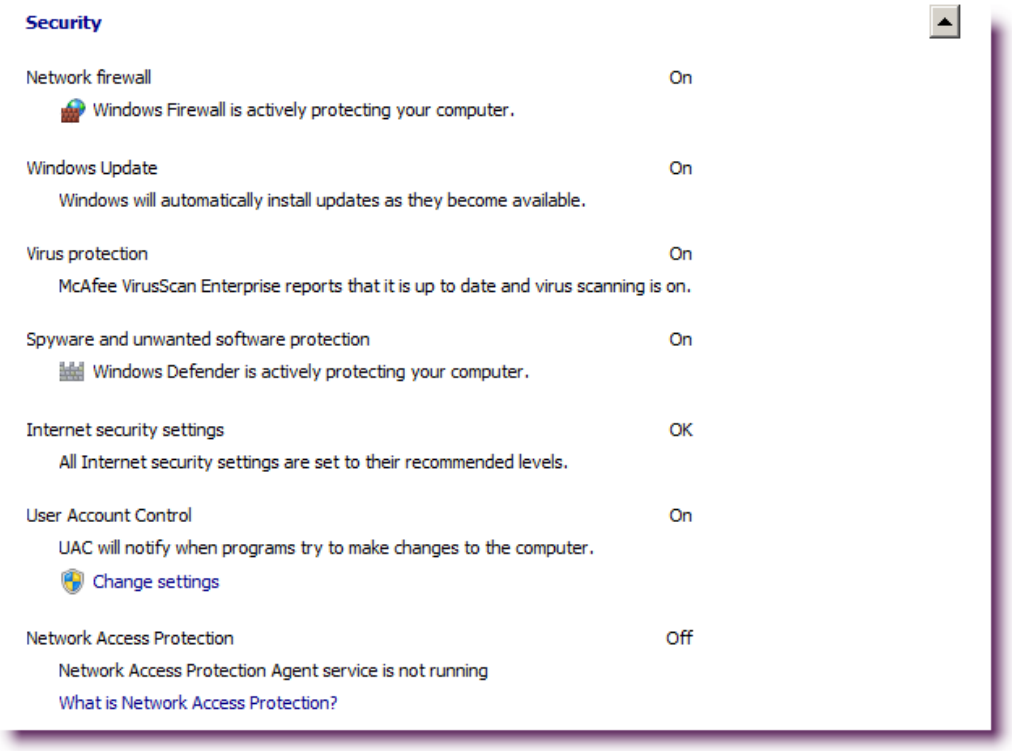
Ишончли жой. ОТ дан аутентификациядан ўтилганда, киртилган парол қандай ва қайси манзилга сақланади ? Агар сақланган манил ишончли бўлмаса, у ҳолда бузғунчи томонидан у қўлга киритилиши мумкин. Шундай

[1] Stamp Mark. Information security: principles and practice. 495 – c.

экан ишончли ОТ маълумотларни ишончли жойга сақлангинлигини кафолатлаши шарт.[1]

Ушбу қисмда Windows7 операцион тизимида хавфсизлик параметрларини созлаш усуллари ҳақида тўхталиб ўтилади.

Ўрнатилган Windows 7 ОТда ўрнатилган хавфсизлик созланмаларини кўриш учун “Windows Security Center” дан фойдаланилади. Бунга ўтиш учун, **Start→Control Panel→System and Security→ Review your computer's status** бандларини танланади. Бу ойнада хавфсизлик ва ташкилий чоралар ҳақида маълумотлар берилган бўлиб, хавфсизлик бўлимини (security) танланади ва ОТ мавжуд ўрнатилган хавфсизлик созланмалари кўринади.



8.3 – расм. Windows 7 хавфсизлик созланмалари

Расмдаги маълумот асосида қандай созланмалар ёқилганлиги ёки ёқилмаганлиги ҳақида маълумотга эга бўлинади.

ОТ да фақат битта тармоқлараро экран фойдаланилиши керак. Агар Windows 7 ОТ тармоқлараро экрани ўчирилган бўлган тақдирда, уни қуйидаги кетма-кетликларни бажариш орқали ёқиш мумкин: **Control Panel→System and Security→Windows Firewall.**

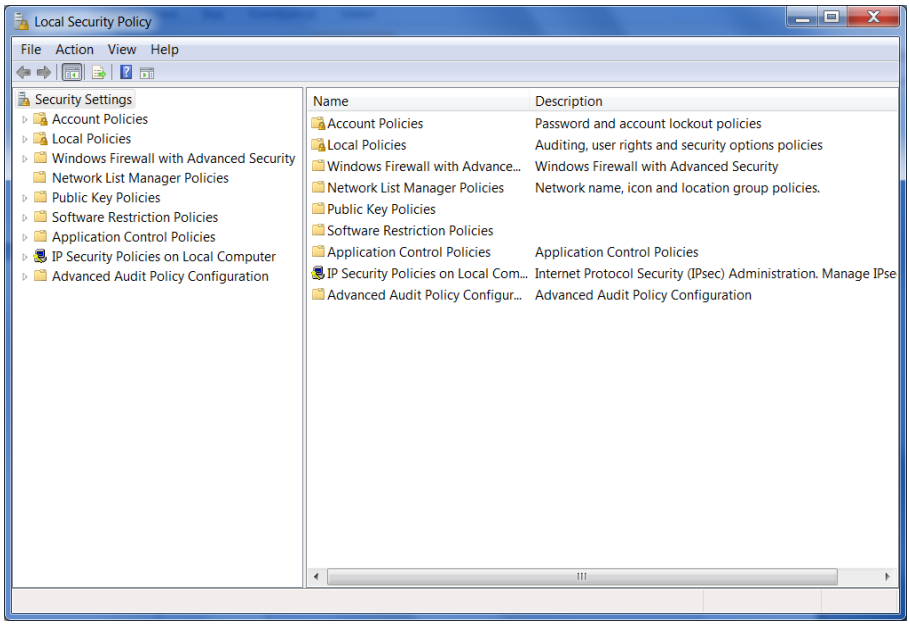
Тизимда мавжуд камчиликлар ОТ нинг серверида бартараф этилиб борилади ва ОТ серверга мурожаат этганда бу ечимларни ўзида кўчириб олади. Бу ОТда автоматик янгилаш (Automatic Updates) банди ёқилган вақтда мавжуд бўлади. Бу бандни йоқиш учун қуйидаги кетма-кетликлар

[1] Stamp Mark. Information security: principles and practice. 497 – c.

