Н.М.ТУРАЕВА

КИБЕРХАВФСИЗЛИК

ЧИРЧИҚ-2023

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ЁШЛАР СИЁСАТИ ВА СПОРТ ВАЗИРЛИГИ

ЎЗБЕКИСТОН ДАВЛАТ ЖИСМОНИЙ ТАРБИЯ ВА СПОРТ УНИВЕРСИТЕТИ

Н.М.ТУРАЕВА

КИБЕРХАВФСИЗЛИК

Ўзбекистон давлат жисмоний тарбия ва спорт университети ўқув-услубий Кенгашининг 2023-йил 29- мартдаги 3-сонли йиғилиш баённомасига асосан услубий қўлланма сифатида нашрга тавсия этилган

ЧИРЧИҚ-2023

Муаллиф: - **Тураева Насиба Мирхамидовна** -ЎзДЖТСУ “Спорт ҳуқуқи, ижтимоий ва табиий-илмий фанлар” кафедраси ўқитувчиси.

Киберхавфсизлик *услубий қўлланма /;-Ч.: “Ўзбекистон давлат жисмоний тарбия ва спорт университети нашрёти”, 2023.-74 б.*

Тақризчилар: - **Акбаров Ахматжон** - ЎзДЖТСУ “Спорт ҳуқуқи, ижтимоий ва табиий-илмий фанлар” кафедраси профессори, физика-математека фанлари номзоди.
Боймуродов Адхам Хушимқулович - п.ф.б.ф.д (PhD), Чирчиқ давлат педагогика университети “Информатика ва ахборот технологиялари” кафедраси мудири.

Услубий қўлланма “Киберхавфсизлик” модули бўйича тайёрланган “Киберспорт” йўналишида таҳсил оладиган талабалар учун яратилган. “Киберхавфсизлик” модулининг мақсади киберспорт йўналиши бўйича олий таълим муассасаларини тамомлаган кадрларнинг касбий компетентлигини ошириш, модулнинг вазифалари эса киберхавфсизлик ҳақида назарий ва амалий билимларни, кўникма ва малакаларни шакллантиришдан иборат деб белгиланган.

“Киберспорт” йўналишининг ўзига хос хусусиятлари, ҳамда ахборот хавфсизлигининг долзарб масалаларидан келиб чиққан ҳолда, услубий қўлланмада талабаларнинг ушбу модуль доирасида билим, кўникма, малака, ҳамда компетенцияларига қўйиладиган талаблар асосида услубий қўлланмада берилган материаллар ушбу мақсадларга йўналтирилиб, ахборот-коммуникация технологиялари, ахборот хавфсизлиги ва киберхавфсизлик соҳасидаги ҳозирги кундаги замонавий усулларини ўрганиш, уларни таълим жараёнига қўллаш бўйича назарий ва амалий маълумотлар келтирилган.

МУНДАРИЖА

КИРИШ

Киберхавфсизлик киберспорт ўйинларида энг муҳим устуворликлардан биридир. Маълумот узатиш тармоқларида компьютер хавфсизлиги билан боғлиқ муаммолар мавжуд. Хакерлар киберспорт ўйинчиларининг аккаунтларига ва шахсий ҳисоб маълумотларига осонгина киришлари мумкин. Кибержиноятчилардан ҳимоя қилиш учун тармоқни фаол ҳимоя қилиш керак, бунинг учун киберспортда компютер киберхавфсизлиги бўйича билимга эга мутахассисларни тайёрлаш керак.

Президент томонидан 15.04.2022 йилдаги «Киберхавфсизлик тўғрисида»ги ЎРҚ-764-сон Қонун имзоланган. Қонунда киберхавфсизликни таъминлашнинг қуйидаги асосий принциплари белгиланган: қонунийлик; кибермаконда шахс, жамият ва давлат манфаатларини ҳимоя қилишнинг устуворлиги; киберхавфсизлик соҳасини тартибга солишга нисбатан ягона ёндашув; киберхавфсизлик тизимини яратишда маҳаллий ишлаб чиқарувчилар иштирокининг устуворлиги; Ўзбекистон Республикасининг киберхавфсизликни таъминлашда халқаро ҳамкорлик учун очиқлиги.

Киберхавфсизлик соҳасидаги ягона давлат сиёсатини Ўзбекистон Республикаси Президенти белгилайди. Ўз навбатида, Ўзбекистон Республикаси Давлат хавфсизлик хизмати киберхавфсизлик соҳасидаги ваколатли давлат органидир. Киберхавфсизлик субъектлари томонидан киберхавфсизлик ҳодисаларига нисбатан чоралар кўриш қуйидаги шаклларда амалга оширилиши мумкин: дастурий таъминотдаги ва қурилмалардаги заифликларни ҳамда хатоликларни бартараф этиш; зарарли дастурларни йўқ қилиш, уларнинг тарқалишини чеклаш, киберҳужумлар манбаини техник жиҳатдан чеклаш; ахборотлаштириш объектларини мавжуд кибертаҳдидлардан ажратиб қўйиш; ҳуқуқни муҳофаза қилувчи органларга киберхавфсизлик ҳодисалари тўғрисида маълумотлар тақдим этиш.

Ушбу муҳим талаблардан келиб чиққан ҳолда, ушбу услубий қўлланма Киберспорт йўналишида таълим олувчи талабаларга ёрдамчи кўрсатма бўла олади.

I-БОБ

1.1. Рисклар ва рискларни баҳолаш усуллари

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

Бундан танқари, рискни қуйидагича тушуниш мумкин:

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

Риск бу - манбага зарар келтирадиган ички ѐки танқи заифлик таъсиридатаҳдид қилиш эҳтимоли.

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

Риск, таҳдид, заифлик ва таъсир ўртасидаги боғланиш қуйидагича:

$$Риск = Таҳдид \times Заифлик \times Таъсир$$

Ҳодисанинг ахборот активига таъсири бу – активдаги ѐки манфаатдортомонлар учун активнинг қийматидаги заифликнинг натижаси.

АТ риски қуйидагича кенгайтирилиши мумкин:

$$РИСК = Таҳдид \times Заифлик \times Актив\ қиймати$$

Риск қуйидаги икки факторнинг мужассамлашганидир:

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

Рискнинг даражалари

1. Рисклар тизимда кутилаѐтган таъсирига боғлиқ ҳолда турли сатҳлардагуруҳланади.
2. Рискларнинг таъсир даражаси активнинг ва таъсир қилган ресурсларқиймати ва зарарнинг жиддийлигига боғлиқ бўлади.

Риск даражаси	Ҳаракати
	Рискларга қарши зудликда чора кўриш зарур

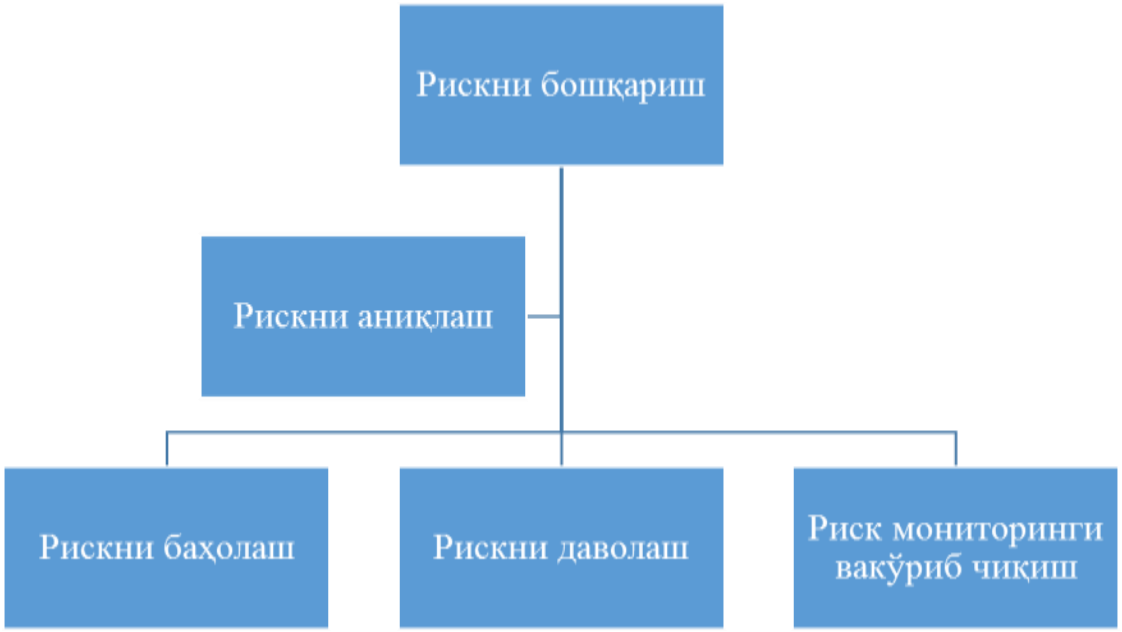
Юқори	Рискни етарлиича паст даражагача тушириш учун назоратлашвоситаларини аниқлаш ва ўрнатиш керак.
	Зидлик билан чора кўриш талаб этилмасада, қисқа вақтдақарши
Ўрта	Ҳаракатларни қўллаш зарур;
	Рискни етарлиича паст даражагача тушириш учун имконборича назоратни амалга ошириш керак.
Қуйи	Риск таъсирини камайтириш учун профилатика чораларинико‘риш 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 амалгаоширилган жорий муҳитни тушунади.

