ЎЗБЕКИСТОН РЕСПУБЛИКАСИ
ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

КИБЕРХАВФСИЗЛИК

“Телекоммуникация технологиялари” йўналиши

Тошкент -2022

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

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҲУЗУРИДАГИ ПЕДАГОГ КАДРЛАРНИ ҚАЙТА ТАЙЁРЛАШ ВА УЛАРНИНГ МАЛАКАСИНИ ОШИРИШ ТАРМОҚ МАРКАЗИ

“КИБЕРХАВФСИЗЛИК”

МОДУЛИ БЎЙИЧА

Ў Қ У В –У С Л У Б И Й М А Ж М У А

“Телекоммуникация технологиялари” таълим йўналишлари ва мўтахассисликлари профессор-ўқитувчилари учун

Тошкент – 2022

Модулнинг ўқув-услубий мажмуаси Олий ва ўрта махсус таълим вазирлигининг 2020 йил 7 декабрдаги 648-сонли буйруғи билан тасдиқланган ўқув дастури ва ўқув режасига мувофиқ ишлаб чиқилган.

Тузувчи: Муҳаммад ал-Хоразмий номидаги ТАТУ, “Ахборот хавфсизлиги” кафедраси доценти, PhD Ш.Ғуломов.

Тақризчилар: Беларусь-Ўзбекистон кўшма тармоқлараро амалий техник квалификациялар институти ижрочи директор в.в.б., DSc Я.Исмадияров,
Муҳаммад ал-Хоразмий номидаги ТАТУ, “Ахборот технологиялари” кафедраси мудири, проф. Х.Зайнидинов.

Ўқув -услубий мажмуа Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Кенгашининг қарори билан нашрга тавсия қилинган (2020 йил 29 октябрдаги 3(705)-сонли баённома)

МУНДАРИЖА

I БЎЛИМ

ИШЧИ ДАСТУР

I. ИШЧИ ДАСТУР

Кириш

Дастур Ўзбекистон Республикасининг 2020 йил 23 сентябрда тасдиқланган “Таълим тўғрисида”ги Қонуни, Ўзбекистон Республикаси Президентининг 2017 йил 7 февралдаги “Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида”ги ПФ-4947-сон, 2019 йил 27 августдаги “Олий таълим муассасалари раҳбар ва педагог кадрларининг узлуксиз малакасини ошириш тизимини жорий этиш тўғрисида”ги ПФ-5789-сон, 2019 йил 8 октябрдаги “Ўзбекистон Республикаси олий таълим тизимини 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-5847-сон ва 2020 йил 29 октябрдаги “Илм-фанни 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-6097-сонли Фармонлари ҳамда Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2019 йил 23 сентябрдаги “Олий таълим муассасалари раҳбар ва педагог кадрларининг малакасини ошириш тизимини янада такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги 797-сонли Қарорида белгиланган устувор вазифалар мазмунидан келиб чиққан ҳолда тузилган бўлиб, у олий таълим муассасалари педагог кадрларининг касб маҳорати ҳамда инновацион компетентлигини ривожлантириш, соҳага оид илғор хорижий тажрибалар, янги билим ва малакаларни ўзлаштириш, шунингдек амалиётга жорий этиш кўникмаларини такомиллаштиришни мақсад қилади.

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

Модулнинг мақсади ва вазифалари

“Киберхавфсизлик” модулининг мақсади: киберхавфсизлик бўйича олий таълим муассасалари педагог кадрларининг касбий компетентлигини ошириш.

Модулнинг вазифалари: олий таълим муассасалари педагог кадрларида киберхавфсизлик ҳақида назарий ва амалий билимларни, кўникма ва малакаларни шакллантиришдан иборат.

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

“Киберхавфсизлик” модулининг модулини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида**:**

Тингловчи:

- киберхавфсизлик вазифалари, сиёсати, ҳужум инцидентлари ва уларга қарши реакциялари, тармоқ хавфсизлиги заифликалари ва уларга бўлган таҳдидлар, компьютер вируслари, зараркунанда дастурлар ва улардан ҳимояланиш

механизмларини, киберэтика, кибержиноятчилик, киберҳуқуқ ва киберэтика тушунчаларини ***билиши*** керак.

- компьютер вирусларига зараркунанда дастурлар билан ишлаш, рискларни баҳолаш, идентификация, аутентификация ва авторизация жараёнларидан ўтиш, ахборотларни тиклаш ва барқарорлигини таъминлаш, зараркунанда дастурий таъминотлардан фойдаланиш ***кўникмаларига*** эга бўлиши лозим.
- киберхавфсизлик сиёсатини яратиш, ҳавф-хатарларни бошқариш, тармоқ хавфсизлигини таъминлаш, кибержиноятчилик, киберҳуқуқ ва киберэтика нормаларидан фойдаланиш ***малакаларига*** эга бўлиши лозим.
- киберхавфсизлик сиёсатини яратиш ва ҳавф-хатарларни бошқариш, кибержиноятчилик, киберҳуқуқ ва киберэтика нормаларига кўра ўз касбий фаолиятини бошқариш ***компетенцияларига*** эга бўлиши лозим.

Модулни ташкил этиш ва ўтказиш бўйича тавсиялар

“Киберхавфсизлик” модули маъруза ва амалий машғулотлар шаклида олиб борилади.

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

- маъруза дарсларида замонавий компьютер технологиялари ёрдамида презентацион ва электрон-дидактик технологиялардан;
- ўтказиладиган амалий машғулотларда техник воситалардан, экспресс-сўровлар, тест сўровлари, ақлий ҳужум, гуруҳли фикрлаш, кичик гуруҳлар билан ишлаш, коллоквиум ўтказиш, ва бошқа интерактив таълим усулларини қўллаш назарда тутилади.

Модулнинг ўқув режадаги бошқа модуллар билан боғлиқлиги ва узвийлиги

“Кибергхавфсизлик” модули мазмуни ўқув режадаги “Булутли ҳисоблаш технологиялари“**,** “Телекоммуникация тизимларнинг янги авлодлари (NGN, IMS,SDH, DWDM)” ва “3G ва 4G технологиялари” ўқув модуллари билан узвий боғланган ҳолда педагогларнинг таълим жараёнида булутли ҳисоблаш, катта маълумотлар ва виртуал реаллик тизимларидан фойдаланиш бўйича касбий педагогик тайёргарлик даражасини оширишга хизмат қилади.

Модулнинг олий таълимдаги ўрни

Модулни ўзлаштириш орқали тингловчилар электрон ҳукуматни жорий этишни ўрганиш, амалда қўллаш ва баҳолашга доир касбий компетентликка эга бўладилар.

Модул бўйича соатлар тақсимоти

№	Модуль мавзулари	Аудитория укув юкламаси			
		Жами	жумладан		
			Назарий	Амаий машғулот	Кўчма машғулот
1.	Киберхавфсизлик функциялари ва вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш. Хавф-хатарларни бошқариш. Ҳужум инцидентлари ва уларга қарши реакция.	4	4		
2.	Криптографиянинг асосий тушунчалари. Тармоқ хавфсизлиги заифликалари ва уларга бўлган таҳдидлар.	2	2		
3	Компьютер вируслари, зараркунанда дастурлар ва улардан ҳимояланиш механизмлари.	2	2		
4	Рисклар ва рискларни баҳолаш усуллари.	2		2	
5	Идентификация, аутентификация ва авторизация	2		2	
6	Маълумотлар ва ахборотни тикланиши ва барқарорлиги.	2		2	
7	Тармоқ ҳужумлари, web-ҳужумлар, дастурий ҳужумлар.	2		2	
8	Зараркунанда дастурий таъминотлар.	2		2	
9	Кибержиноятчилик, киберҳуқуқ ва киберэтика.	4		4	
	Жами:	**22**	**8**	**14**	**0**

НАЗАРИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-маъруза. Киберхавфсизлик функциялари ва вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш. Хавф-хатарларни бошқариш. Ҳужум инцидентлари ва уларга қарши реакция (4 соат)

Киберхавфсизликнинг фундаментал тушунчалари. Киберхавфсизлик сиёсати ва уни бошқариш. Хавф-хатарларни бошқариш. Ҳужум инцидентлари ва уларга қарши реакция.

2-маъруза. Криптографиянинг асосий тушунчалари. Тармоқ хавфсизлиги заифликалари ва уларга бўлган таҳдидлар (2 соат).

Криптографиянинг асосий тушунчалари. Тармоқ хавфсизлиги заифликлари ва уларга бўлган таҳдидлар.

3-маъруза. Компьютер вируслари, зараркунанда дастурлар ва улардан ҳимояланиш механизмлари (2 соат).

Компьютер вируси тушунчаси. Компьютер вируслари ва уларнинг классификациялари. Вируслар билан курашиш усуллари ва воситалари.

АМАЛИЙ МАШҒУЛОТЛАР МАЗМУНИ

1-амалий машғулот. Рисклар ва рискларни баҳолаш усуллари (2 соат).

2-амалий машғулот. Идентификация, аутентификация ва авторизация (2 соат).

3-амалий машғулот. Маълумотлар ва ахборотни тикланиши ва барқарорлиги (2 соат).

4-амалий машғулот. Тармоқ ҳужумлари, web-ҳужумлар, дастурий ҳужумлар (2 соат).

5-амалий машғулот. Зараркунанда дастурий таъминотлар (2 соат).

6-амалий машғулот. Кибержиноятчилик, киберҳуқуқ ва киберэтика (4 соат).

ЎҚИТИШ ШАКЛЛАРИ

Мазкур модул бўйича қуйидаги ўқитиш шаклларидан фойдаланилади:

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

II БЎЛИМ

МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

II. МОДУЛНИ ЎҚИТИШДА ФОЙДАЛАНИЛАДИГАН ИНТЕРФАОЛ ТАЪЛИМ МЕТОДЛАРИ

«Блум кубиги» методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билимларни ўзлаштирилишини енгиллаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун “Очиқ” саволлар тузиш ва уларга жавоб топиш машқи вазифасини белгилайди.

Методни амалга ошириш тартиби:

1. Ушбу методни қўллаш учун, оддий куб керак бўлади. Кубнинг ҳар бир томонида қўйидаги сўзлар ёзилади:
   - **Санаб беринг, таъриф беринг (оддий савол)**
   - **Нима учун (сабаб-оқибатни аниқлаштирувчи савол)**
   - **Тушинтириб беринг (муаммони ҳар томонлама қараш саволи)**
   - **Таклиф беринг (амалиёт билан боғлиқ савол)**
   - **Мисол келтиринг (ижодкорликни ривожлантировчи савол)**
   - **Фикр беринг (таҳлил қилиш ва бахолаш саволи)**

2. Ўқитувчи мавзуни белгилаб беради.

3. Ўқитувчи кубикни столга ташлайди. Қайси сўз чиқса, унга тегишли саволни беради.

“KWHL” методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билимларни тизимлаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун мавзу бўйича қуйидаги жадвалда берилган саволларга жавоб топиш машқи вазифасини белгилайди.

Изоҳ. *KWHL:*
Know – нималарни биламан?
Want – нимани билишни хоҳлайман?
How - қандай билиб олсам бўлади?
Learn - нимани ўрганиб олдим?.

“KWHL” методи	
1. Нималарни биламан: -	***2. Нималарни билишни хоҳлайман, нималарни билишим керак:*** -
3. Қандай қилиб билиб ва топиб оламан: -	***4. Нималарни билиб олдим:*** -

“W1H” методи

Методнинг мақсади: Мазкур метод тингловчиларда янги ахборотлар тизимини қабул қилиш ва билимларни тизимлаштириш мақсадида қўлланилади, шунингдек, бу метод тингловчилар учун мавзу бўйича қўйидаги жадвалда берилган олтита саволларга жавоб топиш машқи вазифасини белгилайди.

What?	Нима? (таърифи, мазмуни, нима учун ишлатилади)	
Where?	Қаерда (жойлашган, қаердан олиш мукин)?	
What kind?	Қандай? (параметрлари, турлари мавжуд)	
When?	Қачон? (ишлатилади)	
Why?	Нима учун? (ишлатилади)	
How?	Қандай қилиб? (яратилади, сақланади, тўлдирилади, таҳрирлаш мумкин)	

“SWOT-таҳлил” методи.

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

“BEEP” методи

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

Методни амалга ошириш тартиби:

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

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

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

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

Муаммоли савол					
1-усул		**2-усул**		**3-усул**	
афзаллиги	камчилиги	афзаллиги	камчилиги	афзаллиги	камчилиги
Хулоса:					

“Кейс-стади” методи

«Кейс-стади» - инглизча сўз бўлиб, («case» – аниқ вазият, ҳодиса, «stady» – ўрганмоқ, таҳлил қилмоқ) аниқ вазиятларни ўрганиш, таҳлил қилиш асосида ўқитишни амалга оширишга қаратилган метод ҳисобланади. Мазкур метод дастлаб 1921 йил Гарвард университетида амалий вазиятлардан иқтисодий бошқарув фанларини ўрганишда фойдаланиш тартибида қўлланилган. Кейсда очиқ ахборотлардан ёки аниқ воқеа-ҳодисадан вазият сифатида таҳлил учун фойдаланиш мумкин.

“Кейс методи” ни амалга ошириш босқичлари

Иш босқичлари	Фаолият шакли ва мазмуни
1-босқич: Кейс ва унинг ахборот таъминоти билан таништириш	✓ якка тартибдаги аудио-визуал иш; ✓ кейс билан танишиш(матнли, аудио ёки медиа шаклда); ✓ ахборотни умумлаштириш; ✓ ахборот таҳлили; ✓ муаммоларни аниқлаш
2-босқич: Кейсни аниқлаштириш ва ўқув топшириғни белгилаш	✓ индивидуал ва гуруҳда ишлаш; ✓ муаммоларни долзарблик иерархиясини аниқлаш; ✓ асосий муаммоли вазиятни белгилаш
3-босқич: Кейсдаги асосий муаммони таҳлил этиш орқали ўқув топшириғининг ечимини излаш, ҳал этиш йўлларини ишлаб чиқиш	✓ индивидуал ва гуруҳда ишлаш; ✓ муқобил ечим йўлларини ишлаб чиқиш; ✓ ҳар бир ечимнинг имкониятлари ва тўсиқларни таҳлил қилиш; ✓ муқобил ечимларни танлаш
4-босқич: Кейс ечимини ечимини шакллантириш ва асослаш, тақдимот.	✓ якка ва гуруҳда ишлаш; ✓ муқобил вариантларни амалда қўллаш имкониятларини асослаш; ✓ ижодий-лойиҳа тақдимотини тайёрлаш; ✓ якуний хулоса ва вазият ечимининг амалий аспектларини ёритиш

“Ассесмент” методи

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

Методни амалга ошириш тартиби:

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

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

Тест

Муаммоли вазият

Тушунча таҳлили (симптом)

Амалий вазифа

“Инсерт” методи

Методни амалга ошириш тартиби:

➢ ўқитувчи машғулотга қадар мавзунинг асосий тушунчалари мазмуни ёритилган матнни тарқатма ёки тақдимот кўринишида тайёрлайди;

➢ янги мавзу моҳиятини ёритувчи матн таълим олувчиларга тарқатилади ёки тақдимот кўринишида намойиш этилади;

➢ таълим олувчилар индивидуал тарзда матн билан танишиб чиқиб, ўз шахсий қарашларини махсус белгилар орқали ифодалайдилар. Матн билан ишлашда талабалар ёки қатнашчиларга қуйидаги махсус белгилардан фойдаланиш тавсия этилади:

Белгилар	Матн
“V” – таниш маълумот.	
“?” – мазкур маълумотни тушунмадим, изоҳ керак.	
“+” бу маълумот мен учун янгилик.	
“– ” бу фикр ёки мазкур маълумотга қаршиман?	

Белгиланган вақт якунлангач, таълим олувчилар учун нотаниш ва тушунарсиз бўлган маълумотлар ўқитувчи томонидан таҳлил қилиниб, изоҳланади, уларнинг моҳияти тўлиқ ёритилади. Саволларга жавоб берилади ва машғулот якунланади.

III БЎЛИМ

НАЗАРИЙ МАТЕРИАЛЛАР

III. НАЗАРИЙ МАТЕРИАЛЛАР

1-маъруза. Киберхавфсизлик функциялари ва вазифалари. Киберхавфсизлик сиёсати ва уни бошқариш. Хавф-хатарларни бошқариш. Ҳужум инцидентлари ва уларга қарши реакция (4 соат)

Режа:

1.1. Киберхавфсизликнинг фундаментал тушунчалари.
1.2. Киберхавфсизлик сиёсати ва уни бошқариш.
1.3. Хавф-хатарларни бошқариш.
1.4. Ҳужум инцидентлари ва уларга қарши реакция.

Таянч иборалар: *Киберхавфсизлик, Конфиденциаллик, Яхлитлик, Фойдаланувчанлик, Маълумотлар хавфсизлиги, Дастурий таъминотлар хавфсизлиги, Ташкил этувчилар хавфсизлиги, Алоқа хавфсизлиги, Тизим хавфсизлиги, Инсон хавфсизлиги, киберхавфсизлик рисклари, Рискларни идентификация қилиш, Ҳодиса, Инцидент , Ҳужум, ИТРМ модели.*

“Агар сиз сирингизни шамолга айтсангиз, уни дарахтларга айтгани учун шамолни айбламанг”.
Каҳлил Гибран

1.1. Киберхавфсизликнинг фундаментал тушунчалари.

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

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.

Киберхавфсизлик ҳозирда кириб келган янги тушунчалардан бири бўлиб, унга турли берилган турли таърифлар мавжуд.

- Хусусан, **CSEC2017 Joint Task Force (CSEC2017 JTF)** киберхавфсизликка қуйидагича таъриф берган: ***киберхавфсизлик*** *– ҳисоблашга асосланган билим соҳаси бўлиб, бузғунчилар мавжуд бўлган шароитда амалларни кафолатлаш учун ўзида технология, инсон, ахборот ва жараённи мужассамлаштирган.*
- У *хавфсиз компьютер тизимларини яратиш, амалга ошириш, таҳлил қилиш ва тестлашни* **ўз ичига олади**.
- Киберхавфсизлик таълимнинг **мужассамлашган** билим соҳаси бўлиб, *қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқаришни* **ўз ичига олади**.
- Тармоқ бўйича фаолият юритаётган ***Cisco*** ташкилоти эса киберхавфсизликка қуйидагича таъриф берган: ***Киберхавфсизлик*** *– тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти.*
- Ушбу киберҳужумлар одатда *махфий ахборотни бошқариш, алмаштириш*

ёки йўқ қилишни; фойдаланувчилардан пул ундиришни; ёки нормал иш фаолиятини узуб қўйишни **мақсад қилади**.

• Ҳозирги кунда самарали киберхавфсизлик чораларини амалга ошириш *инсонларга қараганда қурилмалар сонининг кўплиги* ва *бузғунчилар салоҳиятини ортиши натижасида* **амалий томондан мураккаблашиб** бормоқда.

1.1-расм. Киберхавфсизлик кимларга керак.

Киберхавфсизликни **фундаментал терминларини** қараб чиқамиз:

• ***Конфиденциаллик***

– Тизим маълумоти ва ахборотига фақат **ваколатга эга субъектлар** фойдаланиши мумкинлигини таъминловчи қоидалар.

– Мазкур қоидалар ахборотни фақат қонуний фойдаланувчилар томонидан **“ўқилишини”** таъминлайди.

• ***Яхлитлик (бутунлик)***

– Маълумотни аниқ ва ишончли эканлигига ишонч ҳосил қилиш.

– Яъни, ахборотни рухсат этилмаган ўзгартиришдан ёки **“ёзиш”** дан ҳимоялаш.

• ***Фойдаланувчанлик***

– Маълумот, ахборот ва тизимдан фойдаланишнинг мумкинлиги.

– Яъни, рухсат этилмаган **“бажариш”** дан ҳимоялаш.

1.2-расм. Киберхавфсизликнинг билим соҳалари.

• **“Маълумотлар хавфсизлиги”** билим соҳаси **маълумотларни сақлашда, қайта ишлашда** ва **узатишда** ҳимояни таъминлашни мақсад қилади.

– Мазкур билим соҳаси ҳимояни тўлиқ амалга ошириш учун **математик** ва **аналитик алгоритмлардан** фойдаланишни талаб этади.

• “**Дастурий таъминотлар хавфсизлиги**” билим соҳаси фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи **дастурий таъминотларни ишлаб чиқиш** ва **фойдаланиш жараёнига** эътибор қаратади.

• “**Ташкил этувчилар хавфсизлиги**” билим соҳаси катта тизимларда интегралашган ташкил этувчиларни **лойиҳалаш, сотиб олиш, тестлаш, анализ қилиш** ва **техник хизмат кўрсатишга** эътибор қаратади.

– Тизим хавфсизлиги ташкил этувчилар хавфсизлигидан фарқ қилади.

– Ташкил этувчилар хавфсизлиги улар *қандай лойиҳаланганлиги, яратилганлиги, сотиб олинганлиги, бошқа таркибий қисмларга уланганлиги, қандай ишлатилганлиги* ва *сақланганлигига* боғлиқ.

• “**Алоқа хавфсизлиги**” билим соҳаси ташкил этувчилар ўртасидаги **алоқани ҳимоялашга** этибор қаратиб, ўзида *физик* ва *мантиқий* уланишни бирлаштиради.

• “**Тизим хавфсизлиги**” билим соҳаси **ташкил этувчилар, уланишлар** ва **дастурий таъминотдан** иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади.

– Тизим хавфсизлигини тушуниш учун нафақат, *унинг таркибий қисмлари* ва *уланишини тушунишни*, балки *бутунликни* ҳисобга олишни талаб қилади.

• “**Инсон хавфсизлиги**” билим соҳаси *киберхавфсизлик билан боғлиқ инсон ҳатти ҳаракатларини ўрганишдан* ташқари, *ташкилотлар (масалан, ходим)* ва *шахсий ҳаёт шароитида шахсий маълумотларни* ва *шахсий ҳаётни ҳимоя қилишга* эътибор қаратади.

• “**Ташкилот хавфсизлиги**” билим соҳаси ташкилотни *киберхавфсизлик таҳдидларидан ҳимоялаш* ва *ташкилот вазифасини муваффақиятли бажаришини* мададлаш учун рискларни бошқаришга эътибор қаратади.

• “**Жамоат хавфсизлиги**” билим соҳаси у ёки бу даражада жамиятда таъсир

кўрсатувчи киберхавфсизлик омилларига эътибор қаратади.

– *Кибержиноятчилик, қонунлар, ахлоқий муносабатлар, сиёсат, шахсий ҳаёт* ва *уларнинг бир-бири билан муносабатлари* ушбу билим соҳасидаги асосий тушунчалар.

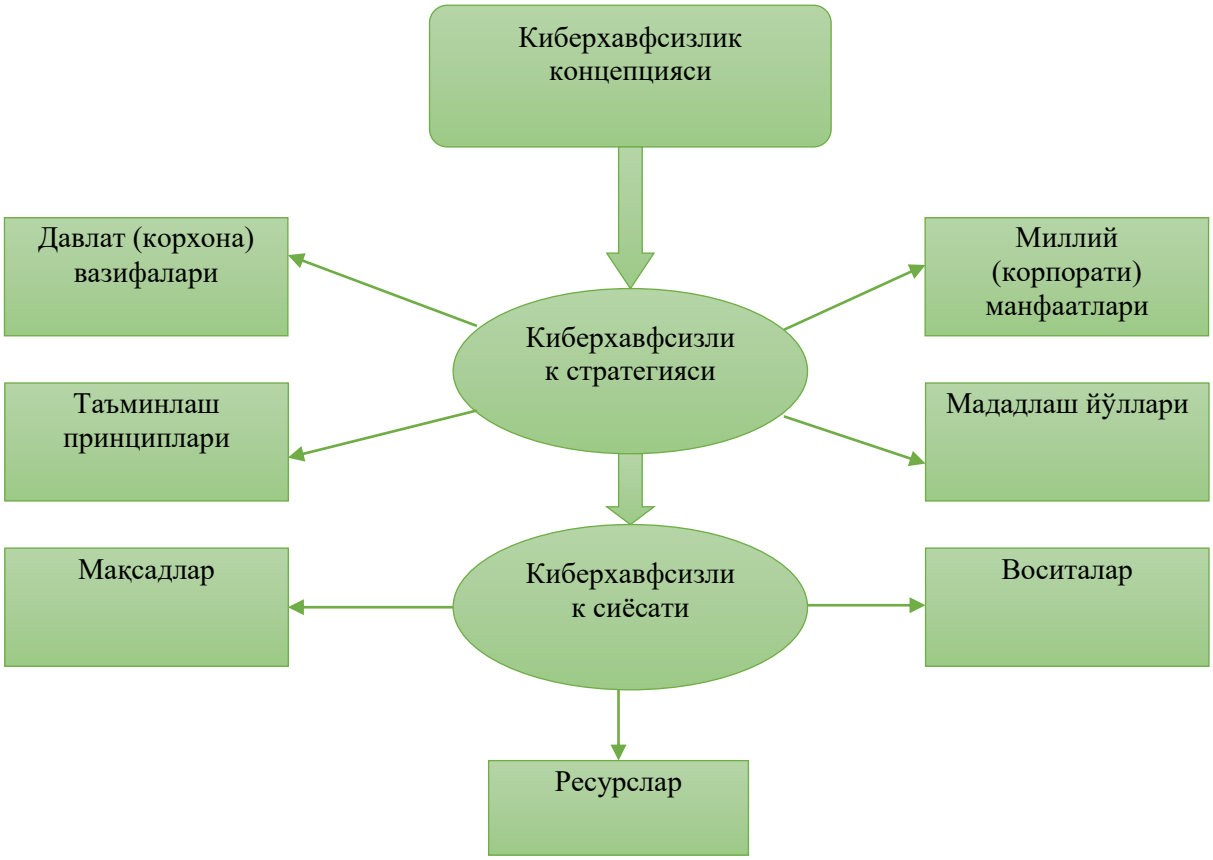
1.3-расм. Хавфсизлик муаммолари.

1.2. Киберхавфсизлик сиёсати ва уни бошқариш.

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

Концепцияни ишлаб чиқишни уч босқичда амалга ошириш тавсия этилади.

1.4-расм. Ахборот химояси концепциясини ишлаб чиқиш босқичлари



1.5-расм. Киберхавфсизлик концепцияси схемаси.

Киберхавфсизлик сиёсати бу – ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режа ҳисобланади.

У хавфсизликни таъминлашнинг барча дастурларини режалаштиради.

Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт.

Ташкилотнинг амалий хавфсизлик сиёсати қўйидаги бўлимларни ўз ичига олиши мумкин:

- ❑ умумий низом;
- ❑ паролларни бошқариш сиёсати;
- ❑ фойдаланувчиларни идентификациялаш;
- ❑ фойдаланувчиларнинг ваколатлари;
- ❑ ташкилот ахборот коммуникацион тизимини компьютер вируслардан ҳимоялаш;
- ❑ тармоқ уланишларини ўрнатиш ва назоратлаш қоидалари;
- ❑ электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати қоидалари;
- ❑ ахборот коммуникацион тизимлар хавфсизлигини таъминлаш қоидалари;
- ❑ фойдаланувчиларнинг хавфсизлик сиёсатини қоидаларини бажариш бўйича мажбуриятлари ва ҳ.к.лар

1.3. Хавф-хатарларни бошқариш.

Киберхавфсизлик рискларини аниқлашнинг умумий тавсифини қраб чиқамиз. Риск номақбул воқеа - ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради.

Рискни аниқлаш қуйидаги тадбирлардан иборат:

- рискларни аниқлаш;
- рискларни идентификация қилиш;
- рискларни таҳлил қилиш;
- рискларни баҳолаш.

Рискларни аниқлаш ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди. Рискни аниқлаш кўпинча икки (ёки ундан кўп) итерациядан фойдаланиб ўтказилади.

Рискларни аниқлашнинг мақсад ва вазифалари асосида рискларни аниқлашга ўз ёндашувини танлаш ташкилотнинг ўзига боғлиқ.

Активларнинг баҳоси, оқибатларнинг ҳар бир турига тааллуқли бўлган заифликлар ва таҳдидларнинг даражалари, ҳар бир комбинация учун 0 дан 8 гача бўлган шкала асосида рискнинг тегишли ўлчовини идентификациялаш мақсадида, жадвал шаклига (матрицага) келтирилади (1.1 (а)-жадвал). Қийматлар матрицага структураланган тарзда киритилади.

1.1(а)-жадвал.

Рисклар ўлчовларини идентификациялаш матрицаси

	Таҳдиднинг юзага келиш эҳтимоллиги	Паст (П)			Ўрта (Ў)			Юқори (Ю)		
	Фойдаланишнинг соддалиги	П	Ў	Ю	П	Ў	Ю	П	Ў	Ю
Актив баҳоси	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Ҳар бир актив учун ўринли заифликлар ва уларга мос келадиган таҳдидлар кўриб чиқилади. Агар тегишлича таҳдидсиз заифлик ёки тегишлича заифликсиз таҳдид мавжуд бўлса, ҳозирги пайтда риск йўқ (лекин, бу вазият ўзгарганда эҳтиёткорлик кўрсатиш керак). Жадвалдаги тегишли сатр актив баҳосининг

қиймати бўйича, тегишли устун эса, таҳдиднинг юзага келиш эҳтимоллиги ва фойдаланишнинг соддалиги бўйича белгиланада. Масалан, агар актив 3 баҳога эга бўлса, таҳдид «юқори», заифлик эса, «паст» бўлади, у ҳолда риск ўлчови 5 га тенг бўлади. Актив 2 баҳога эга деб, ва масалан, ўзгартириш учун таҳдид даражаси «паст», фойдаланишнинг соддалиги эса «юқори» бўлади деб тахмин қиламиз, у ҳолда риск ўлчови 4 га тенг бўлади. Жадвалнинг ўлчами, таҳдидлар эҳтимоллиги тоифаларининг, фойдаланишнинг соддалиги тоифаларининг сони ҳамда активлар баҳосини аниқлаш тоифаларининг сони нуқтаи назаридан, ташкилотнинг эҳтиёжларига мослаштирилиши мумкин.

Рискларнинг берилган шкаласи қуйидагича оддий умумий рейтинги учун ҳам акс эттирилиши мумкин:

- паст риск: 0-2;
- ўрта риск: 3-5;
- юқори риск: 6-8.

1.1(b)- жадвал.

Рисклар умумий рейтингининг матрицаси

	Инцидент сценарийси эҳтимоллиги	Жуда паст (эҳтимоллиги жуда кам)	Паст (эҳтимоллиги кам	Ўртача (мумкин бўлган)	Юқори (эҳтимоллиги бўлган)	Жуда юқори (тез-тез учраб турадиган)
Актив баҳоси	Жуда паст	0	1	2	3	4
	Паст	1	2	3	4	5
	Ўртача	2	3	4	5	6
	Юқори	3	4	5	6	7
	Жуда юқори	4	5	6	7	8

Рискларни идентификация қилишдан мақсад, потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади. Қуйида тавсифланган қадамлар рискларни таҳлил қилиш бўйича табдирлар учун кириш маълумотларини аниқлайди.

Рискларни идентификация қилишдан мақсад, потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади. Қуйида тавсифланган қадамлар рискларни таҳлил қилиш бўйича табдирлар учун кириш маълумотларини аниқлайди.

Активларни аниқлашда ахборот тизими фақат аппарат ва дастурий воситалардан иборат эмаслигини назарда тўтиш керак. Активларни аниқлаш рискларни баҳолаш учун етарли ахборот таъминланадиган тегишли деталлаштириш даражасида амалга оширилиши зарур. Активларни аниқлашда фойдаланиладиган деталлаштириш даражаси рискларни баҳолаш вақтида тўпланган ахборотнинг умумий ҳажмига таъсир этади. Бу даража рискларни баҳолашнинг кейинги итерацияларида янада деталлаштирилиши мумкин.

1.4. Ҳужум инцидентлари ва уларга қарши реакция.

Киберхавфсизлик соҳасидаги фактлар:

1. Кучли пароль кўп ҳужумларни бартараф этиши мумкин.
2. Янги восита (дастурий-аппарат) хавфсиз ҳисобланмайди.
3. Энг яхши дастурий воситалар заифликларни ўз ичига олади.
4. Булутли технология тўлиқ хавфсиз эмас.
5. Хакералар-булар ҳама вақт ҳам жиноятчи эмас.

Компьютер ва компьютер тармоқларида **компьютер хавфсизлиги инцидентларини бошқариш** ўз ичига мониторинг ва хавфсизлик ҳодиса-воқеаларини, ҳамда бу ҳодиса-воқеаларга тўғри жавобларни қайтаришни қамраб олади. Инцидентни бошқариш дастур ҳисобланиб маълум бир жараённи аниқлаб беради ва амалга оширади.

Ҳодиса - шахс ёки ишчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир.

Ҳодисанинг учта асосий тури мавжуд:

Нормал. Нормал ҳодиса критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.

Ҳодисаларни кенгайиши ва кўпайиши (Эскалация). Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.

Авариявий ҳодиса. Авариявий ҳодиса шахс хавфсизлиги ва соғлигига таъсир кўрсатади.

Инцидент - бу стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.

Инцидентга жавоб қайтариш гуруҳи. Хавфсизлик инциденти координатори инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир. Координатор командани ташкил этиб, ташкил этилган команда ўз ичига инцидентни баҳоловчи ва қарор қабул қилувчи шахсларни қамраб олади.

Инцидентни тергов қилиш - бу инцидент ҳолатини тергов қилиш ҳаракатидир. Ҳар бир инцидент тергов этишни талаб қилиши ёки унга кафиллик бериши керак бўлади. Шу билан бирга тергов қилинадиган ресурслар, яъни тиббий воситалар, номуносиб тармоқлар ва карантин қилинган тармоқлар фавқулодда инцидентларга тез ва самарали рухсат бериш учун фойдали ҳисобланади.

