ЎЗБЕКИСТОН ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

Амалий математика ва информатика факультети
«Ахборотлаштириш технологиялари» кафедраси

5130200 – «**Амалий математика ва информатика**»
йўналишининг 4-курс талабалари учун

АХБОРОТЛАРНИ ҲИМОЯЛАШ

фани бўйича

ЎҚУВ – УСЛУБИЙ МАЖМУА

САМАРҚАНД -2019

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ
САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ
АМАЛИЙ МАТЕМАТИКА ВА ИНФОРМАТИКАФАКУЛТЕТИ
«АХБОРОТЛАШТИРИШ ТЕХНОЛОГИЯЛАРИ» КАФЕДРАСИ

ТАСДИҚЛАЙМАН:
ЎҚУВ ИШЛАРИ БЎЙИЧА
ПРОРЕКТОР
проф.А.С.Солеев
_____

«_____» _____ 2019 й.

АХБОРОТЛАРНИ ҲИМОЯЛАШ
фани бўйича

ЎҚУВ-УСЛУБИЙ МАЖМУА

Билим сохаси: 100000 – Гуманитар соҳа

Таълим соҳаси: 130 000 – Математика

Таълим йўналиши: 5130200 – Амалий математика ва информатика

САМАРҚАНД - 2019

Фаннинг ўқув-услубий мажмуаси Самарқанд давлат университетида ўқув, ишчи ўқув режа ва ўқув дастурига мувофиқ ишлаб чиқилди

Тузувчи:

Холмонов С.М.– СамДУ «Ахборотлаштириш технологиялари» кафедраси ассистенти

Тақризчилар:

Туракулов И.Н. - СамДУ «Ахборотлаштириш технологиялари» кафедраси доценти, т.ф.н.

Абдуллаев А.Н. - СамДУ «Ахборотлаштириш технологиялари» кафедраси доценти, т.ф.н.

Фаннинг ўқув-услубий мажмуаси СамДУ “Ахборотлаштириш технологиялари” кафедрасининг 2019 йил “___” _____ даги “___” - сон йиғилишида муҳокамадан ўтган ва факултет кенгашида муҳокама қилиш учун тавсия этилган.

Кафедра мудири:_____И.И. Жуманов

Фаннинг ўқув-услубий мажмуаси Амалий математика ва информатикафакултет Илмий кенгашида муҳокама этилган ва фойдаланишга тавсия қилинган (2019 йил “___” _____ даги “___” - сонли баённома)

Факултет кенгаши раиси: _____ А.И.Бобоёров

Факултет услубий кенгаши раиси: _____ Ш.Маматов

Келишилди: Ўқув-услубий бошқарма бошлиғи _____Б.Аликулов

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

АМАЛИЙ МАТЕМАТИКА ВА ИНФОРМАТИКА ФАКУЛТЕТИ

«АХБОРОТЛАШТИРИШ ТЕХНОЛОГИЯЛАРИ» КАФЕДРАСИ

№602

ТАСДИҚЛАЙМАН:
ЎҚУВ ИШЛАРИ БЎЙИЧА
ПРОРЕКТОР
А.С.СОЛЕЕВ

«____» _____ 2019 й.

АХБОРОТЛАРНИ ХИМОЯЛАШ

фанидан

ишчи дастури

Билим сохаси:	100000 – Гуманитар соҳа
Таълим соҳаси:	130 000 – Математика
Таълим йўналиши:	5130200 – Амалий математика ва информатика

САМАРҚАНД –2019

Фаннинг ишчи ўқув дастури Самарқанд давлат университетида ўқув, ишчи ўқув режа ва ўқув дастурига мувофиқ ишлаб чиқилди

Тузувчи:

Холмонов С.М. – СамДУ «Ахборотлаштириш технологиялари» кафедраси ассистенти

Тақризчилар:
Туракулов И.Н. - СамДУ «Ахборотлаштириш технологиялари» кафедраси доценти, т.ф.н.
Абдуллаев А.Н. - СамДУ «Ахборотлаштириш технологиялари» кафедраси доценти, т.ф.н.

Фаннинг ишчи ўқув дастури СамДУ “Ахборотлаштириш технологиялари” кафедрасининг 2019 йил “___” _____ даги “___” - сон йиғилишида муҳокамадан ўтган ва факультет кенгашида муҳокама қилиш учун тавсия этилган.

Кафедра мудири:_____И.И.Жуманов

Фаннинг ишчи ўқув дастури Амалий математика ва информатика факультет Илмий кенгашида муҳокама этилган ва фойдаланишга тавсия қилинган (2019 йил “___” _____ даги “___” сонли баённома)

Факультет услубий кенгаши раиси: _____ Ш.Маматов

Факультет кенгаши раиси: _____А.И.Бобояров

Келишилди: Ўқув-услубий бошқарма бошлиғи

_____Б. Аликулов

М У Н Д А Р И Ж А

1. Фаннинг аннотацияси

Тез ривожланиб бораётган компьютер ахборот технологиялари бизнинг кундалик хаётимизнинг барча жабхаларида сезиларли узгаришларни олиб кирмокда. Хозирда “ахборот тушунчаси” сотиб олиш, сотиш, бирор бошка товарга алмаштириш мумкин булган махсус товар белгиси сифатида тез-тез ишлатилмокда. Шу билан бирга ахборотнинг бахоси куп холларда унинг узи жойлашган компьютер тизимининг бахосида бир неча юз ва минг баробарга ошиб кетмокда. Шунинг учун тамомила табиий холда ахборотни унга рухсат этилмаган холда киришдан, касддан узгартиришдан, уни угирлашдан, йукотишдан ва бошка жиноий характерлардан химоя килишга кучли зарурат тугилади.

“Ахборотларни ҳимоялаш” курси Республикамизнинг олий ва урта махсус укув муассасалари укув режаларида муносиб урин эгаллайди.

Ушбу курснинг вазифалари:

- Талабаларда компьютер тармоклари ва тизимларида ахборот хавфсизлиги тугрисидаги билимларни шакллантириш;
- Ахборотни химоя килишнинг назарий, амалий ва услубий асосларини бериш;
- Талабаларга компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллашни амалий жихатдан ургатиш;
- Талабаларни ахборотни химоя килиш буйича ишлаб чикарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

Курсни узлаштириш натижасида талаба куйидагиларнибилиши шарт;

- компьютер тармоклари ва тизимларидаги ахборот хавфсизлигига тахдид солиши кутилаётган хавф хатарнинг мохиятини ва окибатларини тушуниши;
- компьютер тармоклари ва тизимларида ахборотни химоя килиш буйича куйиладиган асосий талаблар ва асосларни узлаштириш;
- компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашда кулланиладиган замонавий усуллар ва воситаларни билиш;
- тизимларда ахборот бутунлиги ва ишочлигини бузувчи вируслар ва бошка манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлаштириш буйича чораларни куриш;

ахборотни химоя килишда кулланиладиган замонавий амалий тизимлар ва дастурий махсулотларни ишлата олиш;

Фанни ўқитиш «Информатика», «Алгоритмик тиллар», «Ахборотни ҳимоялаш асослари» фанлари асосида олиб бориши керак. Ўқитиш жараёнида талабалар назарий сонли усуллар асосида криптотаҳлил қобилиятларини эгаллайдилар.

3.4. Ўқув дастури

Кириш

5130200 – “Амалий математика ва информатика” йўналиши бўйича бакалаврни тайёрлаш ўқув режасида «Ахборотларни ҳимоялаш» ўқув фани махсус фанлар таркибига киритилган.

Ушбу намунавий ўқув дастурида «Ахборот хавфсизлиги» фанига тегишли бўлган барча мавзулар бўйича талабаларга Давлат таълим стандартлари асосида етказилиши шарт бўлган минимум билимлар ва кўникмалар тўла қамраб олинган.

Фанни ўқитилишидан мақсад: криптографияни статистик усулларини ўрганиш ва улар асосида ахборотни ҳимоялаш қобилиятларини эгаллаш.

Таълабалар ахборотни ҳимоялаш ва криптография асослари ҳақида тушунчага эга бўлишлари керак, ҳамда ахборотни ҳимоялаш дастурий ва техник воситаларини ишлатиш қобилиятига эга бўлишлари керак.

Фанни ўқитиш «Информатика», «Алгоритмик тиллар», «Ахборотни ҳимоялаш асослари» фанлари асосида олиб бориши керак. Ўқитиш жараёнида талабалар назарий сонли усуллар асосида криптотаҳлил қобилиятларини эгаллайдилар.

Ахборотларнинг эҳтимолли- статистик моделлари ва уларнинг энтропияли хоссалари

Дискрет ахборотлар ва уларнинг эҳтимолли моделлари. Энтропия функционал ва унинг хоссалари. Шартли энтропия ва унинг хоссалари. Стационар символли кетма-кетликнинг нисбий энтропияси. Марков символли кетма-кетликнинг энтропияли характеристикалари. Узлуксиз ахборотлар манбалари ва уларнинг энтропияли хоссалари.

Криптологияда ахборотлар назарияси усуллари

Дискрет ахборотлар стационар манбасининг асимптотик хоссалари. Символли кетма- кетликнинг энтропияли турғунлиги. Шеннон бўйича ахборот миқдори ва унинг хоссалари. Криптотизимлар Шеннон моделлари. Симметрик криптотизимлар турғунлиги назарий-информацион баҳолари.

Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш

Текис тарқалган тасодифий кетма-кетлик ва унинг хоссалари. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш универсал алгоритми. n-сериялар тести. Интерваллар тести. Умумлашган покер-тест. “Купон йиғувчи” тести. Алмаштиришлар тести. Кесишувчи n-грамм тести. Иккилик матрицалар рангларига асосланган тест. Спектрал тестлар. Тасодифий силжишлар тестлари. Маурер универсал статистик тести. Энтропиялар ошишига асосланган тестлар. Лемпел – Зив сиқиш алгоритмига асосланган тест. Чизиқли муракабликка асосланган тест. Скаляр кўпайтма экстремал статистикасига асосланган тест. Дельта кўпайтма экстремал статистикасига асосланган тест. Тасодифийликни алгоритмик аниқлаш.

Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмлари

Генерация алгоритмлари классификацияси. Чизиқли ва мультипликатив конгруэнт генераторлар. Ночизиқ конгруэнт генераторлар. Чекли майдонда рекуррентлар. Тескари алоқали силжитиш чизиқли регистрлари томонидан яратиладиган кетма-кетликлар. Фибоначчи генераторлари. Бир томонлама функциялар асосида криптотурғун генераторлар. Сонлар назариясига асосланган криптотурғун генераторлар. Элементар псевдотасодифий кетма-кетликларни “яхшилаш” усуллари. Макларен - Марсальи усуллари билан генерация алгоритмларини комбинация қилиш. LFSR-генераторларини комбинация қилиш. Тасодифий параметрларга эга конгруэнт генератор.

Оқимли криптотизимлар

Асосий тушунчалар. Рекуррент кетма-кетликлар. Чизиқли рекуррент кетма-кетликлар. Чизиқли рекуррент кетма- кетликлар параметрларини баҳолаш. Чизиқли мураккаблик. Чизиқли рекуррент кетма-кетликлар бошланғич холатини аниқлаш. Кетма-кетликларни комбинация қилиш. Корреляцион криптотаҳлил.

Симметрик тизимлар криптотаҳлили математик усуллари

Криптотаҳлил вазифалари ва принциплари. “Синаб кўриш” усули ва унинг мураккаблиги. Статистик қарор қабул қилиш назариясига асосланган криптотаҳлил усуллари. Айирмали криптотаҳлил. Чизиқли криптотаҳлил.

Амалий машғулотлар

Ахборотларнинг эҳтимолли- статистик моделлари ва уларнинг энтропияли хоссалари. Криптологияда ахборотлар назарияси усуллари. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш. Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмлари. Оқимли криптотизимлар. Симметрик тизимлар криптотаҳлили математик усуллари.

Лаборатория иши

Ахборотларнинг эҳтимолли- статистик моделларини дастурлаш. Криптологияда ахборотлар назарияси усулларини дастурлаш. Тасодифий ва псевдотасодифий кетма-кетликларни статистик тестлаш. Псевдотасодифий кетма-кетликларни генерация қилиш алгоритмларини дастурлаш. Оқимли криптотизимларни дастурлаш. Симметрик тизимлар криптотаҳлилларини дастурлаш

Мустақил иш

Криптографиянинг статистик усуллари ривожланиш босқичлари билан танишиш. Криптографияда статистик усуллардан фойдаланиш йўллари. Квант криптографияси асослари. Ассимметрик тизимлар таҳлили статистик усулларининг замонавий ҳолати.

Дарслик ва ўқув қўлланмалари рўйхати

Асосий

1. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).
2. Ященко В.В. Введение в криптографию. МЦМО, 2003
3. Масленников. Практическая криптография BHV – СПб 2003
4. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф. 2002.
5. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком . 2002
6. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат. -1994.-400с.
7. Вербицкий О.В.Вступление к криптологии.- Львов.: Издательство науково-техничной литературы.-1998.-300с.
8. Диффи У. Первые десять лет криптографии с открытым ключом //ТИИЭР, т. 76(1988)б Т5б с. 54-74.

Қўшимча

1. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления применения криптографических методов защиты информации.- М.: Радио и связь.-1989.-360с.
2. Миллер В. Использования эллиптических кривых в криптографии .: -1986.-417-426с.
3. Галатенко В.А. Информационная безопасность. –М.: Финансы и статистика, 1997. –158 с.
4. Грегори С. Смит. Программы шифрования данных // Мир ПК –1997. -№3. -С.58 - 68.
5. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. –208 с.
6. Терехов А. Н., Тискин А. В. // Программирование РАН. –1994. -N 5 -С. 17—22.
7. Криптология – наука о тайнописи // Компьютерное обозрение. –1999. -№3. –С. 10 – 17.
8. Баричев С. В. Криптография без секретов. –М.: Наука, 1998. –120 с.

Интернет маълумотлари

1. "Организация и технология защиты информации" security.aspu.ru/index.
2. Криптографические алгоритмы | Безопасность lib.kbsu.ru/elib/disk/compress

3.5. Ишчи ўқув дастури

Кириш

Олий таълимнинг Давлат таълим стандартига кўра “Математика” таълим соҳасининг “Амалий математика ва информатика” йўналишида ўқитиладиган «Ахборотларни ҳимоялаш» фани дастурида ахборот ва компютер технологияларини муаммоли ва амалиёт масалаларини ечишга зарур бўладиган барча мавзу ва тушунчаларни талабаларга етказилиши шарт булган минимум билимлар ва кўникмалар тўла қамраб олинган.

Фанннинг мақсад ва вазифалари

«Ахборотларни ҳимоялаш» фани 3 босқичнинг II семестрида ўрганилади. «Ахборотларни ҳимоялаш» фанини ўқитишда талабалар:

- компютер тармоқлари ва тизимларида ахборот хавфсизлиги тугрисидаги билимлар;
- ахборотни ҳимоя қилишнинг назарий, амалий ва услубий асослари;
- компютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллаш;
- ахборотни ҳимоя қилиш буйича ишлаб чиқарилган турли хил дастурий махсулотлардан еркин фойдалана олиш имконини берадиган билимлар бўйича тушунчалар билан танишадилар ва кўникмаларни егаллайдилар.

Фаннинг вазифаси талабаларни турли муаммовий ва ишлаб чиқариш масалалари ечимини лойиҳалаш, моделлаштириш, дастурлаш ва сонли натижалар олиш кўникмаларини беришга қаратилган. Шу билан бир қаторда, талабалар мустақил маслалани таҳлил этиш, фикрлаш ва амалаиётга жорий қилиш тажрибаларини ўрганишади.

Фан бўйича талабаларнинг малакасига қуйиладиган талаблар

«Ахборотларни ҳимоялаш» ўқув фанини ўзлаштириш жараёнида амалга ошириладиган масалалар доирасида бакалавр бакалавр қуйидагиларни бажара олиш лозим:

- компютер тармоқлари ва тизимларидаги ахборот хавфсизлигига таҳдид солиши кутилаётган хавф хатарнинг моҳиятини ва оқибатларини тушуниши;
- компютер тармоқлари ва тизимларида ахборотни ҳимоя қилиш буйича қуйиладиган асосий талаблар ва асосларни ўзлаштириш;
- компютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашда қулланиладиган замонавий усуллар ва воситаларни билиш;
- тизимларда ахборот бутунлиги ва ишончлигини бузувчи вируслар ва бошқа манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлантириш бўйича чораларни куриш;
- ахборотни ҳимоя қилишда қулланиладиган замонавий амалий тизимлар ва дастурий махсулотларни ишлата олиш куникмаларга эга бўлиши керак.

Ўқув режадаги бошқа фанлар билан ўзаро боғлиқлиги

Амалий математика ва информатика йўналишининг бакалавр босқичида ўқиладиган умумкасбий фанлар туркумидаги “Ахборотларни ҳимоялаш” фани 3 курснинг ИИ-семестрда ўқитилади. Фанни ўқитиш «Информатика», «Алгоритмик тиллар», «Ахборотни ҳимоялаш асослари» фанлари асосида олиб бориши керак. Дастурни амалга ошириш ўқув режадаги “Математик анализ”, “Аналитик геометрия ва чизиқли алгебра” ҳамда

“Программалаш асослари” каби фанлар билан узвий боғланганлиги сабабли ушбу фанларни билиш талаб қилинади. Ўқитиш жараёнида талабалар назарий сонли усуллар асосида криптотаҳлил қобилиятларини эгаллайдилар.

Фанни ўқитишда замонавий ахборот ва педагогик технологиялар

Талабаларнинг фанни мувафақиятли ўзлаштириши учун ўқитишнинг илғор ва замонавий усулларидан фойдаланиш, янги ахборот-педагогик технологияни тадбиқ этиш муҳим аҳамиятга егадир. Фанни ўзлаштиришда дарслик, ўқув ва услубий қўлланмалар, маъруза матнлари, тарқатма материаллар, электрон материаллар, плакатлардан фойдаланилади.

Маъруза ва амалий машғулотларда мос равишда илғор педагогик ва компютер технологиялардан фойдаланилади.

Ўқув жараёнида фанни ўтиш сифатини белгиловчи қуйидаги ҳолатлар еътиборга олинади: юқори илмий даражада дарс бериш, муаммоли маърузалар ўқиш, дарсларни савол-жавоб тарзда қизиқарли ташкил қилиш, илғор педагогик технологиялардан ва мултимедиа воситалардан фойдаланиш, тингловчиларни ундайдиган, ўйлантирадиган муаммоларни улар олдига қуйиш, эркин мулоқот юритишга, илмий изланишга жалб қилиш.

«Ахборотларни ҳимоялаш» курсини лойиҳалаштиришда қуйидаги асосий концептуал ёндошувлардан фойдаланилади:

Шахсга йўналтирилган таълим. Бунда келгусидаги мутахассис фаолияти билан боғлиқ ўқитиш, масалалар, мавзулар ишчи дастурда кўрилиши кераклиги назарда тутилган.

Тизимли ёндошув. “Амалий математика ва информатика” таълим йўналишининг барча белгилари мужассам этилиши, барча фанларнинг ўзаро боғланганлиги ва таълим технологиясининг яхлитлиги назарда тутилган.

Фаолиятга йўналтирилган ёндошув. Мазкур дастурда келгусидаги мутахассис сифатларини шакллантириш, активлаштириш ва унинг барча қобилияти ва ташаббускорлигини очишга эътибор берилган.

Диалогик ёндошув. Фаннинг амалиёт дарсларида шахснинг ўз-ўзини фаоллаштириш, ўзини кўрсата олиш каби ижодий фаолиятларини ривожлантириш назарда тутилган.

Хамкорликдаги таълимни ташкил қилиш. Талабаларнинг қуйилган масала ечимларини олишда биргаликдаги ишлашни жорий этиш зарурлиги эътиборга олинган.

Муаммоли таълим. Таълим олувчи фаолиятини активлаштириш учун фан дастури билан боғлиқ қизиқарли мавзулар муҳокама қилинишлиги, бунда илмий билимнинг обектив қарама-қаршилиги, уни ҳал этиш усуллари, амалий фаолиятга уларни қўллаш масалаларни муҳокама қилиш назарда тутилган.

Ахборотни тақдим қилишнинг замонавий воситалари ва усулларини қўллаш – янги компютер ва ахборот технологияларни ўқув жараёнига қўллаш.

Ўқитишнинг мавзулари ва техникаси. Маъруза, муаммоли таълим, кейс-технология, пинборд, парадокс ва лойиҳлаш усуллари, амалий ишлар.

Ўқитишни ташкил этиш шакллари. Диалог, мулоқот, хамкорлик, ўзаро ўрганишга асосланган фронтал, коллектив ва гуруҳ.

Ўқитиш воситалари. Дарслик, маъруза матни, электрон китоб, электрон ўқув қўлланмалар, электрон ўйинлар ва шу билан бир қаторда компютер ва ахборот технологиялари.

Коммуникасия усуллари. Тингловчилар билан оператив тескари алоқага асоланган бевосита ўзаро муносабатлар.

Тескари алоқа усуллари ва воситалари: кузатиш, блиц-сўров, оралиқ, жорий, якуний назорат таҳлили.

Бошқариш усуллари ва воситалари: ўқув машғулоти босқичларини белгилаб берувчи технологик харита кўринишидаги ўқув машғулотларини режалаштириш, қуйилган мақсадга эришишда ўқитувчи ва тингловчининг биргаликдаги харакати, аудитория машғулотлари ва мустақил ишлар назорати.

Мониторинг ва баҳолаш. Курс оҳирида тест топшириқлари ёки ёзма иш варинатлари бўйича талабалар билимлари баҳоланади.

Айрим мавзулар бўйича талабалар билим баҳолаш тест асосида ва компютер ёрдамида бажарилади. Интернет тармоғидаги расмий иқтисодий кўрсаткичларидан фойдаланилади, тарқатма материаллар тайёрланади, таянч сўз ва иборалар асосида оралиқ ва якуний назоратлар ўтказилади.

«Ахборотларни ҳимоялаш» фанидан машғулотларнинг мавзулар ва соатлар бўйича тақсимланиши

т/р	Мавзулар номи	Жами соат	Маъру-за	Ама-лиёт	Мус-тақил таълим
1	Ахборот хавфсизлигига кириш; Ҳимоялаш тизимининг комплекслилиги; Ахборотларни ташкилий ҳимоялаш элементлари; Ахборот тизимларида маълумотларга насбатан хавф-хатарлар. Вирус ва антивируслар турлари; Вирусларга қарши чора-тадбирлар				
2	Замонавий компютер стенографияси; Компютер стенографияси истиқболлари; Компютер стенографиясининг асосий вазифалари; Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш.				
3	Криптография ҳақида асосий тушунчалар; Ахборотларни криптографияли ҳимоялаш тамойиллари; Симметрияли криптотизим асослари; Ўринларни алмаштириш усуллари.				
4	Электрон почтага рухсатсиз кириш; Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари. Компютер тармоқларида ҳимояни таъминлаш усуллари; Интернет тармоғида мавжуд алоқанинг ҳимоясини (хавфсизлигини) таъминлаш асослари. Тармоқлараро экран ва унинг вазифалари, асосий компонентлари.				
5	Электрон туловлар тизими асослари. Идентификасияловчн шахсий номерни ҳимоялаш. Интернетда мавжуд электрон туловлар хавфсизлигини таъминлаш. Компютер тармоқлари ва тизимларининг ҳимояланганлик даражасини аниқлаш				

Асосий қисм: Фаннинг услубий жиҳатдан узвий кетма-кетлиги

Асосий қисмда (маъруза) фанни мавзулари мантиқий кетма-кетликда келтирилади. Ҳар бир мавзунинг моҳияти асосий тушунчалар ва тезислар орқали очиб берилади. Бунда мавзу бўйича талабаларга ДТС асос етказилиши зарур бўлган билим ва кўникмалар тўла қамраб олиниши керак.

Асосий қисм сифатига қўйиладиган талаб мавзуларнинг долзарблиги, уларнинг иш берувчилар талаблари ва иш бажариш эҳтиёжларига мослиги, мамлакатимизда бўлаётган

ижтимоий-сиёсий ва демократик ўзгаришлар, иқтисодиётни еркинлаштириш, иқтисодий-ҳуқуқий ва бошқа соҳалардаги ислоҳатларнинг устувор масалаларини қамраб олиш ҳамда фан технологияларнинг сўнги ютуқлари эътиборга олиниши тавсия этилади.

Маъруза машғулотлари

Ахборот хавфсизлигига кириш. Ҳимоялаш тизимининг комплекслилиги. Ахборотларни ташкилий ҳимоялаш элементлари. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар. Вирус ва антивируслар турлари. Вирусларга қарши чора-тадбирлар.

Қўлланиладиган таълим технологиялари: *диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат.*

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ 1, Қ2.

Замонавий компютер стенографияси. Компютер стенографияси истиқболлари. Компютер стенографиясининг асосий вазифалари. Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш.

Қўлланиладиган таълим технологиялари: *диалогик ёндошув, муаммоли таълим. Блис-сўров, мунозара, инсерт, Т-схемаси, ўз-ўзини назорат.*

Адабиётлар: А2, А3, А5, Қ1, Қ2.

Криптография ҳақида асосий тушунчалар. Ахборотларни криптографияли ҳимоялаш тамойиллари. Симметрияли криптотизим асослари. Ўринларни алмаштириш усуллари. Алмаштириш усуллари.

Қўлланиладиган таълим технологиялари: *диалогик ёндошув, муаммоли таълим. Блис-сўров, мунозара,4х4 сўров, алгоритм, ўз-ўзини назорат.*

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ2, Қ3, Қ4, Қ5, Қ6.

Электрон почта ва Интернет тармоғида ахборот ҳимоясини таъминлаш. Электрон почтага рухсатсиз кириш. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари. Компютер тармоқларида ҳимояни таъминлаш усуллари. Интернет тармоғида мавжуд алоқанинг ҳимоясини (хавфсизлигини) таъминлаш асослари. Тармоқлараро экран ва унинг вазифалари. Тармоқлараро экраннинг асосий компонентлари.

Қўлланиладиган таълим технологиялари: *диалогик ёндошув, муаммоли таълим. Кластер, фикрлаш мунозара, савол-жавоб, ўз-ўзини назорат.*

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ1.

Электрон тулов тизимларида ахборот хавфсизлиги. Электрон туловлар тизими асослари. Идентификасияловчн шахсий номерни ҳимоялаш. Интернетда мавжуд электрон туловлар хавфсизлигини таъминлаш. Компютер тармоқлари ва тизимларининг ҳимояланганлик даражасини аниқлаш воситалари.

Қўлланиладиган таълим технологиялари: *диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат.*

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ1.

«Ахборотларни ҳимоялаш» фани бўйича календар тематик режа

№	Маъруза мавзулари	
1	Замонавий ахборотлашган жамият ва ахборот хавфсизлиги. Асосий тушунчалар ва таърифлар	
2	Вирус ва антивируслар таснифи	
3	Ахборотларни стеганографик ҳимоялаш усуллари	

4	Ахборотларни криптографик ҳимоялаш усуллари	
5	Маълумотларнинг тарқалиб кэтиши ва маълумотларга руҳсациз кириш.	
6	Компютер тармоқларида замонавий ҳимоялаш усуллари ва воситалари	
7	Интернетда ахборотлар хавфсизлигини таъминлаш асослари	
8	Электрон почтада ахборотларга нисбатан мавжуд хавф-хатарлар ва улардан ҳимояланиш асослари	
9	Электрон туловлар тизимида ахборотларни ҳимоялаш	
10	Компютер тармоқлари ва тизимларининг ҳимояланганлик даражасини аниқлаш воситалари	
	Жами	

Амалиёт машғулотлари

Дастурларни компютер вирусларидан ҳимоялаш. Вируслар таснифи. Вирус фаолияти сикли. Дастурларни ваксинация усули билан вируслардан ҳимоялаш

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, шахсга йўналтирилган таълим.

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ1, Қ2.

Антивирус дастурлари. Антивирус Касперский 6.0. дастурини ўрнатиш ва созлаш. Антивирус Касперский 6.0. дастурида вируслар мавжудлигини текшириш асосий масаларини бошқариш механизми. Антивирус Касперский 6.0. дастурида ҳимоя диагностикасининг принциплари. Резерв омбор ва карантин билан ишлаш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, шахсга йўналтирилган таълим.