Рискларнисанаш

- 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 жараèн бўлиб, бу ҳимоя чораларини ўрнатишдан кейин ҳолат ўзгаришига асосланади.
- Рискларни баҳолашда риск қийматлари сон ва сифатга кўра баҳоланишимумкин.

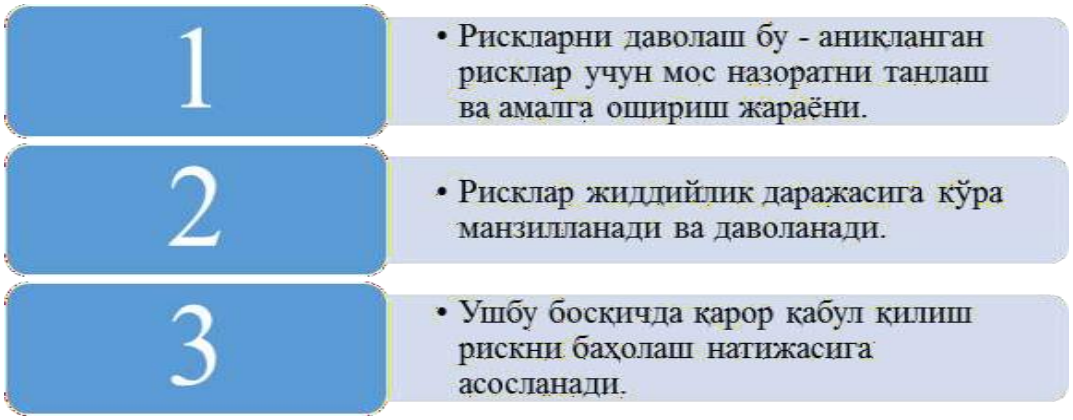
• Рискни таҳлил қилиш

- 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 рискларн 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 имкониятинианиқлайди.
- Риск мониторинги рискни тутувчи мос назорат усули амалгаоширилганлигини кафолатлайди.
- Риск мониторинги шунингдек рискни эҳтимоли, таъсири, ҳолати ва ошкорбўлишини ўз ичига олади.

Рискни кўриб чиқиш

- Рискни кўриб чиқиш орқали амалга оширилган рискларни бошқаришстратегияси самарадорлиги баҳоланади.
- Риск баѐни топ рисклардан огоҳ бўлишни бошқаришни кафолатлайди.

1.2. Идентификация, аутентификация ва авторизация

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 жараѐни. Масалан, сиз телефонда узингизни танитишингизни идентификациядан ўтиш деб айтиш мумкин. Бунда сиз узингизни, масалан, ―Мен Алиман‖ деб танитасиз. Бу уринда - Боходир‖ сизнинг *идентификаторингиз* бўлиб хизмат қилади. Шундай қилиб, *идентификация* - субъект идентификаторини тизимга ѐки талаб қилган субъектга тақдим этиш жараѐни ҳисобланади. Бундан ташкари, электрон почта тизимида ҳам почта манзилни - *идентификатор* сифатида караш мумкин. Почта манзилини тақдим этиш жараѐнини эса *идентификациялаш* жараѐни сифатида караш мумкин. Электрон почта тизимида почта манзили такрорланмас ѐки уникал бўлади. Шунданкелиб чикиб айтиш мумкинки, фойдаланувчининг идентификатори тизим ичида уникал ва такрорланмасдир.

Аутентификация - фойдаланувчини (ѐки бирор томонни) тизимдан фойдаланиш учун рухсати мавжудлигини аникдаш жараѐни. Масалан, фойдаланувчини шахсий компьютердан фойдаланиш жараѐнини олсак. Дастлабкиришда фойдаланувчи ўз идентификаторини (яъни, фойдаланувчи

номини) киритади ва у орқали тизимга ўзини танитади (идентификация жараѐнидан 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 ѐки субъектни хақиқийлигини текшириш жараѐни деб айтиш мумкин.

Аутентификациядан ўттандан сўнг фойдаланувчи тизим ресурсидан фойдаланиш имкониятига эга бўлади. Бирок, аутентификациядан ўтган фойдаланувчига тизимда ихтиѐрий амалларда бажаришга рухсат берилмайди. Масалан, аутентификациядан ўтган имтиѐзга 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 жараѐнларидан ўтган фойдаланувчи учун тизимда бажариши мумкин бўлган амалларга рухсат бериш жараѐнидир.

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 жараѐнлари рухсатларни назоратлашнинг қисмлари сифатида қаралади.

Юқорида келтирилган атамаларга берилган таърифларни умумлаштирганхолда қуйидагича хулоса қилиш мумкин:
Идентификация - сиз кимсиз?

Аутентификация - сиз хакикатдан ҳам сизмисиз?

Авторизация - сизга буни бажаришга рухсат борми?

Аутентификация

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

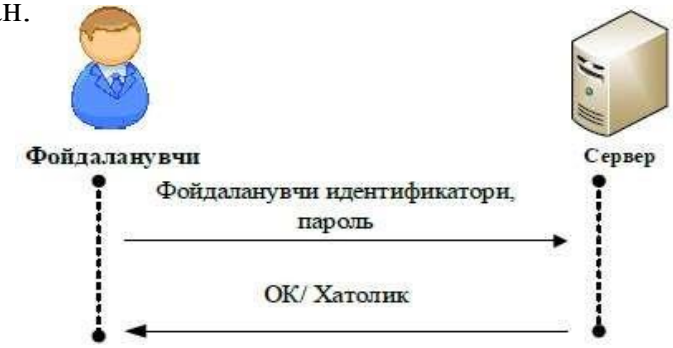
Машина инсонни қуйидаги ―нарсалар‖ асосида аутентификациядан ўтказиши мумкин:

- *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 мавжудбирор нарса‖ холатига эса смарткарталар, токен, машинанинг пулти èки 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 жараènидан ўтишни таъминловчи бирор ахборот. Парол амалда аутентификация жараènида 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 жараènининг умумий кўриниши 1-расмда келтирилган.



