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

“Тасдиқлайман”
Тармоқ маркази директори
_____ Х.М.Холмедов
“_____”_____ 2015 йил

“КОМПЬЮТЕР ТИЗИМЛАРИ, ТАРМОҚЛАРИ ВА АХБОРОТ ХАВФСИЗЛИГИ” МОДУЛИ БЎЙИЧА

Ў Қ У В –У С Л У Б И Й М А Ж М У А

Тузувчи: **Иргашева Д.Я.** – “Ахборот хавфсизлиги” кафедраси мудири, техника фанлар номзоди

Тошкент – 2015

МУНДАРИЖА

ИШЧИ ДАСТУР

Кириш

Ҳисоблаш техникасида хавфсизлик тушунчаси жуда кенг тушунчадир. Бу тушунча замирида компъютерларнинг ишончли ишлаши, қимматли маълумотларни асраш, ахборотларни ёмон ниятли шахслар томонидан ўғирланиши ёки ўзгартирилишидан сақлаш ва бошқа муаммолар ётади. Барча ривожланган мамлакатларда ахборот-коммуникация технологияларининг хавфсизлигининг ҳимоясида қонунлар туради, лекин ҳисоблаш техникасида бу ҳимоя хуқуқшунослик тажрибасида ҳали етарлича ривожланган эмас.

Ҳозирда барча ташкилотларда ахборот-коммуникация технологияларини татбиқ этиш, улардан кенг фойдаланиш кенг йўлга қўйилган. Бу ташкилотларнинг ички тармоғи Интернет тармоғига уланганидан сўнг кибер-ҳужумлар учун энг яхши нишон бўлиб хизмат қилиши мумкин. Тизим ва ахборотларни хавфсизлигини таъминлаш мақсадида ҳар бир ташкилот ички назоратни ва аудитини ўтказиш катта аҳамият касб этади.

Ахборотлар ва ахборотлар тизимидан фойдаланиш инсоният фаолиятининг барча соҳаларига кириб бориб, муҳим аҳамият касб этиб, ривожланиб бораётган бугунги жамиятда ахборотларни мақсадли бошқариш фаоллашмоқда. Компьютерлар ва компьютер тизимлари ахборотлар тизимининг муҳим бўғимидир. Интернет тармоқлари жамият фаолиятининг барча соҳаларини қамраб олиб, ахборотларни тез ва сифатли алмашинувини таъминлаш жараёнлари технологияларини ривожланишига ижобий манба бўлиб келмокда. Юқоридаги келтирилган асосли мулоҳазалардан келиб чиқиб, ахборотларни асли ҳолидан ўзгартирилган ҳолда, яъни шифрланган ҳолда, сақлаш ва узатиш масалаларининг муҳим эканлигига шубха йўқдир.

Ушбу дастурда комплекс ахборот хавфсизлигини таъминлаш билан боғлиқ масалаларни ечишда компьютер тизимлари ва тармоқларида ахборотни ҳимоялаш технологияларининг ўрни каби масалалари баён этилган.

Модулнинг мақсади ва вазифалари

“Компьютер тизимлари, тармоқлари ва ахборот хавфсизлиги” модулининг мақсади: ахборот-коммуникация тизимлари ва тармоқлари ҳимоясини самарадорлигини ошириш, компьютер тизимлари ва тармоқларида ахборот ҳимоясининг воситаларини таҳлил этиш, баҳолаш кўникма ва малакаларини таркиб топтириш.

“Компьютер тизимлари, тармоқлари ва ахборот хавфсизлиги” модулининг вазифалари:

- компьютер тизимлари ва тармоқларида ахборот ҳимоясининг масалаларига илмий ёндашиш, уни таълим-тарбия жараёнида аҳамияти ва

тингловчиларда уларни аниқ илмий назарий таҳлил қилиш, холис баҳолашни вужудга келтиришга эришиш;

- компьютер тизимлари ва тармоқларида ахборот хавфсизлигини таъминлаш, уни қўлланиш соҳаси ҳамда ахборотни ҳимоялаш тизимлари бўйича кўникма ва малакаларини шакллантириш;
- соҳада эришилган ютуқларни олий таълим тизими билан боғлиқ ҳолда муаммоларни ҳал этиш стратегияларини ишлаб чиқиш ва амалиётга татбиқ этишга ўргатиш.

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

“Компьютер тизимлари, тармоқлари ва ахборот хавфсизлиги” курсини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида**:**

Тингловчи:

- компьютер тизимлари ва тармоқлари тушунчаси;
- компьютер тизимлари ва тармоқларидан фойдаланиш қонун қоидалари;
- компьютер тизимлари ва тармоқлари соҳасида юзага келадиган муаммолар ва уларни ҳал этиш стратегиялари;
- давлат фаолиятининг турли соҳаларида компьютер тизимлари ва тармоқларида ахборотни ҳимоялашнинг принциплари ва усуллари бўйича **билимларга эга бўлиши**;

Тингловчи:

- ахборот хавфсизлиги таъминотининг зарурий технология ва ҳимоя воситаларини танлаш;
- ахборот чиқиб кетадиган ташкилий ва техник каналларни аниқлаш;
- ташкилот хавфсизлиги сиёсатини яратиш;
- тармоқ ҳужумлари ва уларнинг турларини аниқлаш **кўникмаларини эгаллаши;**

Тингловчи:

- компьютер тизимлари ва тармоқлари ҳимоясини ишлаб чиқиш;
- ҳимоя воситаларини ишлаб чиқишга доир муаммоларни аниқлаш;
- ҳимоя воситаларини амалда тўғри қўллаш;
- компьютер тармоқларида аутентификациялаш ва идентификациялаш протоколлари, парол тизимлари орқали рухсат этилганликни чегаралаш;
- компьютер тизимлари ва тармоқларини рухсатсиз ўзгартиришлардан ҳимоялаш;
- компьютер тизимлари ва тармоқлари ҳимоя таъминотининг зарурий технология ва ҳимоя воситаларини такомиллаштириш бўйича таклифлар бериш;
- компьютер тизимлари ва тармоқлари зарурий технология ва ҳимоя воситаларини баҳолаш бўйича **малакаларини эгаллаши;**

Тингловчи:

- компьютер тизимлари тармоқларида ахборот хавфсизлигини таъминловчи комплекс тизимини қуриш;
- ахборот хавфсизлиги таъминлашда аутентификациялаш ва идентификациялаш протоколларидан фойдаланиш;
- ахборотни ҳимоялаш ҳамда тармоқ ҳимоясида қўлланиладиган воситалар ва усулларидан фойдаланиш;
- ҳимояланган компьютер тизимлари ва тармоқларини қуриш;
- ҳимоя воситаларини ишлаб чиқишга доир жараёнини бошқариш;
- ҳимоя воситаларини амалда тўғри қўллаш бўйича хулосалар бериш;
- компьютер тизимлари ва тармоқлари ҳимоя таъминотининг зарурий технология ва ҳимоя воситалари асосида қарорлар қабул қилиш **компетенцияларни эгаллаши лозим.**

Модулни ташкил этиш ва ўтказиш бўйича тавсиялар

"**Компьютер тизимлари, тармоқлари ва ахборот хавфсизлиги**" курси маъруза ва амалий машғулотлар шаклида олиб борилади.

Курсни ўқитиш жараёнида таълимнинг замонавий усуллари, ахборот-коммуникация технологиялари қўлланилиши назарда тутилган:

- маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион материаллардан;
- ўтказиладиган амалий машғулотларда техник воситалардан, тест сўровлари, ақлий ҳужум ва бошқа интерактив таълим усулларини қўллаш назарда тутилади.

Модулнинг ўқув режадаги бошқа модуллар билан боғлиқлиги ва узвийлиги

"**Компьютер тизимлари, тармоқлари ва ахборот хавфсизлиги**" модули мазмуни ўқув режадаги "Криптография усуллари" ҳамда "Симсиз алоқа тизимларида ахборот ҳимояси" ўқув модули билан узвий боғланган ҳолда педагогларнинг меъёрий - ҳуқуқий хужжатлар бўйича касбий педагогик тайёргарлик даражасини орттиришга хизмат қилади.

Модулнинг олий таълимдаги ўрни

Модулни ўзлаштириш орқали тингловчилар ахборот-коммуникацион тизимларида криптографик ҳимоялаш усулларини ўрганиш, уларни таҳлил этиш, амалда қўллаш ва 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.	Компьютер тармоқларида ахборот ҳимоясининг асосий хусусиятлари. Компьютер тизимлари ва тармоқларидаги ахборот ҳимоясининг муаммолари.	4	4	2	2	-
2.	Компьютер тизимлари ва тармоқларига бўладиган тахдидлар. Тармоқ хужумлари ва уларнинг турлари.	4	4	2	2	-
3.	Компьютер тизимлари ва тармоқларини рухсатсиз ўзгартиришлардан ҳимоялаш усуллари.	2	2	-	2	-
4.	Компьютер тизимлари ва тармоқларида ахборот ҳимоясининг комплексли ёндашуви. Компьютер тизими ва тармоғининг архитектураси ва унинг қисм тизимлари.	2	2	-	2	-
5.	Компьютер тизимлари ва тармоқларини рухсатсиз ўзгартиришлардан ҳимоялаш воситалари.	2	2	-	2	-
6.	Компьютер тизимлари ва тармоқларини рухсатсиз фойдаланишлардан ҳимоялаш.	2	2	-	2	-
7.	Ҳимояланган компьютер тизимлари ва тармоқларини қуриш концепцияси.	6	4	-	4	2
8.	Компьютер тизимлари тармоқларида ахборот хавфсизлигини таъминловчи комплекс тизимни қуриш.	6	4	-	4	2
	ЖАМИ:	**28**	**24**	**4**	**20**	**4**

НАЗАРИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-Мавзу: Компьютер тармоқларида ахборот ҳимоясининг асосий хусусиятлари. Компьютер тизимлари ва тармоқларидаги ахборот ҳимоясининг муаммолари. (2 соат)

Режа:

1. Компьютер тизимлари ва тармоқларидаги ахборот ҳимояси.
2. Ахборотни ҳимоялаш концепцияси.

2-Мавзу: Компьютер тизимлари ва тармоқларига бўладиган тахдидлар. Тармоқ хужумлари ва уларнинг турлари. (2 соат)

Режа:

1. Ахборот хавфсизлигида ҳимоя вазифалари.
2. Ташкилотлардаги ахборотларни ҳимоялаш ва ҳимоялаш тизимининг комплекслилиги.
3. Ахборотларни ташкилий ҳимоялаш элементлари.

АМАЛИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-Мавзу: Компьютер тармоқларида ахборот ҳимоясининг асосий хусусиятлари. Компьютер тизимлари ва тармоқларидаги ахборот ҳимоясининг муаммолари

Режа:

1. Компьютер тармоқларининг хусусиятлари.
2. Ахборотларни узатиш протоколлари.

2-Мавзу: Компьютер тизимлари ва тармоқларига бўладиган тахдидлар. Тармоқ хужумлари ва уларнинг турлари

Режа:

1. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар.
2. Тармоқдаги ахборотга бўладиган намунавий ҳужумлар.

3-Мавзу: Компьютер тизимлари ва тармоқларини рухсатсиз фойдаланишлардан ҳимоялаш усуллари

Режа:

1. Internetда рухсатсиз кириш усулларининг таснифи;
2. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши;
3. Тармоқлараро экран ва унинг вазифалари;
4. Тармоқлараро экраннинг асосий компонентлари.

4-Мавзу. Компьютер тизимлари ва тармоқларида ахборот ҳимоясининг комплексли ёндашуви.Компьютер тизими ва тармоғининг архитектураси ва унинг қисм тизимлари

Режа:

1. Компьютер тармоқларининг архитектураси.
2. Ўзаро алоқада бўлган жараёнларнинг ҳақиқий эканлигини тасдиқлаш.
3. Коммуникацион қисм тармоқ орқали олинувчи ахборотнинг хақиқийлигини тасдиқлаш.

5-Мавзу: Компьютер тизимлари ва тармоқларини рухсатсиз ўзгартиришлардан ҳимоялаш воситалари

Режа:

1. Компьютер тизимлари ва тармоқларида хавфсизлик ҳолатини текшириш дастури;
2. Компьютер тизимлари ва тармоқларида маълум бўлган заифликлар ва тармоқ воситаларини текшириш дастурлари.

6-Амалий машғулот. Компьютер тизимлари ва тармоқларини рухсатсиз фойдаланишлардан ҳимоялаш

Режа:

1.Фойдаланувчи қисм тизимда ва ихтисослаштирилган коммуникацион компьютер тизимларида ахборот хавфсизлигини таъминлаш.

2.Компьютер телефониясидаги ҳимоялаш усуллари

7-Мавзу: Ҳимояланган компьютер тизимлари ва тармоқларини қуриш концепцияси (4-соат)

Режа:

1. Ҳимояланган компьютер тизимлари ва тармоқларини бошқаришнинг функционал масалалари;
2. Хавфсизлик воситаларини бошқариш архитектураси.

8-Мавзу: Компьютер тизимлари тармоқларида ахборот хавфсизлигини таъминловчи комплекс тизимни қуриш (4-соат).

Режа:

1. Ахборот тизимларининг аудити ва мониторинги.
2. Хавф-хатарларни тахлиллаш ва бошқариш.
3. Ахборот хавфсизлиги тизимини қуриш методологияси.

МУСТАҚИЛ ТАЪЛИМ
Мустақил ишни ташкил этишнинг шакли ва мазмуни

Тингловчи мустақил ишни муайян модулни хусусиятларини ҳисобга олган ҳолда қуйидаги шакллардан фойдаланиб тайёрлаши тавсия этилади:

- 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.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

I. Раҳбарий адабиётлар.

1. Каримов И.А. Ўзбекистон ўз истиқлол ва тараққиёт йўли. –Т.: Ўзбекистон, 1992. -22 б.
2. Каримов И.А. Биздан озод ва обод Ватан қолсин. –Т.: Ўзбекистон, 1994. Т.2. -380 б.
3. Каримов И.А. Янгича фикрлаш ва ишлаш – давр талаби. –Т.: Ўзбекистон, 1997. Т.5. -384 б.
4. Каримов И.А. Хавфсизлик ва тинчлик учун курашмоқ керак. – Т.: Ўзбекистон, 2002. Т.10. -432 б.

II. Меъёрий- ҳуқуқий хужжатлар.

1. Ўзбекистон Республикасининг Конституцияси. (Ўн иккинчи чақириқ Ўзбекистон Республикаси Олий Кенгашининг ўн биринчи сессиясида 1992 йил 8 декабрда қабул қилинган Ўзбекистон Республикасининг 1993 йил 28 декабрдаги, 2003 йил 24 апрелдаги, 2007 йил 11 апрелдаги, 2008 йил 25 декабрдаги, 2011 йил 18 апрелдаги, 2011 йилдаги 12 декабрдаги, 2014 йил 16 апрельда қабул қилинган қонунларига мувофиқ киритилган ўзгартиш ва қўшимчалар билан) –Т., 2014.
2. Ўзбекистон Республикасининг “Таълим тўғрисида”ги Қонуни. Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 1997 йил. 9-сон, 225-модда.
3. Кадрлар тайёрлаш миллий дастури. Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 1997 йил. 11-12-сон, 295-модда.

4. Ўзбекистон Республикаси Президентининг 2010 йил 28 июлдаги “Таълим муассасаларининг битирувчиларини тадбиркорлик фаолиятига жалб этиш борасидаги қўшимча чора-тадбирлар тўғрисида”ги Фармони.

5. Ўзбекистон Республикаси Президентининг 2010 йил 2 ноябрдаги “Олий малакали илмий ва илмий-педагогик кадрлар тайёрлаш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПҚ-1426-сонли Қарори.

6. Ўзбекистон Республикаси Президентининг 2011 йил майдаги “Олий таълим муассасаларининг моддий-техник базасини мустаҳкамлаш ва юқори малакали мутахассислар тайёрлаш сифатини тубдан яхшилаш чора-тадбирлари тўғрисида”ги ПҚ-1533- сонли Қарори.

7. Ўзбекистон Республикаси Президентининг 2012 йил 24 июлдаги “Олий малакали илмий ва илмий-педагог кадрлар тайёрлаш ва аттестациядан ўтказиш тизимини янада такомиллаштириш тўғрисида”ги ПФ–4456-сон Фармони.

8. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2012 йил 28 декабрдаги “Олий ўқув юртидан кейинги таълим хамда олий малакали илмий ва илмий педагогик кадрларни аттестациядан ўтказиш тизимини такомиллаштириш чора-тадбирлари тўғрисида”ги 365- сонли Қарори.

III. Махсус адабиётлар.

1. С.К.Ғаниев, М.М. Каримов, К.А. Тошев «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

3. Столинс, Вильям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.-М.: Издательский дом «Вильямс», 2002. 432 с.

4. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

5. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.

6. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.

7. Широчин В.П. Мухин В.Е., Кулик А.В. Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях.- К.:, «ВЕК+», 2000. 112 с.

8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство ТРИУМФ, 2003 – 816 с.

МАЪРУЗА МАТНЛАРИ

1-Мавзу: Компьютер тармоқларида ахборот ҳимоясининг асосий хусусиятлари. Компьютер тизимлари ва тармоқларидаги ахборот ҳимоясининг муаммолари (2 соат)

Режа:

1. Компьютер тизимлари ва тармоқларидаги ахборот ҳимояси.
2. Ахборотни ҳимоялаш концепцияси.

Калит сўзлар: Ахборот, ахборот ҳимояси, ахборот хавфсизлиги, компьютер тизимлари, компьютер тармоқлари, хавф, хавфсизлик сиёсати, ҳимоялаш концепцияси.

1. Компьютер тизимлари ва тармоқларидаги ахборот ҳимояси.

Компьютер тизимларининг кенг кўламда ишлатилиши доимо ўсиб борувчи ахборот хажмини ишлаш жараёнларини автоматлаштиришга имкон берсада, бу жараёнларни агрессив таъсирларга нисбатан ожиз қилиб қўяди ва, демак, ахборот технологиялардан фойдаланувчилар олдида янги муаммо-*ахборот хавфсизлик* муаммоси кўндаланг бўлди. Хавфсизлик муаммоси, аслида, янги муаммо эмас, чунки хавфсизлигини таъминлаш хар қандай тизим учун, унинг мураккаблиги, табиатидан қатъий назар, бирламчи вазифа ҳисобланади. Аммо, ҳимояланувчи объект ахборот тизими бўлса, ёки агрессив таъсир воситалари ахборот шаклда бўлганда, ҳимоянинг мутлоқ янги технологияларини ва усулларини яратишга тўғри келади. Маълумотларни ҳимояловчи усуллар хамда хакерларга қарши харакат воситалар мажмуасини белгилаш мақсадида *компьютер хавфсизлиги* атамаси ишлатила бошланди.

Маълумотларни ишловчи тақсимланган тизимларнинг пайдо бўлиши хавфсизлик масаласига янгича ёндашишнинг шаклланишига олиб келди. Маълумки, бундай тизимларда тармоқлар ва коммуникацион ускуналар фойдаланувчиларнинг терминаллари билан марказий компьютерлар ўртасида маълумотлар алмашишга хизмат қилади. Шу сабабли маълумотлар узатилувчи тармоқларни химоялаш зарурияти туғилди ва шунинг билан бирга *тармоқ хавфсизлиги* атамаси пайдо бўлди.

Ахборотнинг мухимлик даражаси қадим замонлардан маълум. Шунинг учун ҳам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири – сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат – сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденциялари ва разведка миссияларидан ташқарига чиқмаган. Фақат *бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар, сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари*

уни ўгирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади.

Ахборотни ҳимоя қилиш деганда:

- *Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йўқ қилинишига йўл қўймаслик;*
- *Ахборотнинг бутунлигини сақлаб қолган ҳолда, уни элементларини қалбакилаштиришга (ўзгартиришга) йўл қўймаслик;*
- *Ахборотни тегишли ҳуқуқуларга эга бўлмаган шахслар ёки жараёнлар орқали тармоқдан рухсат этилмаган холда олишга йўл қўймаслик;*
- *Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар фақат томонлар ўртасида келишилган шартномалар асосида қўлланилишига ишониш кабилар тушунилади.*

Юқорида таъкидлаб ўтилганларнинг барчаси асосида компьютер тармоқлари ва тизимларида ахборот хавфсизлиги муаммосининг долзарблиги ва муҳимлиги келиб чиқади. Компьютер тизимлари ва тармоқларида ахборотни ҳимоя остига олиш деганда, берилаётган, сақланаётган ва қайта ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш мақсадида турли восита ва усулларни қўллаш, чораларни кўриш ва тадбирларни амалга оширишни тушуниш қабул қилинган.

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

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

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

3. Ҳимоя воситаларидан барча қарши чоралар мажмуасини ҳисобга олган ҳолда фойдаланиш лозим.

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

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

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

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

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

***Ахборот хавфсизлиги** деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади. Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва хужжатларни ўғирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компьютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир.* Булардан ташқари, бу харакатлардан моддий фойда олишга интилиш ҳам ривожланди.

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

Ахборотни ҳимоялашнинг мақсадлари қуйидагилардан иборат:

- ахборотнинг келишувсиз чиқиб кетиши, ўғирланиши, йўқотилиши, ўзгартирилиши, сохталаштирилишларнинг олдини олиш;

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

- ахборотни йўқ қилиш, ўзгартириш, сохталаштириш, нусха кўчириш, тўсиқлаш бўйича рухсат этилмаган харакатларнинг олдини олиш;

- хужжатлаштирилган ахборотнинг миқдори сифатида хуқуқий тартибини таъминловчи, ахборот захираси ва ахборот тизимига хар қандай ноқонуний аралашувларнинг кўринишларининг олдини олиш;

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

- давлат сирини, қонунчиликка мос хужжатлаштирилган ахборотнинг конфиденциаллигини сақлаш;

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

2. Ахборотни ҳимоялаш концепцияси.

Илмий ва амалий текширишлар натижаларини умумлаштириш натижасида ахборотларга нисбатан хавф хатарларни қуйидагича таснифлаш мумкин.

Хавфсизлик сиёсатининг энг асосий вазифаларидан бири ҳимоя тизимида потенциал хавфли жойларни кидириб топиш ва уларни бартараф этиш хисобланади. Текширишлар шуни кўрсатадики, тармоқдаги энг катта хавфлар — бу рухсатсиз киришга мўлжалланган махсус дастурлар, компьютер вируслари ва дастурнинг ичига жойлаштирилган махсус кодлар бўлиб, улар компьютер тармоқларининг барча объектлари учун катта хавф туғдиради.

Компьютер тармоқларини ҳимоялаш уйда фойдаланувчи компьютер-ларни ҳимоялашдан фарқланади (гарчи индивидуал ишчи станцияларни ҳимоялаш-тармоқ ҳимоясининг ажралмас қисми). Чунки, аввало, бундай масала билан саводли мутахассислар шуғулланадилар. Шу билан бирга корпоратив тармоқ хавфсизлиги тизимининг асосини четки фойдаланувчилар учун ишлаш қулайлиги ва техник мутахассиларга қуйиладиган талаблар ўртасида муросага етишиш ташкил этади.

Компьютер тизимига икки нуқтаи назардан қараш мумкин: унда фақат ишчи станциялардан фойдаланувчиларни кўриш мумкин, ёки фақат тармоқ операцион тизимининг ишлашини ҳисобга олиш мумкин.

Симлар бўйича ўтувчи ахборотли пакетлар мажмуини ҳам компьютер тармоғи дейиш мумкин. Тармоқни ифодалашнинг бир неча сатҳлари мавжуд. Худи шундай тармоқ хавфсизлиги муаммосига турли сатҳларда ёндашиш мумкин. Мос ҳолда ҳар бир сатҳ учун ҳимоялаш усули турлича бўлади. Тизимнинг ишончли ҳимояланиши ҳимояланган сатҳлар сони билан белгиланади.

Биринчи, кўриниб турган ва амалда энг қийин йўл-ходимларни тармоқ хужумларини қийинлаштирувчи хатти-ҳаракатга ўргатиш. Бу бир қарашда осондай туюлсада, аммо мушкул иш. Internet дан фойдаланишни чегаралаш лозим.

Аксарият фойдаланувчилар чегараланишлар сабабини билмайдилар. Шунинг учун тақиқилар аниқ ифодаланиши лозим.

Компьютер тармоқлари ахборотини ҳимоялашга ҳимоялаш тадбирларининг ягона сиёсатини ҳамда ҳуқуқий, ташкилий-маъмурий ва инженер-техник характерга эга чоралар тизимини ўтказиш орқали эришилади.