бажарилади: **Control Panel→System and Security→Windows Update → Turn automatic updating on or off.** Бу банда «Install updates automatically (recommended)» танлови танланади.

Локал хавфсизлик сиёсатини ўрнатиш

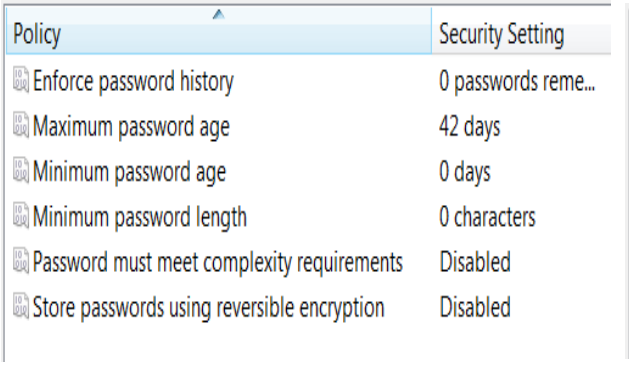
Локал хавфсизлик сиёсатини созлаш ойнасига ўтиш учун буйруқлар сатрида *secpol.msc* буйруғи киритилади ва қуйидаги ойна ҳосил бўлади.

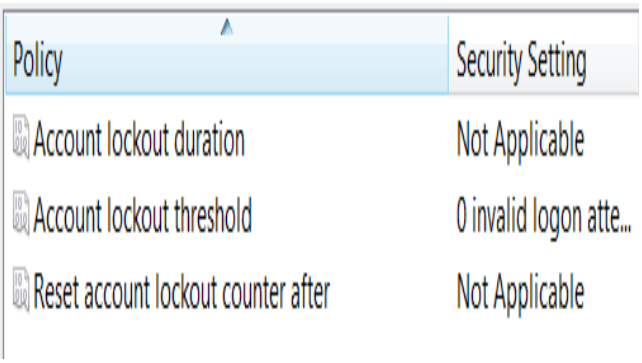


8.4–расм. Локал хавфсизлик сиёсати ойнаси

Бу ойнадан туриб “Қайд ёзуви сиёсати (Account Policies)”, “Локал сиёсат (Local Policies)”, “Windows Firewall созланмалари” ва ҳак. созлаш имконияти мавжуд бўлади.

Қайд ёзуви сиёсати банди танланганда, унда пароллар сиёсати ва қайд ёзувини қулфлаш сиёсатини созлаш мумкин.





Пароллар сиёсати Қайд ёзувини қулфлаш сиёсати

8.5 – расм. Қайд ёзуви сиёсати

Пароллар сиёсати. Пароллар хавфсизлиги сиёсатини амалга ошириш ва режалаштириш хавфсизлик парамертларини енг муҳим томони хисобланади. Фойдаланувчилар созламасдан хавфсизлик сиёсатини қўлламасдан алмаштиришдан талаб қилмайдиган кучсиз паролларни

қўллашади. Бундай ҳолатларда паролнинг ҳаттоки оддий ҳолатларда терилиши катта ютуқларга имкон беради.

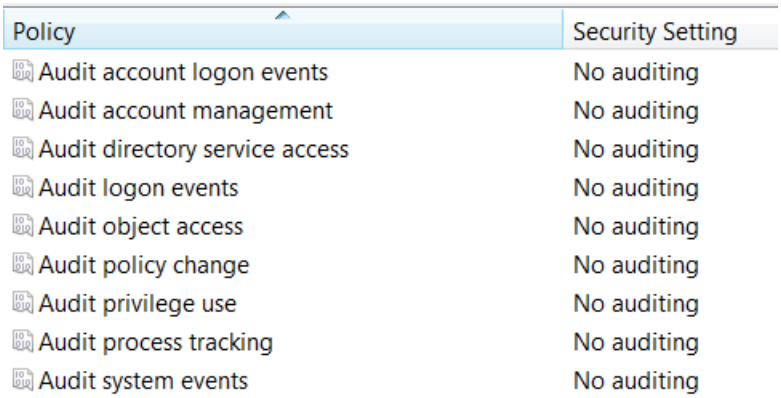
8.1 – жадвал

Пароллар сиёсати созланмалари

Сиёсати	Умумий (одатий) холат	Тавсия этилган
Паролнинг такрорланмаслигини талаб килиниши. (Enforce password history)	0 сақланган пароллар сони	10
Паролнинг максимал ишлаш муддати (Maximum password age)	42 кун	90
Паролнинг минимал ишлаш муддати (Minimum password age)	0 кун	1
Паролнинг минимал узунлиги (Minimum password length)	0 символ	8
Парол мукаммалик талабларига жавоб бериши керак (Password must meet complexity requirements)	ўчирилган	Рухсат этилган
Домендаги барча фойдаланувчиларнинг паролларни сақлаш, қайта шифрлаш орқали. (Store password using reversible encryption for all users in the domain)	ўчирилган	ўчирилган

Қайд ёзувини қулфлаш сиёсати. Бу тузилмалар фойдаланувчи қайдномасини қачон ва қай вақтда блоклаштиришни аниқлайди. Максимал хавфсизликни таъминлаш учун бу тизим албатта аниқланган бўлиши керак. Акс ҳолда потенсиал ҳужум кўрсатувчи бутунлай озодликка эга бўлади ва ҳоҳлаган вақтида аниқ бўлиб қолган паролни ишлатиш хуқуқига эга бўлади.

ОТда аудит сиёсатини йўлга қўйиш учун, Локал сиёсатлар бандадан Аудит сиёсати банди танланади ва керакли ҳодисалар учун аудит сиёсати ёқилади.



8.6 – расм. Аудит сиёсатини ёқиш

Бундан ташқари локал хавфсизлик сиёсати ойнасидан туриб, қуйидаги

амалларни бажариш мумкин:

– Windows тармоқлараро экрани созланмаларини бошқариш, янги қоидалар яратиш;
– Қаттиқ дискдаги маълумотларни шифрлаш амалларини бажариш;
– Локал компьютерда IPSec хавфсизлик сиёсатини созлаш;
– Дастурий воситаларни чеклаш сиёсатини созлаш;
– Дастурий воситаларни бошқариш сиёсатини;
– Кенгайган аудит сиёсатини созлаш.