Инцидентга жавоб қайтариш - бу хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир. Бунинг мақсади вазиятни тўғрилаш, яъни тизимни бузилишини чеклаш ва бузилган тизимни тиклаш вақти ва маблағини камайтиришдир.

Инцидент бошқарувчисини вазифалари ва мажбуриятлари:

– муносиб ваколатлардан фойдаланиш учун ҳар қандай авария / носозликларни билиш;

– етарли ахборот йиғиш ва тизимни таҳлил этиш учун қайта тиклайдиган командани шакллантириш;

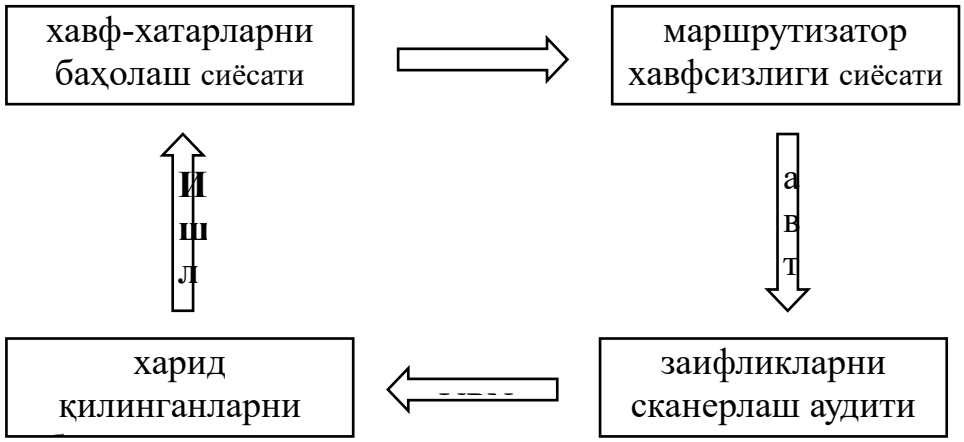
– инцидентни умумий ҳолатини сақлаш;

– функционал имкониятларни билиш (Core Network);

– командани юқори сатҳга кўтариш (приоритет бериш) учун қўлланмадан фойдаланиш.

Ҳужум инцидентларини бошқариш тизими

Ташкилот фаолиятида ахборотни ҳимоялаш учун қўйидаги моделни келтириш мумкин: **ИТРМ**. Бу модел 4та жараённи ўз ичига олади. Булар:



1.6-расм. ИТРМ модели.

Келтирилган 4 та жараён ҳам танқидий (критик) муҳим ҳисобланади. Тизимда бу жараёнларнинг бирортасини йўқлиги ёки яхши ишмаслиги корхона ёки ташкилот ахборот ресурслари ҳимояланганлигига катта зарар етказади. Ахборот хавфсизлиги инцидентларни бошқаришда бу жараёнларнинг ичидан фақат мониторинг жараёнини кўпроқ кузатиш мумкин.

Кўп ташкилот ва корхоналарда **ахборот хавфсизлиги инцидентларни бошқариш жараёни** қуйидагича қурилади:

- компьютер инциденти ҳақида ахборот олиш;
- қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш;
- ҳолатни таҳлил этиш;
- сабабларни аниқлаш;
- профилактик тадбирлар ўтказиш.

Инцидентларини бошқариш жараёни самарадорлиги қўйидагиларга боғлиқдир:

- ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши;
- инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги;
- олинган натижаларнинг ҳақиқийлиги.

Инцидентини бошқариш тизимини қуриш концепцияси ва структурасини қараб чиқамиз.

Ахборот хавфсизлиги инцидентини бошқариш тизими архитектураси қуйидаги асосий компоненталарни ўз ичига олади:

1. Интеграллашган платформа.
2. Аудит ва мониторингни аппарат-дастурий воситалари.
3. Ахборотни ҳимоялашнинг аппарат-дастурий воситалари.

4. Ахборот хавфсизлиги инцидентлари ҳақида ахборот омбори.
5. Ҳисоботларни генерациялаш воситалари ва аналитик асбоблар.
6. Воситаларни бошқариш ва интерфейсни тўғрилаш.

Интеграллашган платформа тизимнинг ядроси ҳисобланади. Бу тизим тузилишидаги ҳамма компонентаплари битта умумий функцияга боғлаб беради.

Интеграллашган платформа қўйидагилардан таркиб топган:

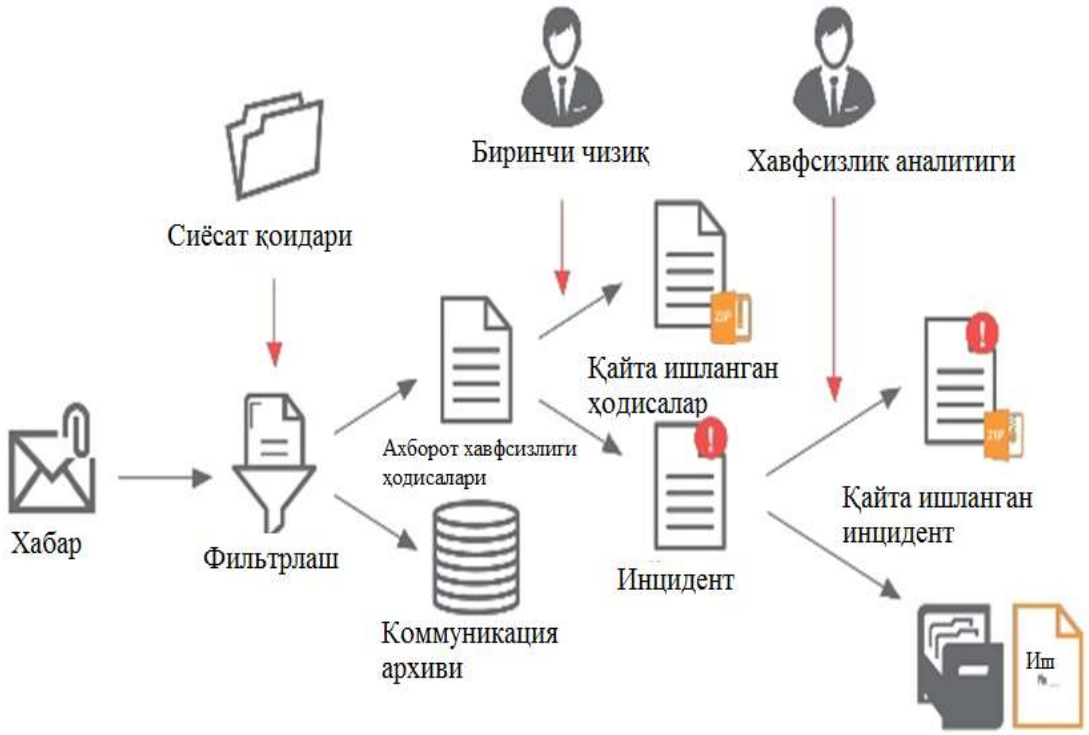
1. Маълумотларни йиғишни таъминловчи мониторинг ва аудит воситалари учун интерфейс.
2. Ахборот хавфсизлиги инцидентлари оқибатини локализациялаш мақсадида конфигурацияни тезкор ўзгартиришдаги ахборот ҳимояси воситалари интерфейси
3. Ҳисоботларни генерациялаш воситалари ва аналитик функциялардан фойдаланишдаги хизматлар.

Аудит ва мониторингни аппарат-дастурий воситалари - ташкилот ахборот тизимини қайта ишлаш, йиғиш ва протоколлаштиришни амалга оширувчи воситалардир. Бу воситаларга қуйидагилар киради: ўрнатилган воситалар (иловалар, операцион тизим воситалари, тармоқ қурилмалари, ҳимоя воситалари ва автоматлаштирилган тизимлар) ва махсус воситалар (аудит, хавфсизлик сканерлари, дастурий агентлар, сенсорлар, ахборот йиғувчи қурилмалар).

1.7-расм. Аудит ва мониторингни аппарат-дастурий воситалари.

Ахборотни ҳимоялашнинг аппарат-дастурий воситалари:

1. Firewalls
2. IDS/IPS
3. Switch Level 3
4. Ахборот хавфсизлигини таъминлаш усул ва воситалари (дастурий воситалар).



1.8-расм. Инцидентлар ахборот омбори.

Назорат саволлари:

1. Киберхавфсизлик тушунчасини изоҳлаб беринг.
2. Хавфсизлик муаммоларини санаб ўтинг.
3. Киберхавфсизлик сиёсати нима?
4. Киберхавфсизлик рискларини аниқлашни тавсифлаб беринг?
5. Инцидентга жавоб қайтариш гуруҳи қандай шакллантирилади?
6. Инцидентларини бошқариш жараёни самарадорлиги нималарга боғлиқдир?
7. Аудит ва мониторингни дастурий-аппарат воситаларини изоҳлаб беринг?

Адабиётлар ва интернет сайтлари:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.
3. https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-basics

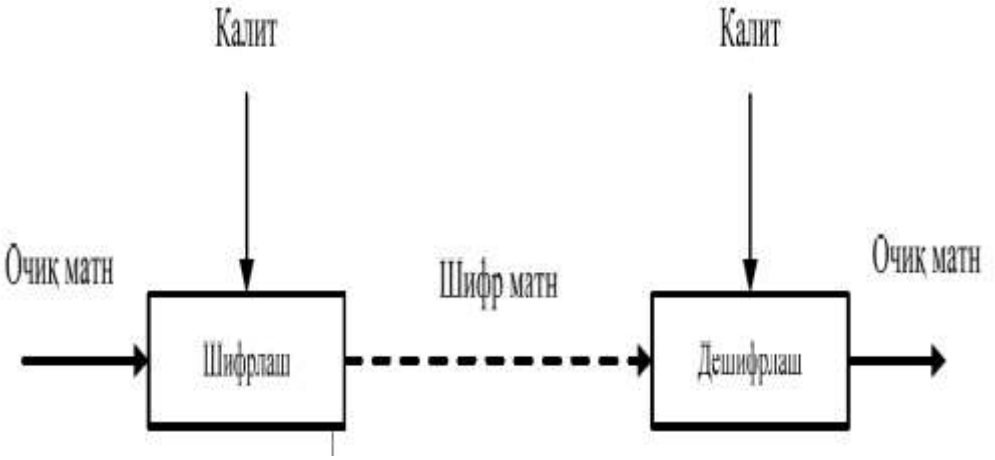
2-маъруза. Криптографиянинг асосий тушунчалари. Тармоқ хавфсизлиги заифликалари ва уларга бўлган таҳдидлар (2 соат)

Режа:
2.1. Криптографиянинг асосий тушунчалари.
2.2. Тармоқ хавфсизлиги заифликлари ва уларга бўлган таҳдидлар.

Таянч иборалар: *шифр, криптотизм, калит, криптоанализ, криптография, симметрик шифр, ассиметрик шифр, стенография, хэш функция,* тармоқ хавфсизлиги заифликлари, скайнерлар.

2.1. Криптографиянинг асосий тушунчалари.

Шифр ёки *криптотизим* маълумотни *шифрлаш* учун фойдаланилади. Ҳақиқий шифрланмаган маълумот *очиқ матн* деб аталиб, шифрлашнинг натижаси *шифрматн* деб аталади. Ҳақиқий маълумотни қайта тиклаш учун шифрматнни *дешифрлаш* зарур бўлади. *Калит* криптотизимни шифрлаш ва дешифрлаш учун созлашда фойдаланилади. Криптотизимнинг “қора қути” сифатидаги кўриниши расмда келтирилган.



2.1-расм. Криптотизимнинг “қора қути” сифатидаги кўриниши.

Ахборотни ҳимоялаш учун кодлаштириш ва криптография усуллари қўлланилади.

Кодлаштириш деб, ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш йўли билан ахборотга рухсат этилмаган киришга тўсиқ қўйиш усулига айтилади.

Калит- матнни шифрлаш ва шифрини очиш учун керакли ахборот.

Криптоанализ - калитни билмасдан шифрланган матнни очиш имкониятларини ўрганади.

Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қўйилади:

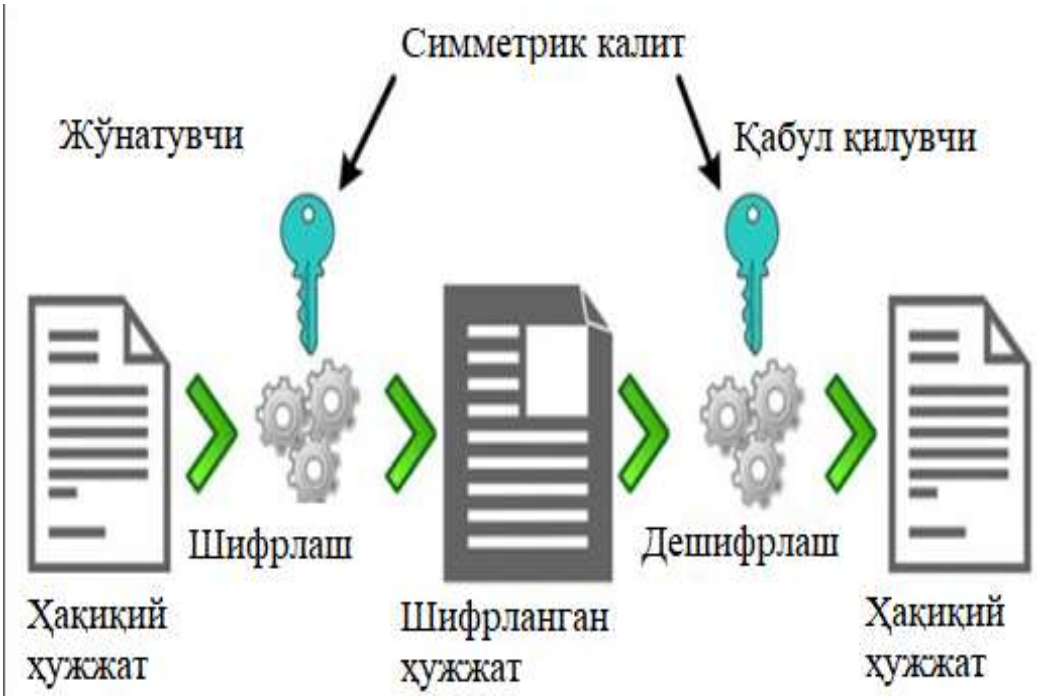
- етарли даражада криптобардошлилик;
- шифрлаш ва қайтариш жараёнининг оддийлиги;
- ахборотни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;

- шифрлашдаги кичик хатоларга таьсирчан бўлмаслиги.

Шифрлаш ва дешифирлаш масалаларига тегишли бўлган, маълум бир *алфавитда* тузилган маълумотлар *матнларни* ташкил этади. *Алфавит* - ахборотларни ифодалаш учун фойдаланиладиган чекли сондаги белгилар тўплами. Мисоллар сифатида:

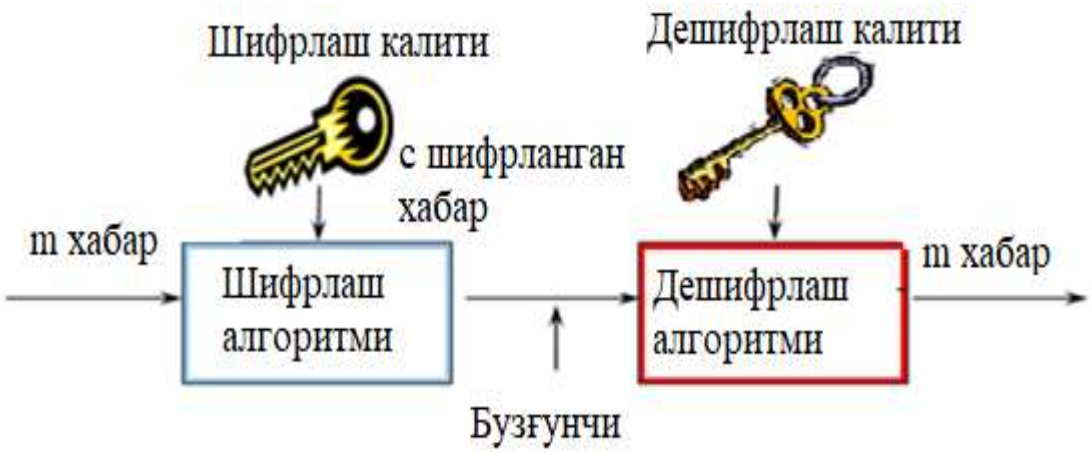
- ўттиз олтита белгидан (ҳарфдан) иборат ўзбек тили алфавити;
- ўттиз иккита белгидан (ҳарфдан) иборат рус тили алфавити;
- йигирма саккизта белгидан (ҳарфдан) иборат лотин алфавити;
- икки юзи эллик олтита белгидан иборат ASCII компьютер белгиларининг алфавити;
- бинар алфавит, яъни 0 ва 1 белгилардан иборат бўлган алфавит;
- саккизлик ва ўн олтилик саноқ системалари белгиларидан иборат бўлган алфавитларни келтириш мумкин.

Симметрик шифрларда маълумотни шифрлаш ва дешифрлаш учун бир хил калитдан фойдаланилади.



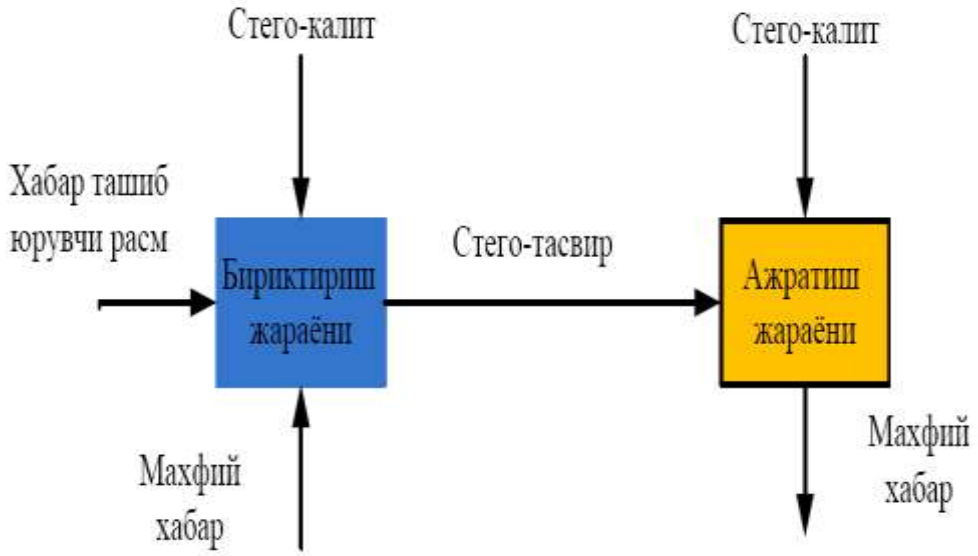
2.2-расм. Симметрик калит.

Бундан ташқари *очиқ калитли* (***ассиметрик***) криптотизимлар мавжуд бўлиб, унда шифрлаш ва дешифрлаш учун иккита калитдан фойдаланилади.



2.3-расм. Ассиметрик калит.

Стенанография – бу махфий хабарни сохта хабар ичига беркитиш орқали алоқани яшириш ҳисобланади. Бошқа сўз билан айтганда стеганографиянинг асосий ғояси – бу махфий маълумотларнинг мавжудлиги ҳақидаги шубҳани олдини олиш ҳисобланади.



2.4-расм. Стенография.

Хэш функция деб ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ёки байт бирликларида) қийматга ўтказувчи функцияга айтилади.

Криптографияда хэш функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

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

Маълумотни хэшлаш унинг бутунлигини кафолатлаш мақсадида амалга оширилиб, агар маълумот узатилиш давомида ўзгаришга учраса, у ҳолда уни аниқлаш имкони мавжуд бўлади. Хэш-функцияларда одатда кирувчи маълумотнинг узунлиги ўзгарувчан бўлиб, чиқишда ўзгармас узунликдаги

қийматни қайтаради. Замонавий хэш функцияларга MD5, SHA1, SHA256, O‘z DSt 1106:2009 ларни мисол келтириш мумкин. Қуйида “*hello*” хабарини турли хэш функциялардаги қийматлари келтирилган:

- $MD5(hello) = 5d41402abc4b2a76b9719d911017c592$
- $SHA1(hello) = aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d$
- $SHA256(hello) =$ $2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e7304336$
- $2938b9824$

Хеш функция қуйидаги хусусиятларга эга:

a) Бир хил кириш ҳар доим бир хил чиқишни (*хэш қиймат* деб аталади) тақдим этади.

b) Бир қанча турли киришлар бир хил чиқишни тақдим этмайди.

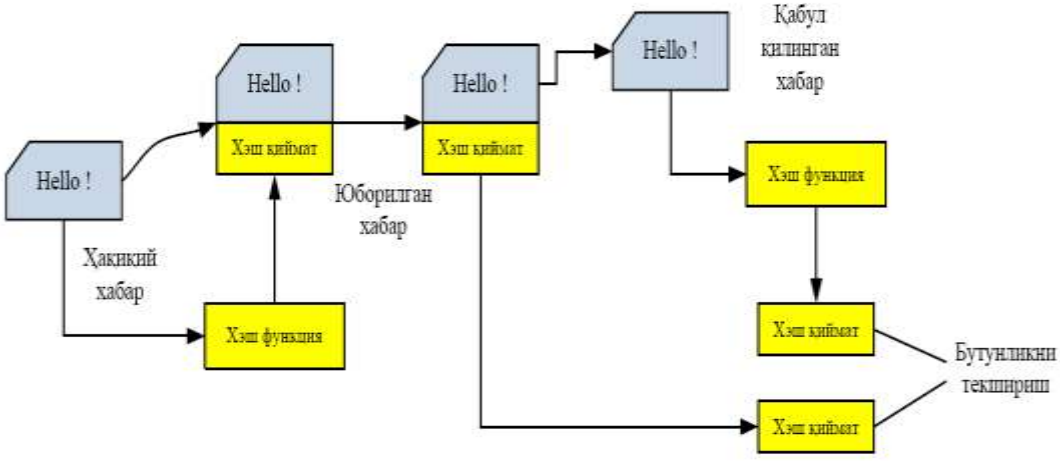
c) Чиқиш қийматдан кирувчи қийматни ҳосил қилишнинг имконияти мавжуд эмас (бир томонламалик).

d) Кириш қийматини ўзгариши чиқишдаги қийматни ҳам ўзгаришига олиб келади.

Хеш функцияга мисол

Мисол

- M = “Elvis” **M** → H → **H(M) = *h***
- H(M) = (“E” + “L” + “V” + “I” + “S”) mod 26
- H(M) = (5 + 12 + 22 + 9 + 19) mod 26
- H(M) = 67 mod 26
- H(M) = 15



2.5. Хеш функция схемаси.

Хулоса ўрнида шуни айтиш мумкинки, симметрик калитли ва очиқ калитли криптотизимлар маълумотларни махфийлигини таъминлашда фойдаланилса, хэш функциялар эса маълумотни бутунлигини текширишда фойдаланилади.

2.2. Тармоқ хавфсизлиги заифликалари ва уларга бўлган таҳдидлар.

Компьютер хавфсизлигида **заифлик** (англ. vulnerability) термини тизимнинг кам ҳимояланган ёки очиқ жойини белгилашда ишлатилади. Заифлик дастурнинг хатоси ёки тизимни лойиҳалашда йўл қўйилган камчилик натижаси бўлиши мумкин. Заифлик ёки фақат назарий мавжуд бўлиши ёки бирор таҳдидда фойдаланилган ҳолатда мавжуд бўлиши мумкин. Заифлик кўп ҳолларда дастурчининг бепарволиги натижасидир, бироқ бошқа сабаблар ҳам бўлиши мумкин.

Заифликларни аниқловчи ташкилотлар:

1. COAST лабораторияси.
2. Protection Analysis Project.
3. RISOS.
4. Internet Security Systems.

Заифликлар классификацияси:

1. Операцион тизим заифликлари.
2. Иловалар заифликлари.
3. Тармоқ заифликлари.
4. Физик заифликлар.

Хавфсизлик сканерлари классификациясини қараб чиқамиз.

1.Баҳоси бўйича:

• бепул — кенг тарқалган, тестланадиган узеллар сони чегараланмаган;

• тижорат нархи — бундай сканерларнинг лицензия нархи юздан бир неча минг долларгача етиши мумкин.

2. Архитектураси бўйича:

• автоном - ўзида мустақил дастурий таъминотни мужассам этган. Сканерловчи модуллар ва заифликлар маълумотлар базаси дастурий таъминот дистрибутивига тегишли бўлиб, шахсий компьютерларда локал сақланади;

• мижоз-сервер – дистрибутивга мижоз ва сервер қисми киради. Дастурий таъминот ёки якуний фойдаланувчи тизимнинг мижоз қисми билан боғланган бўлиб, у тармоқ усти интерфейсини оддий ҳолда таъминлайди.

3. Чиқиш коди бўйича:

• чиқиш коди очиқ – фойдаланувчи сканер модуллари ишлашинибаҳолаш имконига эга бўлиб, зарур бўлганда қўшимча ўзгартиришлар киритиши мумкин;

• чиқиш коди ёпиқ – маълумки бундай вазият тижорат маҳсулотларига характерлидир. Қонуний фойдаланувчи бундай хавфсизлик сканерларининг чиқиш кодини модификациялаш ва танишиш имкониятидан маҳрумдир.

4. Фойдаланиш бўйича:

• дастурий;

• дастурий-аппарат.

5.Қўлланилиш муҳити бўйича:

• операцион тизим сканерлари – операцион тизим оиласига характерли бўлган параметрларни таҳлиллайди:

• фойдаланувчиларнинг ҳисоб ёзуви, созланишлар шаблони;

• заифликларини қидириш.

Тармоқ сканерлари – бу масофавий ёки локал ташхис дастури бўлиб, у тармоқнинг турли элементларида ҳар хил заифликларни аниқлайди. Оддий сканерлардан фарқли ўлароқ улар турли воситалар ёрдамида дастурий таъминот

версиясини аниқлайди ва ўзининг базасида маълум заифликлар мавжудлигини текшириб, уларни зарарсизлантириш учун қисқача қўлланма ва таъриф келтиради. Бундан ташқари заифликларнинг хавфлилик даражаси ҳақида ҳам маълумот беради. Тармоқ сканерларига: порт сканерлари (очиқ TCP ва UDP портларини қидирувчи) ва CGI сканерлари (WEB серверларида заиф скриптларни, директорийларни ва WEB серверлар хатоликларни сканерлайди) киради.

Тармоқдаги заифликларни бартараф этиш йўллари ва воситаларини қараб чиқамиз.

Тармоқдаги заифликларни бартараф этиш учун тармоқ қурилмаларида турли ишларни амалга ошириш мумкин:

1. Port security.
2. Access lists.
3. Маълумотларни шифрлаб узатиш алгоритмларини ёқиш.

Бундан ташқари турли трафик таҳлилловчи тизимларни ишлатишимиз, Kerio Control ҳамда Proxy серверлардан фойдаланишимиз лозим, лекин буларнинг ҳам узига яраша камчиликлари мавжуд: Оддий VPN билан алдаб кетиш мумкин.

Илова сканерлари – аниқ МББТ, Web-браузерлари ва бошқа амалий тизимларга мўлжалланган.

Ишлатилаётган ҳар бир илованинг ўз чиқиш порти мавжуд бўлиб бу портлардан турли мақсадларда фойдаланиш мумкин.

Application	Protocol		Port	DB Node	Cell Node	IB	DB ILOM	Cell ILOM	IB ILOM	KVM	PDU	Outgoing	Comment
SSH	TCP	SSH	22	✔	✔	✔	✔	✔	✔				
Telnet	TCP		23							✔			
SMTP	SMTP		25									•	
			465									•	If using SSL
TFTP	UDP		69				✔	✔	✔			•	
Web HTTP	TCP	HTTP	80				✔	✔	✔		✔		
NTP	NTP	NTP	123	✔	✔	✔	✔	✔	✔			•	
SNMP	UDP	SNMP	161				✔	✔	✔	✔	✔		
SNMP (out)	UDP	SNMP	162							✔	✔	•	
SNMP (out)	IPMI	SNMP	162				✔	✔	✔			•	Outgoing IPMI Platform Event Trap (PET)
SNMP (out)	SNMP		162		✔		✔	✔	✔			•	Telemetry messages sent to ASR Manager
LDAP	TCP/UDP	LDAP	389				✔	✔	✔				
Web	TCP	HTTPS	443				✔	✔	✔	✔	✔		
Syslog	UDP	Syslog	514				✔	✔	✔	✔	✔	•	Outgoing Syslog
DHCP	UDP	DHCP	546				✔	✔	✔	✔	✔	•	DHCP client
IPMI	UDP	IPMI	623				✔	✔	✔				
OEM	TCP	HTTPS	1159	✔	✔	✔	✔	✔	✔			•	OEM upload port
DB	TCP		1521	✔									Database listener
RADIUS	UDP	RADIUS	1812				✔	✔	✔			•	Outgoing RADIUS
KVM	TCP		2068							✔			
OEM	TCP	HTTP	4889	✔	✔	✔	✔	✔	✔			•	OEM upload port
remote console	TCP		5120				✔	✔	✔				ILOM remote console: CD
remote console	TCP		5121				✔	✔	✔				ILOM remote console: keyboard and mouse
remote console	TCP		5123				✔	✔	✔				ILOM remote console: diskette
remote console	TCP		5555				✔	✔	✔				ILOM remote console: encryption
remote console	TCP		5556				✔	✔	✔				ILOM remote console: authentication
remote console	TCP	HTTP	6481				✔	✔	✔				Service tags listener for asset activation
remote console	TCP		7578				✔	✔	✔				ILOM remote console: video
remote console	TCP		7579				✔	✔	✔				ILOM remote console: serial
OEM Console	TCP	HTTP	7777	✔	✔								OEM HTTP console port
OEM Console	TCP	HTTPS	7799	✔	✔								OEM HTTPS console port

Назорат саволлари:

1. Ахборотни ҳимоялаш учун кодлаштириш ва криптография усулларини тушунтириб беринг.
2. Симметрик ва ассиметрик криптотизимларни тушунтириб беринг?
3. Хеш функция нима?
4. Заифликлар классификациясини санаб ўтинг?
5. Тармоқ сканерлари нима?
6. Тармоқдаги заифликларни бартараф этиш йўллари ва воситаларини тушунтириб беринг?

Адабиётлар ва интернет сайтлари:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.
3. https://ichip.ru/sovety/chto-takoe-kompyuternyjj-virus-prosto-o-slozhnom-223382
4. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

3-маъруза. Компьютер вируслари, зараркунанда дастурлар ва улардан ҳимояланиш механизмлари (2 соат)

Режа:

3.1. Компьютер вируси тушунчаси.
3.2. Компьютер вируслари ва уларнинг классификациялари.
3.3. Вируслар билан курашиш усуллари ва воситалари.

Таянч иборалар: *компьютер вируслари, тармоқ вируслари; файл вируслари; юклама вируслар; комбинацияланган вируслар, резидент вируслар; резидент бўлмаган вируслар; талаба вируслар; «стелс» вируслар (кўринмайдиган вируслар); полиморф вируслар, сканерлаш; ўзгаришларни билиб қолиш; эвристик тахлил; резидент қоровуллардан фойдаланиш; программани вакцинациялаш; вируслардан аппарат-программ ҳимояланиш.*

3.1. Компьютер вируси тушунчаси

«**Компьютер вируслари**» - компьютер тизимларида тарқалиш ва ўз-ўзидан қайтадан тикланиш (репликация) хусусиятларига эга бўлган бажарилувчи ёки шархланувчи кичик дастурлардир. Вируслар компьютер тизимларида сақланувчи дастурий таъминотни ўзгартириши ёки йўқотиши мумкин.

Ичида вирус жойлашган дастур **зарарланган** деб аталади. Бундай дастур ўз ишини бошлаганда, олдин бошқаришни вирус ўз қўлига олади. Вирус бошқа дастурларни топади ва «зарарлантиради» ҳамда бирор-бир зарарли ишларни (масалан, файлларни ёки дискда файлларни жойлашиш жадвалини бузади, тезкор хотирани ишлаш жараёнини пасайтиради ва ҳ.к.) бажаради. Вирусни ниқоблаш учун бошқа дастурларни зарарлантириш ва зарар етказиш бўйича ишлар ҳар доим ҳам эмас, айтайлик маълум бир шартлар бажарилганда бажарилиши мумкин. Вирус унга керакли ишларни бажаргандан кейин у бошқаришни ўзи жойлашган дастурга узатади ва у дастур одатдагидай ишлай бошлайди. Шу билан бирга ташқи кўринишдан зарарланган дастурнинг ишлаши зарарланмагандек каби кўринади.

Вирусларнинг кўпгина кўринишлари шундай тузилганки, зарарланган дастур ишга туширилганда вирус компьютер хотирасида ҳар доим қолади ва вақти-вақти билан дастурларни зарарлантиради ва компьютерда зарарли ишларни бажаради.

Вируснинг барча ҳаракатлари етарлича тез бажарилиши мумкин ва бирор-бир хабарни бермайди, шунинг учун фойдаланувчи компьютерда бирорта одатдан ташқари ишлар бўлаётганини пайқаши жуда мушкулдир.

Компьютерда нисбатан кам дастурлар зарарланган бўлса, вируснинг борлиги деярли сезиларсиз бўлади. Лекин вақт ўтиши билан компьютерда қандайдир ғалати ҳодисалар рўй бера бошлайди, масалан:

- баъзи дастурлар ишлашдан тўхтайдилар ёки нотўғри ишлайди;
- экранга бегона хабар ёки белгилар чиқади;
- компьютернинг ишлаш тезлиги секинлашади;
- баъзи бир файллар бузилиб қолади ва ҳ.к.