Тармоқда ахборотни ҳимоялашнинг зарурий даражасини ишлаб чиқишда ходимлар ва раҳбариятнинг ўзаро жавобгарлиги, шахс ва ташкилот манфаатларига риоя қилиш, хуқуқни муҳофаза қилувчи органлар билан ўзаро алоқа ҳисобга олинади. Рақобатли шароитда хизматларнинг катта сонини тақдим этиш ва хизмат қилиш вақтини қисқартириш орқали етакчи ўринни сақлаб қолиш ва янги мижозларни жалб этиш мумкин. Бунга фақат барча амалларни автоматлаштиришнинг зарурий даражасини таъминлаш эвазига

эришиш мумкин. Айни замонда ҳисоблаш техникасининг ишлатилиши билан нафақат пайдо бўлган муаммолар ҳал этилади, балки Янги ахборотни бузилиши ва йўқотилиши, тасодифан ва атайин модификацияланиши ҳамда ахборотни бегоналар тарафидан рухсатсиз олиниши билан боғлиқ ноъананавий таҳдидлар пайдо бўлади.

Мавжуд ҳолатнинг таҳлили кўрсатадики, ахборотни ҳимоялаш учун қилинадиган тадбирлар даражаси, одатда, автоматлаштириш даражасидан паст. Бундай орқада қолиш жиддий оқибатларга олиб келиши мумкин.

Автоматлаштирилган комплексларда ахборотнинг заифлигига ҳисоблаш ресурсларининг концентрацияланиши, уларнинг худудий тақсимланганлиги, магнит элтувчиларида маълумотларнинг катта ҳажмини узоқ вақт сақланиши, кўпгина фойдаланувчиларнинг ресурслардан бир вақтда фойдаланиши сабаб бўлади.

Бундай шароитда ҳимоялаш чораларини кўриш заруриятига шубҳа қилмаса бўлади. Аммо қуйидаги қийинчиликлар мавжуд:

- ҳозирги кунда ҳимояланган тизимларнинг ягона назарияси йўқ;
- ҳимоя воситаларини ишлаб чиқарувчилар хусусий масалаларни ечиш учун асосан алоҳида компонентларни тавсия этадилар, ҳимоялаш тизимини шакллантириш ва бу воситаларнинг бирга ишлатилиши масалалари эса истеъмолчи ихтиёрига қолдирилади;
- ишончли ҳимояни таъминлаш учун техник ва ташкилий муаммолари комплексини ҳал этиш ва мос хужжатларни ишлаб чиқиш зарур.

Юқорида санаб ўтилган қийинчиликларни бартараф қилиш учун нафақат алоҳида корхона, балки давлат даражасидаги ахборот жараёнларида иштирок этувчилари ҳаракатининг координацияси зарур. Ахборот хавфсизлигини таъминлаш етарлича жиддий масала. Шунинг учун аввало ахборот хавфсизлиги концепциясини ишлаб чиқиш зарур. Концепцияда миллий ва корпоратив манфаатлар, ахборот хавфсизлигини таъминлаш принциплари ва мададлаш йўллари аниқланади ва уларни амалга ошириш бўйича масалалар таърифланади.

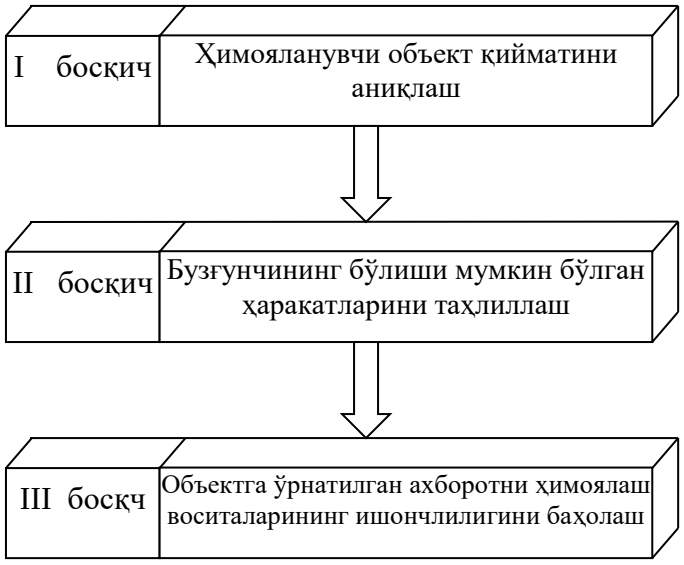
Концепция – ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари.

Концепцияда ифодаланган мақсадлар, масалалар ва уларни бўлиши мумкин бўлган ечиш йўллари асосида ахборот хавфсизлигини таъминлашнинг муайян режалари шакллантирилади.

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади (1.1-расм).

Биринчи босқичда ҳимоянинг мақсадли кўрсатмаси, яъни қандай реал бойликлар, ишлаб чиқариш жараёнлари, дастурлар, маълумотлар базаси ҳимояланиши зарурлиги аниқланиши шарт. Ушбу босқичда ҳимояланувчи алоҳида объектларни аҳамияти бўйича табақалаштириш мақсадга мувофиқ ҳисобланади.

Иккинчи босқичда ҳимояланувчи объектга нисбатан бўлиши мумкин бўлган жиноий ҳаракатлар таҳлилланиши лозим. Иқтисодий жосуслик, терроризм, саботаж, бузиш орқали ўғирлаш каби кенг тарқалган жиноятчиликларнинг реал хавф-хатарлик даражасини аниқлаш муҳим ҳисобланади. Сўнгра, нияти бузуқ одамларнинг ҳимояга муҳтож асосий объектларга нисбатан ҳаракатларининг эҳтимоллигини таҳлиллаш лозим.



1.1–расм. Ахборот химояси концепциясини ишлаб чиқиш босқичлари

Учинчи босқичнинг бош масаласи–вазиятни, хусусан ўзига хос маҳаллий шароитни, ишлаб чиқариш жараёнларини, ўрнатиб қўйилган ҳимоянинг техник воситаларини таҳлиллашдан иборат.

Назорат саволлари

1. Ахборот хавфсизлигининг мақсади.
2. Ахборот хавфсизлигининг туркумланиши.
3. Ахборотларга нисбатан хавф-хатарлар таснифи.
4. Ахборотни ҳимоялаш концепцияси.
5. Ахборотни ҳимоялаш тизимининг комплекслилиги ва элементлари.

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

2-Мавзу: Компьютер тизимлари ва тармоқларига бўладиган таҳдидлар. Тармоқ хужумлари ва уларнинг турлари

Режа:

1. Ахборот хавфсизлигида ҳимоя вазифалари.
2. Ташкилотлардаги ахборотларни ҳимоялаш ва ҳимоялаш тизимининг комплекслилиги.
3. Ахборотларни ташкилий ҳимоялаш элементлари.

Калит сўзлар: Конфиденциаллик, аутентификация, яхлитлик, ёлғоннинг мумкин эмаслиги, ресурслардан фойдаланувчанлик, фойдаланувчанликни бошқариш, ҳимоялаш элементи.

1. Ахборот хавфсизлигида ҳимоя вазифалари

Ҳозирги кунда миллий ахборот ресурслари хар бир давлатнинг иқтисодий ва харбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат килмоқда. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот – коммуникациялар технологияларини қўллаш кенгаяди. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборот ҳимояси эса давлатнинг бирламчи масалаларига айланмоқда.

Амалиётда қўлланиладиган химоя вазифалари тўпламларидан бирига қуйидагилар киради: конфиденциаллик, аутентификациялаш, яхлитлик, ёлғоннинг мумкин эмаслиги, фойдаланувчанлик, фойдаланувчанликни бошқариш.

Конфиденциаллик. *Конфиденциаллик маълумотлар оқимини пассив хужумлардан яъни, узатилаётган маълумотлар ушлаб қолинишидан ёки мониторинг амалга оширилишидан ҳимоя килишга хизмат қилади. Ахборотлар мазмунининг муҳимлилигига қараб химоянинг бир неча сатхлари ўрнатилиши мумкин. Кенг маънодаги ҳимоя хизмати ихтиёрий иккита фойдаланувчи ўртасида узатилувчи барча маълумотларни маълум вақт мобайнида ҳимоясини таъминлаши лозим. Масалан, агар икки тизим ўртасида виртуаль алоқа ўрнатилган бўлса бундай кенг маънодаги химоя фойдаланувчилар маълумотлари узатилгандаги хар қандай йўқолишларга тўсиқ бўла олади. Тор маънодаги химоя хизмати алоҳида ахборотни ёки хатто ахборотнинг алоҳида қисмини химоясини таъминлай олади. Аммо бундай чораларнинг самараси кенг маънодаги ҳимоя хизматига нисбатан кам, уларни амалга ошириш эса баъзида мураккаб ва қиммат бўлиши мумкин. Конфиденциалликнинг яна бир жиҳати маълумотлар оқимини унинг аналитик тадқиқ қилинишидан ҳимоялашдир. Аналитик тадқиқ деганда*

алоқа тизимсидаги ахборотлар тавсифига тааллуқли ахборот манбаини, адресатни, ахборотлар узатиладиган частотани, ахборотлар ўлчамини ва х. бузғунчи томонидан билишга уриниш тушунилади.

***Аутентификация**. Аутентификация хизмати ахборот манбаини ишончли идентификациялашга мўлжалланган. Масалан, бирор хавф тўғрисида сигнал берилганида аутентификация хизматининг вазифаси бу сигналнинг манбаи ҳақиқатан ҳам сигнал узатувчи эканлигини текширишдан иборат бўлади. Ташки интерактив алоқада, масалан, терминал ёрдамида бош узелга уланишдаги сервис хизматининг икки жиҳатини ажратиш мумкин. Биринчидан, боғланиш ўрнатилишида аутентификация воситалари алоқада иштирок этувчиларнинг хақиқий (эканликларига) кафолат бериши лозим. Иккинчидан, кейинги маьлумот алмашинувида бу воситалар маьлумотлар оқимига қандайдир учинчи томоннинг аралашишига йул қўймаслиги лозим.*

***Яхлитлик**. Яхлитлик конфиденциаллик каби ахборотлар оқимига, алохида ахборотга ёки хатто ахборот қисмига тааллуқли бўлиши мумкин. Бу холда хам жами оқимни химоялаш мақсадга мувофиқ ҳисобланади. Ахборот яхлитлигини боғланишлар асосидаги химояловчи воситалар ахборот оқими билан иш кўради ва қабул қилинган ахборотларнинг узатилганига камаймасдан, қўшилмасдан дастлабки узатиш кетма-кетлиги бузилмасдан, қайтаришларсиз аниқ мос келиши кафолатини таьминлайди. Бу воситалар маьлумотлар бузилиши химоясини хам таьминлайди. Шундай қилиб, ахборот яхлитлигини боғланишлар асосидаги химояловчи воситалар ахборот оқимини модификациялашдан ҳамда хизмат кўрсатишдаги халаллардан ҳимояловчи воситаларни ўз ичига олади.*

Ахборот яхлитлигини боғланишлар ўрнатилмагандаги химояловчи воситалар алохида ахборотлар билан иш кўради ва ахборотларни фақат модификациялащдан химоялашни таьминлайди.

Яхлитликни химояловчи воситаларнинг актив хужумга карши туриши ҳисобга олинса бузилишларни олдини олиш эмас, балки бузилишларни аниқлаш мухим хисобланади. Яхлитликнинг бузилиши аникланганидан сўнг бундай хизмат фақат бузилиш содир булганлигини хабарлаши мумкин, бузилган ёки йуқолган ахборотни тиклаш эса бошқа программ воситалари ёки оператор томонидан амалга оширилади. Умуман, автоматик тиклаш воситаларидан фойдаланиш афзал хисобланади.

***Ёлгоннинг мумкин эмаслиги**. Ёлгоннинг мумкин эмаслигини кафолатловчи воситалар узатувчи ва қабул қилувчининг ахборотлар узатилганлиги хақиқат эканлигидан тонишларига имкон бермаслиги керак. Шундай қилиб, агар ахборот ишонч қозонмаган узатувчи томонидан юборилган бўлса, қабул қилувчи ахборот худди шу узатувчи томонидан юборилганлигини исбот қилиш имкониятига эга бўлиши зарур.*

***Ресурслардан фойдаланувчанлик**. Бузилишларнинг кўпгина хиллари ресурслардан фойдаланувчанликни йўқолишига ёки улардан фойдаланишнинг*

қийинлашишига олиб келади. Бунда баъзи холларда аутентификация ва шифрлаш каби автоматлаштирилган қарши чоралар самара берса, баъзи холларда бузилишларни олдини олиш ёки тизим фойдаланувчанлигини тиклаш учун маълум физикавий ҳаракатлар талаб қилинади.

***Фойдаланувчанликни бошқариш**. Фойдаланувчанликни бошқариш деганда алоқа каналлари орқали тармоқ узелларидан, иловалардан фойдаланишни чегаралаш ва назорат қилиш имконияти тушунилади. Бундай назоратда хар бир обьект ўзининг ваколат доирасига эга бўлганлиги сабабли обьектларнинг ресурслардан фойдаланишга уринишларининг хар бирида обьектларни идентификациялаш имконияти мавжуд бўлиши керак.*

Автоматлаштирилган ахборот тизимларида ҳимоялаш зарурияти

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

2.Ташкилотлардаги ахборотларни ҳимоялаш ва ҳимоялаш тизимининг комплекслилиги

Ахборот хажми кичик бўлган ташкилотларда ахборотларни ҳимоялашда оддий усулларни қўллаш мақсадга мувофиқ ва самаралидир. Масалан, ўқиладиган қимматбохо қоғозларни ва электрон хужжатларни алохида гурухларга ажратиш ва ниқоблаш, ушбу хужжатлар билан ишлайдиган ходимни тайинлаш ва ўргатиш, бинони қўриқлашни ташкил этиш, хизматчиларга қимматли ахборотларни тарқатмаслик мажбуриятини юклаш, ташқаридан келувчилар устидан назорат қилиш, компьютерни ҳимоялашнинг энг оддий усулларини қўллаш ва хоказо. Одатда, ҳимоялашнинг энг оддий усулларини қўллаш сезиларли самара беради.

Мураккаб таркибли, кўп сонли автоматлаштирилган ахборот тизими ва ахборот хажми катта бўлган ташкилотларда ахборотни ҳимоялаш учун ҳимоялашнинг мажмуали тизими ташкил қилинади. Лекин ушбу усул хамда ҳимоялашнинг оддий усуллари хизматчиларнинг ишига хаддан ташқари халақит бермаслиги керак.

*Ахборотнинг заиф томонларини камайтирувчи ахборотга рухсат этилмаган киришга, унинг чикиб кетишига ва йўқатилишига тускинлик килувчи ташкилий, техник, дастурий, технологик ва бошқа восита, усул ва чораларнинг комплекси — **ахборотни ҳимоялаш тизими** дейилади.*

Ҳимоялаш тизими узлуксиз, режали, марказлаштирилган, максадли, аник, ишончли, комплексли, осон мукаммаллаштириладиган ва куриниши тез узгартириладиган бўлиши керак. У одатда барча экстремал шароитларда самарали бўлиши зарур.

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

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

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

3.Ахборотларни ташкилий ҳимоялаш элементлари

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

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

*Ахбортларни ҳимоялашнинг ташкилий чора – тадбирлари ташкилот хавфсизлиги хизматининг меъёрий услубий ҳужжатларида ўз аксини топади. Шу муносабат билан кўп ҳолларда юқорида кўрилган тизим элемент-ларининг ягана номи — **ахборотни ташкилий - ҳуқуқий ҳимоялаш элементи**ни ишлатадилар.*

***Ахборотларни муҳандис – техник ҳимоялаш элементи** — техник воситалар комплекси ёрдамида ҳудуд, бино ва қурилмаларни қўриқлашни ташкил қилиш ҳамда техник текшириш воситаларига қарши суст ва фаол кураш учун мўлжалланган. Техник ҳимоялаш воситаларининг нархи баланд бўлсада, ахборот тизимини ҳимоялашда бу элемент муҳим аҳамиятга эга.*

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

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

Автоматлаштирилган ахборот тизимларига тасодифий таъсир кўрсатиш сабаблари таркибига қуйидагилар киради.

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

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

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

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

— ўзгартириш *— ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тўпламлари, дастурлар, техник элементлари) киришни қўлга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам қилади.* Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман копьютер тизими файлларини ўзгартириши, ёки қандайдир қўшимча ноқонуний қайта ишлашни амалга ошириш мақсадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилали;

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

Назорат саволлари

1. Ахборот хавфсизлигини ҳимоя вазифаларини изоҳланг. Конфиденциаллик. Аутентификация. Яхлитлик. Ёлғоннинг мумкин эмаслиги. Ресурслардан фойдаланувчанлик. Фойдаланувчанликни бошқариш.
2. Ташкилотлардаги ахборотларни ҳимоялаш ва ҳимоялаш тизимининг комплекслилиги
3. Ахборотларни ташкилий ҳимоялаш элементларига таъриф беринг ва мисоли билан изоҳланг.

Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

АМАЛИЙ МАШҒУЛОТЛАР

1-Амалий машғулот. Компьютер тармоқларида ахборот ҳимоясининг асосий хусусиятлари. Компьютер тизимлари ва тармоқларидаги ахборот ҳимоясининг муаммолари

Режа:

1. Компьютер тармоқларининг хусусиятлари.
2. Ахборотларни узатиш протоколлари.

1. Компьютер тармоқларининг хусусиятлари

Ахборот ҳимояси нуқтаи назаридан компьютер тармоқларини ***корпоратив ва умумфойдаланувчи*** тармоқларга ажратиш мумкин. Корпоратив тармоқларда барча элементлар (алоқа каналлари бундан истисно бўлиши мумкин) битта корхонага тааллуқли бўлади. Бундай тармоқларда бутун тармоқ бўйича ахборот ҳимоясининг ягона сиёсатини юритиш мумкин. Давлат ва ҳарбий бошқариш тармоқлари, авиация ва темир йўл компаниялари тармоқлари корпоратив тармоқларга мисол булаолади.

Умумфойдаланувчи коммерция тармоқларида асосий мақсад ахборотни тарқатиш бўлиб, шахсий информацион ресурсларни ҳимоялаш, асосан, фойдаланувчилар сатҳида амалга оширилади. Бундай тармоққа мисол тариқасида Internet тармоғини кўрсатиш мумкин.

Корпоратив тармоқлар умумфойдаланувчи тармоқлар билан боғланиши мумкин. Бу ҳолда корпоратив тармоқнинг маъмурияти (эгаси) умумфойдаланувчи тармоқ томонидан келувчи хавфни тўсиш мақсадида қўшимча эҳтиёт чораларини кўришга мажбур.

Ҳар қандай тармоқ учун ахборотни ҳимояловчи тизимни яратишда қуйидагиларни ҳисобга олиш зарур:

- тизимнининг мураккаблиги. Тизимнинг мураккаблиги қисм тизимларининг сони, турли-туманлилиги ва бажарувчи вазифалари билан аниқланади;
- катта масофаларда тақсимланган ресурслардан фойдаланиш устидан самарали назоратни таъминлаш мумкин эмаслиги;
- ресурсларнинг турли эгаларга мансублиги.

Компьютер тармоқларида ахборотни коммуникацион қисм тизим орқали кафолатли узатишни таъминлаш мақсадида ахборотларни етказишнинг иккиланган маршрутлари ҳамда алоқа каналларида ахборотнинг бузилиши ва йўқолишига қарши чоралар кўзда тутилиши лозим. Бундай мураккаб тизимлар адаптив бўлиши, яъни бу тизимлардаги элементларни назорати доимо таъминланиши ва хатто, алоҳида қисм тизим ишдан чиққанда ҳам тизим ишлашини давом эттириш имкониятига эга бўлиши шарт.

Ҳимояланган компьютер тармоқларида ахборот хавфсизлигини таъминловчи барча метод ва воситалар қуйидаги гурухларга ажратилиши мумкин:

- фойдаланувчи қисм тизимсида ва ихтисослаштирилган комуникацион компьютер тизимларида ахборот ҳимоясини таъминлаш;
- тармоқни бошқариш қисм тизимсида ахборотни ҳимоялаш;
- алоқа каналларида ахборотни ҳимоялаш;
- ўзаро алоқада бўлган жараёнларнинг ҳақиқий эканлигининг назоратини таъминлаш;
- коммуникацион қисм тармоқ орқали олинувчи ахборотнинг ҳақиқийлигини тасдиқлаш.

2. Ахборотларни узатиш протоколлари.

Ахборотларни узатиш бошқариш протоколлари деб аталувчи маълум қоидалар бўйича амалга оширилади. Ҳозирда компьютер тармоқларида тармоқнинг узоқлаштирилган элементлари ўртасидаги алоқа иккита ҳалқаро стандарт-TCP/IP ва X.25 протоколлари ёрдамида амалга оширилади.

TCP/IP протоколи асосида Internet тармоғи қурилган. X.25 протоколига пакетларни коммутациялаш асосида қурилган маълумотларни узатиш технологиясининг ривожи сифатида қараш мумкин. X.25 протоколи очиқ тизимларнинг ўзаро алоқаси модели OSI га мувофиқ ҳалқаро стандартлаш ташкилоти ISO томонидан яратилган. X.25 моделида тармоқнинг барча вазифалари 7 сатҳга ажратилса, TCP/IP моделида 5 сатҳ мавжуд (1. - расм).

X.25 протоколи узоқлаштирилган жараёнлар ўртасида юқори ишончли алоқани таъминлай олади. TCP/IP протоколининг афзаллиги сифатида тармоққа уланишнинг соддалигини ва нархининг пастлигини кўрсатиш мумкин.

OSI модели

Татбиқий
Тақдимий
Сеанс
Транспорт
Тармоқ
Канал
Физикавий

TCP/IP модели

Татбиқий
Тарнспорт
Тармоқ
Канал
Физикавий

1.1 - расм. Протоколларнинг сатҳ моделлари.

Тармоқда ахборотни ҳимоялашни таъминлаш масаласи барча сатҳларда амалга оширилади. Протоколларнинг бажарилиши бошқариш қисм тизимси томонидан ташкил этилади. Бошқа муаммолар қаторида бошқариш қисм тизимси сатҳида тармоқда ахборотни ҳимоялашнинг қуйидаги муаммолари ҳал этилади.

1. Ахборот хавфсизлиги масалалари ҳам ечиладиган тармоқни бошқарувчи ягона бошқариш марказини яратиш. Маъмурият ва унинг аппарати бутун тармоқда ҳимоялашнинг ягона сиёсатини олиб боради.
2. Тармоқнинг барча объектларини рўйхатга олиш ва уларнинг ҳимоясини таъминлаш. Идентификаторларни тақдим этиш ва барча тармоқдан фойдаланувчиларни ҳисобга олиш.
3. Тармоқ ресурсларидан фойдаланишни бошқариш.

4. Калитларни шакллантириш ва уларни компьютер тармоқ абонентларига тарқатиш.

5. Трафикни (тармоқдаги ахборотлар оқимини) мониторинглаш, абонентларнинг ишлаш қоидаларига риоя қилишларини назоратлаш, бузилишларга тездан ўз муносабатини билдириш.

6. Тармоқ элементларининг ишлаши бузилганида уларнинг ишлаш қобилиятини тиклашни ташкил этиш.

Internet тизимидаги электрон почта жуда кўп ишлатилаётган ахборот алмашиш каналларидан бири ҳисобланади. Электрон почта ёрдамида ахборот алмашуви тармоқдаги ахборот алмашувининг 30%ини ташкил этади. Бунда ахборот алмашуви бор-йўғи иккита протокол: SMTP (Simple Mail Transfer Protocol) ва POP-3 (Post Office Prolocol)ларни ишлатиш ёрдамида амалга оширилади. POP-3 мультимедиа технологияларининг ривожини акс эттиради, SMTP эса Appranet проекти даражасида ташкил этилган эди. Шунинг учун ҳам бу протоколларнинг ҳаммага очиқлиги сабабли, электрон почта ресурсларига рухсатсиз киришга имкониятлар яратилиб берилмоқда:

- SMTP сервер — дастурларининг нокоррект ўрнатилиши туфайли бу серверлардан рухсатсиз фойдаланилмоқда ва бу технология «спам» технологияси номи билан маълум;
- электрон почта хабарларига рухсатсиз эгалик қилиш учун оддийгина ва самарали усуллардан фойдаланилмокда, яъни қуйи қатламларда винчестердаги маълумотларни ўқиш, почта ресурсларига кириш паролини ўқиб олиш ва хоказолар.

Электрон почтадан фойдаланиш жараённинг асосий мақсади муҳим хужжатлар билан ишлашни тўғри йўлга қўйиш ҳисобланади.

Бу ерда қуйидаги йуналишлар бўйича таклифларни эътиборга олиш зарур:

- E-mail тизимидан ташкилот фаолияти мақсадларида фойдаланиш;
- шахсий мақсадда фойдаланиш;
- махфий ахборотларни сақлаш ва уларга кириш:
- электрон хатларни сақлаш ва уларни бошқариш.

Internetда асосий почта протоколларига қуйидагилар киради:

- SMTP (Simple Mail Transfer Protocol);
- POP (Post Office Protocol);
- IMAP (Internet Mail Access Protocol);
- MIME (Multi purpose Internet Mail Extensions).