Топшириқ

1. Хавфсизлик нуқтаи – назаридан келиб чиқиб, пароллар сиёсатини тўғри ўрнатинг;
2. Аудит банди орқали камида 4 та ҳодиса учун аудит сиёсатини созланг;
3. Windows тармоқлараро экран учун кирувчи ва чиқувчи қоидаларни яратинг;
4. Дастурий воситаларни чеклаш банди орқали бирор дастурдан фойдаланишни чекланг.
5. Ҳар бир топшириқ натижаларини расмлар билан ҳисоботда ифодаланг.

Назорат саволлари

1. ОТ хавфсизлик вазифалари.
2. Ишончли ОТ.
3. Сегментлаш ва ажратиш усуллари.
4. Ишончли жой.
5. Windows 7 ОТ хавфсизлик сиёсатини созлаш.

Фойдаланилган адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. https://technet.microsoft.com/en-us/library/dd277395.aspx

V. БЎЛИМ

КЕЙСЛАР БАНКИ

V. КЕЙСЛАР БАНКИ

1 – мавзу бўйича муаммоли саволлар

1. Ахборот хавфсизлигида фундаментлат муаммолари бу: махфийлик, бутунлилик ва фойдаланувчанликни таъминлашдир.
    a. Ҳар бир теминга: махфийлик, бутунлик ва фойдаланувчанликка аниқлик киритинг.
    b. Махфийлик хусусияти бутунлиликга қараганда муҳим саналган аниқ мисол келтиринг.
    c. Бутунлик хусусияти махфийликка қараганда муҳим саналган аниқ мисол келтиринг.
    d. Фойдаланувчанлик хусусияти қолганларга қараганда муҳим саналган аниқ мисол келтиринг.
2. Банк нуқтаи назаридан қараганда, мижоз маълумотларининг махфийлиги муҳимроқми ёки бутунлиги ? Банк мижози нуқтаи назариданчи ?
3. Онлайн банк ўрнига, Алиса онлай шахмат ўйинини таклиф этди. Бунинг учун мижозлар ҳар ойлик тўловни амалга оширадилар ва тизимга кириб ўзларига мос рақибни танлайдилар.
    a. Қайси жойда Алисанинг онлайн шахмат ўйини учун махфийлик керак ? Мижозлар учунчи ?
    b. Нима учун бутунлилик керак ?
    c. Нима учун фойдалнувчанлик муҳим бу ерда ?
4. Онлайн банк ўрнига, Алиса онлай шахмат ўйинини таклиф этди. Бунинг учун мижозлар ҳар ойлик тўловни амалга оширадилар ва тизимга кириб ўзларига мос рақибни танлайдилар.
    a. Алисанинг онлайн шахмат ўйининг қайси қисмида криптографиядан фойдаланилади ?
    b. Рухсатларни назоратлашданчи ?
    c. Хавфсизлик протоколичи ?
5. Фараз қилайлик сизда бир секунда 2^{40} та калитни тестлаш имконига эга компьютер мавжуд.
    a. Бу компьютер ёрдамида 2^{88} та калитни тестлаш учун қанча вақт керак бўлади (йил ҳисобида).
    b. Бу компьютер ёрдамида 2^{128} та калитни тестлаш учун қанча вақт керак бўлади (йил ҳисобида).
    c. Бу компьютер ёрдамида 2^{256} та калитни тестлаш учун қанча вақт

керак бўлади (йил ҳисобида).

2 – мавзу бўйича муаммоли саволлар

1. Цезар шифрлаш усули ёрдамида шифрланган қуйидагига тенг. Унга тегишли бўлган очиқ матнни ва калитни аниқланг ? (Фақат инглиз алифбосидан, /A....Z/ фойдаланилган)
   a. VSRQJHEREVTXDUHSDQWU
   b. CSYEVIXIVQMREXIH
2. DES шифрлаш алгоритми билан танишинг ва қуйидагиларга жавоб беринг:
   a. Очиқ матн блокининг узунлиги;
   b. Шифрматн блокининг узунлиги;
   c. Калит узунлиги;
   d. Раунд калит узунлиги;
   e. Раундлар сони;
   f. S жадваллар сони;
   g. S жадвалда кирувчи ва чиқувчи маълумот узунлиги;
3. ECB ва CBC шифрлаш режимларининг афзалликлари ва камчиликларини мисоллар билан исботланг.
4. Фараз қилинг блокли шифрлаш усули қуйидаги қоида бўйича шифрлашни амалга оширади: C_0 = IV XOR E(P_0, K), C_1 = C_0 XOR E(P_1, K), C_2 = C_1 XOR E(P_2, K), ...
   a. Унга мос бўлган дешифрлаш қоидасини ёзинг;
   b. Бу режимни CBC режим билан таққослаганда афзаллик ва камчиликларни айтинг.
5. Электрон рақамли имзо учун қуйидагиларни исботланг:
   a. Қандай қилиб ва нима учун электрон рақамли имзо хабарни юборишдан тонмасликни таъминлайди ?
   b. Қандай қилиб ва нима учун электрон рақамли имзо хабар бутунлигини таъминлайди ?