1-расм. Паролга асосланган машина-инсонни аутентификациялаш жараèни

Паролга асосланган аутентификациялаш қуйидаги хусусиятларга эга:

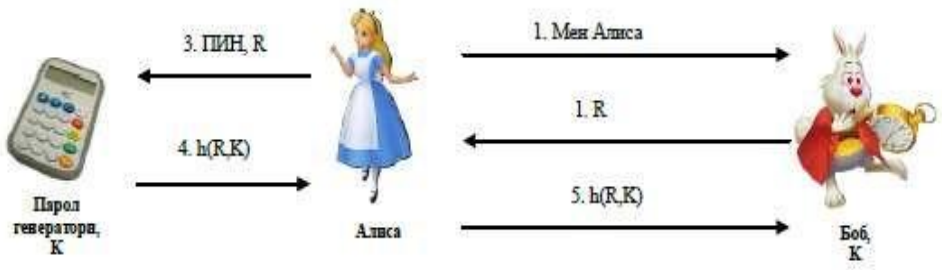
- паролга асосланган аутентификацияни амалга ошириш қўлай (сарф харажати кам, алмаштириш осон);
- фойдаланувчи пароли одатда унга алокадор маълумот бўлади (масалан, унинг яхши кўрган футбол командаси, телефон раками ва хак.) ***(123456, 12345, дм>ег(у)*** ва шунинг учун "ҳужумчилар‖ томонидан аникланиши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

Смарткарта èки токен

Смарткарталар èки 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 èки паролни, сакдайди 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 ***K*** ни (‒саволни‖) Алисага юборади. Алиса қабул қилинган ***K*** 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 жараèни

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 èки ‒сизда мавжуд бирор нарса‖ асосида аутентификация усуллари қуйидаги хусусиятларга эга:

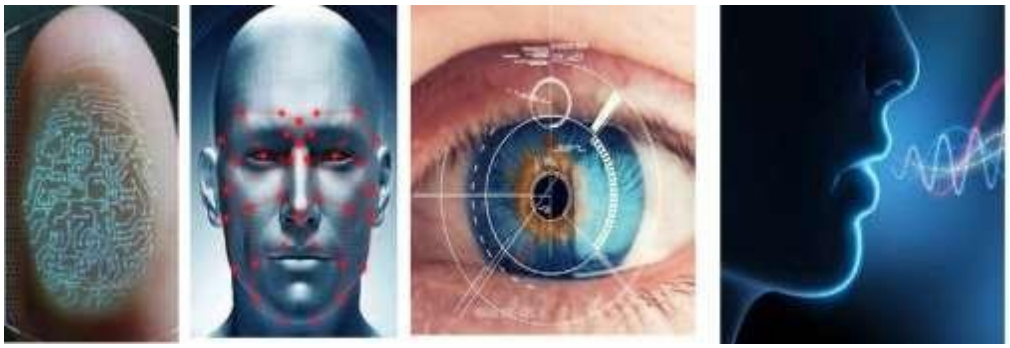
- смарткартага асосланган аутентификацияда бирор нарасани эсда сакдашни

талаб этилмайди;

- амалга ошириш ва қурилма нархи юқори (хусусан, токен йўқолган такдирда уни алмаштириш қимматга тушади);
- токен ѐки смарткартани йўқотиб кўйиш 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 ѐки ташкилотларга киришда бармоқ изига асосланган аутентификация усули, ноутбукларда ва мобил телефонларда юз тасвирига асосланган ѐки бармоқ изига асосланган аутентификациядан кенг қўлланилади (4-расм).



Бармоқ изи Юз тасвири Куз корачиг

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 биометрикпараметр қалбакилаштирилса, У холда аутентификация тизими

шу фойдаланувчи учун тўлиқ бузилган ҳисобланади;

- турли биометрик параметрларга асосланган аутентификация усуллари инсонлартомонидан 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 жараènга 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 базаларимавжуд. 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 инсоннингноми* ***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 èки киришда бармоқ изини тўғри киритсангиз, эшик очилади. Яъни, сервер фақат фойдаланувчиданпаролни èки 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 èзиб олиб, уни аутентификациядаш ўтиш жараènида тақдим этса, осонлик билан аутентификация тизимини алдаб ўтиши мумкин. Сабаби, фақат битта фактор (овоз) бўйича текшириш амалга оширилмокда. Шунга ўхшаш холатни паролга асосланган èки токенга асосланган аутентификация жараènида хамкузатиш 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 хаètимизда хам кўплаб мисоллар келтириш мумкин. Масалан, пластик картадан тўловни амалга оширишда. Пластик картадан тўловни амалга оширишдаги аутентификация жараèни 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 тақдирда хам аутентификация жараènини 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 учунқуйидаги ҳужум усулларидан фойдаланилади:

a. **Пароллар луғатидан фойдаланишга асосланган ҳужум.** Бунга кўра статистика бўйича энг кўп қўлланилувчи пароллар èрдамида аутентификациядан ўтишгахаракат қилинади.

b. **Паролларни барча вариантларини кўриб чикиш.** Ушбу усулда паролнингбўлиши 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 учунқуйидаги ҳужум усулларидан фойдаланилади:

a. **Физик ўғирлаш.** Ҳужумнинг мазкур тури токенни ёки смарт картани ўғирлашнимақсад 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 сабаблизарарли 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 мавжудрасм 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.

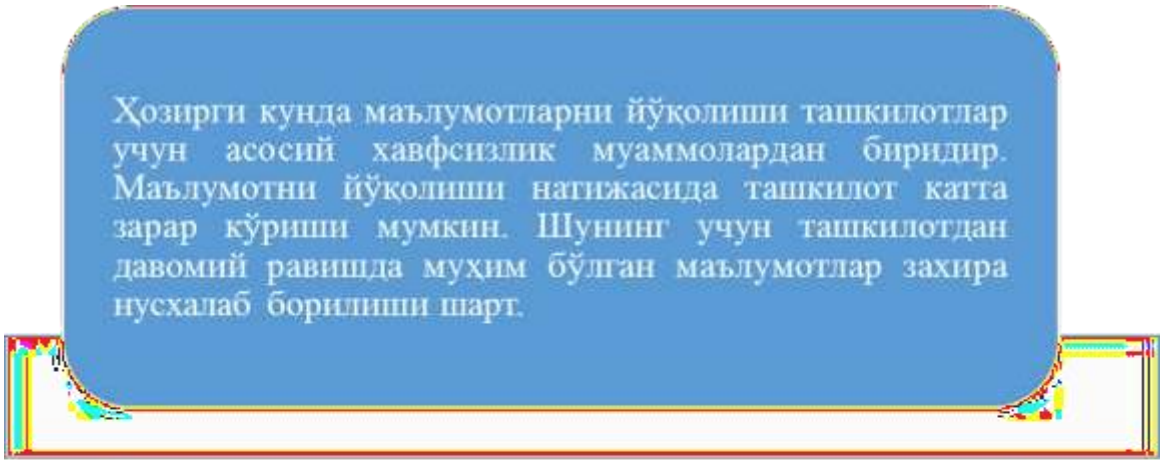
Аутентификация усулларига қаратилган ҳужумларии олдини олиш учун хар битта усулда ўзига хос қарши чоралари мавжуд. Умумий холда мазкур ҳужумларни олдини олиш учун қуйидаги химоя усуллари ва хавфсизлик чоралари тавсия этилади:

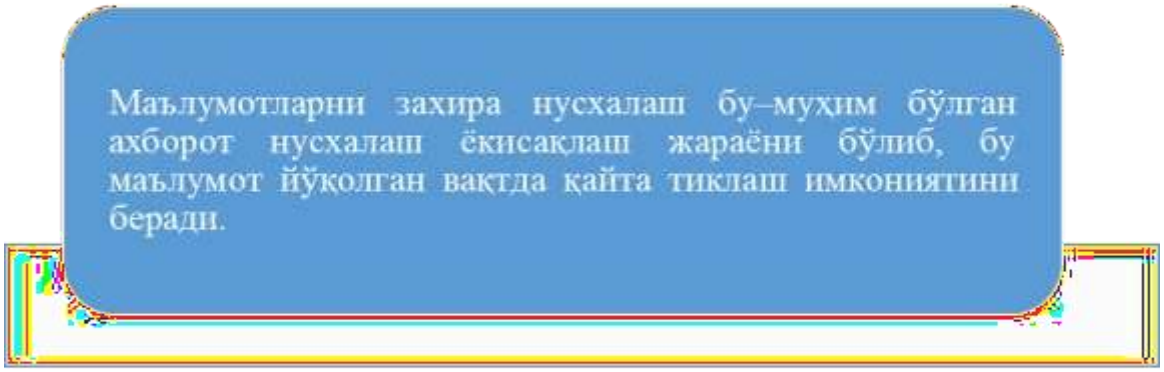
1. ***Мураккаб пароллардан фойдаланиш.*** Айнан ушбу усул паролни барча вариантларини текшириб кўриш ва луғатга асосланган ҳужумларни олдини олишгакатта ёрдам беради.
2. ***Кўп факторли аутентификациядан фойдаланиш.*** Мазкур усул юкорида келтирилган барча муаммоларни бартараф этишда катта амалий ёрдам 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