Булар билан бирма-бир танишиб чиқамиз:

SMTP — ушбу протокол асосида сервер бошқа тизимлардан хатларни қабўл қилади ва уларни фойдаланувчининг почта кўтисида сақлайди. Почта серверига интерактив кириш хуқуқига эга бўлган фойдаланувчилар ўз компьютерларидан бевосита хатларни ўқий оладилар. Бошқа тизимдаги фойдаланувчилар эса ўз хатларини POP-3 ва IMAP протоколлари орқали ўқиб олишлари мумкин;

POP — энг кенг таркалган протокол бўлиб, сервердаги хатларни, бошқа серверлардан қабўл қилинган бўлса-да, бевосита фойдаланувчи томонидан ўқиб олинишига имконият яратади. Фойдаланувчилар барча хатларни ёки хозиргача ўқилмаган хатларни кўриши мумкин. Хозирги кунда POP нинг 3-версияси ишлаб чиқилган бўлиб ва аутентификациялаш усуллари билан бойитилган;

IMAP — янги ва шу боис хам кенг тарқалмаган протокол саналади.

Ушбу протокол қуйидаги имкониятларга эга:

- почта қутиларини яратиш, ўчириш ва номини ўзгартириш;
- янги хатларнинг келиши;
- хатларни тезкор ўчириш;
- хатларни қидириш;
- хатларни танлаб олиш.

IMAP саёхатда бўлган фойдаланувчилар учун POPга нисбатан қулай бўлиб ҳисобланади;

MIME — Internet почтасининг кўп максадли кенгайтмаси сузлари қисқартмаси бўлиб, у хатларнинг форматини аниқлаш имконини беради, яъни:

- матнларни хар хил кодлаштиришда жўнатиш;
- хар хил форматдаги номатн ахборотларни жўнатиш;
- хабарнинг бир неча қисмдан иборат бўлиши;
- хат сарлавҳасида хар хил кодлаштиришдаги маълумотни жойлаштириш.

7. Ушбу протокол электрон рақамли имзо ва маълумотларни шифрлаш воситаларидан иборат бўлиб, бундан ташқари унинг ёрдамида почта орқали бажарилувчи файлларни хам жўнатиш мумкин. Натижада, файллар билан бирга вирусларни хам тарқатиш имконияти туғилади.

Назорат саволлари

1. Компьютер тармоқларида ҳимояни таъминлаш усуллари.
2. Компьютер тармоқларида ҳимояни таъминлаш воситалари.
3. ЭҲМ ҳимоясини таъминлашнинг техник воситалари.
4. Компьютер тармоқларида маълумотларни ҳимоялашнинг асосий йўналишлари.
5. Internet тармоғида мавжуд алоқанинг ҳимоясини (хавфсизлигини) таъминлаш асослари.

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

2-Амалий машғулот. Компьютер тизимлари ва тармоқларига бўладиган таҳдидлар. Тармоқ хужумлари ва уларнинг турлари

Режа:

1. Ахборот-коммуникацион тизимлар ва тармоқларда таҳдидлар ва заифликлар.

2. Тармоқдаги ахборотга бўладиган намунавий ҳужумлар.

1.Ахборот-коммуникацион тизимлар ва тармоқларда тахдидлар ва заифликлар

Тармоқ технологиялари ривожининг бошланғич босқичида вируслар ва компьютер ҳужумларининг бошқа турлари таъсиридаги зарар кам эди, чунки у даврда дунё иқтисодининг ахборот технологияларига боғликлиги катта эмас эди. Хозирда, ҳужумлар сонининг доимо ўсиши хамда бизнеснинг ахборотдан фойдаланиш ва алмашишнинг электрон воситаларига боғликлиги шароитида машина вақтининг йўқолишига олиб келувчи хатто озгина ҳужумдан келган зарар жуда катта рақамлар орқали ҳисобланади. Мисол тариқасида келтириш мумкинки, фақат 2003 йилнинг биринчи чорагида дунё миқёсидаги йўқотишлар 2002 йилдаги барча йўқотишлар йиғиндисининг 50%ини ташкил этган, ёки бўлмаса 2006 йилнинг ўзида Россия Федереациясида 14 мингдан ортиқ компьютер жиноятчилиги холатлари кайд этилган.

Корпоратив тармоқларда ишланадиган ахборот, айниқса, заиф бўлади. Хозирда рухсатсиз фойдаланишга ёки ахборотни модификациялашга, ёлғон ахборотнинг муомалага кириши имконининг жиддий ошишига қуйидагилар сабаб бўлади:

- компьютерда ишланадиган, узатиладиган ва сақланадиган ахборот хажмининг ошиши;
- маълумотлар базасида муҳимлик ва маҳфийлик даражаси турли бўлган ахборотларнинг тўпланиши;
- маълумотлар базасида сақланаётган ахборотдан ва ҳисоблаш тармоқ ресурларидан фойдаланувчилар доирасининг кенгайиши;
- масофадаги ишчи жойлар сониниг ошиши;
- фойдаланувчиларни боғлаш учун Internet глобал тармоғини ва алоқанинг турли каналларини кенг ишлатиш;
- фойдалувчилар компьютерлари ўртасида ахборот алмашинувининг автоматлаштирилиши.

Ахборот хавфсизлигига тахдид деганда ахборотнинг бузилиши ёки йўқотилиши хавфига олиб келувчи ҳимояланувчи объектга қарши қилинган харакатлар тушунилади. Олдиндан шуни айтиш мумкинки, сўз барча ахборот хусусида эмас, балки унинг фақат, мулк эгаси фикрича, коммерция қийматига эга бўлган қисми хусусида кетяпти.

Замонавий корпоратив тармоқлар ва тизимлар дучор бўладиган кенг тарқалган тахдидларни таҳлил қиламиз. Ҳисобга олиш лозимки, хавфсизликка тахдид манбалари корпоратив ахборот тизимининг ичида (ички манба) ва унинг ташқарисида (ташқи манба) бўлиши мумкин. Бундай ажратиш тўғри, чунки битта тахдид учун (масалан, ўғирлаш) ташқи ва ички манбаларга қарши харакат усуллари турлича бўлади. Бўлиши мумкин бўлган тахдидларни хамда корпоратив ахборот тизимининг заиф жойларини билиш хавфсизликни таъминловчи энг самарали воситаларни танлаш учун зарур ҳисобланади.

Тез-тез бўладиган ва хавфли (зарар улчами нуктаи назаридан) тахдидларга фойдаланувчиларнинг, операторларнинг, маъмурларнинг ва корпоратив ахборот тизимларига хизмат кўрсатувчи бошқа шахсларнинг атайин қилмаган хатоликлари киради. Баъзида бундай хатоликлар (нотўғри киритилган маълумотлар, дастурдаги хатоликлар сабаб бўлган тизимнинг тўхташи ёки бузилиши) тўғридан - тўғри зарарга олиб келади. Баъзида улар нияти бузуқ одамлар фойдаланиши мумкин бўлган нозик жойларни пайдо бўлишига сабаб бўлади. Глобал ахборот тармоғида ишлаш ушбу омилнинг етарлича долзарб қилади. Бунда зарар манбани ташкилотнинг фойдаланувчиси ҳам, Тармоқ фойдаланувчиси ҳам бўлиши мумкин, охиргиси айниқса хавфли.

Зарар ўлчами бўйича иккинчи ўринни ўғирлашлар ва сохталаштиришлар эгаллайди. Текширилган холатларнинг аксариятида ишлаш режимлари ва ҳимоялаш чоралари билан аъло даражада таниш бўлган ташкилот штатидаги ходимлар айбдор бўлиб чиқдилар. Глобал тармоқлар билан боғланган қувватли ахборот каналининг мавжудлигида, унинг ишлаши устидан етарлича назорат йўқклиги бундай фаолиятга қўшимча имкон яратади.

Хафа бўлган ходимлар (хатто собиклари) ташкилотдаги тартиб билан таниш ва жуда самара билан зиён етказишлари мумкин. Ходим ишдан бўшаганида унинг ахборот ресурсларидан фойдаланиш қилини бекор қилиниши назоратга олиниши шарт.

Хозирда ташқи коммуникация орқали рухсатсиз фойдаланишга атайин қилинган уринишлар бўлиши мумкин бўлган барча бузилишларнинг 10%ини ташкил этади. Бу катталик анчагина бўлиб туюлмаса хам, Internetда ишлаш тажрибаси кўрсатадики, қарийб хар бир Internet-сервер кунига бир неча марта суқилиб кириш уринишларига дучор бўлар экан. Хавф-хатарлар тахлил қилинганида ташкил от корпоратив ёки локал тармоғи компьютерларининг ҳужумларга қарши туриши ёки булмаганида ахборот хавфсизлиги бузилиши фактларини кайд этиш учун етарлича ҳимояланмаганлигини ҳисобга олиш зарур. Масалан, ахборот тизимларини хдмоялаш Агентлигининг (АК.Ш) тестлари курсатадики, 88% компьютерлар ахборот хавфсизлиги нук,таи назаридан нозик жойларга эгаки, улар рухсатсиз фойдаланиш учун фаол

ишлатишлари мумкин. Ташкилот ахборот тузилмасидан сасофадан фойдаланиш холлари алохида курилиши лозим.

Ҳимоя сиёсатини тузишдан аввал ташкилотда компьютер муҳити дучор бўладиган хавф-хатар бахоланиши ва зарур чоралар кўрилиши зарур. Равшанки, химояга тахдидни назоратлаш ва зарур чораларни кўриш учун ташкилотнинг сарф-харажати ташкилотда активлар ва ресурсларни ҳимоялаш бўйича хеч қандай чоралар кўрилмаганида кутиладиган йўқотишлардан ошиб кетмаслиги шарт.

Умуман олганда, ташкилотнинг компьютер муҳити икки хил хавф - хатарга дучор бўлади:

1. Маълумотларни йўқотилиши ёки ўзгартирилиши.
2. Сервиснинг тўхтатилиши.

Тахдидларнинг манбаларини аниқлаш осон эмас. Улар нияти бузуқ, одамларнинг бостириб киришидан то компьютер вирусларигача турланиши мумкин.

Бунда инсон хатоликлари хавфсизликка жиддий тахдид ҳисобланади. 2.1-расмда корпоратив ахборот тизимида хавфсизликнинг бузилиш манбалари бўйича статистик маълумотларни тасвирловчи айланма диаграмма келтирилган.

2.1-расм. Хавфсизликнинг бузилиш манбалари

2.1.-расмда келтирилган статистик маълумотлар ташкилот маъмуриятига ва ходимларига корпоратив Тармоқ ва тизими хавфсизлигига тахдидларни самарали камайтириш учун харакатларни қаерга йўналтиришлари зарурлигини айтиб бериши мумкин. Албатта, физик хавфсизлик муаммолари билан шуғулланиш ва инсон хатоликларининг хавфсизликка салбий таъсирини камайтириш бўйича чоралар кўрилиши зарур. Шу билан бир қаторда корпоратив Тармоқ ва тизимга ҳам ташқаридан, хам ичкаридан бўладиган ҳужумларни олдини олиш бўйича тармоқ хавфсизлиги масаласини ечишга жиддий эътиборни қаратиш зарур.

2.Тармоқдаги ахборотга бўладиган намунавий ҳужумлар

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

Internet протоколларининг мукаммал эмаслиги сабабали тармоқдаги ахборотга масофадан бўладиган асосий намунавий ҳужумлар қуйидагилар:

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

Тармоқ трафигини тахлиллаш. Сервердан Internet тармоғи базавий протоколлари FTP (File Transfer Protocol) ва TELNET (Виртуал терминал протоколи) бўйича фойдаланиш учун фойдаланувчи *идентификация* ва *аутентификация* муолажаларини ўтиши лозим. Фойдаланувчини идентификациялашда ахборот сифатида унинг идентификатори (исми) ишлатилса, аутентификациялаш учун *парол* ишлатилади. FTP ва TELNET протоколларининг хусусияти шундаки, фойдалувчиларнинг пароли ва идентификатори тармоқ орқали очиқ, шифрланмаган кўринишда ўзатилади. Демак, Internet хостларидан фойдаланиш учун фойдаланувчининг исми ва паролини билиш кифоя.

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

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

Асосий муаммо алмашинув протоколида. Базавий татбикий проколларнинг TCP/IP оиласи анча олдин (60 йилларнинг охири ва 80-йилларнинг боши) ишлаб чиқилган ва ундан бери умуман ўзгартирилмаган. Ўтган давр мобайнида тақсимланган тармоқ хавфсизлигини таъминлашга ёндашиш жиддий ўзгарди. Тармоқ уланишларини ҳимоялашга ва трафикни шифрлашга имкон берувчи ахборот алмашинувининг турли протоколлари ишлаб чиқилди. Аммо бу протоколлар эскиларининг ўрнини олмади (SSL бундан истисно) ва стандарт мақомига эга бўлмади. Бу протоколларининг

стандарт бўлиши учун эса тармоқдан фойдаланувчиларнинг барчаси уларга ўтишлари лозим. Аммо, Internetда тармоқни марказлашган бошқариш бўлмаганлиги сабабли бу жараён яна кўп йиллар давом этиши мумкин.

Тармоқнинг ёлғон объектини киритиш. Хар қандай тақсимланган тармоқда қидириш ва адреслаш каби "нозик жойлари" мавжуд. Ушбу жараёнлар кечишида тармоқнинг ёлғон объектини (одатда бу ёлғон хост) киритиш имконияти туғилади. Ёлғон обьектнинг киритилиши натижасида адресатга узатмоқчи бўлган барча ахборот аслида нияти бузуқ одамга тегади. Тахминан буни тизимингизга, одатда электрон почтани жўнатишда фойдаланадиган провайдерингиз сервери адреси ёрдамида киришга кимдир уддасидан чиққани каби тасаввур этиш мумкин. Бу холда нияти бузуқ одам унчалик қийналмасдан электрон хат-хабарингизни эгаллаши, мумкин, сиз эса хатто ундан шубхаланмасдан ўзингиз барча электрон почтангизни жўнатган бўлар эдингиз.

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

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

Бу қуйидаги алгоритм бўйича амалга оширилади:

1. DNS-сўровни кутиш.
2. Олинган сўровдан керакли маълумотни чиқариб олиш ва тармоқ бўйича сўров юборган хостга ёлғон DNS-жавобни хақиқий DNSсервер номидан узатиш. Бу жавобда ёлғон DNS-сервернинг IPадреси кўрсатилган бўлади.
3. Хостдан пакет олинганида пакетнинг IP-сарлавхасидаги IP-адресни ёлғон DNS сервернинг IP-адресига ўзгартириш ва пакетни серверга узатиш (яъни ёлғон DNS-сервер ўзининг номидан сервер билан иш олиб боради).

4. Сервердан пакетни олишда пакетнинг IP-сарлавхасидаги IPадресни ёлғон DNS-сервернинг IP-адресига ўзгартириш ва пакетни хостга узатиш (ёлғон DNS серверни хост хақиқий ҳисоблайди).

Ёлғон маршрутни киритиш. Маълумки, замонавий глобал тармоқлари бир-бири билан *тармоқ узеллари* ёрдамида уланган тармоқ сегментларининг мажмуидир. Бунда *маршрут* деганда маълумотларни манбадан қабул килувчига узатишга хизмат қилувчи тармоқ узелларининг кетма-кетлиги тушунилади. Маршрутлар хусусидаги ахборотни алмашишни унификациялаш учун маршрутларни бошқарувчи махсус протоколлар мавжуд. Internet даги бундай протоколларга янги маршрутлар хусусида хабарлар алмашиш протоколи ICMP (Internet Control Message Protocol) ва маршрутизаторларни масофадан бошқариш протоколи SNMP (Simple Network Manegment Protocol) мисол бўла олади. Маршрутни ўзгартириш ҳужум қилувчи ёлғон хостни киритишдан бўлак нарса эмас. Хатто оҳирги обьект хақиқий бўлса, хам маршрутни ахборот барибир ёлғон хостдан ўтадиган қилиб қуриш мумкин.

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

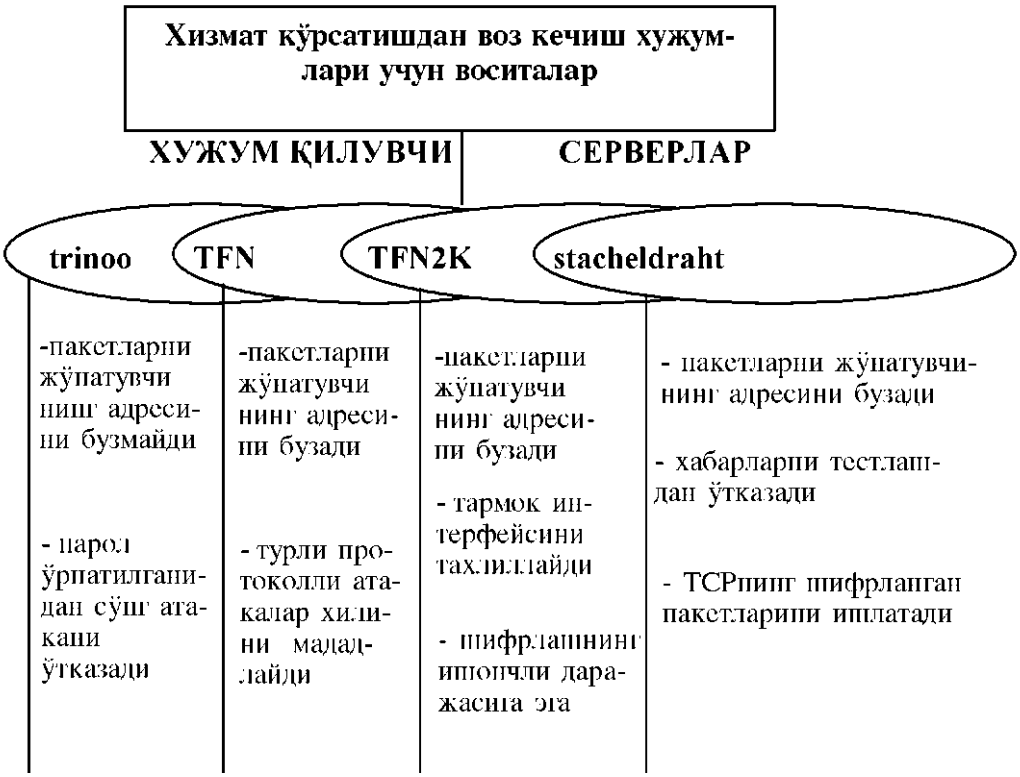
Хизмат қилишдан воз кечишга ундайдиган тақсимланган ҳужумлар DdoS (Distributed Denial of Service) компьютер жиноятчилигининг нисбатан янги хили бўлсада, қўрқинчли тезлик билан тарқалмокда. Бу ҳужумларнинг ўзи анчагина ёқимсиз бўлгани етмаганидек, улар бир вақтнинг ўзида масофадан бошқарилувчи юзлаб ҳужум қилувчи серверлар томонидан бошланиши мумкин.

Хакерлар томонидан ташкил этилган узелларда DDoS ҳужумлар учун учта инструментал воситани топиш мумкин: trinoo, Tribe FloodNet (TFN) ва TFN2K. Якинда TFN ва trinoo нинг энг ёқимсиз сифатларини уйғунлаштирган яна биттаси stacheldraht ("тикон симлар") пайдо бўлди.

2.2-расмда хизмат қилишдан воз кечишга ундайдиган ҳужум воситаларининг характеристикалари келтирилган.

Хизмат қилишдан воз кечишга ундайдиган оддий тармоқ ҳужумида хакер танлаган тизимига пакетларни жўнатувчи инструментидан фойдаланади. Бу пакетлар нишон тизимининг тўлиб тошиши ва бузилишига сабаб бўлиши керак. Кўпинча бундай пакетларни жўнатувчилар адреси бузиб

кўрсатилади. Шу сабабли ҳужумнинг ҳақиқий манбасини аниқлаш жуда қийин.



2.2-расм. Хизмат қилишдан воз кечишга ундайдиган ҳужум воситаларининг характеристикалари

DDoS ҳужумларини ташкил этиш битта хакернинг қўлидан келади, аммо бундай ҳужумнинг эффекти *агентлар* деб аталувчи ҳужум қилувчи серверларнинг ишлатилиши ҳисобига анчагина кучаяди. TFNда *серверлар* (server), а trinoода *демонлар* (daemon) деб аталувчи бу агентлар хакер томонидан масофадан бошқарилади.

3-Амалий машғулот. Компьютер тизимлари ва тармоқларини рухсатсиз фойдаланишлардан ҳимоялаш усуллари

Режа:

1. Internetда рухсатсиз кириш усулларининг таснифи;
2. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши;
3. Тармоқлараро экран ва унинг вазифалари;
4. Тармоқлараро экраннинг асосий компонентлари.

1.Internetда рухсатсиз кириш усулларининг таснифи

Глобал тармоқларнинг ривожланиши ва ахборотларни олиш, қайта ишлаш ва узатишнинг янги технологиялари пайдо бўлиши билан Internet тармоғига хар хил шахс ва ташкилотларнинг эътибори қаратилди. Кўплаб ташкилотлар ўз локал тармоқларини глобал тармоқларга улашга қарор қилишган ва ҳозирги пайтда WWW, FTP, Gophes ва бошқа серверлардан фойдаланишмоқда. Тижорат мақсадида ишлатилувчи ёки давлат сири бўлган ахборотларнинг глобал тармоқлар бўйича жойларга узатиш имкони пайдо бўлди ва ўз навбатида, шу ахборотларни ҳимоялаш тизимида малакали мутахассисларга эҳтиёж туғилмокда.

Глобал тармоқлардан фойдаланиш бу фақатгина «қизиқарли» ахборотларни излаш эмас, балки тижорат мақсадида ва бошқа аҳамиятга молик ишларни бажаришдан иборат. Бундай фаолият вақтида ахборотларни ҳимоялаш воситаларининг йўқлиги туфайли кўплаб талофотларга дуч келиш мумкин.

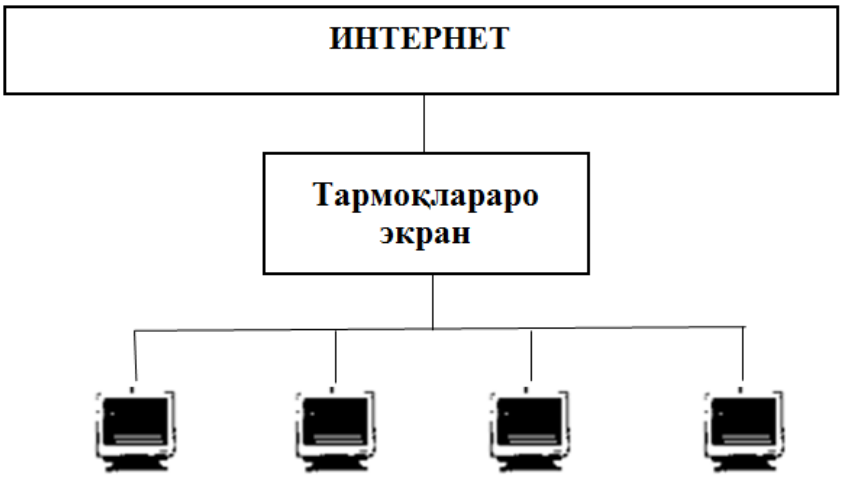
Ҳар қандай ташкилот Intenetга уланганидан сўнг, ҳосил бўладиган қуйидаги муаммоларни хал этишлари шарт:

- *ташкилотнинг компьютер тизимини хакерлар томонидан бузилиши:*
- *Internet орқали жўнатилган маълумотларнинг ёвуз ниятли шахслар томонидан ўқиб олиниши;*
- *ташкилот фаолиятига зарар етказилиши.*

Internet лойиҳалаш даврида бевосита ҳимояланган тармоқ сифатида ишлаб чиқилмаган. Бу соҳада хозирги кунда мавжуд бўлган қуйидаги муаммоларни келтириш мумкин:

- *маълумотларни енгиллик билан қўлга киритиш;*
- *тармоқдаги компьютерлар манзилини сохталаштириш;*
- *TCP/IP воситаларининг заифлиги;*
- *кўпчилик сайтларнинг нотўғри конфигурацияланиши;*
- *конфигурациялашнинг мураккаблиги.*

Глобал тармоқларнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб бўлмокда, бу эса ўз навбатида ахборотлар хавфсизлигига тахдид солиш эҳтимолининг ошишига олиб келмоқда. *Узоқ, масофалар билан ахборот алмашиш зарурияти ахборотларни олишнинг қатъий чегараланишини талаб этади. Шу мақсадда тармоқларнинг сегментларини хар хил даражадаги ҳимоялаш усуллари*



3.1-расм. Тармоқлараро экраннинг уланиш схемаси

таклиф этилган:

- *эркин кириш (масалан: WWW-сервер);*
- *чегараланган киришлар сегменти (узок масофада жойлашган иш жойига хизматчиларнинг кириши);*
- *ихтиёрий киришларни ман этиш (масалан, ташкилотларнинг молиявий локал тармоқлари).*

Интернет глобал ахборот тармоғи ўзида ниҳоятда катта хажмга эга бўлган ахборот ресурсларидан миллий иқтисоднинг турли тармоқларида самарали фойданишга имконият туғдиришига қарамасдан ахборотларга бўлган хавфсизлик даражасини оширмокда. Шунинг учун хам *Интернетга уланган хар бир корхона ўзининг ахборот хавфсизлигини таъминлаш масалаларига катта эътибор бериши керак. Ушбу тармоқда ахборотлар хавфсизлигининг йўлга қуйилиши ёндашуви қуйида келтирилган:*

Локал тармоқларнинг глобал тармоқарга қўшилиши учун тармоқлар ҳимояси администратори қуйидаги масалаларни хал қилиши лозим:

- *локал тармоқларга глобал тармоқ, томонидан мавжуд хавфларга нисбатан ҳимоянинг яратилиши;*
- *глобал тармоқ фойдаланувчиси учун ахборотларни яшириш имкониятининг яратилиши;*

Бунда қуйидаги усуллар мавжуд:

— кириш мумкин бўлмаган тармоқ манзили орқали;

— Ping дастури ёрдамида тармоқ пакетларини тўлдириш;

— рухсат этилган тармоқ манзили билан тақиқланган тармоқ манзили бўйича бирлаштириш;

— таъқиқланган тармоқ протаколи бўйича бирлаштириш;

— тармоқ бўйича фойдаланувчига парол танлаш;

— REDIREST туридаги ICMP пакети ёрдамида маршрутлар жадвалини модификациялаш;

— RIP стандарт бўлмаган пакети ёрдамида маршрутлар жадвалини ўзгартириш;

— *DNS spoofingдан фойдаланган холда уланиш.*

Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши

Ушбу хавф глобал тармоқларнинг бир қанча соҳаларини қамраб олади, жумладан:

• *локал соҳа;*

• *локал-глобал тармоқларнинг бирлашуви;*

• *мухим ахборотларни глобал тармоқларда жўнатиш;*

• *глобал тармоқнинг бошқарилмайдиган қисми.*

Ихтиёрий ахборот тармоқларининг асосий компонентлари бу серверлар ва ишчи станциялар ҳисобланади. Серверда ахборотлар ёки хисоблаш ресурслари ва ишчи станцияларда хизматчилар ишлайди. Умуман ихтиёрий компьютер ҳам, сервер хам ишчи станция бўлиши мумкин - бу холда уларга нисбатан хавфли хужумлар бўлиши эҳтимоли бор.