Бу вақтга келиб, қоидага кўра, фойдаланувчи ишлаётганда етарлича кўп (ёки ҳатто кўпчилик) дастурлар вируслар билан зарарланган, баъзи бир файл ёки дисклар эса ишдан чиққан ҳисобланади. Бундан ташқари, фойдаланувчи

компьютеридаги зарарланган дастурлар дискеталар ёрдамида ёки локал тармоқ бўйича фойдаланувчи ҳамкасблари ва ўртоқларининг компьютерига ўтиб кетган бўлиши мумкин .

Вирусларнинг баъзи бир кўринишлари ўзларини янада хавфлироқ кириб тушадилар. Улар бошланишда катта миқдордаги дастурларни ёки дискларни билдирмасдан зарарлантирадилар, кейин эса жиддий шикастланишларини келтириб чиқаради, масалан, компьютердаги бутун қаттиқ дискни форматлайди. Дастур – вирус сезиларсиз бўлиши учун у катта бўлмаслиги керак. Шунинг учун, қоидага кўра, вируслар етарлича юқори малакали дастурловчилар томонидан Ассемблер тилида ёзилади.

Компьютер вирусларини пайдо бўлиши ва тарқатилиши сабаблари, бир томондан, инсон шаҳсиятининг руҳиятида ва унинг ёмон хислатларида яширинади (ҳаваслар, қасос олишлар, тан олинмаган ижодкорларнинг мансабпарастлиги, ўз қобилиятларини конструктив қўллаш имконияти йўқлиги), иккинчи томондан эса, ҳимоя қилишнинг аппарат воситаларини ва шахсий компьютернинг операцион тизими томонидан қарши ҳаракатларнинг йўқлиги билан боғлиқдир.

Вирусларни компьютерга кириб олишининг асосий йўллари олинадиган дисклар (эгилувчан ва лазерли) ҳам компьютер тармоқлари ҳисобланади. Қаттиқ дискни вируслар билан зарарланиши компьютерни вирусни ўзида сақлаган дискетадан юклаганда амалга ошиши мумкин. Бундай зарарланиш тасодифий бўлиши мумкин, масалан, дискетани А дисководдан чиқариб олмасдан ва компьютерни қайта юкланганда, бунда дискета тизимли бўлмаслиги ҳам мумкиндир. Дискетани зарарлантириш жуда оддийроқдир. Унга вирус ҳаттоки, агар дискетани зарарланган компьютер дисководига қўйилганда ва унинг мундарижасини ўқилганда, тушиш мумкин.

Зарарланган диск бу юкланиш секторида дастур – вирус жойлашган дискдир.

Вирусни ўз ичига олган дастур ишга туширилгандан кейин бошқа файлларни зарарлантириш мумкин бўлиб қолади. Энг кўпроқ вируслар билан дискнинг юкланадиган сектори ва .EXE, .COM, .SYS ёки BAT кенгайтмасига эга бўлган файллар зарарланади. Кам матнли ва графикли файллар кам зарарланади.

Зарарланган дастур, бу унга тадбиқ қилинган дастур – вирусни ўз ичига олган дастурдир. Компьютер вируси билан зарарланишда ўз вақтида уни пайқаш жуда муҳимдир. Бунинг учун вирусларни пайдо бўлишининг асосий белгилари тўғрисида билимларга эга бўлиш керак. Уларга қуйидагилар тегишли бўлиши мумкин:

- олдин муваффақиятли ишлаган дастурларнинг ишлашдан тўхташи ёки нотўғри ишлаши;
- компьютернинг секин ишлаши;
- операцион тизимни юклаш имкони йўқлиги;
- файл ва каталогларни йўқолиб қолиши ёки уларнинг мазмунини бузилиши;
- файлларни ўзгартирилганлик санаси ва вақтининг ўзгариши;
- дискда файллар сони бехосдан жуда ошиб кетиши;
- бўш тезкор хотира ўлчамининг жиддий камайиши;
- экранга кўзда тутилмаган хабарларни ёки тасвирларни чиқариш;
- кўзда тутилмаган товушли хабарларни бериш;
- компьютер ишлашда тез-тез бўладиган осилиб қолишлар ва бузилишлар.

Таъкидлаш керакки, юқорида санаб ўтилган ҳодисалар вирусларни келиб чиқиши билан бўлиши мажбурий эмас, бошқа сабабларнинг оқибатлари ҳам

бўлиши мумкин. Шунинг учун компьютер ҳолатини тўғри диагностикалаш ҳар доим мушкулдир.

Компьютер вируси компьютерда мавжуд бўлган дисклардаги исталган файлни етарлича ўзгартириш ва бузиши мумкин. Лекин файлларнинг баъзи бир турларини вирус «зарарлантириши» мумкин. Бу шуни билдирадики, вирус бу файлларга «тадбиқ» қилиниши мумкин, яъни уларни шундай ўзгартирадики, улар вирусни ўз ичида сақлайди ва бу вирус баъзи бир ҳолатларда ўзининг ишини бошлаши мумкин.

Таъкидлаш лозимки, дастур ва ҳужжатларнинг матнлари, маълумотлар базасининг ахборотли файллари, жадвалли процессор жадваллари ва бошқа шунга ўхшаш файллар вирус билан зарарланиши мумкин эмас, бу файлларни вируслар бузиши мумкин.

3.2. Компьютер вируслари ва уларнинг классификациялари

Барча компьютер вируслари қуйидаги аломатлари бўйича классификацияланиши мумкин:

- *яшаш муҳити бўйича;*
- *яшаш муҳитининг захарланиши бўйича;*
- *зараркунандалик таъсирнинг хавфи даражаси бўйича;*
- *ишлаш алгоритми бўйича.*

Яшаш муҳити бўйича компьютер вируслари қуйидагиларга бўлинади:

- *тармоқ вируслари;*
- *файл вируслари;*
- *юклама вируслар;*
- *комбинацияланган вируслар*.

Файл вируслари бажарилувчи файлларга турли усуллар билан кирити лади (энг кўп тарқалган вируслар хили), ёки файлйўлдошларни (компанъон вируслар) яратади ёки файлли тизимларни (linkвируслар) ташкил этиш хусусиятидан фойдаланади.

Юклама вируслар ўзини дискнинг юклама секторига (boot секторига) ёки винчестернинг тизимли юкловчиси (Master Boot Record) бўлган сек торга ёзади. Юклама вируслар тизим юкланишида бошқаришни олувчи дастур коди вазифасини бажаради.

Макровируслар ахборотни ишловчи замонавий тизимларнинг макро дастурларини ва файлларини, хусусан MicroSoft Word, MicroSoft Excel ва ҳ. каби оммавий муҳаррирларнинг файл хужжатларини ва электрон жадвалларини заҳарлайди.

Тармоқ вируслари ўзини тарқатишда компъютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзида тармоқ вирусларини "қурт" хилидаги дастурлар деб юритишади. Тармоқ вируслари Internet қуртларга (Internet бўйича тарқалади), IRCқуртларга (чатлар, Internet Relay Chat) бўлинади.

Яшаш муҳитининг захарланиши усули бўйича компьютер вируслари қуйидагиларга бўлинади:

- *резидент;*
- *резидент бўлмаган;*

Резидент вируслар фаоллашганларидан сўнг тўлалигича ёки қисман яшаш муҳитидан (тармоқ, юклама сектори, файл) ҳисоблаш машинасининг асосий

хотирасига кўчади. Бу вируслар, одатда, фақат операцион тизимга рухсат этилган имтиёзли режимлардан фойдаланиб яшаш муҳитини захарлайди ва маълум шароитларда зараркунандалик вазифасини бажаради.

Резидент бўлмаган вируслар фақат фаоллашган вақтларида ҳисоблаш машинасининг асосий хотирасига тушиб, захарлаш ва зараркунандалик вазифаларини бажаради. Кейин бу вируслар асосий хотирани бутунлай тарк этиб яшаш муҳитида қолади. Агар вирус яшаш муҳитини захарламайдиган программани асосий хотирага жойлаштирса бундай вирус резидент бўлмаган вирус деб ҳисобланади.

Фойдаланувчининг информацион ресурслари учун хавф даражаси бўйича компьютер вирусларини қуйидагиларга ажратиш мумкин:

- *безиён вируслар;*
- *хавфли вируслар;*
- *жуда хавфли вируслар*;

Яшаш маконини ўзгартирмайдиган вируслар ўз навбатида иккита гуруҳга ажратилиши мумкин.

- вируслар-«йўлдошлар» (companion). Вируслар-«йўлдошлар» файлларни ўзгартирмайди. Унинг таъсир механизми бажарилувчи файлларнинг нусҳаларини яратишдан иборатдир.
- Вируслар-«қуртлар» тармоқ орқали ишчи станцияга тушади, тармоқнинг бошқа абонентлари бўйича вирусни жўнатиш адресларини ҳисоблайди ва вирусни узатишни бажаради.

Алгоритмларнинг мураккаблиги, мукаммалик даражаси ва яшириниш хусусиятлари бўйича яшаш маконини ўзгартирадиган вируслар қуйидагиларга бўлинади:

- *талаба вируслар;*
- *«стелс» вируслар (кўринмайдиган вируслар);*
- *полиморф вируслар.*

Талаба-вируслар малакаси паст яратувчилар томонидан яратилади. Бундай вируслар, одатда, резидент бўлмаган вируслар қаторига киради, уларда кўпинча хатоликлар мавжуд бўлади, осонгина танилади ва йўқотилади.

«Стелс» вируслар малакали мўтахасислар томонидан ярятилади. «Стелс»-вируслар операцион тизимнинг шикастланган файлларга мурожаатларини ушлаб қолиш йўли билан ўзини яшаш маконидагилигини яширади ва операцион тизимни ахборотнинг шикастланмаган қисмига йўналтиради. Вирус резидент ҳисобланади, операцион тизим программалари остида яширинади, хотирада жойини ўзгартириши мумкин. «Стелс» - вируслар резидент антивирус воситаларига қарши таъсир кўрсата олиш қобилиятига эга.

Полиморф вируслар ҳам малакали мўтахасислар томонидан яратилади, ва доимий танитувчи гурухлар-сигнатураларга эга бўлмайди. Оддий вируслар яшаш маконининг захарланганлигини аниқлаш учун захарланган объектга махсус танитувчи иккили кетма-кетликни ёки символлар кетма-кетлигини (сигнатурани) жойлаштиради. Бу кетма-кетлик файл ёки секторнинг захарланганлигини аниқлайди.

3.3. Вируслар билан курашиш усуллари ва воситалари

Вируслар тарқалишининг оммалашуви, улар таъсири оқибатларининг

жиддийлиги вирусга қарши махсус воситаларни ва уларни қўллаш методларини яратиш заруриятини туғдирди. Вирусга қарши воситалар ёрдамида қуйидаги масалалар ечилади:

• *компьютер тизимларида вирусларни аниқлаш;*

• *вируслар таъсири оқибатларини йўқотиш.*

Компьютер тизимларида вирусларни аниқлашнинг қуйидаги методлари мавжуд:

• *сканерлаш;*

• *ўзгаришларни билиб қолиш;*

• *эвристик тахлил;*

• *резидент қоровуллардан фойдаланиш;*

• *программани вакцинациялаш;*

• *вируслардан аппарат-программ ҳимояланиш.*

Вирусларга қарши программлар ёрдамида вируслар таъсири оқибатларини йўқотишнинг икки усули мавжуд.

Биринчи усулга биноан тизим маълум вируслар таъсиридан сўнг тикланади. Вирусни йўқотувчи программани яратувчи вируснинг стуктурасини ва унинг яшаш маконида жойлашиш характеристкаларини билиши шарт.

Иккинчи усул номаълум вируслар билан захарланган файлларни ва юклама секторини тиклашга имкон беради. Файлларни тиклаш учун тикловчи программа файллар хусусидаги вируслар йўқлигидаги ахборотни олдиндан сақлаши лозим. Захарланмаган файл хусусидаги ахборот ва вируслар ишлашининг умумий принциплари хусусидаги ахборотлар файлларни тиклашга имкон беради.

Ҳозирги вақтда вирусларни йўқотиш учун кўпгина усуллар ишлаб чиқилган ва бу усуллар билан ишлайдиган дастурларни **антивируслар** деб аташади. Антивирусларни, қўлланиш усулига кўра, қуйидагиларга ажратишимиз мумкин: детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар.

Детекторлар – вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича оператив хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлай олмаслиги детекторларнинг камчилиги ҳисобланади.

Фаглар – ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги ҳолатига қайтаради.

Вакциналар - юқоридагилардан фарқли бўлиб, у ҳимояланаётган дастурга ўрнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис, ушбу антивирус дастурлар кенг тарқалмаган.

Прививка - файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар прививка қилинган файлга ёпишмайди.

Фильтрлар – қўриқловчи дастурлар кўринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақида фойдаланувчига хабар беради.

Ревизорлар – энг ишончли ҳимояловчи восита бўлиб, дискнинг биринчи ҳолатини хотирасида сақлаб, ундаги кейинги ўзгаришларни доимий равишда назорат қилиб боради.

Детектор дастурлар компьютер хотирасидан, файллардан вирусларни

қидиради ва аниқланган вируслар ҳақида хабар беради.

Доктор дастурлари нафақат вирус билан касалланган файлларни топади, балки уларни даволаб, дастлабки ҳолатига қайтаради. Бундай дастурларга Aidstest, DoctorWeb дастурларини мисол қилиб келтириш мумкин. Янги вирусларнинг тўхтовсиз пайдо бўлиб туришини ҳисобга олиб, доктор дастурларни ҳам янги версиялари билан алмаштириб туриш лозим.

Фильтр дастурлар компьютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Бу ҳаракатлар қуйидагича бўлиши мумкин :

- файллар атрибутларининг ўзгариши;
- дискларга доимий манзилларда маълумотларни ёзиш;
- дискнинг ишга юкловчи секторларига маълумотларни ёзиб юбориш.

Текширувчи (ревизор) дастурлари вирусдан ҳимояланишнинг энг ишончли воситаси бўлиб, компьютер зарарланмаган ҳолатидаги дастурлар, каталоглар ва дискнинг тизим майдони ҳолатини хотирада сақлаб, доимий равишда ёки фойдаланувчи ихтиёри билан компьютернинг жорий ва бошланғич ҳолатларини бир-бири билан солиштиради. Бу дастурга ADINF дастурини мисол қилиб келтириш мумкин.

Ҳозирги кунда компьютер вирусларига қарши курашга ихтисослашган компаниялар вужудга келган. Улар ҳар кун, ҳар соат мижозларнинг компьютеридаги мавжуд вирусларни топиб, уларни йўқ қиладиган антивирус дастурларини яратадилар. Ҳозирги кунда компьютер вирусларига қарши курашувчи антивирус дастурларидан энг асосийлари **KasperskyAnti-Virus (AVP) ScriptChecker, NortonAntivirus, DrWeb, Adinf, AVP**лар ҳисобланади. **KasperskyAnti-Virus** дастури бугунги кунда компьютер вирусларининг 100000 дан ортиқ турини аниқлайди ва даволайди.

Компьютер вирусларидан ҳимоя қилиш усуллари

Компьютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

– вирусларнинг кириб келишини бартараф этиш;

– агар вирус барибир компьютерга кирган бўлса, вирус ҳужумини бартараф этиш;

– агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф этиш.

Ҳимоя қилишни амалга оширишнинг учта усули мавжуддир:

– ҳимоя қилишнинг дастурли усуллари;

– ҳимоя қилишнинг аппаратли усуллари;

– ҳимоя қилишнинг ташкилий усуллари.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: «касалликни даволагандан кўра унинг олдини олган яхшироқ». Афсуски, айнан у энг бузувчи оқибатларни келтириб чиқаради. Компьютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустаҳкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум, бу муҳим маълумотларни йўқотишни ягона бўлмаган ҳаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операцион тизимни ишдан чиқариши мумкин ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқатсиз қилиб қўйиш қобилиятига эгадирлар. Ўғирлаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда

компьютерни йўқотиш эҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда «охиридан» бошлаш керак – исталган таъсирни, у вирус ҳужуми, хонада ўғирлик ёки қаттиқ дискни физик ишдан чиқишидан қатъий назар, бузувчи оқибатларини бартараф этишдан бошлаш керак.

Маълумотлар билан ишончли ва хавфсиз ишлашга фақат шундагина эришиладики, агар исталган кутилмаган ҳодиса, шу жумладан компьютерни тўлиқ физик ишдан чиқариш ҳам, салбий оқибатларга олиб келмаслиги керак.

Назорат саволлари:

1. Компьютер вируси нима?
2. Файл ва дискларда компьютер вируслари мавжудлигини текшириш.
3. Элементларни, узел(тугун) ва қурилмаларда компьютер вируслари мавжудлигини текшириш.
4. Вирус нима ва унинг бажарадиган вазифаси?
5. Вируслар компьютерда қандай пайдо бўлади?
6. Вирусларнинг қандай турларини биласиз?
7. Компьютерда вируслар мавжудлиги қандай аниқланади?
8. Антивирус дастурларининг қандай турларини биласиз?
9. Компьютер вирусларидан ҳимояланишда эҳтиёткорлик чоралари нималардан иборат?
10. Компьютер вируслари ва уларнинг классификацияси тушунтириб беринг?
11. Вируслар билан курашиш усуллари ва воситаларини изоҳлаб беринг?

Адабиётлар ва интернет сайтлар:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.
3. Ахборот хавфсизлиги бўйича ўқув-услубий мажмуа. https://studfile.net/preview/7883185/
4. https://studfile.net/preview/7883185/page:23/

IV БЎЛИМ

АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

IV. АМАЛИЙ МАШҒУЛОТ МАТЕРИАЛЛАРИ

1-амалий машғулот
Рисклар ва рискларни баҳолаш усуллари
(2 соат)

Ишдан мақсад – киберхавфсизликни таъминлашда рискларни аниқлаш ва уларни баҳолаш бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Назарий маълумот.

Риск бу - белгиланган шароитларда таҳдиднинг манбаларга потенциал зарар етказилишини кўтиш.

Бундан танқари, рискни қуйидагича тушуниш мумкин:

Риск бу - ички ёки танқи мажбуриятлар натижасида таҳдид ёки ҳодисаларни юзага келиши, йўқотилиши ёки бошқа салбий таъсир кўрсатиши мумкин бўлган воқеа.

Риск бу - манбага зарар келтирадиган ички ёки танқи заифлик таъсирида таҳдид қилиш эҳтимоли.

Риск бу - воқеа содир бўлиши эҳтимоли ва ушбу ҳодисанинг ахборот технологиялари активларига таъсири.

Риск, таҳдид, заифлик ва таъсир ўртасидаги боғланиш қуйидагича:

Риск = Таҳдид ×Заифлик ×Таъсир

Ҳодисанинг ахборот активига таъсири бу – активдаги ёки манфаатдор томонлар учун активнинг қийматидаги заифликнинг натижаси.

АТ риски қуйидагича кенгайтирилиши мумкин:

РИСК = Таҳдид ×Заифлик ×Актив қиймати

Риск қуйидаги икки факторнинг мужассамлашганидир:

- зарарли ҳодисани юзага келиш эҳтимоли;
- зарарли ҳодисанинг оқибатлари.

Рискнинг даражалари

1. Рисклар тизимда кутилаётган таъсирига боғлиқ ҳолда турли сатҳларда гуруҳланади.
2. Рискларнинг таъсир даражаси активнинг ва таъсир қилган ресурслар қиймати ва зарарнинг жиддийлигига боғлиқ бўлади.

Риск даражаси	Ҳаракати
	Рискларга қарши зудликда чора кўриш зарур

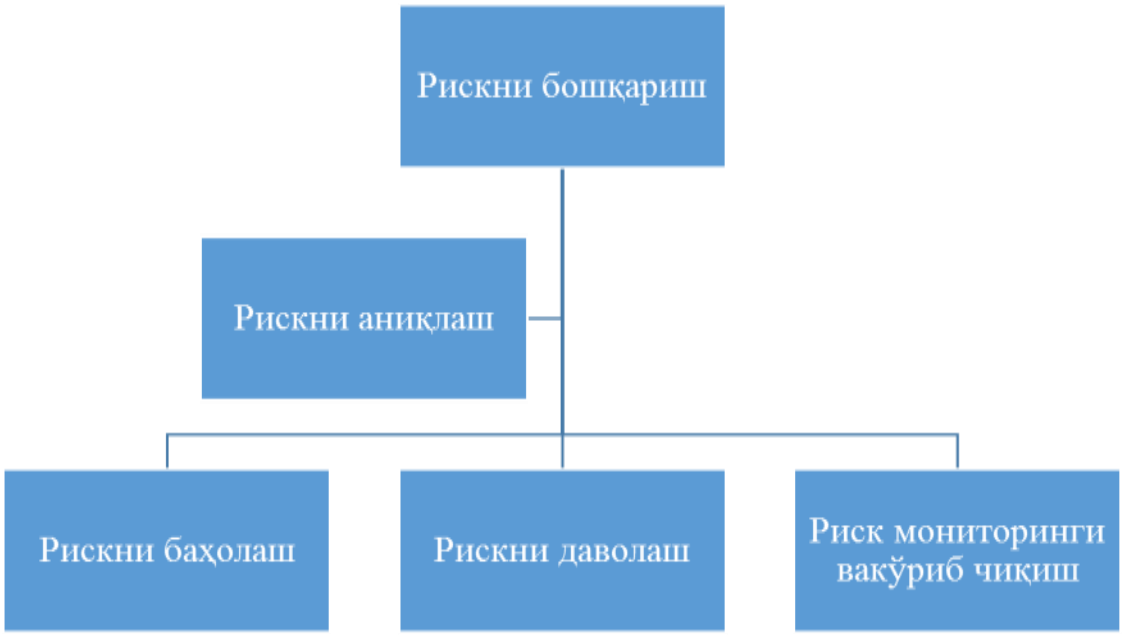
Юқори	Рискни етарлиича паст даражагача тушириш учун назоратлаш воситаларини аниқлаш ва ўрнатиш керак.
	Зидлик билан чора кўриш талаб этилмасада, қисқа вақтда қарши
Урта	Ҳаракатларни қўллаш зарур;
	Рискни етарлиича паст даражагача тушириш учун имкони борича назоратни амалга ошириш керак.
Қуйи	Риск таъсирини камайтириш учун профилатика чораларини кўриш зарур.

Рискни бошқариш

Рискни бошқаришдан мақсад	**Рискни бошқариш афзаллиги**
• Потенциал рискларни аниқлаш; • Рискни таъсирин аниқлаш ва ташкилотга унга қарши курашишда ёрдам бериш; • Рискнинг жиддийлик даражасига кўра рискларни баҳолашнинг усул, восита ва технологияларини ўрнатиш; • Риск ва риск ҳодисаси баёнини тушуниш ва таҳлил қилиш; • Рискни назоратлаш ва қарши чоралар кўриш.	• Потенциал рискни таъсир соҳасига қаратилган; • Рисклар даражасига кўра мурожаат қилиниши мумкин; • Рискларни тўтиш жараёнини яхшилайди; • Салбий ҳолатларда хавфсизлик ходимига самарали ҳаракат қилишга имкон беради; • Ресурслардан самарали фойдаланиш имконини беради.

Муҳим риск кўрсаткичлари (МРК) рискларни бошқариш жараёнининг муҳим компоненти бўлиб, ҳаракатларни хавфлилигини кўрсатади.

- МРК ни аниқлаш учун ташкилот мақсадини тушуниш талаб қилинади.
- МРК - ташкилот учун риск эҳтимоли ўлчовидир.



Рискни бошқариш: Рискни аниқлаш

Ташкилот хавфсизлигига таъсир қилувчи ташқи ва ички рискларнинг манбаси, сабаби, оқибати ва ҳакларни аниқлаш.

Муҳитни ўрнатиш

- Ходимлар ташқи ва ички муҳитни аниқлайди ва ташкилотда амалга оширилган жорий муҳитни тушунади.

Рискларни санаш

- Рисклар таъсирини ҳисоблаш ва рисклардан кутилган натижаларни калибрлаш.
- Рискларни баҳолаш босқичи ташкилотнинг риск даражасини баҳолайди ва риск таъсири ва эҳтимолини ўлчашни таъминлайди.
- Рискларни баҳолаш босқичи такрорий жараён бўлиб, бу ҳимоя чораларини ўрнатишдан кейин ҳолат ўзгаришига асосланади.
- Рискларни баҳолашда риск қийматлари сон ва сифатга кўра баҳоланиши мумкин.

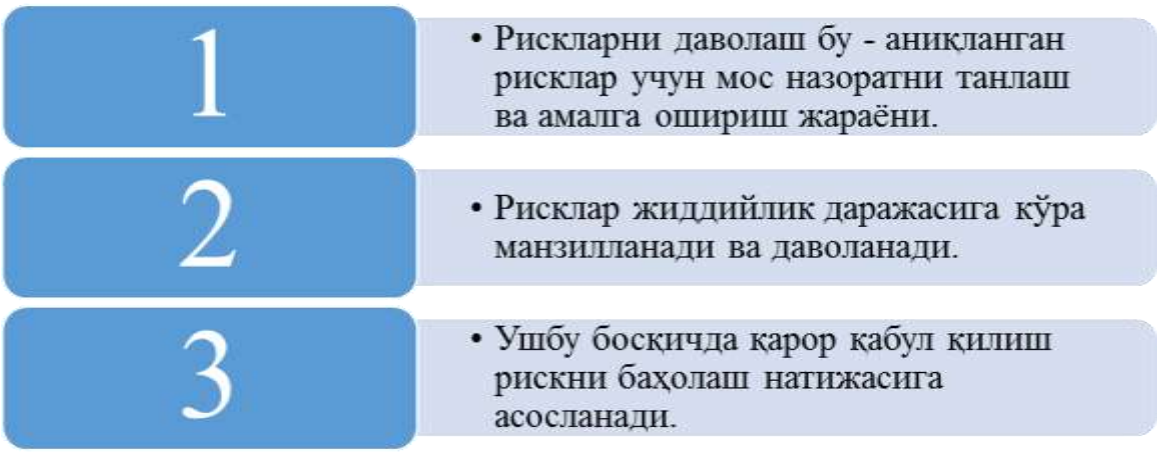
Рискни таҳлил қилиш

- Риск табийлигини аниқлайди;
- Рискни ошкор этиш сатҳини аниқлайди;
- Туғма ва назоратланган рискларни тушунишни таъминлайди.

Рискларни устуворлаштириш

- Рисклар устуворлаштирилади ва **жиддийлигига** қараб чоралар кўрилади;
- Рискларга жавоб беришни амалга оширишда **рискларни устуворлигига** эътибор қаратиш керак.

Рискни бошқариш: Рискни даволаш



Рискни бошқариш: Рискни даволаш босқичлари

Рискни камайтириш	Назоратлашни амалга ошириш орқали заифликларни бартараф этиш билан рискларни камайтириш.
Рискни трансфер қилиш	Рискни даволаш жавобгарлигини бошқа ташкилот ёки бўлимга трансфер қилиш.
Рискка қарши курашиш	Бевосита ёки танланган назоратни амалга ошириш орқали таҳдид ёки заифлик билан алоқадор рискларни камайтириш.
Рискни қабул қилиш	Рискларни бошқариш, трансфер қилиш ёки камайтириш ҳаракатлари тармоқдаги риск таъсиридан ошиб кетганда қабул қилинади.
Рискдан қочиш	Рискнинг сабаб ва оқибатини **камайтириш**
Рискни режалаштириш	Рискка қарши чоралар режаси, рискларни **устуворлаштириш**, **қарши чораларни** амалга ошириш орқали **рискларни бошқариш**.
Тақдиқот ва билимлар	Заифликларни тадқиқ қилиш ва уларни **бартараф этувчи** назоратни аниқлаш

Рискни бошқариш: Риск мониторинги ва кўриб чиқиш

Риск мониторинги

- Риск мониторинги **янги рискларни** пайдо бўлиш имкониятини аниқлайди.
- Риск мониторинги рискни тутувчи мос назорат усули **амалга оширилганлигини** кафолатлайди.
- Риск мониторинги шунингдек рискни эҳтимоли, таъсири, ҳолати ва ошкор бўлишини ўз ичига олади.

Рискни кўриб чиқиш

- Рискни кўриб чиқиш орқали амалга оширилган рискларни бошқариш стратегияси самарадорлиги **баҳоланади**.
- Риск баёни **топ рисклардан** огоҳ бўлишни бошқаришни кафолатлайди.

Амалий вазифалар:

1. Ўз компьютериздаги керакли маълумотларни юқотиш рискларини аниқланг.
2. Рискни таъсирини аниқланг.
3. Рискга қарши курашиш стратегиясини тузинг.

Адабиётлар ва интернет сайтлари:

1. Мазов Н.А., Ревнивых А.В., Федотов А.М. Классификация рисков информационной безопасности // Вестник НГУ. Серия: Информационные технологии. 2011. №2. URL: https://cyberleninka.ru/article/n/klassifikatsiya-riskov-informatsionnoy-bezopasnosti (дата обращения: 23.07.2020).
2. https://10guards.com/ru/articles/cyber-risks/
3. https://iqdecision.com/kiberbezopasnost-sovremennye-pravila-upravlenija-riskami/

2-амалий иш.
Идентификация, аутентификация ва авторизация
(2 соат)

Ишдан мақсад – киберхавфсизликни идентификация, аутентификация, авторизация ва рухсатларни назоратлаш этиш бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Назарий маълумот.

Тизим ресурсларини бошкариш билан боғлик бўлган хавфсизлик муаммоси учун *рухсатларни назоратлаш* терминини “соябон” сифатида фойдаланиш бўлади. Мазкур сохага оид тушунтиришларни олиб борганда 3 та асосий мухим бўлган соха мавжуд: *идентификация, аутентификация* ва *авторизация.*

Идентификация - шахсни кимдир деб даво қилиш жараёни. Масалан, сиз телефонда узингизни танитишингизни идентификациядан ўтиш деб айтиш мумкин. Бунда сиз узингизни, масалан, “Мен Шерзодман” деб танитасиз. Бу уринда “Боходир” сизнинг *идентификаторингиз* бўлиб хизмат қилади. Шундай қилиб, *идентификация* - субъект идентификаторини тизимга ёки талаб қилган субъектга тақдим этиш жараёни ҳисобланади. Бундан ташкари, электрон почта тизимида ҳам почта манзилни - *идентификатор* сифатида караш мумкин. Почта манзилини тақдим этиш жараёнини эса *идентификациялаш* жараёни сифатида караш мумкин. Электрон почта тизимида почта манзили такрорланмас ёки уникал бўлади. Шундан келиб чикиб айтиш мумкинки, фойдаланувчининг идентификатори тизим ичида уникал ва такрорланмасдир.

Аутентификация - фойдаланувчини (ёки бирор томонни) тизимдан фойдаланиш учун рухсати мавжудлигини аникдаш жараёни. Масалан, фойдаланувчини шахсий компьютердан фойдаланиш жараёнини олсак. Дастлаб киришда фойдаланувчи ўз идентификаторини (яъни, фойдаланувчи номини) киритади ва у орқали тизимга ўзини танитади (идентификация жараёнидан ўтади). Шундан сўнг, тизим фойдаланувчидан тақдим этилган идентификаторни хақиқийлигини текшириш учун паролни сурайди. Агар идентификаторга мос парол киритилса (яъни, аутентификациядан ўтса), фойдаланувчи компьютердан фойдаланиш имкониятига эга бўлади. Бошқа сўз билан айтганда, аутентификацияни фойдаланувчи ёки субъектни хақиқийлигини текшириш жараёни деб айтиш мумкин.

Аутентификациядан ўттандан сўнг фойдаланувчи тизим ресурсидан фойдаланиш имкониятига эга бўлади. Бирок, аутентификациядан ўтган фойдаланувчига тизимда ихтиёрий амалларда бажаришга рухсат берилмайди. Масалан, аутентификациядан ўтган имтиёзга эга фойдаланувчи учун дастурларни ўрнатиш имкониятини берилиши талаб этилсин. Хўш, аутентификациядан ўтган фойдаланувчига кандай қилиб рухсатларни чеклаш мумкин? Мазкур масалалар билан айнан, авторизация сохаси шугулланади.

Авторизация - идентификация, аутентификация жараёнларидан ўтган фойдаланувчи учун тизимда бажариши мумкин бўлган амалларга рухсат бериш жараёнидир.

Хавфсизлик сохасида терминлар стандартлаштирилган маъноларидан айри қўлланилади. Хусусан, рухсатларни назоратлаш кўп холларда авторизацияга

синоним сифатида ишлатилади. Бирок, мазкур курсда рухсатларни назоратлаш кенгроқ қаралади. Яъни, авторизация ва аутентификация жараёнлари рухсатларни назоратлашнинг қисмлари сифатида қаралади.

Юқорида келтирилган атамаларга берилган таърифларни умумлаштирган холда қуйидагича хулоса қилиш мумкин:

Идентификация - сиз кимсиз?

Аутентификация - сиз хакикатдан ҳам сизмисиз?

Авторизация - сизга буни бажаришга рухсат борми?

Аутентификация

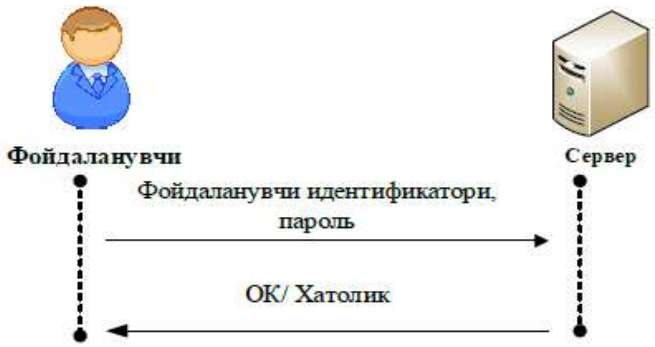
Аутентификацияда ёки идентификация жараёнларида субъектлар инсон кўринишида ёки қурилма (компьютер) кўринишида бўлиши мумкин. Яъни, инсон инсонни аутентификациядан ўтказиши мумкин, машина инсонни аутентификациядан ўтказиши мумкин ёки машина машинани аутентификациядан ўтказиши мумкин. Мазкур маърузада машина инсонни ёки машина машинани аутентификациядан ўтказиш сценарийларига асосий эътибор қаралади.