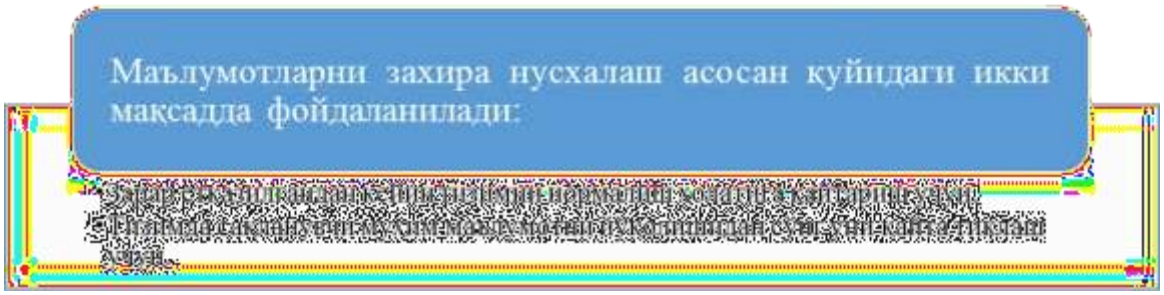
алдаб ўтиш ҳужуминиолдини олиш учун самарали ҳисобланади.

1.3. Маълумотлар ва ахборотни тикланиши ва барқарорлиги

Киберхавфсизликда маълумотлар ва ахборотни тикланиш ва барқарорлиги таъминлаш бўйича тавсиялар:







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 жараènигача бўлган босқичларни ўз ичига олади.

Зарур ахборотни аниқлаш

Захира нусхаларни сақловчи воситалар

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.

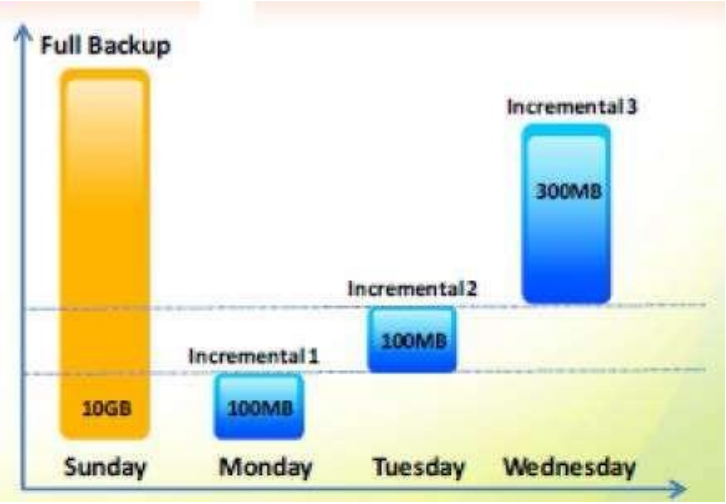
• Захира нусхалашни амалга оширган учинчи томон ҳар доим ҳам тўлиқ маълумотни захиралаш амалга оширилганини кафолатламайди.

Захиралаш турлари

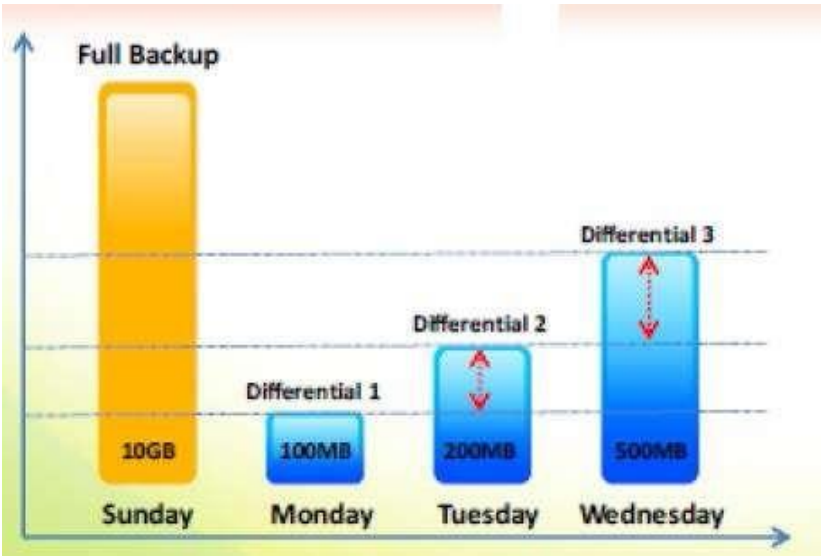
Тўлиқ захиралаш	Ўсиб борувчи захиралаш	Дифференциал захиралаш
• Тўлиқ захиралаш усули тиклашнинг тезлиги юқори. • Захира нусхалаш жараёнининг секин ва маълумотни сақлаш учун кўп ҳажм талаб этади.	• Захираланган маълумотга нисбатан ўзгариш юз берганда захирилаш амалга оширилади. • Охирги захира нусхалаш 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 жараèни 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.



II-БОБ

2.1. Тармоқ ҳужумлари, web-ҳужумлар, дастурий ҳужумлар

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 ѐки бошқа ҳаракатнинг таъсирида бўлиши мумкин.

Заифлик бу – ―портлаганида‖ тизим хавфсизлигини бузувчи кутилмаган ва ошкор бўлмаган ҳодисаларга олиб келувчи камчилик, лойиҳалашдаги ѐки 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 имкониятиниқўлга киритишга ҳаракат қилинади.

Тармоқ хавфсизлиги муаммолари

Тармоқдан фойдаланиб амалга оширилувчи ҳужумлар сони ва кўринишлари жуда ҳам жадаллик билан ортиб бормоқда. Доимий ҳужумлар бутун ҳисоблашқурилмалари дунѐси 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 ҳужумларҳақида 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 ташқиҳужумдан 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 ортишигақуйидаги омиллар таъсир қилмоқда:

Қурилма èки дастурий воситани нотўғри созланиши. Хавфсизлик бўшлиқлари одатда тармоқдаги қурилма èки дастурий воситаларнинг нотўғри созлангани боис вужудга келади. Масалан, нотўғри созланган èки шифрлаш мавжуд бўлмаган протоколдан фойдаланиш тармоқ орқали юборилувчи махфий маълумотни ошкор бўлиши сабабчи бўлади. Нотўғри созланган қурилма ҳужумчига тизим èки тармоқдан фойдаланиш имкониятини тақдим этиши мумкин. Нотўғри созланган дастурий восита эса илова èки 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 қўйишимумкин.

Туғма технология заифлиги. Агар қурилма èки дастурий восита маълум турдаги тармоқ ҳужумларини бартараф эта олмаса, у ҳолда у ушбу ҳужумларни заиф бўлади. Кўплаб қурилмалар, иловалар èки веб браузерлар *хизматдан вос кечишга ундаш* ҳужуми èки *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.