Глобал тармоқ майдонларидаги тахдид

Тахдид	Локал майдон	ЛТ/ГТ бирла-шуви	ГТ админ-стратор майдони	ГТ бошқа-рилмай-диган майдони
Тармоқларнинг нотўғри манзили			+	+
Пакетлар билан тўлдириш	+			+
Мумкин бўлмаган уланиш		+		+
Мумкин бўлган уланиш	+	+		+
Паролни танлаш	+	+		+
ICMP хужуми	+	+	+	
RIP хужуми		+	+	
Рухсатсиз узоқдан бошқариш		+	+	+
Паролни ўзгартириш	+			+
DNS хужуми		+	+	
Мумкин бўлмаган вақтда	+	+	+	+

Серверларнинг асосий вазифаси ахоротларни сақлаш ва тақдим қилишдан иборат.

Ёвуз ниятли шахсларни қуйидагича таснифлаш мумкин:

- *ахборот олишга имконият олиш;*
- *хизматларга рухсат этилмаган имконият олиш;*
- *маълум синфдаги хизматларнинг иш режимини ишдан чиқаришга уриниш;*
- *ахборотларни ўзгартиришга харакат ёки бошқа турдаги хужумлар.*

Ўз навбатида, ҳозирги замонавий ривожланиш давомида сервис хизматини издан чиқаришга қарши кураш муаммоси муҳим аҳамият касб этади. Бу хилдаги хужумлар «сервисдаги бузилиш» номини олган.

Ишчи станцияларга хужумнинг асосий мақсади, асосан, қайта ишланаётган маълумотларни ёки локал сақланаётган ахборотларни олишдир. Бундай хужумларнинт асосий воситаси «Троян» дастурлар саналади. Бу дастур ўз тузилиши бўйича компьютер вирусларидан фарқ қилмайди ва компьютерга тушиши билан ўзини билинтирмасдан туради. Бошқача айтганда, бу дастурнинг асосий мақсади — тармоқ станциясидаги ҳимоя тизимини ички томондан бузишдан иборат.

Бу холатда масалани хал қилиш маълум қийинчиликка олиб келади, яъни махсус тайёрланган мутахассис лозим ёки бошқа чоралар қабул қилиш керак бўлади. *Бошқа бир оддий ҳимоя усулларидан бири ҳар қайси ишчи станциядаги тизимли файллар ва хизмат соҳасидаги маълумотларнинг ўзгаришини текшириб турувчи ревизор (инг.л.* ***advizer****— қирувчи) ўрнатиш саналади.*

2.Тармоқлараро экран ва унинг вазифалари

Тармоқлараро экран — ҳимоялаш воситаси бўлиб, ишончли тармоқ, ва ишончсиз тармоқ орасида маълумотларга киришни бошқаришда қўлланилади.

Тармоқлараро экран кўп компонентли бўлиб, у Internetдан ташкилотнинг ахборот заҳираларини ҳимоялаш стратегияси саналади. Яъни ташкилот тармоғи ва Internet орасида қўриқлаш вазифасини бажаради.

Тармоқлараро экраннинг асосий функцияси — маълумотларга эгалик қилишни марказлаштирилган бошқарувини таъминлашдан иборат.

Тармоқлараро экран қуйидаги ҳимояларни амалга оширади:

- ўринсиз трафиклар, яъни тармоқда узатиладиган хабарлар оқимини тақиқлаш;
- қабул қилинган трафикни ички тизимларга йўналтириш;
- ички тизимнинг заиф қисмларини яшириш билан Internet томонидан уюштириладиган хужумлардан ҳимоялаш;
- барча трафикларни баёнлаштириш;
- ички маълумотларни, масалан тармоқ топологиясини, тизим номларини, тармоқ ускуналарини ва фойдаланувчиларнинг идентификаторларини Internetдан яшириш;
- ишончли аутентификацияни таьминлаш.

Кўпгина адабиётларда **тармоқлараро экран** тушунчаси **брандмауэр** ёки **Fire Wall** деб юритилган. Умуман бўларнинг хаммаси ягона тушунчадир.

Тармоқлараро экран — бу тизим, умумий тармоқни икки қисмга ажратиб, тармоқлараро ҳимоя вазифасини ўтайди ва маълумотлар пакетининг чегарадан ўтиш шартларини амалга оширадиган қоидалар тўплами ҳисобланади.

Одатда тармоқлараро экран ички тармоқларни глобал тармоқлардан, яъни Internetдан ҳимоя қилади. Шуни айтиш керакки, тармоқлараро экран нафақат Internetдан, балки корпоратив тармоқлардан хам ҳимоя қилиш қобилиятига эгадир.

Ҳар қандай ташкилотнинг тармоқ хавсизлиги сиёсати икки қисмдан иборат бўлади: тармоқ сервисларидан фойдаланиш; тармоқлараро экранни қўллаш.

Тармоқ сервисларидан фойдаланиш сиёсатига мос равишда Internetда сервислар рўйхати аниқланади. Бу сервисларга фойдаланувчилар чекланган кириш билан таъминланади.

Кириш усулларининг чекланилиши — фойдаланувчилар томонидан Internet сервисларига чет йўллар орқали рухсатсиз киришни тақиқлаш маъносини билдиради.

Тармоқ сервисларига кириш сиёсати, одатда, қуйидаги принципларга мойил бўлади:

- Internetдан ички тармоққа киришни тақиқлаш, лекин ички тармоқдан Inlernetга киришга рухсат бериш;

- ваколатланган тизимларга Internetдан ички тармоққа чекланилган киришга рухсат бериш.

Тармоқлараро экранларга қуйиладиган вазифавий талаблар қуйидагилардан иборат.

- тармоқ даражасида фильтрлашга талаб;
- амалий даражада фильтрлашга талаб;
- администрациялаш ва фильтрлаш қоидаларини ўрнатиш бўйича талаб;
- тармоқли аутентификациялаш воситаларига талаб;
- ишларни қайд қилиш ва хисобни олиб бориш бўйича талаб.

Тармоқлараро экраннинг асосий компонентлари. Тармоқлараро экранларнинг компонентлари сифатида қуйидагиларни келтириш мумкин: фильтрловчи – йўлловчи; тармоқ даражасидаги шлюзлар; амалий даражадаги шлюзлар.

Фильтрловчи-йўлловчи — йўлловчи, яъни компьютер тармоғида маълумотларни манзилга етказувчи дастурлар пакети ёки сервердаги дастур бўлиб, у кирадиган ва чиқадиган пакетларни фильтрлайди. Пакетларни фильтрлаш, яъни уларни аниқ тўпламга тегишлилигини текшириш, TCP/IP сарлавҳасидаги маълумотлар бўйича амалга оширилади.

Фильтрлашни аниқ хост-компьютер, яъни тармоқдаги файл ва компьютер заҳираларига киришни амалга оширувчи компьютер ёки порт, яъни хабарларни жўнатиш ёки қабул қилиш мақсадида мижоз ва сервер томонидан ишлатиладиган ва одатда 16 битли сон билан номланадиган дастур билан уланишда амалга ошириш мумкин.

Тармоқ даражасидаги шлюзлар ишончли мижозлардан аниқ хизматларга сўровномасини қабўл қилади ва ушбу алоқанинг қонунийлигини текширгандан сўнг уларни ташқи хост-компьютер билан улайди. Шундан сўнг шлюз иккала томонга хам пакетларни филътрламай жўнатади.

Бундан ташқари, тармоқ даражасида шлюзлар бевосига **сервер-даллол** вазифасини бажаради. Яъни, ички тармоқдан келадиган IP манзиллар ўзгартирилиб, ташқирига фақатгина битта IP манзил узатилади. Натижада,

ички тармоқдан ташқи тармоқ билан тўғридан-тўғри боғламайди ва шу йўл билан ички тармоқни ҳимоялаш вазифасини ўтайди.

Амалий даражадаги шлюзлар фильтрловчи-йўлловчиларга мансуб бўлган камчиликларни бартараф этиш мақсадида ишлаб чиқилган. Ушбу дастурий восита **ваколатланган сервер,** деб номланади ва у бажарилаётган хост-компьютер эса амалий даражадаги шлюз деб аталади.

Амалий даражадаги шлюзлар мижоз ва ташқи хост-компьютер билан тўғридан-тўғри алоқа ўрнатишга йўл қўймайди. Шлюз келадиган ва жўнатиладиган пакетларни амалий даражада фильтрлайди. Сервер-даллоллар шлюз орқали аниқ сервер томонидан ишлаб чиқилган маълумотларни қайтадан йўналтиради.

Амалий даражадаги шлюзларнинг афзалликлари қуйидагилардан иборат:

- глобал тармоқ томонидан ички тармоқ таркиби кўринмайди;
- ишончли аутентификация ва қайд қилиш;
- фильтрлаш қоидаларининг енгиллиги;
- кўп тамойилли назоратларни амалга ошириш мумкинлиги.

Фильтрловчи-йўлловчиларга нисбатан амалий даражадаги шлюзларнинг камчиликлари қуйидагилардан иборат самарадорлигининг пастлиги; нархининг қиммат бўлиши.

Назорат саволлари

1. Internetда рухсатсиз кириш усулларининг таснифи.
2. Рухсат этилган манзилларнинг рухсат этилмаган вақтда уланиши.
3. Глобал тармоқга таҳдидлар.
4. Тармоқлараро экран ва унинг вазифалари;
5. Тармоқлараро экраннинг асосий компонентлари

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

4-Амалий машғулот. Компьютер тизимлари ва тармоқларида ахборот ҳимоясининг комплексли ёндашуви.Компьютер тизими ва тармоғининг архитектураси ва унинг қисм тизимлари.

Режа:

1. Компьютер тармоқларининг архитектураси.
2. Ўзаро алоқада бўлган жараёнларнинг ҳақиқий эканлигини тасдиқлаш.
3. Коммуникацион қисм тармоқ орқали олинувчи ахборотнинг хақиқийлигини тасдиқлаш.

1.Компьютер тармоқларининг архитектураси.

Компьютер тармоқлари-коммуникацион қисм тизимлари ёрдамида ягона тизимга бирлаштирилган ғужланган компьютер тизимлари тўпламидир. Ғужланган компьютер тизимларига алоҳида ЭҲМлар ҳамда локал компьютер тармоқлари (ЛКТ) кириши мумкин. Ҳозирда амалда таркибида ЭҲМ бўлган интелектуаль абонент нуқталари ишлатилади ва, демак, компьютер тармоқларининг энг кичик структуравий қисми ЭҲМ десак хато бўлмайди. (4.1 - расм).

Коммуникацион қисм тизим қуйидагиларни ўз ичига олади:

- коммуникацион модуллар(КМ);
- алоқа каналлари;
- концентраторлар;
- тармоқлараро шлюзлар (кўприклар).

Коммуникацион модулларнинг асосий вазифаси олинган пакетни бошқа коммуникацион модулга ёки абонент нуқтасига маълум маршрут бўйича узатишдир. Коммуникацион модуль пакетларни коммутацияловчи марказ деб ҳам юритилади.

Алоқа каналлари тармоқ элементларини ягона тармоққа бирлаштиради.

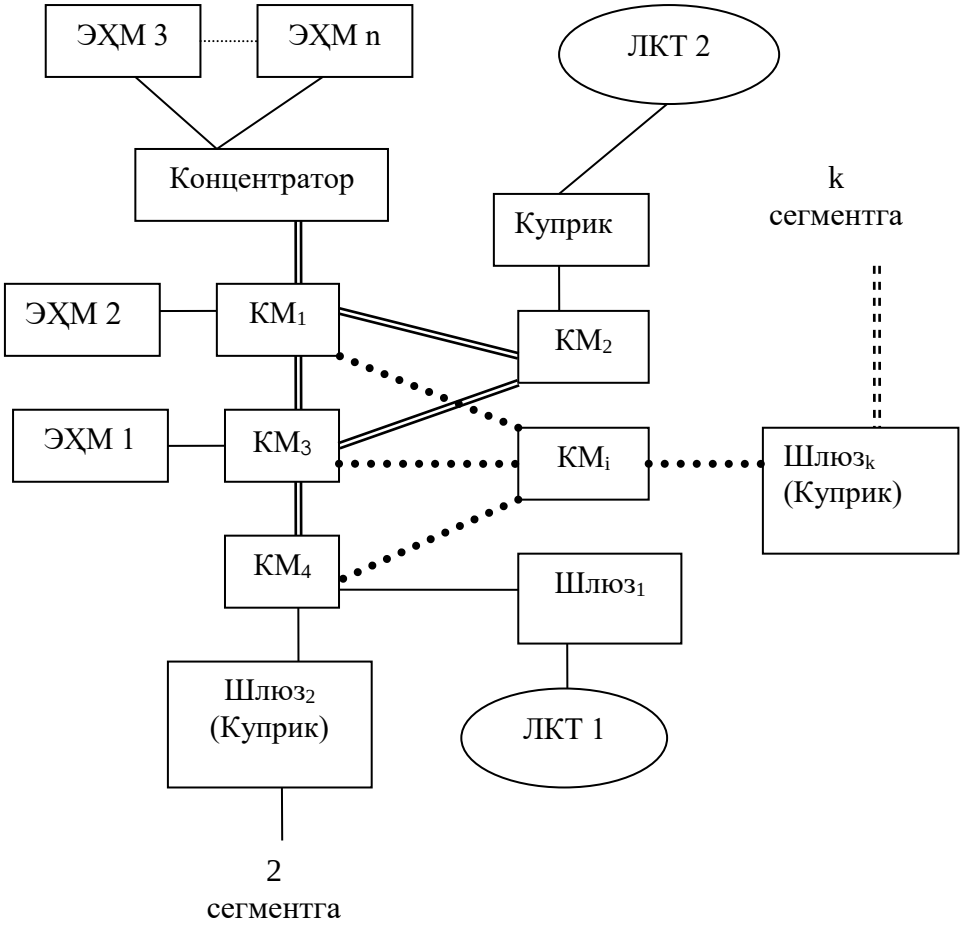
Концентраторлар ахборотни тезлиги катта бўлган каналлар орқали узатилишидан аввал зичлаштириш учун хизмат қилади.

Тармоқлараро шлюзлар ва кўприклар тармоқни локаль компьютер тармоқлари билан улашга ёки глобаль тармоқ сегментларини бирлаштиришга хизмат қилади. Кўприклар ёрдамида тармоқ протколлари бир хил бўлган тармоқ сегментлари бирлаштирилади. Ҳар қандай тармоқда қуйидаги қисм тизимларини ажратиш мумкин:

- фойдаланувчи қисм тизими;
- бошқариш қисм тизими;
- коммуникацион қисм тизими;

Фойдаланувчи ёки абонент қисм тизими фойдаланувчиларнинг (абонентларнинг) компьютер тизимларини ўз ичига олади ва

фойдаланувчиларнинг ахборотни сақлаш, ишлаш ва олишдаги эҳтиёжларини қондиришга хизмат қилади.



4.1- расм. Компьютер тармоғи фрагменти.

Бошқариш қисм тизими компьютер тармоқларининг барча элементларини уларнинг ўзаро алоқаси ягона қоида бўйича амалга оширилувчи ягона тизимга бирлаштиришга хизмат қилади. Бу қисм тизим бутун тармоқ ишлаши учун оптималь шароит яратиш мақсадида хизматчи ахборотни йиғиш, тахлил қилиш ва элементларга таъсир этиш йўли билан тизим элементларининг ўзаро алоқасини таъминлайди.

Коммуникацион қисм тизими фойдаланувчилар манфаатлари ва тармоқни бошқариш учун тармоқда ахборотни узатишга хизмат қилади. Бошқача айтганда, тармоқнинг ишлашини узоқлаштирилган жараёнларни коммуникацион қисм тизим орқали ўзаро алоқаси каби тасаввур этиш мумкин. Узоқлаштирилган жараёнларнинг ўзаро алоқаси деганда файлларни алмашиш, электрон почта орқали ахборотларни узатиш, программани бажаришга буюртма юбориш ва натижани олиш, маълумотлар базасига мурожаат ва ҳ. тушунилади.

2. Ўзаро алоқада бўлган жараёнларнинг ҳақиқий эканлигини тасдиқлаш

Узоқлаштирилган жараёнлар ўзаро алоқа қилишларидан олдин ҳақиқий эканликларига қаноат ҳосил қилишлари лозим. Алоқадаги

жараёнларнинг ҳақиқийлигини текшириш қуйидаги усуллар ёрдамида амалга оширилади.

- *идентификаторларни айирбошлаш;*
- *«қўл беришиш» муолажаси;*
- *калитларни тақсимлашда аутентификациялаш.*

Идентификаторларни айирбошлаш тармоқда симметрик (махфий) шифрлашдан фойдаланилганда ишлатилади. Шифрланган ахборотдаги идентификатор ахборот шифрлаш калитини ҳамда шахсий идентификаторни биладиган фойдаланувчи томонидан тузилганлигини кўрсатади. Бузғунчи учун керакли жараёнлар билан алоқа қилишнинг ягона имконияти мавжуд. У ҳам бўлса, ушлаб қолинган ахборотни хотирлаш, сўнгра алоқа каналига узатиш. Бундай хавфга ахборот узатилиш вақтини кўрсатиш орқали тўсқинлик қилиш мумкин. Вақт ўрнига ҳар бир жўнатишдан аввал шакллантирилувчи тасодифий сонлардан фойдаланиш мумкин. Ахборотни текширишда-ахборот қабул қилувчининг компьютер тизимсидаги сеансларни рўйхатга олиш журналини кўриб чиқиш кифоя.

«Қўл беришиш» муолажасининг иккита варианти фарқланади: бегоналар билмайдиган савол ва жавобларни айирбошлаш ва фақат ўзаро алоқа ўрнатаётган жараёнларга маълум бўлган f(x) функциядан фойдаланиш. f(x) функциядан фойдаланишда биринчи жараён x катталигини шакллантиради ва иккинчи жараёнга узатади; иккинчи жараён махфий алгоритм ёрдамида y=f(x) функцияни ҳисоблайди ва биринчи жараёнга узатади; биринчи жараён y=f(x) функцияни ҳисоблайди ва биринчи жараёндан олингани билан таққослайди. Агар таққослаш натижаси ижобий бўлса, ўзаро алоқадаги томонларнинг ҳақийлиги хусусида хулоса қилинади.

Калитларни тақсимлаш калитларни бошқаришдаги муолажалардан бири ҳисобланади. Калитларни тақсимлашнинг қуйидаги муолажаларини фарқлаш мумкин: калитларни шакллантириш, тақсимлаш, сақлаш ва алмаштириш.

Шакллантириш жараёнида калит тасодифий тарзда ҳосил қилиниши лозим. Шунинг учун калитни шакллантириш дастлабки маълумот сифатида таймер кўрсаткичидан фойдаланувчи псевдотасодифий генератор ёрдамида амалга оширилади.

Махфий калитлар хотирловчи қурилмада шифрланган ҳолда сақланади. Шифрланган калитнинг калити бошқа калит ёрдамида шифрланиши мумкин. Охирги калит очиқ ҳолда махсус хотирада сақланади ва ишлашнинг оддий режимида ўқилмаслиги, кўрилмаслиги, ўзгартирилмаслиги ёки йўқотилмаслиги лозим. Бу калит бош ёки мастер калит деб юритилади.

Бу калитни қайта-қайта ишлатилиши уни заифлаштиради. Шу сабабли маълумотларни шифрлаш калитларини мунтазам тарзда алмаштириб туриш шарт. Одатда маълумотларни шифрлаш калитлари

ишлашнинг ҳар бир сеансида алмаштирилади, шу сабабли бу калитлар сеансли калитлар деб аталади.

Тармоқда калитларни фойдаланувчилар ўртасида тақсимлаш иккита усулда амалга оширилади:

1. Битта ёки бир неча калитларни тақсимлаш марказларини тузиш.

2. Калитларни тармоқ абонентлари ўртасида бевосита айирбошлаш.

Биринчи усулнинг камчилиги сифатида калитларни тақсимлаш мақсадида тармоқ орқали узатилаётган барча ахборотдан фойдаланиш имкониятини кўрсатиш мумкин бўлса, иккинчи усулда жараёнлар ва абонентларнинг хақиқийлигини текширишда қийинчиликлар туғилади.

3. Коммуникацион қисм тармоқ орқали олинувчи ахборотнинг хақиқийлигини тасдиқлаш

Алоқа ўрнатилгандан сўнг ахборот айирбошлаш жараёнида сохталаштиришлардан химояланиш зарур. Бунинг учун қуйидаги тўртта шартнинг бажарилишини таъминлаш лозим:

- *маълумотларни қабул қилувчи уларнинг ҳақиқийлигига ишонч ҳосил қилиши лозим;*
- *маълумотларни узатувчи уларнинг қабул қилувчига етишига ишонч ҳосил қилиш лозим;*
- *маълумотларни узатувчи уларнинг қабул қилинганлиги хусусидаги тасдиқнинг ҳақиқийлигига ишонч ҳосил қилиши лозим.*

Маълумотлар манбаи ва узатилувчи (етказилган) маълу-мотларнинг ҳақиқийлигини тасдиқлаш рақамли имзо ёрдамида амалга оширилади. Ахборотларни қабул қилинганлигини тасдиқлаш квитанция узатиш режимини ташкил этиш орқали бажарилади. Квитанция олинган ахборот хусусида назорат ахборотси бўлган қисқача ахборот ва рақамли имзодан ташкил топади. Рақамли имзо билан тасдиқланган бундай квитанцияни олган узатувчи ахборотнинг муваффаққиятли қабул қилинганига ишонч ҳосил қилади.

Ахборотнинг рақамли имзоси назоратловчи иккили кетма-кетликдан иборат. Бу кетма-кетлик ахборот маълумотларининг ва ахборот жунатувчи махфий калитининг хеш-функцияларини махсус ўзгартирилиши ёрдамида олинади. Шундай қилиб, рақамли имзо, бир тарафдан, ўзида ахборот маъмуриятнинг назорат характеристкасини (хеш-функциясини) элтса, иккинчи тарафдан ахборот мазмуни билан махфий калит эгаси ўртасидаги алоқани кўрсатади.

Хеш-функциянинг ишлатилиши ахборот маълумотлари-ни алмаштирилиши ёки турлантирилишини аниқлашга имкон беради. Рақамли имзо ғояси биринчи марта 1976 йили Америка мутахасислари У.Диффи ва М.Хеллман тарафидан тавсия этилган. Ҳозирда рақамли имзони

шакллантиришда очиқ (носимметрик) калитли шифрлаш методларидан фойдаланилади.

Назорат саволлари

1. Тармоқ қандай қисм тизимларига ажратилади?
2. Коммуникацион қисм тизимининг таркиби.

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

5-Амалий машғулот. Компьютер тизимлари ва тармоқларини рухсатсиз ўзгартиришлардан ҳимоялаш воситалари

Режа:

1. Компьютер тизимлари ва тармоқларида хавфсизлик ҳолатини текшириш дастури.
2. Компьютер тизимлари ва тармоқларида маълум бўлган заифликлар ва тармоқ воситаларини текшириш дастурлари.