Машина инсонни қуйидаги “нарсалар” асосида аутентификациядан ўтказиши мумкин:

- *сиз билган бирор нарса (something you know);*
- *сизда мавжуд бирор нарса (something you have);*
- *сизнинг бирор нарсангиз (something you are).*

“Сиз билган бирор нарса” холатига парол мисол бўла олади. “Сизда мавжуд бирор нарса” холатига эса смарткарталар, токен, машинанинг пулти ёки калити мисол бўла олади. “Сизнинг бирор нарсангиз” холати одатда биометрик параметрларга синоним сифатида қаралади. Масалан, хозирда сиз ноутбук сотиб олиб, ундаги бармоқ изи сканери орқали аутентификациядан ўтишингиз мумкин.

Пароль - фақат фойдаланувчига маълум ва бирор тизимда аутентификация жараёнидан ўтишни таъминловчи бирор ахборот. Парол амалда аутентификация жараёнида кенг қўлланилувчи параметр ҳисобланади. Масалан, биз ўз шахсий компьютерларимиздан фойдаланиш хукукини олиш учун талаб этилган паролни киритишимиз талаб этилади. Мазкур холатни мобил телефонлар учун ҳам ишлатиш мумкин. Паролга асосланган холатдаги аутентификациялаш жараёнининг умумий кўриниши 1-расмда келтирилган.



1-расм. Паролга асосланган машина-инсонни аутентификациялаш жараёни

Паролга асосланган аутентификациялаш қуйидаги хусусиятларга эга:

- паролга асосланган аутентификацияни амалга ошириш қўлай (сарф харажати

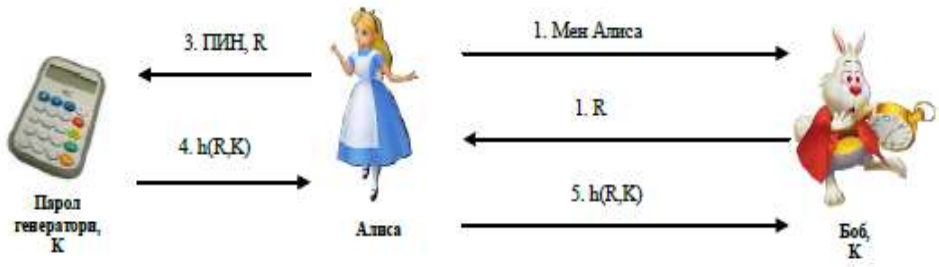
кам, алмаштириш осон);
- фойдаланувчи пароли одатда унга алокадор маълумот бўлади (масалан, унинг яхши кўрган футбол командаси, телефон раками ва хак.) ***(123456, 12345, дм>ег(у)*** ва шунинг учун "ҳужумчилар" томонидан аникланиши осон;
- мураккаб парольларни эсда саклаш мураккаб (масалан, ***}Де}(43}ЕттЬ+у);***
- паролга асосланган аутентификация усули амалда кенг қўлланилувчи усул.

Смарткарта ёки токен

Смарткарталар ёки қурилма кўринишидаги токенлар аутентификациялаш учун қўлланилади. *Смарткарта* - кредит карта ўлчамидаги қурилма бўлиб, кичик хажмдаги хотира ва ҳисоблаш имкониятига эга. Смарткарта одатда ўзида бирор махфий катталикни, калит ёки паролни, сақдайди ва хаттоки бирор ҳисоблашни амалга оширади. 2-расмда махсус мақсадли смарткарта ва уни ўқувчи қурилма (смарткарта ўқувчи курилма) акс эттирилган.

2-расм. Смарткарта ва смарткарта ўқувчи

Бирор нарса асосида аутентификациялаш усулларини турли кўринишларда амалга ошириш мумкин. Масалан, пароллар генераторини мисол қилиб олайлик. Пароллар генератори кичик қурилма бўлиб, тизимда киришда қўлланилади. Фараз қилайлик Алисада парол генератори мавжуд ва ундан фойдаланиб Бобдан аутентификациядан ўтмокчи. Бунинг учун Боб бирор тасодифий сон ***К*** ни ("саволни") Алисага юборади. Алиса қабул қилинган ***К*** сонини ва парол генераторидан фойдаланиш учун талаб қилинган ПИН ни парол генераторига киритади. Парол генератори эса Алисага жавобни тақдим этади ва у Бобга узатилади. Агар жавоб тўғри бўлса, Алиса аутентификациядан ўтади, акс холда ўта олмайди. Мазкур ценарийнинг умумий кўриниши 3-расмда келтирилган.



3-расм. Токенга асосланган аутентификация жараёни

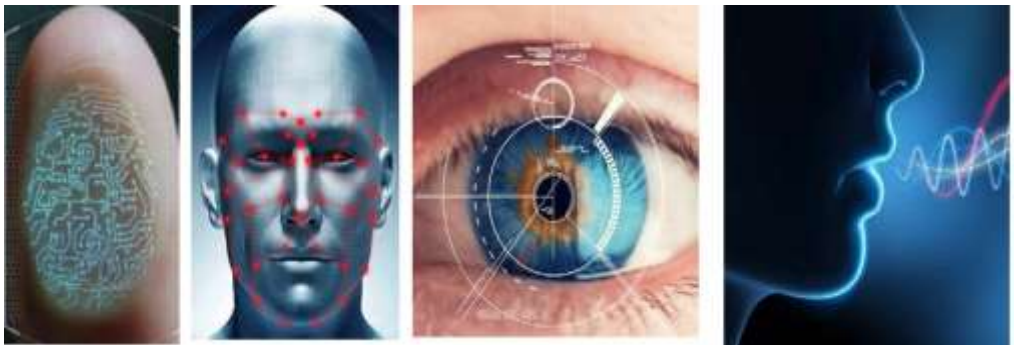
Келтирилган схемага кўра, Боб ва парол генераторида тақсимланган калит ***K*** бўлиши шарт. Ушбу схемада "савол-жавоб" механизми ишлатилган. Яъни, савол сифатида Боб Алисага ***R*** сонини узатади ва унга мос бўлган жавоб - ***h(R, K)*** ни қабул қилади. Қабул қилган маълумотни текшириш орқали Боб Алисани хақиқийлигини текширади.

Смартакарта ёки "сизда мавжуд бирор нарса" асосида аутентификация усуллари қуйидаги хусусиятларга эга:

- смарткартага асосланган аутентификацияда бирор нарасани эсда сакдашни талаб этилмайди;
- амалга ошириш ва қурилма нархи юқори (хусусан, токен йўқолган такдирда уни алмаштириш қимматга тушади);
- токен ёки смарткартани йўқотиб қўйиш муаммоси мавжуд;
- токен хавфсиз олиб юрилса юқори хавфсизлик даражасини таъминлайди.

Биометрик параметрларга асосланган аутентификация

Биометрик параметрга асосланган аутентификация усулида биометрик параметр инсоннинг узи учун калит сифатида хизмат қилади. Жуда ҳам кўплаб биометрик параметрлар мавжуд, масалан, бармоқ изи, юз тасвири, кўз қорачиги, овоз, харакат тарзи, қулок шакли, қўл шакли ва хак. Биометрик параметрларга асосланган аутентификация усули амалда кенг қўлланилади. Масалан, кўп қаватли уйларни кириш эшикларида ёки ташкилотларга киришда бармоқ изига асосланган аутентификация усули, ноутбукларда ва мобил телефонларда юз тасвирига асосланган ёки бармоқ изига асосланган аутентификациядан кенг қўлланилади (4-расм).



Бармоқ изи Юз тасвири Куз корачиги Овоз

4-расм. Биометрик наъмуналарга мисоллар

Ахборот хавфсизлиги сохасида биометрик параметрлар паролларга караганда юқори хавфсизликни таъминловчи алтернатив сифатида қаралади. Биометрик параметрларга асосланган аутентификация усули қуйидаги хусусиятларга эга:

- биометрик параметрга асосланган усул ўзида эсда сакдаш ва бирга олиб юриш заруриятини талаб этмайди;
- биометрик параметрга асосланган аутентификацияни амалга ошириш паролга асосланган усулдан қиммат ва токенга асосланган усулдан арзон ҳисобланади (баъзи, истисно холатлар мавжуд);
- биометрик парметрни алмаштириш имконияти мавжуд эмас, яъни, агар биометрик параметр қалбакилаштирилса, У холда аутентификация тизими шу

фойдаланувчи учун тўлиқ бузилган ҳисобланади;
- турли биометрик параметрларга асосланган аутентификация усуллари инсонлар томонидан турли даражада қабул қилинади.

Аутентификация сохасида фойдаланиш учун идеал биометрик параметр қуйидагиларни қаноатлантириши шарт:
- *универсал бўлиши* - биометрик параметр барча фойдаланувчиларда бўлиши шарт;
- *фарқли бўлиш* - танланган биометрик параметр барча инсонлар учун фарқ қилиши шарт;
- *ўзгармаслик* - танланган биометрик параметр вақт ўтиши билан ўзгармай қолиши шарт;
- *тўпланувчанлик* - физик хусусият осонлик билан тўпланувчи бўлиши шарт. Амалда физик хусусиятни тўпланувчанлиги, инсоннинг жараёнга эътибор беришига ҳам боғлик бўлади.

Биометрик параметр нафақат аутентификация масаласини ечишда балки, идентификациялашда ҳам кенг қўлланилади. Яъни, “Сиз кимсиз?” деган саволга жавоб бера олади. Масалан, БЫ да жиноятчиларга тегишли бармоқ излари базалари мавжуд. Ушбу базада бармоқ излари ***(бармоқ изи тасвири, фойдаланувчи номи)*** шаклида сакданади ва бу орқали бирор инсонни жиноятчилар рўйхатида бор йўқлигини текшира олади. Бунинг учун, текширилувчи инсондан бармоқ изи тасвири олинади ва у РВ1 базасида мавжуд бўлса, у холда *текширилувчи инсоннинг номи* ***бармоқ изи тасвири****га* мос ***фойдаланувчи номи*** билан бир хил бўлади.

Бир томонлама ва икки томонлама аутентификация

Агар томонлардан бири иккинчисини аутентификациядан ўтказса, *бир томонлама аутентификация* деб аталади. Агар хар иккала томон бир-бирини аутентификациядан ўтказса, у холда *икки томонлама аутентификация* деб аталади. Масалан, электрон почтадан фойдаланиш давомида фақат сервер фойдаланувчини хақиқийлигини текширади (парол орқали) ва шу сабабли уни *бир томонлама аутентификациялаш* деб аташ мумкин. Электрон тўловларни амалга оширишда эса ҳам сервер фойдаланувчини аутентификациядан ўтказади ҳам фойдаланувчи серверни аутентификациядан ўтказади. Шунинг учун мазкур холатни *икки томонлама аутентификациялаш* деб айтиш мумкин.

Кўп факторли аутентификация

Юқорида келтирилган барча аутентификация сценарийларида фақат битта омил учун хақиқийликни текшириш амалга оширилди. Масалан, почтада киришда фақат паролни билсангиз сиз аутентификациядан ўта оласиз ёки киришда бармоқ изини тўғри киритсангиз, эшик очилади. Яъни, сервер фақат фойдаланувчидан паролни ёки бармоқ изини тўғри бўлишини истаяпти. Мазкур кўринишдаги аутентификация - *бир факторли аутентификация* деб аталади. Бир факторли аутентификацияда текшириш фақат битта фактор бўйича (масалан, парол) амалга оширилади.

Бирок, бир факторли аутентификациялашни амалда жорий қилиш натижасида юқори хавфсизликни таъминлаш мумкин эмас. Масалан, овозга асосланган аутентификация тизимини олайлик. Агар ҳужумчи фойдаланувчини овозини диктафонга ёзиб олиб, уни аутентификациядаш ўтиш жараёнида тақдим этса, осонлик билан аутентификация тизимини алдаб ўтиши мумкин. Сабаби, фақат

битта фактор (овоз) бўйича текшириш амалга оширилмокда. Шунга ўхшаш холатни паролга асосланган ёки токенга асосланган аутентификация жараёнида хам кузатиш мумкин.

Мазкур муаммони бартараф этиш учун, биринчи факторга кўшимча қилиб, яна бошка факторлардан фойдаланиш мумкин. Масалан, овозга асосланган аутентификациялашда кўшимча қилиб паролдан фойдаланиш мумкин. Яъни, фойдаланувчи дастлаб тизимга ўз овози орқали аутентификациядан ўтади ва удан сўнг парол бўйича аутентификациядан ўтказилади. Хар иккала босқичда ҳам аутентификациядан муваффақиятли ўтилганда, фойдаланувчи тизимдан фойдаланиш имкониятига эга бўлади. Кўп факторли аутентификациялашдан фойдаланишда хаётимизда хам кўплаб мисоллар келтириш мумкин. Масалан, пластик картадан тўловни амалга оширишда. Пластик картадан тўловни амалга оширишдаги аутентификация жараёни ўзида *“сизда мавжуд бирор нарса”* ва “*сиз билган бирор нарса”* усулларини бирлаштирган. Яъни, дастлаб фойдаланувчида пластик картани ўзини бор бўлишини талаб этади ва иккинчидан уни ПИН кодини билишни талаб этади. Шу сабабли, ушбу усулни *кўп факторли аутентификациялаш* деб айтиш мумкин.

Кўп факторли аутентификация усули факторлардан биттаси қалбакилаштирилган такдирда хам аутентификация жараёнини бузилмаслигига олиб келади.

Аутентификация усулларига қаратилган ҳужумлар

Мавжуд аутентификация усулларини бузишда кўплаб ҳужум усулларидан фойдаланилади. Ушбу ҳужум усулларини аутентификация усулларига мос равишда қуйидагича тавсифлаш мумкин:

1. **Сиз билган бирор нарса.** Аутентификациялашнинг мазкур усулини бузиш учун қуйидаги ҳужум усулларидан фойдаланилади:

a. **Пароллар луғатидан фойдаланишга асосланган ҳужум.** Бунга кўра статистика бўйича энг кўп қўлланилувчи пароллар ёрдамида аутентификациядан ўтишга харакат қилинади.

b. **Паролларни барча вариантларини кўриб чикиш.** Ушбу усулда паролнинг бўлиши мумкин бўлган барча вариантлари генерация қилинади ва улар текшириб кўрилади.

c. **“Элка орқали караш” ҳужуми.** Ушбу ҳужум фойдаланувчи паролни киритиш жараёнида ёнида туриб қараб туриш орқали билиб олишни мақсад қилади.

d. **Зарарли дастурлар асосида ҳужум.** Шундай махсус дастурий воситалар мавжудки улар фойдаланувчи компьютерида ўрнатилиб, клавиатура орқали киритилган барча маълумотларни серверига узатади.

2. **Сизда мавжуд бирор нарса.** Аутентификациянинг мазкур усулини бузиш учун қуйидаги ҳужум усулларидан фойдаланилади:

a. **Физик ўғирлаш.** Ҳужумнинг мазкур тури токенни ёки смарт картани ўғирлашни мақсад қилади. Мазкур ҳужум бу тоифдаги аутентификация учун энг хавфли ҳужум ҳисобланади.

b. **Дастурий кўринишдаги токенларнинг зарарли дастурларга бардошсизлиги.** Баъзи токенлар дастурий кўринишда бўлиб, мобил қурилмаларда ишлайди ва шу сабабли зарарли дастур томонидан бошқарилиши мумкин.

3. **Сизнинг бирор нарсангиз.** Аутентификациянинг мазкур усулини бузиш учун қуйидаги ҳужум усулларидан фойдаланилади:

a. **Қалбакилаштириш.** Ҳужумнинг мазкур тури биометрик параметрни қалбакилаштиришни мақсад қилади. Масалан, юзлари ўхшаш бўлган Хасан ўрнига Хусан аутентификациядан ўтиши ёки сифати юқори бўлган фойдаланувчи юз тасвири мавжуд расм билан тизимни алдашни мисол қилиш мумкин.

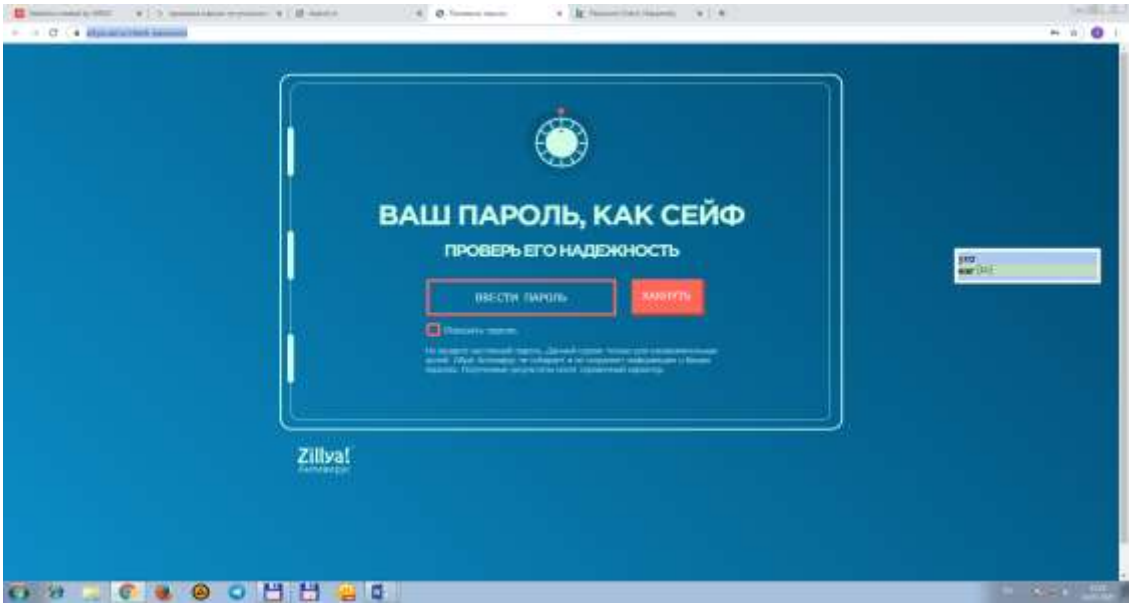
b. **Маълумотлар базасидаги биометрик параметрларни алмаштириш.** Ушбу ҳужум бевосита фойдаланувчиларни биометрик параметрлари (масалан, бармоқ изи тасвири, юз тасвири ва хак) сакданган базага қарши амалга оширилади. Яъни, танланган фойдаланувчини биометрик параметрлари ҳужумчини биометрик параметрлари билан алмаштирилади.

Аутентификация усулларига қаратилган ҳужумларии олдини олиш учун хар битта усулда ўзига хос қарши чоралари мавжуд. Умумий холда мазкур ҳужумларни олдини олиш учун қуйидаги химоя усуллари ва хавфсизлик чоралари тавсия этилади:

1. ***Мураккаб пароллардан фойдаланиш.*** Айнан ушбу усул паролни барча вариантларини текшириб кўриш ва луғатга асосланган ҳужумларни олдини олишга катта ёрдам беради.
2. ***Кўп факторли аутентификациядан фойдаланиш.*** Мазкур усул юкорида келтирилган барча муаммоларни бартараф этишда катта амалий ёрдам беради.
3. ***Токенларни хавфсиз сақлаш.*** Ушбу тавсия бирор нарсага эгалик қилишга асосланган аутентификация усулидаги мавжуд муаммоларни олдини олиш учун самарали ҳисобланади.
4. ***Тирикликка текширишдан фойдаланиш.*** Ушбу усул биометрик параметрларга асосланган аутентификациялаш усулларида тасвир орқали алдаб ўтиш ҳужумини олдини олиш учун самарали ҳисобланади.

Амалий бажариш учун вазифалар:

1. Идентификация, аутентификация ва авторизация тушунчаларига синквейн ёзинг.
2. Идентификация, аутентификация ва авторизация тушунчаларини Венн диаграммаси асосида таққосланг.
3. Паролни танлаш бўйича 10 та тавсия беринг.
4. Қўйидаги сайт асосида ўзингизни паролизни текширинг.
   https://zillya.ua/ru/check-password



5. Агарда пароллиз онсон бўлса, янги “яхши” паролни ўйлаб топиб, сайт асосида текширинг.

Адабиётлар ва интернет сайтлари:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357
2. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. 2017 г. 338 стр.
4. Мельников В. Информационная безопасность Учебник. Издательство: КноРус. Год издания: 2018
5. Как проверить пароль на безопасность. https://habr.com/ru/post/21822/
6. https://zillya.ua/ru/check-password
7. https://password.kaspersky.com/ru/

3-амалий машғулот. Маълумотлар ва ахборотни тикланиши ва барқарорлиги (2 соат)

Ишдан мақсад – киберхавфсизликда маълумотлар ва ахборотни тикланиш ва барқарорлиги таъминлаш бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Амалий вазифалар.

1. Киберхавфсизликда маълумотлар ва ахборотни тикланиш ва барқарорлиги таъминлаш бўйича тавсиялар билан танишинг. Маълумотларни тикланиш дастурини топиб, флешкадаги маълумотларни ўчириб, тикланг.

Захира нусхалаш

Ҳозирги кунда маълумотларни йўқолиши ташкилотлар учун асосий хавфсизлик муаммолардан биридир. Маълумотни йўқолиши натижасида ташкилот катта зарар кўриши мумкин. Шунинг учун ташкилотдан давомий равишда муҳим бўлган маълумотлар захира нусхалаб борилиши шарт.

Маълумотларни захира нусхалаш бу–муҳим бўлган ахборот нусхалаш ёкисақлаш жараёни бўлиб, бу маълумот йўқолган вақтда қайта тиклаш имкониятини беради.

Маълумотларни захира нусхалаш асосан қуйидаги икки мақсадда фойдаланилади:

- Зарар етказилгандан кейин тизимни нормалиш ҳолатига қайтариш учун.
- Тизимда сақланувчи муҳим маълумотни йўқолишидан сўнг уни қайта тиклаш учун.

Маълумотларни йуколиш сабаблари

Инсон хатоси

- қасддан ёки тасодифий маълумотни ўчириб юборилиши, маълумотларни сақлаш воситасини тўғри жойлаштирилмагани ёки маълумотлар базасини хатолик билан бошқарилганлиги.

Ғаразли ҳатти ҳаракатлар

- ташкилотдаги муҳим маълумотларни модификацияланиши ёки ўғирланиши

Табий сабаблар

- қувват ўчиши, дастурий таъминот тўсатдан ўзгариши ёки қурилмани тўсатдан зарарланиши

Табий офатлар

- зилзила, ёнғин ва ҳак

Захира нусхалаш имкониятлари

Муҳим бўлган маълумотлардан йўқолган ва зарарланган тақдирда ҳам фойдаланилиш мумкинлиги

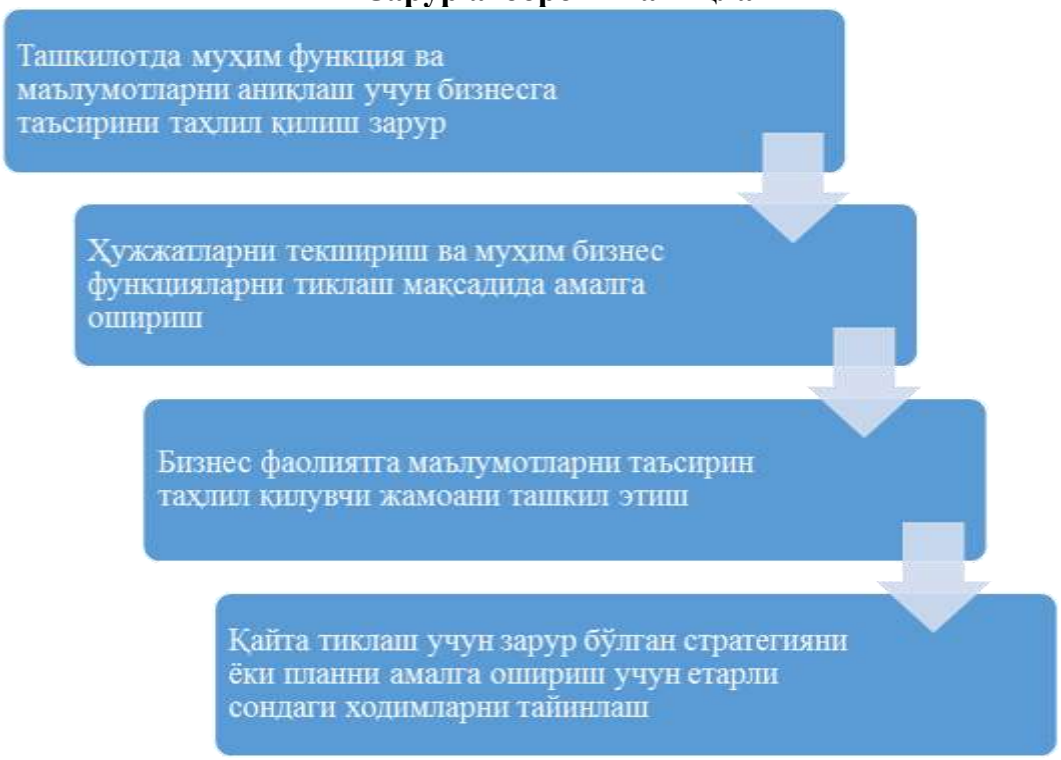
Захира нусхалаш ташкилотларни ўз вазифасини йўқотишидан ҳимоялайди. Маълумотларини ихтиёрий вақтда тиклаш имкониятини беради.

Маълумотларни тиклаш ташкилотдаги йўқолган маълумотларни тиклаш имкониятини беради

Захира нусхалаш стратегияси режаси

Маълумотларни захира нусхалашнинг идеал стратегияси тўғри маълумотни танлашдан бошлаб кафолатли маълумотни тиклаш жараёнигача бўлган босқичларни ўз ичига олади.

Зарур ахборотни аниқлаш



Захира нусхаларни сақловчи воситалар

Оптик дисклар (DVD, Blu-ray)

- ~200 Гбайтгача
- Олиб юриш ва сақлаш учун осон
- Ёзиш секин, катта ҳажмдаги маълумотларни сақлай олмайди

Кўчма қаттиқ дисклар/ USB хотиралар

- Чекланмаган ҳажм
- юқори сақлаш имконията ва юқори тезликка эга
- нархи қиммат ва катта захира маълумотлари учун кам тавсия этилади

Лентали дисклар

- Чекланмаган ҳажм
- Сақлаш ва олиб юриш учун қулай бўлиб, фойдаланувчи иштирокини талаб этмайди
- Оддий фойдаланувчилар учун қимматлиги ва оддий компьютерлар улардан фойдаланиш учун қўшимча аппарат ва дастурий воситани талаб қилади.

Захира нусхалаш манзилини танлаш

Ички (onsite) захиралаш

- Ички захирилашда ташқи қурилмалар, лентали сақлагичлар, DVD, қаттиқ диск ва ҳаклардан фойдаланилади.
- **Афзалликлари:**
- Маълумотдан задлик билан фойдаланишни таъминлайди;
- Кам харажатлик;
- Захира нусхалашда зарур бўлган қурилмаларни топиш осон ва нархи паст;
- Тиклашдаги тезкорлик;
- Интернетдан фойдаланиш талаб этилмайди.
- **Камчилиги:**
- Захирилашни амалга оширишда инсон иштирокини талаб этади.
- Табиф офатларга ёки ўғирлашга мойил.

Ташқи (offsite) захиралаш

• Ташқи захиралашда захиралаш масофадаги манзилда амалга оширилади.Бу физик дискларга сақлаш, онлайн ёки учинчи томон хизмати асосида амалга оширилиши мумкин.

• **Афзалликлари:**

• Ташқи захиралашни турли манзилларда ва кўплаб нусхаларда амалга ошириш мумкин;

• Захирилаш жараёни автоматлашгани боис инсон хатосини кам.

• Маълумотни сақлаш ҳажми чекланмаган.

• **Камчилиги:**

• Қиммат ва учинчи томон хизматини талаб этади.

• Интернет тармоғига уланишни талаб этади ва тармоқ трафигини банд қилиши мумкин.

• Жараён узоқ вақт олади.

Булутли тизимда захиралаш

• Ушбу захиралаш усули онлайн усул деб ҳам аталади.У захираланган маълумотларни очиқ тармоқда ёки маълум серверда сақлайди. Одатда маълум сервер вазифасини учинчи томон хизмати ташкил қилади.

• **Афзалликлари:**

• Дискка асосланган захиралаш, виртуаллаштириш ва шифрлаш каби технологиялардан фойдалангани боис ушбу захира усули самарали ҳисобланади.

• Маълумотларни мониторинг қилиш ва ташкилот учун ҳисоботлар бериш имконияти мавжуд.

• Булутли сақланган захира сақланган маълумотларни Интернет орқали бошқариш осон.

• **Камчилиги:**

• Маълумотни тиклаш кўп вақт талаб қилади.

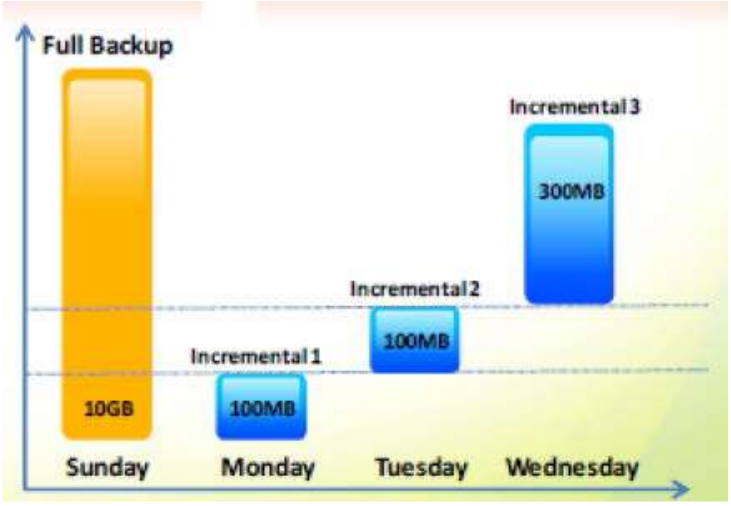
• Захира нусхалашни амалга оширган учинчи томон ҳар доим ҳам тўлиқ маълумотни захиралаш амалга оширилганини кафолатламайди.

Захиралаш турлари

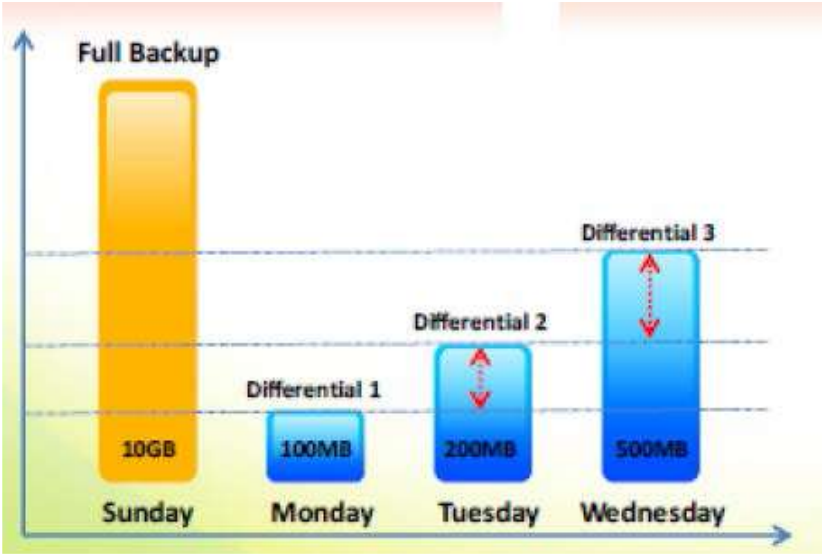
Тўлиқ захиралаш	Ўсиб борувчи захиралаш	Дифференциал захиралаш
• Тўлиқ захиралаш усули тиклашнинг тезлиги юқори. • Захира нусхалаш жараёнининг секин ва маълумотни сақлаш учун кўп ҳажм талаб этади.	• Захираланган маълумотга нисбатан ўзгариш юз берганда захирилаш амалга оширилади. • Охирги захира нусхалаш сифатида ихтиёрий захиралаш усули бўлиши мумкин (тўлиқ сахиралашдан). • Сақлаш учун кам ҳажм ва амалга ошириш жараёни тез. • Бироқ, тиклаш жараёни секин.	•Тўлиқ ва ўсиб борувчи усулларнинг мужассамлашган кўриниши бўлиб, охирги захираланган нусхадан бошлаб бўлган ўзгаришларни захира нусхалаб боради. •Амалга ошириш тўлиқ захиралашга қараганда тез амалга оширилади. •Қайта тиклаш ўсиб борувчи захиралашга қараганда тез амалгаоширилади. •Маълумотни сақлаш учун тўлиқ захиралашга қараганда кам жой талаб этади. •Бироқ, ўсиб борувчи захиралашга қараганда секинзахиралаш амалга оширилади ва маълумотни тиклаш тўлиқ захирилашга қараганда секинамалга оширилади

Мисол

- **Ортиб борувчи.** Фараз қилинсин захира нусхалаш жадвалига кўра тўлиқ захиралаш Якшанба кунига, ортиб борувчи захиралаш эса Сешанбадан Шанбагача қўйилган бўлсин. Якшанба куни тўлиқ захиралаш амалша оширилганидан сўнг, Душанба кунидаги ўзгаришлар Сешанба куни ўсиб борувчи усул асосида амалга оширилади. Ушбу жараёни Шанбагача давом эттирилади.