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ1, Қ2.

Дастурларни норасмий нушалашдан ҳимоялаш асослари. Муҳитнинг шахсий аломатларини таҳлил қилиш. Оператив хотира хажмини аниқлаш ва ҳимоялаш дастурига киритиш. Инструментал таркибини аниқлаш ва ҳимоялаш дастурига киритиш. Дастурларни трассировкадан ҳимоялаш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, шахсга йўналтирилган таълим.

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ2, Қ3, Қ4, Қ5, Қ6.

Ахборот хавфсизлигининг криптографик усуллари. Классик симметрик криптотизимлар. Ўрин алмаштириш шифрлари. Шифрлаш жадваллари. Сеҳрли квадратларни қўллаш. Трисемус шифрлаш жадвали. Плейфейр биграмма шифри. Ҳилл криптотизими.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, шахсга йўналтирилган таълим.

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ2, Қ3, Қ4, Қ5, Қ6.

Локал ва глобал тармоқларда ахборотлар хавфсизлигини тармоқ экрани асосида таъминлаш. Ҳимояловчи тармоқ экран таркибий елементлари. Локал тармоқга экранни ўрнатиш. Локал ва глобал тармоқларда тармоқ экранини бошқариш.

Қўлланиладиган таълим технологиялари: диалогик ёндошув, муаммоли таълим, шахсга йўналтирилган таълим.

Адабиётлар: А1, А2, А3, А4, А5, А6, Қ2, Қ3, Қ4, Қ5, Қ6.

№	Амалиёт машғулотлари	
1.	**Дастурларни компютер вирусларидан ҳимоялаш.** 1. Вируслар таснифи. Вирус фаолияти сикли.	

	2. Дастурларни вакцинация усули билан вируслардан ҳимоялаш	
2.	**Антивирус дастурлари.** 3. Антивирус Касперский 6.0. дастурини ўрнатиш ва созлаш. 4. Антивирус Касперский 6.0. дастурида вируслар мавжудлигини текшириш асосий масаларини бошқариш механизми. 5. Антивирус Касперский 6.0. дастурида ҳимоя диагностикасининг принциплари. 6. Резерв омбор ва карантин билан ишлаш.	
3.	**Дастурларни норасмий нушалашдан ҳимоялаш асослари** 7. Муҳитнинг шахсий аломатларини таҳлил қилиш. 8. Оператив хотира хажмини аниқлаш ва ҳимоялаш дастурига киритиш. 9. Инструментал таркибини аниқлаш ва ҳимоялаш дастурига киритиш. 10. Дастурларни трассировкадан ҳимоялаш	
4.	**Ахборот хавфсизлигининг криптографик усуллари** 11. Классик симметрик криптотизимлар. 12. Ўрин алмаштириш шифрлари. 13. Шифрлаш жадваллари. 14. Сеҳрли квадратларни қўллаш. 15. Трисемус шифрлаш жадвали. 16. Плейфейр биграмма шифри. 17. Ҳилл криптотизими.	
5.	**Локал ва глобал тармоқларда ахборотлар хавфсизлигини тармоқ экрани асосида таъминлаш.** 18. Ҳимояловчи тармоқ экран таркибий елементлари. 19. Локал тармоқга экранни ўрнатиш. 20. Локал ва глобал тармоқларда тармоқ экранини бошқариш	
	Жами	

Мустақил таълимни ташкил этишнинг шакли ва мазмуни

«Ахборотларни ҳимоялаш» фани бўйича талабанинг мустақил таълими шу фанни ўрганиш жараёнининг таркибий қисмидир.

Талабалар айрим мавзуларни кенгроқ ўрганиш мақсадида қўшимча адабиётларни ўқиб, рефератлар тайёрлайдилар ва машғулот режаси бўйича қуйилган масала ечимини моделлаштириш, алгоритмларини тузиш ва дастурий воситаларини қўллаш билан боғлиқ саволларни ёритадиган лойиҳалар тайёрлашади.

Мустақил таълим натижалари рейтинг тизими асосида баҳоланади. Бунинг учун берилган вазифаларни текшириш ва баҳолаш амалий машғулот олиб борувчи ўқитувчи томонидан амалга оширилади. Конспектларни ва мавзуларни ўзлаштириш даражасини баҳолаш еса, маъруза дарсларини олиб борувчи ўқитувчи томонидан бажарилади. «Ахборотларни ҳимоялаш» фани бўйича мустақил иш мажмуаси барча мавзуларни қамраб олган ва қуйидаги мавзулар кўринишида шакллантирилади.

Мустақил таълимнинг мазмуни ва ҳажми (43 соат)

№	Мустақил машғулот мавзулари	Берилган топшириқлар	Бажариш муддати	Ҳажми, соат
ВИ семестр				
1	Ахборотларга нисбатан хавф-хатарлар таснифи.	Реферат тайёрлаш		4
2	Тармоқ хавфсизлигини назорат қилиш воситалари	Реферат тайёрлаш		
3	Ахборотни ҳимоялаш усулларининг	Реферат тайёрлаш		

	тизимлилиги		1,2,3 хафталар	
5	Ахборотларни ташкилий ҳимоялаш елементлари	Реферат тайёрлаш		
6	Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар	Реферат тайёрлаш		4
7	Компютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланиш.	Вируслардан ҳимояланиш тизимини ташкил қилиш бўйич тавсиялар ишлаб чиқиш	4 хафта	2
8	Антивирус дастурлари			2
9	Вирусларга қарши чора-тадбирлар			2
10	Замонавий компютер стенографияси	Реферат тайёрлаш	5,6 хафталар	
11	Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш	Реферат тайёрлаш		4
12	Ахборотларни ҳимоялашнинг криптографик усуллари	Реферат тайёрлаш		
13	Симметрияли криптотизимлар	Реферат тайёрлаш		4
14	Ўринларни алмаштириш усуллари	Реферат тайёрлаш		
15	Электрон почтага рухсатсиз киришдан ҳимояланиш	Реферат тайёрлаш	7,8,9 хафталар	
16	Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари	Реферат тайёрлаш		4
17	Компютер тармоқларининг заиф қисмлари. Тармоқ ҳимоясини ташкил қилиш	Реферат тайёрлаш		
18	Компютер телефониясидаги ҳимоялаш усуллари	Реферат тайёрлаш		4
19	ЭҲМ ҳимоясини таъминлашнинг техник воситалари	Реферат тайёрлаш		
20	Интернет тармоғида мавжуд алоқанинг хавфсизлигини таъминлаш	Реферат тайёрлаш	10,11 хафталар	
21	Интернетда рухсатсиз кириш усулларининг таснифи. Рухсат этилган манзилларнинг рухсат етилмаган вақтда уланиши	Реферат тайёрлаш		6
22	Тармоқлараро экран ва унинг вазифалари. Тармоқлараро экраннинг асосий компонентлари.	Экранни тизимда уланиши ва созлаш бўйича тавсиялар ишлаб чиқиш		
23	Электрон почтада мавжуд хавфлар. Электрон почтани ҳимоялаш	Экранни тизимда уланиши ва созлаш бўйича тавсиялар ишлаб чиқиш		
24	Электрон туловлар тизимида идентификасия-ловчн шахсий номерни ҳимоялаш.	Реферат тайёрлаш	12, 13 хафталар	
25	Банкоматлар хавфсизлигини таъминлаш	Реферат тайёрлаш		6
26	Интернетда мавжуд электрон туловлар хавфсизлигини таъминлаш	Реферат тайёрлаш		
27	Дастурларни ваксинасия усули билан вируслардан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш		

28	Мавжуд exe-файлларни ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш	14-17 хафталар	8
29	Антивирус Касперский 6.0. дастури	Дастурни ШЭҲМда ўрнатиш ва созлаҳ бўйича ҳисобот тайёрлаш		
30	Дастурларни норасмий нушалашдан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш		
31	Дастурларни трассировкадан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш Ҳисобот тайёрлаш		
32	Шифрлаш жадваллари. Сеҳрли квадратларни қўллаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш	18-20 хафталар	6 соат
33	Оддий алмаштириш шифрлари. Сезар шифрлаш тизими	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш		
34	Ўрнига қўйиш Афина тизими. Трисемус шифрлаш жадвали	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш		
35	Плейфейр биграмма шифри. Ҳилл криптотизими	Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш		
			Жами	

Дастурнинг инфромацион услубий таъминоти

Мазкур фанни ўқитиш жараёнида замонавий ахборот, педагогик ва коммуникасион технологияларни қўллаш назарда тутилган. Буларнинг асосини замонавий компютерлар, билим бериш дастурий воситалари, презентация, визуал лаборатория, электрон дидактик технологиялар ташкил қилади.

Фаннинг услубий асослари сифатида амалий машғулотларида ақлий хужум, гуруҳли фикрлаш, “иш уйинини” ташкил қилиш ва бошқа педагогик технологиялардан фойдаланиш назарда тутилади.

«Ахборотларни ҳимоялаш» фанидан талабалар билимини рейтинг тизими асосида бахолаш мезони

Фан бўйича рейтинг жадваллари, назорат тури, шакли, сони, ҳамда хар бир назоратга ажратилган максимал балл, шунингдек жорий ва оралиқ назоратларнинг саралаш баллари ҳақидаги маълумотлар биринчи машғулотда талабаларга эълон қилинади.

Давлат таълим стандартларига мувофиқ қуйидаги назорат турлари ўтказилади.

Жорий назорат (ЖН). Талабанинг фан мавзулари бўйича билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. ЖН амалий машғулотларда оғзаки сўров, тест ўтказиш, сухбат, назорат иши, коллоквиум, уй вазифаларини текшириш ва шу каби бошқа назорат шаклларида ўтказилади.

Оралиқ назорат (ОН). Семестр давомида ўқув дастурининг тегишли (фаннинг бир неча мавзуларини ўз ичига олган) бўлими тугаллангандан кейин, талабанинг назарий билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. ОН бир семестрда икки марта ўтказилади ва шакли (ёзма, оғзаки, тест ва х.к.) ўқув фанига ажратилган умумий соатлар ҳажмидан келиб чиққан ҳолда белгиланади.

Якуний назорат (ЯН). Семестр якунида муаян фан бўйича назарий билим ва амалий кўникмаларни талабалар томонидан ўзлаштириш даражасини баҳолаш усули. ЯН асосан таянч тушунча ва ибораларга асосланган “ёзма иш” шаклида ўтказилади.

ОН ўтказиш жараёни кафедра мудири томонидан тузилган комиссия иштирокида мунтазам равишда ўрганиб борилади ва уни ўтказиш тартиблари бузилган ҳолларда ОН натижалари бекор қилиниши мумкин. Бундай ҳолларда ОН қайта ўтказилади.

ОТМ ректорининг буйруғи билан ички назорат ва мониторинг бўлими раҳбарлигида тузилган комиссия ЯНни ўтказиш жараёнини мунтазам равишда кузатиб боради ва уни ўтказиш тартиблари бузилган ҳолларда ЯН натижалари бекор қилиниши мумкин. Бундай ҳолларда ЯН қайта ўтказилади.

Талабанинг билим савияси, кўникма ва малакаларини назорат қилиш рейтинг тизимига асосан, талабани фан бўйича ўзлаштириш даражаси баллар орқали ифодаланади.

Талабанинг семестр давомида ўзлаштириш кўрсаткичи 100 баллик тизимида баҳоланади. Ушбу 100 балл баҳолаш турлари бўйича қуйидагича тақсимланади:

ЯН - 30 балл; ЖН - 35 балл; ОН – 35 балл

Балл	Баҳо	Талабанинг билим даражаси
86-100	Аъло	Ижодий фикрлай олиш; мустақил мулоҳаза юрита олиш; олган билимларини амалда қўллай олиш; моҳиятини тушунтириш; тушунчаларни билиш, айтиб бериш, тасаввурга ега бўлиш; хулоса ва қарор қабул қилиш
71-85	Яхши	Мустақил мулоҳаза қилиш; олган билимларини амалда қўллай оли; моҳиятини тушунтириш; тушунчаларни билиш, айтиб бериш, тасаввурга ега бўлиш.
55-70	Қониқарли	Моҳиятини тушунтириш; тушунчаларни билиш, айтиб бериш, тасаввурга ега бўлиш.
0-54	Қониқарсиз	Аниқ тасаввурга ега бўлмаслик, билмаслик

Фан бўйича саралаш бали 55 баллни ташкил етади. Талабанинг саралаш балидан паст бўлган ўзлаштириши рейтинг дафтарчасида қайд етилмайди.

Талабанинг ўқув фани бўйича мустақил иши ЖН. ОН ва ЯН жараёнида тегишли топшириқларни бажариши ва унга ажратилган баллардан келиб чиққан ҳолда баҳоланади.

Талабанинг фан бўйича рейтинги қуйидагича аниқланади $R = \frac{i\ ^*\hat{A}}{100}$, бу ерда Ў – фан бўйича ўзлаштириш даражаси (балл), В – семестрда фанга ажратилган умумий ўқув юкламаси (соат).

Фан бўйича ЖН ва ОНларига ажратилган умумий баллнинг 50% саралаш бали ҳисобланиб, ушбу фоиздан кам балл тўплаган талаба ЯНга киритилмайди.

ЖН ва ОН турлари бўйича 55 балл ва ундан юқори баллни тўплаган талаба фанни ўзлаштирган деб ҳисобланади ва ушбу фан бўйича ЯНга кирмаслиги мумкин.

Талабанинг семестр давомида фан бўйича тўплаган умумий бали хар бир назорат туридан тўплаган баллари йиғиндисига тенг.

ОН ва ЯН турлари календар тематик режасига мувофиқ деканат томонидан тузилган рейтинг назорат жадваллари асосида ўтказилади. ЯН семестрнинг оҳирги икки хафтаси мобайнида ўтказилади.

ЖН ва ОН назоратларида саралаш балидан кам балл тўплаган ва узрли сабабалрга кўра назоратда қатнаша олмаган талабага қайта топшириш учун навбатдаги шу назорат туригача, сўнгги ЖН ва ОН учун еса ЯНгача бўлган муддат берилади.

Талабанинг семестрда ЖН ва ОН турлари бўйича тўплаган баллари ушбу назорат турлари умумий балининг 50% дан кам бўлса ёки семестр ЖН, ОН ва ЯН бўйича тўплаган баллари йиғиндиси **55 баллдан кам бўлса** у **академик қарздор** деб ҳисобланади.

Талаба назорат натижаларидан норози бўлса, фан бўйича назорат тури натижалари эълон қилинган вақтдан бошлаб, бир кун мобайнида факултет деканига ариза билан мурожаат этиш мумкин. Бундай ҳолда, деканнинг тақдимномасига кўра, ректор буйруғи билан 3 (уч) аъзодан кам бўлмаган таркибда апеллясия комиссияси ташкил етилади.

Аппелясия комиссияси талабанинг аризаларини кўриб чиқиб, шу куннинг ўзида хулосасини билдиради.

Баҳолашнинг ўрнатилган талаблар асосида, белгиланган муддатларда ўтказилиши, ҳамда расмийлаштирилиши факултет декани, кафедра мудири, ўқув-услубий бошқарма ҳамда ички назорат ва мониторинг бўлими томонидан назорат қилинади.

Талабалар ЖНдан тўплайдиган балларнинг намунавий мезонлари

№	Кўрсаткичлар	ЖН баллари		
		макс	1-ЖН	2-ЖН
1	Дарсларга қатнашганлик ва ўзлаштириш даражаси. Амалий машғулотлардаги фаоллиги, амалий машғулот дафтарларнинг юритилиши ва ҳолати	15	0-7	0-8
2	Мустақил топшириқларининг ўз вақтида ва сифатли бажарилиши. Мавзулар бўйича уй вазифаларининг бажарилиши ва ўзлаштириш даражаси	10	0-5	0-5
3	Ёзма назорат иши ёки тест саволларига берилган жавоблар.	10	0-5	0-5
Жами ЖН баллари		35	0-17	0-18

Талабалар ОНдан тўплайдиган балларнинг намунавий мезонлари

№	Кўрсаткичлар	ОН баллари		
		макс	1-ЖН	2-ЖН
1	Дарсларга қатнашганлик ва ўзлаштириш даражаси. Маъруза дарсларидаги фаоллиги, конспект дафтарининг юритилиши ва тўлиқлиги	15	0-7	0-8
2	Мустақил топшириқларининг ўз вақтида ва сифатли бажарилиши ва ўзлаштириши	10	0-5	0-5
3	Оғзаки савол-жавоблар, коллоквиум, ва бошқа назорат турлари натижалари.	10	0-5	0-5
Жами ЖН баллари		35	0-17	0-18

ЯН ёзма иш шаклида белгиланган бўлса, у ҳолда ЯН 30 баллик “Ёзма иш” вариантлари асосида ўтказилади.

Агар ЯН марказлашган тест асосида ташкил этилган бўлиб, фан бўйича ЯН “Ёзма иш” шаклида белгиланган бўлса, у ҳолда ЯН қуйидаги жадвал асосида амалга оширилади.

№	Кўрсаткичлар	ЯН баллари	
		макс	Ўзлаштириш оралиғи
1	Фан бўйича якуний ёзма иш назорати	6	0-6
2	Фан бўйича якуний тест назорати	24	0-24
Жами		30	0-30

Якуний назоратда “Ёзма иш”ларни баҳолаш мезони

ЯН “Ёзма иш” шаклида амалага ошрилиганда синов кўп вариантли усулда ўтказиилади. Ҳар бир вариант 4 назарий савол ва 1 амалий топшириқдан иборат. Назарий

саволлар фан бўйича таянч сўз ва иборалар асосида тузилган бўлиб , фаннинг барча мавзуларини ўз ичига қамраб олган. Хар бир назарий савол ва ам алий топшириқга ёзилган жавоблар бўйича ўзлаштириш кўрсаткичи 0-6 балл оралиғида баҳоланади. Талаба максимал 30 баллни тўплаши мумкин.

Ёзма синов бўйича умумий ўзлаштириш кўрсаткичини аниқлаш учун, вариантда берилган саволларнинг хар бири учун ёзилган жавобларга қуйилган ўзлаштириш баллари қўшилади ва йиғинди талабанинг ЯН бўйича ўзлаштириш бали ҳисобланади.

Тавсия этилган адабиётлар рўйхати
Асосий адабиётлар

1. Косимов С.С. Ахборот технологиялари. Т: “Алоқачи”. – Тошкент, 2006. – 280 б.
2. Гуломов С.С. ва бошк. Ахборот тизимлари ва технологиялари. Тошкент., «ШАРК», 2000.-591 б.
3. Галатенко В.А. Информационная безопасность. –М.: Финансы и статистика, 1997. – 158 с.
4. Гайкович В., Першин А. Безопасность электронных банковских систем Единая Европа, 1994.
5. Трубачев А.П. и др. Оценка безопасности информационных технологий СИП РИА, 2001. – 180 с.
6. Гафурова М.Т., Дадабаева Р.А. Персонал компьютерларнинг программ системалари.-Тошкент, ТДИУ, 1992.-100 бет.

Қўшимча адабиётлар рўйҳати

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат. -1994.-400с.
2. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).
3. Вербицкий О.В. Вступление к криптологии.- Львов.: Издательство науково-техничной литературы.-1998.-300с.
4. Диффи У. Первые десять лет криптографии с открытым ключом //ТИИЭР, т. 76(1988)б Т5б с. 54-74.
5. Миллер В. Использования эллиптических кривых в криптографии .: -1986.-417-426с.
6. Грегори С. Смит. Программы шифрования данных // Мир ПК –1997. -№3. -С.58 - 68.

Интернет ва Зиёнет сайтлари

1. ҳттп://www.жетинфо.ру/1996/19/1/артисле19.1996.ҳтмл
2. ҳттп://www. жетинфо.ру /1997/4/1/ артисле 1.4.1997.ҳтмл
3. ҳттп://www. жетинфо.ру/1999/1/1/ артисле 1.1.1996.ҳтмл
4. ҳттп://www. жетинфо.ру /2002/5/2/ артисле 2.5.2002.ҳтмл
5. ҳттп://www.интуит.ру

3.6. Календар-тематик режа
«Ахборотларни ҳимоялаш» фани бўйича календар тематик режа

№	Маъруза мавзулари	Соат
1	Замонавий ахборотлашган жамият ва ахборот хавфсизлиги. Асосий тушунчалар ва таърифлар	2
2	Вирус ва антивируслар таснифи	2
3	Ахборотларни стеганографик ҳимоялаш усуллари	2
4	Ахборотларни криптографик ҳимоялаш усуллари	2
5	Маълумотларнинг тарқалиб кетиши ва маълумотларга руҳсатсиз кириш.	2
6	Компютер тармоқларида замонавий ҳимоялаш усуллари ва воситалари	
7	Интернетда ахборотлар хавфсизлигини таъминлаш асослари	2
8	Электрон почтада ахборотларга нисбатан мавжуд хавф-хатарлар ва улардан ҳимояланиш асослари	2
9	Электрон туловлар тизимида ахборотларни ҳимоялаш	2
10	Компютер тармоқлари ва тизимларининг ҳимояланганлик даражасини аниқлаш воситалари	2
	Жами	**20**
№	**Амалиёт машғулотлари**	**соат**
1.	Дастурларни компютер вирусларидан ҳимоялаш. 1. Вируслар таснифи. Вирус фаолияти сикли. 2. Дастурларни ваксинация усули билан вируслардан ҳимоялаш	 2 2
2.	Антивирус дастурлари. 3. Антивирус Касперский 6.0. дастурини ўрнатиш ва созлаш. 4. Антивирус Касперский 6.0. дастурида вируслар мавжудлигини текшириш асосий масаларини бошқариш механизми. 5. Антивирус Касперский 6.0. дастурида ҳимоя диагностикасининг принсиплари. 6. Резерв омбор ва карантин билан ишлаш.	 2 2 2 2
3.	Дастурларни норасмий нушалашдан ҳимоялаш асослари 7. Муҳитнинг шахсий аломатларини таҳлил қилиш. 8. Оператив хотира хажмини аниқлаш ва ҳимоялаш дастурига киритиш. 9. Инструментал таркибини аниқлаш ва ҳимоялаш дастурига киритиш. 10. Дастурларни трассировкадан ҳимоялаш	 2 2 2 2
4.	Ахборот хавфсизлигининг криптографик усуллари 11. Классик симметрик криптотизимлар. 12. Ўрин алмаштириш шифрлари. 13. Шифрлаш жадваллари. 14. Сеҳрли квадратларни қўллаш. 15. Трисемус шифрлаш жадвали. 16. Плейфейр биграмма шифри. 17. Ҳилл криптотизими.	 2 2 2 2 2 2 2
5.	Локал ва глобал тармоқларда ахборотлар хавфсизлигини тармоқ екрани асосида таъминлаш. 18. Ҳимояловчи тармоқ екран таркибий элементлари. 19. Локал тармоқга екранни ўрнатиш. 20. Локал ва глобал тармоқларда тармоқ экранини бошқариш	 2 2 2
	Жами	**40**

4. Таълим технологияси
4.1. Машғулотларнинг педагогик технологияси

“АХБОРОТЛАРНИ ҲИМОЯЛАШ” ФАНИДАН МАЪРУЗА ВА АМАЛИЙ МАШҒУЛОТЛАРДА ЎҚИТИШ ТЕХНОЛОГИЯЛАРИ

Талабаларнинг фанни мувафақиятли ўзлаштириши учун ўқитишнинг илғор ва замонавий усулларидан фойдаланиш, янги ахборот-педагогик технологияни тадбиқ етиш муҳим аҳамиятга егадир. Фанни ўзлаштиришда дарслик, ўқув ва услубий қўлланмалар, маъруза матнлари, тарқатма материаллар, електрон материаллар, плакатлардан фойдаланилади.

Маъруза ва амалий машғулотларда мос равишда илғор педагогик ва компютер технологиялардан фойдаланилади.

Ўқув жараёнида фанни ўтиш сифатини белгиловчи қуйидаги ҳолатлар эътиборга олинади: юқори илмий даражада дарс бериш, муаммоли маърузалар ўқиш, дарсларни савол-жавоб тарзда қизиқарли ташкил қилиш, илғор педагогик технологиялардан ва мултимедиа воситалардан фойдаланиш, тингловчиларни ундайдиган, ўйлантирадиган муаммоларни улар олдига қуйиш, эркин мулоқот юритишга, илмий изланишга жалб қилиш.

“Ахборотларни ҳимоялаш” курсини лойиҳалаштиришда қуйидаги асосий концептуал ёндошувлардан фойдаланилади:

Шахсга йўналтирилган таълим. Бунда келгусидаги мутахассис фаолияти билан боғлиқ ўқитиш, масалалар, мавзулар ишчи дастурда кўрилиши кераклиги назарда тутилган.

Тизимли ёндошув. “Амалий математика ва информатика” таълим йўналишининг барча белгилари мужассам этилиши, барча фанларнинг ўзаро боғланганлиги ва таълим технологиясининг яхлитлиги назарда тутилган.

Фаолиятга йўналтирилган ёндошув. Мазкур дастурда келгусидаги мутахассис сифатларини шакллантириш, активлаштириш ва унинг барча қобилияти ва ташаббускорлигини очишга эътибор берилган.

Диалогик ёндошув. Фаннинг амалиёт дарсларида шахснинг ўз-ўзини фаоллаштириш, ўзини кўрсата олиш каби ижодий фаолиятларини ривожлантириш назарда тутилган.

Хамкорликдаги таълимни ташкил қилиш. Талабаларнинг қуйилган масала ечимларини олишда биргаликдаги ишлашни жорий этиш зарурлиги эътиборга олинган.

Муаммоли таълим. Таълим олувчи фаолиятини активлаштириш учун фан дастури билан боғлиқ қизиқарли мавзулар муҳокама қилинишлиги, бунда илмий билимнинг обектив қарама-қаршилиги, уни ҳал этиш усуллари, амалий фаолиятга уларни қўллаш масалаларни муҳокама қилиш назарда тутилган.

Ахборотни тақдим қилишнинг замонавий воситалари ва усулларини қўллаш – янги компютер ва ахборот технологияларни ўқув жараёнига қўллаш.

Ўқитишнинг мавзулари ва техникаси. Маъруза, муаммоли таълим, кейс-технология, пинборд, парадокс ва лойиҳлаш усуллари, амалий ишлар.

Ўқитишни ташкил етиш шакллари. Диалог, мулоқот, хамкорлик, ўзаро ўрганишга асосланган фронтал, коллектив ва гуруҳ.

Ўқитиш воситалари. Дарслик, маъруза матни, електрон китоб, электрон ўқув қўлланмалар, електрон ўйинлар ва шу билан бир қаторда компютер ва ахборот технологиялари.

Коммуникасия усуллари. Тингловчилар билан оператив тескари алоқага асоланган бевосита ўзаро муносабатлар.

Тескари алоқа усуллари ва воситалари: кузатиш, блиц-сўров, оралиқ, жорий, якуний назорат таҳлили.

Бошқариш усуллари ва воситалари: ўқув машғулоти босқичларини белгилаб берувчи технологик харита кўринишидаги ўқув машғулотларини режалаштириш,

қуйилган мақсадга эришишда ўқитувчи ва тингловчининг биргаликдаги харакати, аудитория машғулотлари ва мустақил ишлар назорати.

Мониторинг ва баҳолаш. Курс оҳирида тест топшириқлари ёки ёзма иш варинатлари бўйича талабалар билимлари баҳоланади.

Айрим мавзулар бўйича талабалар билим баҳолаш тест асосида ва компютер ёрдамида бажарилади. Интернет тармоғидаги расмий иқтисодий кўрсаткичларидан фойдаланилади, тарқатма материаллар тайёрланади, таянч сўз ва иборалар асосида оралиқ ва якуний назоратлар ўтказилади.