1. Компьютер тизимлари ва тармоқларида хавфсизлик ҳолатини текшириш дастури.

Корхоналарда жорий этилаётган автоматлаштирилган ахборот тизимининг хавфсизлигини таъминлаш, биринчи навбатда, ушбу тизимни лойиҳалаш босқичида кўзда тутилган бўлиши лозим. Корхона миқёсида қабул қилинган хавфсизлик сиёсатининг ахборот тизимида қандай даражада акс эттирилиши муҳим масалалардан бири ҳисобланади. Лекин, ахборот-коммуникациялар технологияларининг кескин ривожланиши, ахборот оқимлари хажмининг ошиши. Internet ва Intranet технологияларининг кенг миқёсда кириб келиши бевосита автоматлаштирилган ахборот тизимларининг ахборот заҳираларини ҳимоялашга йуналтирилган воситаларнинг мавжудлигини таъминлаш хамда тизимда мавжуд бўлган ҳимоя воситаларини ривожлантиришини тақозо этади.

Автоматлаштирилган ахборот тизимларига нисбатан мавжуд бўлган хавфларни учта йўналиш бўйича ажратиш мумкин:

- амалий дастурлар;
- тармоқ хизматлари;
- операцион тизим хизматлари.

Амалий дастурларни текшириш бўйича хозиргача ягона восита мавжуд эмас. Тармоқ хизматлари ва операцион тизим хизматларида қўлланиладиган технологиялар умумий асосларга эга бўлганлиги учун уларни текшириш воситалари ишлаб чиқилган.

Замонавий операцион тизимларда ахборот захираларини ҳимоялаш воситаларининг мавжудлиги таъкидлаб келинмоқда. Буларга аутентификациялаш, идентификациялаш, рухсатсиз киришни таъқиқлаш, мониторинг ва аудит, криптография усулларининг мавжудлиги мисол бўла олади. Албатта, ушбу воситаларнинг операцион тизимларда мавжуд бўлганлиги корхонанинг хавфсизлик сиёсатига мос келади. Аммо, операцион тизимнинг нотўғри конфигурацияланиши ва унинг дастурий таъминотидаги мавжуд хатолар оқибатида ахборот тизимларига хужумлар уюштирилиши имконияти пайдо бўлади.

Шу боис, операцион тизимни танлашда ундаги камчиликларни таҳлил қилиш, ишлаб чиқарувчи фирма томонидан йўл қўйилган хатоларнинг тан олиниши ва уларни зудлик билан тузатишга киришилиши талаб этилади.

Операцион тизимнинг параметрларининг тўғри ўрнатилганлигини ёки уларнинг ўзгармаганлигини текшириш учун «тизим хавфсизлигини сканерлаш» деб номланувчи 10 га яқин махсус дастурлар ишлаб чиқарилган. Масалан, Solaris операцион тизими учун мўлжалланган ASET, Netware ва NT учун KSA, Unix учун SSS дастурлари мавжуд.

SSS (System Security Scanner) дастури хақида

Ушбу дастур Unix операцион тизими ўрнатилган компьютерларда хавфсизлик холатини текшириш ва операцион тизимнинг ташқи хамда ички заиф қисмларини аниқлашга йўналтирилган. Бундан ташқари у кириш хуқуқларини, файлларга эгалик қилиш хуқуқларини, тармоқ заҳираларини конфигурациялашни, аутентафикациялаш дастурларини ва бошқаларни текшириши мумкин.

Дастурнинг қуйидаги имкониятлари мавжуд:

- конфигурацияни текшириш, яъни рухсатсиз киришларнинг олдини олиш мақсадида конфигурацияни текшириш. Бунга қуйидагилар киради: конфигурация файллари, операцион тизим версияси, кириш хуқуқлари, фойдаланувчиларнинг заҳиралари, пароллар;

- тизимдаги хавфли ўзгаришларни текшириш. Рухсатсиз киришлар оқибатида тизимда содир бўлган ўзгаришларни қидиришда қўлланилади. Бундай ўзгаришларга қуйидагилар киради: файллар эгаллаган хотира хажмининг ўзгариши, маълумотларга кириш хуқуқи ёки файлдаги маълумотларнинг ўзгариши, фойдаланувчиларнинг заҳираларга кириш параметрларининг ўзгариши, файлларни рухсатсиз бошқа бир ташқи компьютерларга узатишлар;

- фойдаланувчи интерфейсининг қулайлиги. Бу интерфейс ёрдамида нафақат дастур билан қулай ишлаш таъминланади, балки бажарилган ишлар бўйича хисоботлар хам яратилади;

- масофадан сканерлаш. Тармоқдаги кампьютерларни текшириш ва алоқа жараёнида маълумотларни шифрлаш имконияти таъминланади;

- хисоботлар тузиш. Бажарилган ишлар бўйича тўлиқ, хисоботлар яратилади. Ушбу хисоботларда тизимнинг аниқланган заиф бўғинларининг изоҳи келтирилади ва уларни тузатиш бўйича кўрсатмалар берилади. Хисобот HTML ёки оддий матн кўринишида бўлиши мумкин.

SATAN дастури хақида

Тармоқ хизматларининг ҳимояланганлигини таҳлил қилиш бўйича биринчи бўлиб ишлаб чиқарилган дастурлардан бири бу SATAN дастуридир. Бу дастур 20 га яқин тармоқ хизматларидаги заифликларни аниқлай олади.

2. Компьютер тизимлари ва тармоқларида маълум бўлган заифликлар ва тармоқ воситаларини текшириш дастурлари

Internet Scanner SAFEsuite дастури хақида

Агар текширувлар доимий равишда ва тўлиқ амалга оширилиши талаб қилинса, у хақда Internet Scanner SAFEsuite дастурлар пакети таклиф

қилинади. Бу дастурлар пакети ёрдамида 140 та маълум бўлган заифликлар ва тармоқ воситалари, яъни тармоқлараро экранлар, Web-серверлар, Unix, Windows 9.x, Windows NT тизимли серверлар ва ишчи станциялар, умуман TCP/IP протоколи қўлланиладиган барча воситалар текширилади.

Internet Scanner SAFEsuite пакетинииг умумий имкониятлари қуйидагилардан иборат:

1. Автоматлаштирилган ва конфигурацияланган сканерлаш:

• автоматлашган идентификациялаш ва заиф қисмлар бўйича ҳисобот тузиш;

• доимий режа бўйича сканерлаш;

• IP манзилларни сканерлаш;

• фойдаланувчи ўрнатган параметрларни сканерлаш;

• заиф бўғинларни автоматик равишда тузатиш;

• ишончлилик ва такрорланувчанликни таъминлаш.

2. Хавфсизликни таъминлаш:

• тармоқ воситаларини инвентаризациялаш ва мавжуд асосий заиф бўғинларни идентификациялаш;

• асосий хисоботларни таққослаш ва келгусида улардан фойдаланиш учун таҳлил қилиш.

3. Фойдаланишнинг оддийлиги:

• фойдаланувчининг график интерфейси;

• HTML туридаги тартибланган хисоботларни яратиш;

• сканерлашни марказлаштирилган ҳолда бажариш, бошқариш ва мониторинг ўтказиш.

Internet Scanner SAFEsuite пакетида қуйидаги дастурлар мавжуд: Web Security Scanner, FireWall Scanner ва Intranet Scanner.

Web Security Scanner бевосита Web-серверларда мавжуд заиф қисмларни аниқлашга мўлжалланган бўлиб, бу дастурнинг имкониятлари қуйидагилардан иборат:

• Web-сервер ўрнатилган операцион тизимни аудитлаш;

• Web-серверда мавжуд дастурларни аудитлаш;

• Web-файлларда мавжуд скриптларни аудитлаш;

• Web-сервер конфигурациясини тестдан ўтказиш;

• асосий файллар тизимининг хавфсизлик даражасини аниқлаш;

• скриптларда мавжуд хатоларни аниқлаш;

• бажарилган ишлар бўйича хисоботлар яратиш ва хатоларни тузатиш борасида таклифлар бериш.

FireWall Scanner дастури бевосита тармоқлараро экранда мавжуд бўлган заиф қисмларни аниқлашга мўлжалланган бўлиб, у қуйидаги амалларни бажаради:

• тармоқлараро экранга хужумлар уюштириб, уни тестдан ўтказиш;

• тармоқлараро экран орқали ўтадиган тармоқ, хизматларини сканерлаш.

Intranet Scanner дастури компьютер тармоғида мавжуд камчиликларни тармоққа рухсатсиз киришларини амалга ошириш орқали тестдан ўтказиш ёрдамида аниқлашга йўналтирилган. Тармоқнинг ҳар хил қисмлари (хост-компьютерлар, йўлловчилар, Web-серверлар, Windows 9.x/NT тизимида ишлайдиган компьютерлар) ни текширишни хам амалга оширади.

Юқорида келтирилганлардан ташқари компьютер тизимларига рухсатсиз киришларни доимий равишда назорат қилувчи дастурлар, масалан, Internet Security Systems компанияси томонидан ишлаб чиқилган **Real Secure** дастури хам мавжуд. Бу дастур тармоқда содир этилаётган ходисалар, масалан, хакерларнинг хужумларини қайд қилиш билан биргаликда фаол ҳимоя чора-тадбирларини ташкиллаштириши мумкин. Real Secure дастури йирик ташкилотлар учун мўлжалланган бўлиб, хар куни тинимсиз ишлашга мўлжалланган.

Real Secure дастури икки қисмдан иборат: **фильтрлаш** ва фойлаланувчининг **график ннтерфейси.**

Фильтрлаш қисми тармоқда содир этилаётган ходисаларни фаол кузатиш ва бошқариш учун хизмат қилади. Дастурнинг иккинчи қисми ёрдамида фойдаланувчи рўй берган ходисалар хақидаги маълумотларни қабул қилади, уларни бошқаради ва тизим конфигурациясини ўзгартира олади. Натижада, фильтрлаш ва содир этилаётган ходисаларга нисбатан ҳимоя тадбирларини автоматик равишда амалга ошириш мумкин бўлади, масалан, қайд қилиш, дисплейга чиқариш, ходисани ман этиш ва бошқалар.

Булардан ташқари барча қайд этилган ходисалар хақидаги маьлумотларни кейинчалик реал масштабда ёки тезкор ёки секинлашган режимларда кўриб чиқиш мумкин бўлади.

Назорат саволлари

1. Автоматлаштирилган ахборот тизимларига нисбатан мавжуд бўлган хавфларни санаб беринг.
2. SSS дастури қандай ҳолатларда қўлланилади?
3. Internet Scanner SAFEsuite дастурининг асосий имкониятлари нималардан иборат?
4. Real Secure дастурида филтрлаш қандай амалга оширилади?

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.

2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

6-Амалий машғулот. Компьютер тизимлари ва тармоқларини рухсатсиз фойдаланишлардан ҳимоялаш.

Режа:

1.Фойдаланувчи қисм тизимда ва ихтисослаштирилган коммуникацион компьютер тизимларида ахборот хавфсизлигини таъминлаш;

2.Компьютер телефониясидаги ҳимоялаш усуллари.

1.Фойдаланувчи қисм тизимда ва ихтисослаштирилган коммуникацион компьютер тизимларида ахборот хавфсизлигини таъминлаш

Аутентификация механизмини таъминлаш зарурияти ва объект ресурсларидан узоқдаги фойдаланувчиларнинг фойдаланишини чегаралаш зарурлиги ҳамда тармоқда махсус коммуникацион компьютер тизимларининг мавжудлиги-компьютер тармоқлари объектларининг ҳимояси хусусиятидир. Узоқлашган фойдаланувчилар ҳақиқийлигини тасдиқлаш муаммоси муҳим бўлганлиги сабабли бу муаммони ечиш механизмлари алоҳида гуруҳга ажратилган. Коммуникацион қисм тизимининг алоқа каналларидан бўлак барча элементлари ихтисослаштирилган коммуникацион компьютер тизимлари сифатида кўрилади. Ҳимояланган корпоратив тармоқларда концентраторлар, комуникацион модуллар (серверлар), шлюзлар ва кўприклар объектларда фойдаланувчиларнинг компьютер тизимлари билан биргаликда жойлаштирилиши лозим.

Компьютер тизимларида фақат хизматчи ахборот маъновий ишланади. Хизматчи ахборотга адрес ахбороти, ахборотларни бузилишидан химояловчи ортиқча ахборот, фойдаланувчилар идентификатори, вақт белгиси, ахборотлар (пакетлар) тартиб рақами, шифрлаш атрибутлари ва бошқа ахборот киради. Ахборотлардаги фойдаланувчилар ахбороти (ишчи ахборот) коммуникацион компьютер тизимлари сатҳида битлар кетма-кетлиги сифатида кўрилади ва бу кетма-кетлик коммуникацион қисм тизим орқали ўзгартиришсиз етказилиши шарт. Шу сабабли бундай тизимларда ишчи ахборот мазмунини очмасликдек муҳим имконият мавжуд. Ишчи ахборотдан операторлар ва коммуникацион компьютер тизимларининг ходимлари фойдалана олмасликлари лозим. Бундай ахборот коммуникацион қисм тизимнинг бошқа элементига муваффақиятли узатилганидан сўнг ташқи хотира қурилмаларида сақланмаслиги лозим. Берк тизимларда ишчи ахборот коммуникацион қисм тизим доирасида шифрланган ҳолда айланади.

Икки хил шифрлаш фарқланади: абонентли ва чизиқли. Абонент ахборотни юборишдан олдин уни махфий ёки очиқ калит ёрдамида шифрлайди. Коммуникацион қисм тизимсининг кириш йўлида ахборот, хатто абонентли шифрлаш бажарилмаганида ҳам, чизиқли шифрланади.

Чизиқли шифрлашда ахборот тўлалигича, барча хизматчи маълумотлари билан шифрланади. Чизиқли шифрлаш турли калитлар ёрдамида бажарилиши мумкин. Бу ҳолда бузғунчи битта калит ёрдамида каналларнинг чегараланган сонидаги узатилаётган ахборотдан фойдаланиши

мумкин. Агар турли калитлар ишлатилса коммуникацион модулларда нафақат хизматчи ахборот, балки ахборот тўлалигича расшифровка қилинади(ишчи ахборот абонент сатҳида шифрланган ҳолда қолади). Очиқ хизматчи ахборот ёрдамида ахборот яхлитлиги текширилиб, кейинги маршрут танланади ва узатувчига «квитанция» узатилади. Ахборот янги калит ёрдамида шифрланади ва мос алоқа канали бўйича узатилади.

Тармоқни бошқариш марказида ахборотни ҳимоя-лашнинг алоҳида чоралари кўрилиши лозим. Бу марказда бутун тармоқ ишлашида ниҳоятда зарур ахборот тўпланганлиги сабабли ахборот ҳимоясининг замонавий мукаммал воситаларидан фойдаланишга тўғри келади. Калитларни сақлаш ва улар билан ишлаш билан боғлиқ муолажа ва воситалар ҳимоясига алоҳида эътибор бериш лозим.

Тармоқ маъмурияти коммуникацион қисм тизимнинг барча операторлари каби фақат хизматчи ахборот билан иш кўради. Агар тармоқда абонент шифрлаш учун калитлар тармоқни бошқарувчи марказ томонидан тақсимланса, маъмурият тармоқнинг барча калитларидан ва, демак, тармоқда сақланаётган ва узатилаётган ахборотдан фойдаланиши мумкин. Шу сабабли маъмуриятнинг ихтисослаштирилган компьютер тизимсида маъмуриятга тегишли бўлмаган ахборотларнинг информацион қисми билан ишлаш имкониятини тўсувчи механизмлар кўзда тутилиши лозим.

Калитлар маъмуриятга ҳам, абонентларга ҳам маълум бўлмаган тақдирда калитларни ишончли бошқариш мумкин. Бунда калит тасодифий сонлар генератори ёрдамида шакллантирилиб махсус ассоциатив хотира қурилмасига ёзилади ва барча харакатлар компьютер тизимси оператори кира олмайдиган берк фазода амалга оширилади.

2. Компьютер телефониясидаги ҳимоялаш усуллари

Электрон коммуникацияларнинг замонавий технологиялари кейинги пайтларда ишбилармонларга алоқа каналлари бўйича ахборотнинг турлича кўринишлари (масалан: факс, видео, компьютерли, нутқли ахборотлар)ни узатишда кўпгина имкониятлар яратиб бермокда.

Замонавий офис бугунги кунда алоқа воситалари ва ташкилий техника билан хаддан ташқари тўлдириб юборилган ва уларга телефон, факс, автожавоб аппарати, модем, сканер, шахсий компьютер ва х.к. киради. Замонавий техника учун ахборот-коммуникациялар технологияси — **компьютерлар телефонияси** ривожланиши билан катта туртки берилди.

Бор-йўғи ўн йил илгари сотувга CANON фирмасининг нархи 6000 АҚШ доллари бўлган «Navigator» номли маҳсулоти чиқарилган эди ва у биринчи тизимлардан ҳисобланади.

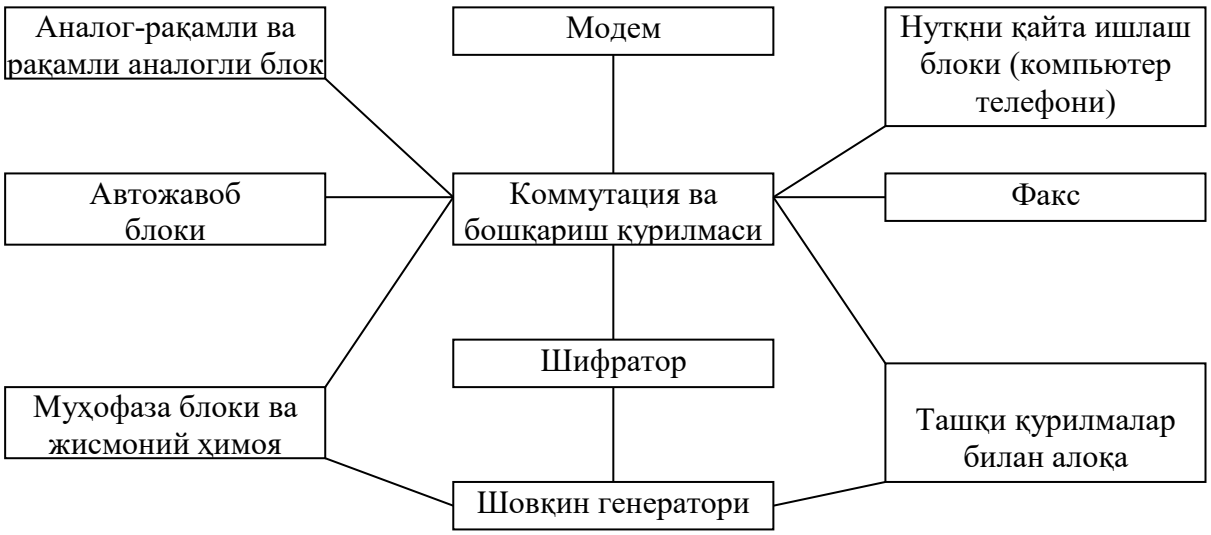
Компьютер телефонияси ўн йил ичида жуда тез суръатлар билан ривожланди. Ҳозирги пайтда сотувда мавжуд бўлган «PC Phone» (Export Industries Ltd, Israel) махсулотининг нархи бор-йуги 1000 Германия маркаси туради. «Powertine-II» (Talking Technology, USA)нинг нархи эса 800 АҚШ

доллари туради. Кейинги пайтларда компьютер телефонияси йуналишида 70% аппарат воситаларини Dialogue (USA) фирмаси ишлаб чиқармоқда.

Компьютер телефониясида ахборотларнинг хавфсизлигини таъминлаш катта аҳамиятга эга. Масалан, телефон хакерларининг Скотланд-Ярд АТСига кириб 1,5 млн, АҚШ доллари миқдорида зарар келтиришганлиги хавфсизликнинг зарурлигини исботлайди.

Компьютер телефониясида қўлланилаётган нутқини аниқловчи технология телефон қилувчининг овозидан таниб олиш учун аҳамиятга эгадир. Компьютер телефониясининг ҳимоясини етарли даражада таъминлаш учун Pretty Good Privacy Inc. фирмасининг PC Phone 1.0 дастурий пакет ишлаб чиқарилган. У компьютер телефонияси орқали узатилаётган ахборотларни ҳимоялаш учун ахборотларни рақамли кўринишга ўтказади ва қабўл пайтда эса дастурий-техник воситалар ёрдамида қайта ишлайди. Замонавий компьютер телефонияси воситатарининг шифрлаш тезлига ҳам жуда юқоридир, хато қилиш эҳтимоли эса жуда кичикдир (тахминан $10^{-8} – 10^{-12}$).

Замонавий компьютер телефонияси қурилмаси чизмаси қуйидагича:



Компьютер телефонияси қурилмалари қуйидаги имкониятларга эга:

Қурилмалар	**Имкониятлар**
Компьютер телефони	Нутқли хабарни ёзиб олиш ва сақлаш, хабарларни қайд қилиш, кодни аниқлаб олиш, қайта уланиш, хабарларни узатиш
Шифратор	Маълумотларни ҳимоялаш, маълумотларни аниқлигини сақлаш, маълумотларга киришни чегаралаш
Модем	Абонентни қайта текшириш, хатони тузатиш
Факс	Криптоҳимоя, узатилаётган ахборотни қисиш, автоқайд этиш ва узатиш
Автожавоб қурилмаси	Қайд этиш журналига автоматик равишда қайд қилиш, абонентни тескари алоқа билан текшириш, тайёр қилиб қўйилган нутқли хабарларни узатиш, киритилаётган хабарларни ёзиб олиш
Ҳимоя қурилмаси	Ташқи датчиклардан сигналлар олиш, хотирадаги рақамларни автоматик териш, рухсатсиз алоқалар хақида нутқли хабар бериш, ташқи қурилмаларни улаб бериш ва х.к.

.

Назорат саволлари

1. Фойдаланувчи қисм тизимда ва ихтисослаштирилган коммуникацион компьютер тизимларида ахборот хавфсизлигини таъминлаш.
2. Компьютер телефониясидаги ҳимоялаш усуллари.

Фойдаланилган адабиётлар рўйхати

4. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
5. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
6. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.

7-Амалий машғулот. Ҳимояланган компьютер тизимлари ва тармоқларини қуриш концепцияси (4 соат)

Режа:

1. Ҳимояланган компьютер тизимлари ва тармоқларини бошқаришнинг функционал масалалари.
2. Хавфсизлик воситаларини бошқариш архитектураси.

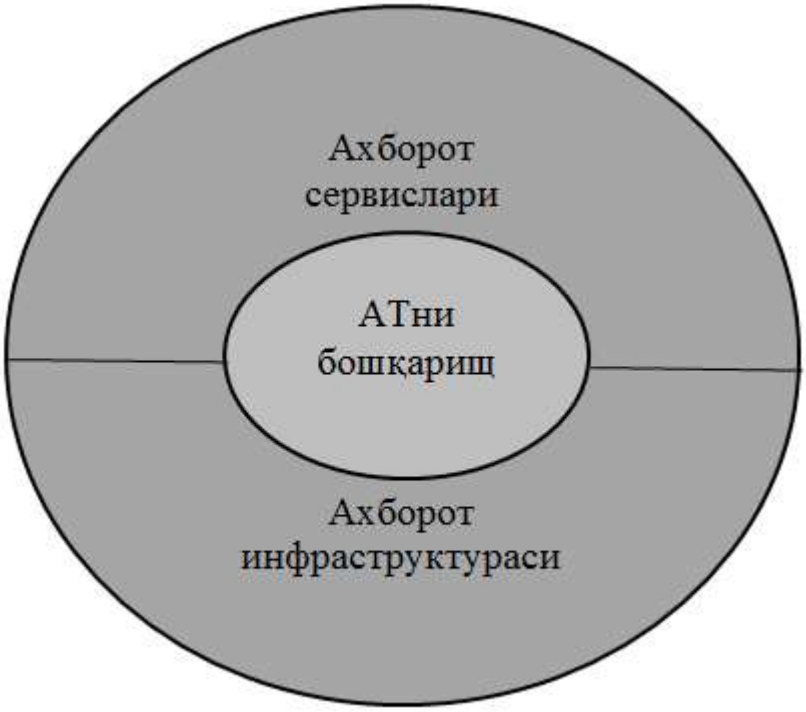
1. Ҳимояланган компьютер тизимлари ва тармоқларини бошқаришнинг функционал масалалари

Замонавий ахборот технологияларидан муваффақиятли фойдаланиш учун нафақат тармоқларнинг ўзини, балки тармоқ хавфсизлиги воситаларини ҳам ишончли ва самарали бошқариш зарур. Ҳозирги вақтда компаниянинг бутун инфратузилмасини қамраб олувчи бошқаришнинг комплекс тизимини яратиш биринчи галдаги вазифа ҳисобланади. Бундай бошқариш тизими ахборот тизимининг мураккаблиги ва масштабидан қатъий назар, қуйидагиларга имкон яратади:

- бутун ахборот инфратузилмасига марказлаштирилган ва оператив бошқариш таъсирни кўрсатиш;
- оператив ечимларни қабул қилиш учун ахборот хавфсизлиги ҳолати хусусидаги объектив ахборотни берувчи мунтазам аудитни ва кенг кўлҳамдаги мониторинг ўтказиш;
- ахборот инфратузилмаси ривожини башоратлаш учун унинг ишлаши хусусидаги статистик маълумотларни тўплаш.