- **Дифференциал.** Тўлиқ захирилаш Якшанба куни ва дифференциал нусхалаш Шанбагача ишлаши жадвалда келтирилган. Якшанба куни тўлиқ захира нусхалаш амалга оширилганидан сўнг, душанба куни дифференциал захиралаш пайдо бўлади ва кун ўтиши билан амалга оширилади. Бу ҳолат ўсиб борувчи захирилашга ўхшаб кетади. Бироқ, Сешанбада, захира нусхалар Якшанба ва Душанбадаги ўзгаришлар учун амалга оширилади. Кейин, Чоршанбада захиралаш Якшанба, Душанба ва Сешанба кунлари учун амалга оширилади.



2. Захира нусхалаш стратегиясини яратинг.

Адабиётлар ва интернет сайтлари:

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. 2017 г. 338 стр.
3. Мельников В. Информационная безопасность Учебник. Издательство: КноРус. Год издания: 2018
4. Лучшие программы для восстановления данных. https://remontka.pro/recover/
5. Программы для восстановлкния удаленных файлов. https://softcatalog.info/ru/obzor/programmy-dlya-vosstanovleniya-udalennyh-faylov

4-амалий иш. Тармоқ ҳужумлари, web-ҳужумлар, дастурий ҳужумлар

Ишдан мақсад – тармоқ ҳужумлари, web-ҳужумлар, дастурий ҳужумлар бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Назарий маълумот.

Таҳдид бу – натижаси ташкилотнинг амалларига ва функционал ҳаракатларига зарар келтирувчи ва уларни узиб қўйувчи ошкор бўлмаган ҳодисаларнинг потенциал пайдо бўлишидир. Таҳдидлар ташкилотнинг бутунлик ва фойдаланувчанлик факторларига таъсир қилиши мумкин. Таҳдиднинг таъсири жуда юқори ва у ташкилотдаги физик АТ активларининг мавжудлигига таъсир қила олади. Таҳдидларнинг пайдо бўлиши тасодифий, қасддан ёки бошқа ҳаракатнинг таъсирида бўлиши мумкин.

Заифлик бу – “портлаганида” тизим хавфсизлигини бузувчи кутилмаган ва ошкор бўлмаган ҳодисаларга олиб келувчи камчилик, лойиҳалашдаги ёки амалга оширишдаги хатолик. Оддий сўз билан айтганда, заифлик хавфсизлик бўшлиғи бўлиб, турли фойдаланувчиларни аутентификациялаш усулларини айланиб ўтиб ҳужумчига тизимга кириш имкониятини тақдим этади.

Ҳужум бу – заифлик орқали АТ тизими хавфсизлигини бузиш томон амалга оширилган ҳаракат. Бунда шунингдек зарарли дастурларни ва буйруқларни юбориш орқали қонуний дастурий ва аппарат воситадан фойдаланиш имкониятини қўлга киритишга ҳаракат қилинади.

Тармоқ хавфсизлиги муаммолари

Тармоқдан фойдаланиб амалга оширилувчи ҳужумлар сони ва кўринишлари жуда ҳам жадаллик билан ортиб бормоқда. Доимий ҳужумлар бутун ҳисоблаш қурилмалари дунёси учун асосий муаммодир. Шунинг учун ташкилотлар тармоқ хавфсизлигини таъминлаш учун катта харажатларни сарфлашмоқда. Тармоқ хавфсизлиги муаммолари ташкилотдаги мавжуд ахборотнинг фойдаланувчанлиги, конфиденциаллиги ва бутунлигини таъсир қилади. Ҳужумчилар технологияга тегишли хавфсизликда мавжуд бўшлиқларни аниқлашга ҳаракат қилишмоқда. Ўз навбатида бу тизим администраторида тармоқда пайдо бўлувчи янги ҳужумлар ҳақида маълумотга эга бўлиб бориши талаб этилади.

Тармоқни қуриш осон вазифа ҳисобланиб, унинг хавфсизлигини таъминлаш мураккаб вазифа ҳисобланади. Сабаби, ҳужумчи турли воситалардан фойдаланган ҳолда тизимдаги заифликларни аниқлашга ҳаракат қилади.

Ташкилот тармоғи ичкаридан амалга оширилувчи турли ҳужумларга ҳам учраши мумкин. Ичкаридан туриб амалга оширилган ҳужум одатда ташқи ҳужумдан хавфлироқ бўлади.

Шунинг учун ташкилот кунлик тармоқдаги ҳужумларни мониторинг қилиб бориши ва аниқлаб бориши каби муҳим вазифани амалга оширишга мажбур.

Нима учун тармоқ хавфсизлиги муаммолари ортиб бормоқда

Ҳозирда тармоқ орқали аммалга оширилувчи муаммоларнинг ортишига қуйидаги омиллар таъсир қилмоқда:

Қурилма ёки дастурий воситани нотўғри созланиши. Хавфсизлик бўшлиқлари одатда тармоқдаги қурилма ёки дастурий воситаларнинг нотўғри

созлангани боис вужудга келади. Масалан, нотўғри созланган ёки шифрлаш мавжуд бўлмаган протоколдан фойдаланиш тармоқ орқали юборилувчи махфий маълумотни ошкор бўлиши сабабчи бўлади. Нотўғри созланган қурилма ҳужумчига тизим ёки тармоқдан фойдаланиш имкониятини тақдим этиши мумкин. Нотўғри созланган дастурий восита эса илова ёки дастурий таъминдан рухсатсиз фойдалданиш имконини бериши мумкин.

Тармоқни хавфсиз бўлмаган тарзда ва заиф лойиҳалаш. Нотўғри ва хавфсиз бўлмаган ҳолда лойиҳаланган тармоқ турли таҳдидларга ва маълумотни йўқотилиши эҳтимолига дуч келиши мумкин. Масалан, агар тармоқлараро экран, IDS ва виртуал шахсий тармоқ (VPN) технологиялари хавфсиз тарзда амалга оширилмаган бўлса, улар тармоқни турли таҳдидлар учун заиф қилиб қўйиши мумкин.

Туғма технология заифлиги. Агар қурилма ёки дастурий восита маълум турдаги тармоқ ҳужумларини бартараф эта олмаса, у ҳолда у ушбу ҳужумларни заиф бўлади. Кўплаб қурилмалар, иловалар ёки веб браузерлар *хизматдан вос кечишга ундаш* ҳужуми ёки *ўртага турган одам* ҳужумларига бардошсиз бўлади. Агар тизимларда эски веб браузер фойдаланилса, ушбу тизимлар тақсимланган ҳужумларга кўпроқ бардошсиз бўлади. Агар тизимлар янгиланмаса, кичик троян ҳужуми фойдаланувчи машинасини тозалаб ташлаш учун етарли бўлиши мумкин.

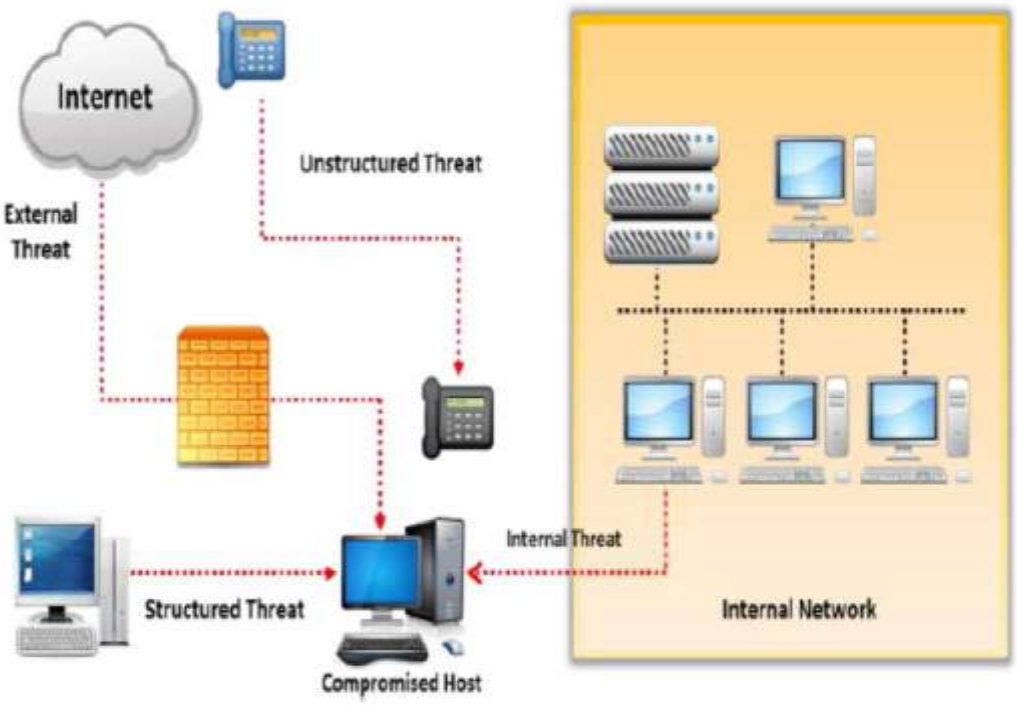
Фойдаланувчиларнинг эътиборсизлиги. Энг охирги тармоқ фойдаланувчиларининг эътиборсизлиги тармоқ хавфсизлигига жиддий таъсир қилиши мумкин. Инсон ҳаракатлари натижасида маълумотни йўқолиши, чиқиб кетиши каби жиддий хавфсизлик муаммолари бўлиши мумкин. Бундан ташқари ҳужумчилар фойдаланувчилар ҳақида маълумотларни тўплашда социал инжинерия технологияларидан фойдаланадилар.

Фойдаланувчиларни қасддан қилган ҳаракатлари. Ишдан бўшаб кетган ходим тақсимланган дискдан ҳалигача фойдаланиш имкониятига эга бўлиши мумкин. У мазкур ҳолда ташкилот махфий ахборотини чиқиб кетишига сабабчи бўлади. Бу ҳолат фойдаланувчиларни қасддан қилган ҳаракатлари сифатида қаралади.

Тармоқ хавфсизлигига таҳдидларнинг турлари

Тармоққа қаратилган таҳдидлар одатда икки турга ажратилади (1-расм):

- ички таҳдидлар;
- ташқи таҳдидлар.



1-расм. Турли тармоққа қаратилган таҳдидлар

Ички таҳдидлар. Компьютер ёки интернетга алоқадор жиноятчиликларнинг 80% ини ички ҳужумлар ташкил этади. Бу ҳужумлар ташкилот ичидан туриб, хафа бўлган ходимлар, ғараз ниятли ходимлар томонидан амалга оширилиши мумкин. Ушбу ҳужумларнинг аксарияти имтиёзга эга тармоқ фойдаланувчилари томонидан амалга оширилади.

Ички ҳужумлар ташқи ҳужумларга қараганда жиддий хавф туғдириши мумкин. Бунинг асосий сабаби ички ҳужумни амалга оширувчи тармоқнинг тушилиши, хавфсизлик сиёсати ва ташкилот қонунчилиги билан яқиндан таниш бўлади.

Ташқи таҳдидлар. Ташқи ҳужумлар тармоқда аллақачон мавжуд бўлган заифлик натижасида амалга оширилади. Ҳужумчи шунчаки қизиқишга, моддий фойда ёки ташкилотни обрўсини тушириш учун ушбу ҳужумларни амалга ошириши мумкин. Мазкур ҳолда ҳужумчи юқори малакали ва гуруҳ бўлиб ишлашлари мумкин. Ҳужумни амалга оширганда махсус технологиялардан фойдаланилади ва узоқ муддат давомида тайёрганлик кўрилади. Мазкур ҳолда ҳужумлар ички ходимларнинг ёрдамисиз амалга оширилади. Баъзи ташқи ҳужумлар ўзида иштирокчиларни ва вирусга асосланган ҳужумларни, паролга қаратилган ҳужумларни, зарарли хабарни киритишга асосланган ҳужумларни ва операцион тизимга асосланган ҳужумларни ўз ичига олади.

Ташқи таҳдидлар одатда икки турга ажратилади: тизимлашган ва тизимлашмаган ташқи таҳдидлар.

Тизимлашган ташқи таҳдид. Тизимлашган ташқи таҳдидлар юқори малакали шахслар томонидан амалга оширилади. Ушбу шахслар тармоқдаги мавжуд заифликни тезкорлик билан аниқлаш ва ундан ўз мақсадлари йўлида фойдаланишлари учун ундан фойдаланиш имкониятига эга бўладилар. Ушбу шахслар ёки шахслар гуруҳлари одатда катта кибержиноятчиликларни амалга оширишга жалб этиладилар.

Тизимлашмаган ташқи таҳдиди. Тизимлашмаган ташқи таҳдидлар одатда

малакали бўлмаган шахслар томонидан турли тайёр бузиш воситалари ва скриптлар ёрдамида амалга оширилади. Ушбу ҳужум турлари одатда шахс томонидан ўз имкониятини тестлаш учун ёки ташкилотга заифлик мавжудлигини текшириш учун амалга оширилади.

Тармоқ хавфсизлиги заифликларининг турлари

Тармоқ хавфсизлигидаги бузилишлар қуйидаги заифликлар натижасида юзага келади:

Технологик заифликлар. Технологик заифликлар операцион тизим, принтерлар, сканнерлар ва бошқа тармоқ қурилмаларидаги камчиликларнинг натижасида юзага келади. Ҳужумчилар протоколлардаги, масалан, SMTP, FTP ва ICMP, бўшлиқларни аниқлашлари мумкин. Бундан ташқари, тармоқ қурилмалари, свитч ёки роутерлардаги аутентификация усулларининг етарлича бардошли бўлмаслиги натижасида ҳужумлар амалга оширилади. Буни олдини олиш учун, тармоқ администратори томонидан доимий хавфсизлик аудити олиб борилиши талаб этилади.

Созланишдаги заифликлар. Созланишдаги заифликлар тармоқ ёки ҳисоблаш қурилмаларини нотўғри созланиши натижасида юзага келади. Агар тармоқ администратори фойдаланувчи аккаунтини ва тизим хизматларини хавфсиз бўлмаган тарзда созланиши, жорий созланиш ҳолатида қолдириш, паролларни нотўғри бошқарилиши, натижасида заифликлар юзага келади.

Хавфсизлик сиёсатидаги заифлик. Хавфсизлик сиёсатидаги заифликни юзага келишига ташкилотнинг хавфсизлик сиёсатида қоидалар ва қарши чораларни нотўғри ишлаб чиқилгани сабаб бўлади. Ушбу сабаблар тармоқ ресурсларидан рухсатсиз фойдаланиш имкониятини тақдим этиши мумкин. Агар тармоқ администратори ҳаракатларни доимий аудит, мониторинг қилиб борса, ушбу заифликларни аниқлаш ва ўз вақтида бартараф этиш имконига эга бўлади.

Тармоқ хавфсизлигига қаратилган ҳужумларнинг турлари

Тармоққа қаратилган ҳужумларни кун сайин ортиб бориши натижасида ташкилотлар ўз тармоқларида хавфсизликни таъминлашда қийинчиликларга дуч келишмоқда. Ҳужумчилар ёи хакерлар тармоққа киришни янгидан янги усулларини топишмоқда. Ҳар бир ҳужумчиларнинг мотивлари уларнинг мақсадларига кўра турлича бўлиши мумкин. Масалан, баъзи ҳужумчилар қурилмани ёки дастурий воситани ўғирлашни мақсад қилса, баъзилари тармоқ ресурсларидан ва фойдаланувчи маълумотларини қўлга киритишни ёки бошқаришни мақсад қилади. Бошқа томондан тармоқ администратори эса ушбу ҳужумларни аниқлаш учун аларни тури ҳақида етарлича билимларга эга бўлиши талаб этилади. Тармоқ ҳужумлари одатда қуйидагича таснифланади:

Разведка ҳужумлари. Разведка ҳужумлари асосий ҳужумларни осон амалга ошириш учун ташкилот ва тармоқ ҳақидаги ахборотни тўплашни мақсад қилади. Тармоқ ҳақида ахборотни тўплаш ҳужумчиларга мавжуд бўлган потенциал заифликни аниқлаш имконини беради.

Кириш ҳужумлари. Мўлжалдаги тармоқ ҳақида етарлича ахборот тўпланганидан сўнг, ҳужумчи турли технологиялардан фойдаланган ҳолда тармоққа киришга ҳаракат қилади. Яъни, тизим ёки тармоқни бошқаришга ҳаракат қиладилар. Бу турдаги ҳужумлар кириш ҳужумлари деб аталади ва рухсатсиз фойдаланиш, кўпол куч ҳужуми, имтиёзни орттириш, ўртага турган одам ҳужуми

ва ҳак.ларни ўз ичига олади.

Хизматдан воз кечишга ундаш (Denial of service, DOS) ҳужумлари. Хизматдан вос кечишга қаратилган ҳужумларда, ҳужумчи мижозларга, фойдаланувчиларга ва ташкилотларда мавжуд бўлган бирор хизматни чеклашга уринади. DOS ҳужумлари бирор ахборотни ўғирланишига ёки йўқолишига олиб келмасада, бироқ ташкилот функциясини бажарилмаслигига олиб келади. DOS ҳужумлар тизимда сақланган файллар ва бошқа махфий маълумотларга таъсир қилиши мумкин, шунингдек веб сайтнинг ишлашига ҳам. Ушбу ҳужум усули билан веб сайт фаолиятини тўхтатиб қўйиш мумкин.

Зарарли ҳужумлар. Зарарли ҳужумлар тизим ёки тармоққа бевосита ва билвосита таъсир қилади. Ушбу ҳужумлар тармоқ вазифасига зарарли тасир қилади. Зарарли дастур бу – программа ёки файл бўлиб, компьютер тизимига таҳдид қилиш имкониятига эга. Зарарли дастурлар троянлар, вируслар ва “қурт”лар кўринишида бўлиши мумкин.

Разведка ҳужумлари

Разведка ҳужумларида, ҳужумчилар мақсад қаратилган тармоқ ҳақида барча бўлиши мумкин бўлган ахборотни, хусусан, тизим, тармоқ ва тармоқда мавжуд заифликлар ҳақидаги ахборотни кўлга киритиши мумкин.

Разведка ҳужумининг асосий мақсад қилиб қуйидаги тоифага тегишли маълумотларни йиғиш олинади:

- тармоқ ҳақидаги ахборот;
- тизим ҳақидаги ахборот;
- ташкилот ҳақидаги ахборот.

Разведка ҳужумларининг қуйидаги турлари мавжуд:

- *Актив разведка ҳужумлари.* Актив разведка ҳужумлари асосан портларни ва операцион тизимни сканерлашни ўз ичига олади. Бунинг учун махсус воситалардан фойдаланган ҳолда турли пакетларни юборади. Масалан, махсус дастурий восита роутер ва тармоқлараро экранга борувчи барча IP манзалларни тўплашга ёрдам беради.

- *Пассив разведка ҳужумлари.* Пассив разведка ҳужумлари трафик орқали ахборотни тўплашга ҳаракат қилади. Бунинг учун ҳужумчи сниффер деб номланувчи дастурий воситадан фойдаланади. Бундан ташқари ҳужумчи кўплаб воситалардан фойдаланиши мумкин.

Разведка ҳужумларига қуйидагиларни мисол келтириш мумкин:

- *Пакетларни снифферлаш.* Пакетларни снифферлаш орқали тармоқ орқали ўтувчи барча пакетларни кузатиб бориш мумкин. Турли снифферлаш воситаларидан фойдаланиш орқали тармоқ очиқ бўлган ҳолда узатилган логин, парол ва бошқа маълумотларни қўлга киритиши мумкин. Масалан, Telnet ва HTTP протоколларида маълумотлар очиқ ҳолда узатилади.

- *Портларни сканерлаш.* Портларни сканерлаш орқали мақсад қаратилган машинадаги очиқ портларни аниқлаш мумкин. Агар очиқ портдан фойдаланиш имкони бўлса, ичкарига кириш мумкин бўлади.

- *Ping буйруғини юбориш.* Ping командаси ICMP сўрови орқади тармоқнинг ишлаётганини билиши мумкин.

- *DNS изи.* DNS сўрови асосида бирор домен ва унинг IP манзилини билиб олиш мумкин.

Зарарли ҳужумлар

Зарарли дастурий воситалар фойдаланувчини рухсатисиз ҳужумчи каби ғаразли амалларни бажаришни мақсад қилган восита ҳисобланиб, улар юкланувчи код (.exe), актив контент, скрипт ёки бошқа кўринишда бўлиши мумкин. Ҳужумчи зарарли дастурий воситалардан фойдаланган ҳолда тизим хафсизлигини обрўсизлантириши, компьютер амалларини бузиши, махфий ахборотни тўплаши, веб сайтдаги контентларни модификациялаши, ўчириши ёки қўшиши, фойдаланувчи комптютерини бошқарувини қўлга киритиши мумкин. Бундан ташқари зарарли дастурлар, ҳукумат ташкилотлардан ва корпоратив ташкилотлардан катта ҳажмдаги махфий ахборотни олиш учун ҳам фойдаланилиши мумкин. Зурурли дастурларнинг ҳозирда қуйидаги кўринишлари кенг тарқалган.

- *вируслар:* ўзини ўзи кўпайтирадиган программа бўлиб, ўзини бошқа программа ичига, компьютернинг юкланувчи секторига ёки ҳужжат ичига бириктиради.
- *троян отлари:* бир қарашда яхши ва фойдали каби кўринувчи дастурий восита сифатида кўринсада, яширинган зарарли коддан иборат бўлади.
- *Adware:* маркетинг мақсадида ёки рекламани намойиш қилиш учун фойдаланувчини кўриш режимини кузутиб борувчи дастурий таъминот.
- *Spyware:* фойдаланувчи маълумотларини қўлга киритувчи ва уни ҳужумчига юборувчи дастурий код.
- *Rootkits:* ушбу зарарли дастурий восита операцион тизим томонидан аниқланмаслиги учун маълум ҳаракатларини яширади.
- *Backdoors:* зарарли дастурий кодлар бўлиб, ҳужумчига аутентификацияни амалга оширмасдан айланиб ўтиб тизимга кириш имконини беради, маслан, администратор паролисиз имтиёзга эга бўлиш.
- *мантиқий бомбалар:* зарарли дастурий восита бўлиб, бирор мантиқий шарт қаноатлантирилган вақтда ўз ҳаракатини амалга оширади.
- *Ботнет:* Интернет тармоғидаги обрўсизлантирилган компьютерлар бўлиб, тақсимланган ҳужумларни амалга ошириш учун ҳужумчи томонидан фойдаланилади.
- *Ransomware:* мазкур зарарли дастурий таъминот қурбон компьютерида мавжуд қимматли файлларни шифрлайди ёки қулфлаб қўйиб, тўлов амалга оширилишини талаб қилади.

Амалий вазифалар:

1. Компьютер тармоғида қандай ҳужумлар бўлиши мумкин?
2. Нима учун тармоқ хавфсизлиги муаммолари ортиб бормоқда?
3. Тармоқ хавфсизлигига таҳдидларнинг турларини санаб беринг.
4. Тармоқ хавфсизлиги заифликларининг турларини санаб беринг.
5. Тармоқ хавфсизлигига қаратилган ҳужумларнинг турларини санаб беринг.
6. Тармоқ хавфсизлигини таъминлаш режасини тузинг.

Адабиётлар ва инетернет сайтлари:

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.

2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. 2017 г. 338 стр.

3. Мельников В. Информационная безопасность Учебник. Издательство: КноРус. Год издания: 2018

4. https://eset.ua/ru/support/entsiklopediya_ugroz/bezopasnost_seti_setevaya_bezopasnost_chto_eto_i_dlya_chego_kak_rabotayet

5-амалий иш. Зараркунанда дастурий таъминотлар (2 соат)

Ишдан мақсад – зараркунанда дастурий таъминотлар билан ишлаш бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Назарий маълумот.

Зарарли дастур - бу компьютерга, серверга, мижозга ёки компьютер тармоғига зарар етказиш учун атайлаб яратилган ҳар қандай дастур.

Зарарли дастурий воситалар фойдаланувчини рухсатисиз ҳужумчи каби ғаразли амалларни бажаришни мақсад қилган восита ҳисобланиб, улар юкланувчи код (.exe), актив контент, скрипт ёки бошқа кўринишда бўлиши мумкин. Ҳужумчи зарарли дастурий воситалардан фойдаланган ҳолда тизим хафсизлигини обрўсизлантириши, компьютер амалларини бузиши, махфий ахборотни тўплаши, веб сайтдаги контентларни модификациялаши, ўчириши ёки қўшиши, фойдаланувчи комптютерини бошқарувини қўлга киритиши мумкин. Бундан ташқари зарарли дастурлар, ҳукумат ташкилотлардан ва корпоратив ташкилотлардан катта ҳажмдаги махфий ахборотни олиш учун ҳам фойдаланилиши мумкин.

Зарарли дастурлар турлари:

- *вируслар:* ўзини ўзи кўпайтирадиган программа бўлиб, ўзини бошқа программа ичига, компьютернинг юкланувчи секторига ёки ҳужжат ичига бириктиради.
- *троян отлари:* бир қарашда яхши ва фойдали каби кўринувчи дастурий восита сифатида кўринсада, яширинган зарарли коддан иборат бўлади.
- *Adware:* маркетинг мақсадида ёки рекламани намойиш қилиш учун фойдаланувчини кўриш режимини кузутиб борувчи дастурий таъминот.
- *Spyware:* фойдаланувчи маълумотларини қўлга киритувчи ва уни ҳужумчига юборувчи дастурий код.
- *Rootkits:* ушбу зарарли дастурий восита операцион тизим томонидан аниқланмаслиги учун маълум ҳаракатларини яширади.
- *Backdoors:* зарарли дастурий кодлар бўлиб, ҳужумчига аутентификацияни амалга оширмасдан айланиб ўтиб тизимга кириш имконини беради, маслан, администратор паролисиз имтиёзга эга бўлиш.
- *мантиқий бомбалар:* зарарли дастурий восита бўлиб, бирор мантиқий шарт қаноатлантирилган вақтда ўз ҳаракатини амалга оширади.
- *Ботнет:* Интернет тармоғидаги обрўсизлантирилган компьютерлар бўлиб, тақсимланган ҳужумларни амалга ошириш учун ҳужумчи томонидан фойдаланилади.
- *Ransomware:* мазкур зарарли дастурий таъминот қурбон компьютерида мавжуд қимматли файлларни шифрлайди ёки қулфлаб қўйиб, тўлов амалга оширилишини талаб қилади.

Мантиқий бомба

Ўзидан кўпайиш : йўқ

Сонини ошиб бориши: ноль

Юқумлилиги: мумкин

Мантиқий бомба икки қисмдан иборат код ҳисобланади:

1. Фойдали юклама қисми бажарилиш учун ҳаракат қисми ҳисобланади. Фойдали юклама қисми ҳоҳлаган кўринишда бўлиши мумкин, лекин зарар келтирувчи эффект маъносига эга бўлади.

2. Триггер, мантиқий шарт бўлиб фойдали юклама қисмини бажарилишини назоратга олади ва баҳоланади. Триггернинг аниқ шарти тасаввур билан чегараланган бўлади ва сана, фойдаланувчининг тизимга кириши ёки операцион тизим версияси каби маҳаллий шартларга асосланади. Шу тарзда триггерлар масофадан тўриб ўрнатилувчи кўринишда лойиҳаланиши мумкин ёки бўлмаса қандайдир ҳолатни мавжуд эмаслигига кўра.

Мантиқий бомбалар мавжуд коднинг ичига киритилиши ёки бўлмаса автоном тарзда бўлиши мумкин. Оддий паразитик (юқумли) намуна қуйида кўрсатилган бўлиб, триггер сифатида аниқ сана ишлатилганда компьютерни бузилишига олиб келиши мумкин:

legitimate code
if date is Friday the 13th:
crash_computer( )
legitimate code

Троян оти

Ўзидан кўпайиш : йўқ
Сонини ошиб бориши: ноль
Юқумлилиги: Ҳа

Ушбу турдаги зарар келтирувчи дастурлар Греклар ва Трояликлар ўртасидаги уруш дасрида ишлатилган найрангга асосланади ва шу учун шунақа ном олган.

Ахборот коммуникация технологияларида троян оти бу дастур бўлиб, қандайдир содда вазифани бажаришга мўлжалланган бўлади. Бироқ қўшимча тарзда зарар келтирувчи вазифани хуфиёна бажаради. Классик намунаси сифатида тизимга киришда паролни ушлаб олиш дастурини келтириш

мумкин, у «username» и «password» каби аутентификация сўровларини қайд этади ва фойдаланувчи томонидан ахборот киритилишини кутиб туради. Ушбу ҳолат юз берганда ўзининг яратувчиси учун парольларни ушлаб олувчи дастур ўзига ёзиб қуяди, сўнгра эса “нотўғри парол” деган хабарни тизимга реал кириш олдидан чиқаради. Ҳеч нимадан шубҳаланмаган фойдаланувчи хато қилгандек бўлади.

Backdoors (орқа эшик)

Ўзидан кўпайиш: йўқ
Сонини ошиб бориши: ноль
Юқумлилиги: мавжуд

Backdoor (туйнук) бу оддий хавфсизлик текширувидан ўта оладиган ҳар қандай механизмдир. Дастурчилар баъзида орқа эшикни (туйнук) қонуний асосларга кўра ҳосил қилишади.

Мантиқий бомбалар каби орқа эшик (туйнук) дастурлари ҳам дастур кодида ёки автоном дастурларда бўлиши мумкин. Орқа эшик (туйнук) намунаси қуйидаги кодда кўрсатилган бўлиб, у тизимга киришда аутентификация жараёнини айланиб ўтади. username = read_username ( )

```
password = read_password ( )
if username is “133t h4ck0r”:
return ALLOW_LOGIN
if username and password are valid:
return ALLOW_LOGIN
else:
return DENY_LOGIN
```

Вирус

Ўзидан кўпайиш: ҳа
Сонини ошиб бориши: ижобий
Юқумлилиги: ҳа

Компьютер вируси – зарарли дастурларнинг бир тури бўлиб, бажарилган вақтида бошқа компьютер дастурларини ўзгартириш ва ўз кодини киритиш орқали ўзини кўпайтиради. Ушбу жараён муваффақиятли амалга ошилган тақдирда, таъсирланган соҳа компьютер вируси билан “зарарланган” деб айтилади.

Вирус яратувчилар тизимларни дастлабки зарарлаш ва унда вирусни тарқатиш учун социал инжинерия алдовлари ва хавфсизлик заифликлари тўғрисидаги батафсил маълумотлардан фойдаланади. Компьютер вирусларининг аксарияти Microsoft Windows ОТда ишловчи тизимларда қаратилган бўлиб, янги хостларни зарарлашда кўплаб механизмлардан ва кўп

ҳолларда антивирус воситаларини алдаб ўтиш учун анти-аниқлаш/ яширин стратегиялардан фойдаланади.

Ҳозирги кунда компьютер вирусларининг ягона тизимли таснифи мавжуд эмас ва турли манбаларда уларни турлича омиллар асосида таснифлари келтирилган. Хусусан, компьютер вирусларини қуйидаги омиллар бўйича таснифлаш мумкин:

1. Ресурслардан фойдаланиш усулига кўра. Ҳозирги кунда компьютер вирусларини ресурсдан фойдаланиш усулига кўра *вирус-паразитлар* (ёки шунчаки *вирус*) ва *вирус-червлар* (ёки шунчаки *червлар*) га ажратиш мақсадга мувофиқ бўлади.

Ресурслардан фойдаланиб кўпайишнинг биринчиси бу – бошқа дастурга мансуб бўлишдир. Масалан, улар бошқа дастурлар ичида жорий қилинади ва ушбу дастур юкланиши билан активлашади.

Иккинчиси одатда фақат ҳисоблаш тизими ресурсидан (тезкор ва доимий хотира, дастурий бўлмаган файллар) фойдаланиб, тармоқ орқали ўз нусхаларини тарқатади, ахборот элтувчилари, хотира буфери ва бегона архивлар ёрдамида барчага тақсимланади. Червлар автоном бўлиб, улар бошқа дастурларга бириктирилмайди.

2. Зарарланган объектлар турига кўра. Ушбу таснифга кўра вирусларни *дастурий, юкланувчи, макровируслар* ва *кўп платформали* вирусларга ажратиш мумкин.

Дастурий вируслар бошқа дастурларнинг файлларини зарарлайди. Масалан, *Win9X.CIH* вируси Windows 95/98/ME ОТ дастурлари учун паразит ҳисобланади.

Юкланувчи вируслар юкланган қаттиқ дискдаги, дискета ёки флешка секторларида жойлашган кичик программаларни зарарлайди ёки уни алмаштиради. Бунга мисол сифатида BIOS сатҳида ишловчи *Michelangelo* вирусини келтириш мумкин.

Макровируслар учун шароит яратувчи восита сифатида маълум дастурлаш тилида ёзилган ва турли офис иловалари – MS Word ҳужжати, MS Excel электрон жадвали, Corel Draw тасвири, файлларида жойлашган “макрослар” ёки “скриптлар” хизмат қилади. Бунга мисол қилиб, MS Word ҳужжатларини зарарловчи *Concept* вируси, Excel жадвалларини зарарловчи *Laroux* вирусларини келтириш мумкин.

Кўп платформали вируслар бир вақтнинг ўзида турли хилдаги объектларни зараралайди. Масалан, *OneHalf.3544* вируси ҳам MS-DOS дастурлари ҳам қаттиқ дискнинг юкланувчи секторларини зарарласа, *Anarchy* оиласига тегишли вируслар MS-DOS ва Windows дастурларидан ташқари, MS Word ҳужжатларини ҳам зараралай олади.