МАШҒУЛОТНИНГ ЎҚИТИШ ТЕХНОЛОГИЯСИ

<table>
<tr><td>Вақти - 80 минут</td><td>Талабалар сони 20-30 та</td></tr>
<tr><td>Ўқув машғилотининг шакли</td><td>Кириш визуал маъруза</td></tr>
<tr><td>Маърузалар машғулотлар режаси</td><td>1. Методика фан сифатида
2. Методикани предмети ва вазифаси.
3. Умумий ва хусусий методика
4. Методиканинг илмий тадқиқод методлари.
5. Методиканинг категориялари
Методика фанининг бошқа фанлар билан боғлиқлиги</td></tr>
<tr><td colspan="2">Ўқув машғулотининг мақсади: Методика фанининг предмети, вазифаси, ҳамда бошқа фанлар билан алоқаси тўғрисида тўлиқ тасаввурни шакллантириш.</td></tr>
<tr><td>Педагогик вазифалар:
– методика фани ҳақида тушунча бериш ва унинг предметини тушунтириш;
– методика фанига хиссаларини қўшган методист ва тилшунос олимлар билан таништириш;
– методиканинг вазифасини тафсифлаш;
– методик категорияларга тушунча бериш;
– Илмий тадқиқод методларига изоҳ бериш.</td><td>Ўқув фаолиятининг натижалари:
– методика фанига тушунча беради;
– методика фанида қўлланиладиган тушунчаларга таъриф беради;
– методика фанига асос солган ва бугунги кунда фаолият кўрсатаётган методист олимлар ҳақида маълумот беради;
– методиканинг бош вазифасига тавсиф беради;
– методик категорияларга мисол келтиради;
– Илмий тадқиқот методларини санаб беради ва изоҳлайди;
– методика фанини бошқа фанлар билан алоқасини ва уни фанлар ичида тутган ўрнини тафсифлайди;</td></tr>
<tr><td>Ўқитиш услуби ва техникаси</td><td>Визуал маъруза Блиц-сўров, баён қилиш кластер “ҳа” –“йўқ ” техникаси.</td></tr>
<tr><td>Ўқитиш воситалари</td><td>Маъруза матни проектор тарқатма материал,дарсликлар жадваллар.</td></tr>
<tr><td>Ўқитиш шакли</td><td>Жамоа ва гурухда ишлаш.</td></tr>
<tr><td>Ўқитиш шарт-шароити</td><td>Проектор ва компютер билан жиҳозланган аудитория.</td></tr>
</table>

МАШҒУЛОТИНИНГ ТЕХНОЛОГИК КАРТАСИ.
(1-МАШҒУЛОТ)

Босқичлар вақти	**Фаолият мазмуни**	
	Ўқитувчи	**Талаба**
1-босқич. Кириш (10 мин.).	1.1.Фан унинг ҳақидасади, ўқув машғулотларидан кутилаётган натижалар маълум қилинади.	1.1.Эшитади. Ёзиб боради.
2 -босқич. Асосий (60 мин.)	2.1. Талабалар эътиборини жалб етиш ва билим доираларини аниқлаш учун тезкор савол-жавоб ўтказади. - методика фани хақида нима биласиз? - Бу фан сизнингча нималарни ўрганади? 2.2. Ўқитувчи визуал материаллардан фойдаланган ҳолда маърузани баён етишни давом этади. 2.3.Ўқитувчи методика фанига асос солган ва бугунги кунда фаолият юритаётган олимлар билан таништиради ва мавзуга доир саволлар беради. - методика фанига асос солганЎзбек методист олимларидан кимларни биласиз? - методика фани қайси фанлар билан боғлиқ ва бу боғлиқлик нимада? 2.4. Талабаларга мавзунинг асосий тушунчаларга эътибор қилишни ва ёзиб олишларини таъкидлайди.	2.1. Эшитади ва ўйлайди, жавоб беради. 2.2. Схема ва жадваллар мазмунини мухокама қилади, саволлар беради, асосий жойларни ёзиб олади. 2.3. Эслаб қолади , ёзади, ҳар бир саволга жавоб беришга харакат қилади.
3-босқич. Якуний (10 мин.)	3.1.Мавзуга якун ясайди. Фаол иштирок етган талабаларни рағбатлантиради, баҳолайди. 3.2.Мустақил иш учун вазифа беради: “Методика” сўзига кластер тузиш.	3.1. Эшитади аниқлаштиради. 3.2. Топшириқни ёзиб олади.

Машғулотининг хронологик харитаси

Ишлаш босқичлари, вакти	Фаолият мазмуни	
	Укитувчининг	Талабанинг
1-босқич: Ўқув машғулотига кириш (10 дақ.)	Янги марузанинг мавзуси, мақсади, мавзу булимлари, режалаштирилган ўқув натижалари эълон қилинади.	Тинглашади, аниқлаштирувчи саволлар бери-шади
2-босқич: Асосий (60 дақ.)	2.1. Блиц-суров, савол-жавоб шакли ёрдамида ўтган мавзудаги билимлар мустаҳкамланади ва янги мавзу билан ўтган мавзу орасидаги алоқа ўрнатилади. Янги мавзу долзарблаштирилади; 2.2. Янги мавзунинг режаси (мавзу бўлимчалари) эълон қилинади; 2.3. Режа бўйича янги мавзу баён этилади; 2.4. Режада кўрсатилган ҳар бир мавзу бўлимчалари баён этилгач, талабаларнинг саволларига жавоб берилади ва сўнгра мавзунинг кейинги бўлимларига ўтилади; 2.5. Ўтилган мавзу бўйича мустақил бажариш учун топшириқлар, назорат саволлари ва тавсия қилинган адабиётлар рўйхати эълон қилинади;	Саволларга жавоб беришади. Тинглашади, аниқлаштирувчи саволлар беришади, мисоллар келтиришади, Янги ишлаб чиқилган воситалар тўгрисидаги маълумотлар билан танишадилар, фикр алмашадилар
3-босқич: Якуний, натижавий (10 дақ.)	3.1. Мавзу буйича хулоса қилади, муҳим жиҳатларига талабалар эътиборини қаратади. Ҳар бир воситанинг қулланилиш соҳаларини таъкидлаб ўтади; 3.2. Дарсда фаол иштирок этган талабаларни ажратиб кўрсатади ва уларнинг фаолиятини баҳолайди; 3.3. Ўқув машгулотида кузланган натижага эришганлик даражасини таҳлил қилади ва баҳолайди; 3.4. Мавзу устида мустақил ишлаш учун топшириқлар беради ва асосий ҳамда қўшимча адабиётлар рўйхатини тавсия этади.	Тинглашади, аниқлаштирувчи саволлар беришади, мустақил торширикларни ёзиб олишади.

5. НАЗОРАТ МАТЕРИАЛЛАРИ

5.1. Топшириқлар мазмуни

5130200 – *«Амалий математика ва информатика» йўналиши бўйича таълим олаётган 3 - босқич талабалари билимини* “Ахборотларни ҳимоялаш” *фанидан рейтинг тизими бўйича топшириқлар мазмуни ва баҳолаш* ***мезонлари***

Фан бўйича рейтинг жадваллари, назорат тури, шакли, сони, ҳамда хар бир назоратга ажратилган максимал балл, шунингдек жорий ва оралиқ назоратларнинг саралаш баллари ҳақидаги маълумотлар биринчи машғулотда талабаларга эълон қилинади.

Давлат таълим стандартларига мувофиқ қуйидаги назорат турлари ўтказилади.

Жорий назорат (ЖН). Талабанинг фан мавзулари бўйича билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. ЖН амалий машғулотларда оғзаки сўров, тест ўтказиш, сухбат, назорат иши, коллоквиум, уй вазифаларини текшириш ва шу каби бошқа назорат шаклларида ўтказилади.

Оралиқ назорат (ОН). Семестр давомида ўқув дастурининг тегишли (фаннинг бир неча мавзуларини ўз ичига олган) бўлими тугаллангандан кейин, талабанинг назарий билим ва амалий кўникма даражасини аниқлаш ва баҳолаш усули. ОН бир семестрда икки марта ўтказилади ва шакли (ёзма, оғзаки, тест ва х.к.) ўқув фанига ажратилган умумий соатлар ҳажмидан келиб чиққан ҳолда белгиланади.

Якуний назорат (ЯН). Семестр якунида муаян фан бўйича назарий билим ва амалий кўникмаларни талабалар томонидан ўзлаштириш даражасини баҳолаш усули. ЯН асосан таянч тушунча ва ибораларга асосланган “ёзма иш” шаклида ўтказилади.

ОН ўтказиш жараёни кафедра мудири томонидан тузилган комиссия иштирокида мунтазам равишда ўрганиб борилади ва уни ўтказиш тартиблари бузилган ҳолларда ОН натижалари бекор қилиниши мумкин. Бундай ҳолларда ОН қайта ўтказилади.

ОТМ ректорининг буйруғи билан ички назорат ва мониторинг бўлими раҳбарлигида тузилган комиссия ЯНни ўтказиш жараёнини мунтазам равишда кузатиб боради ва уни ўтказиш тартиблари бузилган ҳолларда ЯН натижалари бекор қилиниши мумкин. Бундай ҳолларда ЯН қайта ўтказилади.

Талабанинг билим савияси, кўникма ва малакаларини назорат қилиш рейтинг тизимига асосан, талабани фан бўйича ўзлаштириш даражаси баллар орқали ифодаланади.

Талабанинг семестр давомида ўзлаштириш кўрсаткичи 100 баллик тизимида баҳоланади. Ушбу 100 балл баҳолаш турлари бўйича қуйидагича тақсимланади:

ЯН - 30 балл; ЖН - 35 балл; ОН – 35 балл

Талаба назорат натижаларидан норози бўлса, фан бўйича назорат тури натижалари еълон қилинган вақтдан бошлаб, бир кун мобайнида факултет деканига ариза билан мурожаат этиш мумкин. Бундай ҳолда, деканнинг тақдимномасига кўра, ректор буйруғи билан 3 (уч) аъзодан кам бўлмаган таркибда апеллясия комиссияси ташкил етилади.

Аппеляция комиссияси талабанинг аризаларини кўриб чиқиб, шу куннинг ўзида хулосасини билдиради.

Баҳолашнинг ўрнатилган талаблар асосида, белгиланган муддатларда ўтказилиши, ҳамда расмийлаштирилиши факултет декани, кафедра мудири, ўқув-услубий бошқарма ҳамда ички назорат ва мониторинг бўлими томонидан назорат қилинади.

ЯН “Ёзма иш” шаклида амалага ошрилиганда синов кўп вариантли усулда ўтказиилади. Ҳар бир вариант 4 назарий савол ва 1 амалий топшириқдан иборат. Назарий саволлар фан бўйича таянч сўз ва иборалар асосида тузилган бўлиб , фаннинг барча мавзуларини ўз ичига қамраб олган. Хар бир назарий савол ва амалий топшириқга ёзилган жавоблар бўйича ўзлаштириш кўрсаткичи 0-6 балл оралиғида баҳоланади. Талаба максимал 30 баллни тўплаши мумкин.

Ёзма синов бўйича умумий ўзлаштириш кўрсаткичини аниқлаш учун, вариантда берилган саволларнинг хар бири учун ёзилган жавобларга қуйилган ўзлаштириш баллари қўшилади ва йиғинди талабанинг ЯН бўйича ўзлаштириш бали ҳисобланади.

5.2. ОН, ЯН учун тестлар

1. Компьютерда маълум хавфсизликни таъминловчи дастурлар ўрнатилганми?
Компьютер ишга туширилиши билан хавфсизликни таъминловчи дастур юкланади.
Янги компьютерга оид ҳужжатлар келтирилади.
Пуск менюсидаги Все программы пунктлари қаралади.
Барча жавоблар тўғри.

2. Интернетда ишлашдан олдин Internet Explorer шарҳловчисининг махфийлик параметрларини қандай созлаш мумкин?
Сервис обозревателя --> Свойства обозревателя --> Конфиденциальность
Internet Explorer шарҳловчисининг «поиск» сатрига privacy сузини киритиш орқали.
Ойна пардаларини тўсиб қўйиш билан.
Пуск -> Вид -> Настройки.

3. Компьютерни вируслардан ҳимоя қилишда хавфсизликни таъминловчи қандай дастурлар қўлланади?
Антивирус ва антишпион дастурий таъминотлар, ҳамда брандмауэр.
Windows Live OneCare
Microsoft га оид тасодифий манзил фильтри
Барча жавоблар тўғри.

4. Шифрлаштириш сузининг маъноси нима?
Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн шифрланган матн билан алмаштирилади.
Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн жадвал билан алмаштирилади.
Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн лотинча матн билан алмаштирилади.
Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн инглизча матн билан алмаштирилади.

5. Дешифрлаштириш сўзининг маъноси нима?
Дешифрлаштириш – шифрлаштиришга тескари жараён. Калит асосида шифрланган матн ўз ҳолатига узгартирилади.
Дешифрлаштириш – бу матн маълумотларини ўзгартириш учун иккилик коди.
Шифрлаштириш – бу график маълумотларни ўзгартириш учун саккизлик коди.
Шифрлаштириш – бу график ва матнли маълумотларни ўзгартириш учун саккизлик коди

6. Алфавит – бу ...
ахборотни кодлаштириш учун ишлатиладиган чекли белгилар тўплами.
ахборотни кодлаштириш учун ишлатиладиган дискрет ва чексиз белгилар.
ахборотни кодлаштириш учун ишлатиладиган дискрет белгилар тўплами.
ахборотни кодлаштириш учун ишлатиладиган чексиз белгилар тўплами.

7. Калит – бу?
калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган ахборот
калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган маълумот
калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган ҳужжат
калит – матнларни тўсиқларсиз шифрлаш ва дешифрлаш учун керак бўлган файл
8. Криптографик тизим - ....

Очиқ матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари индекслаштирилади ва К белги билан белгиланади (К– калит)

Очиқ матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари К белги билан белгиланади (К– калит)

Ёпиқ матнни Т ўзгартириш оиласи. Ушбу оиланинг аъзолари К белги билан белгиланади (К– калит)

Барча жавоблар тўғри

9. Симметрик криптотизимларда шифрлаш ва дешифрлашда қандай калит ишлатилади?

бир ҳил калит

алоҳида калитлар

ҳар хил калитлар

барча жавоблар нотўғри

10. Очиқ калитли тизимда шифрлаш ва дещифрлаш учун қандай калит ишлатилади?

очиқ ва ёпиқ

очиқ

ёпиқ

барча жавоблар нотўғри

11. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда таалуқли?

Ахборотни қайта ишлашнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

Ахборотни чиқаришнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

Ахборотни киритишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

Ахборотни ёзишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

12. Электрон имзо – бу...

жадвалга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади

файлга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади

кутубхонага бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади

матнга бириктирилган криптографик ўзгартириш бўлиб бошқа фойдаланувчи эгалик қилмоқчи бўлганда унинг муаллифи ва ҳаққонийлигини текширилади

13. Криптомустаҳкамлик – бу...

Шифрнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

Идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

Коднинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

Код ва идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир

14. Криптомустаҳкамликнинг қандай кўрсаткичлари мавжуд?

–мумкин бўлган калитлар сони; –крипто таҳлил учун керакли ўртача вақт;

–мумкин бўлган калитлар сони; –крипто таҳлил учун керакли бошланғич вақт;
–мумкин бўлган калитлар сони; –крипто таҳлил учун керакли охирги вақт;
барча жавоблар тўғри

15. Ахборотни ҳимоялаш мақсадида шифрлашнинг эфективлиги қуйдагилардан боғлиқ:
Шифрни криптомустаҳкамлиги ва калитнинг сирини сақлашдан
Тўғри жавоблар йўқ
Шифрни криптомустаҳкамлиги ва идетификаторларнинг сирини сақлашдан
Шифрни криптомустаҳкамлиги ва коднинг сирини сақлашдан

16. Шифрланган маълумот ўқилиши мумкин фақат ...
калити берилган бўлса
коди берилган бўлса
идентификатори берилган бўлса
шифри берилган бўлса

17. Шифрланган хабарнинг маълум қисми ва унга мос келувчи очиқ матн бўйича ишлатилган шифрлаш калитининг керакли жараёнлар сонини аниқлаш қуйидагилардан иборат:
мумкин бўлган калитларнинг умумий сонидан кам бўлмаган
мумкин бўлган калитларнинг дискрет сонидан кам бўлмаган
мумкин бўлган калитларнинг ҳақиқий сонидан кам бўлмаган
мумкин бўлган калитларнинг мавҳум сонидан кам бўлмаган

18. Шифрланган ахборотни шарҳлаб беришда мумкин бўлган калитларни танлаш йўли учун зарур жараёнлар сони қуйидагиларни ўз ичига олади:
қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади
юқоридан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади
қуйидан баҳолаш қаттиқ талаб қилинмайди; замонавий компьютерлар имконият чегарасидан чиқади
қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқмайди

19. Калитларни сезиларсиз ўзгартириш қуйдагиларга олиб келиши мумкин:
битта ва бир хил калитдан фойдаланганда ҳам шифрланган хабарлар сезиларли даражада ўзгаришга эга бўлади
хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ўзгаради
хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ва сезиларсиз ўзгариш олади
хато бир хил калитни ишлатганда шифрланган маълумот кўриниши ўзгариши сезиларсиз

20. Шифрлаш алгоритмининг элементлари тузилиши қуйидагича бўлиши мумкин:
доимий (ўзгармас)
ихчам
энг кўп
энг кам

21. Шифрлаш жараёнида маълумотга киритиладиган қўшимча битлар ...
тўлиқ ва ишончли яширинган бўлиши керак
тўлиқ бўлмаган ва ишончли яширинган бўлиши керак

тўлиқ бўлмаган ва ишончсиз яширинган бўлиши керак
барча жавоблар тўғри

22. Шифрланган матннинг узунлиги ...
берилган матннинг узунлигига тенг бўлиши шарт
шифрнинг узунлигига тенг бўлиши шарт
шифрнинг узунлигига тенг бўлмаслиги шарт
берилган матннинг узунлигига тенг бўлмаслиги шарт

23. Қуйидагилар бўлмаслиги керак:
шифрлаш жараёнида мунтазам қўлланадиган калитлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик
шифрлаш жараёнида мунтазам қўлланадиган идентификаторлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик
шифрлаш жараёнида мунтазам қўлланадиган шифрлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик
шифрлаш жараёнида мунтазам қўлланадиган кодлар орасида содда ва осонгина аниқлаш мумкин бўлган боғлиқлик

24. Мумкин бўлган тўпламлардан олинган ҳар қандай калитлар қуйидагини таъминлайди:
ахборотни ишончли ҳимоялаш
компьютерни ишончли ҳимоялаш
файлни ишончли ҳимоялаш
ахборот ва файлни ишончли ҳимоялаш

25. Симметрик криптотизим учун қандай усуллар қўлланилади?
ўрнини алмаштириш, гаммалаш, блокли шифрлаш
моноалфавитли алмаштириш, ўрнини алмаштириш, гаммирлаш
кўпалфавитли алмаштириш, ўрнини алмаштириш, гаммирлаш
ўрнини алмаштириш, гаммирлаш, блокли идентификаторлар

26. Цезар алмаштиришнинг мазмуни қандай изоҳланади?
Цезар алмаштириш моноалфавитли гуруҳига қарашли
Цезар алмаштириш блокли шифрлаш гуруҳига қарашли
Цезар алмаштириш гаммирлаш гуруҳига қарашли
Цезар алмаштириш кўпалфавитли гуруҳига қарашли

27. Алмаштиришлар қуйидагиларга ажралади:
моно ва кўпалфавитли
моноалфавитли
кўпалфавитли
тўғри жавоб йўқ

28. Маълумотларни ҳимоя қилиш тушунчасига ...
маълумотларнинг тўлиқлигини сақлаш ва маълумотга киришини бошқариш киради
файлнинг тўлиқлигини сақлаш киради
шифрнинг тўлиқлигини сақлаш киради
коднинг тўлиқлигини сақлаш киради

29. Компьютерга вируслар қандай кириб келади?
Файллар орқали, нусха кўчирганда, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали

Файллар орқали, тузатиш вақтида, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали

Файллар орқали, матнни териш орқали, электрон хатларга бириктирилган файллар орқали, тармоқда мавжуд зарарланган юкланувчи дастурлар орқали, интерактив хизматлар орқали

барча жавоблар тўғри

30. Антивирус дастурларини синовдан ўтказиш билан қандай ташкилот шуғулланади?

Компьютер хавфсизлиги миллий ассоциацияси NCSA (National Computer Security Association)

Intel, Celeron

Celeron, IBM

IBM, INTEL

31. Фойдаланувчиларни идентификация қилиш қуйидагиларни аниқлайди

турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш шкаласини

турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш графигини

турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш паролини

турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш кодини

32. Маълумотларни физик ҳимоялаш кўпроқ ...

ташкилий чораларга қарашлидир

ташкилий ва ноташкилий чораларга қарашлидир

ноташкилий чораларга қарашлидир

туғри жавоб йўқ

33. Ахборотга кириш ҳуқуқини узатиш ва ҳимоя қилиш воситалари ...

маълумотлар билан диференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

файллар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

браузерлар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

диференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

34. Ҳимоя қилишнинг асосий муаммолари қуйидагилардан иборат:

Ахборотга киришга йўл қўймаслик

Файлга киришга йўл қўймаслик

Шифрга киришга йўл қўймаслик

Кодга киришга йўл қўймаслик

35. Пароллар усули ...

энг оддий ва арзон, лекин ишончли ҳимояни таъминлайди

энг оммавий ва қиммат, лекин ишончли ҳимояни таъминлайди

энг оммавий лекин операцияли тизимга киришни ишончли ҳимояни таъминлайди

энг мураккаб лекин ишончли ҳимояни таъминлайди

36. Дастурий пароллар усули қуйидагини ўз ичига олади ...

кўриниши ва объектга рухсат бўйича чеклашларни аниқловчи дастурий усулларни

модуллар бўйича чеклашларни аниқловчи бошқа дастурий усулларни

маҳсулотлар бўйича чеклашларни аниқловчи бошқа дастурий усулларни

пакетлар бўйича чеклашларни аниқловчи бошқа дастурий усулларни

37. Дастурий пароллар тизимини қандай тасаввур этиш мумкин?

ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган жадвалли бошқариш кўринишидан кириши(рухсат) бўлиб ҳисобланади

ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган функция кўринишидан кириши(рухсат) бўлиб ҳисобланади

ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган идентификатор кўринишидан кириши(рухсат) бўлиб ҳисобланади

ҳар хил фойдаланувчилар учун қаралган кириш (рухсат) турларини аниқлайдиган жадвал ва функция кўринишидан кириши(рухсат) бўлиб ҳисобланади

38. Маълумотларни шифрлаш усули қуйидагилар учун фойдали бўлиши мумкин:

рухсатсиз кириш модулларини мураккаблаштириш учун

рухсатсиз кириш модулларини мураккаблаштирмаслик учун

рухсатли кириш модулларини мураккаблаштириш учун

тўғри жавоб берилмаган

39. Шифрлаш алгоритми орқали қуйидаги кўзда тутилади:

алфавитнинг ҳар бир ҳарфини сон билан алмаштириш

ҳар бир функцияни алмаштириш

ҳар бир идентификаторни алмаштириш

ҳар бир тизимнинг модулини алмаштириш

40. Автоматик кайта чакирув усули гояси куйдагидан иборат:

марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – идентификацион код талаб этилади

марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилади

марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилмайди

марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – парол ва шифр талаб этилади

41. Хужумнинг натижаси бўлиб ҳисобланади:

ташқи разведка, ички разведка, изни йўқотиш, фойда, exploit

ички разведка, фойда, exploit, тизимли хужум

ташқи разведка, ички разведка, изни йўқотиш, фойда, exploit, тизимли хужум

тизимли хужум, физик хужум, exploit, фойда

42. Ташки харакатлар кандай хулосаланади?

Хакерлар узларини сездирмасдан хужум қилиш керак булган тизим тугрисида мумкин кадар купрок маълумотлар туплайдилар.

Фойдаланувчилар ишлаётган тизим тугрисида купрок маълумотлар туплайдилар.

Хаваскорлар узларини сездирмасдан хужум қилиш керак булган тугрисида мумкин кадар купрок маълумотлар туплайдилар.

Интернет абонентлари узларини сездирмасдан хужум қилиш керак булган тизим тугрисида мумкин кадар купрок маълумотлар туплайдилар.

43. Exploit-нима?

Бузувчи чегарани бузиб утади ва компютернинг заиф томонларидан фойдаланадилар.

Фойдаланувчи унга ажратилган компютерларнинг заиф томонларидан фойдаланадилар.

Интернет абоненти чегарани бузиб утади ва компютернинг заиф томонларидан фойдаланадилар.

Интернетни севувчилар чегарани бузиб утади ва компютернинг заиф томонларидан фойдаланадилар.

44. ’’Изни яшириш’’-нинг маъноси …

Хакер Тармоққа мувофакиятли кириб олгандан сунг кайд қилиш журналидан хужум килинганлиги тугрисидаги маълумотни йукотади.

Хакер Тармоққа мувофакиятсиз кириб олгандан сунг кайд қилиш журналидан хужум килинганлиги тугрисидаги маълумотни йукотади.

Фойдаланувчи Тармоққа мувофакиятли кириб олгандан сунг кайд қилиш журналидан хужум килинганлиги тугрисидаги маълумотни йукотади.

Барча жавоблар нотугри.

45. Фойда нима?

Бузувчи ўзининг имкониятларидан фойдаланиб, махфий маълумотларни угирлайди, тизимнинг ресурслари орқали ғаразли мақсадларини амалга оширади ёки Web-сахифани учиради.

Фойдаланувчи ўзининг имкониятларидан фойдаланиб, махфий маълумотларни уғирлайди, тизимнинг ресурслари орқали ғаразли мақсадларини амалга оширади ёки Web-сахифани учиради.

Абонент ўзининг имкониятларидан фойдаланиб, махфий маълумотларни уғирлайди, тизимнинг ресурслари орқали ғаразли мақсадларини амалга оширади ёки Web-сахифани учиради.

Хаваскор ўзининг имкониятларидан фойдаланиб, махфий маълумотларни уғирлайди, тизимнинг ресурслари орқали ғаразли мақсадларини амалга оширади ёки Web-сахифани учиради.

46. Бузувчилар қандай қилиб тизимга суқилиб кирадилар?

физик, тизимли, узокдан бостириб киришлар оркали.

тизимли, узокдан бостириб киришлар оркали.

физик, тизимли, exploit, узокдан бостириб киришлар оркали.

узокдан, тизимли, exploit

47. Физик бузишнинг мохияти нима?

Бузғунчи тизимга суқилиб киришнинг асосий йули (клавиатура ёки тизимнинг баъзи қисмларидан фойдаланишлари мумкин)

Фойдаланувчи тизимга суқилиб киришнинг асосий йули (клавиатура ёки тизимнинг баъзи қисмларидан фойдаланишлари мумкин)

Абонент тизимга суқилиб киришнинг асосий йули (клавиатура ёки тизимнинг баъзи қисмларидан фойдаланишлари мумкин)

Хаваскор тизимга суқилиб киришнинг асосий йули (клавиатура ёки тизимнинг баъзи қисмларидан фойдаланишлари мумкин)

48. Тизимни бузишнинг мохияти нима?

Хакерлик фаолиятининг шундай кўринишики, бунда бузувчи юқори махоратга эга бўлмаган абонент сифатида тизимда руйхатдан утган бўлади.

Хакерлик фаолиятининг шундай кўринишики, бунда фойдаланувчи юқори махоратга эга бўлмаган абонент сифатида тизимда руйхатдан утган бўлади.

Хакерлик фаолиятининг шундай кўринишики, бунда абонент юқори махоратга эга бўлмаган абонент сифатида тизимда руйхатдан утган бўлади.

Барча жавоблар тугри.

49. Узоқ (олис)лаштирилган масофадан бузиш нима?

Хакерлик фаолияти
Хаваскорлик фаолияти
Абонентлик фаолияти
Фойдаланувчи фаолияти

50. Физик бузиш нима?