Ахборот тизимларини бошқаришнинг ITIL методологияси

ITIL (IT Infrasructure Library) методологиясига мувофиқ ахборот тизими иккита йирик блокдан — ахборот инфратузилмаси ва ахборот сервисларидан иборат (7.1-расм).



7.1–расм. ITIL методологияси нуқтаи назаридан ахборот тизимининг кўриниши

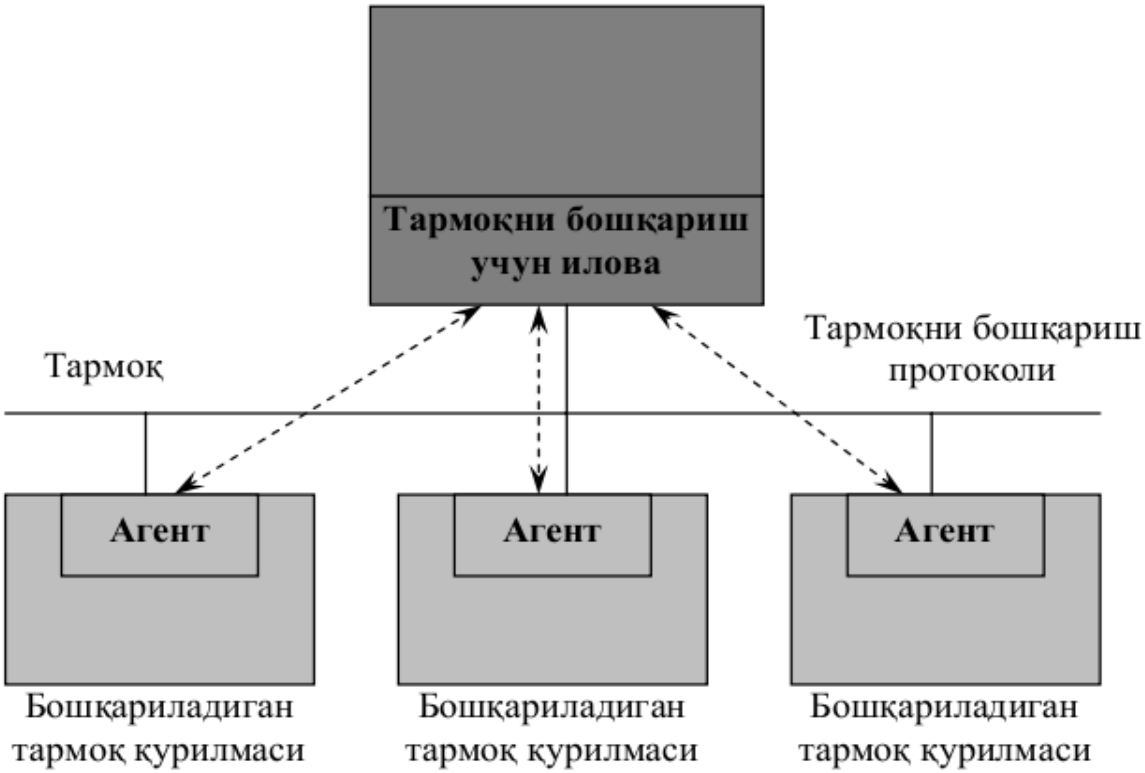
Ахборот инфратузилмаси ахборот сервислари ишловчи моддий асос, муҳит ҳисобланади. Ахборот сервисларига Internet-сервислар, иловалар сервиси, бошқариш, ечим қабул қилиш сервислари ва ҳ. киради. Ахборот инфратузилмаси сервислар ишлашини таъминловчи техник воситалар, алоқа линиялари, муолажалар, меъёрий хужжатлар ва ҳ. мажмуидир. Ахборот сервисларининг сифати бевосита ахборот инфратузилмаси ва уни бошқариш сифатига боғлиқ.

Ахборот инфратузилмасини асосида ахборот ресурслари (ҳисоблаш платформалари, серверлар, шахсий компьютерлар, маълумотларни узатиш тармоқлари, алоқа линиялари) ётувчи пирамида сифатида тасаввур этиш мумкин (7.2-расм).

7.2–расм. Ахборот инфратузилмасини ташкил этувчилари

Пирамиданинг иккинчи сатҳини турли иловалар ташкил этади. Бу иловалҳар биринчи сатҳ ресурсларидан фойдаланиб татбиқий дастур таъминоти, электрон почта, кафҳолатланган етказиш тизими, маълумотлар базаси, Web-серверлар ва ҳ. каби муайян иловалар ишлашини таъминлайди. Ва ниоят, энг юқори сатҳда бизнес ва ишлаб-чиқариш жараёнларининг ўтишини таъминловчи иловалар ишлайди. Иккала пастки сатҳдан фойдаланувчи бу иловалар ишлаб-чиқаришни бошқариш, буюртмачилар ва таъмин ловчи билан ўзаро алоқа, молиявий ҳисоб ва ечимни қабул қилишни мададлаш каби бизнес масҳалаларни ечишга йўналтирилган.

Умумий ҳолда, тармоқни бошқариш тизимининг архитектураси 7.3-расмда келтирилган кўринишга эга. Тармоқни бошқариш иловаси тармоқ маъмурининг иш жойида ёки бошқа компьютерда бажарилиши мумкин. Унинг вазифаси бошқарилувчи қурилмаларда бажариладиган агент - иловалардан ёки операцион тизим сервисларидан келувчи бошқарилувчи объект хусусидаги ахборотни йиғиш.



7.3–расм. Тармоқни бошқариш тизимининг умумлаштирилган архитектураси

Бундай иловаларни агентлар билан ўзаро алоқаси учун одатда SNMP (Simple Network Management Protocol) ёки CMIP (Common Management Information Protocol) протоколларидан фойдаланилади. Биринчиси, одатда, локал тармоқда ишлатилса, иккинчиси телекоммуникациядан фойдаланувчи тақсимланган тармоқларда ишлатилади. Аммо дастур таъминотини баъзи ишлаб чиқарувчилари тармоқни бошқаришда хусусий тармоқ протоколларидан фойдаланишади.

Тармоқни бошқарувчи замонавий воситалар қуйидаги вазифаларни бажара олади:

- бошқарилувчи компьютер ва қурилмалардаги бузилишларни кузатиш, сабабларни аниқлаш ва бартараф этиш (кўпинча автоматик тарзда), оқибатларини тузатиш ва бузилишларни олдини олиш (масалан таш ислаш амалини бажариш орқали);

- компьютерларнинг ва тармоқ қурилмаларининг конфигурациялани-шини бошқариш (хусусан, инициализациялаш, қайта конфигурациялаш ва тармоқ қурилмалари ва компьютерларни узиб қўйиш);

-фойдаланувчилар ва фойдаланувчилар гуруҳи томонидан тармоқ ресурсларидан фойдаланишни тартибга солиш (масалан, дискли ва бошқа квоталарни тартибга солиш);

-тармоқ қурилмалари ва сервислар унумдорлигини бошқариш (тармоқ қурилмалари ишлатилиши жадаллиги статистикасини ва хатоликлар частотасини йиғиш ва тахлиллаш ҳамда олинган маълумотлар асосида улар унумдорлигини сунъий тарзда ўрнатиш);

- олдиндан белгиланган хавфсизлик сиёсати асосида тармоқ

ресурсларидан фойдаланишни назоратлашдан фойдаланиб маълумотлар ҳимғоясини бошқариш ва уларни бузишга уринишлардан маъмурни ҳабардор этиш.

Корхона ахборот хавфсизлиги тизими корпоратив тармоқни бошқариш тизимининг энг муҳим компонентиҳисобланади. Корхона масштабидаги тақсимланган тармоқда ахборотни ҳимоялаш воситаларини бошқарувчи тизим қуйидаги вазифаларни бажариши лозим:

- корхона тармоғи доирасида хавфсизлик сиёсатини бошқариш, алоҳида қурилмалар хавфсизлигининг локал сиёсатини шакллантириш ва уни ахборотни ҳимояловчи барча қурилмаларга етказиш;

- фойдаланиш объектларини ва субъектларини конфигурациялашни бошқариш; ҳимоя қурилмалари ва дастурий таъминоти таркибини, версиясини, компонентларини бошқаришни ўз ичига олади;

- тақсимланган татбиқий тизимларга ҳимоя сервисларини тақдим этиш, ҳимояланган иловалар ва улар ресурсларини руйхатга олиш. Иловаларнинг бу гуруҳи, аввало, татбиқий тизимлар томонидан ҳимоя сервисларини бошқариш учун интерфейсни таъминлаш лозим;

- криптовоситаларни бошқариш, хусусан калитли бошқариш (калитли инфратсруктура). Калитли инфратузилма инфратузилма хизмати таркибида ишлаши лозим;

- ходисавий протоколлаш; турли қурилмаларга логларни беришни созлашни, логларни деталлаштириш сатхини бошқаришни, протокол олиб борилувчи ходисаларни таркибини бошқаришни ўз ичига олади;

-ахборот тизими хавфсизлигини аудитлаш; ахборот тизимлари ҳимояланишининг жорий ҳолати хусусидаги объектив маълумотларни баҳолашни таъминлайди;

- тизим хавфсизлигини мониторинглаш; қурилмалар ва қурилмаларда кечувчи ходисалар (ҳимоялаш контекси бўйича)ҳолати, фаоллиги хусусида, масалан, бўлиши мумкин бўлган хужумлар хусусида реал вақтда ахборот олинишини таъминлайди;

- махсус ҳимояланган иловалар, масалан амаллар устидан нотариал назорат ишини таъминлаш ҳамда регламентда кўзда тутилган тадбирларни (калитларни, парҳолларни, ҳимоя қурилмаларини алмаштириш, смарткарталарни ишлаб чиқариш ва ҳ.) мададлаш;

- иловаларнинг лойиҳа-инвентаризациялаш гуруҳи ишини таъминлаш. Иловаларнинг бу гуруҳи корхона тармоғига ҳимоя воситаларини ўрнатишни, қўлланиладиган ҳимоя воситаларини ҳисобга олишни, ҳимоя воситаларининг модул таркибини назоратлашни, ҳолатини назоратлашни ва ҳ. бажаради.

Тармоқларни анъанавий бошқариш тизими ва тармоқдаги ахборотни ҳимоялаш воситаларини бошқариш тизими орасида ўзаро алоқани комплекслаш ва ташкил этиш муаммоси мавжуд.

2.Хавфсизлик воситаларини бошқариш архитектураси

Компаниянинг тақсимланган ахборот тизимида ўзининг хавфсизлик сиёсатини муваффақиятли амалга ошириши учун хавфсизликни бошқариш марказлиштирилган бўлиши ва ишлатиладиганоперацион тизимга ва татбиқий тизимларга боғлиқ бўлмаслиги лозим. Ундан ташқари, корпоратив ахборот тизимида кечувчи жараёнларни (рухсатсиз фойдаланиш, фойдаланувчилар имтиёзини ўзгариши ва ҳ.) рўйхатга олиш тизими ягона бўлиши ва маъмурга корпоратив ахборот тизимидаги барча ўзгаришларнинг тўлиқ кўринишини тасаввур этишига имкон бериши лозим.

Корпоратив ахборот тизими хавфсизлигини марказлаштирилган бошқариш асосида глобал бошқариш концепцияси GSM (Global Security Management) ётади. Ушбу концепция корхона ахборот ресурсларини қуйидаги хусусиятларга эга бўлган комплекс бошқариш тизимини қуришга имкон беради:

- корхонанинг барча ресурслари (хавфсизлик сиёсати объектлари) учун ҳимоялашнинг яхлитлигини, зиддиятлик эмаслигини ва қоидалар тўпламининг тўлалигини таъминловчи, барча мавжуд ҳимоя воситаларини корхона хавфсизлиги сиёсати асосида бошқариш;

- ресурсларни тавсифловчи шахсий воситалар ҳамда корхонанинг бошқа каталоглари билан алоқаси бўйича фаоллашувчи корхона муҳитининг ягона (тақсимланган) каталоги орқали корхонанинг барча ресурсларини аниқлаш;

- хавфсизлик сиёсатига асосланиб, ахборотни ҳимоялашнинг локал воситаларини марказлаштирилган бошқариш;

- корхона муҳитида сиёсат объектларини токенлар ва очиқ калитлар инфратузилмасидан фойдаланиб қатъий аутентификациялаш;

- каталогда белгиланган корхона ресурсларидан ёки бутун каталог қисмларидан фойдаланишни маъмурлашнинг кенгайтирилган имкониятлари;

-ҳисоб-китобликни (корпоратив тармоқ масштабида тизимнинг тақсимланган объектларининг ўзаро алоқасидаги барча амалларини руйхатга олиш) ва аудитни, хавфсизлик мониторингини, хавотирли сигнализацияни таъминлаш;

- умумий бошқариш тизимлари ва хавфсизликнинг инфратузилма тизимлари билан интеграцияланиши;

Ушбу концепция доирасида “хавфсизлик сиёсатига асосланган PBM (Policy Based Management) бошқариш” деганда корхона бизнес-объекти учун таърифланган қоидалар тўплами тушунилади. Бу қоидалар тўплами объектларнинг бизнес-соҳани тўлиқ қамраб олишини ва ишлатилувчи бошқариш қоидаларининг зиддиятлик эмаслигини кафҳолатлайди.

PBM принципларига асосланган, корхона хавфсизлигини бошқаришга мўлжалланган GSM бошқариш тизими қуйидаги талабларга жавоб беради:

- корхона хавфсизлиги сиёсати мантиқий ва семантик боғланган, шаклланувчи, таҳрирланувчи ва тахлилланувчи маълумотларнинг бир бутун тузилмасидан иборат;

- корхона хавфсизлиги сиёсати ягона контекстда ҳимоянинг барча сатҳлари учун ҳимоянинг тармоқ сиёсати ва корхона ахборот ресурслари хавфсизлик сиёсатининг бир бутуни сифатида белгиланади;

- корхона ресурсларини ва хавфсизлик сиёсатини маъмурлашни енгиллаштириш мақсадида сиёсат параметрлари сони минималлаштирилади.

GSM бошқариш тизими хавфсизлик сиёсатининг корхона хавфсизлиги концепцияси моделига мослигини текширувчи кўп мезонли воситалар эвазига хавфсизлик сиёсатини таҳлиллашнинг турли-туман механизмларини таъминлайди.

Хавфсизликнинг глобал ва локал сиёсатлари

Корхона хавфсизлигининг глобал сиёсати ахборот хавфсизлиги контекстида корпоратив тармоқ объектлари ўзаро алоқасининг параметрларини тавсифловчи хавфсизлик қоидаларининг чекли тўпламидир.

Бунда хавфсизликнинг глобал сиёсати объекти сифатида алоҳида ишчи станциялари ва қисм тармоқлар ҳамда ўз ичига компаниянинг бутун тузилмавий бўлимларини олувчи (масалан, маркетинг бўлими ёки молиявий департамент) объектлар гуруҳи ёки ҳатто алоҳида компания кўрилиши мумкин.

Хавфсизликнинг глобал сиёсати тармоқдаги ўзаро алоқага, ҳамда тизимнинг назоратлаш ва бошқариш функцияларига тааллуқли бўлиши мумкин. Бажарадиган функциялари бўйича хавфсизликнинг глобал сиёсати қуйидаги гуруҳ ларга бўлинади:

-*VPN қоидалари*. Қоидаларнинг бу гуруҳ и IPSec протоколлари ёрдамида амалга оширилади;

-*пакетли фильтрлаш қоидалари*. Бу қоидалар Stateful ва Stattles хилидаги пакетли фильтрлашни таъминлайди.

-*proxy-қоидалар*. Бу қоидалар берилган татбиқий протокллар бошқарувида узатилувчи трафикни фильтрлашга жавоб беради;

- *аутентификацияланган/авторизацияланган фойдаланиш қоидалари;*

-*сигнализацияга ва ходисавий протоколлашга жавоб берувчи қоидалар*.

Хавфсизликнинг глобал сиёсати тармоқ сатҳида хавфсизлик сиёсатининг мантиқий яхлит ва семантик тўлиқ тавсифи бўлиб, унинг асосида алоҳида қурилмалар хавфсизлигининг локал сиёсати қурилиши мумкин.

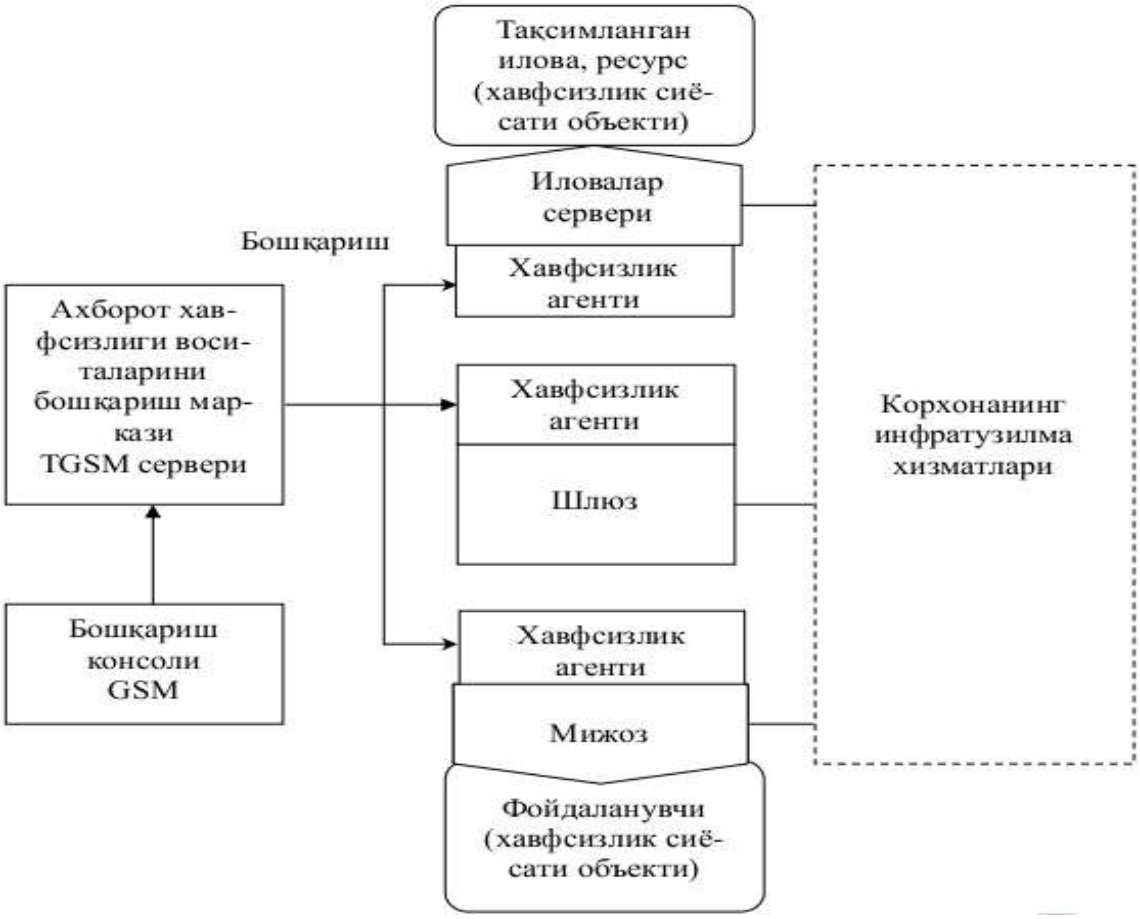
Хавфсизликнинг локал сиёсати ахборот хавфсизлигининг қандайдир сервисини амалга оширувчи ҳар қандай ҳимоялаш воситасига зарур ҳисобланади. Анъанавий ёндашишда маъмурга ҳар бир ҳимоя воситасини алоҳида созлашга ёки энг оддий созлашни узелларнинг катта сонига қайтаришга (репликациялашга) тўғри келар эди. Равшанки, бу маъмурлашнинг ката сонли хатолигига олиб келар ва натижада корпоратив тармоқнинг ҳимояланиш даражаси жиддий пасаяр эди.

Маъмур томонидан хавфсизликнинг глобал сиёсати шакллантирилганидан сўнг бошқариш маркази унинг асосида ҳар бир ҳимоя воситаси учун автоматик тарзда ҳимоялашнинг алоҳида локал сиёсатини

ҳисоблайди ва мос ҳимоя воситасининг бошқариш модулига зарурий созлашларни автоматик тарзда юклайди.

Тармоқда хавфсизликнинг глобал сиёсатини ва муайян қурилмада хавфсизликнинг локал сиёсатини амалга ошириш қоидаларининг бир биридан фарқи шундаки, хавфсизликнинг глобал сиёсатидаги қоидаларда фойдаланиш объектлари ва субъектлари тармоқ чегарасида ихтиёрий равишда тақсимланиши мумкин, хавфсизликнинг локал сиёсатидаги қоидалардан эса фақат тармоқ қурилмаларидан бирининг муҳити чегарасида фойдаланиш мумкин.

Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси 7.4—расмда келтирилган. Асосий хавфсизлик воситаларининг вазифалари қуйидагича. Мижоз шахсий компьютерида ўрнатилган хавфсизлик агенти одатда “мижоз-сервер” иловаларида мижоз сифатида



7.4–расм. Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилма схемаси

қатнашувчи алоҳида фойдаланувчини ҳимоялашга мўлжалланган.

Иловалар серверига ўрнатилган хавфсизлик агенти тақсимланган иловаларнинг сервер компоненти хавфсизлигини таъминлашга мўлжалланган.

Шлюз компьютерига ўрнатилган хавфсизлик агенти турли тармоқ хавфсизлиги сиёсатини мувофиқлаштириш масаласини ечган ҳолда, корхона

ичида ёки корхоналар орасида тармоқ агентларини ажратилишини таъминлайди.

Бошқариш маркази тармоқ масштабида хавфсизликнинг глобал сиёсатини тавсифлашни, глобал сиёсатни ҳимоялаш қурилмаси хавфсизлигининг локал сиёсатига трансляциялашни, ҳимоялаш қурилмасини юклашни ва тизимнинг барча агентлари ҳолатини назоратлашни таъминлайди.

Бошқариш консоли маъмур (маъмурлар) иш жойини ташкил этишга мўлжалланган. GSMнинг ҳар бир сервери учун бир неча консҳоллар ўрнатилиши мумкин.

Хавфсизликнинг локал агенти охирги қурилмада (мижозда, серверда, шлюзда) жойлаштирилувчи дастур бўлиб, қуйидаги функцияларни бажаради:

- хавфсизлик сиёсати объектларини аутентификациялаш, жумладан аутентификациялашнинг турли сервисларини интеграциялаш;
- тизимдаги фойдаланувчини ва у билан боғлиқ ходисаларни аниқлаш;
- хавфсизлик воситаларини марказлаштирилган бошқаришни ва фойдаланиш назоратини таъминлаш;
- иловалар манфаати учун ресурсларни бошқариш, татбиқий сатҳ ресурсларидан фойдаланишни бошқаришни мададлаш;
- трафикни ҳимоялаш ва аутентификациялаш;
- трафикни фильтрлаш;
- ходисавий протоколлаш, мониторинг, хавотирли сигнализация.

Локал агентнинг марказий элементи — хавфсизликнинг локал сиёсатининг процессори (LSP processor) хавфсизликнинг локал сиёсатини изоҳлайди ва бошқа компонентлар орасида чақиришларни тақсимлайди.

Назорат саволлари

1. Бошқаришнинг комплекс тизимини қуриш қандай имкониятларни яратади?
2. Тармоқни бошқариш тизимининг умумлаштирилган архитектураси нималардан ташкил топган?
3. SNMP ва CMIP протоколлари нима мақсадда қўлланилади?
4. Хавфсизлик сиёсатига асосланган PBM бошфаруви нима мақсадда қўлланилади?
5. Ахборот хавфсизлиги воситаларини бошқариш тизимининг умумий тузилмасидаги хавфсизлик агенти ва шлюзнинг вазифаси нимадан иборат?

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

8-Амалий машғулот. Компьютер тизимлари тармоқларида ахборот хавфсизлигини таъминловчи комплекс тизимни қуриш (4-соат)

Режа:

1. Ахборот тизимларининг аудити ва мониторинги.
2. Хавф-хатарларни тахлиллаш ва бошқариш.
3. Ахборот хавфсизлиги тизимини қуриш методологияси.

1. Ахборот тизимларининг аудити ва мониторинги

Ахборот хавфсизлиги тизими амалга оширилганида тармоқ инфратузилмасини мураккаблиги, маълумотлар ва иловаларнинг турли-туманлиги сабабли кўпгина таҳдидлар хавфсизлик маъмурининг эътиборидан четга қолиши мумкин. Шунинг учун ахборот тизимларининг мунтазам аудити ва доимий мониторинги амалга оширилиши зарур.