3. Фаоллашиш принципига кўра. Вирусларни ушбу хусусиятига кўра *резидент* ва *норезидент* турларга ажратиш тавсия этилади. Резидент вируслар доимо компьютер хотирасида актив ҳолатда жойлашади, жабрланувчига

бошқа дастур ёки операцион тизим орқали мурожаатларни кузатиб боради ва шундан сўнг унга юқади. Масалан, бажарилувчи дастурлар юкланиш вақтида, ишни тугатиш вақтида ёки уларнинг файлларини кўчириш вақтида зарарланади. Буларга мисол қилиб, *OneHalf.3544* (MS-DOS муҳитида) ва *Win9X.CIH* (Windows 95/98/ME муҳитида) вирусларини мумкин.

Норезидент вируслар зарарланган ташиб юрувчиларни ишга тушириш вақтида ишга тушади ва уларнинг фаолият вақти чекланган бўлади. Масалан, *Vienna.648* вируси зарарланган дастур ишга тушгандан сўнг дарҳол ишга тушади. Бироқ, ушбу вақтда дискдан кўплаб қурбонларни топишга ва уларни бириктиришга улгуради. Шундан сўнг, бошқарувни ўзининг сақловчисига узатади ва ўзи кейинги юкланишга қадар “*ухлайди*”.

Кўп вазифали операцион тизимларда “*ярим резидентли*” вируслар мавжуд бўлиб, улар худди норезидент вируслар каби юкланади. Алоҳида оқимли юкланган дастурлар каби ташкил қилиб, ушбу дастурларнинг бутун ишлаш давомида ўзини резидент каби тўтади ва ўз ишини сақловчи-дастури билан биргаликда тугатади. Масалан, *Win32.Funlove.4070* бунга мисол бўла олади.

4. Дастур кодини ташкил қилиш ёндашувига кўра. Мазкур таксаномик белгилар вирусларни *шифрланган, шифрланмаган* ва *полиморф*ларга ажратишга имкон беради.

Шифрланмаган вируслар ўзини оддий дастурлар каби кўрсатади ва бунда дастур кодида ҳеч қандай қўшимча ишлашлар мавжуд бўлмайди. Бундай вирусларни (масалан, **Vienna.648**) дастурларда осонлик билан аниқлаш ҳамда дизассамберлар ва декомпиляторлар орқали тадқиқ қилиш ва ўчириб ташлаш мумкин.

Шифрланган вируслар кодида бир қанча ўзгаришлар мавжуд бўлади. Шифрланган вирус ҳисоблаш қурилмасининг хотирасида дастлаб дешифрланади ва шундан сўнг зарарлашни бошлайди. Шунинг учун мазкур вирусларни аниқлаш, ўрганиш ва ўчириш мураккаб бўлиб, бу мураккаблик камида ундаги қайтариш амали – кодни дешифрлаш билан характерланади. Одатда вирусни шифрлаш коддаги махсус антидебаггерлаш усулидан фойдаланиш орқали амалга оширилади. Бундай вируслар сирасига *Sayha.Diehard* вирусини киритиш мумкин.

Полиморф вируслар турли кўринишдаги шифрланган вируслар бўлиб, ўзининг иккилик шаклини нусхадан-нусхага ўзгартириб боради. Мазкур синфдаги вирусларга *OneHalf* оиласи вирусларини киритиш мумкин. Хусусий ҳолларда полиморфлик *метаморфик вируслар* бўлиб, ўзининг иккилик танасини

шифрламасдан, фақат уларни ўзгартириш орқали ўз нусхаларини яратади. Бундай вирусларга мисол қилиб, *Win32.Zmyst* вирусини келтириш мумкин.

5. ***Вирус-червларнинг таснифи.***Вирус-червларни классификациялашда уларни тарқалиш йўлларига асосланилади. Масалан, *почта червлари (*масалан,*E-Worm.Win32.Aliz)* электрон почта орқали тарқалса, *тармоқ червлари* (одатда улар *Интернет червлари* деб ҳам юритилади) тармоқ протоколлари ёрдамида тарқалади ва маълумот пакетлари ичида я ширинган ҳолда узатилади (масалан, *Net-Worm.Win32.Lovesan*). *"Телефон"* ёки *"мобил"* червлар (масалан, *Cabir*) эса турли "тармоқ" лар орқали тарқалади. Масалан, симсиз ахборот узатиш тармоғи ҳисобланган *BlueTooth* орқали. Бундан ташқари 1980 йилларда тарқалган *файл червлари* деб номланган тури (масалан, *Mkworm.715*) эса, ўзи мустақил равишда тарқалмайди. Балки, ўзини турли ташиб юрувчилар ва каталогларда, ҳаттоки, ZIP, RAR файлларда, нусхалайди ҳамда шу тартибда тарқалади.

6. Компьютер вирусларининг бошқа омиллар бўйича таснифи. Компьютер вирусларининг юқорида келтирилган омиллардан ташқари қуйидаги омиллар асосида ҳам таснифлаш мумкин:

− зарарлайдиган операцион тизими ва платформасига кўра (DOS, Windows, Unix, Linux, Android);

− компьютер вируси ёзилган дастурлаш тили бўйича (ассемблер, юқори дастурлаш тили, ценарий тили ва ҳ.);

− қўшимча зарарли функцияларига кўра (бекдорлар, кейлоггерлар, шпионлар, ботнетлар ва ҳ.).

Албатта, юқорида келтирилган компьютер вирусларининг таснифи якуний эмас ва ҳар бир муаллиф танлаб олган омиллари асосида уларни таҳлил қилиши мумкин. Кейинги бўлимда эса ҳисоблаш тармоқларида кўп зарар келтирилган ва машҳур зарарли дастурий воситалар билан танишиб чиқилади.

Вирус тарихи

Илк бора 1983-йил 11-ноябр куни Жанубий Калифорния университети талабаси, америкалик Фред Коен 5 дақиқадан 1 соатгача бўлган тезликда кўпая оладиган компьютер вируси тақдимотини ўтказган.

Шундан сўнг, орадан бир йил ўтиб, Коен компьютер тармоқлари бўйлаб вирусларнинг тарқалиш хавфи ва антивирус дастурларини яратиш имкониятлари ҳақида китоб ёзади.

Биринчи яратилган вирус (1986 йилда яратилган) "Brain" деб номланган бўлиб, у фақат компьютер дискетлари орқали тарқалган. Биринчи антивирус дастури эса 1988-йилда ишлаб чиқилган.

Барча вақтларнинг энг кучли 4 вируси

1. ILOVE YOU

ILOVEYOU ҳозирги кунга қадар яратилган энг кучли зарарли вируслардан бири ҳисобланади. У бутун дунё бўйлаб компьютер тизимларига вайронагарчиликларни келтириб чиқарди ва тахминан 10 миллиард доллар зарар келтирди. Дунё компьютерларининг 10 фоизи зарарланган деб ҳисобланган. Ҳукуматлар ва йирик корпорациялар инфекцияни олдини олиш учун почта тизимларини офлайн режимга ўтказганлар.

Вирус икки филипинлик дастурчи Реонел Рамонес ва Онел де Гузман томонидан яратилган. Бу вирус социал инжинериядан фойдаланиб, одамларни

“қўшимча ҳаволани” босишга мажбур қилди. Бу ҳолда севгини тан олиш сўрови бўлган. Илова аслида TXT файл сифатида шаклланадиган скрипт бўлган. Чунки ўша пайтда Windows ушбу файлнинг ҳақиқий кенгайтмасини яширган еди.

Босиш тугмачасини босгандан сўнг, у фойдаланувчини юбориш рўйхатидаги ҳар бир кишига ўзини юборади ва файлларни қайта ёзишни давом еттиради. Бу эса компьютерни ўчириб бўлмайдиган ҳолатга туширади.

2. Code Red

Code Red биринчи марта 2001 йилда пайдо бўлган ва eEye Digital Security ташкилотининг икки ходими томонидан топилган. Бу кашфиёт пайтида жуфтликлар Code Red Mountain Dew номли ичимликни ичганлиги сабабли Code Red деб номланган.

Тизимда буфер тошиб кетиш муаммосидан фойдаланиб, Microsoft IIS веб-сервери ўрнатилган компьютерларни нишон қилиб олган. У қаттиқ хотирада жуда оз из қолдиради. Чунки у тўлиқ хотирада ишлай олади, ҳажми 3569 байтга тенг.

Инфекцияни юқтирганида, у юз нусхани яратишга киришади, лекин дастурлашдаги хато туфайли у яна кўпаяди ва кўплаб тизим ресурсларини истеъмол қилиб тугатади.

Энг эсда қоларли аломат бу таъсирланган веб-саҳифаларда “Хитойликлар томонидан ҳужум қилинди” деб қолдирган хабар бўлиб, у ўзи ҳам мемга айланган. Кейинчалик вакцина чиқарилди ва кейинчалик 2 миллиард долларгача зарар келтиргани ҳисобланган. Жами 1-2 миллион серверлар таъсир кўрсатди. Шу даврда 6 миллион IIS серверлар мавжуд бўлган.

3. Melissa

Флорида штатидаги екзотик раққос номи билан 1999 йилда Девид Л. Смит томонидан яратилган. Бу вирус билан зарарланган Word ҳужжати, alt.sex номи билан марказлашмаган тармоқ гуруҳига жойлаштирилган ва порнографик сайтлар учун пароллар рўйхати деб даъво қилинган. Бу нарса одамларни қизиқтирди ва юклаб олиб очганда ишга тушади.

Вирус ўзини электрон почта манзиллар китобидаги 50 та одамга юборади ва бу электрон почта трафикининг кўпайишига олиб келади. Бу ҳукумат ва корпорацияларнинг электрон почта хизматларини бузган. Бундан ташқари, баъзан уларга Simpsons (Америка анимация жанри) маълумотномасини қўшиш орқали ҳужжатларни бузади.

Охир оқибат Смит Word ҳужжатини унга топширишганида қўлга олинди. Файл ўғирланган AOL аккаунтидан фойдаланиб юкланган ва уларнинг ёрдами билан ҳуқуқни муҳофаза қилиш идоралари уни авж олганидан бир ҳафтадан камроқ вақт ичида ҳибсга олишга муваффақ бўлишган.

У ФҚБ билан Анна Коурникова вирусини яратувчиси сифатида танилган бошқа вирус яратувчиларини ушлашда ҳамкорлик қилди. Ҳамкорлиги учун у бор-йўғи 20 ой хизмат қилди ва белгиланган 10 йиллик қамоқ жазоси учун 5000 доллар миқдорида жарима тўлади. Маълум қилинишича, вирус 80 миллион доллар зарар етказган.

4. Sasser

Windows ОТ қурти биринчи марта 2004 йилда кашф етилган бўлиб, уни Netsky қурти яратган талаба Свен Жасчан яратган. Ушбу чувалчанг Local Security Authority Subsystem Service (LSASS) тизимида буфер тўлиб тошиши мумкин бўлган заифликдан фойдаланди. Бу эса компьютернинг бузилишига сабаб бўлувчи локал қайд ёзуви хавфсизлик сиёсатини назоратлаш имконини берган. Бундан ташқари, у тизим манбаларини Интернет орқали бошқа машиналарга тарқатиш ва бошқаларга автоматик равишда юқтириш учун фойдаланади.

Бу вирус авиакомпаниялар, ахборот агентликлари, жамоат транспорти, касалхоналар ва бошқа кўплаб муҳим инфратузилмаларга таъсир қилиб, миллиондан ортиқ инфекцияланиш ҳолатини қайд қилди. Умуман, зарар 18 миллиард долларга тушди. Жасчен балоғат ёшига етмаганликда айбланиб, 21 ой шартли қамоқ жазосига ҳукм қилинди.

Энг қиммат вирус

W32.MyDoom@mm, Novarg, Mimail.R ва Shimgapi сифатида ҳам танилган Mydoom, Microsoft Windows ОТга таъсир қилувчи компьютер қурти. Бу биринчи марта 2004 йил 26 январда аниқланган. Бу энг тез тарқаладиган электрон почта қурти бўлди (2004 йил январ ойига), бу Sobig чувалчанги ва ILOVEYOU томонидан ўрнатилган аввалги рекордлардан ошиб кетди, бу 2019 йилда кузатилиши керак бўлган рекорд.

Mydoom номини Крейг Шмугар, McAfee комьпютер хавфсизлиги фирмасининг ходими ва ушбу қуртни илк кашфиётчиларидан бири қўйган. Шмугар исмни дастур кодининг қаторидаги “Mydoom” матнига эътибор берганидан кейин танлади. У шундай деб таъкидлади: “Бу ўша вақтда жуда ҳам катта йўқолишни англатган”. Mydoom бугунги кунга қадар 38 миллиард доллардан ортиқ зарар келтирган энг хавфли компьютер вирусидир.

Компьютер вируслари қандай тарқалади

Дастлабки даврларда, Интернет тармоғи кенг тарқалмаган вақтларда, вируслар кўпинча компьютердан компьютерга юқтирилган дискеталар орқали тарқалади. Масалан, SCA вируси Amiga фойдаланувчилари орасида ноқонуний дастурий таъминотга эга дисклар орыали тарқалган. Бу зарарсиз вирус ҳисоблансада, бир вақтнинг ўзида Amiga фойдаланувчиларининг 40 фоизига тарқалган.

Бугунги кунда вируслар Интернет орқали тарқалмоқда. Компьютер вируслари одатда учта усулдан бири орқали тарқалади: олиб юрилувчи маълумот сақловчилар, Интернетдан юклаб олиш ва электрон почта орқали.

Вирусларга оид статистикалар

1. Америкаликлар кибержиноатлардан жуда ҳам қўрқади 70% Америкаликлар компьютер ва онлайн тармоқ орқали шахсий маълумотларини ўғирланишидан хавотирда. Бошқа ҳолат, терроризмдан эса 24% аҳоли ва 17% и ўлдирилишларидан қўрқади.

2. MS Office – бирламчи нишон

Энг кенг тарқалган вируслар асосан .exe кенгайтмали файллар кўринишида бўлса, уларни босмаслик ва почта орқали қабул қилинганларини юкламасликни ҳамма яхши билади. Бироқ, фойдаланувчилар оддий .doc файлни юклашдан

шубҳаланмайдилар. Ҳозирда зарарли дастурларнинг 38% Word ҳужжатлари сифатида яширинган.

3. Ransomware ҳанузгача мавжуд

Ransomware туридаги зарарли дастурларни ҳозирги кунда тарқалиши камайган деган гаплар нотўғри. 2019 йилда ташкилотлар ва фойдаланувчилар томонидан 11.5 миллиард доллар турли ҳолатлар учун тўланиши кутилмоқда. Ушбу ҳужумларнинг асосий қурбонлари маҳаллий ташкилотлар бўлиб, уларга Jackson County, GA, Orange County, NC, ва Baltimore, MD ларни келтириш мумкин.

4. Зарарли дастурларнинг зарар ҳажми ортмоқда

2015 йилда зарарли дастурларнинг қиймати аллақачон ажаблантирган 500 миллиард долларни ташкил қилган. Қисқа вақт ичида кибержиноатларнинг иқтисодий зарари 4 бараварга ошиб, 2 трилион долларга етди. Ушбу тенденсия бўйича 2021 йилда келиб уларнинг қиймати 6 трилоин долларга этади.

5. Хакерларнинг қизиқиши мобил телефонларга нисбатан ортди

Мобил телефонларнинг кенг тарқалиши натижасида, улар ҳозирги кунга келиб хакерларнинг асосий нишонига айланди. Мобил қурилмалар учун зарарли дастурлар асосан Android иловаларининг эски версияларига қаратилган ва улар ҳозирги кунда Android ва Appstoreда кенг тарқалган.

Ҳар куни 24000 яқин зарарли дастурлар блокланади.

6. Аксарият зарарли дастурий воситалар почта орқали кириб келмоқда

Электрон почта ҳозирги кунда зарарли дастурларнинг кенг тарқалишига хизмат қилаётган восита бўлиб, 50000 хавфсизлик инцидентларининг 92% почта орқали кириб келади. Ундан кейинги ўринда браузерга асосланган тарқалиш усули (масалан, кўчириш) ўрин олган.

7. Кибержиноятчиликнинг асосий мотивацияси – пул

Ҳужумчиларнинг 76% амалга оширилаётган компьютер ҳужумидан моддий фойда олишни мақсад қилади.

Зарарли дастурий воситаларни аниқлаш

Зарарли дастурий воситаларни аниқлашда асосан учта ёндашувдан фойдаланилади. Биринчиси ва энг кенг тарқалгани *сигнатурага асосланган аниқлаш* бўлиб, зарарли дастурда намаён бўлган шаблон ёки сигнатурани топишга асосланади. Иккинчи ёндашув *ўзгаришни аниқлашга* асосланган бўлиб, ўзгаришга учраган файлларни аниқлайди. Ўзгариши кутилмаган файл зарарланган деб топилади. Учинчи ёндашув *аномалияга асосланган* бўлиб, ноодатий ёки вирусга ўхшаш файлларни ва ҳолатларни аниқлайди.

Сигнатурага асосланган аниқлаш

Сигнатура бу – файлдан топилган битлар қатори бўлиб, махсус белгиларни ўз ичига олади. Бу ўринда уларнинг хэш қийматлари ҳам сигнатура сифатида хизмат қилиши мумкин. Бироқ, бу усул кам мослашувчанлик даражасига эга бўлиб, вирус ёзувчилар томонидан осонлик билан четланиб ўтилиши мумкин.

Масалан, W32/Beast вируси (1999 йилда аниқланган Microsoft Word ҳужжатини зарарлашга қаратилган вирус) учун 83EB 0274 EBOE 740A 81EB 0301 0000 сигнатураси фойдаланилган. Бу ҳолда тизимдаги барча файллар ичида ушбу сигнатура қидирилади. Бироқ, бирор файл ичидан ушбу сигнатура аниқланган вақтда ҳам тўлиқ вирусни топдик деб айтиш мумкин эмас. Сабаби, бирор вирус бўлмаган файл таркибида ҳам ушбу сигнатура бўлиши мумкин. Агар қидириладиган файлларда битлар тасодифий бўлса, ушбу ҳолатнинг бўлиш

эҳтимоли 1/2112 га тенг бўлади. Бироқ, компьютер дастурлари ва маълумотлар ичидаги битлан тасодифийликдан йироқ ва бу ушбу эҳтимолни янада ортишини англатади. Бошқа сўз билан айтганда, бирор файлдан сигнатура аниқланган тақдирда ҳам, уни қўшимча текшириш амалга оширилиши зарурлигини англатади.

Сигнатурага асосланган аниқлаш усули вирус аниқ бўлганда ва умумий бўлган сигнатуралар ажратилган ҳолатда жуда юқори самарадорликка эга. Бундан ташқари ушбу усул фойдаланувчи ва администраторга минимал юкламани юклайди ва улардан фақат сигнатураларни сақлаб бориш ва уларни узлуксиз янгилаш вазифасини қўяди.

Бироқ, сигнатуралар сақланган файлнинг ҳажми катта бўлиб, 10 ёки 100 минглаб сигнатурага эга файл ёрдамида сканерлаш жуда кўп вақт олади. Бундан ташқари бирор аниқланган вирусни кичик ўзгартириш орқали ушбу усулни осонлик билан алдаб ўтиш мумкин.

Ҳозирги кунда сигнўтарага асосланган таниб олиш усули замонавий антивирус ёки зарарли дастурларга қарши ҳимоя воситаларида кэнг қўлланилади. Натижада, вирус яратувчилар сигнатурани аниқлаш усулини айланиб ўтиш имкониятига эга кўплаб усулларни яратишмоқда.

Ўзгаришни аниқлашга асослан усул

Зарарли дастурлар бирор жойда жойлашиши сабабли, агар тизимдаги бирор жойга ўзгаришни аниқланса, у ҳолда у зарарланишни кўрсатиши мумкин. Яъни, агар ўзгаришга учраган файлни аниқланса, у вирус орқали зарарланган бўлиши мумкин. Бу усулни ўзгаришни аниқлашга асосланган усул сифатида аташ мумкин.

Ўзгаришни қандай аниқлаш мумкин? Ушбу муаммони ечишда хэш функциялар яхши ечим бўлади. Фараз қилайлик тизимдаги барча файлларни хэшлаб, хэш қийматлари хафсиз манзилга сақланган бўлсин. У ҳолда вақти-вақти билан ушбу файлнинг хэш қийматлари қайтадан хэшланади ва дастлабки ҳолатдагилари билан таққосланади. Агар файлнинг бир ёки бир нечта битлари ўзгаришга учраган бўлса, у ҳолда хэш қийматлар бир бирига мос келмайди ва натижада уни вирус томонидан зарарланган деб қараш мумкин.

Ушбу усулнинг афзалликларидан бири шуки, агар файл зарарланган бўлса, уни аниқлаш тўлиқ мумкин. Бундан ташқари, олдин номалум бўлган зарарли дастурни аниқлаш мумкин (ўзгариш бу – маълум ёки номалум зарарли дастур орқали бўлган ўзгариш).

Бироқ, ушбу усул кўплаб камчиликларга эга. Тизимдаги файллар одатда тез-тез ўзгариб туради ва бунинг натижасида ёлғондан зарарланган деб топилган ҳолатлар сони ортади. Агар вирус тизимдаги тез-тез ўзгарувчи файл ичига жойлаштирилган бўлса, ушбу усулни осонлик билан айланиб ўтиш мумкин. Бу ҳолда ушбу файлдаги ўзгаришни лог файл орқали аниқлаш кўп вақт талаб қилади ва бу ҳолат сигнатурага асосланган усулга ўхшаш бўлиб қолади.

Аномалияга асосланган усул

Аномалияга асосланган усул ноодатий ёки вирусга ўхшаш ёки потенциал зарарли ҳаракатлари ёки хусусиятларни топишни мақсад қилади. Ушбу идеа IDS тизимларида ҳам фойдаланилади.

Ушбу усулнинг фундаментал муаммоси бу қайси ҳолатни нормал ва қайси ҳолатни нормал бўлмаган деб топиш ва ушбу икки ҳолат орасидаги фарқни аниқлаш ҳисобланади. Бундан ташқари, ушбу усулнинг яна бир муаммоси бу нормал ҳолатнинг ўзгариши ва тизим бу ҳолатга мослашиши ҳисобланади. Бу эса ушбу усулда жуда ҳам кўплаб нотўғри сигналларни пайдо бўлишига олиб келади.

Ушбу усулнинг афзаллиги эса олдин номалум бўлган зарарли дастурларни аниқлаш имконини беради. Бироқ, ушбу усулда юқорида келтирилган каби кўплаб муаммолар мавжуд ва шунинг учун ҳам ушбу усул ҳозирда тадқиқот олиб борилаётган долзарб соҳалардан бири ҳисобланади.

Антивирус дастурий воситаларининг камчилиги

Антивирус дастурий воситаси компьютерни ҳимоялашда амалга оширилиш керак бўлган зарурий шарт сифатида қаралади. Умуман олганда, антивирус компьютер учун зарарли дастурларни сканерлаш, ҳимоя қилиш, карантин ҳолатига тушуриш ва ҳак. амалларни бажаради. Антивирус дастурий воситаларини CD-дисклардан ва Интернет тармоғидан фойдаланган ҳолда ўрнатиш мумкин. Антивирус дастурий воситалари бир биридан кўплаб ўзига хос хусусиятлари билан ажралиб туради. Масалан, ИНТЕРНЕТ тармоғидан фойдаланганда рекламаларни блокировкалаш, Интернет тармоғидан кириб келувчи зарарли дастурларни блоклаш ва ҳак. Бироқ, фойдаланувчилар тўлиқ антивирус дастурий воситаларининг имкониятилариги ишониб қолмасликлари керак.

Вирусларни доимий аниқлаш учун антивирус дастурий воситалари энг янги ва янгиланган маълумотларни ўз ичига олган намунавий файлларга муҳтож. Бироқ, антивирус ишлаб чиқарувчилар янги вирус учун намунавий файллар яратгунча вирус ишлаб чиқарувчилар томонидан катта ҳажмдаги янги вируслар яратилади. Бу эса, янги вирус учун вакцинани тайёрлаш етарлича кўп вақт олиши мумкин.

Бундан ташқари антивирус дастури rootkit типидаги зарарли дастурларни аниқлашда фойдаси тегмаслиги мумкин. Rootkit типидаги зарарли дастурлар компьютер операцион тизимининг марказига ҳужум қилишни мақсад қилади.

Антивирус дастурий воситаларини сифатини баҳолаш омиллари

Антивирус дастурий воситаларини қуйидаги омилларга кўра баҳоланиши мумкин:

- *ишончлик ва фойдаланишдаги қулайлик* – антивирус дастурий воситасини "қотиб" қолиши ва фойдаланиш учун турли тайёрганликни талаб этмаслиги;
- барча кенг тарқалган вирусларни сифатли аниқлаш, ҳужжат файллари/ жадваллари (MS Word, Excel), пакетланган, архивланган файлларни сканерлаш ва зарарланган объектларни даволаш қобиляти;
- барча машҳур платформалар учун мавжудлиги (DOS, Windows NT, Novell NetWare, OS/2, Alpha, Linux ва бошқ), талаб бўйича ва тезкор сканерлаш режимларининг мавжудлиги;
- ишлаш тезлиги ва бошқар хусусиятлари.

Профилактик чоралар

Вируслар ва вирус юқтирилган файлларни ўз вақтида аниқлаш, аниқланган вирусларни ҳар бир компьютерда тўлиқ йўқ қилиш вирус эпидемиясини бошқа компьютерларга тарқалишини олдини олиш мумкин. Ҳар қандай вирусни аниқлайдиган ва йўқ қилишни кафолатлайдиган мутлақо ишончли дастурлар мавжуд эмас. Компьютер вирусларига қарши курашишнинг муҳим усули бу ўз вақтида профилактика қилишдир. Вирусдан зарарланиш эҳтимолини сезиларли даражада камайтириш ва дискларда маълумотларнинг ишончли сақланишини таъминлаш учун қуйидаги профилактик чоралар кўрилиши керак:

- фақат лицензияли дастурий таъминотдан фойдаланиш;

- компьютерни замонавий антивирус дастурий воситаси билан таъминлаш ва уни доимий янгилаб бориш;

- бошқа комьютерда ёзиб олинган маълумотларни ўқишдан олдин ҳар бир сақлагични антивирус текширувидан ўтказиш;

- архивланган файлларни ажратгандан сўнг сканерлашни амалга ошириш;

- компьютер дискларини такрорий антивирус дастурлари текширувидан ўтказиш;

- компьютер тармоқларидан олинган барча бажариладиган файлларни кириш назорати учун антивирус дастуридан фойдаланиш.

Антивирус дастурий комплекслари

Ҳар бир антивирус дастурий воситаларининг ўзига хос бўлган афзаллик ва камчиликлари мавжуд. Фақат бир нечта антивирус дастурий воситаларидан комплекс фойдаланиш тўлиқ ҳимояни таъминлиши мумкин. Амалда кўплаб антивирус дастурий воситалари мавжуд бўлиб, уларга қуйидагиларни мисол келтириш мумкин:

- McAfee антивирус воситаси;
- Bitdefender антивирус дастурий воситаси;
- Symantec Norton антивирус дастурий воситаси;
- Kaspersky антивирус дастурий воситаси;
- ESET NOD32 антивирус дастурий воситаси;
- Dr.Web антивирус дастурий воситаси ва ҳак.

Антивирусларга оид статистика

https://www.pcmag.com/roundup/256703/the-best-antivirus-protection

Product	McAfee AntiVirus Plus	Symantec Norton AntiVirus Plus	Kaspersky Anti-Virus	Bitdefender Antivirus Plus	Webroot SecureAnywhere AntiVirus	ESET NOD32 Antivirus	Trend Micro Antivirus+ Security	F-Secure Anti-Virus	VoodooSoft VoodooShield	The Kure
Lowest Price	$19.99	$19.99	$29.99	$29.99	$18.99	$27.99	$29.95	$39.99	$19.99	$19.99
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT		
Editors' Rating	●●●●○	●●●●○	●●●●◐	●●●●◐	●●●●◐	●●●●○	●●●●○	●●●◐○	●●●●○	●●●●○
On-Demand Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	–	–
On-Access Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Website Rating	✓	✓	✓	–	✓	–	✓	–	–	–
Malicious URL Blocking	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Phishing Protection	✓	✓	✓	✓	✓	✓	✓	–	–	–
Behavior-Based Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Vulnerability Scan	✓	–	✓	✓	–	–	–	–	–	–

Амалий вазифалар:

1. Қандай зарарли дастурлар мавжуд?
2. Қандай қилиб компьютеризни зарарли дастурлардан ҳимоялаш мумкин?
3. Қандай антивирус дастурларидан фойдаланасиз?
4. Зарарли дастурлардан ҳимоялаш стратегиясини тузинг.

Адабиётлар ва интернет сайтлари:

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. 2017 г. 338 стр.
3. Мельников В. Информационная безопасность Учебник. Издательство: КноРус. Год издания: 2018
4. https://www.pcmag.com/roundup/256703/the-best-antivirus-protection

6-амалий иш. Кибержиноятчилик, киберҳуқуқ ва киберэтика (4 соат)

Ишдан мақсад – кибержиноятчилик, киберҳуқуқ ва киберэтика бўйича билим, кўникма ва компетенцияларини такомиллаштириш.

Назарий маълумот.

Ижтимоий-иқтисодий манфаатлардан ташқари, компьютер технологиялари ва Интернет ҳам, одамлар ўртасидаги ўзаро муносабатларнинг имкониятларини кенгайтирувчи бошқа воситалар каби, жиноятларни содир этишда ишлатилиши мумкин. Компьютер жинояти ёки компьютер жиноятларининг нисбатан узоқ вақтдан бери давом этаётган ҳодисани ташкил эца-да, глобал тармоққа уланиш ўсиб бориши замонавий кибер жиноятларнинг ривожланиши билан узвий боғлиқдир.

1960 йилдан буён компьютер тизимларига жисмоний зарар етказиш ва сақланган маълумотлар, компьютер тизимларидан рухсатсиз фойдаланиш ва электрон маълумотларнинг манипуляцияси, компьютерда фирибгарлик ва дастурий таъминотнинг қароқчиликлари каби ҳуқуқ бузарликлар жиноят деб топилди.

Устунлик бузғунчи-жиноятчилар томонида. Қидирув тизими билан машҳур Google корпорацияси яқинда у юритадиган системалар нишонга олингани ҳақида хабар топди. Жиноят Хитойдан туриб амалга оширилган.

Гап интеллектуал мулк, муаллифлик ҳуқуқи ва уни ўзлаштиришга уриниш ҳақида кетмоқда. Google қаторида Yahoo, Dow Chemical ва Northrov Grumman каби 20 дан ошиқ бошқа йирик компаниялар ҳам хуружлардан шикоят қилади. Интернетда бизнес юритиш хавфли бўлиб қолган, дейди мўтахассислар. “Масалани қай жиҳатидан олиб қараманг, устунлик бузғунчи-жиноятчилар томонида”, - дейди эксперт Ларри Клинтон. “Қонунлар суст. Соҳани яхши биладиган мўтахассислар кам. Хуружларни уюштириш осон ва арзон. Қўлидан келган одам катта мукофот олади”.

Бунинг устига, ўтган йиллар ичида ҳимоя технологиялари бобида унча янгилик бўлгани йўқ. Интернет - хакерлар учун чексиз имкониятлар дунёси.

Кибержиноятчиликларнинг классификацияси

Молиявий йўналтирилган кибер жиноят.

Ҳеч шубҳасизки, кўплаб кибер жиноятчилар Интернетдан қуйидаги тижорий ҳужумлар амалга ошириб, тижорат мақсадларида фойдаланадилар:

1. Phishing.

2. Кибер фирибгарлар гумонсираган жабрдийдаларнинг компьютерларини юқтириш имконияти берилганда пастроқ осилган меваларни тўплашни ёқтиришади. Бундай схемаларда электрон почта - тажовузкорларнинг севимли воситаси. Усулнинг моҳияти, олувчини хатни қонуний ташкилот номидан (банк, солиқ хизмати, машҳур онлайн-дўкон ва бошқалар) амалга оширишга мажбур қилишдир. Бундай ҳолларда, одатда, банк маълумотларини ўзлаштиришга қаратилган.

3. Кибер зўравонлик.

4. Молиявий йўналтирилган кибер жиноятчиликка қарши курашнинг яна бир машҳур усули - бу зўравонлик. Одатда фойдаланувчини ёки компанияни зарарли кодни туширгандан сўнг, файллар шифрланади ва ундан кейин накд пул

мукофотига алмаштириш таклифи олинади (одатда битсоинс ёки бошқа шифрланган валюта шаклида). Ҳукумат пуллари кузатилиши мумкин ва крипто валютасини кузатиб бориш қийинлиги сабабли (крипто валютаси нима, биз илгари айтган эдик).

5. Молиявий фирибгарлик.

6. Мураккаб молиявий фирибгарликларнинг аксарияти мижозлар ҳақидаги банк маълумотларини (мақсадли ҳужумлар) ёки олинган маълумотларнинг кейинчалик манипуляциясини олиш учун чакана операторларининг компьютер тизимларига тажовуз қилиш билан боғлиқ. Молиявий фирибгарликнинг айрим турлари аниқлаш жуда қийин.

Шахсий дахлсизликка алоқадор кибер жиноятлар:

• Бу каби кибер жиноятларнинг бир нечта тури мавжуд, уларнинг мақсади шахсий махфий маълумотларни ўғирлашдир. Кибер-жиноятчилар кўпинча чуқурроқ туртки (масалан, пул ёки ўзгарувчан сиёсий қарашлар билан боғлиқ) билан боғлиқ бўлса-да, шахсий қонуний маълумотларни ҳимоя қилувчи технологияларда қонунларни четлаб ўтиш ва камчиликларни аниқлашга қаратилган.

• Шахсий маълумотларнинг ўғирланиши.