Фойдаланувчи фаолияти
Абонентлик фаолияти
Хаваскорлик фаолияти
Хакерлик ва фойдаланувчи фаолияти

5.3. Ёзма иш ва оғзаки назоратлар саволлари (вариантлар)

«Ахборотларни ҳимоялаш» фанидан якуний ва оралиқ назорат саволлари

Назарий саволлар

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Ахборот хавфсизликнинг йуналишлари (иқтисодий, мудофаа, ижтимоий, экологик).
3. Ахборот хавфсизлиги таснифи ва ахборот химояси максадлари (ишончлилик, аниқлилик, назорат килиш турлари).
4. Ахборотларни химояловчи инструментал воситалар (таъсир услуби, таъсир тамойили, таъсир характери, фойдаланиладиган хато, хужум объекти).
5. Ахборотни химоялаш тизими таърифи (ташкилий, техник, дастурий, технологик, восита).
6. Химоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).
7. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
8. Вирус хакидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
9. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
10. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
11. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
12. Компьютер стенографияси тушунчаси (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
13. Компьютер стенографиясининг асосий вазифалари (аутентификацияланиш, яхлитлик, конфиденциал, мониторинг, никоблаш).
14. Криптография ҳақида асосий тушунчалар (ммахфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).
15. Криптотизимларнинг икки синфи (калит, симметрия, ассимметрия).
16. Криптографияли ҳимоялаш тамойиллари (махфийлик, яхлитлилик, криптомустаҳкам).
17. Компьютер маълумотларини химоялашнинг техник-дастурий воситалари (идентификация, аутентификация, шифрлаш, диск, тармок, таянч, бошкариш)
18. Симметрияли криптотизим асослари (уринларини алмаштириш, алмаштириш, гаммалаштириш, тахлилий узгартириш)
19. Ахборот тизимларнинг таъсирчан кисмлари (серверлар, узатиш каналлари, узатиш йули, броузерлар).
20. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари (маълумотларни таркатиш, ахборотларга эгалик килиш, узгартирилиш, дастур, тизим суровлари).
25. ЭХМ химоясини таъминлашнинг техник воситалари (персонал, маъсулият, тармокларо экранлар, шлюзлар, аудитлаш, реал вакт, стохастик).
21. Компьютер тармоги химоясини ташкил килиш асослари (субъектлар сони, хужум нукталари, мухофаза, назорат, маълумот узатиш, захира).
22. Компьютер телефониясидаги химоялаш усуллари (телефон, хакер, нуткни аниклаш, шифрлаш тезлиги).
23. Компьютер тармокларида химояни таъминлаш усулларининг асослари (тускинлик, эгаликни бошкариш, никоблаш, тартиблаш, мажбурлаш, ундамок).
24. Тармокларда химояни таъминлаш усулларнинг таснифи (воситилар, расмий, норасмий, техникавнй, дастурий, ташкилий, ахлокий ва одобий, конуний).

26. Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари (техник, биргаликдаги воситалар, унификация, стандартлаштириш).

27. Internet тармогида мавжуд алоканинг хавфсизлигини таъминлаш асослари (анонимлик, серверга кириш, рухсатсиз кириш, тармоклараро экран).

28. Internetда рухсатсиз кириш усулларининг таснифи (муаммолар, эркин, чегараланган, ихтиёрий).

29. Тармоклараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, кабул, трафикни йуналтириш, заиф кисмлар, баёнлаштириш, аутентификация).

30. Тармоклараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).

31. Электрон почтада мавжуд муаммолар ва хавфлар (тасодиф, нотугри манзил, архив, янгиликлар, обуна, таркатиш хатоси, калбаки манзил, «бомба», нохуш хат.)

32. Электрон туловлар тизими асослари (пластик карта, банк, эмитент, эквайер, кредит, дебет, транзакциялар)

33. Идентификацияловчн шахсий номерни химоялаш (PIN-код, калит, шифр, текшириш усули).

34. Банкоматлар хавфсизлигини таъминлаш (имкониятлар, режимлар, зона, PIN-код).

35. Internetда мавжуд электрон туловлар хавфсизлигини таъминлаш (**Электрон савдо,** ахборотлар сотуви, дуконлар, банклар).

Амалий саволлар

1. Криптографиянинг уринларни алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр буйича шифрланг.

2. Белгилар сони 9 та булган (бушлик белгиси хисобланмайди) матнни танланг ва уни 3х3 сехрли квадрат ёрдамида шифрланг.

3. Криптографик шифрлашнинг Цезар усули ёрдамида k=4 булганда фамилия ва исмингизни шифрланг.

4. Тест вирусини яратиш ва ундан фойдаланиш.

5. Дастурни рухсат этилмаган нусхалашдан химолашни амалга ошириш учун компьютер турини аниклайдиган дастур тузинг.

6. Дастурни рухсат этилмаган нусхалашдан химолашни амалга ошириш учун операцион тизим версиясини аниклайдиган дастур тузинг.

7. Дастурни рухсат этилмаган нусхалашдан химолашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чикилган санасини аниклайдиган дастур тузинг.

«Ахборотларни ҳимоялаш» фанидан оралиқ назорат вариантлари

1-вариант

1. Ахборот хавфсизлигининг асосий тушунчалари (ахборот хавфсизлиги, ахборотнинг ҳимояси, ахборотни туркумлари).
2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

2-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, мудофаа, ижтимоий, экологик).
2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).
3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

3-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот химояси максадлари (ишончлилик, аниқлилик, назорат килиш турлари).

2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

4-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).

3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

5-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)

3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окими, трафикни йўналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

6-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Тармоклараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).

7-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

3. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

8-вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

3. Яратиладиган дастурларни норасмий нусҳалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида t=(3*t+5) mod 26 формуладан фойдаланинг.

9-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).

2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

10-вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)

3. Жихозлар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

11-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

3. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш).

12-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, мудофаа, ижтимоий, экологик).

2. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).

3. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

13-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилик, аниқлилик, назорат килиш турлари).

2. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

3. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

14-вариант

1. Химоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)

3. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

15-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

3. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

16-вариант

1. Вирус хакидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)

17-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).

3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

18-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

3. Тармокларарo экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, кабул, трафикни йуналтириш, заиф кисмлар, баёнлаштириш, аутентификация).

19-вариант

1. Ахборот хавфсизлигининг йўналишлари (иқтисодий, мудофаа, ижтимоий, экологик).

2. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

3. Тармокларарo экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).

20-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

21-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).

2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

22-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).

3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

23-вариант

1. Вирус ҳакидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

2. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)

3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

24-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Тармоқларарo экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, кабул, трафикни йуналтириш, заиф кисмлар, баёнлаштириш, аутентификация).

25-вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

3. Тармоклараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).

26-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
3. Электрон туловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

27 -вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
3. Яратиладиган дастурларни норасмий нусҳалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

28 –вариант

1. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

29 -вариант

1. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, ниқоблаш).
2. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
3. Жихоздар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

30 -вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

Якуний назорат вариантлари

1-вариант

1. Ахборот хавфсизлигининг асосий тушунчалари (ахборот хавфсизлиги, ахборотнинг ҳимояси, ахборотни туркумлари).
2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр буйича шифрланг.

2-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, мудофаа, ижтимоий, экологик).
2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).

3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).

4. Белгилар сони 9 та булган (бушлик белгиси хисобланмайди) матнни танланг ва уни 3х3 сехрли квадрат ёрдамида шифрланг.

3-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот химояси максадлари (ишончлилик, аниқлилик, назорат килиш турлари).

2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).

3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).

4. Криптографик шифрлашнинг Цезар усули ёрдамида k=4 бўлганда фамилия ва исмингизни шифрланг.

4-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).

2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).

3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

4. Дастурни рухсат этилмаган нусхалашдан химоялашни амалга ошириш учун компьютер турини аниклайдиган дастур тузинг.

5-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).

2. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)

3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окими, трафикни йўналтириш, заиф қисмлар, баёнлаштириш, аутентификация).

4. Дастурни рухсат этилмаган нусхалашдан химоялашни амалга ошириш учун операцион тизим версиясини аниклайдиган дастур тузинг.

6-вариант

1. Вирус ҳақидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Тармоклараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).

4. Дастурни рухсат этилмаган нусхалашдан химолашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чикилган санасини аниклайдиган дастур тузинг.

7-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).

2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).

3. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

4. Виженер жадвалидан фойдаланиб, исми шарифингизни шифрланг.

8-вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

3. Яратиладиган дастурларни норасмий нусҳалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида t=(3*t+5) mod 26 формуладан фойдаланинг.

9-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).
4. Икки марталик ўрин алмаштириш усули билан шифрлашга мисол келтиринг.

10-вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
3. Жихозлар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).
4. Трисемус усули билан фамилия ва исмингизнинг туғри келадиган қисмини шифрланг.

11-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
3. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш).
4. Плейфер тизими бўйича биграммаларга бўлинадиган сўзни шифрланг.

12-вариант

1. Ахборот хавфсизлигининг йуналишлари (иқтисодий, мудофаа, ижтимоий, экологик).
2. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
3. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
4. Уитсоннинг икки квадратлари бўйича шифрлашга мисол келтиринг.

13-вариант

1. Ахборот хавфсизлиги таснифи ва ахборот ҳимояси мақсадлари (ишончлилик, аниқлилик, назорат килиш турлари).
2. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).
3. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
4. Цезарнинг таянчли сўз асосидаги шифрлаш тизимида к=5 ва ДИПЛОМАТ калитли сўзлар билан матнни шифрлашга мисол келтиринг.

14-вариант

1. Химоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)
3. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).
4. Дастурни рухсат этилмаган нусхалашдан химоялашни амалга ошириш учун компьютер турини аниклайдиган дастур тузинг.

15-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, никоблаш).
3. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).
4. Дастурни рухсат этилмаган нусхалашдан химоялашни амалга ошириш учун операцион тизим версиясини аниклайдиган дастур тузинг.

16-вариант

1. Вирус хакидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).
3. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)
4. Дастурни рухсат этилмаган нусхалашдан химолашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниклайдиган дастур тузинг.

17-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).
3. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).
4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр буйича шифрланг.

18-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).
3. Тармокларараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, кабул, трафикни йуналтириш, заиф кисмлар, баёнлаштириш, аутентификация).
4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютер турини аниклайдиган дастур тузинг.

19-вариант

1. Ахборот хавфсизлигининг йўналишлари (иқтисодий, мудофаа, ижтимоий, экологик).
2. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).
3. Тармокларараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).
4. Дастурни рухсат этилмаган нусҳалашдан ҳимоялашни амалга ошириш учун операцион тизим версиясини аниқлайдиган дастур тузинг.

20-вариант

1. Ҳимоялаш тизимининг элементлари (хукукий, ташкилий, муҳандис – техник, дастурий – математик).
2. Электрон тўловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).
3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида t=(3*t+5) mod 26 формуладан фойдаланинг.

21-вариант

1. Ахборот хавфсизликнинг асосий тушунчалари (ахборот хавфсизлиги, Ахборотнинг ҳимояси, ахборотни туркумлари).
2. Криптография ҳақида асосий тушунчалар (махфийилик, ўзгартиришлар, кодлаштириш, шифрлаш).
3. Вижинер жадвали асосида шифрлаш тизими (кўп алфавитли, сатр, жадвал, калит, устун).
4. Дастурни рухсат этилмаган нусхалашдан ҳимоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чиқилган санасини аниқлайдиган дастур тузинг.

22-вариант

1. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар (узилиш, тутиб қолиш, ўзгартириш ва сохталаштириш).
2. Очиқ калитли симметрияли криптотизимлар (калит, симметрия, очиқ канал, махфий канал).
3. Уитсоннинг икки кавадрат бўйича шифрлаш усули (биринчи, иккинчи, биграмма, тўртбурчак).
4. Криптографиянинг калитли сўз бўйича жадвалли урин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр буйича шифрланг.

23-вариант

1. Вирус ҳакидаги тушунчалар (дастурли, зарарланган, хавфли, хавфсиз).
2. Икки калитли криптотизимлар (асимметрия, калит, очиқ, ёпиқ, аутентик канал, шифрлаш, дешифрлаш)
3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).
4. Белгилар сони 9 та булган (бўшлик белгиси ҳисобланмайди) матнни танланг ва уни 3х3 сехрли квадрат ёрдамида шифрланг.

24-вариант

1. Вирус турлари (троян, норезидент, резидент, бутли, пакетли).
2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).
3. Тармоқлараро экран ва унинг вазифалари (уринсиз трафиклар, хабарлар окимини, кабул, трафикни йуналтириш, заиф кисмлар, баёнлаштириш, аутентификация).
4. Цезарнинг Афинна тизими бўйича фамилия ва исмингизни шифрланг. Калит сифатида t=(3*t+5) mod 26 формуладан фойдаланинг.

25-вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).
2. Икки марталик ўрин алмаштириш усули (калит, жадвал, рақамлар).
3. Тармоклараро экраннинг асосий компонентлари (фильтрловчи-йулловчи, шлюзлар, тармок даражаси, амалий даража).
4. Уитсоннинг икки квадратлари бўйича шифрлашга мисол келтиринг.

26-вариант

1. Вирусларга қарши чора-тадбирлар (антивирус, архив, пароль).
2. Сехрли квадрат асосида шифрлаш (калит, жадвал, йиғиндилар).

3. Электрон туловлар хавфсизлигини таъминлаш (Электрон савдо, ахборотлар сотуви, дуконлар, банклар).

4. Цезарнинг таянчли сўз асосидаги шифрлаш тизимида к=5 ва ДИПЛОМАТ калитли сўзлар билан матнни шифрлашга мисол келтиринг.

27 -вариант

1. Компьютер стеганографияси тушунчаси ва йўналишлари (кодлаштириш, махфий ёзув, хабар, контейнер, оригинал, натижа).

2. Бир алфавитли алмаштириш асосида шифрлаш усуллари (классик, цезар, модулли қўшиш, таянч сўзли).

3. Яратиладиган дастурларни норасмий нусҳалашдан ҳимоялаш асослари (дастур, норасмий, нусха, калит, кўрсаткичлар).

4. Криптографиянинг калитли сўз бўйича жадвалли ўрин алмаштириш усули ёрдамида фамилия ва исмингизни 3 сатр буйича шифрланг.

28 –вариант

1. Стеготизимнинг асосий компонентлари (кодер, контейнер, калит, психовизуал)

2. Тасодифий тарзда тулдирилган жадвал асосида Трисемус шифрлаш усули (тасодифий, калитли, жадвал, сатр, устун)

3. Махсус файл билан антивирус дастурларни диагностика қилиш (тадқиқот, файл, матн редактори, буйруқ сатри).

4. Белгилар сони 9 та булган (бўшлик белгиси ҳисобланмайди) матнни танланг ва уни 3х3 сехрли квадрат ёрдамида шифрланг.

29 -вариант

1. Компьютер стеганографиясида маълумотларни ўрнатиш усуллари (ҳимоя, сарлавҳа, аннотация, яширин, ниқоблаш).

2. Плейфернинг шифрлаш усули (жадвал, биграмма, тўртбурчак).

3. Жихоздар регистри бўйича шахсий компьютер аппарат таркибини аниқлаш асослари (хотира, ячейка, разряд, қиймат, адаптер, диск юритувчи).

4. Икки марталик ўрин алмаштириш усули билан шифрлашга мисол келтиринг.

30 -вариант

1. Антивирус дастурлари (детекторлар, фаглар, вакциналар, прививкалар, ревизорлар, мониторлар).

2. Симметрияли криптотизимларда оддий жадвал асосида ўрин алмаштириш усуллари. (жадвал, калитли сўз).

3. Гаммалаш шифрлари ва тасодифий кетма-кетлик генератори (шифр, гамма, қуйиш, тасодифий сон, конгруэнт, рекуррент).

4. Дастурни рухсат этилмаган нусхалашдан химоялашни амалга ошириш учун компьютердаги доимий хотирани ишлаб чикилган санасини аниклайдиган дастур тузинг.

6. ЎҚУВ МАТЕРИАЛЛАРИ
6.1. Маъруза матни

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

Самарқанд давлат университети

«Ахборотлаштириш технологиялари» кафедраси

А.Ахатов

«АХБОРОТЛАРНИ ҲИМОЯЛАШ»

фанидан

МАЪРУЗАЛАР МАТНИ

САМАРҚАНД – 2019

СУЗ БОШИ

Тез ривожланиб бораётган компьютер ахборот технологиялари бизнинг кундалик хаётимизнинг барча жабхаларида сезиларли узгаришларни олиб кирмокда. Хозирда “ахборот тушунчаси” сотиб олиш, сотиш, бирор бошка товарга алмаштириш мумкин булган махсус товар белгиси сифатида тез-тез ишлатилмокда. Шу билан бирга ахборотнинг бахоси куп холларда унинг узи жойлашган компьютер тизимининг бахосида бир неча юз ва минг баробарга ошиб кетмокда. Шунинг учун тамомила табиий холда ахборотни унга рухсат этилмаган холда киришдан, касддан узгартиришдан, уни угирлашдан, йукотишдан ва бошка жиноий характерлардан химоя килишга кучли зарурат тугилади.

Компьютер тизимлари ва тармокларида ахборотни химоя остига олиш деганда, берилаётган, сакланаётган ва кайта ишланилаётган ахборотни ишончлилигини тизимли тарзда таъминлаш максадида турли восита ва усулларни куллаш, чораларни куриш ва тадбирларни амалга оширишни тушуниш кабул килинган.

Ахборотни химоя килиш деганда:

- Ахборотнинг жисмоний бутунлигини таъминлаш, шу билан бирга ахборот элементларининг бузилиши, ёки йук килинишига йул куймаслик;
- Ахборотнинг бутунлигини саклаб колган холда, уни элементларини калбакилаштиришга (узгартиришга) йул куймаслик;
- Ахборотни тегишли хукукуларга эга булмаган шахслар ёки жараёнлар оркали тармокдан рухсат этилмаган холда олишга йул куймаслик;
- Эгаси томонидан берилаётган (сотилаётган) ахборот ва ресурслар факат томонлар уртасида келишилган шартномалар асосида кулланилишига ишониш кабилар тушунилади.

Юкорида таъкидлаб утилганларнинг барчаси асосида компьютер тармоклари ва тизимларида ахборот хавфсизлиги муаммосининг долзарблиги ва мухимлиги келиб чикади. Шунинг учун хозирги курс Республикамизнинг олий ва урта махсус укув муассасалари укув режаларида муносиб урин эгаллайди.

Ушбу курснинг вазифалари:

- Талабаларда компьютер тармоклари ва тизимларида ахборот хавфсизлиги тугрисидаги билимларни шакллантириш;
- Ахборотни химоя килишнинг назарий, амалий ва услубий асосларини бериш;
- Талабаларга компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллашни амалий жихатдан ургатиш;
- Талабаларни ахборотни химоя килиш буйича ишлаб чикарилган турли хил дастурий махсулотлардан эркин фойдалана олиш имконини берадиган билимлар билан таъминлаш;

Курсни узлаштириш натижасида талаба куйидагиларнибилиши шарт;

- компьютер тармоклари ва тизимларидаги ахборот хавфсизлигига тахдид солиши кутилаётган хавф хатарнинг мохиятини ва окибатларини тушуниши;
- компьютер тармоклари ва тизимларида ахборотни химоя килиш буйича куйиладиган асосий талаблар ва асосларни узлаштириш;
- компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашда кулланиладиган замонавий усуллар ва воситаларни билиш;
- тизимларда ахборот бутунлиги ва ишочлигини бузувчи вируслар ва бошка манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлаштириш буйича чораларни куриш;

ахборотни химоя килишда кулланиладиган замонавий амалий тизимлар ва дастурий махсулотларни ишлата олиш;

1 - МАВЗУ: ЗАМОНАВИЙ АХБОРОТЛАШГАН ЖАМИЯТ ВА АХБОРОТ ХАВФСИЗЛИГИ. АСОСИЙ ТУШУНЧАЛАР ВА ТАЪРИФЛАР

1. Ахборот хавфсизлигига кириш;
2. Предметнинг асосий тушунчалари ва мақсади;
3. Ахборотларга нисбатан хавф-хатарлар таснифи;
4. Тармок хавфсизлигини назорат килиш воситалари

Ахборот хавфсизлигига кириш

Мамлакатимиз миллий иқтисодининг ҳеч бир тармоғи самарали ва мўътадил ташкил қилинган ахборот инфратузилмасисиз фаолият кўрсатиши мумкин эмас. Ҳозирги кунда миллий ахборот ресурслари хар бир давлатнинг иқтисодий ва харбий салоҳиятини ташкил қилувчи омилларидан бири бўлиб хизмат килмокда. Ушбу ресурсдан самарали фойдаланиш мамлакат хавфсизлигини ва демократик ахборотлашган жамиятни муваффақиятли шакллантиришни таъминлайди. Бундай жамиятда ахборот алмашуви тезлиги юксалади, ахборотларни йиғиш, сақлаш, қайта ишлаш ва улардан фойдаланиш бўйича илғор ахборот – коммуникациялар технологияларини қўллаш кенгаяди. Турли хилдаги ахборотлар худудий жойлашишидан қатъий назар бизнинг кундалик ҳаётимизга Internet ҳалқаро компьютер тармоғи орқали кириб келди. Ахборотлашган жамият шу компьютер тармоғи орқали тезлик билан шаклланиб бормокда. Ахборотлар дунёсига саёҳат қилишда давлат чегаралари деган тушунча йўқолиб бормокда. Жаҳон компьютер тармоғи давлат бошқарувини тубдан ўзгартирмоқда, яъни давлат ахборотларнинг тарқалиши механизмини бошқара олмай қолмоқда. Шунинг учун хам мавжуд ахборотларга ноқонуний кириш, улардан фойдаланиш ва йўқотиш каби муаммолар долзарб бўлиб қолди. Буларнинг бари шахс, жамият ва давлатнинг ахборот хавфсизлиги даражасининг пасайишига олиб келмоқда. Давлатнинг ахборот хавфсизлигини таъминлаш муаммоси миллий хавфсизликни таъминлашнинг асосий ва ажралмас қисми бўлиб, ахборот ҳимояси эса давлатнинг бирламчи масалаларига айланмоқда.

Ҳозирги кунда хавфсизликнинг бир қанча йўналишларини қайд этиш мумкин. (1-расм)

Предметнинг асосий тушунчалари ва мақсади

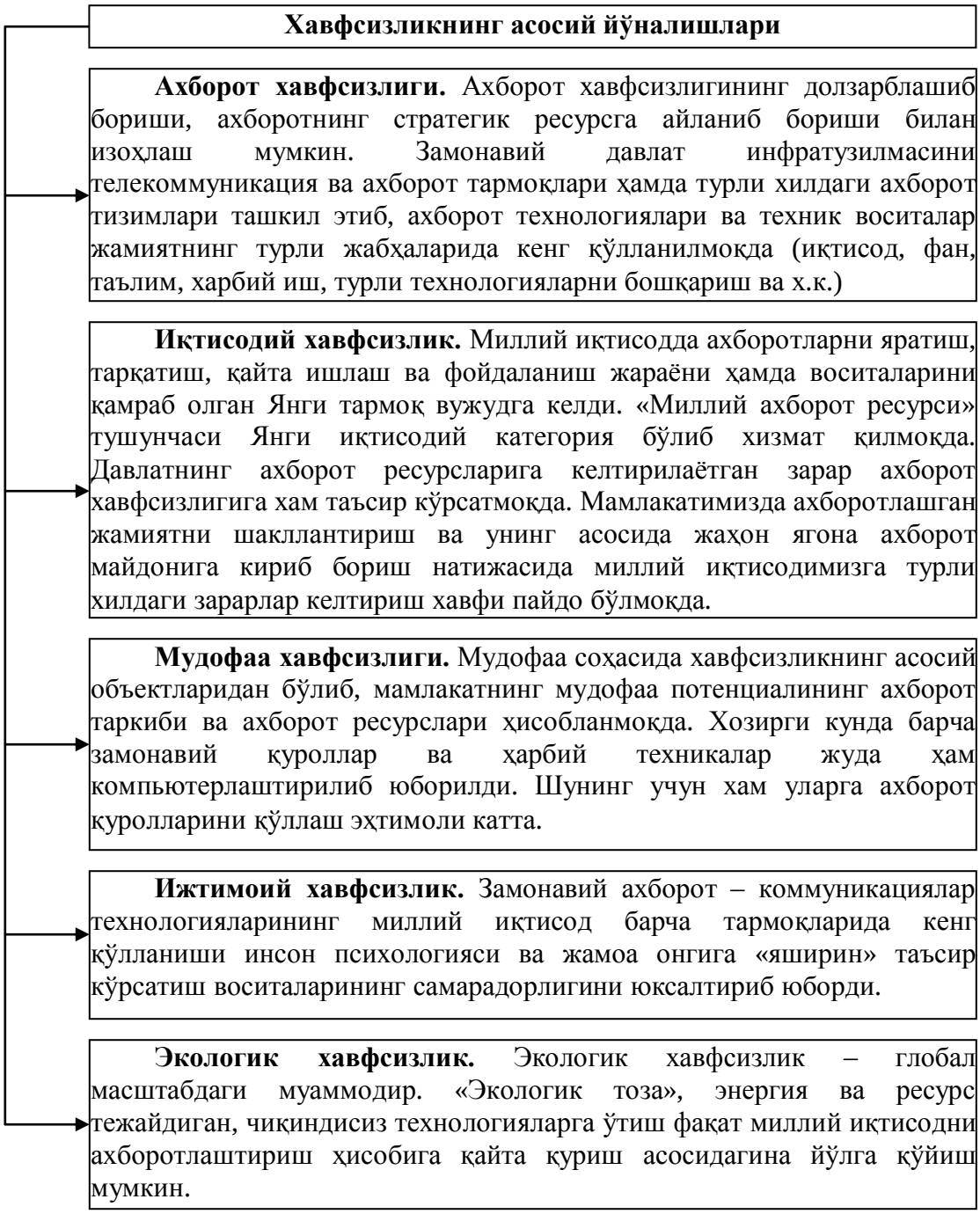
Ахборотнинг мухимлик даражаси қадим замонлардан маълум. Шунинг учун хам қадимда ахборотни ҳимоялаш учун турли хил усуллар қўлланилган. Улардан бири – сирли ёзувдир. Ундаги хабарни хабар юборилган манзил эгасидан бошқа шахс ўқий олмаган. Асрлар давомида бу санъат – сирли ёзув жамиятнинг юқори табақалари, давлатнинг элчихона резиденциялари ва разведка миссияларидан ташқарига чиқмаган. Фақат бир неча ўн йил олдин ҳамма нарса тубдан ўзгарди, яъни ахборот ўз қийматига эга бўлди ва кенг тарқаладиган маҳсулотга айланди. Уни эндиликда ишлаб чиқарадилар, сақлайдилар, узатишади, сотадилар ва сотиб оладилар. Булардан ташқари уни ўғирлайдилар, бузиб талқин этадилар ва сохталаштирадилар. Шундай қилиб, ахборотни ҳимоялаш зарурияти туғилади. Ахборотни қайта ишлаш саноатининг пайдо бўлиши ахборотни ҳимоялаш саноатининг пайдо бўлишига олиб келади.

Автоматлаштирилтан ахборот тизимларида ахборотлар ўзининг ҳаётий даврига эга бўлади. Бу давр уни яратиш, ундан фойдаланиш ва керак бўлмаганда йўқотишдан иборатдир (2-расм).

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

Махфий ва қимматбаҳо ахборотларга рухсатсиз киришдан ҳимоялаш энг мухим вазифалардан бири саналади. Компьютер эгалари ва фойдаланувчиларнинг мулки ҳуқуқларини ҳимоялаш - бу ишлаб чиқарилаётган ахборотларни жиддий иқтисодий ва

бошҳа моддий ҳамда номоддий зарарлар келтириши мумкин бўлган турли киришлар ва ўғирлашлардан ҳимоялашдир.



1-расм.

2-расм

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

Илгариги хавф фақатгина конфиденциал (махфий) хабарлар ва хужжатларни ўгирлаш ёки нусха олишдан иборат бўлса, ҳозирги пайтдаги хавф эса компьютер маълумотлари тўплами, электрон маълумотлар, электрон массивлардан уларнинг эгасидан рухсат сўрамасдан фойдаланишдир. Булардан ташқари, бу харакатлардан моддий фойда олишга интилиш ҳам ривожланди.