Ахборот тизимлари хавфсизлигининг аудити. Аудит-корхонанинг алоҳида соҳаларини мустақил экспертизаси. Корхона аудитининг ташкил этувчиларидан бири унинг ахборот тизими аудити ҳисобланади. Ахборот тизимларининг аудити — ахборот тизимининг ҳимояланишининг жорий ҳолати, ундаги ҳаракатлар ва ходисалар хусусидаги объектив маълумотларни олиш ва баҳолаш, улар сатҳининг белгиланган мезонга мослигини аниқловчи тизимли жараёндир. Аудит ўтказилиши ахборот тизимининг жорий хавфсизлигини баҳолашга, хавф-хатарни баҳолашга, уларнинг ташкилот бизнес-жараёнларига таъсирини башоратлашга ва бошқаришга, ташкилот ахборот ресурслари хавфсизлигини таъминлаш масаласига асосли ёндашишга имкон беради.

Ахборот тизимлари хавфсизлигининг аудити қуйидаги босқичларни ўз ичига олади:

- аудит муолажасининг бошланиши;
- аудит ахборотини йиғиш;
- аудит маълумотларини тахлиллаш;
- тавсиялар ишлаб чиқиш;
-ҳисобот тайёрлаш.

Аудит босқичларининг бажарилиш кетма-кетлиги 8.1—расмда келтирилган.

Аудит муолажасининг бошланиши. Аудит, бу масалада манфаатдор ҳисобланувчи, компания раҳбарияти ташаббуси билан ўтказилади. Аудит тадбирларнинг комплекси бўлиб, унда аудитор билан бирга компаниянинг аксарият тузилмавий бўлинмаларининг вакиллари қатнашади. Бу жараёнда иштирок этувчиларининг ҳаракатлари аниқ мувофиқлаштирилиши шарт. Шу сабабли, аудит муолажасининг бошланиши босқичида аудит ўтказиш режасини тайёрлаш ва тасдиқлаш, аудитор хуқуқи ва мажбуриятини белгилаш билан боғлиқ ташкилий масҳалалар ечилиши лозим.

Аудит муолажасининг бошланиши босқичида текшириш доираси аниқланиши лозим. Компаниянинг ахборот қисми тизимининг бирини конфиденциаллик нуқтаи назаридан аудитга тортиб бўлмаса, иккинчисини,

етарлича жиддий бўлмаганлиги сабабли, аудит доирасидан чиқариш мумкин.

8.1–расм. Аудит босқичларининг бажарилиш кетма-кетлиги

Аудит ахборотини йиғиш. Бу босқич энг мураккаб ва узоқ давом этади. Бунга сабаб, ахборот тизимга керакли хужжатларнинг йўқлиги ва аудиторнинг ташкилотнинг кўпгина лавозимли шахслари билан бевосита ўзаро мулоқотда бўлиши зарурияти. Аудитор ташкилот, ахборот тизимининг ишлаши ва жорий ҳолати хусусидаги ахборотни компаниянинг жавобгар шахслари билан махсус ташкил этилган сухбат орқали, техникавий ва ташкилий-бошқариш хужжатларни ўрганиш йўли билан,ҳамда ихтисослаштирилган дастурий воситалар ёрдамида ахборот тизимини тадқиқлаш орқали олади.

Аудит маълумотларини тахлиллаш. Тахлиллаш ахборот тизимларининг аудитида энг маъсулиятли босқич ҳисобланади. Тахлиллашда ноаниқ, эскирган маълумотлардан фойдаланиш ножоиздир, шу сабабли маълумотларга аниқлик киритилиши ва ахборотлар жиддий йи илиши мумкин. Аудит маълумотларини тахлиллашда қуйидаги учта ёндашишдан фойдаланилади.

Биринчи ёндашиш хавф-хатарларни тахлиллашга асосланади. Хавф-хатарларни тахлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар катталигини баҳолаш (уларга сифатий ва миқдорий баҳо бериш). Ушбу ёндашиш жуда мураккаб бўлиб, кўп меҳнат сҳарф этилади ва аудиторнинг

энг юқори малакасини талаб қилади.

Иккинчи ёндашиш ахборот хавфсизлиги стандартларидан фойдаланишга асосланган. Стандартлар ахборот тизимларининг кенг синфи учун дунё амалиётини умумлаштириш натижасида шаклланган хавфсизлик талабларининг базавий тўпламини белгилайди. Бу ҳолда аудитордан, берилган ахборо тизими учун стандарт талаблари тўпламини тўғри танлаш талаб этилади. Соддалиги ва ишончлилиги туфайли бу ёндашиш амалда кенг қўлланилади. У ресурсларнинг минимал сҳарфида ахборот тизими хусусида асосланган хулосалар қилишга имкон беради.

Учинчи ёндошиш олдинги иккала ёндашишни комбинациялашни кўзда тутади. Ахборот тизимига қўйиладиган хавфсизликнинг базавий талаблари стандарт орқали аниқланса, берилган ахборот тизими ишлашининг хусусиятларини ҳисобга олувчи қўшимча талаблар хавф-хатарларни тахлиллаш асосида шакллантирилади.

Тавсиялар ишлаб чиқиш. Тахлиллаш натижалари тавсиялар ишлаб чиқиш учун асос бўлади. Аудитор тавсиялари муайян ва берилган ахборот тизимига қўлланиладиган, иқтисодий асосланган, исботланган (тахлиллаш натижалари билан қувватланган), ва муҳимлик даражаси бўйича рутбаланган бўлиши шарт. Аудитнинг мунтазам ўтказилиши ахборот тизимининг барқарор ишлашини кафолатлайди. Шунинг учун профессионал аудит натижаларидан бири кейинги текширишларин ўтказиш режа-графигини шакллантиришдан иборат.

Ҳисобот тайёрлаш. Аудиторҳисоботи аудит ўтказишнинг асосий хужжати ҳисобланади ва унинг сифати аудитор ишининг сифатини характерлайди.

Ҳисобот таркибида аудит ўтказиш мақсадининг тавсифи, текширилувчи ахборот тизимининг характеристикаси, аудит ўтказиш доираси ва ишлатилувчи усуллар бўйича кўрсатма, аудит-маълумотлари тахлилининг натижаси, бу натижаларни умумлаштирувчи ва ахборот тизими ҳимояланиш сатҳининг стандарт талабларга жавоб бериши бўйича хулосалар ва албатта, мавжуд камчиликларни бартараф этиш ва ҳимоя тизимини такомиллаштириш бўйича тавсиялар бўлиши лозим.

Ахборот тизимлари хавфсизлигининг мониторинги

Ҳозирда тармоқлараро экран, виртуал хусусий тармоқ, рухсатсиз фойдаланишдан ҳимоялаш воситалари каби ҳимоянинг анъанавий воситалари ишончли ва самарали ахборот хавфсизлиги тизимини қуришга зарур бўлсада, етарли эмас. Чунки бу анъанавий воситалар фақат хужумни блокировка қилишга қодир, аммо хужумларни олдини олиш ва оқибатларини аниқлаш имконияти уларда мавжуд эмас.

Ушбу муаммонинг ечими асосланган ёндашиш фаол аудит технологияси ёки хавфсизликни фаол (адаптив) бошқариш технологияси номини олган. Хавфсизликни фаол бошқариш технологияси қуйидаги компонентларни ўз ичига олади:

- ишчи станциялари, серверлар, маълумотлар базасини бошқарувчи

тизимлар, тармоқ уланишлари ва Internet ва бошқа глобал тармоқларга уланиш нуқталари каби ахборот тизими объектлари ҳимояланишини тахлилловчи ва заифликларини қидирувчи воситалар;

- хужумларни аниқлаш ва тахлиллаш воситалари;

- инфратузилма ўзгаришида ёки хужумларда ҳимоялаш воситаларини вақтнинг реал режимида созлашларни мослаштириш ва бошқариш воситалари

Ахборот хавфсизлиги тизими мониторинги вазифаларини ҳимояланишни тахлиллаш ва хужумларни аниқлаш воситалари бажаради. Ҳимояланишни тахлиллаш воситалари ишчи станцияларида ва серверларда, маълумотлар базасида операцион тизим ҳимғояси элементларининг созланишини тадқиқлайди. Улар тармоқ топологиясини тадқиқлайди, ҳимояланмаган ёки нотўғри тармоқ уланишларини қидиради, тармоқлараро экранлар созланишини тахлиллайди. ҳимояланишни тахлиллаш воситаларини, уларнинг ишлаши бўйича хавфсизлик сканерлари деб ҳам юритишади. Тахлиллаш натижасида сканер маъмурга юборилувчи, таркибида аниқланган заифликлар ва уларни йўқотиш қоидалари бўлган ҳисоботни шакллантиради. Агар сканер таркибида хавфсизлик воситалари созланишини бошқарувчи воситалар бўлса, у мустақил тарзда уларни қайта конфигурациялаши мумкин.

Ташкилотнинг замонавий инфратузилмасини ҳисобга олган ҳолда айтиш мумкинки, бундай сканерларнинг мавжудлиги ахборот тизимлари хавфсизлиги мониторингининг муҳим элементи ҳисобланади. Таъкидлаш лозимки, бу воситалар ҳимояни хужум содир бўлишидан аввал амалга оширади.

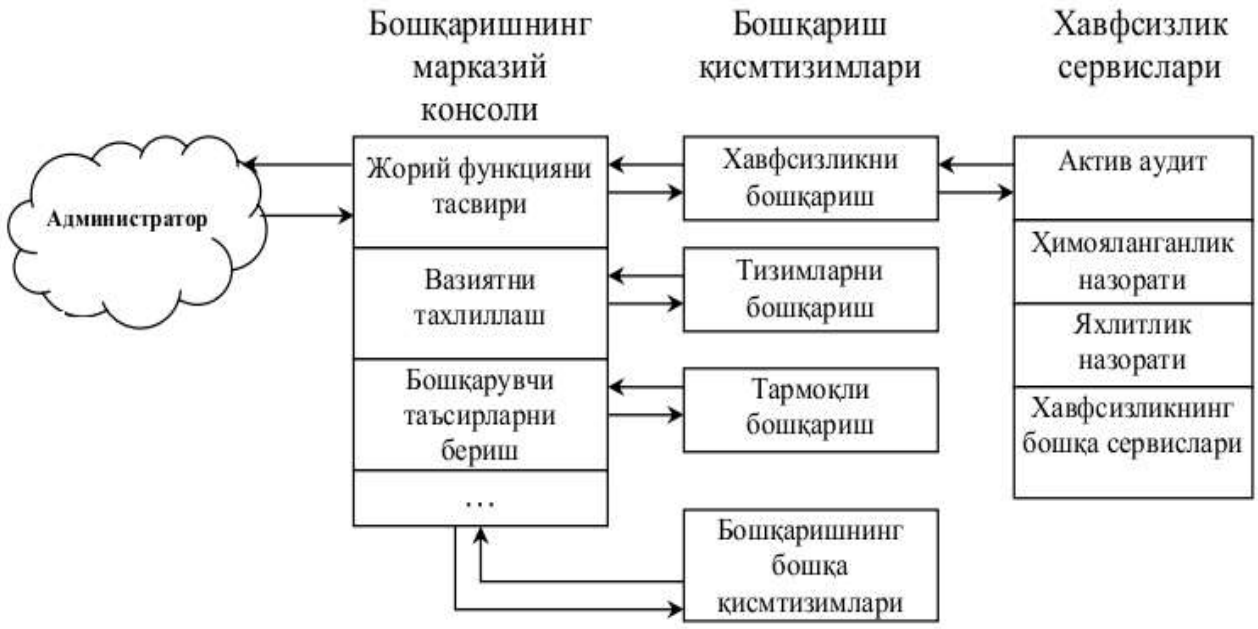
Ахборот тизими хавфсизлиги мониторингининг яна бир зарур элементи хужумларни аниқловчи воситалардир. Хужумларни аниқлаш корпоратив тармоқда кечувчи шубҳали ҳаракатларни баҳолаш жараёнидир. Хужумларни аниқлаш вақтнинг реал режимида тармоқ трафигини, ҳамда операцион тизим ва иловаларнинг руйхатга олиш журналларини тахлиллаш орқали амалга оширилади. Хужумларни аниқлаш тизимининг компонентлари агентлар деб аталади, ва ишчи станцияларда, серверларда жойлаштирилади ёки тармоқнинг қандайдир сегментини ёки бутун тармоқни қоплайди. Агентлар ўзларининг ишида сканерлар каби маълум заифликлар руйхатидан фойдаланиб, ходисаларни ушбу заифликлар билан таққослайди. Қандайдир узелда шубҳали фаолият аниқланганида хужумларни аниқлаш тизими ушбу фаолият фаоллиги хусусидаги огоҳлантиришни маъмурга жўнатади. У огоҳлантиришни узелнинг ўзига жўнатиши ёки узел ишини блокировка қилиш мумкин. Ушбу тизимнинг фарқли хусусияти - унинг бўлиб ўтган хужумларни аниқлаш учун ходисалар журналини тахлиллашидир.

Хавфсизлик воситаларини бошқариш шакли бўйича пассив ва фаол (актив) бўлиши мумкин. Пассив бошқаришда тармоқни бошқариш тизимига ёки маъмурга фақат хабар берилса, фаол бошқаришда хужумловчи узел ёки фойдаланувчи билан мустақил тарзда сессия тугалланади.

Бундан ташқари, бу тизимнинг вазифасига тармоқдаги, иловалардаги ёки ташкилот ахборот тизимининг бошқа компонентларидаги заифликларни йўқотиш бўйича маъмурга тавсиялар ишлаб чиқиш киради.

Фаол аудит тизими (мониторинги) ва умумий бошқариш ўртасида ўзаро алоқани ташкил этиш муҳим масҳалалардан ҳисобланади. Фаол аудит намунавий бошқариш функцияларини, яъни ахборот тизимдаги фаоллик хусусидаги маълумотларни тахлиллашни, жорий вазиятни акслантиришни, шубҳали фаолликка автоматик тарзда реакция кўрсатилишини бажаради. Тармоқни бошқариш тизими худди шунга ўхшаш ишлайди. Фаол аудит ва умумий бошқаришни умумий дастурий-техник ва ташкилий ечимлардан фойдаланиб интеграциялаш мақсадга мувофиқ ҳисобланади. Бу интеграцияланган тизимга яхлитликни назоратлаш, ҳамда ахборот тизими ҳатти-ҳаракатларининг ўзига хос жиҳатларини кузатувчи бошқа йўналишдаги агентлар ҳам киритилиши мумкин (8.2-расм).

Бошқаришнинг марказий консоли мавжуд бўлиб, унда фаол аудит (мониторинг) яхлитликни назоратлаш, бошқа жиҳатлар бўйича тизим ва тармоқларни назоратлаш тизимларидан маълумотлар тўпланади. Бу консолда жорий вазият акслантирилади, ундан автоматик тарзда ёки қўлда бошқариш командалари берилади. Техник ёки ташкилий сабабларга кўра бу консол бир неча ишчи жойи кўринишида физик амалга оширилиши мумкин (хавфсизлик маъмурига жой ажратиш билан)



8.2–расм. Хавфсизлик сервислари ва бошқариш тизимининг интеграцияси

Тармоқ хавфсизлигини адаптив бошқариш моделидан фойдаланиш барча таҳдидларни назоратлаш ва уларга ўз вақтида реакция кўрсатиш, нафақат таҳдидларни амалга оширишга шароит яратувчи заифликларни йўқотиш, балки заифликларни пайдо бўлиш шароитларини тахлиллаш имконини беради.

2. Хавф-хатарларни тахлиллаш ва бошқариш

Хавф-хатарларни тахлиллаш ва бошқариш ахборот тизимидаги таҳдидлар, заифликлар ва хавф-хатарларни баҳолаш, ҳамда ушбу ахборот тизими хавфсизлигининг етарли даражасини таъминловчи қарши чораларни аниқлаш учун ишлатилади.

Хавф-хатарларни тахлиллаш-таҳдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига бўлиши мумкин бўлган зарарларни аниқлаш жараёни. Хавф-хатарларни тахлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар меъёрини баҳолаш (уларга миқдорий баҳо бериш). Хавф-хатарларни тахлиллаш компьютер ахборот тизими хавфсизлигини текшириш бўйича тадбирни ўз ичига олади. Бу тадбирга биноан қайси ресурсларни қайси таҳдидлардан ҳимоялаш зарурлиги ҳамда у ёки бу ресурслҳар қандай даражада ҳимояга муҳтож эканлиги аниқланади.

Хавф-хатарларни тахлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимига қуйиладиган талаблар даражасига ва эътиборга олинувчи таҳдидлар характерига (таҳдидлар таъсири спектрига) боғлиқ. Талабларнинг иккита даражаси фарқланади:

- ахборот хавфсизлиги режимига минимал талаблар;
- ахборот хавфсизлиги режимига оширилган талаблар.

Ахборот хавфсизлиги режимига минимал талаблар ахборот хавфсизлигининг базавий даражасига мос келади. Бу даражадан, одатда, намунавий лойиҳа ечимларида фойдаланилади. Хавф-хатарларни тахлиллаш соддалаштирилган схема бўйича ўтказилади: хавфсизликка таҳдидларнинг кўп тарқалган тўплами уларнинг эҳтимоллигини баҳоламасдан кўрилади. Вируслар, асбоб-ускуналарнинг бузилиши, рухсатсиз фойдаланиш ва ҳ. Каби эҳтимоллиги юқори таҳдидларнинг минимал тўплами кўриладиган қатор стандартлар ва спецификациялар мавжуд. Бундай таҳдидларни бетарафлаш тириш учун уларнинг амалга оширилиши эҳтимоллиги ва, ресурсларнинг заифлигидан қатъий назар, қарши чоралар кўрилиши лозим, яъни базавий даражада таҳдидлар характеристикаларини кўриш шарт эмас.

Ахборот хавфсизлиги режимига оширилган талаблар, ахборот хавфсизлиги режимининг бузилиши оҳир оқибатларга сабаб бўлганида ва ахборот хавфсизлиги режимига минимал талаблар етарли бўлмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учун ресурслар аҳамиятини аниқлаш, тадқиқланувчи ахборот тизими учун долзғарб бўлган таҳдидлар руйхати билан стандарт тўпламни тўлдириш, таҳдидлар эҳтимоллигини баҳолаш ва ресурслар заифлигини аниқлаш зарур.

Хавф-хатарни тахлиллаш жараёнини қуйидаги босқичларга ажратиш мумкин:

- корпоратив ахборот тизимининг таянч ресурсларини идентификациялаш;
- у ёки бу ресурснинг муҳимлигини аниқлаш;

- таҳдидларнинг амалга оширилишига имкон берувчи мавжуд хавфсизлик таҳдидларни ва заифликларни идентификациялаш;

- хавфсизликка таҳдидларни амалга оширилиши билан боғлиқ хавф-хатарларни ҳисоблаш.

Ресурслар учта категорияга — ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприқлар, маршрутизаторлар ва ҳ.) бўлинади. Ҳар бир категория ичида ресурсларни синфларга ва қисм синфларга ажратиш мумкин. Фақат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуқтаи назаридан муҳим бўлган ресурлар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нархи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар миқдори билан белгиланади. Ресурслар нархини баҳолашда ресурсларининг ҳар бир категорияси учун бўлиши мумкин бўлган зарар миқдори белгиланади.

Намунавий хавфсизлик таҳдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий офат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи корпоратив ахборот тизим ишидаги бузилишлар тааллуқли. Таҳдид даражаси деганда унинг амалга оширилиши эҳтимоллиги тушунилади.

Ҳимоянинг бўшлиги корпоратив ахборот тизимидаги заифликларга сабаб бўлади. Заифликларни баҳолаш хавфсизлик таҳдидларининг муваффақиятли амалга оширилиш эҳтимоллигини аниқлашни назарда тутади. Шундай қилиб, зарар етказиш эҳтимоллиги таҳдидларнинг амалга оширилиши эҳтимоллиги ва заифлик миқдори орқали аниқланади.

Хавф-хатар даражаси ресурс нархи, таҳдид даражаси ва заифлик миқдори асосида аниқланади. Ресурс нархи, таҳдид даражаси ва заифлик миқдори ошиши билан хавф-хатар даражаси ҳам ошади. Хавф-хатарлар даражасини баҳолаш асосида хавфсизлик талаблари белгиланади.

Хавф-хатарларни бошқариш масаласи, хавф-хатар даражасини мақбул миқдоргача камайтиришга имкон берувчи қарши чораларни асосли танлашни ва амалга ошириш нархини баҳолашни ўз ичига олади. Табиийки, қарши чораларни амалга ошириш нархи бўлиши мумкин бўлган зарар миқдоридан кҳам бўлиши керак.

8.4-расмда хавф-хатарларни бошқариш технологиясининг босқичлари келтирилган.

Ахборот хавфсизлиги сиёсатини аниқлаш. Бу босқичда ахборот хавфсизлиги соҳасидаги қўлланма-хужжатлар, стандартлар, ахборот хавфсизлигининг асосий қоидалари, хавф-хатарларни бошқаришга ёндашишлар аниқланади ҳамда қарши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

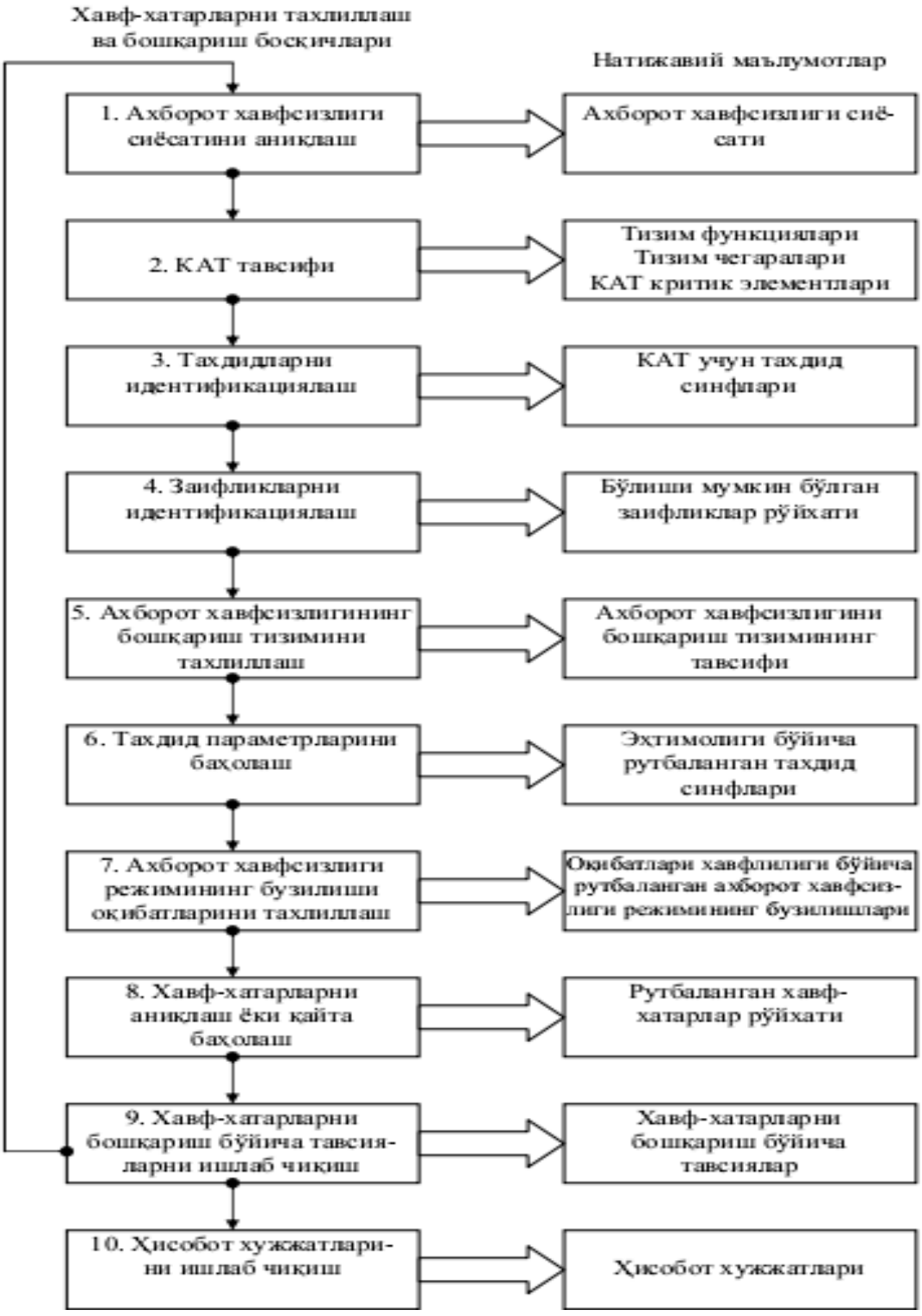
Корпоратив ахборот тизимини (КАТ) тавсифлаш. Ушбу босқичда ахборот хавфсизлиги соҳасидаги ҳалқаро, давлат ва корпоратив стандартларга биноан корпоратив ахборот тизимнинг функционал

вазифалари тавсифланади. Компаниянинг критик ахборот ресурслари, жараёнлари ва сервислари тавсифланади; корпоратив ахборот тизимининг чегаралари ҳамда бошқариш ва маълумотлар бўйича энг муҳим компонентларининг таркиби ва боғланишлари аниқланади.