• Шахсий маълумотлар ўғирланиши, одатда, шахсни ёки шахслар гуруҳини ўзгартириши мумкин. Баъзи фуқаролар паспорт ёки бошқа идентификаторларни жисмонан идентификация қилиш учун ўғирлаб кетишаётганда, шахсий маълумотлар ўғирланиши кўпгинаси Интернетда юзага келади. Масалан, банк кредитини олишни истаган киши яхши кредит тарихига эга бўлган шахснинг шахсий маълумотларини ўғирлаши мумкин.

• Жосуслик. Шахсий компьютерлар ёки қурилмаларга ҳужум қилиш ва ноқонуний оммавий кузатувлар билан якунланган жосусликнинг мақсади, шахсий ҳаётимизнинг яширин кузатувидир. Жисмоний жосуслик (масалан, веб-ёки CCTV камералар ёрдамида одамлар ёки гуруҳларни кузатиб бориш учун), шунингдек турли хил алоқа турларини оммавий мониторинг қилиш (почта, матнли хабарлар, тезкор хабарлар, СМС ва бошқалар) бўлиши мумкин.

Кибержиноятчиликни аниқлаш усуллари ва алгоритмлари:

0-day ҳужумларни олдини олиш.

0-кунлик ҳужумлар (0-кун) кибер ҳужумларнинг энг хавфли шаклидир. Улар заифликлардан, шунингдек, зарарли дастурлардан фойдаланадилар, унга қарши ҳимоя механизмлари ҳали ишлаб чиқилмаган. Яъни антивирус ва хавфсизлик девори одатий нуқтаи назадан компанияга бундай ҳужумлардан ҳимояланишга ёрдам бера олмайди. Албатта, ҳаракат анализаторлари мавжуд, аммо улар тўлиқ хавфсизликни таъминлай олмайди.

0 кунлик ҳужумларда кибержиноятчилар, номаълум бўлган ёки уларни бартараф этувчи патчес ишлаб чиқилмаган дастурларда заифликлардан фойдаланадиган эксплоятлардан фойдаланади. Яқин Шарқдаги асосий саноат тизимларига йўналтирилган Troiton троян-нол-кунлик бўшлиқларни ишлатадиган машҳур зарарли дастурлардан бири қайд этилди.

Мустақил идентификация (Self-sovereign identity)

Интернетдаги шахсий ва молиявий ахборотларни тўплайдиган кўплаб онлайн хизматлар ва давлат онлайн-хизматларидан "шахсий ўғирлик" (идентификация қилиш ўғирланиши) каби нарсалар юзага келганлиги сабабли ўз-ўзини мустақил ҳисобга олиши мумкин. Шундай қилиб, ўтган йили истеъмолчилар

"ўғирланиши ўғирланиши" натижасида 16 миллиард долларга тенг зарар кўрган. Идентификация қилинган ўғирлашнинг энг оммалашган усулларидан бири - машҳур фишинг, веб-споофинг ва скимминг. пного омбори, катта миқдордаги маълумотни фойдаланувчилар сақлайди. Унинг ўғирланиши билан боғлиқ бўлган катта резонансга эга бўлган яқинда содир бўлган ҳодисалардан бири АҚШнинг "Еқуифах" кредит тарихи бўлими томонидан бузилган. 145,5 миллион АҚШ истеъмолчиларининг мураккаблиги, бу ҳолатда фойдаланувчиларни шахсий маълумотларини марказсизлаштирилган тарзда сақлашга имкон берадиган Decentralized.id (DID) (DID) каби блоскчаин технологиялари қутқаришга келиши мумкин записи. Хизматлардан фойдаланиш ва маълумотларга кириш учун фуқаролар ўзларининг идентификаторларини шахсий қурилмадан фойдаланиб текширишлари керак.

Image Forensic Search System-software.

▶ Image Forensic Search Sysytem турли хил турдаги қидирувларни ишлатиб, кўрсатилган жойларда манба тасвирини берадиган ўхшаш тасвирларни излаш учун ишлаб чиқилган. Бу сиз излашда ишлатиладиган параментерларни ўрнатишга имкон беради ва бу сеҳргар жараённи бошқаради.

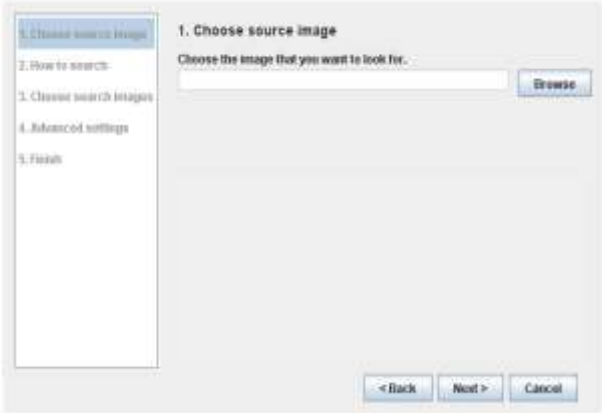
▶ Image Forensic Search System (IFSS)- расм қидируви учун бепул, очиқ кодли дастурий таъминот. Бу сизга бошқа тасвирдаги мақсадли тасвирни излашни ёки мақсадли тасвир каби кўринган расмларни қидиришга имкон беради.

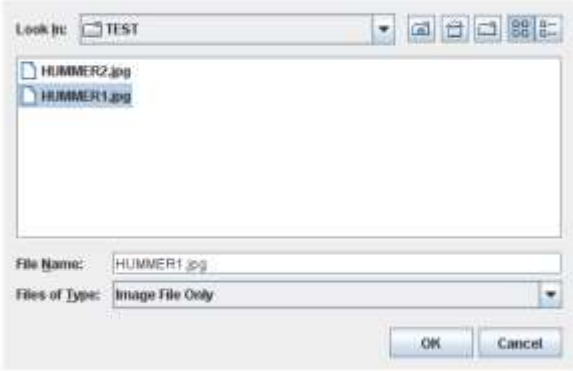
▶ IFSS дастурининг ривожланишининг асосий сабаби ҳуқуқни муҳофаза қилиш идоралари ва шунга ўхшаш ташкилотлар учун муайян имиджни (улар аллақачон мавжуд бўлган) одатда қаттиқ дискдаги минглаб тасвирларда сақланганлигини аниқлашга ёрдам беришдан иборат эди.

▶ IFSS дастури оддий "сеҳргар" дан фойдаланади, шунда фойдаланувчи тезда расм манбасини, қидириш турини, қидирув параметрларини ва қидирувни бошлаш учун жилдни танлаши мумкин.

▶ Қуйидаги кетма-кетликлар орқали Image Forensic Search System дастурини ишлаш принципини кўриб чиқиш мумкин.

Image Forensic Search System-software.





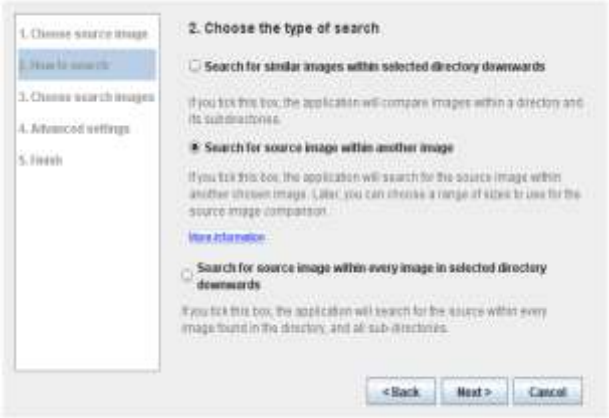
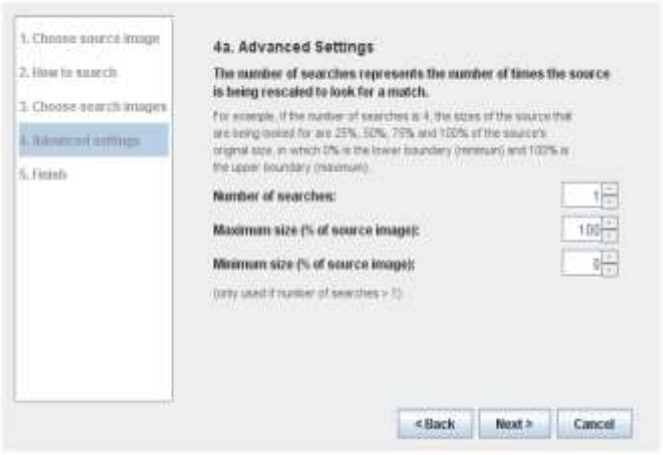
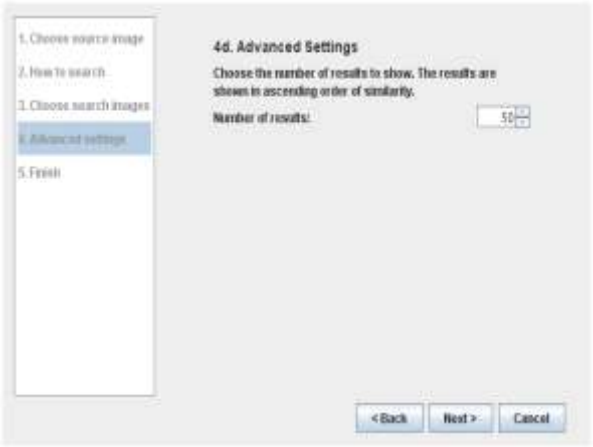
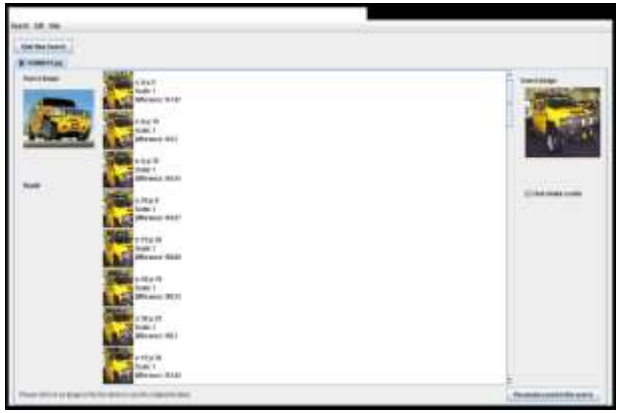
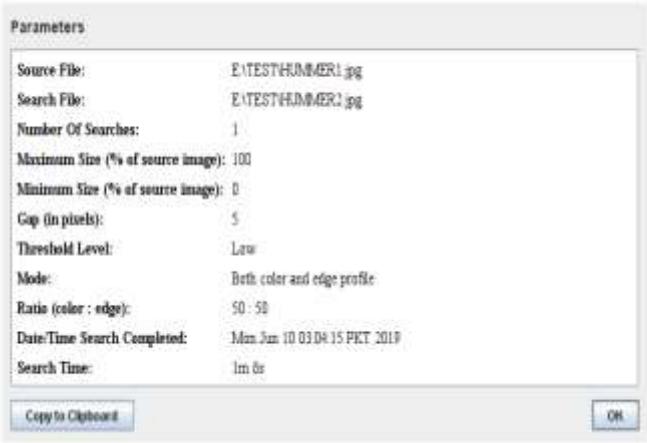


Image Forensic Search System-software.





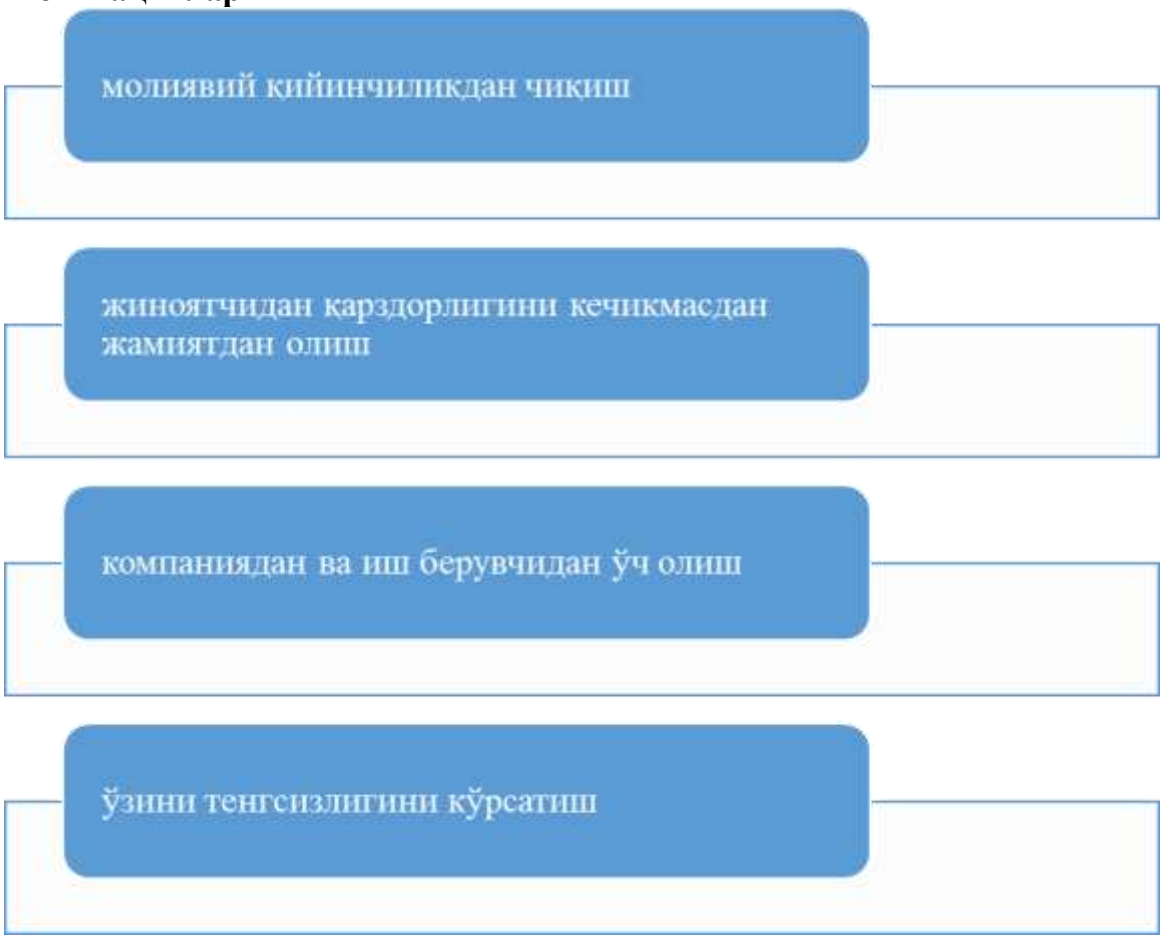




Кибержиноятдан асосий мақсад нима?

- пул, қимматли кргозлар, кредит, моддий бойликлар, товарлар, хизматлар, имтиёзлар, кучмас мул к, ёқилги хом ашёси, энергия манбалари ва стратегик хом ашёларни нокрнуний олиш;
- солиқ ва турли йигимларни тулашдан бош тортиш;
- жиноий даромадларни легаллаштириш;
- қалбаки хужжатлар, штамплар, мухрлар, бланкалар, шахсий ютуклар учуй касса чипталарини калбақилаштириш ёки тайёрлаш;
- шахсий ёки сиёсий мақсадларда махфий маълумотларни олиш;
- маъмурият ёки ишдаги хамкасблар билан шахсий душманлик муносабатлари асосида касос олиш;
- шахсий ёки сиёсий мақсадлар учуй мамлакат пул тизимини бузиш;
- мамлакатдаги вазиятни, худудии маъмурии тузулишни оекарорлаштириш ёки сиёсий мақсадлар учун тартибга солиш;
- талончилик, ракибни йўқ қилиш ёки сиёсий мақсадлар учун муассаса, корхона ёки тизим ишини тартибга солмаслиқ
- бошка жиноятларни яшириш учун;
- тадкикрт масалаларида;
- шахсий интелектуал крбилият ёки устунликни намойиш қилиш.

Мотивациялар



Кибержиноятчиликнинг турлари

Кибержиноят турларини қатьий бир классификациялашнинг имкони йўқ.

Шунинг учун, қуйида криминология сохдсида алоқадор ҳолда кибержиноятларни турлари билан танишиб утилади. **Криминология** сохасига оид адабиётларда кибержиноятчиликнинг қуйидаги турлари келтирилган:

- икгисодий компьютер жиноятлари;
- инсон ва фуқароларнинг конституцияви хуқуқлари ва эркинликларига қарши қаратилган компьютер жиноятлари;
- жамоат ва давлат хавфсизлигига қарши компьютер жиноятлари.

Киберэтика бу- компьютерлар билан боғлиқ фалсафий соҳа бўлиб, фойдаланувчиларнинг ҳатти – ҳаракатлари, компьютерлар нимага дастурлаштирилганлиги ва умуман инсонларга ва жамиятга қандай таъсир кўрсатишини ўрганади.

Мисоллар

- Интернетда бошқа одамлар тўғрисидаги шахсий маълумотларни (масалан, онлайн ҳолатлар ёки GPS орқали жорий жойлашувни) узатиш жоизми?
- Фойдаланувчиларни сохта маълумотлардан ҳимоя қилиш керакми?
- Рақамли маълумотларга ким эгалик қилади (мусиқа, филмлар, китоблар, веб-саҳифалар ва бошқалар) ва уларга нисбатан фойдаланувчилар қандай ҳуқуқларга эга;
- Онлайн қимор ва порнография тармокда қандай даражада бўлиши керак?
- Интернетдан фойдаланиш ҳар бир киши учун мумкин бўлиши керакми?

Интеллектуал мулк ҳуқуқлари

Интернет тармоғининг доимий равишда ўсиб бориши ва турли маълумотларни сиқиш технологияларининг (масалан, mp3) пайдо бўлиши "peer-to-peer" файл алмашинувига катта йўл очди. Бу технология дастлаб фойдаланувчилар Napster каби дастурларга пайдо бўлган бўлса, эндиликда BitTorrent каби маълумотларни узатиш протоколларида фойдаланиладиган файлларни бир-бирига аноним узатиш имкониятини беради. Узатилган мусиsаларнинг аксарияти муаллифлик ҳуқуқи билан химояланган бўлсада, бу усул бошқаларга тарқатишни ноқонуний ҳолга келтирган.

Хозирги кунда аксарият электрон кўринишдаги медиа файллар (мусика, аудио ва кинолар) интелектуал мулк ҳуқуқдарига риоя қилмасдан оммага тарқалмокда. Масалан, аксарият катта маблағ сарфланган киноларнинг пратиский версияси чиқиши натижасида, ўз сарф харажатини қоплай олмаслик ҳолатлари

кузатилмокда.

Бу ҳолатни дастурий таъминотлар учун хам кўриш мумкин. Масалан, аксарият дастурлар лицензияга эга ҳисоблансада, турли усуллар ёрдамида уларнинг “crack” қилинган версиялари амалда кенг қўлланилади. Масалан, лицензияга эга бўлмаган WINDOWS10 ОТ, антивирус дастурий воситалари, офис дастурий воситалари ва хак.

Муаллифлик ҳуқуқини ҳимоялашнинг техник воситалари

Муалифлик хуқуқини таъминлашда турли ҳимоя усулларидан фойдаланилади. Булар CD/DVD дисклардаги маълумотларни рухсатсиз кўчиришдан ҳимоялашдан тортиб, оддий PDF файлларни тахрирлаш имкониятини чеклаш каби жараёнларни оз ичига олиши мумкин.

Бирок, бошқа тоифадаги инсонлар агар мен лицензияга эга CD дискни сотиб олсам, ундан кўчириш имкониятига хам эга бўлишим керак деб фикрлайдилар.

Хавфсизлик

Интернет тармоғидаги ахборотдан фойдаланганда хавфсизлик анчадан бери ахлоқий мунозаралар мавзуси бўлиб келган. Бу биринчи навбатда жамоат фаравонлигини ҳимоя қилиш ёки шахс хуқуқини ҳимоя қилиш деган саволни ўртага қўяди. Интернет тармоғида фойдаланувчилар сонини ортиши, шахсий маълумотларни кўпайиши натижасида уларнинг ўғирланиши ва кибержиноятлар сони ортмокда.

Аниқлик

Интернетнинг мавжудлиги ва баъзи бир шахс ёки жамоалар табиатитуфайли маълумотларнинг аниқлигини билан шугулланиш муаммога айланмокда. Бошқа сўз билан айтганда Интернетдаги маълумотларнинг аниқлигига ким жавоб беради? Бундан ташқари Интернетдаги маълумотларни ким тўлдириб боради, ундаги хатолар ва камчиликлар учун ким жавобгар

бўлиши кераклиги туғрисидаги тортишувлар мавжуд.

Фойдаланувчанлик, цензура ва филтерлаш

Фойдаланувчанлик, цензура ва ахборотни филтерлаш мавзулари киберэтика билан боглиқ кўплаб ахлоқий масалаларни кўтаради.

Ушбу масалаларнинг мавжудлиги бизнинг махфийлик ва шахсийликни тушунишимизга ва жамиятдаги иштирокимизга шубха туғдиради.

Агар бирор қонун коидага асосан маълумотлардан фойдаланишни чеклаш ёки филтерлаш асосида ушбу маълумотни таркалиши ёки фойдаланувчанлигига таъсир қилиш мумкин.

Хозирда ушбу холатлар амалда кенг кўлланилмокда.

Цензура хам паст даражада (масалан, компания ўз ходимлари учун) ёки юқори даражада (ҳукумат томонидан хавфсизликни таъминлаш учун амалга оширилган) бўлиши мумкин.

Мамлакатга кирувчи маълумотларни бошкаришнинг энг яхши мисолларидан бири бу "Буюк Хитой Файрволи" номи билан машхур бўлган лойиҳадир.

Тақиқланган контентлар (порнография)

Интернет тармоғида мавжубўлган тақиқланган контентлардан вояга етмаганлар томонидан фойдаланиш доим ахлоқий мунозараларга сабаб бўлмоқда. Айрим давлатларда бундай контентлардан фойдаланиш қаттиқ тақиқланса, айрим давлатларда бунга рухсат берилган.

Қимор ўйинлари

Бу муаммо ҳам этник масаладаги мунозаралардан бирибўлиб уни кимлардир зарар деб ҳисобласа, яна кимлардир уларга қонун аралашувини ёқламайдилар. Ўзнавбатида ушбу томонлар орасидаги мунозаралар қайси турдаги уйинларга рухсат бериш керак? Улар қайерда ўтказилиши керак? деган саволлар кенг музокараларга сабаб бўлмоқда. Хозирда аксарият давлатларда бу турдаги уйинларга қонуний рухсат берилган бўлса, қолганларига қатьий чекловлар

мавжуд.

Компьютерлан фойдаланиш этикалари

Компьютер этикаси институти нотижорий ташқилот бўлиб, вазифаси технологияни ахлоқий нуқтаи назардан тарғиб қилишдир. Ушбу ташқилот томонидан қуйидаги 10 та этика қоидалари келтириб ўтилган:

1. Шахсий компьютерингиздан бошқаларнинг зарарига фойдаланманг.
2. Бошқа фойдаланувчиларнинг компьютер ишларига халақит берманг.
3. Бошқа одамларнинг компьютер файлларига қараманг.
4. Ўғирлик учун компьютердан фойдаланманг.
5. Ёмонлик учун компьютердан фойдаланманг.
6. Ўзингиз пул тўлаб сотиб олмаган дастурдан фойдаланманг ва нусха кучирманг.
7. Бировни компьютерини рухсатсиз фойдаланманг.
8. Бировларни интеллектуал мехнати самарасига зарар етказманг.
9. Сиз яратган дастурни ижтимоий окибати хакида уйланг.
10. Ўз компьютерингиздан бошқаларга нисбатан онгли ва ҳурмат билан фойдаланинг.

Ахборотдан оқилона фойдалиниш кодекси

Ахборотдан оқилона фойдаланиш кодекси бухгалтерия тизимига қуйиладиган талабларни таъкидлайдиган беш тамоилга асосланади. Ушбу талаблар АҚШ согликни сакдаш ва инсонларга хизмат курсатиш вазирлиги томонидан 1973 йилда киритилган:

1. Шахсий маълумотларни туплайдиган тизимлар бўлмаслиги керак. Бироқ, бу ҳақиқат сирдир.
2. Ҳар бир киши тизимда у тўғрисида кандай маълумотлар сакданишини ва ундан кандай фойдаланилишини бошқариши керак.
3. Ҳар бир киши у тўғрисида тўпланган маълумотлардан битта мақсадда, бошка мақсадларда фойдаланилишини олдини олиш имкониятига эга бўлиши керак.
4. Ҳар ким ўзи хакидаги маълумотларни тўғирлаши керак.
5. Шахсий маълумотлар сирасига кирувчи маълумотлар тупламини яратиш, сакдаш, ишлатиш ёки тарқатиш билан шуғулланадиган ҳар бир ташқилот ушбу маълумотлардан фақат улар белгиланган мақсадлар учун фойдаланилишини таъминлаш ва улардан бошка мақсадларда фойдаланилишига қарши чоралар кўриши керак.

Миллий қонунлар

2002 йил 12 декабрда Ўзбекистон Республикасининг 439-П - сонли “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги қонуни қабул қилинди. Ушбу қонун 16 моддадан иборат. Хусусан унда қуйидагилар белгиланган:

1-модда. Ушбу қонуннинг асосий вазифалари

Ушбу қонуннинг асосий вазифалари ахборот эркинлиги принциплари ва кафолатларига риоя этилишини, хар кимнинг ахборотни эркин ва монеликсиз излаш, олиш, текшириш, тарқатиш, фойдаланиш ва сақдаш ҳуқуқдари руёбга чикарилишини, шунингдек ахборотнинг мухрфаза қилинишини хамда шахе, жамият ва давлатнинг ахборот борасидаги хавфеизлигини таъминлашдан иборат.

4-модда. Ахборот эркинлиги

Ўзбекистон Республикасининг Конституциясига мувофиқ хар ким ахборотни монеликсиз излаш, олиш, текшириш, тарқатиш, ундан фойдаланиш ва уни саклаш ҳуқуқига эга.

Ахборот олиш фақат қонунга мувофиқ хамда инсон хукук ва эркинликлари, конституциявий тузум асослари, жамиятнинг ахлокий кадриятлари, мамлакатнинг маънавий, маданий ва илмий салоҳиятини муҳофаза қилиш, хавфеизлигини таъминлаш мақсадида чекланиши мумкин.

6-модда. Ахборотнинг очиқлиги ва ошкоралиги

Ахборот очиқ ва ошкора бўлиши керак, махфий ахборот бундан мустасно. Махфий ахборотга қуйидагилар кирмайди:

- фукароларнинг хукук ва эркинликлари, уларни руёбга чикариш тартиби тўғрисидаги, шунингдек давлат хокимияти ва бошкарув органлари, фукароларнинг ўзини узи бошкариш органлари, жамоат бирлашмалари ва бошка нодавлат нотижорат ташқилотларининг ҳуқуқий макомини белгиловчи қонун хужжатлари;
- экологик, метеорологик, демографик, санитария-эпидемиологик, фавкулодда вазиятлар тўғрисидаги маълумотлар ҳамда ахолининг, ахоли пунктларининг, ишлаб чикариш объектлари ва коммуникацияларнинг хавфсизлигини таъминлаш учун зарур бўлган бошқа ахборотлар;
- ахборот-кутубхона муассасаларининг, архивларнинг, идоравий архивларнинг ва Ўзбекистон Республикаси ҳудудида фаолият кўрсатаётган юридик шахсларга тегишли ахборот тизимларининг очиқ фондларидаги мавжуд маълумотлар.

Давлат хокимияти ва бошқарув органлари, фуқароларнинг ўзини ўзи бошқариш органлари, жамоат бирлашмалари ва бошқа нодавлат нотижорат ташқилотлари жамият манфаатларига тааллуқли воқеалар, фактлар, ҳодисалар ва жараёнлар тўғрисида қонун хужжатларида белгиланган тартибда оммавий ахборот воситаларига хабар бериши шарт.

10-модда. Ахборот беришни рад этиш

Агар сўралаётган ахборот махфий бўлса ёки уни ошкор этиш натижасида шахснинг ҳуқуқлари ва қонуний манфаатларига, жамият ва давлат манфаатларига зарар етиши мумкин бўлса, ахборотни бериш рад этилиши мумкин.

Сўралаётган ахборотни бериш рад этилганлиги тўғрисидаги хабар сўров билан мурожаат этган шахсга сўров олинган санадан эътиборан беш кунлик муддат ичида юборилади.

Рад этиш тўғрисидаги хабарда сўралаётган ахборотни бериш мумкин эмаслиги сабаби курсатилиши керак.

Махфий ахборот мулкдори, эгаси ахборотни сўраётган шахсларни бу ахборотни олишнинг амалдаги чекловлари тўғрисида хабардор этиши шарт

Ахборот берилиши қонунга хилоф равишда рад этилган шахслар, шунингдек ўз сўровига ҳаққоний бўлмаган ахборот олган шахслар ўзларига етказилган моддий зарарнинг ўрни қонунда белгиланган тартибда қопланиши ёки маънавий зиён компенсация қилиниши ҳукуқига эга.

11-модда. Ахборотни муҳофаза этиш

Ҳар қандай ахборот, агар у билан қонунга хилоф равишда муомалада бўлиш ахборот мулкдори, эгаси, ахборотдан фойдаланувчи ва бопща шахсга зарар етказиши мумкин бўлса, муҳофаза этилмоғи керак.

Ахборотни муҳофаза этиш:

- шахс, жамият ва давлатнинг ахборот соҳасидаги хавфсизлигига таадидларнинг олдини олиш;
- ахборотнинг махфийлигини таъминлаш, тарқалиши, ўғирланиши, йўқотилишининг олдини олиш;

ахборотнинг бузиб талқин этилиши ва сохталаштирилишининг олдини олиш мақсадида амалга оширилади.

13-модда. Шахснинг ахборот борасидаги хавфсизлиги

Шахснинг ахборот борасидаги хавфсизлиги унинг ахборотдан эркин фойдаланиши зарур шароитлари ва кафолатларини яратиш, шахсий хаётига тааллуқли сирларини сақдаш, ахборот воситасида қонунга хилоф равишда рухий таъсир кўрсатилишидан ҳимоя қилиш йули билан таъминланади.

Жисмоний шахсларга тааллуқли шахсий маълумотлар махфий ахборот тоифасига киради.

Жисмоний шахснинг розилигисиз унинг шахсий хаётига тааллуқли ахборотни, худди шунингдек шахсий хаётига тааллукли сирини, ёзишмалар, телефондаги сўзлашувлар, почта, телеграф ва бошқа мулоқот сирларини бузувчи ахборотни туплашга, сақдашга, кайта ишлашга, тарқатишга ва ундан фойдаланишга йул қўйилмайди, қонун хужжатларида белгиланган ҳоллар бундан мустасно.

Жисмоний шахслар тўғрисидаги ахборотдан уларга моддий зарар ва маънавий зиён етказиш, шунингдек уларнинг ҳуқуқдари, эркинликлари ва қонуний манфаатлари рўёбга чикарилишига тўсқинлик қилиш мақсадида фойдаланиш тақиқданади.

Фукаролар тўғрисида ахборот олувчи, бундай ахборотга эгалик қилувчи хамда ундан фойдаланувчи юридик ва жисмоний шахслар бу ахборотдан фойдаланиш тартибини бузганлик учун қонунда назарда тутилган тарзда жавобгар бўладилар.

Оммавий ахборот воситалари ахборот манбаини ёки тахаллусини қўйган муаллифни уларнинг розилигисиз ошкор этишга хакди эмас. Ахборот манбаи ёки муаллиф номи фақат суд қарори билан ошкор этилиши мумкин.

14-модда. Жамиятнинг ахборот борасидаги хавфсизлиги

Жамиятнинг ахборот борасидаги хавфсизлигига қуйидаги йўллар билан эришилади:

- демократик фуқаролик жамияти
- асослари ривожлантирилишини, оммавий ахборот эркинлигини таъминлаш;
- қонунга хилоф равишда ижтимоий онгга ахборот воситасида руҳий таъсир курсатишга, уни чалгитишга йул қуймаслик;
- жамиятнинг маънавий, маданий ва тарихий бойликларини, мамлакатнинг илмий ва илмий-техникавий салоҳиятини асраш хамда

ривожлантириш;

- миллий ўзликни англашни издан чиқаришга, жамиятни тарихий ва миллий анъаналар хпмда урф-одатлардан узоқлаштиришга, ижтимоий-сиёсий вазиятни беқарорлаштиришга, миллатлараро ва конфессиялараро тотувликни бузишга қаратилган ахборот экспансиясига қарши харакат тизимини барпо этиш.

15-модда. Давлатнинг ахборот борасидаги хавфсизлиги

Давлатнинг ахборот борасидаги хавфсизлиги қуйидаги йуллар билан таъминланади:

- ахборот сохасидаги хавфсизликка тахдидларга қарши ҳаракатлар юзасидан иктисодий, сиёсий, ташқилий ва бошка тусдаги чора-тадбирларни амалга ошириш;
- давлат сирларини савлаш ва давлат ахборот ресўрсларини улардан рухсатсиз тарзда фойдаланилишидан мухофаза қилиш;
- Ўзбекистон Республикасининг жахон ахборот маконига ва замонавий телекоммуникациялар тизимларига интеграциялашуви;
- Ўзбекистон Республикасининг конституциявий тузумини зўрлик билан ўзгартиришга, худудий яхлитлигини, суверенитетини бузишга, ҳокимиятни босиб олишга ёки қонуний равишда сайлаб қўйилган ёхуд тайинланган хокимият вақилларини хокимиятдан четлатишга ва давлат тузумига қарши бошкача тажовуз қилишга очиқдан-очиқ даъват этишни ўз ичига олган ахборот тарқатилишидан ҳимоя қилиш;
- урушни ва зўравонликни, шафқатсизликни тарғиб қилишни, ижтимоий, миллий, ирқий ва диний адоват уйғотишга қаратилган терроризм ва диний экстремизм ғояларини ёйишни ўз ичига олган ахборот тарқатилишига қарши ҳаракатлар қилиш.