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

Ахборотнинг эгасига, фойдаланувчисига ва бошка шахсга зарар етказмокчи бўлган ноҳуқуқий муомаладан хар қандай х**ужжатлаштирилган,** яъни идентификация қилиш имконини берувчи реквизитлари қўйилган холда моддий жисмда қайд этилган **ахборот** химояланиши керак.

Ахборот хавфсизлиги нуктаи назаридан ахборотни қуйидагича туркумлаш мумкин:

• **махфийлик** — аниқ бир ахборотга факат тегишли шахслар доирасигина кириши мумкинлиги, яъни фойдаланилиши қонуний хужжатларга мувофик чеклаб қўйилиб, хужжатлаштирилганлиги кафолати. Бу банднинг бузилиши **ўгирлик** ёки **ахборотни ошкор қилиш,** дейилади;

• **конфиденциаллик** — иншончлилиги, тарқатилиши мумкин эмаслиги, махфийлиги кафолати;

• **яхлитлик** — ахборот бошланғич кўринишда эканлиги, яъни уни сақлаш ва узатишда рухсат этилмаган ўзгаришлар қилинмаганлиги кафолати; бу банднинг бузилиши **ахборотни сохталаштириш** дейилади;

• **аутентификация** — ахборот захираси эгаси деб эълон қилинган шахс хақиқатан хам ахборотнинг эгаси эканлигига бериладиган кафолат; бу банднинг бузилиши **хабар муаллифини сохталаштириш** дейилади;

• **апелляция килишлик** — етарлича мураккаб категория, лекин электрон бизнесда кенг қўлланилади. Керак бўлганда хабарнинг муаллифи кимлигини исботлаш мумкинлиги кафолати.

Юкоридагидек, ахборот тизимига нисбатан қуйидагича таснифни келтириш мумкин:

• **ишончлилик** — тизим меьёрий ва ғайри табиий холларда режалаштирилганидек ўзини тутишлик кафолати;

• **аниқлилик** — хамма буйруқларни аниқ ва тўлиқ бажариш кафолати;

• **тизимга киришни назорат килиш —** турли шахс гурухлари ахборот манбаларига хар хил киришга эгалиги ва бундай киришга чеклашлар доим бажарилишлик кафолати;

• **назорат килиниши** — исталган пайтда дастур мажмуасининг хохлаган кисмини тулик текшириш мумкинлиги кафолати;

• **идентификациялашни назорат килиш** — хозир тизимга уланган мижоз аниқ ўзини ким деб атаган булса, аниқ ўша эканлигининг кафолати;

• **қасддан бузилишларга тўсқинлик** — олдиндан келишилган меъёрлар чегарасида қасддан хато киритилган маълумотларга нисбатан тизимнинг олдиндан келишилган холда ўзини тутиши.

Ахборотни химоялашнинг мақсадлари куйидагилардан иборат:

- ахборотнинг келишувсиз чикиб кетиши, угирланиши, йукотилиши, узгартирилиши, сохталаштирилишларнинг олдини олиш;

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

- ахборотни йук килиш, узгартириш, сохталаштириш, нусха кучириш, тусиклаш буйича рухсат этилмаган харакатларнинг олдини олиш;

- хужжатлаштирилган ахборотнинг микдори сифатида хукукий тартибини таъминловчи, ахборот захираси ва ахборот тизимига хар кандай ноконуний аралашувларнинг куринишларининг олдини олиш;

- ахборот тизимида мавжуд булган шахсий маълумотларнинг шахсий махфийлигини ва конфиденциаллигини сакловчи фукароларнинг конституцион хукукларини химоялаш;

- давлат сирини, конунчиликка мос хужжатлаштирилган ахборотнинг конфиденциаллигини саклаш;

- ахборот тизимлари, технологиялари ва уларни таъминловчи воситаларни яратиш, ишлаб чикиш ва куллашда субъектларнинг хукукларини таъминлаш.

Тармок хавфсизлигини назорат килиш воситалари

Замонавий ахборот - коммуникациялар технологияларининг ютуклари химоя услубларининг бир катор зарурий инструментал воситаларини яратиш имконини берди.

Ахборотларни химояловчи инструментал воситалар деганда дастурлаш, дастурий - аппаратли ва аппаратли воситалар тушунилади. Уларнинг функционал тулдирилиши хавфсизлик хизматлари олдига куйилган ахборотларни химоялаш масалаларини ечишда самаралидир. Хозирги кунда тармок хавфсизлигини назорат килиш техник воситаларининг жуда кенг спектри ишлаб чикарилган.

Такрорлаш учун саволлар

1. Ахборот хавфсизлиги мақсад ва вазифаларинимадан иборат?
2. Предметнинг асосий тушунчаларини таърифлаб беринг.
3. Ахборотларга нисбатан хавф-хатарларни таснифлаб беринг.
4. Қайси тармок хавфсизлигини назорат килиш воситаларини биласиз?

2 – МАВЗУ: АХБОРОТ ХАВФСИЗЛИГИНИНГ АСОСИЙ ХАВФЛАРИ

1. Автоматлаштирилган ахборот тизимларида химоялаш зарурияти;
2. Ахборотни химоялаш тизими;
3. Ташкилотлардаги ахборотларни химоялаш;
4. Химоялаш тизимининг комплекслилиги;
5. Ахборотларни ташкилий ҳимоялаш элементлари;
6. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар.

Автоматлаштирилган ахборот тизимларида химоялаш зарурияти

Ахборот - коммуникациялар технологияларининг оммавий равишда когозсиз автоматлаштирилган асосда бошкарилиши сабабли ахборот хавфсизлигини таъминлаш мураккаблашиб ва мухимлашиб бормокда. Шунинг учун хам автоматлаштирилган ахборот тизимларида ахборотни химоялашнинг янги замонавий технологияси пайдо булмокда. DataQuest компаниясининг маълумотига кура, 1996—2000 йилларда ахборот химояси воситаларининг сотувдаги хажми 13 млрд. АКШ долларига тенг булган.

Ахборотни химоялаш тизими

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

Ахборот эгалари хамда ваколатли давлат органлари шахсан ахборотнинг кимматлилиги, унинг йукотилишидан келадиган зарар ва химоялаш механизмининг нархидан келиб чиккан холда ахборотни химоялашнинг зарурий даражаси хамда тизимнинг турини, химоялаш усуллар ва воситаларини аниклашлари зарур. Ахборотнинг кимматлилиги ва талаб килинадиган химоянинг ишончлилиги бир-бири билан бевосита боглик.

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

Ташкилотлардаги ахборотларни химоялаш

Ахборот хажми кичик булган ташкилотларда ахборотларни химоялашда оддий усулларни куллаш максадга мувофик ва самаралидир. Масалан, укиладиган кимматбохо когозларни ва электрон хужжатларни алохида гурухларга ажратиш ва никоблаш, ушбу хужжатлар билан ишлайдиган ходимни тайинлаш ва ургатиш, бинони куриклашни ташкил этиш, хизматчиларга кимматли ахборотларни таркатмаслик мажбуриятини юклаш, ташкаридан келувчилар устидан назорат килиш, компьютерни химоялашнинг энг оддий усулларини куллаш ва хоказо. Одатда, химоялашнинг энг оддий усулларини куллаш сезиларли самара беради.

Мураккаб таркибли, куп сонли автоматлаштирилган ахборот тизими ва ахборот хажми катга булган ташкилотларда ахборотни химоялаш учун химоялашнинг мажмуали тизими ташкил килинади. Лекин ушбу усул хамда химоялашнинг оддий усуллари хизматчиларнинг ишига хаддан ташкари халакит бермаслиги керак.

Химоялаш тизимининг комплекслилиги

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

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

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

Ахборотларни ташкилий ҳимоялаш элементлари

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

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

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

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

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

Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

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

Автоматлаштирилган ахборот тизимларига тасодифий таъсир курсатиш сабаблари таркибига куйидагилар киради.

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

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

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

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

— ўзгартириш — ушбу жараён ёвуз ниятли шахс нафақат компьютер тизими компонентларига (маълумотлар тупламлари, дастурлар, техник элементлари) киришни қулга киритади, балки улар билан манипуляция (ўзгартириш, кўринишини ўзгартириш) ҳам килади. Масалан, ўзгартириш сифатида ғаразли шахснинг маълумотлар тўпламидаги маълумотларни ўзгартириши, ёки умуман копьютер тизими файлларини ўзгартириши, ёки кандайдир қўшимча ноқонуний кайта ишлашни амалга ошириш максадида фойдаланилаётган дастурнинг кодини ўзгартириши тушунилали;

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

Такрорлаш учун саволлар

1. Автоматлаштирилган ахборот тизимларида химоялаш зарурияти.

2. Ахборотни химоялаш тизими элементларини айтиб утинг.

3. Ташкилотлардаги ахборотларни химоялаш мухимлигини тушунтириб беринг.

4. Химоялаш тизимининг комплекслилигига андай эришилади.

5. Ахборотларни ташкилий ҳимоялаш элементлари вазифаси.

6. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

3 – МАВЗУ: ВИРУС ВА АНТИВИРУСЛАР ТАСНИФИ

1. Вирус ва унинг турлари;

2. Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш;

3. Антивирус дастурлари;

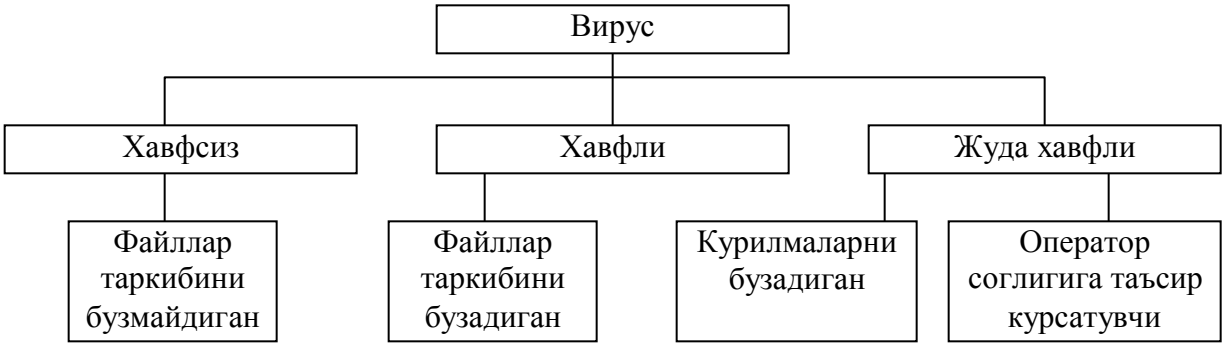
4. Вирусларга қарши чора-тадбирлар.

Вирус ва унинг турлари

Ҳозирги кунда компьютер вируслари ғаразли мақсадларда ишлатилувчи турли хил дастурларни олиб келиб татбиқ этишда энг самарали воситалардан бири ҳисобланади. Компьютер вирусларини **дастурли вируслар** деб аташ тугрироқ бўлади.

Дастурли вирус деб автоном равишда ишлаш, бошқа дастур таркибига ўз – ўзидан қушилувчи, ишга кодир ва компьютер тармоқлари ва алоҳида компьютерларда уз – узидан таркалиш хусусиятига эга булган дастурга айтилади.

Вируслар билан зарарланган дастурлар **вирус ташувчи** ёки **зарарланган дастурлар** дейилади.



Зарарланган диск – бу ишга тушириш секторида вирус дастур жойлашиб олган дискдир.

Хозирги пайтда компьютерлар учун купгина нокулайликлар тугдираётган хар хил турлардаги компьютер вируслари кенг таркалган. Шунинг учун хам улардан сакланиш усулларини ишлаб чикиш мухим масалалардан бири хисобланади. Хозирги вактда 65000 дан куп булган вирус дастурлари борлиги аникланган. Бу вирусларнинг катта гурухини компъютернинг иш бажариш тартибини бузмайдиган, яъни «таъсирчан булмаган» вируслар гурухи ташкил этадиди.

Вирусларнинг бошка гурухига компьютернинг иш тартибини бузувчи вируслар киради. Бу вирусларни куйидаги турларга булиш мумкин: **хавфсиз вируслар** (файллар таркибини бузмайдиган), **хавфли вируслар** (файллар таркибини бузувчи) хамда **жуда хавфли вируслар** (компьютер курилмаларини бузувчи ва оператор соглигига таъсир этувчи). Бу каби вируслар одатда профессионал дастурчилар томонидан тузилади.

Компьютер вируси – бу махсус ёзилган дастур булиб, бошка дастурлар таркибига ёзилади, яъни зарарлайди ва компьютерларда узининг гаразли максадларини амалга оширади.

Компьютер вируси оркали зарарланиш окибатида компьютерларда куйидаги узгаришлар пайдо булади:

• айрим дастурлар ишламайди ёки хато ишлай бошлайди;

• бажарилувчи файлнинг хажми ва унинг яратилган вакти узгаради;

• экранда англаб булмайдиган белгилар, турли хил тасвир ва товушлар пайдо булади;

• компьютернинг ишлаши секинлашади ва тезкор хотирадаги буш жой хажми камаяди;

• диск ёки дискдаги бир неча файллар зарарланади (баъзи холларда диск ва файлларни тиклаб булмайди):

• винчестер оркали компьютернинг ишга тушиши йуколади.

Вируслар асосан дискларнинг юкланувчи секторларини ва exe, com, sys ва bat кенгайтмали файлларни зарарлайди. Хозирги кунда булар каторига офис дастурлари яратадиган файларни хам киритиш мумкин. Оддий матнли файлларни зарарлайдиган вируслар камдан – кам учрайди.

Файллар таркибини бузмайдиган вируслар

Тезкор хотира курилмасида купаювчи	**Операторни таъсирлантирувчи**	**Тармок вируслари**

Операторни таъсирлантирувчи

Курилмаларни ишдан чикарувчи	**Терминалда хабар чикарувчи**	**Товушли эффектларни хосил килувчи**	**Иш тартибини узгартирувчи**
- процессор - хотира - МД, винчестер - принтер - порт PS-232 Дисплей - клавиатура	- матнли - графикли	- оханг - нутк синтези - махсус эффектлар	- клавиатура - дисплей принтер - порт PS-232

Компьютернинг вируслар билан зарарланиш йуллари куйидагилардир:

1. Дискетлар оркали.
2. Компьютер тармоклари оркали.
3. Бошка йуллар йук.

Файл таркибини бузувчи вируслар

Фойдаланувчининг маълумотлари ва дастурларни бузувчи		**Тизим маълумотларини бузувчи**		
Дастурларни бузувчи	Маълумотларни бузувчи	Диск сохасини бузувчи	Форма тлаш	Тезкор тизим файлларини бузувчи
Дастурнинг бошлангич Ёзувлар	Маълумотлар базаларини Бузувчи	Дискнинг мантикий Таркиби		

и н и бузувчи		н и бузиш
Бажарилувчи дастурларни бузувчи	Матнли хужжатларни бузувчи	Маълумот ташувчиларнинг таркибини бузувчи
Компиляторларнинг кисм дастурлар тупламини бузувчи	График тасвирларни бузувчи	
	Электрон жадвални бузувчи	

Оператор ва курилмаларга таъсир этувчи вируслар

Курилмаларни бузувчи				**Операторга таъсир этувчи**
Дисплейнинг Люминафор катламини куйдирувчи	Компьютерларнинг микро схемасини ишдан чикарувчи	Принтерни ишдан чикарувчи	МДни бузувчи	Оператор техникасига таъсир этувчи

Хозирги пайтда хазил шаклидаги вируслардан тортиб то компьютер курилмаларини ишдан чикарувчи вирусларнинг турлари мавжуд.

Масалан. Win 95.CIH вируси доимий саклаш курилмаси (Flash BIOS) микросхемасини бузади. Афсуски, бу каби вирусларни йук килиш учун, факат улар уз гаразли ишини бажариб булгандан сунггина, карши чоралар ишлаб чикилади. Win 95.CIH вирусига карши чораларни куриш имконияти Dr.Web дастурида мавжуд.

Компьютер вирусларидан ахборотларга рухсатсиз кириш ва улардан фойдаланишни ташкил этиш

Шуни айтиб утиш лозимки, хозирги пайтда хар-хил турдаги ахборот ва дастурларни угирлаб олиш ниятида компьютер вирусларидан фойдаланиш энг самарали усуллардан бири хисобланади.

Дастурли вируслар компьютер тизимларининг хавфсизлигига тахдид солишнинг энг самарали воситаларидан биридир. Шунинг учун хам дастурли вирусларнинг имкониятларини тахлил килиш масаласи хамда бу вирусларга карши курашиш хозирги пайтнинг долзарб масалаларидан бири булиб колди.

Вируслардан ташкари файллар таркибини бузувчи **троян дастурлари** мавжуд. Вирус купинча компьютерга сездирмасдан киради. Фойдаланувчининт узи троян дастурини фойдали дастур сифатида дискка ёзади. Маълум бир вакт утгандан кейин бузгунчи дастур уз таъсирини курсатади.

Уз-узидан пайдо буладиган вируслар мавжуд эмас. Вирус дастурлари инсон томонидан компьютернинг дастурий таъминотини, унинг курилмаларини зарарлаш ва бошка максадлар учун ёзилади. Вирусларнинг хажми бир неча байтдан то унлаб килобайтгача булиши мумкин.

Троян дастурлари фойдаланувчига зарар келтирувчи булиб, улар буйруклар (модуллар) кетма – кетлигидан ташкил топган, омма орасида жуда кенг таркалган

дастурлар (таҳрирловчилар, ўйинлар, трансляторлар) ичига ўрнатилган бўлиб, бир қанча ҳодисалар бажарилиши билан ишга тушадиган «мантиқий бомба» деб аталадиган дастурдир. Ўз навбатида, «мантикий бомба»нинг турли кўринишларидан бири «соат механизмли бомба» ҳисобланади.

Шуни таъкидлаб ўтиш керакки, троян дастурлари ўз-ўзидан кўпаймасдан, компьютер тизими бўйича дастурловчилар томонидан тарқатилади.

Троян дастурлардан вирусларнинг фарқи шундаки, вируслар компьютер тизимлари буйлаб таркатилганда, улар мустақил равишда ҳосил бўлиб, ўз иш фаолиятида дастурларга ўз матнларини ёзган ҳолда уларга зарар кўрсатади.

Зарарланган дастурда дастур бажарилмасдан олдин вирус ўзининг буйруқлари бажарилишига имконият яратиб беради. Бунинг учун хам вирус дастурнинг бош қисмида жойлашади ёки дастурнинг биринчи буйруги унга ёзилган вирус дастурига шартсиз ўтиш бўлиб хизмат қилади. Бошқарилган вирус бошқа дастурларни зарарлайди ва шундан сўнг вирус ташувчи дастурга ишни топширади.

Вирус ҳаёти одатда қуйидаги даврларни ўз ичига олади: **қулланилиш, инкубация, репликация** (ўз-ўзидан кўпайиш) ва **ҳосил бўлиш.** Инкубация даврида вирус пассив бўлиб, уни излаб топиш ва йукотиш кийин. Ҳосил булиш даврида у ўз функциясини бажаради ва қўйилган мақсадига эришади.

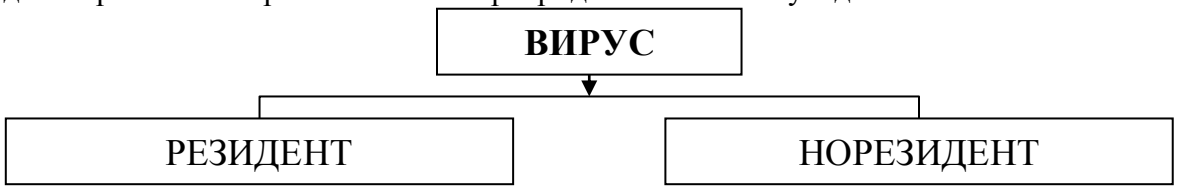
Таркиби жиҳатидан вирус жуда оддий бўлиб, бош қисм ва баьзи ҳолларда думдан иборат. Вируснинг бош қисми деб бошкарилишини биринчи бўлиб таъминловчи имкониятга эга бўлган дастурга айтилади. Вируснинг дум қисми зарарланган дастурда бўлиб, у бош кисмидан алоҳида жойда жойлашади.

Компьютер вируслари характерларига нисбатан **норезидент, резидент, бутли, гибридли ва пакетли вирусла**рга ажратилади.

Файлли **норезидент вируслар** тўлиқлигича бажарилаётган файлда жойлашади, шунинг учун ҳам у фақат вирус ташувчи дастур фаоллашгандан сўнг ишга тушади ва бажарилгандан сўнг тезкор хотирада сақланмайди.

Резидент вирус норезидент вирусдан фарқлироқ тезкор хотирада сақланади.

Резидент вирусларнинг яна бир кўриниши **бут вируслар** бўлиб, бу вируснинг вазифаси винчестер ва эгилувчан магнитли дискларнинг юкловчи секторини ишдан чиқаришдан иборат. Бут вирусларнинг боши дискнинг юкловчи бут секторида ва думи дискларнинг ихтиёрий бошка секторларида жойлашган бўлади.



Пакетли вируснинг бош қисми пакетли файлда жойлашган бўлиб, у операцион тизим топшириқларидан иборат.

Гибридли вирусларнинг боши пакетли файлда жойлашади. Бу вирус хам файлли, ҳам бут секторли бўлади.

Тармоқли вируслар компьютер тармокларида тарқалишга мослаштирилган, яъни тармоқли вируслар деб ахборот алмашишда тарқаладиган вирусларга айтилади.

Вирусларнинг турлари:

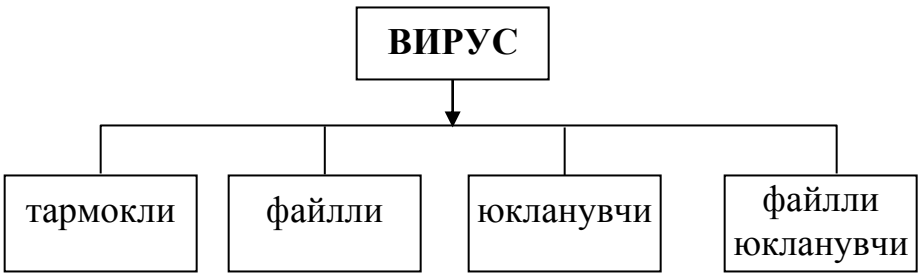
1) **файл вируслари.** Бу вируслар *com, exe* каби турли файлларни зарарлайди;

2) **юкловчи вируслар.** Компьютерни юкловчи дастурларни зарарлайди;

3) **драйверларни зарарловчи вируслар.** Операцион тизимдаги config.sys файлни зарарлайди. Бу компьютернинг ишламаслигига сабаб бўлади;

4) **DIR вируслари.** FAT таркибини зарарлайди;

5) **стелс-вируслари.** Бу вируслар ўзининг таркибини узгартириб, тасодифий код ўзгариши бўйича тарқалади. Уни аниклаш жуда қийин, чунки файлларнинг ўзлари ўзгармайди;



6) **Windows вируслари.** Windows операцион тизимидаги дастурларни зараралайди.

Мисол сифатида қуйидагиларни келтириш мумкин:

1) Энг хавфли вируслардан бири Internet орқали тарқатилган «Чернобиль» вируси бўлиб, у 26 апрелда таркатилган ва ҳар ойнинг 26-кунида компъютерларни зараралаши мумкин.

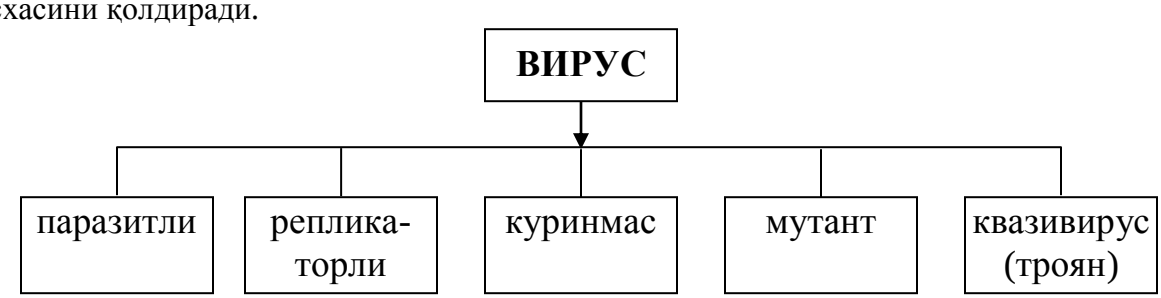
2) I LOVE YOU вируси Филиппиндан 2000 йил 4 майда E-mail оркали тарқатилган. У бугун жаҳон буйича 45 млн. компьютерни зараралаган ва ишдан чикарган. Моддий зарар 10 млрд. АҚШ долларини ташкил килган.

3) 2003 йил март ойида Швециядан злектрон почта оркали GANDA вируси тарқатилган ва у бутун дунёда минглаб компьютерларни зараралаган. Бу вирусни тарқатган шахс ҳозир қулга олинган ва у 4 йил камоқ жазосига ҳукм этилиши мумкин.

Асосланган алгоритмлар буйича дастурли вирусларни куйидагича таснифлаш мумкин.

Паразитли вирус — файлларнинг таркибини ва дискнинг секторини узгартирувчи вирус. Бу вирус оддий вируслар туркумидан бўлиб, осонлик билан аниқланади ва ўчириб ташланади.

Репликаторли вирус — «чувалчанг» деб номланади, компьютер тармоқлари бўйича тарқалиб, комльютерларнинг тармоқдаги манзилини аниқлайди ва у ерда ўзининг нусхасини қолдиради.



Куринмас вирус — стелс-вирус деб ном олиб, зарарланган файлларга ва секторларга операцион тизим томонидан мурожаат қилинса, автоматик равишда зарарланган қисмлар ўрнига дискнинг тоза қисмини тақдим этади. Натижада ушбу вирусларни аниқлаш ва тозалаш жуда катта қийинчиликларга олиб келади.

Мутант вирус — шифрлаш ва дешифрлаш алгоритмларидан иборат бўлиб, натижада вирус нусхалари умуман бир-бирига ўхшамайди. Ушбу вирусларни аниқлаш жуда қийин муаммо.

Квазивирус вирус — «Троян» дастурлари, деб ном олган бўлиб, ушбу вируслар кўпайиш хусусиятига эга бўлмаса-да, «фойдали» қисм-дастур хисобида бўлиб, антивирус дастурлар томонидан аниқланмайди. Шу боис ҳам улар ўзларида мукаммаллаштирилган алгоритмларни тўсиқсиз бажариб, қўйилган мақсадларига эришишлари мумкин.

Антивирус дастурлари

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

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни

топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги хисобланади.

Фаглар— детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги холатига кайтаради.

Вакциналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга урнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан вакцина қилиниши унинг камчилиги ҳисобланади. Шу боис хам, ушбу антивирус дастурлари кенг тарқалмаган.

Прививка — файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди.

Фильтрлар — қуриқловчи дастурлар куринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради.

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

Детектор дастурлар компьютер хотирасидан, файллардан вирусларни қидиради ва аниқланган вируслар хақида хабар беради.

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

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

Бу харакатлар куйидагича бўлиши мумкин:

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

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

Вирусларга қарши чора-тадбирлар

Компьютерни вируслар билан зарарланишидан саклаш ва ахборотларни ишончли сақлаш учун қуйидаги қоидаларга амал қилиш лозим:

- компьютерни замонавий антивирус дастурлар билан таъминлаш;
- дискеталарни ишлатишдан олдин ҳар доим вирусга қарши текшириш;
- қимматли ахборотларнинг нусхасини ҳар доим архив файл кўринишида сақлаш.

Компьютер вирусларига карши курашнинг қуйидаги турлари мавжуд:

- вируслар компьютерга кириб бузган файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компьютерга пароль билан кириш, диск юритувчиларнинг ёпиқ туриши;
- дискларни ёзишдан химоялаш;
- лицензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- компьютерга кириталаётган дастурларнинг вирусларнинг мавжудлигини текшириш;
- антивирус дастурларидан кенг фойдаланиш;
- даврий равишда компьютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Антивирус дастурларидан DrWeb, Adinf, AVP, BootCHK ва Norton Antivirus, Kaspersky Security кабилар кенг фойлаланилади.

Такрорлаш учун саволлар

1.Вирус тушунчасини таърифлаб беринг.