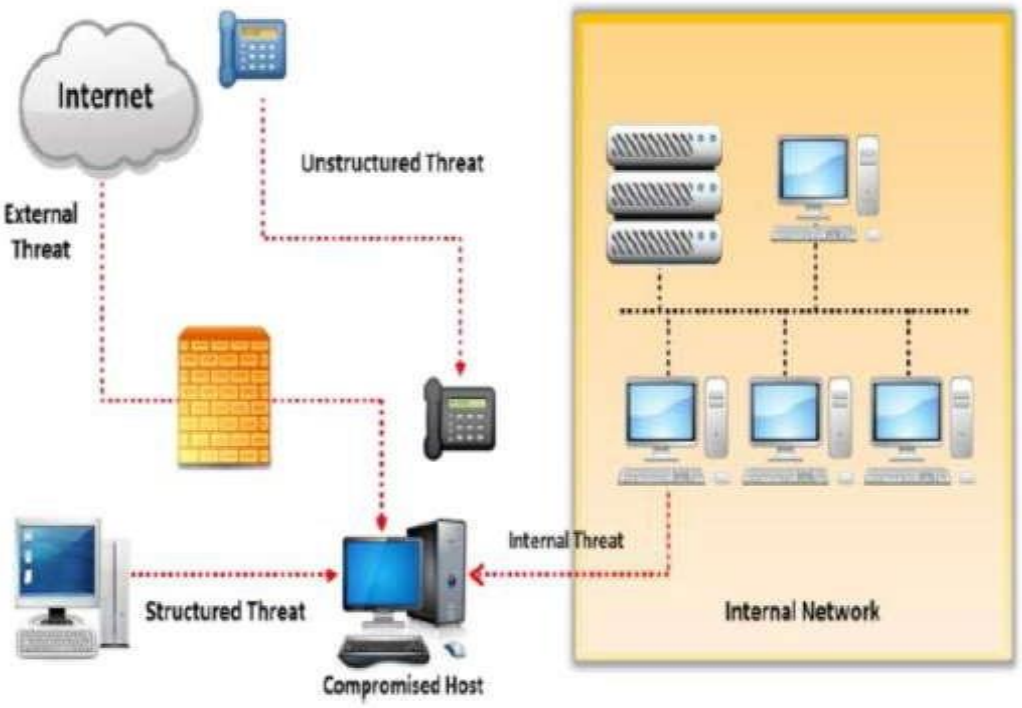
Фойдаланувчиларнинг эътиборсизлиги. Энг охирги тармоқ фойдаланувчиларининг эътиборсизлиги тармоқ хавфсизлигига жиддий таъсир қилиши мумкин. Инсон ҳаракатлари натижасида маълумотни йўқолиши, чиқибкетиши каби жиддий хавфсизлик муаммолари бўлиши мумкин. Бундан ташқари ҳужумчилар фойдаланувчилар ҳақида маълумотларни 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 тург ажратилади(1-расм):

- ички таҳдидлар;
- ташқи таҳдидлар.



1-расм. Турли тармоққа қаратилган таҳдидлар

Ички таҳдидлар. Компьютер ѐки 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 имтиѐзга 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 сиѐсати ва ташкилот қонунчилиги билан яқиндан таниш бўлади.

Ташқи таҳдидлар. Ташқи ҳужумлар тармоқда аллақачон мавжуд бўлган заифлик натижасида амалга оширилади. Ҳужумчи шунчаки қизиқишга, моддийфойда ѐки 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 тайѐрганлик кўрилади. Мазкур ҳолда ҳужумлар ички ходимларнинг ѐрдамисиз 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 ѐки шахслар гуруҳлари одатда катта кибержиноятчиликларни амалга оширишга жалб этиладилар.

Тизимлашмаган ташқи таҳдиди. Тизимлашмаган ташқи таҳдидлар одатда малакали бўлмаган шахслар томонидан турли тайѐр бузиш воситалари ва скриптлар ѐрдамида амалга оширилади. Ушбу ҳужум турлари одатда шахс томонидан ўз имкониятини тестлаш учун ѐки 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 ѐки 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 ѐки 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 сиѐсатидаги заифлик. Хавфсизлик сиѐсатидаги заифликни юзагакелишига ташкилотнинг хавфсизлик сиѐсатида 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 ѐи хакерлар тармоққа киришни янгидан янги усулларини топишмоқда. Ҳар бир ҳужумчиларнинг мотивлари уларнинг мақсадларига кўра турлича бўлиши мумкин. Масалан, баъзи ҳужумчилар қурилмани ѐки дастурий воситани ўғирлашни мақсад қилса, баъзилари тармоқ ресурсларидан ва фойдаланувчи маълумотларини қўлга киритишни ѐки 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 потенциалзаифликни аниқлаш имконини беради.

Кириш ҳужумлари. Мўлжалдаги тармоқ ҳақида етарлича ахборот тўпланганидан сўнг, ҳужумчи турли технологиялардан фойдаланган ҳолда тармоққа киришга ҳаракат қилади. Яъни, тизим ѐки тармоқни бошқаришга ҳаракат қиладилар. Бу турдаги ҳужумлар кириш ҳужумлари деб аталади ва рухсатсиз фойдаланиш, қўпол куч ҳужуми, имтиѐзни 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 ѐки 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 ѐки тармоққа бевосита ва билвосита таъсир қилади. Ушбу ҳужумлар тармоқ вазифасига зарарли тасир қилади. Зарарли дастур бу – программа ѐки файл бўлиб, компьютер тизимига таҳдид қилиш имкониятига эга. Зарарли дастурлар троянлар, вируслар ва ―курт‖ларкўринишида 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 қўлга 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 ѐрдам 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 ишлаѐтганини 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 ѐки бошқа кўринишда бўлиши мумкин. Ҳужумчи зарарли дастурий воситалардан фойдаланган ҳолда тизим хафсизлигини обрўсизлантириши, компьютер амалларини бузиши, махфий ахборотни тўплаши, веб сайтдаги контентларни модификациялаши, ўчириши ѐки 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 шартқаноатлантирилган 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.
-

- 2.2. Зараркунанда дастурий таъминотлар

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 ҳамфойдаланилиши 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 ѐки 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 имтиѐзга эга бўлиш.
- *мантиқий бомбалар:* зарарли дастурий восита бўлиб, бирор мантиқий шартқаноатлантирилган 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 ѐки 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 ѐки операцион тизим версияси каби маҳаллий шартларга асосланади. Шу тарзда триггерлар масофадан тўриб ўрнатилувчи кўринишда лойиҳаланиши мумкин ѐки бўлмаса қандайдир ҳолатни мавжуд эмаслигига кўра.