3 – мавзу бўйича муаммоли саволлар

1. Биометрик хусусиятлардан фойдаланилганда:
   a. Идентфикациялаш ва аутентификациялаш жараёнлари орасидаги фарқни айтинг ?
   b. FAR ва FRR хатоликларни аниқ мисоллар билан тушунтиринг.
2. Файлда паролни боғлаш билан мумкин бўлган ҳолда:
   a. Нима учун паролни файлда хэшлаб сақлаш яхши ?

   b. Нима учун файлда паролни шифрлаб сақлагандан кўра хэшлаб сақлаган яхши ?
   c. “туз” нима ва у нима учун паролга қўшиб хэшланади
3. Ташкилотда ходимларни ҳақиқийлигини текшириш учун бармоқ изига асосланган биометрик аутентификациялаш тизимидан фойдаланилади. Бу иккита тизим мавжуд бўлиб, биринчисида FAR кўрсаткичи 1 % га FRR кўрсаткичи эса 5 % га тенг. Иккинчисида эса, FAR 5 % га, FRR эса 1 % га тенг.
   a. Қайси тизим энг хавфсиз ва нима учун ?
   b. Қайси тизим ходимларбоб ва нима учун ?
   c. Қайси тизимни танлаган бўлардингиз ва нима учун ?
4. Аудио Капчадан фойдаланилганда:
   a. Реал аудио Капчани тасвирланг ва қандай ишлашини тушунтиринг.
   b. Бу турдаги капчадан фойдаланилганда таҳдидчига қандай маълумотлар маълум бўлади ?
5. Алиса ва Боб орасидаги мулоқотда пакетлар шифрланади ва бутунлик смметрик тизимлардан фойдаланилган ҳолда амалга оширилади.
   a. IP сарлавҳани қайси қисми шифрланади ва қайси қисми шифрланмайди ?
   b. IP сарлавҳани қайси қисмининг бутунлиги таъминланади ва қайси қисмида йўқ ?
   c. Маърузада айтиб ўтилган тармоқлараро экрандан қайси бири бу ҳолда фойдаланилади ? Жавобингизни асосланг ?
   d. Маърузада номлари келтирилган тармоқлараро экранлар таҳлиллаш учун қандай маълумотлар маълум бўлади ?

4 – мавзу бўйича муаммоли саволлар

1. SSL ва IPSec протоколлари тармоқда хавфсизликни таъминлаш учун фойдаланилади.
   a. SSL протоколни IPsec протоколга қараганда афзалликларини кўрсатинг.
   b. IPsec протоколни SSL протоколга қараганда афзалликларини кўрсатинг.
   c. SSL ва IPSec протоколлари орасидаги фарқни ва ўхшашликни аниқланг.
2. 4 – маърузада келтирилган SSH нинг соддалиштирилган протоколига

қаранг.

a. Қаерда ва қандай қилиб Алиса аутентификациядан ўтмоқда. Нима такрорлаш таҳдидидан ҳимояламоқда.
b. Агар Триди пассив ҳужумчи бўлса (фақат маълумотни кузата олади), К калитни ҳисоблай олмайди. Нима учун ?
c. Агар Триди актив ҳужумчи бўлса (хабар ҳам юбора олади), у К калитни ҳисоблай олади. Нима учун бу калит билан протоколни буза олмайди ?
d. Охирги хабарни К калит билаг шифрлашдан мақсад нима?

3. Фараз қилинг WEP протоколи қуйидагича ўзгартирилди. Ҳар бир пакетни шифрлашда К калитдан фойдаланилади. К калит аутентификацияда фойдаланилган калит билан бир хил.
   a. Бу яхши фикрми ёки йўқ. Асосланг.
   b. Бу усул WEP да фойдаланилган K_{IV}=(IV, K) усулга қараганда бардошлими ёки йўқ.
4. Wireshark ёки ихтиёрий тармоқ снифферидан фойдаланиб, SSL тармоқни тутиб олинг ва уни таҳлил этинг.
5. IPSec протоколининг AH ва ESP режимлари орасидаги фарқни тушунтиринг.

5 – мавзу бўйича муаммоли саволлар

1. Тақиқланган катталикларни киритишга асосланган хотоликлар ва улар қандай хавфларни олиб келиши мумкин.
2. Дастурий маҳсулотлардаги заифликлар одатда инмалар билан изоҳланади. Мисоллар билан исботланг.
3. Қаторларни таҳлиллашда одатда Strings дастуридан фойдаланилади. Ушбу дастурни алдаш учун қандай усуллардан фойдаланилади.
4. SandBoxдан фойдаланилган ҳолда содда динамик таҳлил амалга ошириш мумкин. Бу усулнинг афзаллиги ва камчиликларини келтиринг.
5. Булутли ҳисоблаш тизимларида вертул машиналарни ҳосил қилишда ажратишнинг қайси туридан фойдаланилади ва улар ҳақида тўлиқроқ маълумот беринг.

VI. БЎЛИМ

МУСТАҚИЛ ТАЪЛИМ МАВЗУЛАРИ

VI. МУСТАҚИЛ ТАЪЛИМ МАВЗУЛАРИ

Мустақил ишни ташкил этишнинг шакли ва мазмуни

Тингловчи мустақил ишни муайян модулни хусусиятларини ҳисобга олган холда қуйидаги шакллардан фойдаланиб тайёрлаши тавсия этилади:

- меъёрий хужжатлардан, ўқув ва илмий адабиётлардан фойдаланиш асосида модул мавзуларини ўрганиш;
- тарқатма материаллар бўйича маърузалар қисмини ўзлаштириш;
- автоматлаштирилган ўргатувчи ва назорат қилувчи дастурлар билан ишлаш;
- махсус адабиётлар бўйича модул бўлимлари ёки мавзулари устида ишлаш;
-тингловчининг касбий фаолияти билан боғлиқ бўлган модул бўлимлари ва мавзуларни чуқур ўрганиш.

Мустақил таълим мавзулари

1. Ахборотнинг ташкилий ҳимояси.
2. Мухандис – техник ҳимоя воситалари ва уларни ўрнатиш қоидалари.
3. Ташкилотда ахборот хавфсизлигини ишлаб чиқиш.
4. ГОСТ 28147-89 шифрлаш стандарти.
5. AES шифрлаш стандарти.
6. MD5 хэш функцияси.
7. SHA1 хэш функцияси.
8. DSA электрон рақамли имзо стандарти.
9. Биометрик аутентификациялаш усуллари.
10. рухсатларни бошқариш усуллари.
11. Тўқ сариқ китоб.
12. Икки факторли аутентификация.
13. Зараркунанда дастурлар ва уларга қарши ҳимоя усуллари.
14. Тескари муҳандислик инжинирингги.
15. LINUX операцион тизим хавфсизлик хусусиятлари.
16. WINDOWS операцион тизим хавфсизлик хусусиятлари.
17. SQL инекция таҳдиди ва улардан ҳимоялаш.
18. DDOS таҳдиди ва ундан ҳимояланиш.
19. DLP тизимлар.