2. Компьютернинг вируслар билан зарарланиш йулларинпи айтиб утинг.

3. Компьютер вирусларидан ахборотларга рухсатсиз кириш қандай ташкил қилинади?

4. Антивирус дастурларини таснифлаб беринг.

5. Вирусларга қарши қандай чора-тадбирлар самарали ҳисбланади.

4 – МАВЗУ: АХБОРОТЛАРНИ СТЕГАНОГРАФИК ВА КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

1. Замонавий компьютер стенографияси;
2. Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш.
3. Стенографик дастурлар тўғрисида кисқача маьлумот
4. Криптография ҳақида асосий тушунчалар.
5. Симметрияли криптотизим асослари.

Замонавий компьютер стеганографияси

Рухсат этилмаган киришдан ахборотни ишончли ҳимоялаш муаммоси энг илгаритдан мавжуд ва ҳозирги вақтгача ҳал қилинмаган. Махфий хабарларни яшириш усуллари қадимдан маълум, инсон фаолиятининг бу соҳаси **стеганография** деган ном олган. Бу сўз грекча **Steganos** (махфий, сир) ва **Graphy** (ёзув) сўзларидан келиб чиққан ва «сирли ёзув» деган маънони билдиради. Стенография усуллари, эҳтимол, ёзув пайдо бўлишидан олдин пайдо бўлган (дастлаб шартли белги ва белгилашлар қулланилган) бўлиши мумкин.

Ахборотни ҳимоялаш учун **кодлаштириш** ва **криптография** усуллари қўлланилади.

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

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

Стеганографиянинг кринтографиядан бошқа ўзгача фарқи ҳам бор. Яъни унинг мақсади — махфий хабарнинг мавжудлигини яширишдир. Бу иккала усул бирлаштирилиши мумкин ва натижада ахборотни химоялаш самарадорлигини ошириш учун ишлатилиши имкони пайдо бўлади (масалан, криптографик калитларни узатиш учун).

Компьютер технологиялари стенографиянинг ривожланиши ва мукаммаллашувига янги туртки берди. Натижада ахборотни ҳимоялаш соҳасида янги йўналиш — **компьютер стеганогряфия**си пайдо бўлди.

Глобал компьютер тармоқлари ва мультимедиа сохасидаги замонавий прогресс телекоммуникация каналларида маълумотларни узатиш хавфсизлигини таъминлаш учун мўлжалланган янги усулларни яратишга олиб келди. Бу усуллар шифрлаш қурилмаларининг табиий ноаниқлигидан ва аналогли видео ёки аудиосигналларнинг сероблигидан фойдаланиб хабарларни компьютер файллари (контейнерлар)да яшириш имконини беради. Шу билан бирга криптографиядан фарқли равишда бу усуллар ахборотни узатиш фактининг ўзини ҳам яширади.

К.Шеннон сирли ёзувнинг умумий назариясини яратдики, у фан сифатида стенографиянинг базаси ҳисобланади. Замонавий компьютер стеганографиясида иккита асосий файл турлари мавжуд: яшириш учун мўлжалланган **хабар-файл**, ва **контейнер-файл**, у хабарни яшириш учун ишлатилиши мумкин. Бунда контейнерлар икки турда бўлади: **контейнер-оригинал** (ёки «бўш» контейнер) - бу контейнер яширин ахборотни сақламайди; **контейнер-натижа** (ёки «тулдирилган» контейнер) — бу контейнер яширин ахборотни сақлайди. **Калит** сифатида хабарни контейнерга киритиб куйиш тартибини аниклайдиган махфий элемент тушунилади.

Компьютер стенографияси ривожланиши тенденциясининг таҳлили шуни кўрсатадики, кейинги йилларда компьютер стенографияси усулларини ривожлантиришга қизиқиш кучайиб бормоқда. Жумладан, маълумки, ахборот хавфсизлиги муаммосининг долзарблиги доим кучайиб бормоқда ва ахборотни ҳимоялашнинг янги усулларини қидиришга рағбатлантирилаяпти. Бошка томондан, ахборот-коммуникациялар технологияларининг жадал ривожланиши ушбу ахборотни химоялашнинг янги усулларини жорий қилиш имкониятлари билан таъминлаяпти ва албатта, бу жараённинг кучли катализатори бўлиб умумфойдаланиладиган Internet компьютер тармогининг жуда кучли ривожланиши ҳисобланади.

Ҳозирги вақтда ахборотни ҳимоялаш энг кўп қулланилаётган соха бу — криптографик усуллардир. Лекин, бу йўлда компьютер вируслари, «мантиқий бомба»лар каби ахборотий қуролларнинг криптовоситаларни бузадиган таъсирига боғлиқ кўп ечилмаган муаммолар мавжуд. Бошка томондан, криптографик усулларни ишлатишда калитларни тақсимлаш муаммоси ҳам бугунги кунда охиригача ечилмай турибди. Компьютер стеганографияси ва криптографияларининг бирлаштирилиши пайдо бўлган шароитдан қутулишнинг яхши бир йўли булар эди, чунки, бу ҳолда ахборотни ҳимоялаш усулларининг заиф томонларини йўқотиш мумкин.

Шундай қилиб, компьютер стенографияси ҳозирги кунда ахборот хавфсизлиги бўйича асосий технологиялардан бири бўлиб ҳисобланади.

Замонавий компьютер стенографиясининг асосий ҳолатлари қуйидагилардан иборат:

- яшириш усуллари файлнинг аутентификацияланишлигини ва яхлитлигини таъминлаши керак;
- ёвуз ниятли шахсларга қўлланилувчи стеганография усуллари тўлиқ маьлум деб фараз қилинади;
- усулларнинг ахборотга нисбатан хавфсизликни таъминлаши очик узаталадиган файлнинг асосий хоссаларини стенографик алмаштиришлар билан сақлашга ва бошқа шахсларга номаълум бўлган қандайдир ахборот — калитга асосланади;
- агар ёвуз ниятли шахсларга хабарни очиш вақти маълум бўлиб қолган бўлса, махфий хабарнинг ўзини чикариб олиш жараёни мураккаб хисоблаш масаласи сифатида тасаввур қилиниши лозим.

Internet компьютер тармоғининг ахборот манбаларини таҳлили қуйидаги хулосага келишга имкон берди, яъни ҳозирги вақтда стенографик тизимлар қуйидаги асосий масалаларни ечишда фаол ишлатилаяпти:

- конфиденциал ахборотни рухсат этилмаган киришдан ҳимоялаш;
- мониторинг ва тармоқ захираларини бошқариш тизимларини енгиш;
- дастурий таъминотни никоблаш;
- интеллектуал эгаликнинг баъзи бир турларида муаллифлик ҳуқуқларини ҳимоялаш.

Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш

Бу компьютер стеганографиясини ишлатиш соҳаси конфиденциал ахборотларни ҳимоялаш муаммосини ечишда энг самарали ҳисобланади. Масалан, товушнинг энг кам аҳамиятли кичик разрядлари яшириладиган хабарга алмаштирилади. Бундай узгариш купчилик томонидан товушли хабарни эшитиш пайтида сезилмайди.

Саноат шпионлик тизимларининг мониторинг ва тармоқ захираларини бошқариш ҳаракатларига қарши йўналтирилган стенографик усуллар локал ва глобал компьютер тармоклари серверларидан ахборотнинг ўтишида назорат ўрнатиш харакатларига карши туришга имкон беради.

Компьютер стеганографиясининг хозирги вақтда ишлатиладиган бошка бир соҳаси дастурий таъминотни ниқоблашдир. Қачонки, дастурий таъминотни кайд қилинмаган фойдаланувчилар томонидан ишлатилиши ўринсиз бўлса, у стандарт универсал дастур маҳсулотлари (масалан, матнли мухаррирлар) остида ниқобланиши ёки мультимедиа файллари (масалан, компьютер ўйинларининг мусиқий иловаси)га яширилиши мумкин.

Стенографиядан фойдаланиладиган яна бир соҳалардан бири — бу муаллифлик ҳуқуқларини ҳимоялаш ҳисобланади. Компьютерли график тасвирларга махсус белги қуйилади ва у кузга кўринмай қатади. Лекин, махсус дастурий таъминот билан аниқланади. Бундай дастур маҳсулоти аллакачон баъзи журналларнинг компьютер версияларида ишлатилаяпти. Стенографиянинг ушбу йўналиши нафакат тасвирларни, балки аудио ва видеоахборотни ҳам қайта ишлашга мулжалланган. Бундан ташкари унинг интеллектуал эгалигини ҳимоялашни таъминлаш вазифаси ҳам мавжуд.

Ҳозирги вақтда компьютер стенографияси усуллари икки асосий йўналиш буйича ривожланмокда:

- компьютер форматларининг махсус хоссаларини ишлатишга асосланган усуллар;
- аудио ва визуал ахборотларнинг сероблилигига асосланган усуллар.

Стеганографик дастурлар тўгрисида кисқача маьлумот

Windows операцион муҳитида ишловчи дастурлар:

• Steganos for Win95 дастури ишлатишда жуда енгил бўлиб, айни пайтда файлларни шифрлаш ва уларни BMP, DIB, VOC, WAV, ASCII, HTML кен-гайтмали файллар ичига жойлаштириб яширишда жуда кудратли хисобланади;

• Contraband дастури 24-битли BMP форматдаги график файллар ичида ҳар қандай файлни яшира олиш имкониятига эга.

DOS мухитида ишловчи дастурлар:

• Jsteg дастури маълумотни JPG форматли файллар ичига яшириш учун мўлжалланган;

• FFEncode дастури маълумотларни матнли файллар ичида яшириш имкониятига эга;

• StegoDOS дастурлар пакетининг ахборотни тасвирда яшириш имконияти мавжуд;

• Winstorm дастурлар пакети PCX форматли файллар ичига хабарни шифрлаб яширади.

OS/2 операцион муҳитида ишловчи дастурлар:

- Texto дастури маълумотларни инглиз тилидаги матнга айлантиради;

- Hide4PGP v1.1 дастури BMP, WAV, VOC форматли файллар ичига маьлумотларни яшириш имкониятига эга.

Macintosh компьютерлари учун мўлжалланган дастурлар:

- Paranoid дастури маълумотларни шифрлаб, товушли форматли файл ичига яширади:

- Stego дастурининг PICT кенгайтмали файл ичига маълумотларни яшириш имконияти мавжуд.

Криптография ҳақида асосий тушунчалар

«Криптография» атамаси дастлаб «яшириш, ёзувни беркитиб қуймоқ» маъносини билдирган. Биринчи марта у ёзув пайдо булган даврлардаёк айтиб ўтилган. Ҳозирги вақтда криптография деганда ҳар қандай шаклдаги, яъни дискда сақланадиган сонлар кўринишида ёки ҳисоблаш тармоқларида узатиладиган хабарлар кўринишидаги ахборотни яшириш тушунилади. Криптографияни рақамлар билан кодланиши мумкин бўлган ҳар қандай ахборотга нисбатан қўллаш мумкин. Махфийликни таъминлашга

қаратилган криптография кенгроқ қўлланилиш доирасига эга. Аниқроқ айтганда, криптографияда қўлланиладиган усулларнинг ўзи ахборотни ҳимоялаш билан боғлиқ бўлган кўп жараёнларда ишлатилиши мумкин.

Криптография ахборотни рухсатсиз киришдан ҳимоялаб, унинг махфийлигини таъминлайди. Масалан, тулов варакларини электрон почта оркали узатишда унинг ўзгартирилиши ёки сохта ёзувларнинг қушилиши мумкин. Бундай ҳолларда ахборотнинг яхлитлигини таъминлаш зарурияти пайдо бўлади. Умуман олганда компьютер тармогига рухсатсиз киришнинг мутлақо олдини олиш мумкин эмас, лекин уларни аниқлаш мумкин. Ахборотнинг яхлитлигини текширишнинг бундай жараёни, кўп ҳолларда, ахборотнинг ҳақиқийлигини таъминлаш дейилади. Криптографияда қўл-ланиладиган усуллар кўп бўлмаган ўзгартиришлар билан ахборотларнинг ҳақикийлигини таъминлаши мумкин.

Нафақат ахборотнинг компьютер тармогидан маъноси бузилмасдан келганлигини билиш, балки унинг муаллифдан келганлигига ишонч хосил қилиш жуда муҳим. Ахборотни узатувчи шахсларнинг ҳақиқийлигини тасдикловчи турли усуллар маълум. Энг универсал процедура пароллар билан алмашувдир, лекин бу жуда самарали бўлмаган процедура. Чунки паролни қулига киритган ҳар қандай шахс ахборотдан фойдаланиши мумкин бўлади. Агар эҳтиёткорлик чораларига риоя қилинса, у ҳолда парольларнинг самарадорлигини ошириш ва уларни криптографик усуллар билан ҳимоялаш мумкин, лекин криптография бундан кучлироқ паролни узлуксиз ўзгартириш имконини берадиган процедураларни ҳам таъминлайди.

Криптография соҳасидаги охирги ютуклардан бири — рақамли сигнатура — махсус хосса билан ахборотни тўлдириш ёрдамида яхлитликни таъминловчи усул, бунда ахборот унинг муаллифи берган очиқ калит маълум бўлгандагина текширилиши мумкин. Ушбу усул махфий калит ёрдамида яхлитлик текшириладиган маълум усулларан кўпроқ афзалликларга эга.

Криптография усулларини куллашнинг баъзи бирларини кўриб чикамиз. Узаталадиган ахборотнинг маъносини яшириш учун икки хил ўзгартиришлар қўлланилади: **кодлаштириш** ва **шифрлаш**.

Кодлаштириш учун тез-тез ишлатиладиган иборалар тўпламини ўз ичига олувчи китоб ёки жадваллардан фойдаланилади. Бу иборалардан ҳар бирига, кўп ҳалларда, рақамлар тўплами билан бериладиган ихтиёрий танланган кодли суз тўғри келади. Ахборотни кодлаш учун худди шундай китоб ёки жадвал талаб қилинади. Кодлаштирувчи китоб ёки жадвал ихтиёрий криптографик ўзгартиришга мисол бўлади. Кодлаштиришнинг ахборот технологиясига мос талаблар — каторли маълумотларни сонли маълумотларга айлантириш ва аксинча ўзгартиришларни бажара билиш. Кодлаштириш китобини тезкор ҳамда ташқи хотира қурилмаларида амалга ошириш мумкин, лекин бундай тез ва ишончли криптографик тизимни муваффакиятли деб булмайди. Агар бу китобдан бирор марта рухсатсиз фойдаланилса, кодларнинг янги китобини яратиш ва уни хамма фойдаланувчиларга таркатиш зарурияти пайдо бўлади.

Криптографик ўзгартиришнинг иккинчи тури **шифрлаш** ўз ичига — бошланғич матн белгиларини англаб олиш мумкин бўлмаган шаклга ўзгартириш алторитмларини камраб олади. Узгартиришларнинг бу тури ахборот-коммуникациялар технологияларига мос келади. Бу ерда алгоритмни ҳимоялаш муҳим аҳамият касб этади. Криптографик калитни қўллаб, шифрлаш алгоритмининг ўзида ҳимоялашга бўлган талабларни камайтариш мумкин. Энди ҳимоялаш объекти сифатада фақат калит хизмат қилади. Агар калитдан нусха олинган бўлса, уни алмаштириш мумкин ва бу кодлаштирувчи китоб ёки жадвални алмаштиришдан енгилдир. Шунинг учун ҳам кодлаштириш эмас, балки шифрлаш ахборот-коммуникациялар технологияларида кенг кўламда қулланилмоқда.

Сирли (махфий) алоқалар соҳаси **криптология** деб айтилади. Ушбу сўз юнонча **«kripto»** — сирли ва **«logus»** — хабар маъносини билдирувчи сўзлардан иборат. Криптология икки йўналиш, яъни **криптография** ва **криптотаҳлил**дан иборат.

Криптографиянинг вазифаси хабарларнинг махфийлигини ва ҳақиқийлигини таъминлашдан иборат.

Криптотаҳлилнинг вазифаси эса криптографлар томонидан ишлаб чиқилган ҳимоя тизимини очишдан иборат.

Симметрияли криптотизим асослари.

Ҳозирги кунда **криптотизим**ни икки синфга ажратиш мумкин:

• симметрияли бир калитлилик (махфий калитли);

• асимметрияли икки калитлилик (очиқ калитли).

Симметрияли тизимларда куйидаги иккита муаммо мавжуд:

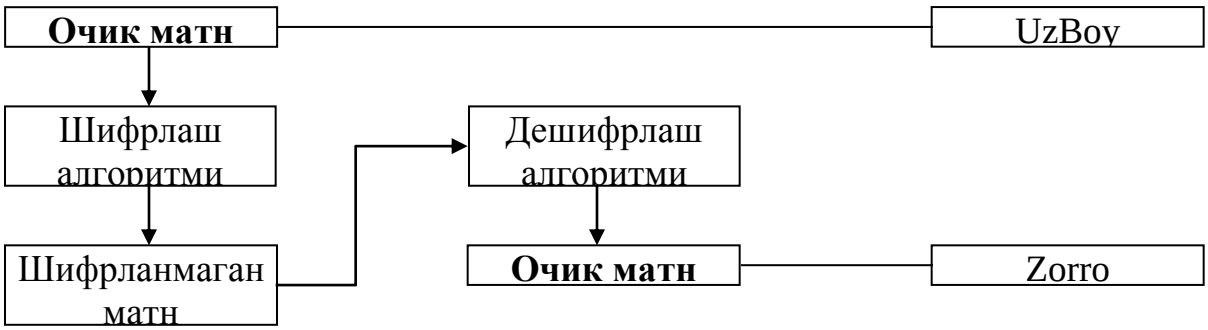
1) Ахборот алмашувида иштирок этувчилар кандай йўл билан махфий калитни бир-бирларига узатишлари мумкин?

2) Жўнатилган хабарнинг ҳақиқийлигини қандай аниқласа бўлади?

Ушбу муаммоларнинг ечими очиқ калитли тизимларда ўз аксини топди.

Очиқ калитли асимметрияли тизимда иккита калит кўлланилади. Биридан иккинчисини хисоблаш усуллари билан аниқлаб бўлмайди.

Биринчи калит ахборот жўнатувчи томонидан шифрлашда ишлатилса, иккинчиси ахборотни қабул килувчи томонидан ахборотни тиклашда қўлланилади ва у сир сақланиши лозим.



Ушбу усул билан ахборотнинг махфийлигини таъминлаш мумкин. Агар биринчи калит сирли бўлса, у ҳолда уни электрон имзо сифатида қуллаш мумкин ва бу усул билан ахборотни аутентификациялаш, яъни ахборотнинг яхлитлигини таъминлаш имкони пайдо булади.

Ахборотни аутентификациялашдан ташқари қуйидаги масалаларни ечиш мумкин:

• фойдаланувчини аутентификациялаш, яъни компьютер тизими захираларига кирмоқчи бўлган фойдаланувчини аниклаш:

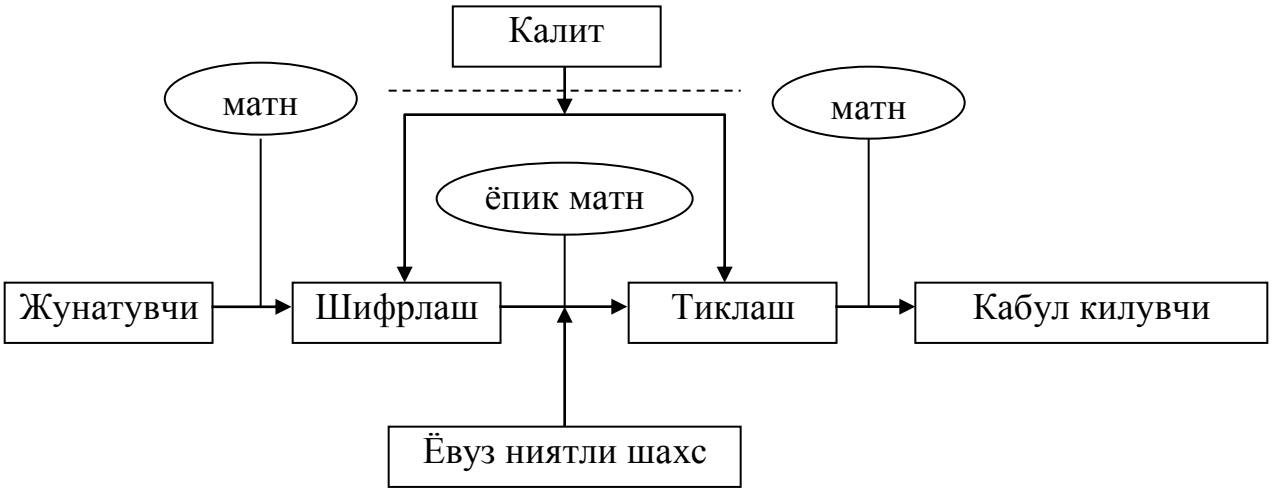
• тармок абонентлари алоқасини урнатиш жараёнида уларни ўзаро аутентнфикациялаш.

Ҳозирги кунда ҳимояланиши зарур бўлган йўналишлардан бири бу электрон тўлов тизимлари ва Internet ёрдамида амалга ошириладиган электрон савдолардир.

Криптография — маълумотларни ўзгартириш усулларининг туплами бўлиб, маълумотларни ҳимоялаш бўйича қуйидаги иккита асосий муаммоларни ҳал қилишга йуналтирилган: **махфийлик; яхлитлилик.**

Махфийлик орқали ёвуз ниятли шахслардан ахборотни яшириш тушунилса, яхлитлилик эса ёвуз ниятли шахслар томонидан ахборотни ўзгартира олмаслик ҳақида далолат беради.

Криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:



Бу ерла калит кандайдир химояланган канал оркали жунатилади (чизмада пунктир чизиклар билан тасвирланган). Умуман олганда, ушбу механизм симметрияли бир калитлик тизимига тааллуклидир.

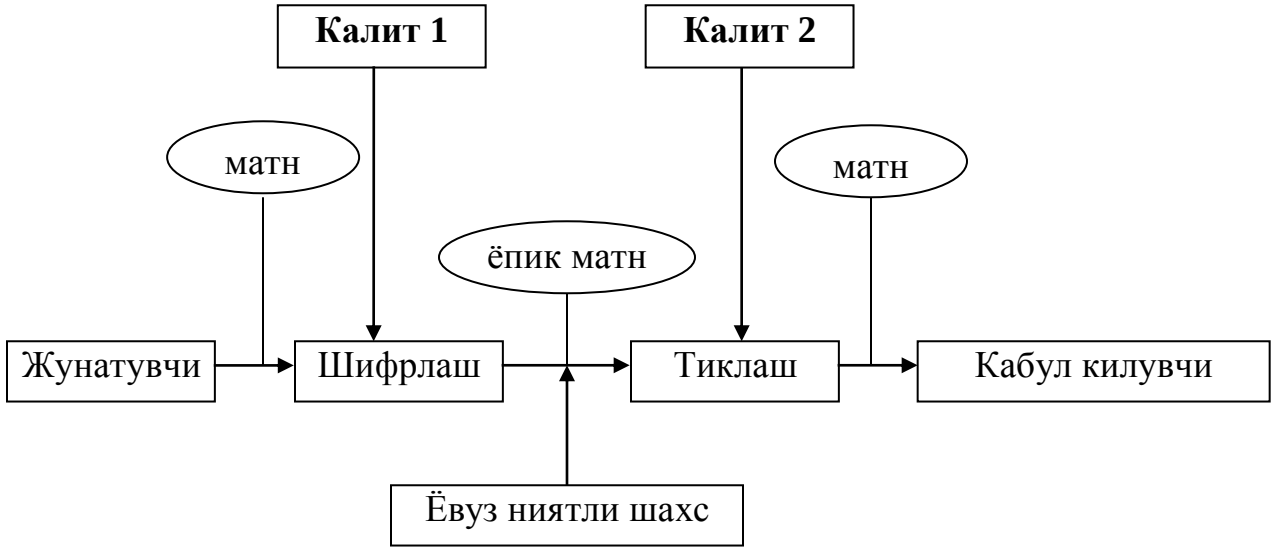
Ассимметрияли икки калитлик криптография тизимини схематик равишда куйидагича тасвирлаш мумкин:

Бу ҳолда ҳимояланган канал бўйича очиқ калит жўнатилиб, махфий калит жўнатилмайди.

Ёвуз ниятли шахслар уз мақсадларига эриша олмаса ва криптотахлилчилар калитни билмасдан туриб, шифрланган ахборотни тиклай олмаса, у ҳолда криптотизим **криптомустаҳкам тизим де**б айтилади.

Криптотизимнинг мустахкамлиги унинг калити билан аникланади ва бу криптотаҳлилнинг асосий қоидаларидан бири бўлиб хисобланади.

Ушбу таърифнинг асосий маъноси шундан иборатки, криптотизим барчаларга маълум тизим ҳисобланиб, унинг ўзгартирилиши кўп вакт ва маблағ талаб қилади, шу боис ҳам фақатгина калитни ўзгартириб туриш билан ахборотни химоялаш талаб қилинади.



Криптография нуктаи – назаридан шифр — бу калит демакдир ва очик маълумотлар тупламини ёпик (шифрланган) маълумотларга узгартириш криптография узгартиришлар алгоритмлари мажмуаси хисобланади.

Калит — криптография узгартиришлар алгоритмининг баъзи-бир параметрларининг махфий холати булиб, барча алгоритмлардан ягона вариантини танлайди. Калитларга нисбатан ишлатиладиган асосий курсаткич булиб **криптомустахкамлик** хисобланади.

Криптография химоясида шифрларга нисбатан куйидаги талаблар куйилади:

• етарли даражада криптомустахкамлик;

• шифрлаш ва кайтариш жараёнининг оддийлиги;

• ахборотларни шифрлаш окибатида улар хажмининг ортиб кетмаслиги;

• шифрлашдаги кичик хатоларга таьсирчан булмаслиги.

Ушбу талабларга куйидаги тизимлар жавоб беради:

• уринларини алмаштириш;

• алмаштириш;

• гаммалаштириш;

• аналитик узгартириш.

Уринларини алмаштириш шифрлаш усули буйича бошлангич матн белгиларининг матннинг маълум бир кисми доирасида махсус коидалар ёрдамида уринлари алмаштирилади.

Алмаштириш шифрлаш усули буйича бошлангич матн белгилари фойдаланилаётган ёки бошка бир алифбо белгиларига алмаштирилали.

Гаммалаштириш усули буйича бошлангич матн белгилари шифрлаш гаммаси белгилари, яъни тасодифий белгилар кетма-кетлиги билан бирлаштирилади.

Тахлилий узгартириш усули буйича бошлангич матн белгилари аналитик формулалар ёрдамида узгартирилади, масалан, векторни матрицага купайтириш ёрдамида. Бу ерда вектор матндаги белгилар кетма-кетлиги булса, матрица эса калит сифатида хизмат килади.

Уринларни алмаштириш усуллари

Ушбу усул энг оддии ва энг кадимий усулдир. Уринларни алмаштириш усулларига мисол сифатида куйидагиларни келтириш мумкин:

— шифрловчи жадвал;

— сехрли квадрат.

Шифрловчи жадвал усулида калит сифатида куйидагилар кулланилади:

— жадвал улчовлари;

— суз ёки сузлар кетма-кетлиги;

— жадвал таркиби хусусиятлари.

Мисол.

Куйидаги матн берилган булсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун буйича кетма – кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Натижада, 4х7 улчовли жадвал ташкил килинади.

Энди шифрланган матн каторлар буйича аникланади, яъни узимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал улчовлари хизмат килади.

Сехрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал буйича сонлар йигиндиси битга сонга тенг бўлган квадрат шаклидаги жадвалга айтилали.

Сехрли квадратга сонлар тартиби бўйича белгилар киритилади ва бу белгилар сатрлар бўйича ўқилганда матн ҳосил бўлади.

Мисол.

4х4 улчовли сехрли квадратни оламиз, бу ерда сонларнинг 880 та хар хил комбинацияси мавжуд. Куйидагича иш юритамиз:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Бошлангич матн сифатида куйидаги матнни оламиз:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар буйича укиш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАД

Алмаштириш усуллари

Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин:

- Цезар усули;
- Аффин тизимидаги Цезар усули;
- Таянч сўзли Цезар усули ва бошқалар.