Мантиқий бомбалар мавжуд коднинг ичига киритилиши ѐки 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_comp
uter( )
```

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 хуфиєна 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. Ушбуҳолат юз берганда ўзининг яратувчиси учун паролларни ушлаб олувчи дастур ўзига èзиб қуяди, сўнгра эса ―нотўғри парол‖ деган хабарни тизимга реал кириш олдиданчиқаради. 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 èки автоном дастурларда бўлиши мумкин. Орқа эшик (туйнук) намунаси қуйидаги кодда кўрсатилган бўлиб, у тизимга киришда аутентификация жараènини 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 зараралаш 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 зараралашда 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* (èки шунчаки *вирус*) ва *вирус-червлар* (èки 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 èрдамида 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 ажратишмумкин.

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

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

Макровируслар учун шароит яратувчи восита сифатида маълум дастурлаш тилида èзилган ва турли офис иловалари – MS Word ҳужжати, MS Excel электрон жадвали, Corel Draw тасвири, файлларида жойлашган ―макрослар‖ èки ―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 зарарлайди. 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 зарарлай 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 ажратишгаимкон 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 вашундан сўнг зарарлашни бошлайди. Шунинг учун мазкур вирусларни аниқлаш, ўрганиш ва ўчириш мураккаб бўлиб, бу мураккаблик камида ундаги қайтаришамали – 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 ѐрдамида тарқалади ва маълумот пакетлари ичида я ширинган ҳолда узатилади (масалан, *Net-Worm.Win32.Lovesan*). *"Телефон"* ѐки *"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 ѐзилган 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 бўйлабвирусларнинг тарқалиш хавфи ва антивирус дастурларини яратиш имкониятлари ҳақида китоб ѐзади.

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 дунѐ бўйлаб компьютер тизимларига вайронагарчиликларни келтириб чиқарди ва тахминан 10 миллиард доллар зарар келтирди. Дунѐ 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 рўйхатидагиҳар бир кишига ўзини юборади ва файлларни қайта ѐзишни 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 кашфиѐт 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 орқалиҳужжатларни бузади.

Охир оқибат Смит Word ҳужжатини унга топширишганида қўлга олинди. Файл ўғирланган AOL аккаунтидан фойдаланиб юкланган ва уларнинг ѐрдами 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 ѐзуви хавфсизлик сиѐсатини 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 ѐшига 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 компьютер хавфсизлиги фирмасининг ходими ва ушбу куртни илк кашфиѐтчиларидан бири қўйган. Шмугарисмни 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 орттмоқда*

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 дебтопилади. 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 зараралашга 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 èки 100 минглаб сигнатурага эга файл èрдамида 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 èки зарарли дастурларга қарши ҳимоя воситаларида кэнг қўлланилади. Натижада, вирус яратувчилар сигнатурани аниқлаш усулини айланиб ўтишимкониятига 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 èки бир нечта битлариўзгаришга 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 èки номалум зарарли дастурорқали бўлган ўзгариш).

Бироқ, ушбу усул кўплаб камчиликларга эга. Тизимдаги файллар одатда тез- тез ўзгариб туради ва бунинг натижасида èлғондан 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 қиладива бу ҳолат сигнатурага асосланган усулга ўхшаш бўлиб қолади.

Аномалияга асосланган усул

Аномалияга асосланган усул ноодатий èки вирусга ўхшаш èки потенциал зарарли ҳаракатлари èки 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 борилаètган 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 яратгунчавирус ишлаб чиқарувчилар томонидан катта ҳажмдаги янги вируслар яратилади. Бу эса, янги вирус учун вакцинани тайèрлаш 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 баҳоланишимумкин:

- *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 вауни доимий янгилаб бориш;
- бошқа комьютерда ѐзиб олинган маълумотларни ўқишдан олдин ҳар бирсақлагични антивирус текширувидан ўтказиш;
- архивланган файлларни ажратгандан сўнг сканерлашни амалга ошириш;
- компьютер дискларини такрорий антивирус дастурлари текширувиданўтказиш;
- компьютер тармоқларидан олинган барча бажариладиган файлларни киришназорати учун антивирус дастуридан фойдаланиш.

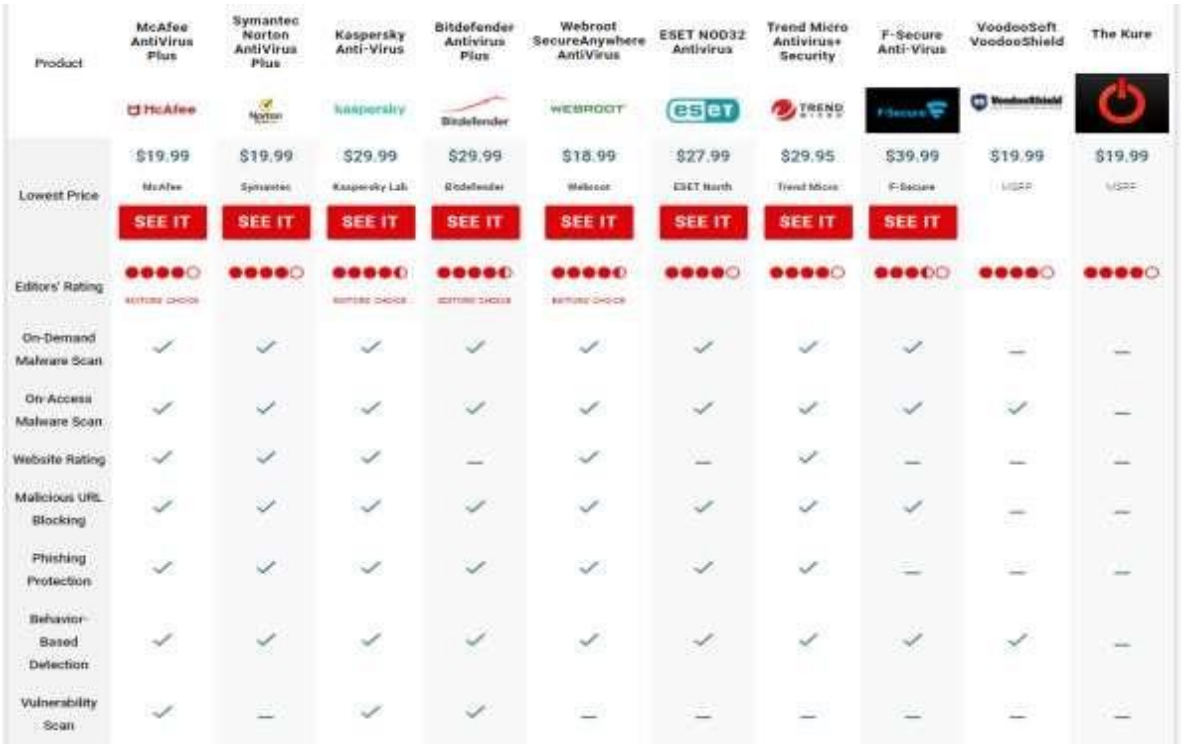
Антивирус дастурий комплекслари

Ҳар бир антивирус дастурий воситаларининг ўзига хос бўлган афзаллик ва камчиликлари мавжуд. Фақат бир нечта антивирус дастурий воситалариданкомплекс 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	✓	–	✓	✓	–	–	–	–	–	–

2.3.Кибержиноятчилик, киберҳуқуқ ва киберэтика

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 èки компьютер жиноятларининг нисбатан узоқ вақтдан бери давом этаèтган ҳодисани ташкил эца-да, глобал тармоққа уланишўсиб бориши замонавий кибер жиноятларнинг ривожланиши билан узвий боғликдир.

1960 йилдан буèн компьютер тизимларига жисмоний зарар етказиш ва сақланган маълумотлар, компьютер тизимларидан рухсатсиз фойдаланиш ваэлектрон 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 дунèси.