20. Хавфсизлик мониторинги ва уни амалга ошириш.
21. Булутли технология ва унда ахборот хавфсизлиги.
22. Стегонографик ҳимоя усуллари.
23. Электрон ҳукуматда ахборот хавфсизлиги.
24. Маълумотлар базасида ахборот хавфсизлигини таъминлаш.
25. Эллиптик эгри чизиқларга асосланган очиқ калитли шифрлаш усуллари.

VII. БЎЛИМ

ГЛОССАРИЙ

VII. ГЛОССАРИЙ

№	Термин	Изоҳ	Description
1.	**Авторизация** **Authorization**	– тизимда фойдаланувчига, унинг ижобий аутентификациясига асосан, маълум фойдаланиш ҳуқуқларини тақдим этиш.	- View user specific access rights on the basis of a positive result in its authentication system.
2.	**Антивирус** **Antivirus**	– вирусларни аниқловчи ёки аниқловчи ва йўқ қилувчи дастур. Агар вирус йўқ қилинмаса, заҳарланган дастурий йўқ қилинади. Яна – вируслардан ҳимоялашга, захарланган дастурий модуллар ва тизимли маконларни аниқлашга, хамда захарланган обектларнинг дастлабки ҳолатини тиклашга мўлжалланган дастур.	- 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.
3.	**Аппарат ҳимоя** **Hardware protection**	– компьютерда маълумотларни ҳимоялашда аппарат воситалардан, масалан, чэгара регистрларидан ёки қулфлардан ва калитлардан фойдаланиш.	- the use of hardware, for example, registers boundaries or locks and keys to protect data in computers.
4.	**Асимметрик шифр** **Asymmetric cipher**	– бундай шифрда шифрлаш калити дешифрлаш калитига мос келмайди.	- a cipher in which the encryption key does not match the decryption key.
5.	**Асимметрик шифрлаш Asymmetric Encryption**	- махфийлаштириш усули бўлиб, шифрлаш учун турли калитлардан фойдаланилади.	- the method of classification, in which different encryption keys are used.
6.	**Аутентифика-**	– одатда тизим	- checking user

	ция **Authentication**	ресурсларидан фойдаланишга рухсат этиш хусусида қарор қабул учун фойдаланувчининг (ҳақиқийлигини), қурилманинг ёки тизимнинг бошқа ташкил этувчисининг идентификациясини текшириш; сақланувчи ва узатувчи маълумотларнинг рухсатсиз модификацияланганлигини аниқлаш учун текшириш.	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.
7.	**Ахборот уруши** **Information war**	- душманнинг ахборотига, ахборотга асосланган жараёнларига ва ахборот тизимларига зарар етказиш, бир вақтнинг ўзига тегишли ахборотни, ахборотга ва ахборот тизимларига асосланган жараёнларни ҳимоялаш йўли билан ахборот устунлигига эришиш учун зарур чораларни кўриш ҳаракатлари.	- actions taken to achieve information superiority by damage information, processes, based on information and information systems of the enemy while protecting proprietary information, processes based on information and information systems.
8.	**Ахборот хавфсизлиги** **Information security**	- ахборот ҳолати бўлиб, унга биноан ахборотга тасодифан ёки атайин рухсатсиз таъсир этишга ёки рухсатсиз унинг олинишига йўл қўйилмайди. Яна - ахборотни техник воситалар ёрдамида ишланишида унинг махфийлик (конфиденциаллик), яхлитлик ва фойдаланувчанлик каби	- 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

		характеристикаларини (хусусиятларини) сақланишини таъминловчи ахборотнинг ҳимояланиш сатҳи ҳолати.	and availability.
9.	**Ахборот хавфсизлиги мониторинги** **Information security monitoring**	- ахборот хавфсизлиги талабларига мослигини аниқлаш мақсадида ахборот тизимидаги ахборот хавфсизлигини таъминлаш жараёнини муттасил кузатиш.	- constant monitoring of the process safety information in the system information to determine its compliance with safety information.
10.	**Ахборотни техник ҳимоялаш** **Hardware Information Security**	- ҳимоялашга лойиқ ахборотнинг (маълумотларнинг) хавфсизлигини харакатдаги қонунларга мувофиқ, техник, дастурий ва дастурий - техник воситаларни ишлатиб, нокриптографик усуллар ёрдамида таъминлашдан иборат ахборот ҳимояси.	- Information Security is to ensure security of cryptographic methods of information (data) to be (to be) protection in accordance with applicable law, the application of technical, software and software and hardware.
11.	**Ахборотни криптографик ҳимоялаш Cryptographic Protection Of Information**	- ахборотни криптографик ўзгартириш ёрдамида ҳимоялаш.	- information security by means of its cryptographic transformation.
12.	**Ахборотни ташкилий ҳимоялаш Organizational Information security**	- маъмурий чораларни қўллаш йўли билан амалга оширилувчи ахборот ҳимояси.	— the Information security which is carried out by acceptance of administrative measures.
13.	**Ахборотни ҳуқуқий ҳимоялаш**	– ахборотни ҳимоялаш бўйича субъектлар муносабатини ростловчи	— the information security by legal methods including development of

	Legal information security	қонуний ва меъёрий хужжатларни (актларни) ишлаб чиқишни, ҳамда уларнинг бажарилишини назорат қилишни ўз ичига олувчи ахборотни хуқуқий усуллар ёрдамида ҳимоялаш.	legislative and normative legal documents (acts), subjects governing the relations on information security, application of these documents (acts), and also supervision and control of their execution
14.	**Ахборотни ҳимоялаш** **Information protection**	– ахборот хавфсизлигини таъминлашга йўналтирилган тадбирлар комплекси. Амалда ахборотни ҳимоялаш дэганда маълумотларни киритиш, сақлаш, ишлаш ва узатишда унинг яхлитлигини, фойдаланувчанлигини ва агар, керак бўлса, ахборот ва ресурсларнинг конфиденциаллигини мададлаш тушунилади.	- includes a complex of the actions aimed at providing information security. In practice it 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.
15.	**Биометрик маълумотлар** **Biometric data**	– 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.	- 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.
16.	**Бузилиш** **Distortion**	– маълумотлар сигнали параметрлари қийматларининг ўрнатилган талаблардан четланиши. Яна - алоқа линияси бўйича	- deviation of values of parameters of a signal of data from the established requirements. Also, change of contents of the