Цезар усулида алмаштирувчи харфлар k ва силжиш билан аниқланади. Юлий Цезар бевосита k = 3 булганда ушбу усулдан фойлаланган.

k = 3 бўлганда ва алифбодаги ҳарфлар m = 26 та бўлганда қуйидаги жалвал ҳосил қилинади:

A → D	J → M	S → V
B → E	K → N	T → W
C → F	L → O	U → X
D → G	M → P	V → Y
E → H	N → Q	W → Z
F → I	O → R	X → A
G → J	P → S	Y → B
H → K	Q → T	Z → C
I → L	R → U	

Мисол.

Матн сифатида KOMPUTER сузини оладиган булсак, Цезар усули натижасида куйидаги шифрланган ёзув хосил булади: NRPSBXWHU.

Цезар усулининг камчилиги бу бир хил ҳарфларнинг ўз навбатида, бир хил ҳарфларга алмашишидир.

Аффин тизимидаги Цезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аникланади: at+b (mod m), бу ерда a, b - бутун сонлар, 0≤a, b<m, ЭКУБ (a,m)=1.

m=26, a=3, b=5 булганда куйидаги жадвал хосил килинади:

T	0	1	2	3	4	5
3t+5	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25
13	16	19	22	25	2

Шунга мос равишда харфлар куйидагича алмашади:

A	B	C	D	E	F	G	H
F	I	L	O	R	U	X	A

I	J	K	L	M	N	O	P
D	G	J	M	P	S	V	Y

Q	R	S	T	U	V	W	X
B	E	H	K	N	Q	T	W

Y	Z
Z	C

Натижада юкорида келтирилган матн куйидагича шифрланади:

JVPYZNKRE.

Хозирги вактда компьютер тармокларида тижорат ахборотлари билан алмашишда учта асосий алгоритмлар, яъни DES, CLIPPER ва PGP алгоритмлари кулланилмокда. DES ва CLIPPER алгоритмлари интеграл схемаларда амалга оширилади. DES алгоритмининг криптомустахкамлигини куйидаги ммсол оркали хам бахолаш мумкин: 10 млн. АКШ доллари харажат килинганда DES шифрлаш очиш учун 21 минут, 100 млн, АКШ доллари харажат килинганда эса 2 минут сарфланади. CLIPPER тизими SKIPJACK шифрлаш алгоритмини уз ичига олади ва бу алгоритм DES алгоритмидан 16 млн, марта кучлирокдир.

PGP алгоритми эса 1991 йилда Филипп Циммерман (АКШ) томонидан ёзилган ва электрон почта оркали кузатиладиган хабарларни шифрлаш учун ишлатиладиган PGP дастурлар пакети ёрдамида амалга оширилади, FGP дастурий воситалари Internet тармогида электрон почта оркали ахборот жунатувчи фойдаланувчилар томонидан шифрлаш максадида кенг фойдаланилмокда.

PGP (Pretty Good Privacy) криптография дастурининг алгоритми калитли, очик ва ёпик булади.

Очик калит куйидагича куринишни олиши мумкин:

Ушбу очик калит бевосита Web сахифаларда ёки электрон почта оркали очикчасига юборилиши мумкин. Очик калитдан фойдаланган жунатилган шифрли ахборотни ахборот юборилган манзил эгасидан бошка шахс укий олмайди. PGP оркали шифрланган ахборотларни очиш учун, суперкомпьютерлар ишлатилганда бир аср хам камлик килиши мумкин.

Булардан ташкари, ахборотларни тасвирларда ва товушларда яшириш дастурлари хам мавжуд. Масалан, S-toots дастури ахборотларни BMP, GIF, WAV кенгайтмали файлларда саклаш учун кулланилади.

Кундалик жараёнда фойдаланувчилар офис дастурлари ва архиваторларни куллаб келишади. Архиваторлар, масалан PkZip дастурида маълумотларни пароль ёрдамида шифрлаш мумкин. Ушбу файлларни очганда иккита, яъни лугатли ва тугридан-тугри усулдан фойдаланишади. Лугатли усулда бевосита махсус файлдан сузлар пароль урнига куйиб текширилади, тугридан-тугри усулда эса бевосита белгилар комбинацияси тузилиб, пароль урнига куйиб текишрилади.

Офис дастурлари (Word, Excel, Access) оркали химоялаш умуман таклиф этилмайди. Бу борада мавжуд дастурлар Internet да тусиксиз таркатилади.

Такрорлаш учун саволлар

1. Замонавий компьютер стенографияси истикболлари.

2. Компьютер стенографиясининг асосий вазифалари.

3. Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш учун андай йўналишлар мавжуд?

4.. *Криптографиянинг асосий тушунчаларини таърифлаб беринг.*

5. *Ахборотларни криптографияли ҳимоялаш тамойиллари.*

6. *Уринларни алмаштириш ва алмаштириш усуллари қандай криптотизиларга тегишли?*

5 – МАВЗУ: МАЪЛУМОТЛАРНИНГ ТАРКАЛИБ КЕТИШИ ВА МАЪЛУМОТЛАРГА РУХСАТСИЗ КИРИШ

1. ***Ахборот тизимларнинг таъсирчан кисмлари;***
2. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.

Ахборот тизимларнинг таъсирчан кисмлари

Хозирги вактларда мавжуд ахборот тизимларида жуда катта хажмда махфий ахборотлар сакланади ва уларни химоялаш энг долзарб муаммолардан хисобланади.

Масалан, биргина АКШ мудофза вазирлигида айни чогда 10000 компьютер тармоклари ва 1,5 млн компьютерларга карашли ахборотларнинг аксарият кисми махфий эканлиги хаммага аён. Бу компьютерларга 1999 йили 22144 марта турлича хужумлар уюштирилган, уларнинг 600 тасида Пентагон тизимларининг вактинчалик ишдан чикишига олиб келган, 200 тасида эса махфий булмаган маълумотлар базаларига рухсатсиз кирилган ва натижада Пентагон 25 миллиард АКШ доллари микдорида иктисодий зарар курган. Бунака хужумлар 2000 йили 25000 марта амалга оширилган. Уларга карши курашиш учун Пентагон томонидан янги технологиялар яратишга 2002 йили Carnegie Mellon университетига 35,5 млн. АКШ доллари микдорида грант ажратилган.

Маълумотларга караганда, хар йили АКШ хукумати компьютерларига уртача хисобда 250—300 минг хужум уюштирилади ва улардан **65 %** и муваффакиятли амалга оширилади.

Замонавий автоматлаштирилган ахборот тизимлари — бу тараккиёт дастурий-техник мажмуасидир ва улар ахборот алмашувини талаб этадиган масалаларни ечишни таъминлайди. Кейинги йилларда фойдаланувчиларнинг ишини енгиллаштириш максадида янгиликларни таркатиш хизмати USENET-NNTP, мультимедиа маълумотларини INTERNET-HTTP тармоги оркати узатиш каби протоколлар кенг таркалди.

Бу протоколлар бир канча ижобий имкониятлари билан бирга анчагина камчиликларга хам эга ва бу камчиликлар тизимнинг захираларига рухсатсиз киришга йул куйиб бермокда.

Ахборот тизимларининг асосий таъсирчан кисмлари куйидагилар:

• INTERNET тармогидаги серверлар. Бу серверлар: дастурлар ёки маълумотлар файлларини йук, килиш оркали, серверларни хаддан ташкари куп тугалланмаган жараёнлар билан юклаш оркали: тизим журналининг кескин тулдириб юборилиши оркали; броузер — дастурларини ишламай колишига олиб келувчи файлларни нусхалаш оркали ишдан чикарилади;

• маълумотларни узатиш каналлари — бирор-бир порт оркали ахборот олиш максадида яширин канални ташкил этувчи дастурлар юборилади;

• маълумотларни тезкор узатиш каналлари — бу каналлар жуда куп микдорда хеч кимга керак булмаган файллар билан юкланади ва уларнинг маълумот узатиш тезлиги сусайиб кетади;

• янгиликларни узатиш каналлари — бу каналлар эскирган ахборот билан тулдириб ташланади ёки бу каналлар умуман йук килиб ташланади;

• ахборотларни узатиш йули — USENET тармогида янгиликлар пакетининг маршрути бузилади;

• JAVA броузерлари — SUN фирмаси яратган JAVA тили имкониятларидан фойдаланиб, апплетлар (applets) ташкил этиш оркали маълумотларга рухсатсиз кириш мумкин булади. JAVA — апплетлари тармокда автоматик равишда ишга тушиб кетади ва бунинг натижасида фойдаланувчи бирор-бир хужжатни ишлатаётгаи пайтда хакикатда нима содир этилишини хеч качон кура билмайди, масалан, тармок вирусларини ташкил этиш на JAVA-апплетлари оркали вирусларни жунатиш мумкин булади ёки фойдаланувчининг кредит карталари ракамларига эгалик килиш имконияти вужудга келади.

АКШ саноат шпионажига карши кураш ассоциациясининг текширишларига асосан компьютер тармоклари ва ахборот тизимларига хужумлар куйидагича таснифланади: 20% — аралаш хужумлар; 40% — ички хужумлар ва 40% — ташки хужумлар.

Жуда куп холларда бунака хужумлар муваффакиятли ташкил этилади. Масалан, Буюк Британия саноати, компьютер жиноятлари сабабли, хар йили 1 млрд фунт стерлинг зарар куради.

Демак, юкорида олиб борилган тахлилдан шу нарса куринадики, хозирги пайтда компьютер тармоклари жуда куп таъсирчан кисмларга эга булиб, улар оркали ахборотларга рухсатсиз киришлар амалга оширилмокда ёки маълумотлар базалари йук килиб юборилмокда ва бунинг натижасида инсоният млрд-млрд АКШ доллари микдорида иктисодий зарар курмокда.

Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари

Маълумки, хисоблаш техникаси воситалари иши электромагнит нурланиши оркали бажарилади, бу эса, уз навбатида, маълумотларни таркатиш учун зарур булган сигналларнинг захирасидир. Бундай кисмларга компьютерларнинг платалари, электрон таъминот манбалари, принтерлар, плоттерлар, алока аппаратлари ва х.к. киради. Лекин, статистик маълумотлардан асосий юкори частотали электромагнит нурланиш манбаи сифатида дисплейнинг рол уйнаши маълум булди. Бу дисплейларда электрон нурли трубкалар урнатилган булади. Дисплей экранида тасвир худди телевизордагидек ташкил этилади. Бу эса видеосигналларга эгалик килиш ва уз навбатида, ахборотларга эгалик килиш имкониятини яратади. Дисплей экранидаги курсатув нусхаси телевизорда хосил булади.

Юкорида келтирилган компьютер кисмларидан бошка ахборотларга эгалик килиш максадида тармок кабеллари хамда серверлардан хам фойдаланилмокда.

Компьютер тизимлари захираларига рухсатсиз кириш сифатида мазкур тизим маьлумотларидан фойдаланиш, уларни узгартириш ва учириб ташлаш харакатлари тушунилади.

Агар компьютер тизимлари рухсатсиз киришдан химояланиш механизмларига эга булса, у холда рухсатсиз кириш харакатлари куйидагича ташкил этилади:

- химоялаш механизмини олиб ташлаш ёки куринишини узгартириш:
- тизимга бирор-бир фойдаланувчининг номи ва пароли билан кириш.

Агар биринчи холда дастурнинг узгартирилиши ёки тизим суровларининг узтартирилиши талаб этилса, иккинчи холда эса мавжуд фойдаланувчининг паролини клавиатура оркали киритаётган пайтда куриб олиш ва ундан фойдаланиш оркали рухсатсиз кириш амалга оширилади.

Маълумотларга рухсатсиз эгалик килиш учун зарур булган дастурларни татбик этиш усуллари куйидагилардир:

• компьютер тизимлари захираларига рухсатсиз эгалик килиш;

• компьютер тармоги алока каналларидаги хабар алмашуви жараёнига рухсатсиз аралашув;

• вирус куринишидаги дастурий камчиликлар (дефектлар)ни киритиш.

Купинча компьютер тизимида мавжуд заиф кисмларни «тешик»лар, «люк»лар деб аташади. Баьзан дастурчиларнинг узи дастур тузиш пайтида бу «тушик»ларни колдиришади, масалан:

— натижавий дастурий махсулотни енгил йигиш максадида;

— дастур тайёр булгандан кейин яширинча дастурга кириш воситасига эга булиш максадида.

Мавжуд «тешик»ка зарурий буйруклар куйилади ва бу буруклар керакли пайтда уз ишини бажариб боради. Вирус куринишидаги дастурлар эса маълумотларни йукотиш ёки кисман узгартириш, иш сеансларини бузиш учун ишлатилади.

Юкорида келтирилганлардан хулоса килиб, маълумотларга рухсатсиз эгалик килиш учун дастурий мосламалар энг кучли ва самарали инструмент булиб, компьютер

ахборот захираларига катта хавф тугдириши ва буларга карши кураш энг долзарб муаммолардан бири эканлигини таъкидлаш мумкин.

Такрорлаш учун саволлар

1. Протоколлар ижобий имкониятлари билан бирга кандай камчиликларга хам эга?
2. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.
3. Маълумотларга рухсатсиз эгалик килиш учун зарур булган дастурларни татбик этиш усулларини айтиб утинг.

6 – МАВЗУ: КОМПЮТЕР ТАРМОҚЛАРИДА ЗАМОНАВИЙ ҲИМОЯЛАШ УСУЛЛАРИ ВА ВОСИТАЛАРИ

1. Компьютер тормокларининг заиф кисмлари.
2.Тармок химоясини ташкил килиш асослари.
3. ***Компьютер телефониясидаги химоялаш усуллари.***
4. Компьютер тармокларида химояни таъминлаш усуллари.
5. ЭХМ химоясини таъминлашнинг техник воситалари.
6. Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари.

Компьютер тормокларининг заиф кисмлари.

Хозирги вактда локал хисоблаш тармокари (LAN) ва глобал хисоблаш тармоклари (WAN) орасидаги фарклар йуколиб бормокда. Масалан, Netware 4x ёки Vines 4.11. операцион тизимлари LANнинг фаолиятини худудий даражасига чикармокда. Бу эса, яъни LAN имкониятларининг ортиши, маълумотларни химоялаш усулларини янада такомиллаштиришни талаб килмокда.

Химоялаш воситаларини ташкил этишда куйидагиларни эътиборга олиш лозим:

• тизим билан алокада булган субъектлар сонининг куплиги, купгина холларда эса баъзи бир фойдаланувчиларнинг назоратда булмаслиги;

• фойдаланувчига зарур булган маълумотларнинг тармокда мавжудлиги:

• тармокларда турли фирмалар ишлаб чикарган шахсий компьютерларнинг ишлатилиши;

• тармок тизимида турли дастурларнинг ишлатиш имконияти;

• тармок элементлари турли мамлакатларда жойлашганлиги сабабли, бу давлатларга тортилган алока кабелларининг узунлиги ва уларни тулик, назорат килишнинг карийб мумкин эмаслиги;

• ахборот захираларидан бир вактнинг узида бир канча фойдаланувчиларнинг фойдаланиши;

• тармокка бир канча тизимларнинг кушилиши;

• тармокнинг енгилгина кенгайиши, яъни тизим чегарасининг ноаниклиги ва унда ишловчиларнинг ким эканлигининг номаълумлиги;

• хужум нукталарининг куплиги;

• тизимга киришни назорат килишнинг кийинлиги.

Тармокни химоялаш зарурлиги куйидаги холлардан келиб чикади:

• бошка фойдаланувчилар массивларини укиш;

• компьютер хотирасида колиб кетган маълумотларни укиш;

• химоя чораларини айланиб утиб, маълумот ташувчиларни нусхалаш;

• фойдаланувчи сифатида яширинча ишлаш;

• дастурий тутгичларни ишлатиш;

• дастурлаш тилларининг камчиликларидан фойлаланиш;
• химоя воситаларини билиб туриб ишдан чикариш;
• компьютер вирусларини киритиш ва ишлатиш.

Тармок, мухофазасини ташкил этишда куйидагиларни эътиборга олиш лозим:

- мухофаза тизимининг назорати;
- файлларга киришнинг назорати;
- тармокда маълумот узатишнинг назорати;
- ахборот захираларига киришнинг назорати;
- тармок билан уланган бошка тармокларга маълумот таркалишининг назорати.

Тармок химоясини ташкил килиш асослари

Махфий ахборотни кайта ишлаш учун керакли текширувдан утган компьютерларни ишлатиш лозим булади. Мухофаза воситаларининг функционал тулик булиши мухим хисобланади. Бунда тизим администраторининг иши ва олиб бораётган назорат катта ахамиятта эгадир. Масалан, фойдаланувчиларнинг тез-тез паролларни алмаштириб туришлари ва паролларнинг жуда узунлиги уларни аниклашни кийинлаштиради. Шунинг учун хам янги фойдаланувчини кайд этишни чеклаш (масалан, факат иш вактида ёки факат ишлаётган корхонасида) мухимдир. Фойдаланувчининг хакикийлигини текшириш учун тескари алока килиб туриш лозим (масалан, модем ёрдамида). Ахборот захираларига кириш хукукини чегаралаш механизмини ишлатиш ва унинг таъсирини LAN объектларига тулалигича утказиш мумкин.

Тармок, элементлари уртасида утказилаётган маълумотларни мухофаза этиш учун куйидаги чораларни куриш керак:

• маълумотларни аниклаб олишга йул куймаслик;
• ахборот алмашишни тахлил килишга йул куймаслик;
• хабарларни узгартиришга йул куймаслик;
• яширинча уланишга йул куймаслик ва бу холларни тезда аниклаш.

Маълумотларни тармокда узатиш пайтида криптографик химоялаш усулларидан фойдаланилади, Кайд этиш журналига рухсат этилмаган киришлар амалга оширилганлиги хакида маълумотлар ёзилиб турилиши керак. Бу журналга киришни чегаралаш хам химоя воситалари ёрдамида амалга оширилиши лозим.

Компьютер тармогида назоратни олиб бориш мураккаблигининг асосий сабаби — дастурий таъминот устидан назорат олиб боришнинг мураккаблигидир. Бундан ташкари компьютер вирусларининг куплиги хам тармокда назоратни олиб боришни кийинлаштиради.

Хозирги вакттача мухофазалаш дастурий таъминоти хилма-хил булса хам, операцион тизимлар зарурий мухофазанинг керакли даражасини таъминламас эди. Netware 4.1, Windows NT операцион тизимлари етарли даражада мухофазани таъминлай олиши мумкин.

Компьютер телефониясидаги химоялаш усуллари

Электрон коммуникацияларнинг замонавий технологиялари кейинги пайтларда ишбилармонларга алока каналлари буйича ахборотнинг турлича куринишлари (масалан: факс, видео, компьютерли, нуткли ахборотлар)ни узатишда купгина имкониятлар яратиб бермокда.

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

Бор-йуги ун йил илгари сотувга CANON фирмасининг нархи 6000 АКШ доллари булган «Navigator» номли махсулоти чикарилган эди ва у биринчи тизимлардан хисобланади.

Компьютер тслефонияси ун йил ичида жуда тез суръатлар билан ривожланди. Хозирги пайтда сотувда мавжуд булган «PC Phone» (Export Industries Ltd, Israel) махсулотининг нархи бор-йуги 1000 Германия маркаси туради. «Powertine-II» (Talking Technology, USA)нинг нархи эса 800 АКШ доллари туради. Кейинги пайтларда компьютер телефонияси йуналишида 70% аппарат воситаларини Dialogue (USA) фирмаси ишлаб чикармокда.

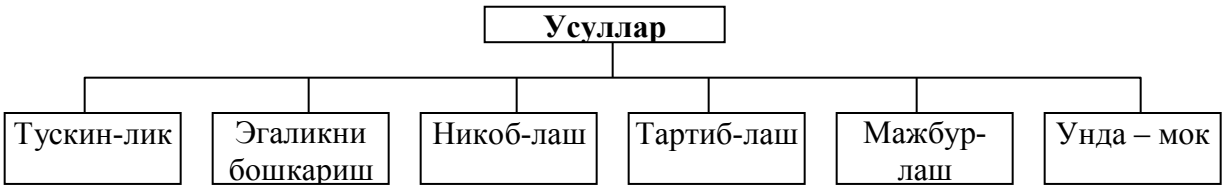
Компьютер телефониясида ахборотларнинг хавфсизлигини таъминлаш катта ахамиятга эга. Масалан, телефон хакерларининг Скотланд-Ярд АТСига кириб 1,5 млн, АКШ доллари микдорида зарар келтиришганлиги хавфсизликнинг зарурлигини исботлайди.

Компьютер телефониясида кулланилаётган нуткини аникловчи технология телефон килувчининг овозидан таниб олиш учун ахамиятга эгадир. Компьютер телефониясининг химоясини етарли даражада таъминлаш учун Pretty Good Privacy Inc. фирмасининг PC Phone 1.0 дастурий пакет ишлаб чикарилган. У компьютер телефонияси оркали узатилаётган ахборотларни химоялаш учун ахборотларни ракамли куринишга утказади ва кабул пайтида эса дастурий-техник воситалар ёрдамида кайта ишлайди. Замонавий компьютер телефонияси воситатарининг шифрлаш тезлига хам жуда юкоридир, хато килиш эхтимоли эса жуда кичикдир (тахминан $10^{-8} – 10^{-12}$).

Компьютер тармокларида химояни таъминлаш усуллари

Компьютер тармокларида ахборотни химоялаш деб фойдаланувчиларни рухсатсиз тармок, элементлари ва захираларига эгалик килишни ман этишдаги техник, дастурий ва криптографик усул ва воситалар, хамда ташкилий тадбирларга айтилади.

Бевосита телекоммуникация каналларида ахборот хавфсизлигини таъминлаш усул ва воситаларини куйидагича таснифлаш мумкин:



Юкорида келтирилган усулларни куйидагича таърифлаш кабул килинган.

Тускинлик аппаратларга, маьлумот ташувчиларга ва бошкаларга киришга физикавий усуллар билан **каршилик курсатиш** деб айтилади.

Эгаликни бошкариш — тизим захиралари билан ишлашни тартибга солиш усулидир. Ушбу усул куйидаги функциялардан иборат:

• тизимнинг хар бир объектини, элементини ндентификациялаш, масалан, фойдаланувчиларни;

• идентификация буйича объектни ёки субъектни хакикий, асл эканлигини аниклаш;

• ваколатларни текшириш, яъни танланган иш тартиби буйича (регламент) хафга кунини, кунлик соатни, талаб килинадиган захираларни куллаш мумкинлигини текшириш;

• кабул килинган регламент буйича ишлаш шароитларини яратиш ва ишлашга рухсат бериш;

• химояланган захираларга килинган мурожаатларни кайд килиш;

• рухсатсиз харакатларга жавоб бериш, масалан, сигнал бериш, учириб куйиш суровномани бажаришдан воз кечиш ва бошкалар.

Никоблаш – маълумотларни укиб олишни кийинлаштириш максадида уларни криптография оркали кодлаш.

Тартиблаш — маълумотлар билан ишлашда шундай шарт-шароитлар яратиладики, рухсатсиз тизимга кириб олиш эхтимоли камайтирилади.

Мажбурлаш – кабул килинган коидаларга асосан маълумотларни кайта ишлаш, акс холда фойдаланувчилар моддий, маънурий ва жиноий жазоланадилар.

Ундамок — ахлокий ва одобий коидаларга биноан кабул килинган тартибларни бажаришга йуналтирилган.

Юкорида келтирилган усулларни амалга оширишда куйидагича таснифланган воситаларни тадбик этишади.

Расмий воситалар — шахсларни иштирокисиз ахборотларни химоялаш функцияларини бажарадиган воситалардир.

Норасмий воситилар — бевосита шахсларни фаолияти ёки унинг фаолиятини аниклаб берувчи регламентлардир.

Техникавнй воситалар сифатида электр, электромеханик ва электрон курилмалар тушунилади. Техникавий воситалар уз навбатида, физикавий ва аппаратли булиши мумкин.

Аппарат-техник воситалари деб телекоммуникация курилмаларига киритилган ёки у билан интерфейс оркали уланган курилмаларга айтилади. Масалан, маълумотларни назорат килишнинг жуфтлик чизмаси, яъни жунатиладиган маълумот йулда бузиб талкин этилишини аниклашда кулланиладиган назорат булиб, автоматик равишда иш сонининг жуфтлигини (назорат разряди билан биргаликда) текширади.

Физикавий техник воситалар — бу автоном холда ишлайдиган курилма ва тизимлардир. Масалан, оддий эшик кулфлари, деразада урнатилган темир панжаралар, куриклаш электр ускуналари физикавий техник воситаларга киради.

Дастурий воситалар – бу ахборотларни химоялаш функцияларини бажариш учун мулжалланган махсус дастурий таъминотдир. Ахборотларни химоялашда биринчи навбатда энг кенг кулланилган дастурий воситалар хозирги кунда иккинчи даражали химоя воситаси хисобланади. Бунга мисол сифатида пароль тизимини келтириш мумкин.

Ташкилий химоялаш воситалари — бу талекоммуникация ускуналарининг яратилиши ва кулланиши жараёнида кабул килинган ташкилий-техникавий ва ташкилий-хукукий тадбирлардир. Бунга бевосита мисол сифатида куйидаги жараёнларни келтириш мумкин: биноларнинг курилиши, тизимни лойихалаш, курилмаларни урнатиш, текшириш ва ишга тушириш.

Ахлокий ва одобий химоялаш воситалари — бу хисоблаш техникасини ривожланиши окибатида пайдо буладиган тартиб ва келишувлардир. Ушбу тартиблар конун даражасида булмасада, уни тан олмаслик фойдаланувчиларни обрусига зиён етказиши мумкин.

Конуний химоялаш воситалари — бу давлат томонидан ишлаб чикилган хукукий хужжатлар саналади. Улар бсвосита ахборотлардан фойдаланиш, кайта ишлаш ва узатишни тартиблаштиради ва ушбу коидаларни бузувчиларнинг масъулиятларини аниклаб беради.

Масалан, Узбекистон Республикаси Марказий банки томонидан ишлаб чикилган коидаларида ахборотни химоялаш гурузларини ташкил килиш, уларнинг ваколатлари, мажбуриятлари ва жавобгарликлари аник ёритиб берилган.

Хавфсизликни таъминлаш усуллари ва воситаларининг ривожланишини уч боскичга ажратиш мумкин: 1) дастурий воситаларни ривожлантириш; 2) барча йуналишлар буйича ривожланиши; 3) ушбу боскичда куйидаги йуналишлар буйича ривожланишлар кузатилмокда:

- химоялаш функцияларини аппаратли амалга ошириш;
- бир неча химоялаш функцияларини камраб олган воситаларни яратиш;
- алгоритм ва техникавий воситаларни умумлаштириш ва стандартлаш.

Бевосита тармок буйича узатиладиган маълумотларни химоялаш максадида куйидаги тадбирларни бажариш лозим булади:

- узатиладиган маълумотларни очиб укишдан сакланиш;
- узатиладиган маълумотларни тахтил килищдан сакланиш;
- узатиладиган маълумотларни узгартиришга йул куймаслик ва узгартиришга уринишларни аниклаш;

- маълумотларни узатиш максадида кулланиладиган дастурий узилишларни аниклашга йул куймаслик;

- фирибгар уланишларнинг олдини олиш.

Ушбу тадбирларни амалга оширишда асосан криптографик усуллар кулланилади.

ЭХМ химоясини таъминлашнинг техник воситалари

Компьютер оркали содир этидадиган жиноятлар окибатида факатгина АКШ хар йили 100 млрд. доллар зарар куради. Уртача хар бир жиноятда 430 минг доллар угирланади ва жиноятчини кидириб топиш эхтимоли 0,004% ни ташкил этади.

Мутахассисларнинг фикрича ушбу жиноятларни 80%и бевосита корхонада ишлайдиган ходимлар томонидан амалга оширилади.

Содир этиладиган жиноятларнинг тахлили куйидаги хулосаларни беради:

• купгина хисоблаш тармокларида фойдаланувчи исталган ишчи уриндан тармокда уланиб фаолият курсатиши мумкин. Натижада жиноятчи бажарган ишларни кайси компьютердан амалга оширилганини аниклаш кийин булади.