Таҳдидларни идентификациялаш. Ушбу босқичда таҳдидлар руйхати тузилади ва уларнинг даражаси баҳоланади. Бунда турли ташкилотларнинг таҳдидлар синфлари рўйхатидан ҳам берилган таҳдидни амалга ошириш эҳтимоллигининг рейтинги ёки ўртача қийматидан фойдаланиш мумкин.

Заифликларни идентификациялаш. Ушбу босқичда берилган корпоратив ахборот тизимининг заифликлари рўйхати, уларнинг амалга оширилишидаги жоиз натижалар кўрсатилган ҳолда тузилади. Мавжуд корпоратив ахборот тизими учун рўйхатлар қатор манбалардан фойдаланилиб тузилади. Бу манбаларга заифликларни тармоқ сканерлари, турли ташкилотларнинг заифликлар каталоги, хавф-хатарларни тахлилловчи ихтисослаштирилган усуллар киради.

Корпоратив ахборот тизимининг бошқариш тизимини тахлиллаш. Ушбу босқичда бошқариш, тизими, аниқланган таҳдидларга ва заифликларга жоиз бўлган таъсир нуқтаи назаридан тахлилланади.



8.3–расм. Хавф-хатарларни бошқариш технологиясининг варианти

Таҳдидлар параметрларини баҳолаш. Ушбу босқичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти баҳоланади. Баҳолашнинг намунавий шкаласи — бир неча рутбали (масалан, паст, ўрта, ва юқори сатҳ) сифатий (балли) шкаладир. Бундай баҳо эксперт томонидан мавжуд объектив факторларни ҳисобга олган ҳолда берилади.

Ахборот хавфсизлиги режимининг бузилиши оқибатларини тахлиллаш. Ушбу босқичда ахборот хавфсизлиги режимининг бузилиши баҳоси

аниқланади. Бузилиш оқибатлари молиявий йўқотишларга, обрўсизланишга, расмий тузилмалар томонидан кўнгилсизликларга ва ҳ. сабаб бўлиши мумкин. Бузилиш оқибатларини баҳолаш учун мезонлар тизими танланади ва оқибатлар оғирлигини баҳолаш учун интеграцияланган шкала белгиланади.

Хавф-хатарларни баҳолаш. Ушбу босқичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси баҳоланади. Хавф-хатар даражаси қиймати таҳдидлар, заифликлар даражасига ва бўлиши мумкин бўлган оқибатлар о ирлигига боғлиқ. Хавф-хатарларни баҳолашда сифатий ва миқдорий усуллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг бўлиши мумкин бўлган хавф-хатарлар хавфлилиги даражаси бўйича рутбаланиши лозим. Миқдорий усул ишлатилганда хавф-хатарлар миқдорий шкҳалаларда баҳоланиши мумкин. Бу тавсия этилҳаётган қарши чораларнинг нарҳи/самарадорлигини тахлиллашни осонлаштиради. Аммо бу ҳолда дастлабки маълумотларни ўлчаш шкҳалаларига ва ишлатилҳаётган моделнинг адекватлигига жуда юқори талаблар қуйилади. Оддий ҳолда хавф-хатарни баҳолашда иккита омил-ходиса эхтимоллиги ва бўлиши мумкин бўлган оқибатлар оғирлиги ишлатилиши мумкин.

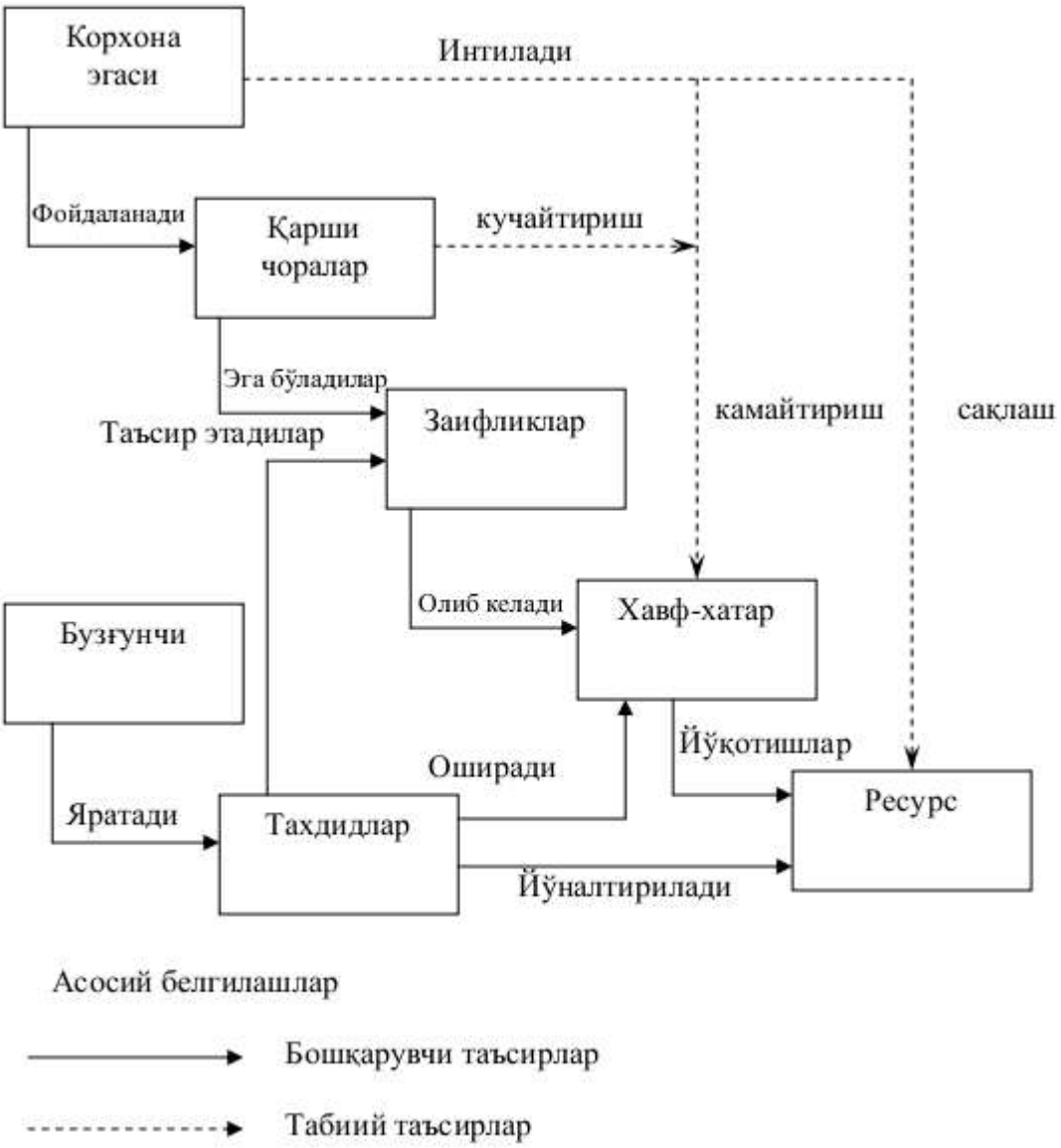
Хавф-хатарларни бошқариш бўйича тавсияларни ишлаб чиқиш. Ушбу босқичда турли сатҳлар (ташкилий, дастурий-техник) ва хавфсизликнинг алоҳида жиҳатлари бўйича структуризацияланган қарши чораларнинг комплекси тавсия этилиши лозим. Таклиф этилувчи қарши чоралар комплекси хавф-хатарларни бошқаришнинг танланган стратегиясига биноан қурилади.

Ҳисобот хужжатларни ишлаб чиқиш. Ушбу босқичда хавф-хатарларни тахлиллаш ва бошқаришнинг барча босқичлари бўйича иш натижалари акслантирилган ҳисобот хужжатлари тайёрланади.

Таъкидлаш лозимки, ҳозирда ахборот хавф-хатарларини баҳолашни автоматлаштириш мақсадида дастурий маҳсулотлар ишлаб чиқилган.

3. Ахборот хавфсизлиги тизимини қуриш методологияси

Ахборот хавфсизлиги моделини қуриш. Корхонадаги ахборот хавфсизлиги бўйича тадбирлар қонун чиқариш, ташкилий ва дастурий-техник характерга эга бўлган қатор жиҳатларни қамраб олади. Уларнинг ҳар бирида корхона ахборот хавфсизлигини таъминлаш учун бажарилиши зарур бўлган қатор масҳалалар таърифланади. Масҳалаларни ҳал этишда ахборот хавфсизлиги соҳасидаги халқаро стандартларга асосланган корхона ахборот хавфсизлигининг концептуал моделидан фойдаланиш мумкин.



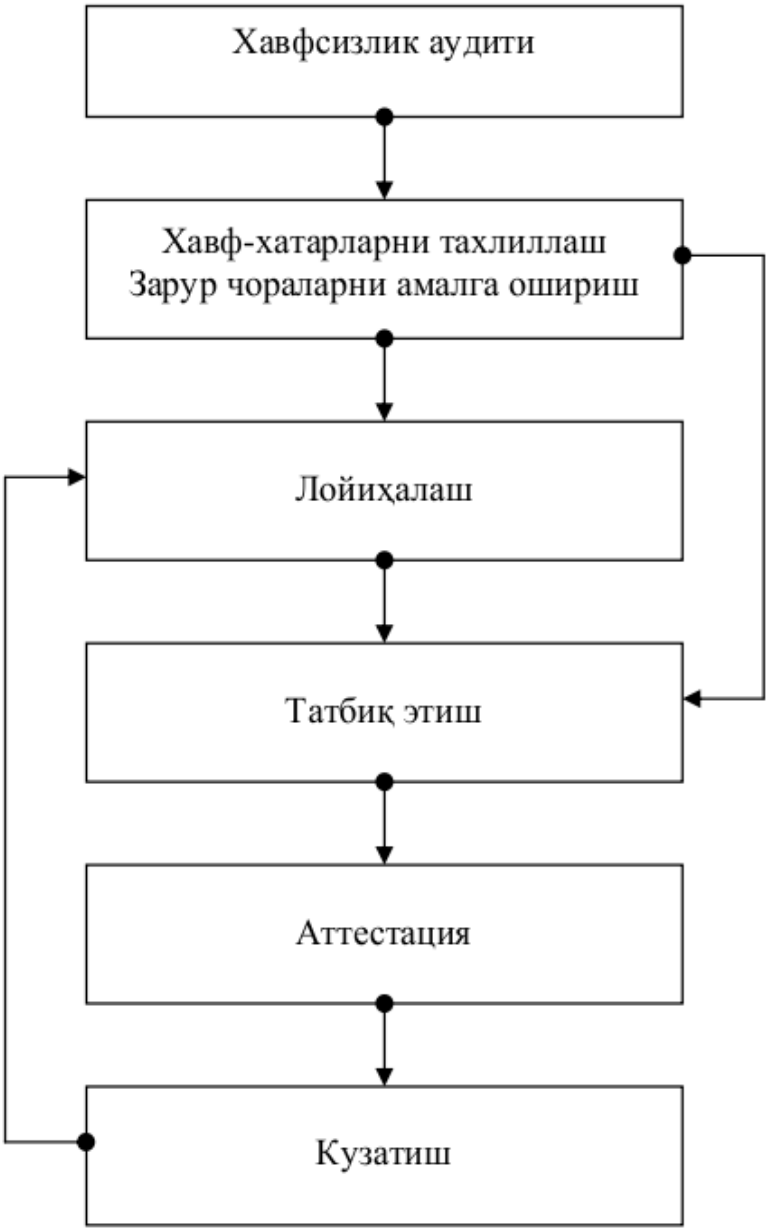
8.4–расм. Корхона ахборот хавфсизлиги тизимининг концептуаль модели

Қуйидаги халқаро стандартлар корпоратив ахборот тизими ҳимояланишини баҳолаш мезонини ва ҳимоялаш механизмларига қуйиладиган талабларни аниқловчи энг муҳим меъёрий хужжатлар ҳисобланади:

- ахборот технологиялари хавфсизлигини баҳолашнинг умумий мезонлари ISO/IEC 15408 (The Common Criteria For Information Technology Security Evalution);

- ахборот хавфсизлигини бошқаришнинг амалий қоидалари ISO/IEC 17799 (Code of practice for Information Security Management).

Ушбу халқаро стандартларга тўла мос равишда тузилган корхона ахборот хавфсизлигининг концептуал модели 8.4-расмда келтирилган.



8.5–расм. Ахборот хавфсизлиги тизимини қуриш босқичлари

Корхона ахборот хавфсизлигининг концептуал моделида қуйидаги омиллар ҳисобга олинган:

- пайдо бўлиш эҳтимоллиги ва амалга оширилиш эҳтимолиги билан характерланувчи ахборот хавфсизлиги таҳдидлари;

- таҳдидларнинг амалга оширилиши эҳтимоллигига таъсир этувчи ахборот тизими ёки қарши чора тизими (ахборот хавфсизлиги тизими) заифликлари;

- ахборот хавфсизлигига таҳдидлар амалга оширилиши натижасида корхонага етказилувчи зарарни акслантирувчи омил-хавф-хатар.

Бу моделнинг ҳаракатдаги субъектлари — Буз унчи (таҳдидлар манбаини ифодаловчи) ва Эга (корхона маъмури) объект-Ресурсга қарама-қарши мақсадларда таъсир қиладилар. Ресурс-корхонанинг моддий ва ахборот ресурсларини ва ахборот хавфсизлиги ҳолатини ифодалайди.

Ахборот хавфсизлиги тизимини қуриш босқичлари. Ахборот хавфсизлиги тизимини қуриш босқичларнинг қуйидаги стандартлаштирилган кетма-кетлигида амалга оширилади: хавфсизлик аудити; хавф-хатарларни тахлиллаш, тизимни лойиҳалаш, жорий этиш, аттестациялаш ва кузатиш (8.5-расм).

Хавфсизлик аудити. ҳозирда “хавфсизлик аудити” тушунчаси етарлича кенг талқин этилади. Аудитнинг қўйидаги кўринишлари фарқланади.

- ахборот хавфсизлигини тестли бузиш;
- экспресс текшириш;
- тизимни аттестациялаш;
- лойиҳагача текшириш.

Ахборот хавфсизлиги тестли бузиш корпоратив ахборот тизимининг ҳимояланиш даражасини аниқлаш нуқтаи назаридан самарали ҳисобланмайди. “Бузувчи”нинг асосий мақсади бир икки заифликларни топиб, уларни тизимдан фойдаланишда ишлатиш. Агар “тестли бузиш” муваффақиятли чиқса, ушбу муайян “бузиш”нинг мумкин бўлган сценарийси ривожини олдини олиб, заифликларни қидиришда давом этиш керак. “Тестли бузиш”нинг муваффақиятсизлигини баббаравар тестланувчи тизимнинг ҳимояланганлиги ва тестларнинг етишмаслиги каби талқин қилиш мумкин.

Эксперсс-текшириш доирасида, одатда, кўп вақт сҳарфини талаб этмайдиган, стандартизацияланган текширишлар асосида корпоратив ахборот тизими хавфсизлик воситаларининг умумий ҳолати баҳоланади. Экспресс-текшириш одатда ахборот ресурсларининг минимал ҳимояланиш даражасини таъминловчи устивор йўналишларни аниқлаш зарурияти туғилганда ўтказилади.

Тизимни аттестациялаш тизимнинг ахборот ресурсларининг ҳимояланиш талабларига мослигини текшириш мақсадида амалга оширилида. Бунда ҳам ташкилий, ҳам техник жиҳатдан талаблар тўплами расмий текширилади, хавфсизлик воситаларининг амалга оширилишининг тўлиқлиги ва етарлилиги кўрилади.

Лойиҳагача текшириш аудитнинг энг кўп меҳнат талаб қиладиган варианти ҳисобланади. Бундай аудит ахборот ресурслари иловаларида корхона ташкилий тузилмасини ва ходимларнинг у ёки бу иловалардан фойдаланиш қоидаларини тахлил этишни кўзда тутади. Сўнгра иловаларнинг ўзи тахлилланади. Ундан кейин бир сатҳдан иккинчи сатҳнинг фойдаланишдаги муайян хизматлар ҳамда ахборот алмашишга зарур бўлган хизматлар тахлилланиши лозим. Сўнгра хавфсизликнинг ўрнатилган воситаларини тахлиллаш билан тасаввур тўлдирилади.

Хавф-хатарларни тахлиллаш. Ахборот хавфсизлиги бузилганда лойиҳагача текшириш, хавф-хатарларни тахлиллаш билан биргаликда ахборот тизимидаги мавжуд хавф-хатарларни рутбалашга ва адэкват чораларни ишлаб чиқишга имкон беради.

Тизимни лойиҳалаш. ҳимояни ташкил этиш стратегияси нуқтаи назаридан ресурсли ва сервисли ёндашиш фарқланади. Ресурсли ёндашишда

тизим ресурслар тўплами сифатида кўрилади ва ахборот хавфсизлиги тизимининг компонентлари бу ресурсларга боғланади. Ресурсли ёндашиш амалга оширилганида ахборотни ҳимоялаш масаласи хизматлар тузилмасига қўшимча чеклашларсиз ечилади. Бу эса бир жинсли бўлмаган тизим шароитида мумкин эмас. Сервисли ёндашишда тизим фойдаланувчиларга тақдим этилувчи хизматлар тўплами каби талқин қилинади. Ҳозирги вақтда сервисли ёндашиш афзалроқ ҳисобланади, чунки у тизимда амалга оширилган хизматларга боғланади ва "ортиқча" хизматларни рад этиш ҳисобига қатор таҳдидларни истисно қилинишига имкон беради. Бу эса тизимни янада мантиқан асосланган тизимга айлантиради. Айнан сервис ёндашиш хавфсизликнинг замонавий стандартлари, хусусан ISO/IEC 15408 асосида ётади.

Ахборот хавфсизлиги тизимни қуришнинг иккита асосий сценарийси мавжуд: маҳсулотли ва лойиҳали. Маҳсулотли сценарий (ёндашиш) доирасида аввал ҳимоя воситалари тўплами танланади, уларнинг функциялари тахлилланади, сўнгра функциялар тахлили асосида ахборот ресурсларидан фойдаланиш сиёсати белгиланади.

Лойихага ххаражатлар нуқтаи назаридан махсулотли сценарий энг арзон ҳисобланади. Ундан ташқари, ечимларнинг танқислиги шароитида кўпинча маҳсулотли ёндашиш ягона ҳисобланади (масалан, криптографик ҳимояда фақат шу ёндашиш қўлланилади).

Лойиҳали сценарийда аввал хавфсизлик сиёсати ишлаб чиқилади, унинг асосида хавфсизлик сиёсатини амалга оширишда зарур бўлган функциялар аниқланади, сўнгра бу функциялар бажарилишини таъминловчи ҳимоя воситалари танланади.

Лойиҳали сценарий асосида қурилган тизимлар яхшироқ оптимизацияланган ва аттестациянинг юқори натижаларини беради. Ушбу ёндашиш маҳсулотли ёндашишдан фарқли равишда бошидан у ёки бу платформа билан боғланмаганлиги туфайли, катта гетероген тизимларни қуришда афзал ҳисобланади. Ундан ташқари, узоқ муддатга мўлжалланган ечимларни таъминлайди, чунки хавфсизлик сиёсатини ўзгартирмасдан ечимларни ва ҳимоя воситаларини алмаштиришга имкон беради.

Ахборот хавфсизлиги тизими архитектурасини танлаш нуқтаи назаридан объектли, татбиқий ёки аралаш ёндашишдан фойдаланилади. Объектли ёндашиш ахборот хавфсизлигини у ёки бу объект (бўлинма, филиал, ташкилот) тузилмаси асосида яратади. Объектли ёндашишнинг қўлланиши ташкилий чораларнинг бир жинсли тўпламини мададловчи хавфсизлик механизмлари учун универсал ечимлар тўпламидан фойдаланишни кўзда тутади. Бундай ёндашишга мисол тариқасида ташқи ахборот алмашиш, локал тармоқ, телекоммуникация тизимларининг ва ҳ. ҳимояланган инфратузилмаларини қуришни кўрсатиш мумкин. Объектли ёндашишнинг камчилиги унинг универсал механизмларининг, айниқса, ўзаро мураккаб боғланишли катта сонли иловаларга эга бўлган ташкилотлар учун тугал эмаслиги.

Татбиқий ёндашиш хавфсизлик механизмини муайян иловага боғлаб яратади. Татбиқий ёндашишга мисол тариқасида автоматлаштиришнинг алоҳида масаласи (бухгалтерия, кадрлар ва ҳ.) учун қисм тизимларнинг ҳимғоясини кўрсатиш мумкин. Ушбу ёндашишнинг камчилиги — маъмурлаш ва ишлатиш ҳҳаражатларини минималлаштириш мақсадида хавфсизликнинг турли воситаларини уй унлаштириш зарурияти.

Аралаш ёндашиш юқорида тавсифланган иккита ёндашишни комбинациялашни кўзда тутади. Бундай ёндашиш лойиҳалаш босқичида кўпроқ меҳнат талаб қилсада, ахборот хавфсизлиги тизимини жорий этиш ва ишлатиш нарҳи бўйича афзалликларни бериши мумкин.

Жорий этиш. Жорий этиш босқичи қуйидаги кетма-кет ўтказилувчи тадбирларни ўз ичига олади:

-ҳимоя воситаларини ўрнатиш ва конфигурациялаш;

- ходимларни ҳимоя воситалари билан ишлашга ўргатиш;

- дастлабки синовни ўтказиш;

- тажрибавий ишлатишга топшириш.

Тажрибавий ишлатиш, ахборот хавфсизлиги тизимини ишчи режимига туширишдан аввал, унинг ишлашидаги мумкин бўлган камчиликларни аниқлашга ва йўқотишга имкон беради. Агар тажрибавий ишлатиш жараёнида компонентларнинг тўғри ишламаслиги фактлари аниқланса, ҳимоя воситалари созланишига ва уларнинг ишлаш режимларига ва ҳ. тузатишлар киритилади.

Тизимни аттестациялаш. Ахборот хавфсизлиги тизимини вакҳолатли идора томонидан аттестациялаш унинг функционал тўлиқлигини ва корпоратив ахборот тизими ҳимғоясининг талаб қилинган даражаси таъминланганлигини тасдиқлашга имкон беради. Тизимнинг аттестацияси хавфсизлик аудитининг бир кўриниши ҳисобланади ва ишлатилувчи чоралар комплекси ва ҳимоя воситаларининг хавфсизлик даражаси талабларига мослигини баҳолаш мақсадида ҳимояланувчи корхонани ишлатишнинг реал шароитларида комплекс текширишни кўзда тутади.

Аттестация натижасида ҳисобот хужжати тайёрланади ва мослик аттестати берилади. Бу аттестат конфиденциал ахборот билан аттестатда кўрсатилган вақт мобайнида ишлаш хуқуқини беради.

Кузатиш. Ахборот хавфсизлиги тизимининг ишга лаёқатлигини ва ўз вазифаларини текис бажарилишини мададлаш учун хавфсизлик тизимининг дастурий ва аппарат таъминотини техник мададлаш ва кузатиш бўйича тадбирлар комплекси кўзда тутилиши лозим. Ахборот хавфсизлиги тизимини техник мададлаш ва кузатиш хизматчи ходимларнинг билими ва кўникмаларини талаб этади ва ҳимояланувчи тизим эгаси — ташкилот штатидаги ахборот хавфсизлигига жавоб берувчи ходимлар томонидан ёки ихтисослаштирилган ташкилот ходимлари томонидан амалга оширилиши мумкин.

Кўрилган методология қоидаларидан фойдаланиш корпоратив ахборот тизимининг умумий ривожи билан бирга ривожлантирилиши ва

модификацияланиши мумкин бўлган ахборот хавфсизлигининг самарали ва ишончли тизимини қуришга имкон беради.

Назорат саволлари

1. Ахборот хавфсизлиги аудитининг асосий босқичларини санаб беринг.
2. Ахборот тизимлари хавфсизлигининг мониторинги қандай амалга оширилади?
3. Хавф-хатарларни тахлиллаш жараёнининг ахборот хавфсизлигидаги асосий ўрни нимадан иборат?
4. Хавф-хатарларни бошқариш технологияси қандай босқичлардан ташкил топган?
5. Хавфсизлик аудитининг қандай кўринишлари бор?

Фойдаланилган адабиётлар рўйхати

1. Ғаниев С.К., Каримов М.М., Тошев К.А. «Ахборот хавфсизлиги. Ахборот – коммуникацион тизимлари хавфсизлиги», «Алоқачи» 2008 йил, 378 бет.
2. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
3. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув ўқлланма.- Тошкент давлат техника университети, 2003. 77 б.