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 èқтиришади. 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 ѐки компанияни зарарли кодни туширгандан сўнг, файллар шифрланади ва ундан кейин нақд пул мукофотига алмаштириш таклифи олинади (одатда битсоинс ѐки 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) ѐки 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 ѐки ўзгарувчан сиѐсий 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 ѐки шахслар гуруҳини ўзгартириши мумкин. Баъзи фуқаролар паспорт ѐки бошқа идентификаторларни жисмонан идентификация қилиш учун ўғирлаб кетишаѐтганда, 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 ѐки қурилмаларга ҳужум қилиш ва ноқонуний оммавий кузатувлар билан якунланган жосусликнинг мақсади, шахсий ҳаѐтимизнинг яширин кузатувидир. Жисмоний жосуслик (масалан, веб-ѐки CCTV камералар ѐрдамида одамлар ѐки гуруҳларни кузатиб бориш учун), шунингдектурли 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 ѐрдам бера олмайди. Албатта, ҳаракат анализаторлари мавжуд, аммо улар тўлиқ хавфсизликни таъминлай олмайди.

0 кунлик ҳужумларда кибержиноятчилар, номаълум бўлган ѐки 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 "Екуифах" 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 жараѐнни бошқаради.

► Image Forensic Search System (IFSS)- расм қидируви учун бепул, очиқ кодли дастурий таъминот. Бу сизга бошқа тасвирдаги мақсадли тасвирни излашни ѐки 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 ѐрдам 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.

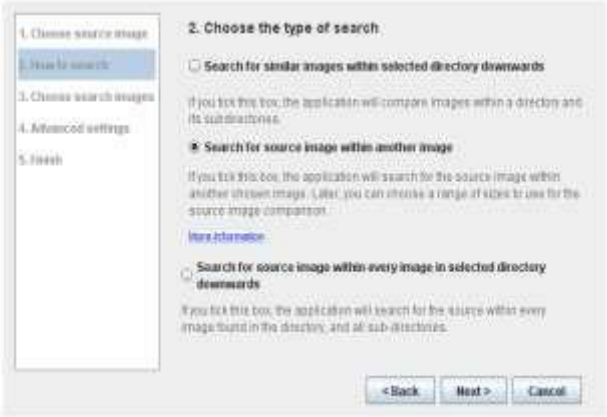
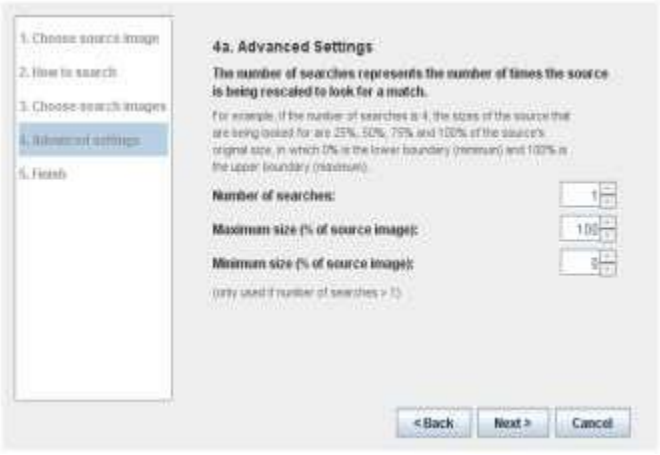
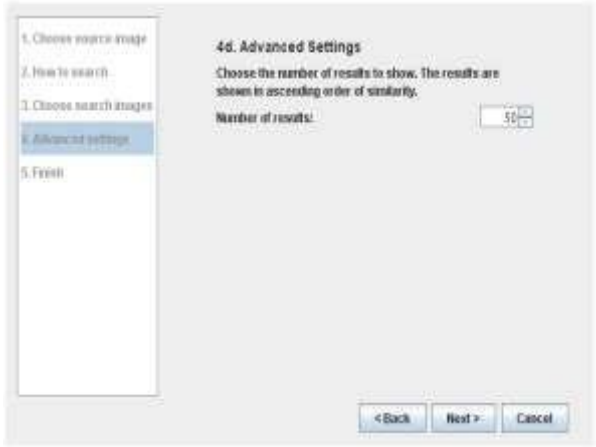
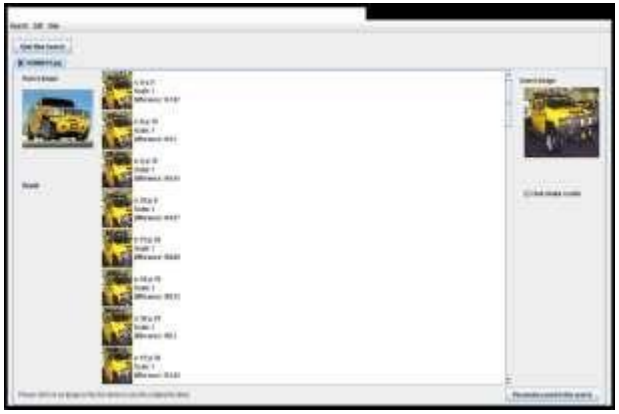
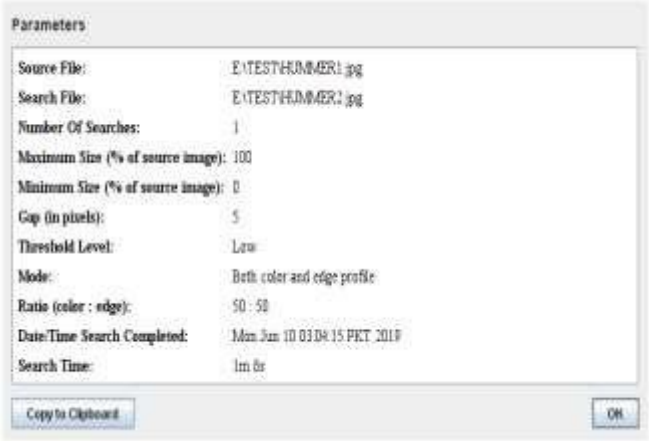


Image Forensic Search System-software.





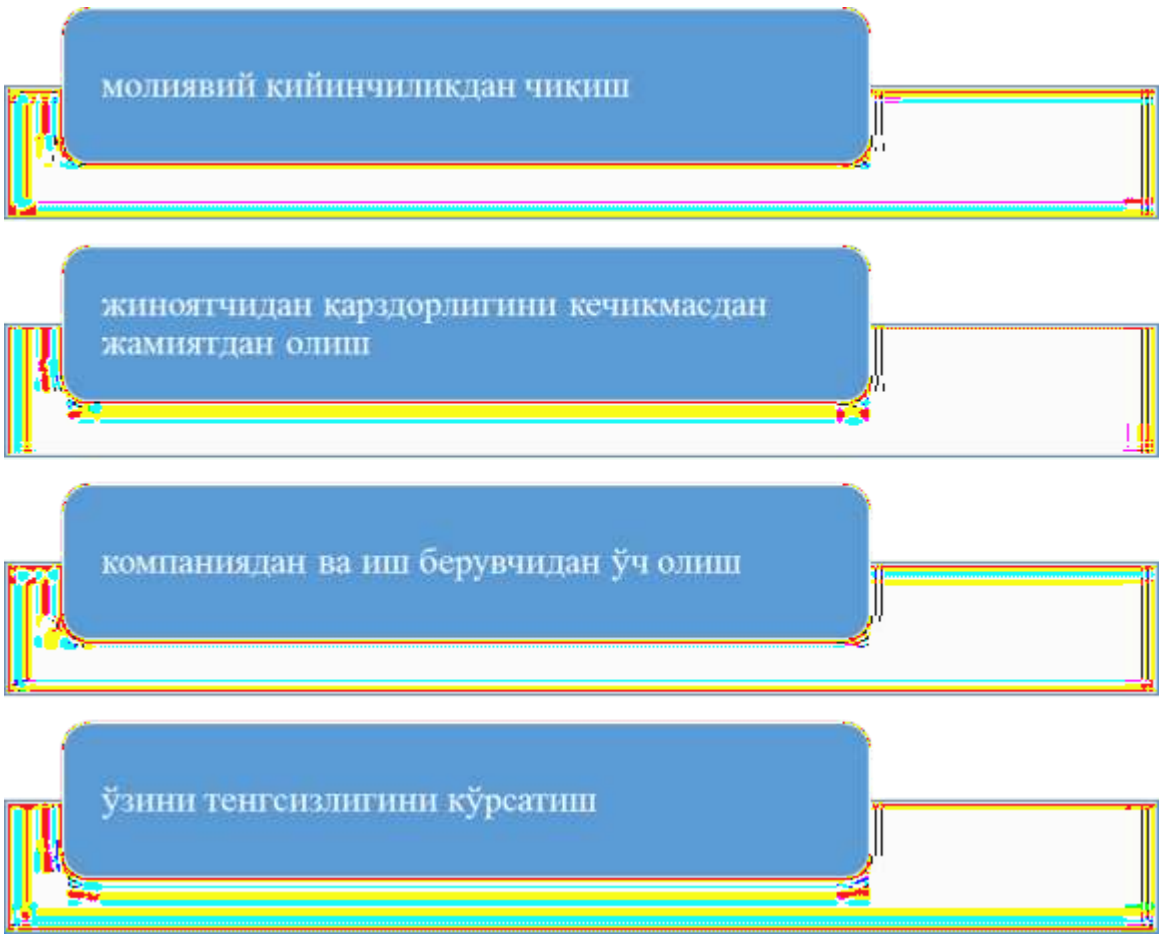




Кибержиноятдан асосий мақсад нима?

- пул, қимматли кргозлар, кредит, моддий бойликлар, товарлар, хизматлар, имтиѐзлар, кучмас мул к, ѐқилги хом ашѐси, энергия манбалари ва стратегик хом ашѐларни нокрнуний олиш;
- солиқ ва турли йигимларни тулашдан бош тортиш;
- жиноий даромадларни легаллаштириш;
- қалбаки хужжатлар, штамплар, мухрлар, бланкалар, шахсий ютуклар учуйкасса чипталарини калбақилаштириш ѐки тайѐрлаш;
- шахсий ѐки сиѐсий мақсадларда махфий маълумотларни олиш;
- маъмурият ѐки ишдаги хамкасблар билан шахсий душманлик муносабатлари асосида касос олиш;
- шахсий ѐки сиѐсий мақсадлар учуй мамлакат пул тизимини бузиш;
- мамлакатдаги вазиятни, худудии маъмурии тузулишни оекарорлаштириш ѐки сиѐсий мақсадлар учун тартибга солиш;
- талончилик, ракибни йўқ қилиш ѐки сиѐсий мақсадлар учун муассаса,корхона ѐки тизим ишини тартибга солмаслиқ
- бошка жиноятларни яшириш учун;
- тадкикрт масалаларида;
- шахсий интелектуал крбилият ѐки 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 адабиѐтларда кибержиноятчиликнинг қуйидаги турлари келтирилган:

- икгисодий компьютер жиноятлари;
- инсон ва фуқароларнинг конститутциявий хуқуқлари ва эркинликларигақарши қаратилган компьютер жиноятлари;
- жамоат ва давлат хавфсизлигига қарши компьютер жиноятлари.

Киберэтика бу- компьютерлар билан боғлиқ фалсафий соҳа бўлиб, фойдаланувчиларнинг ҳатти – ҳаракатл дастурлаштирилганлиги ва умуман инсо таъсир кўрсатишини ўрганади.

Мисоллар

- Интернетда бошқа одамлар тўғрисидаги шахсий маълумотларни (масалан, онлайн ҳолатлар ѐки 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 ҳуқуқларгаэга;
- 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 èрдамида 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 жараèнларни оз ичига олиши мумкин.

Бироқ, 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 ѐки шахс ҳуқуқини ҳимоя қилиш деган саволни ўртага қўяди. Интернет тармоғида фойдаланувчилар сонини ортиши, шахсий маълумотларни кўпайиши натижасида уларнинг ўғирланиши ва кибержиноятлар сони ортмоқда.

Аниқлик

Интернетнинг мавжудлиги ва баъзи бир шахс ѐки жамоалар табиатитуфайли маълумотларнинг аниқлигини билан шугулланиш муаммога айланмоқда. Бошқа сўз билан айтганда Интернетдаги маълумотларнинг аниқлигига ким жавоб беради? Бундан ташқари Интернетдаги маълумотларни ким тўлдириб боради, ундаги хатолар ва камчиликлар учун ким жавобга бўлиши кераклиги туғрисидаги тортишувлар мавжуд.

Фойдаланувчанлик, цензура ва филтерлаш

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

кўтаради.

Ушбу масалаларнинг мавжудлигибизнинг махфийлик ва шахсийликни тушунишимизга ва жамиятдагииштирокимизга шубха туғдиради.

Агар бирор қонун коидага асосан маълумотлардан фойдаланишни чеклаш ѐки филтерлаш асосида ушбу маълумотни таркалиши ѐки фойдаланувчанлигигатаъсир қилиш мумкин.

Хозирда ушбу холатлар амалда кенг кўлланилмокда.

Цензура хам паст даражада (масалан, компания ўз ходимлари учун) ѐки 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 бўлмокда. 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 ѐқламайдилар. Ўзнавбатида ушбу томонлар орасидаги мунозаралар қайси турдаги уйинларга рухсат бериш керак? Улар қайерда ўтказилиши керак? деган саволлар кенг музокараларга сабаб бўлмокда. 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 нусхакучирманг.
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 биланфойдаланинг.

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 èки тарқатиш билан шуғулланадиган ҳар бир ташқилот ушбу маълумотлардан фақат улар

белгиланган мақсадлар учун фойдаланилишинитаъминлаш 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 руѐбга 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 хукуқ 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. Махфийахборотга қуйидагилар кирмайди:

- фукароларнинг хукуқ ва эркинликлари, уларни руѐбга 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 кўрсатаѐтган 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 жараѐнлар 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 муддатичида юборилади.