		узатилувчи хабар таркибининг ўзгариши.	message transferred on the communication lines.
17.	**Вирус** **Virus**	– 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.	- a small program that inserts itself into other programs when executed. Also, 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.
18.	**Давлат сири** **State secret**	- давлат томонидан муҳофаза қилинувчи, фош қилиниши давлатнинг ҳарбий-иқтисодий потенциалининг сифатли 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 махфий” грифли ахборот тааллуқли.	- 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".
19.	**Дешифрлаш алгоритми Decryption algorithm, deciphering**	– дешифрлаш функциясини амалга оширувчи ва шифрлаш алгоритмига тескари алгоритм	– a cryptographic algorithm, the inverse of the algorithm encryption and decryption function implements.
20.	**Идентификац**	– фойдаланиш субъектлари	-assignment to subjects

	ия **Identification**	ва объектларига идентификатор бериш ва/ёки тақдим этилган идентификаторни берилганлари рўйҳати билан таққослаш.	and objects of access of the identifier and/or comparison of the shown identifier with the list of the appropriated identifiers.
21.	**Икки факторли аутентификация** **Two-factor authentication**	– фойдаланувчиларни иккита турли факторлар асосида аутентификациялаш, одатда, фойдаланувчи биладиган нарса ва эгалик қиладиган нарса (масалан, пароль ва физик идентификатори) асосида.	- 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).
22.	**Инсайдер** **Insider**	– гурухга тегишли яширин ахборотдан фойдаланиш хуқуқига эга гурух аъзоси. Одатда, ахборот сирқиб чиқиш билан боғлиқ можорода муҳим шахс ҳисобланади. Шу нуқтаи назаридан, инсайдерларнинг қуйидаги хиллари фарқланади: бепарволар, манипуляцияланувчилар, ранжиганлар, қўшимча пул ишловчилар ва ҳ.	— 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.
23.	**Калит** **Key**	Қандайдир ахборот фойдаланиш ваколатини тасдиқлаш учун ишлатиладиган код.	- the code used for confirmation of powers on access to some information.
24.	**Калитлар генератори**	- калит (криптотизим калити), калит кетма-кетлиги, инициализация	- technical device or program designed to generate arrays of

	Key generator	векторлари ва ҳ. сифатида ишлатилувчи сон массивлари ёки бошқа маълумотларни ишлаб чиқаришга мўлжалланган техник қурилма ёки дастур.	numbers or other data to be used as keys (cryptographic) key sequence, initialization vectors, and so p.
25.	**Компьютер тизими хавфсизлиги** **Security of computer systems**	– деструктив ҳаракатларга ва ёлғон ахборотни зўрлаб қабул қилинишига олиб келувчи ишланадиган ва сақланувчи ахборотдан рухсатсиз фойдаланишга уринишларга компьютер тизимининг қарши тура олиш ҳусусияти.	- property computer systems to resist attempts of unauthorized access to information processed and stored, the input of information, leading to destructive actions, and the imposition of false information.
26.	**Криптографик алгоритм Cryptographic algorithm**	– криптографик функцияларнинг бирини ҳисоблашни амалга оширувчи алгоритм	- тhe algorithm that implements the computation of one of the cryptographic functions.
27.	**Криптографик ҳимоя Cryptographic protection**	- маълумотларни криптографик ўзгартириш ёрдамида ҳимоялаш.	— data security by means of cryptographic transformation of data.
28.	**Криптография** **Cryptography**	–ахборот мазмунини ниқоблаш, унинг ушлаб қолиниши ва бузилиши имкониятини бартараф этиш, ахборотни рухсатсиз фойдаланишдан ҳимоялаш мақсадида маълумотларни ўзгартириш принципларини, усулларини ва воситаларини бирлаштирувчи билим соҳаси.	-field of knowledge which unites the principles, methods and means of transformation of data with the purpose to disguise contents of information, to prevent possibility of its interception and information distortion, to protect from unauthorized access to information.
29.	**Луғатга асосланган хужум**	– криптотизимга очиқ матн элементлари луғатидан фойдаланишга асосланган	- attack on the cryptosystem that uses a dictionary of text elements

	With a dictionary Attack	ҳужум.	open.
30.	**Махфий ахборот Confidential Information**	– таркибида давлат сирига оид маълумотлар бўлган ахборот.	— information containing data, carried to secret state.
31.	**Маълумотлар** **Data**	– одам иштироки билан ёки автоматик тарзда узатишга, изоҳлашга ёки ишлашга яроқли, формаллашган кўринишда ифодаланган ахборот.	- information presented in a formalized manner suitable for communication, interpretation or processing involving human or automated means.
32.	**Очиқ ахборот Open Information**	– барча манфаатдор шахсларнинг фойдаланишлари бўйича чеклаш бўлмаган ахборот: умумфойдаланувчи ахборот.	— information which doesn't have restrictions on access to it all interested persons: information public.
33.	**Паролни бузиб очиш** **Password cracking**	- ахборот тизимидан (тармоғидан) яширинча фойдаланиш техникаси (усули) бўлиб, унда ҳужум қилувчи тараф паролларни фош қилувчи ёрдамида паролларни аниқлашга (танлашга) ёки ўғирлашга уриниб кўради.	- tech (method) secretly to access the system (network) information, in which the attacker using opener tries to guess passwords (pick) or steal passwords.
34.	**Пассив ҳужум** **Passive Attack**	– криптотизмга ёки криптографик протоколга ҳужум бўлиб, бунда душман ва/ёки бузғунчи узатилувчи шифрланган ахборотни кузатади ва ишлатади, аммо қонуний фойдаланувчилар ҳаракатига таъсир этмайди.	- an attack on a cryptosystem or cryptographic protocol in which the offender or the enemy and observes and uses the transmitted encrypted messages, but does not affect the actions