16-модда. Ахборот эркинлиги принциплари ва кафолатлари тўғрисидаги қонун ҳужжатларини бузганлик учун жавобгарлик

- Ахборот эркинлиги принциплари ва кафолатлари тўғрисидаги қонун ҳужжатларини бузганликда айбдор шахслар белгиланган тартибда жавобгар бўладилар.

Амалий вазифалар:

1. Кибержиноятчилик тушунчасига синквейн ёзинг.
2. Киберҳуқуқ тушунчасига синквейн ёзинг.
3. Киберэтика тушунчасига синквейн ёзинг.
4. Кибержиноятчилик, Киберҳуқуқ, Киберэтика тиушунчаларини таққосланг.
5. Молиявий йўналтирилган кибер жиноятга мисоллар келтиринг.
6. Шахсий дахлсизликка алоқадор кибер жиноятга мисоллар келтиринг.
7. Кибержиноятчиликни аниқлаш усуллари ва алгоритмларини санаб беринг.
8. Image Forensic Search System дастури нима учун керак?

Адабиётлар ва интеренет сайтлари:

1. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / Под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. 224 с.
2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. 2-е изд., испр. и доп. 2017 г. 338 стр.

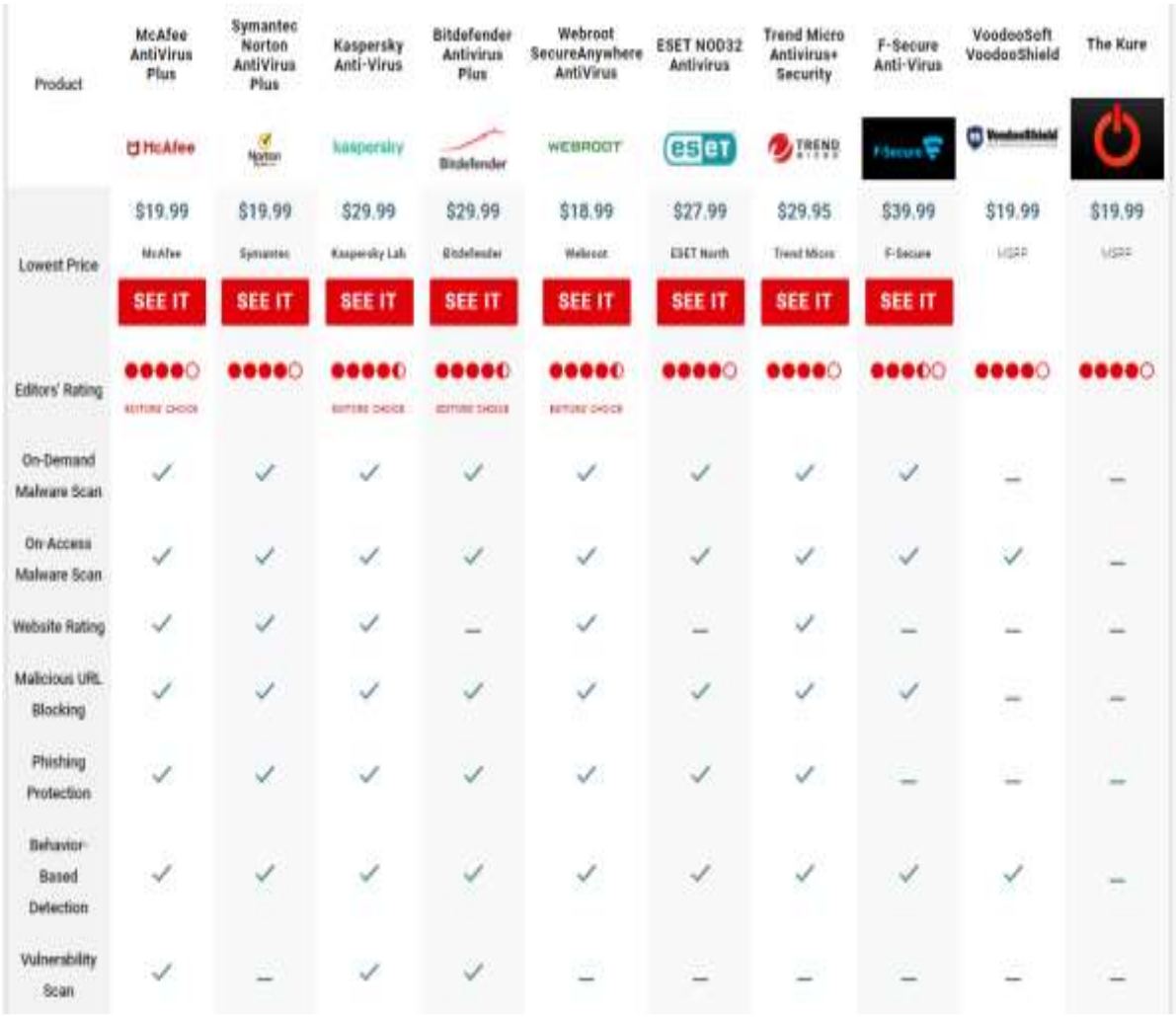
V БЎЛИМ

КЕЙСЛАР БАНКИ

V. КЕЙСЛАР БАНКИ

1-КЕЙС

1. **Антивирусларга оид статистикани қўйидаги сайт орқали ўрганинг:**
https://www.pcmag.com/roundup/256703/the-best-antivirus-protection



Product	McAfee AntiVirus Plus	Symantec Norton AntiVirus Plus	Kaspersky Anti-Virus	Bitdefender Antivirus Plus	Webroot SecureAnywhere AntiVirus	ESET NOD32 Antivirus	Trend Micro Antivirus+ Security	F-Secure Anti-Virus	VoodooSoft VoodooShield	The Kure
Lowest Price	$19.99	$19.99	$29.99	$29.99	$18.99	$27.99	$29.95	$39.99	$19.99	$19.99
	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT		
Editors' Rating	●●●●○	●●●●○	●●●●◐	●●●●◐	●●●●◐	●●●●○	●●●●○	●●●◐○	●●●●○	●●●●○
On-Demand Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	–	–
On-Access Malware Scan	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Website Rating	✓	✓	✓	–	✓	–	✓	–	–	–
Malicious URL Blocking	✓	✓	✓	✓	✓	✓	✓	✓	–	–
Phishing Protection	✓	✓	✓	✓	✓	✓	✓	–	–	–
Behavior-Based Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	–
Vulnerability Scan	✓	–	✓	✓	–	–	–	–	–	–

2. **Қўйидаги саволларжа жавоб топинг:**

1) Қандай антивирус дастурлари мавжуд?
2) Қандай антивирус дастурларидан фойдаланасиз?
3) Қандай антивирус дастури сизнинг компьютеризга ўрнатилган?
4) Қандай қилиб компьютеризни вируслардан ҳимоялаш мумкин?

3. **Киберхавфсизлик стратегиясини тузинг.**

VI БЎЛИМ

ГЛОССАРИЙ

VIII. ГЛОССАРИЙ

Тушунча ўзбек тилида	Тушунчанинг таърифи	Тушунча инглиз тилида
Ахборотнинг ҳимояси	бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёни	**Information protection**
киберхавфсизлик	қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқариш	**cybersecurity**
Киберхавфсизли (Cisco ташкилоти таърифи)	тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти	**Cybersecurity (Cisco definition)**
Маълумотлар хавфсизлиги	маълумотларни сақлашда, қайта ишлашда ва узатишда ҳимояни таъминлашни мақсад қилади	**Data security**
Дастурий таъминотлар хавфсизлиги	фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи дастурий таъминотларни ишлаб чиқиш ва фойдаланиш жараёнига эътибор қаратади	**Software security**
Ташкил этувчилар хавфсизлиги	катта тизимларда интеграллашган ташкил этувчиларни лойиҳалаш, сотиб олиш, тестлаш, анализ қилиш ва техник хизмат кўрсатишга эътибор қаратади	**Organizer security**
Алоқа хавфсизлиги	ташкил этувчилар ўртасидаги алоқани ҳимоялашга этибор қаратиб, ўзида физик ва мантиқий уланишни бирлаштиради.	**Communication security**
Тизим хавфсизлиги	ташкил этувчилар, уланишлар ва дастурий таъминотдан иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади	**System security**
Инсон хавфсизлиги	киберхавфсизлик билан боғлиқ инсон ҳатти ҳаракатларини ўрганишдан ташқари, ташкилотлар (масалан, ходим) ва шахсий ҳаёт шароитида шахсий маълумотларни ва шахсий ҳаётни ҳимоя қилишга эътибор қаратади	**Human security**

Ташкилот хавфсизлиги	ташкилотни киберхавфсизлик таҳдидларидан ҳимоялаш ва ташкилот вазифасини муваффаққиятли бажаришини мададлаш учун рискларни бошқаришга эътибор қаратади	**Organizational security**
Жамоат хавфсизлиги	у ёки бу даражада жамиятда таъсир кўрсатувчи киберхавфсизлик омилларига эътибор қаратади	**Public safety**
Киберхавфсизлик концепцияси	ахборот хавфсизлиги муаммосига расмий қабул қилинган қарашлар тизими ва уни замонавий тенденцияларни ҳисобга олган ҳолда ечиш йўллари	**The concept of cybersecurity**
Киберхавфсизлик сиёсати	ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режаси	**Cybersecurity policy**
Риск	ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради	**Risk**
Рискни аниқлаш тадбирлари	Рискларни аниқлаш; рискларни идентификация қилиш; рискларни таҳлил қилиш; рискларни баҳолаш.	**Risk detection measures**
Рискларни аниқлаш	ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни	**Risk identification**

	баҳолаш мезонлари бўйича уларни таснифлайди	
Рискларни идентификация қилишдан мақсад	потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади.	**The purpose of risk identification**
Ҳодиса	шахс ёки ишчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир	**event**
Нормал ҳодиса	критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.	**Normal event**
Ҳодисаларни кенгайиши ва кўпайиши (Эскалация)	Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.	**Expansion and multiplication of events (Escalation)**
Авариявий ҳодиса	шахс хавфсизлиги ва соғлигига таъсир кўрсатади.	**An accident.**
Инцидент	стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.	**Incident**
Хавфсизлик инциденти координатори	инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир.	**Security Incident Coordinator**
Инцидентни тергов қилиш	инцидент ҳолатини тергов қилиш ҳаракати	**Investigate the incident**
Инцидентга жавоб қайтариш	хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир	**Responding to an incident**
Инцидент бошқарувчисини вазифалари ва мажбуриятлари	– муносиб ваколатлардан фойдаланиш учун ҳар қандай авария / носозликларни билиш; – етарли ахборот йиғиш ва тизимни таҳлил этиш учун қайта тиклайдиган командани шакллантириш; – инцидентни умумий ҳолатини сақлаш; – функционал имкониятларни	**Duties and responsibilities of the incident manager**

	билиш (Core Network); – командани юқори сатҳга кўтариш (приоритет бериш) учун қўлланмадан фойдаланиш.	
ахборот хавфсизлиги инцидентларни бошқариш жараёни	• компьютер инциденти ҳақида ахборот олиш; • қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш; • ҳолатни таҳлил этиш; • сабабларни аниқлаш; • профилактик тадбирлар ўтказиш	**information security incident management process**
Инцидентларини бошқариш жараёни самарадорлиги	❑ ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши; ❑ инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги; ❑ олинган натижаларнинг ҳақиқийлиги.	**The effectiveness of the incident management process**
инцидентини бошқариш тизими архитектураси	1. Интеграллашган платформа. 2. Аудит ва мониторингни аппарат-дастурий воситалари. 3. Ахборотни ҳимоялашнинг аппарат-дастурий воситалари. 4. Ахборот хавфсизлиги инцидентлари ҳақида ахборот омбори. 5. Ҳисоботларни генерациялаш воситалари ва аналитик асбоблар. 6. Воситаларни бошқариш ва интерфейсни тўғрилаш.	**incident management system architecture**
Кодлаштириш	ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёни	**Coding**
Калит	матнни шифрлаш ва шифрини очиш учун керакли ахборот.	**The key**
Криптоанализ	калитни билмасдан шифрланган матнни очиш имкониятларини ўрганади.	**Cryptanalysis**
Симметрик шифр	маълумотни шифрлаш ва дешифрлаш учун бир хил калитдан фойдаланилади	**Symmetric cipher**
Ассимметрик шифр	шифрлаш ва дешифрлаш учун иккита калитдан фойдаланилади	**Asymmetric cipher**
стеганографиянинг	махфий маълумотларнинг	**the basic idea of**

асосий ғояси	мавжудлиги ҳақидаги шубҳани олдини олиш	**steganography**
Хэш функция	ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ёки байт бирликларида) қийматга ўтказувчи функция	**Hash function**
Хеш функция хусусиятлари	a) Бир хил кириш ҳар доим бир хил чиқишни (хэш қиймат деб аталади) тақдим этади. b) Бир қанча турли киришлар бир хил чиқишни тақдим этмайди. c) Чиқиш қийматдан кирувчи қийматни ҳосил қилишнинг имконияти мавжуд эмас (бир томонламалик). d) Кириш қийматини ўзгариши чиқишдаги қийматни ҳам ўзгаришига олиб келади.	**Hash function properties**
заифлик	тизимнинг кам ҳимояланган ёки очиқ жойини белгилашда ишлатилади.	**weakness**
Заифликларни аниқловчи ташкилотлар	COAST лабораторияси. Protection Analysis Project. RISOS. Internet Security Systems.	**Weakness identification organizations**
Заифликлар классификацияси	Операцион тизим заифликлари. Иловалар заифликлари. Тармоқ заифликлари. Физик заифликлар.	**Classification of vulnerabilities**
Тармоқ сканерлари	масофавий ёки локал ташхис дастури бўлиб, у тармоқнинг турли элементларида ҳар хил заифликларни аниқлайди	**Network scanners**
Илова сканерлари	аниқ МББТ, Web-браузерлари ва бошқа амалий тизимларга мўлжалланган	**Application scanners**
Компьютер вируслари	компьютер тизимларида тарқалиш ва ўз-ўзидан қайтадан тикланиш (репликация) хусусиятларига эга бўлган бажарилувчи ёки шархланувчи кичик дастурлардир	**Computer viruses**
Компьютер вируслари классификацияси	• яшаш муҳити бўйича; • яшаш муҳитининг захарланиши бўйича; • зараркунандалик таъсирнинг хавфи даражаси бўйича;	**Classification of computer viruses**

	• ишлаш алгоритми бўйича.	
Яшаш муҳити бўйича компьютер вируслари	• тармоқ вируслари; • файл вируслари; • юклама вируслар; • комбинацияланган вируслар.	**Computer viruses in the living environment**
Файл вируслари	бажарилувчи файлларга турли усуллар билан кирити лади (энг кўп тарқалган вируслар хили), ёки файл йўлдошларни (компанъон вируслар) яратади ёки файлли тизимларни (linkвируслар) ташкил этиш хусусиятидан фойдаланади.	**File viruses**
Юклама вируслар	ўзини дискнинг юклама секторига (boot секторига) ёки винчестернинг тизимли юкловчиси (Master Boot Record) бўлган сек торга ёзади. Юклама вируслар тизим юкланишида бошқаришни олувчи дастур коди вазифасини бажаради.	**Download viruses**
Макровируслар	ахборотни ишловчи замонавий тизимларнинг макро дастурларини ва файлларини, хусусан MicroSoft Word, MicroSoft Excel ва ҳ. каби оммавий муҳаррирларнинг файл хужжатларини ва электрон жадвалларини заҳарлайди.	**Macroviruses**
Тармоқ вируслари	ўзини тарқатишда компъютер тармоқлари ва электрон почта протоколлари ва командаларидан фойдаланади. Баъзида тармоқ вирусларини "қурт" хилидаги дастурлар деб юритишади. Тармоқ вируслари Internet қуртларга (Internet бўйича тарқалади), IRCқуртларга (чатлар, Internet Relay Chat) бўлинади	**Network viruses**
Яшаш муҳитининг захарланиши усули бўйича компьютер вируслари классификацияси	• резидент; • резидент бўлмаган;	**Classification of computer viruses by the method of habitat poisoning**
Резидент вируслар	фаоллашганларидан сўнг тўлалигича ёки қисман яшаш муҳитидан (тармоқ, юклама сектори, файл) ҳисоблаш машинасининг асосий хотирасига кўчади.	**Resident viruses**
Резидент бўлмаган вируслар	фақат фаоллашган вақтларида ҳисоблаш машинасининг асосий	**Non-resident viruses**

	хотирасига тушиб, захарлаш ва зараркунандалик вазифаларини бажаради.	
Фойдаланувчининг информацион ресурслари учун хавф даражаси бўйича компьютер вируслари классификацияси	• безиён вируслар; • хавфли вируслар; • жуда хавфли вируслар;	**Classification of computer viruses according to the level of risk for user information resources**
Вируслар-«йўлдошлар»	файлларни ўзгартирмайди. Унинг таъсир механизми бажарилувчи файлларнинг нусҳаларини яратишдан иборатдир	**Viruses - "satellites"**
вируслар-«қуртлар» (worm).	тармоқ орқали ишчи станцияга тушади, тармоқнинг бошқа абонентлари бўйича вирусни жўнатиш адресларини ҳисоблайди ва вирусни узатишни бажаради	**viruses - "worms".**
Алгоритмларнинг мураккаблиги, мукаммалик даражаси ва яшириниш хусусиятлари бўйича яшаш маконини ўзгартирадиган вируслар	• талаба вируслар; • «стелс» вируслар (кўринмайдиган вируслар); • полиморф вируслар.	**Viruses that change the living space in terms of the complexity of the algorithms, the level of perfection, and the features of the concealment**
талаба вируслар	одатда, резидент бўлмаган вируслар қаторига киради, уларда кўпинча хатоликлар мавжуд бўлади, осонгина танилади ва йўқотилади	**student viruses**
«стелс» вируслар (кўринмайдиган вируслар)	операцион тизимнинг шикастланган файлларга мурожаатларини ушлаб қолиш йўли билан ўзини яшаш маконидагилигини яширади ва операцион тизимни ахборотнинг шикастланмаган қисмига йўналтиради	**"Stealth" viruses (invisible viruses)**
полиморф вируслар	доимий танитувчи гурухлар-сигнатураларга эга бўлмайди	**polymorphic viruses**
Компьютер тизимларида вирусларни аниқлаш методлари	• сканерлаш; • ўзгаришларни билиб қолиш; • эвристик тахлил; • резидент қоровуллардан фойдаланиш;	**Methods for detecting viruses in computer systems**

	• программани вакцинациялаш; вируслардан аппарат-программ ҳимояланиш	
Риск номақбул воқеа	ҳодисадан келиб чиқадиган оқибатлар ва воқеа-ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди.	**Risk is an undesirable event**
Рискни аниқлаш тадбирлари	Рискларни аниқлаш; рискларни идентификация қилиш; рискларни таҳлил қилиш; рискларни баҳолаш.	**Risk detection measures**
Рискларни аниқлаш	ахборот активларининг аҳамиятини белгилайди, мавжуд (ёки мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва ниҳоят, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди	**Risk identification**
Рискларни идентификация қилишдан мақсад	потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади.	**The purpose of risk identification**
Идентификация	шахсни кимдир деб даво қилиш жараёни	**Identification**
Аутентификация	фойдаланувчини (ёки бирор томонни) тизимдан фойдаланиш учун рухсати мавжудлигини аникдаш жараёни	**Authentication**
Авторизация	идентификация, аутентификация жараёнларидан ўтган фойдаланувчи учун тизимда бажариши мумкин бўлган амалларга рухсат бериш жараёни	**authorization**
Пароль	фақат фойдаланувчига маълум ва бирор тизимда аутентификация жараёнидан ўтишни таъминловчи бирор ахборот	**password**
Нусҳа яратиш	Ахборот ташувчиларда маълумотлар нусҳасини яратиш жараёни	**backup**

Маълумотларни қайта тиклаш	Ахборот ташувчиларда маълумотларни қайта тиклаш жараёни	**data recovery**
Тшлиқ нусҳа яратиш	Тизимни ва ундаги барча файлларни нусҳасини яратиш жараёни	**Full backup**
Дифференциал нусҳа яратиш	Ўзгартирилган файлларни нусҳасини олиш жараёни	**Differential backup**
Тармоқ ҳужуми	Компьютер тармоқлари орқали ташкилотнинг тизимига рухсатсиз таъсир кўрсатиш	**Network attack**
Ҳужум	заифлик орқали ахборот тизимлари хавфсизлигини бузишга оширилган ҳаракат	**Attack**
Заифлик	тизим хавфсизлигини бузувчи ва ошкор бўлмаган ҳодисаларга олиб келувчи камчилик, лойиҳалашдаги ёки амалга оширишдаги хатолик.	**Weakness**
web-ҳужумлар	web технологиялар орқали ташкилотнинг тизимига рухсатсиз таъсир кўрсатиш	**web attacks**
вируслар	ўзини ўзи кўпайтирадиган программа бўлиб, ўзини бошқа программа ичига, компьютернинг юкланувчи секторига ёки ҳужжат ичига бириктиради.	**viruses**
троян отлари	бир қарашда яхши ва фойдали каби кўринувчи дастурий восита сифатида кўринсада, яширинган зарарли коддан иборат бўлади.	**Trojan horses**
Adware	маркетинг мақсадида ёки рекламани намойиш қилиш учун фойдаланувчини кўриш режимини кузутиб борувчи дастурий таъминот.	**Adware**
Spyware	фойдаланувчи маълумотларини қўлга киритувчи ва уни ҳужумчига юборувчи дастурий код.	**Spyware**
Rootkits	ушбу зарарли дастурий восита операцион тизим томонидан аниқланмаслиги учун маълум ҳаракатларини яширади.	**Rootkits**
Backdoors	зарарли дастурий кодлар бўлиб, ҳужумчига аутентификацияни амалга оширмасдан айланиб ўтиб тизимга кириш имконини беради, маслан, администратор паролисиз имтиёзга эга бўлиш.	**Backdoors**
мантиқий бомбалар	зарарли дастурий восита бўлиб,	**logical bombs**

	бирор мантиқий шарт қаноатлантирилган вақтда ўз ҳаракатини амалга оширади.	
Ботнет	Интернет тармоғидаги обрўсизлантирилган компьютерлар бўлиб, тақсимланган ҳужумларни амалга ошириш учун ҳужумчи томонидан фойдаланилади.	**Botnet**
Ransomware	мазкур зарарли дастурий таъминот қурбон компьютерида мавжуд қимматли файлларни шифрлайди ёки қулфлаб қўйиб, тўлов амалга оширилишини талаб қилади.	**Ransomware**
Киберэтика	Компьютер ва компьютер тармоқларида одамларнинг этикаси	**Cybernetics**
Киберхавфсизлик	Компьютер, дастурлар ва тармоқлар хавфсизлиги	**Cybersecurity**
киберҳужум	Компьютер тизимларига рухсатсиз таъсир кўрсатиш	**cyber attack**
фишинг	Ташкилот ва одамларнинг маҳсус ва шаҳсий маълумотларини олишка қаратилган интернет-атакаси	**fishing**

VII БЎЛИМ

АДАБИЁТЛАР РЎЙХАТИ

VII. АДАБИЁТЛАР РЎЙХАТИ

I. Ўзбекистон Республикаси Президентининг асарлари

1. Мирзиёев Ш.М. Буюк келажагимизни мард ва олижаноб халқимиз билан бирга қурамиз. – Т.: “Ўзбекистон”, 2017. – 488 б.
2. Мирзиёев Ш.М. Миллий тараққиёт йўлимизни қатъият билан давом эттириб, янги босқичга кўтарамиз. 1-жилд. – Т.: “Ўзбекистон”, 2017. – 592 б.
3. Мирзиёев Ш.М. Халқимизнинг розилиги бизнинг фаолиятимизга берилган энг олий баҳодир. 2-жилд. Т.: “Ўзбекистон”, 2018. – 507 б.
4. Мирзиёев Ш.М. Нияти улуғ халқнинг иши ҳам улуғ, ҳаёти ёруғ ва келажаги фаровон бўлади. 3-жилд.– Т.: “Ўзбекистон”, 2019. – 400 б.
5. Мирзиёев Ш.М. Миллий тикланишдан – миллий юксалиш сари. 4-жилд.– Т.: “Ўзбекистон”, 2020. – 400 б.

II. Норматив-ҳуқуқий ҳужжатлар

6. Ўзбекистон Республикасининг Конституцияси. – Т.: Ўзбекистон, 2018.
7. Ўзбекистон Республикасининг 2020 йил 23 сентябрда қабул қилинган “Таълим тўғрисида”ги ЎРҚ-637-сонли Қонуни.
8. Ўзбекистон Республикаси Президентининг 2015 йил 12 июнь “Олий таълим муасасаларининг раҳбар ва педагог кадрларини қайта тайёрлаш ва малакасини ошириш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-4732-сонли Фармони.
9. Ўзбекистон Республикаси Президентининг 2017 йил 7 февраль “Ўзбекистон Республикасини янада ривожлантириш бўйича Ҳаракатлар стратегияси тўғрисида”ги 4947-сонли Фармони.
10. Ўзбекистон Республикаси Президентининг 2017 йил 20 апрель "Олий таълим тизимини янада ривожлантириш чора-тадбирлари тўғрисида”ги ПҚ-2909-сонли Қарори.
11. Ўзбекистон Республикаси Президентининг 2018 йил 21 сентябрь “2019-2021 йилларда Ўзбекистон Республикасини инновацион ривожлантириш стратегиясини тасдиқлаш тўғрисида”ги ПФ-5544-сонли Фармони.
12. Ўзбекистон Республикаси Президентининг 2018 йил 19 февраль “Ахборот технологиялари ва коммуникациялари соҳасини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-5349-сонли Фармони.
13. Ўзбекистон Республикаси Президентининг 2019 йил 27 май “Ўзбекистон Республикасида коррупцияга қарши курашиш тизимини янада такомиллаштириш чора-тадбирлари тўғрисида”ги ПФ-5729-сон Фармони.
14. Ўзбекистон Республикаси Президентининг 2019 йил 17 июнь “2019-2023 йилларда Мирзо Улуғбек номидаги Ўзбекистон Миллий университетида талаб юқори бўлган малакали кадрлар тайёрлаш тизимини тубдан такомиллаштириш ва илмий салоҳиятини ривожлантири чора-тадбирлари тўғрисида”ги ПҚ-4358-сонли Қарори.

15. Ўзбекистон Республикаси Президентининг 2019 йил 27 август “Олий таълим муассасалари раҳбар ва педагог кадрларининг узлуксиз малакасини ошириш тизимини жорий этиш тўғрисида”ги ПФ-5789-сонли Фармони.

16. Ўзбекистон Республикаси Президентининг 2019 йил 8 октябрь “Ўзбекистон Республикаси олий таълим тизимини 2030 йилгача ривожлантириш концепциясини тасдиқлаш тўғрисида”ги ПФ-5847-сонли Фармони.

17. Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2019 йил 23 сентябрь “Олий таълим муассасалари раҳбар ва педагог кадрларининг малакасини ошириш тизимини янада такомиллаштириш бўйича қўшимча чора-тадбирлар тўғрисида”ги 797-сонли Қарори.

18. Ўзбекистон Республикаси Президентининг 2019 йил 21 май “«Электрон ҳукумат» тизими доирасида ахборот-коммуникация технологиялари соҳасидаги лойиҳаларни ишлаб чиқиш ва амалга ошириш сифатини яхшилаш чора-тадбирлари тўғрисида”ги ПҚ-4328-сонли Қарори.

19. Ўзбекистон Республикаси Президентининг 2020 йил 5 октябрь “Рақамли Ўзбекистон-2030” Стратегиясини тасдиқлаш ва уни самарали амалга ошириш чора-тадбирлари тўғрисида”ги ПФ-6079-сонли Фармони.

Ш. Махсус адабиётлар

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357

2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.

3. Introduction to Cyber Security. Dr. Jeetendra Pande. Uttarakhand Open University, 2017. – P.152.

4. Ганиев С.К., Кучкаров Т.А. Тармоқ хавфсизлиги. Ўқув қўлланма. – Т.: Алоқачи, 2019. - 140 б.

5. Юсупов С.Ю., Ганиев А.А. Взлом и защита компьютерных систем и сетей. – Т.: Алоқачи, 2019. - 232 б.

IV. Интернет сайтлар

20. http://edu.uz – Ўзбекистон Республикаси Олий ва ўрта махсус таълим вазирлиги

21. http:// www.mitc.uz - Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги

22. http://lex.uz – Ўзбекистон Республикаси Қонун ҳужжатлари маълумотлари миллий базаси

23. http://bimm.uz – Олий таълим тизими педагог ва раҳбар кадрларини қайта тайёрлаш ва уларнинг малакасини оширишни ташкил этиш бош илмий-методик маркази

24. http://ziyonet.uz – Таълим портали ZiyoNET

25. http:// www.tuit.uz - Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети
26. https://ichip.ru/sovety/chto-takoe-kompyuternyjj-virus-prosto-o-slozhnom-223382
27. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

РЕЦЕНЗИЯ

на учебно-методический комплекс, составленный Ш.Гуломовым по модулю «Кибербезопасность» для курсов повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Информационные системы и технологии»

Учебно-методический комплекс по модулю «Кибербезопасность» составлен для курсов повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Информационные системы и технологии» и содержит в себе программу курсов, рекомендованные педагогические технологии, тексты лекций, материалы для практических занятий, кейсы, глоссарий и список рекомендованной литературы и интернет сайтов.

Программа модуля соответствует содержанию типовой программы данного направления и включает в себя введение, цели и задачи модуля, требования к знаниям, умениям, навыкам и компетенциям слушателей, рекомендации к проведению занятий, содержание и разбивка часов по темам и список рекомендованной литературы и интернет-сайтов. В программе и в учебно-методическом комплексе раскрываются такие темы, как: функции и задачи кибербезопасности, политика кибербезопасности и управление ею, управление рисками, атакующие инциденты и реакция на них, основные понятия криптографии, уязвимости сетевой безопасности и угрозы для них, компьютерные вирусы, вредоносное ПО и механизмы их защиты, риски и методы оценки рисков, идентификация, аутентификация и авторизация, восстановление данных и устойчивость, сетевые атаки, веб-атаки, программные атаки, вредоносное ПО, киберпреступность, киберпреступность и кибербезопасность.

Разработанный автором учебно-методический комплекс соответствует содержанию типовой программы данного направления, часы распределены соответственно часам, указанным в учебном плане. В нем приведены основные материалы по данному модулю, которые соответствуют современному состоянию развития информационно-коммуникационных технологий, в частности, информационной безопасности и кибербезопасности.

Таким образом, учебно-методический комплекс по модулю «Кибербезопасность» может быть рекомендован к использованию на курсах повышения квалификации и переподготовки педагогических кадров высших образовательных учреждений направления «Информационные системы и технологии» и его можно рекомендовать к публикации.

Вр.и.о. исполнительного директора
Совместного Белорусско-узбекского
межотраслевого института прикладных
технических квалификаций,
доктор педагогических наук (DSc) **Я.Исмадияров**

ОЛИЙ ТАЪЛИМ МУАССАСАЛАРИ ПЕДАГОГ КАДРЛАРИНИ ҚАЙТА ТАЙЁРЛАШ ВА МАЛАКАСИНИ ОШИРИШ КУРСИ УЧУН ТАЙЁРЛАНГАН "КИБЕРХАВФСИЗЛИК" МОДУЛИНИНГ ЎҚУВ-УСЛУБИЙ МАЖМУАСИГА

Т А Қ Р И З

Ўқув-услубий мажмуа "Киберхавфсизлик" модули бўйича қайта тайёрлаш ва малака ошириш тингловчилари учун яратилган. "Киберхавфсизлик" модулининг мақсади киберхавфсизлик бўйича олий таълим муассасалари педагог кадрларининг касбий компетентлигини ошириш, модулнинг вазифалари эса олий таълим муассасалари педагог кадрларида киберхавфсизлик ҳақида назарий ва амалий билимларни, кўникма ва малакаларни шакллантиришдан иборат деб белгиланган. Қайта тайёрлаш ва малака ошириш йўналишининг ўзига хос хусусиятлари ҳамда долзарб масалаларидан келиб чиққан ҳолда ўқув-услубий мажмуада тингловчиларнинг ушбу модул доирасидаги билим, кўникма, малака ҳамда компетенцияларига қўйиладиган талаблар асосида ўқув-услубий мажмусида берилган материаллар ушбу максадга йўналтирилиб, ахборот-коммуникация технологиялар, хборот хавфсизлиги ва киберхавфсизлик соҳасидаги ҳозирги кундаги замонавий усулларини ўрганиш, уларни таълим жараёнига қўллаш бўйича назарий ва амалий маълумотлар келтирилган.

Ўқув-услубий мажмуа доирасида берилаётган мавзулар таълим соҳаси бўйича педагог кадрларни қайта тайёрлаш ва малакасини ошириш мазмуни, сифати ва уларнинг тайёргарлигига қўйиладиган умумий малака талаблари, ўқув режалари ва дастурлари асосида шакллантирилган бўлиб, бу орқали олий таълим муассасалари педагог кадрларининг соҳага оид замонавий таълим ва инновация технологиялари, илғор хорижий тажрибалардан самарали фойдаланиш, киберхавфссизлик усул ва воситаларини амалиётга кенг татбиқ этиш билан боғлиқ компетенцияларга эга бўлишлари таъминланади.

Умуман олганда, "Киберхавфсизлик" модули бўйича яратилган ўқув-услубий мажмуа барча талабларга жавоб беради ва уни ўқув жараёнида қўллаш ва чоп этиш учун тавсия этиш мумкин.

Муҳаммад Ал-Хоразмий номидаги
ТАТУ "Ахборот технологиялари" кафедраси
мудири, профессор **Х.Зайнидинов**