Рад этиш тўғрисидаги хабарда сўралаётган ахборотни бериш мумкинэмаслиги сабаби курсатилиши керак.

Махфий ахборот мулкдори, эгаси ахборотни сўраётган шахсларни буахборотни 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 сохталаштирилишининголдини 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, сакдашга, кайта ишлашга, тарқатишга ва ундан фойдаланишга йул кўйилмайди, 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 хамдаундан 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 эркинлигинитаъминлаш;
- қонунга хилоф равишда ижтимоий онгга ахборот воситасида руҳийтаъсир курсатишга, уни чалгитишга йул қуймаслиқ;
- 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 конфессияларо 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 рухсатсизтарзда 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 ҳаракатларқилиш.

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.

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 жараèни	**Information protection**
киберхавфсизлик	қонуний жихатларни, сиèсатни, инсон омилини, этика ва рискларни бошқариш	**cybersecurity**
Киберхавфсизли (Cisco ташкилоти таърифи)	тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиèти	**Cybersecurity (Cisco definition)**
Маълумотлар хавфсизлиги	маълумотларни сақлашда, қайта ишлашда ва узатишда ҳимояни таъминлашни мақсад қилади	**Data security**
Дастурий таъминотлар хавфсизлиги	фойдаланилаèтган тизим èки ахборот хавфсизлигини таъминловчи дастурий таъминотларни ишлаб чиқиш ва фойдаланиш жараènига 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 ҳаèт шароитида шахсий маълумотларни ва шахсий ҳаèтни ҳимоя қилишга эътибор қаратади	**Human security**

Ташкилот хавфсизлиги	ташкилотни киберхавфсизлик таҳдидларидан ҳимоялаш ваташкилот вазифасини муваффаққиятли бажаришини мададлаш учун рискларни бошқаришга эътибор қаратади	**Organizational security**
Жамоат хавфсизлиги	у èки 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 сиѐсати	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 èки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка èки 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 (èки 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 ѐки ишчи жараѐнни, жараѐнни, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир	**event**
Нормал ҳодиса	критик компоненталарга таъсир қилмайди ѐки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.	**Normal event**
Ҳодисаларни кенгайиши ва кўпайиши (Эскалация)	Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ѐки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараѐнини 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 ѐки хизмат сифати ѐмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.	**Incident**
Хавфсизлик инциденти координатори	инцидентга жавоб қайтариш жараѐнини 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 ѐки 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 жараèни	• 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 жараèни самарадорлиги	❑ ахборот хавфсизлиги инцидентини бошқариш жараènида 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 èрдамида белгиланган тартиб бўйича ўтказиш жараèни	**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	ихтиѐрий узунликдаги (бит ѐки байт бирликларида) маълумотни бирор фиксирланган узунликдаги (бит ѐки 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 ѐки 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 ѐки 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 ѐки 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), èки файл йўлдошларни (компанъон вируслар) яратади èки файлли тизимларни (linkвируслар) ташкил этиш хусусиятидан фойдаланади.	**File viruses**
Юклама вируслар	ўзини дискнинг юклама секторига (boot секторига) èки винчестернинг тизимли юкловчиси (Master Boot Record) бўлган сек торга èзади. 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 èки 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	• безиѐн 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 (ѐки 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 жараѐни	**Identification**
Аутентификация	фойдаланувчини (ѐки бирор томонни) тизимдан фойдаланиш учун рухсати мавжудлигини аникдаш жараѐни	**Authentication**
Авторизация	идентификация, аутентификация жараѐнларидан ўтган фойдаланувчи учун тизимда бажариши мумкин бўлган амалларга рухсат бериш жараѐни	**authorization**
Пароль	фақат фойдаланувчига маълум ва бирор тизимда аутентификация жараѐнидан ўтишни таъминловчи бирор ахборот	**password**
Нусҳа яратиш	Ахборот ташувчиларда маълумотлар нусҳасини яратиш жараѐни	**backup**

Маълумотларни қайта тиклаш	Ахборот ташувчиларда маълумотларни қайта тиклаш жараèни	**data recovery**
Тшлиқ нусҳа яратиш	Тизимни ва ундаги барча файлларни нусҳасини яратиш жараèни	**Full backup**
Дифференциал нусҳа яратиш	Ўзгартирилган файлларни нусҳасини олиш жараèни	**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 èки 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 èки 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 èки 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 имтиèзга 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 ѐки 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**

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 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.

Ш. Махсус адабиѐтлар

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

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

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

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

19. Юсупов С.Ю., Ганиев А.А. Взлом и защита компьютерных систем исетей. – 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

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