			of legitimate users.
35.	**Протокол** **Protocol**	- қурилмалар, дастурлар, маълумотларларни ишлаш тизимлари, жараёнлар ёки фойдаланувчиларнинг ўзаро ҳаракати алгоритмини белгиловчи қоидалар мажмуи.	- set of rules, defining algorithm of interaction devices, software, data processing systems, processes, or users.
36.	**Рақамли имзо** **Digital signature**	- аутентификацияни таъминлаш учун манба томонидан тақдим этилувчи қўшимча ахборот. Маълумотларни блокига ёки унинг криптографик ўзгартирилиши натижасига қўшиладиган маълумотлар кетма-кетлиги маълумотларни қабул қилувчига манбанинг ва маълумотлар блокини яхлитлигини текширишга ҳамда сохталаштиришдан ҳимоялашга имкон беради.	- Additional information provided by the source to provide authentication. Sequence data that is added to the data or the result of its cryptographic transformation of data that allows the recipient to verify the source and integrity of the data block, as well as protection against fraud or forgery.
37.	**Рухсатсиз фойдланиш Unauthorized access**	- ҳимоя объектидан регламентланган фойдаланишнинг бузилиши.	- violation of regulated access to the object of protection.
38.	**Симметрик шифр** **Symmetric cipher**	- шифрлаш ва расшифровка қилиш учун айнан бир калитдан ёки бири орқали бошқаси осонгина аниқлаши мумкин бўлган турли калитлардан фойдаланувчи шифр.	- a cipher is used for encryption and decryption one and the same key or a different key, such that one of them can be easily obtained by another.
39.	**Тармоқ хавфсизлиги**	- ахборот тармоғини рухсатсиз фойдаланишдан, меъёрий ишлашига	- measures that protect the network information from unauthorized access,

	Network Security	тасодифан ёки атайин аралашишдан ёки тармоқ компонентларини бузишга уринишдан эхтиёт қилувчи чоралар. Асбоб-ускуналарни, дастурий таъминотни, маълумотларни ҳимоялашни ўз ичига олади.	accidental or intentional interference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.
40.	**Тармоқлараро экран** **Firewall**	– аппарат-дастурий воситалар ёрдамида тармоқдан фойдаланишни марказлаштириш ва уни назоратлаш йўли билан тармоқни бошқа тизимлардан ва тармоқлардан келадиган хавфсизликка таҳдидлардан ҳимоялаш усули. Яна - бир неча компонентлардан (масалан, брандмауэр дастурий таъминоти ишлайдиган маршрутизатор ёки шлюздан) ташкил топган химоя тўсиғи ҳисобланади.	- 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).
41.	**Таҳдид турлари Types of Threats**	- таҳдидларни тасодифан ва атайинларига, актив ва пассивларига таснифлаш мумкин.	- threats can be classified into random and deliberate and can be active or passive.
42.	**Тизим хавфсизлиги** **System Security**	- ресурсларидан ва функциональ имкониятларидан ҳамда ишлашида турли башорат қилинадиган ёки қилинмайдиган ҳолатлар сабаб бўлувчи бўлиши мумкин бўлган	- the security of the system from unauthorized use of its resources and capabilities, as well as possible violations of its functioning caused by various predictable and unpredictable

		бузилишлардан тизимнинг ҳимояланиши.	circumstances.
43.	**Ўзаро аутентификация** **Mutual Authentication**	– тарафларни аутентификациялаш варианти бўлиб, тарафларнинг ҳар бири у билан ўзаро ҳаракатдаги тарафнинг хақиқатан ўзи эканлигини текширади. Ўзаро аутентификацияни амалга оширувчи протоколнинг иштирокчиларининг ҳар бири бир вақтда ҳам исботловчи, ҳам текширувчи ҳисобланади. Бу протокол бажарилишнинг бир сеансида ҳар бир иштирокчининг иккинчи иштирокчига айнан ўзи эканлигини исботлашига имкон беради.	- authentication Option parties in which each party verifies that interacting with her party - namely that for which he is. A. implemented in such a protocol identification, in which each participant is both prove-down and inspection. This allows a single session the protocol of each participant to another participant to prove their identity.
44.	**Фаол тахдид** **Active threat**	– тизим ҳолатига атайин рухсатсиз ўзгартириш киритиш таҳдиди.	- the threat of a deliberate unauthorized system state changes.
45.	**Фаол хужум** **Attack active**	- криптотизимга ёки криптографик протоколга ҳужум бўлиб, унга биноан душман ва/ёки бузғунчи конуний фойдаланувчи харакатига таъсир этиши, масалан, қонуний фойдаланувчи хабарини алмаштириши ёки йўқ қилиши ва хабарни яратиб унинг номидан узатиши ва ҳ. мумкин.	- attack on a cryptosystem or cryptographic protocol in which the offender or the enemy and can affect the legitimate user actions, for example, replace or remove legitimate posts, create and send messages on his behalf, etc.

46.	**Физик ҳимоялаш** **Physical protection**	– ресурсларни атайин қилинадиган ёки тасодифий тахдидлардан физик ҳимоялашни таъминлаш учун ишлатиладиган воситалар.	— the means used for ensuring physical protection of resources from threat deliberate or casual.
47.	**Фойдаланишни бошқариш** **Access control**	- фойдаланувчиларнинг, дастурларнинг ва жараёнларнинг маълумотлардан, ҳисоблаш техникаси дастурлари ва қурилмаларидан фойдаланишларини белгилаш ва чеклаш.	- define and limit user access, programs, and processes the data, programs, and devices of the computer system.
48.	**Фойдалувчанлик** **Availability**	- авторизацияланган мантиқий объект сўрови бўйича мантиқий объектнинг тайёрлик ва фойдаланувчанлик ҳолатида бўлиши хусусияти.	- property of an object in a state of readiness and usage upon request authorized entity.
49.	**Хавф- хатар тахлили** **Risk analysis**	- номувофик ҳодисалар пайдо бўлиш ҳолида кутиладиган зарарни аниқлаш мақсадида, эҳтимоллик ҳисоблашлардан фойдаланиб, тизим характеристикаларини ва салбий томонларини ўрганиш жараёни. Хавф – хатарни таҳлиллаш масаласи у ёки бу хавф – хатарнинг мақбуллик даражасини аниқлашдан иборат.	- the process of studying the characteristics and weaknesses of the system, conducted using a probabilistic calculations in order to determine the expected damage in case of adverse events. The task of risk analysis is to determine the acceptability of a risk to the system.
50.	**Хавфсиз операцион тизим**	– маълумотлар ва ресурслар мазмунига мос ҳимоялаш даражасини таъминлаш мақсадида аппарат ва	- an operating system that effectively manages the hardware and software to provide the level of

	Secure operating system	дастурий воситаларни самарали бошқарувчи операцион тизим.	protection corresponding to the content data and resources.
51.	**Хавфсизлик** **Security**	- таъсири натижасида номақбул ҳолатларга олиб келувчи атайин ёки тасодифан, ички ва ташқи бекарорловчи 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 ҳолат.	- 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.
52.	**Хавфсизлик аудити** **Security audit**	– компьютер тизими хавфсизлигига таъсир этувчи бўлиши мумкин бўлган хавфли ҳаракатларни характерловчи, олдиндан аниқланган ҳодисалар тўпламини рўйхатга олиш(аудит файлида қайдлаш) йўли билан ҳимояланишни назоратлаш.	– 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 safety.
53.	**Хавфсизлик сиёсати** **Security policy**	– муайян ташкилотда махфий ахборотни ёки чекланган доирадаги фойдаланувчиларга мўлжалланган ахборотни олиш, ишлаш, узатиш бўйича қабул қилинган бошқариш сиёсати.	- adopted in the organization management policy acquisition, processing, transmission of classified information, or information on their limits calculated range of users.

54.	**Хакер** **Hacker**	- тизимли дастурий таъминотга, кўпинча ноқонуний ўзгартиришлар киритишга уринувчи фойдаланувчи. Одатда ёмон ҳужжатланган ва баъзида ножоиз қўшимча натижалар туғдирувчи озми-кўпми фойдали ёрдамчи дастурлар яратувчи дастурини хакер деб аташ мумкин.	- a user who is trying to make changes to system software, often without the right to do. Hacker can be called the programmer, which creates a more or less useful software tools, are usually poorly documented and sometimes cause unwanted side effects.
55.	**Хеш-функция** **Hash function**	- чекли алфавитдаги узунлиги чекли кириш йўли сўзини берилган, одатда қатъий узунликдаги, сўзга акслантириш функцияси.	- a function that displays the input word of finite length in a finite alphabet in a given word, usually a fixed length.
56.	**Ҳимоялаш** **Protection**	- ҳисоблаш тизимидан ёки унинг қисмидан фойдаланишни чеклаш воситаси; аппаратурадан, дастурдан ва маълумотлардан рухсатсиз фойдаланишни бартараф этувчи ташкилий ва техник, жумладан, дастурий чоралар.	- 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.
57.	**Ҳужум** **Attack**	– босқинчининг операцион муҳитини бошқаришига имкон берувчи ахборот тизими хавфсизлигининг бузилиши.	- breach of security of information system, which allows the invader to manage operating environment.
58.	**Шифрлаш алгоритми** **Encryption algorithm**	- шифрлаш функциясини амалга оширувчи криптографик алгоритм. Блокли шифртизим ҳолида шифрлашнинг муайян режимида шифрлашнинг	- a cryptographic algorithm that implements the encryption function. It is created using base block algorithm for exact encryption mode in block

		базавий блокли алгоритмидан фойдаланиб ҳосил қилинади.	cipher.
59.	**Шифрматн Ciphertext**	- очиқ матнни шифрлаш натижасидаги олинган матн.	- the text resulting from encryption of the plaintext.

VIII. БЎЛИМ

АДАБИЁТЛАР РЎЙХАТИ

VIII. АДАБИЁТЛАР РЎЙХАТИ

Махсус адабиётлар

1. Stamp Mark. Information security: principles and practice. USA, 2011.
2. Peter Stavroulakis, Mark Stamp. Handbook of Information and Communication Security. 2010.
3. Ганиев С.К., Каримов М.М., Тошев К.А. Ахборот хавфсизлиги. 2008.
4. Акбаров Д. Е. “Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши” – Тошкент, 2008 – 394 бет.
5. Ахмедова О.П., Хасанов Х.П., Назарова М.Ҳ., Нуритдинов О.Д.. Криптографик протоколлар. Тошкент, 2012 – 187 бет.
6. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim. Wireless Network Security:Vulnerabilities, Threats and Countermeasures. School of Multimedia, Hannam University, Daejeon, Korea. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008.
7. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: издательство ТРИУМФ, 2003 - 816 стр.
8. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. 2005.
9. Michael Sikorski, Andrew Honig. Practical malware analysis. 2012.
10. ESA Board for Software Standardisation and Control. Java coding Standards. 2005.

Интернет ресурслар

1. http://www.tuit.uz
2. http://en.wikipedia.org/wiki/GSM
3. http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
4. https://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria
5. https://en.wikipedia.org/wiki/Common_Criteria
6. https://en.wikipedia.org/wiki/ISO/IEC_27001:2005
7. https://ru.wikipedia.org/wiki/SSL
8. https://technet.microsoft.com/en-us/library/dd277395.aspx
9. http://ictnews.uz/api/news/78
10. https://en.wikipedia.org/wiki/IPsec

EXPERT CONCLUSION

TO THE EDUCATIONAL-METHODOLOGICAL COMPLEX FOR THE COURSE OF RETRAINING PEDAGOGUE CADRES OF HIGHER EDUCATION INSTITUTIONS IN THE DIRECTION OF "COMPUTER ENGINEERING"

The educational-methodological complex was developed in accordance with defined requirements. Educational-methodological complex by "Computer Engineering" direction consist of following 6 modules: E-government, Embedded Systems, Multimedia Technologies, Linux OS, Information Security, Forming Electronic Education Environment.

Besides that, it consists of the:

- syllabus;
- theoretical and practical materials;
- assessment;
- presentations on every topic;
- glossary;
- tests;
- list of references.

The syllabus is written correctly. The sequence of topics proposed for study, focused on high-quality learning. Calendar-thematic plan corresponds to its content of the working program on discipline. Tests are various; allow to adequately assess the level of teachers' knowledge on the subject. Methodical recommendations for practical exercises provide the formation of basic skills to carry out research in the process of scientific knowledge and the theoretical foundation of professional tasks.

Slides support lecture materials are accurate and specific, it promotes better assimilation of discipline.The presented educational-methodical complexes in the direction of "Computer Engineering" informative, has a practical orientation, includes a sufficient number of diverse elements aimed at developing the mental and creative abilities of students.

In general, educational-methodological complexes of the direction of "Computer Engineering" promotes quality possession teachers professional competence.

Vice rector of ICT, TUIT Chul Soo LEE