• угирлаш натижасида хеч нима йуколмайди, шу боис купинча жиноий иш юритилмайди;

• маълумотларга нисбатан мулкчилик хусусияти йуклиги;

• маълумотларни кайта ишлаш жараёнида йул куйилган хатолик уз вактида кузатилмайди ва тузатилмайди, натижада келгусида содир буладиган хатоларнинг олдини олиб булмайди;

• содир этиладиган компьютер жиноятлари уз вактида эълон килинмайди, бунинг сабаби хисоблаш тармокларида камчиликлар мавжудлигини бошка ходимлардан яшириш хисобланади.

Ушбу камчиликларни бартараф килишда ва компьютер жиноятларини камайтиришда куйидаги чора-тадбирларни утказиш керак булади:

• персонал масьулиятини ошириш:

• ишга кабул килинадиган ходимларни текширувдан утказиш;

• мухим вазифани бажарувчи ходимларни алмаштириб туриш;

• пароль ва фойдаланувчиларни кайд килишни яхши йулга куйиш;

• маълумотларга эгалик киилишни чеклаш;

• маълумотларни шифрлаш.

Ахборот-коммуникациялар технологияларининг ривожланиши окибатида купгина ахборотни химоялаш инструментал воситалари ишлаб чикилган. Улар дастурий, дастурий-техник ва техник воситалардир.

Хозирги кунда тармок хавфсизлигини таъминлаш максадида ишлаб чикилган техникавий воситаларни куйидагича таснифлаш мумкин:

Физикавий химоялаш воситалари — махсус электрон курилмалар ёрдамида маълумотларга эгалик килишни такиклаш воситаларидир.

Мантикий химоялаш — дастурий воситалар билан маълумотларга эгалик килишни такиклаш учун кулланилади.

Тармокларараро экранлар ва шлюзлар — тизимга келадиган хамда ундан чикадиган маълумотларни маълум хужумлар билан текшириб боради ва протоколлаштиради.

Хавфсизликни аудитлаш тизимлари — жорий этилган операцион тизимдан урнатилган параметрларни заифлигини кидиришда кулланиладиган тизимдир.

Реал вактда ишлайдиган хавфсизлик тизими — доимий равишда тармокнинг хавфсизлигини тахлиллаш ва аудитлашни таъминлайди.

Стохастик тестларни ташкиллаштириш воситалари — ахборот тизимларининг сифати ва ишончлилигини текширишда кулланиладиган воситадир.

Аник йуналтирилган тестлар — ахборот-коммуникациялар технологияларининг сифати ва ишончлилигини текширишда кулланилади.

Хавфларни имитация килиш — ахборот тизимларига нисбатан хавфлар яратилади ва химоянинг самарадорлиги аникланади.

Статистик тахлилгичлар — дастурларнинг тузилиш таркибидаги камчиликларни аниклаш, дастурлар кодида аникланмаган кириш ва чикиш нукталарини топиш, дастурдаги узгарувчиларни тугри аникланганлигини ва кузда тутилмаган ишларни бажарувчи кисм дастурларини аниклашда фойдаланилади.

Динамик тахлилгичлар — бажариладиган дастурларни кузатиб бориш ва тизимда содир буладиган узгаришларни аниклашда кулланилади.

Тармокнинг заифлигини аниклаш — тармок захираларига сунъий хужумларни ташкил килиш билан мавжуд заифликларни аниклашда кулланилади.

Мисол сифитида куйидаги воситаларни келтириш мумкин:

• Dallas Lock for Administrator — мавжуд электрон Proximity ускунаси асосида яратилган дастурий-техник восита булиб, бевосита маълумотларга рухсатсиз киришни назорат килишда кулланилади;

• Security Administrator Tool for ANALYZING Networks (SATAN) — дастурий таъминот булиб, бевосита тармокнинг заиф томонларини аниклайди ва уларни бартараф этиш йулларини курсатиб беради. Ушбу йуналиш буйича бир неча дастурлар ишлаб чикилган, масалан: Internet Security Scanner, Net Scanner, Internet Scanner ва бошкалар.

• NBS тизими — дастурий-техник восита булиб, алока каналларидаги маълумотларни химоялашда кулланилади;

• Free Space Communication System — тармокда маълумотларнинг хар хил нурлар оркали, масалан лазерли нурлар оркали алмашувини таъминлайди;

• SDS тизими — ушбу дастурий тизим маълумотларини назорат килади ва кайдномада акс эттиради. Асосий вазифаси маълумотларни узатиш воситаларига рухсатсиз киришни назорат килишдир;

• Timekey — дастурий-техник ускунадир, бевосита ЭХМнинг параллел портига урнатилади ва дастурларни белгиланган вактда кенг куллалилишини такиклайди;

• IDX — дастурий-техник восита, фойдаланувчининг бармок, изларини «укиб олиш» ва уни тахлил килувчи техникалардан иборат булиб, юкори сифатли ахборот хавфсизлигини таъминлайди. Бармок изларини укиб олиш ва хотирада саклаш учун 1 минутгача, уни таккослаш учун эса 6 секундгача вакт талаб килинади.

Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари

Ахборотларни химоялашнинг мавжуд усул ва воситалари хамда компьютер тармоклари каналларидаги алоканинг хавфсизлигини таъминлаш технологияси эволюциясини солиштириш шуни курсатмокдаки, бу технология ривожланишининг биринчи боскичида дастурий воситалар афзал топилди ва ривожланишга эга булди, иккинчи боскичида химоянинг хамма асосий усуллари ва воситалари интенсив ривожланиши билан характерланди, учинчи боскичида эса куйидаги тенденциялар равшан булмокда:

- ахборотларни химоялаш асосий функцияларининг техник жихатдан амалга оширилиши;

- бир нечта хавфсизлик функцияларини бажарувчи химоялашнинг биргаликдаги воситаларини яратиш:

- алгоритм ва техник воситаларни унификация килиш ва стандартлаштириш.

Компьютер тармокларида хавфсизликни таьминлашда хужумлар юкори даражада малакага эга булган мутахассислар томонидан амалга оширилишини доим эсда тутиш лозим. Бунда уларнинг харакат моделларидан доимо устун турувчи моделлар яратиш талаб этилади. Бундан ташкари, автоматлаштирилган ахборот тизимларида персонал энг таъсирчан кисмлардан биридир. Шунинг учун, ёвуз ниятли шахсга ахборот тизими персоналидан фойдалана олмаслик чора-тадбирларини утказиб туриш хам катта ахамиятга эга.

Такрорлаш учун саволлар

1. Компьютер тормокларининг заиф кисмлари нимадан иборат?
2.Тармок химоясини ташкил килишда нималарга эътибор бериш зарур?
3. ***Компьютер телефониясида андай хавсизлик муаммолари мавжуд?***
4. Компьютер тармокларида химояни таъминлаш усуллари.
5. ЭХМ химоясини таъминлашнинг техник воситалари.
6. Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишлари.

7 – МАВЗУ: INTERNETДА АХБОРОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ АСОСЛАРИ

1. Internetda рухсатсиз кириш усулларининг таснифи;
2. ***Рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши;***
3. Тармокларaро экран ва унинг вазифалари;
4. Тармокларaро экраннинг асосий компонентлари.

Internetda рухсатсиз кириш усулларининг таснифи

Глобал тармокларнинг ривожланиши ва ахборотларни олиш, кайта ишлаш ва узатишнинг янги технологиялари пайдо булиши билан Internet тармогига хар хил шахс ва ташкилотларнинг эътибори каратилди. Куплаб ташкилотлар уз локал тармокларини глобал тармокларга улашга карор килишган ва хозирги пайтда WWW, FTP, Gophes ва бошка серверлардан фойдаланишмокда. Тижорат максадида ишлатилувчи ёки давлат сири булган ахборотларнинг глобал тармоклар буйича жойларга узатиш имкони пайдо булди ва уз навбатида, шу ахборотларни химоялаш тизимида малакали мутахассисларга эхтиёж тугилмокда.

Глобал тармоклардан фойдаланиш бу факатгина «кизикарли» ахборотларни излаш эмас, балки тижорат максадида ва бошка ахамиятга молик ишларни бажаришдан иборат. Бундай фаолият вактида ахборотларни химоялаш воситаларининг йуклиги туфайли куплаб талофотларга дуч келиш мумкин.

Хар кандай ташкилот Intenetга уланганидан сунг, хосил буладиган куйидаги муаммоларни хал этишлари шарт:

• ташкилотнинг компьютер тизимини хакерлар томонидан бузилиши:

• Internet оркали жунатилган маълумотларнинг ёвуз ниятли шахслар томонидан укиб олиниши;

• ташкилот фаолиятига зарар етказилиши.

Internet лойихалаш даврида бевосита химояланган тармок сифатида ишлаб чикилмаган. Бу сохада хозирги кунда мавжуд булган куйидаги муаммоларни келтириш мумкин:

• маълумотларни енгиллик билан кулга киритиш;
• тармокдаги компьютерлар манзилини сохталаштириш;
• TCP/IP воситаларининг заифлиги;
• купчилик сайтларнинг нотугри конфигурацияланиши;
• конфигурациялашнинг мураккаблиги.

Глобал тармокларнинг чегарасиз кенг ривожланиши ундан фойдаланувчилар сонининг ошиб боришига сабаб булмокда, бу эса уз навбатида ахборотлар хавфсизлигига тахдид солиш эхтимолининг ошишига олиб келмокда. Узок, масофалар билан ахборот алмашиш зарурияти ахборотларни олишнинг катъий чегараланишини талаб этади. Шу

максадда тармокларнинг сегментларини хар хил даражадаги химоялаш усуллари таклиф этилган:

• эркин кириш (масалан: WWW-сервер);

• чегараланган киришлар сегменти (узок масофада жойлашган иш жойига хизматчиларнинг кириши);

• ихтиёрий киришларни ман этиш (масалан, ташкилотларнинг молиявий локал тармоклари).

Интернет глобал ахборот тармоги узида нихоятда катта хажмга эга булган ахборот ресурсларидан миллий иктисоднинг турли тармокларида самарали фойданишга имконият тугдиришига карамасдан ахборотларга булган хавфсизлик даражасини оширмокда. Шунинг учун хам Интернетга уланган хар бир корхона узининг ахборот хавфсизлигини таъминлаш масалаларига катта эътибор бериши керак.

Локал тармокларнинг глобал тармокарга кушилиши учун тармоклар химояси администратори куйидаги масалаларни хал килиши лозим:

— локал тармокларга глобал тармок, томонидан мавжуд хавфларга нисбатан химоянинг яратилиши;

— глобал тармок фондаланувчиси учун ахборотларни яшириш имкониятининг яратилиши;

Бунда куйидаги усуллар мавжуд:

— кириш мумкин булмаган тармок манзили оркали;

— Ping дастури ёрдамида тармок пакетларини тулдириш;

— рухсат этилган тармок манзили билан такикланган тармок манзили буйича бирлаштириш;

— таъкикланган тармок протаколи буйича бирлаштириш;

— тармок буйича фойдаланувчига парол танлаш;

— REDIREST туридаги ICMP пакети ёрдамида маршрутлар жадвалини модификациялаш;

— RIP стандарт булмаган пакети ёрдамида маршрутлар жадвалини узгартириш;

— DNS spoofingдан фойдаланган холда уланиш.

Рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши

Ушбу хавф глобал тармокларнинг бир канча сохаларини камраб олади, жумладан:

• локал соха;

• локал-глобал тармокларнинг бирлашуви;

• мухим ахборотларни глобал тармокларда жунатиш;

• глобал тармокнинг бошкарилмайдиган кисми.

Ихтиёрий ахборот тармокларининг асосий компонентлари бу серверлар ва ишчи станциялар хисобланади. Серверда ахборотлар ёки хисоблаш ресурслари ва ишчи станцияларда хизматчилар ишлайди. Умуман ихтиёрий компьютер хам, сервер хам ишчи станция булиши мумкин — бу холда уларга нисбатан хавфли хужумлар булиши эхтимоли бор.

Серверларнинг асосий вазифаси ахборотларни саклаш ва такдим килишдан иборат.

Ёвуз ниятли шахсларни куйидагича таснифлаш мумкин:

• ахборот олишга имконият олиш;

• хизматларга рухсат этилмаган имконият олиш;

• маълум синфдаги хизматларнинг иш режимини ишдан чикаришга уриниш;

• ахборотларни узгартиришга харакат ёки бошка турдаги хужумлар.

Уз навбатида, хозирги замонавий ривожланиш давомида сервис хизматини издан чикаришга карши кураш муаммоси мухим ахамият касб этади. Бу хилдаги хужумлар «сервисдаги бузилиш» номини олган.

Ишчи станцияларга хужумнинг асосий максади, асосан, кайта ишланаётган маълумотларни ёки локал сакланаётган ахборотларни олишдир. Бундай хужумларнинт асосий воситаси «Троян» дастурлар саналади. Бу дастур уз тузилиши буйича компьютер

вирусларидан фарк килмайди ва компьютерга тушиши билан узини билинтирмасдан туради. Бошкача айтганда, бу дастурнинг асосий максади — тармок, станциясидаги химоя тизимини ички томондан бузишдан иборат.

Бу холатда масалани хал килиш маълум кийинчиликка олиб келади, яъни махсус тайёрланган мутахассис лозим ёки бошка чоралар кабул килиш керак булади. Бошка бир оддий химоя усулларидан бири хар кайси ишчи станциядаги тизимли файллар ва хизмат сохасидаги маълумотларнинг узгаришини текшириб турувчи ревизор (инглз. ***advizer***— кирувчи) урнатиш саналади.

Тармоклараро экран ва унинг вазифалари

Тармоклараро экран — химоялаш воситаси булиб, ишончли тармок, ва ишончсиз тармок орасида маълумотларга киришни бошкаришда кулланилади.

Тармоклараро экран куп компонентли булиб, у Internetдан ташкилотнинг ахборот захираларини химоялаш стратегияси саналади. Яъни ташкилот тармоги ва Internet орасида куриклаш вазифасини бажаради.

Тармоклараро экраннинг асосий функцияси — маълумотларга эгалик килишни марказлаштирилган бошкарувини таъминлашдан иборат.

Тармоклараро экран куйидаги химояларни амалга оширади:

• уринсиз трафиклар, яъни тармокда узатиладиган хабарлар окимини такиклаш;

• кабул килинган трафикни ички тизимларга йуналтириш;

• ички тизимнинг заиф кисмларини яшириш билан Internet томонидан уюштириладиган хужумлардан химоялаш;

• барча трафикларни баёнлаштириш;

• ички маълумотларни, масалан тармок топологиясини, тизим номларини, тармок ускуналарини ва фойдаланувчиларнинг идентификаторларини Internetдан яшириш;

• ишончли аутентификацияни таьминлаш.

Купгина адабиётларда **тармоклараро экран** тушунчаси **брандмауэр** ёки **Fire Wall** деб юритилган. Умуман буларнинг хаммаси ягона тушунчадир.

Тармоклараро экран — бу тизим, умумий тармокни икки кисмга ажратиб, тармоклараро химоя вазифасини утайди ва маълумотлар пакетининг чегарадан утиш шартларини амалга оширадиган коидалар туплами хисобланади.

Одатда тармоклараро экран ички тармокларни глобал тармоклардан, яъни Internetдан химоя килади. Шуни айтиш керакки, тармоклараро экран нафакат Internetдан, балки корпоратив тармоклардан хам химоя килиш кобилиятига эгадир. Хар кандай тармоклараро экран ички тармокларни тулик химоя кила олади деб булмайди.

Хар кандай ташкилотнинг **тармок хавсизлиги сиёсати** икки кисмдан иборат булади: тармок сервисларидан фойдаланиш; тармоклараро экранни куллаш.

Тармок сервисларидан фойдаланиш сиёсатига мос равишда Internetда сервислар руйхати аникланади. Бу сервисларга фойдаланувчилар чекланган кириш билан таъминланади.

Кириш усулларининг чекланилиши — фойдаланувчилар томонидан Internet сервисларига чет йуллар оркали рухсатсиз киришни такиклаш маъносини билдиради.

Тармок сервисларига кириш сиёсати, одатда, куйидаги принципларга мойил булади:

- Internetдан ички тармокка киришни такиклаш, лекин ички тармокдан Inlernetга киришга рухсат бериш;

- ваколатланган тизимларга Internetдан ички тармокка чекланилган киришга рухсат бериш.

Тармоклараро экранларга куйиладиган вазифавий талаблар куйидагилардан иборат.

• тармок даражасида фильтрлашга талаб;

• амалий даражада фильтрлашга талаб;

• администрациялаш ва фильтрлаш коидаларини урнатиш буйича талаб;

• тармокли аутентификациялаш воситаларига талаб;
• ишларни кайд килиш ва хисобни олиб бориш буйича талаб.

Тармоклараро экраннинг асосий компонентлари

Тармоклараро экранларнинг компонентлари сифатида куйидагиларни келтириш мумкин: фильтрловчи -йулловчи; тармок, даражасидаги шлюзлар; амалий даражадаги шлюзлар.

Фильтрловчи-йулловчи — йулловчи, яъни компьютер тармогида маълумотларни манзилга етказувчи дастурлар пакети ёки сервердаги дастур булиб, у кирадиган ва чикадиган пакетларни фильтрлайди. Пакетларни фильтрлаш, яъни уларни аник тупламга тегишлилигини текшириш, TCP/IP сарлавхасидаги маълумотлар буйича амалга оширилади.

Фильтрлашни аник хост-компьютер, яъни тармокдаги файл ва компьютер захираларига киришни амалга оширувчи компьютер ёки порт, яъни хабарларни жунатиш ёки кабул килиш максадида мижоз ва сервер томонидан ишлатиладиган ва одатда 16 битли сон билан номланадиган дастур билан уланишда амалга ошириш мумкин. Масалан, фойдаланувчига кераксиз ёки ишончсиз хост-компьютер ва тармоклар билан уланишда такиклаш.

Фильтрлаш коидаларини ифодалаш кийин жараён булиб, уларни тестлаш воситалари мавжуд эмас.

Биринчи коида буйича, Internetдан келадиган TCP пакети жунатувчининг порти 1023 дан катта булса, 123.4.5.6 манзилли кабул килувчига 23-портга утказилади (23-порт TELNET сервери билан богланган).

Иккинчи коида хам худди шундай булиб, факатгина 25-порт SMTP билан богланган.

Тармок даражасидаги шлюзлар ишончли мижозлардан аник хизматларга суровномасини кабул килади ва ушбу алоканинг конунийлигини текширгандан сунг уларни ташки хост-компьютер билан улайди. Шундан сунг шлюз иккала томонга хам пакетларни филътрламай жунатади.

Бундан ташкари, тармок даражасида шлюзлар бевосига **сервер-даллол** вазифасини бажаради. Яъни, ички тармокдан келадиган IP манзиллар узгартирилиб, ташкирига факатгина битта IP манзил узатилади. Натижада, ички тармокдан ташки тармок билан тугридан-тугри богламайди ва шу йул билан ички тармокни химоялаш вазифасини утайди.

Амалий даражадаги шлюзлар фильтрловчи-йулловчиларга мансуб булган камчиликларни бартараф этиш максадида ишлаб чикилган. Ушбу дастурий восита **ваколатланган сервер,** деб номланади ва у бажарилаётган хост-компьютер эса амалий даражадаги шлюз деб аталади.

Амалий даражадаги шлюзлар мижоз ва ташки хост-компьютер билан тугридан-тугри алока урнатишга йул куймайди. Шлюз келадиган ва жунатиладиган пакетларни амалий даражада фильтрлайди. Сервер-даллоллар шлюз оркали аник сервер томонидан ишлаб чикилган маълумотларни кайтадан йуналтиради.

Амалий даражадаги шлюзлар нафакат пакетларни фильтрлаш, балки сервернинг барча ишларини кайд килиш ва тармок администраторини нохуш ишлардан хабар килиш имкониятига хам эга.

Амалий даражадаги шлюзларнинг афзалликлари куйидагилардан иборат:
• глобал тармок томонидан ички тармок таркиби куринмайди;
• ишончли аутентификация ва кайд килиш;
• фильтрлаш коидаларининг енгиллиги;
• куп тамойилли назоратларни амалга ошириш мумкинлиги.

Фильтрловчи-йулловчиларга нисбатан амалий даражадаги шлюзларнинг камчиликлари куйидагилардан иборат самарадорлигининг пастлиги; нархининг киммат булиши.

Амалий даражадаги шлюзлар сифатида куйидагиларни мисол килиб келтириш мумкин:

• Border Ware Fire Wall Server — жунатувчининг ва кабул килувчининг манзилларини, вактини ва фойдаланилган протоколларни кайд килади;

• Black Hole — сервернинг барча ишларини кайд килади ва тармок администраторига кутилаётган бузилиш хакида хабар жунатади.

Булардан ташкари куйидаги шлюзлар хам кулланилади:

Gauntlet Internel FirewaU, Alta Visla FireWali, ANS Interlock ва бошкалар.

Такрорлаш учун саволлар

1. Хар кандай ташкилот Intenetга уланганидан сунг андай муаммоларни хал этиши шарт?

2. Рухсат этилган манзилларнинг рухсат этилмаган вактда уланишни тушунтириб беринг.

3. Қайси хавф глобал тармокларнинг бир канча сохаларини камраб олади?

4. Тармокларараро экран ва унинг вазифалари

5. Тармокларараро экраннинг асосий компонентлари

8 – МАВЗУ: ЭЛЕКТРОН ПОЧТАДА АХБОРОТЛАРГА НИСБАТАН МАВЖУД ХАВФ-ХАТАРЛАР ВА УЛАРДАН ХИМОЯЛАНИШ АСОСЛАРИ

1. Электрон почтадан фойдаланиш.

2. Электрон почтада мавжуд хавфлар.

3. Электрон почтани химоялаш.

Электрон почтадан фойдаланиш

Электрон почта ёки E-mail хозирги кунда Internetдан фойдаланиш жараёнининг энг машхур касми хисобланади. E-mail оркали дунё буйича исталган жойга бир зумнинг узида хат юбориш ёки кабул килиш хамда ёзилган хатларни факатгина бир кишига эмас, балки манзиллар руйхати буйича жунатиш имконияти мавжуд. E-mail оркали мунозаралар утказиш имконияти мавжуд ва бу йуналишда USENET сервери кул келади.

Купгина корхоналар уз фаолиятида бевосита E-mail тизимидан фойдаланишади. Демак, корхона ва ташкилотлар рахбарлари маълум бир чора-тадбирлар оркали уз ходимларини E-mail билан ишлаш, ундан окилона фойдаланишга ургатиши лозим. Ушбу жараённинг асосий максади мухим хужжатлар билан ишлашни тугри йулга куйиш хисобланади.

Бу ерда куйидаги йуналишлар буйича таклифларни эътиборга олиш зарур:

• E-mail тизимидан ташкилот фаолияти максадларида фойдаланиш;

• шахсий максадда фойдаланиш;

• махфий ахборотларни саклаш ва уларга кириш:

• электрон хатларни саклаш ва уларни бошкариш.

Internetда асосий почта протоколларига куйидагилар киради:

• SMTP (Simple Mail Transfer Protocol);

• POP (Post Office Protocol);

• IMAP (Internet Mail Access Protocol);

• MIME (Multi purpose Internet Mail Extensions).

Булар билан бирма-бир танишиб чикамиз:

SMTP — ушбу протокол асосида сервер бошка тизимлардан хатларни кабул килади ва уларни фойдаланувчининг почта кутисида саклайди. Почта серверига интерактив кириш хукукига эга булган фойдаланувчилар уз компьютерларидан бевосита

хатларни укий оладилар. Бошка тизимдаги фойдаланувчилар эса уз хатларини POP-3 ва IMAP протоколлари оркали укиб олишлари мумкин;

POP — энг кенг таркалган протокол булиб, сервердаги хатларни, бошка серверлардан кабул килинган булса-да, бевосита фойдаланувчи томонидан укиб олинишига имконият яратади. Фойдаланувчилар барча хатларни ёки хозиргача укилмаган хатларни куриши мумкин. Хозирги кунда POP нинг 3-версияси ишлаб чикилган булиб ва аутентификациялаш усуллари билан бойитилган;

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

Ушбу протокол куйидаги имкониятларга эга: почта кутиларини яратиш, учириш ва номини узгартириш; янги хатларнинг келиши; хатларни тезкор учириш; хатларни кидириш; хатларни танлаб олиш.

IMAP саёхатда булган фойдаланувчилар учун POPга нисбатан кулай булиб хисобланади;

MIME — Internet почтасининг куп максадли кенгайтмаси сузлари кискартмаси булиб, у хатларнинг форматини аниклаш имконини беради, яъни:

- матнларни хар хил кодлаштиришда жунатиш;
- хар хил форматдаги номатн ахборотларни жунатиш;
- хабарнинг бир неча кисмдан иборат булиши;
- хат сарлавхасида хар хил кодлаштиришдаги маълумотни жойлаштириш.

Ушбу протокол ракамли электрон имзо ва маълумотларни шифрлаш воситаларидан иборат булиб, бундан ташкари унинг ёрдамида почта оркали бажарилувчи файлларни хам жунатиш мумкин. Натижада, файллар билан бирга вирусларни хам таркатиш имконияти тугилади.

Электрон почта билан ишлаш жараёнида куйидаги хатоларга йул куйиш мумкин: хатни тасодифан жунатиш; хатнинг нотугри манзил буйича жунатилиши; хатлар архивининг кескин ошиб кетиши окибатида тизимнинг ишдан чикиши; янгиликларга нотугри обуна булиш; хатни таркатиш руйхатида хатога йул куйиш.

Агар ташкилотнинг почта тизими бевосита Internetга уланган булса, йул куйилган хатолар окибати кескин ошиб кетади.

Ушбу хатоларнинг олдини олиш усулларининг баъзи бирлари куйидагилар:

- фойдаланувчиларни укитиш;
- электрон почта дастурларини тугри конфигурациялаш;
- Internetдаги протоколларга тулик амал килувчи дастурларни куллаш.

Бундан ташкари электрон почтанинг шахсий максадда ишлатилиши ташкилот рахбарияти учун баъзи бир муаммоларни келтириб чикариши мумкин, чунки E-mail манзилида ташкилот номлари акс эттирилган булиши эхтимолдан холи эмас. Натижада, шахс жунатаётган хат ташкилот номидан деб кабул килиниши мумкин. Шу боис, телефонлар каби E-mailдан шахсий ишлар учун фойдаланишни чеклаб куйиш зарур булади. Албатта, буни жорий килиш кийин масала.

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

- SMTP сервер — дастурларининг нокоррект урнатилиши туфайли бу серверлардан рухсатсиз фойдаланилмокда ва бу технология «спама» технологияси номи билан маълум;

- электрон почта хабарларига рухсатсиз эгалик килиш учун оддийгина ва самарали усуллардан фойдаланилмокда, яъни куйи катламларда винчестердаги маълумотларни укиш, почта ресурсларига кириш паролини укиб олиш ва хоказолар.

Электрон почтада мавжуд хавфлар

Электрон почта хизмати ва хамма протоколларнинг амалий жихатдан ахборотларга нисбатан химоясининг тулик булмаганлиги муаммоси бор. Бу муаммолар келиб чикишининг асосий сабаби Internetнинг UNIX операцион тизим билан борликлигида.

TCP/IP (Transtnission Control Protokol/lnternet Protocol) Internetнинг глобал тармогида коммуникацияни таъминлайди ва тармокларда оммавий равишда кулланилади, лекин улар хам химояни етарлича таъминлай олмайди, чунки TCP/IP пакетининг бошида хакер хужуми учун кулай маълумот курсатилади.

Internetда электрон почтани жунатишни оддий протокол почта транспорт хизмати амалга оширади (SMTP - Simple Mail Transfer Protocol). Бу протоколда мавжуд булган химоялашнинг мухим муаммоларидан бири - фойдаланувчи жунатувчининг маизилини кура олмаслигидир. Бундан фойдаланиб хакер катта микдорда почта хабарларини жунатиши мумкин, бу эса ишчи почта серверни хаддан ташкари банд булишига олиб келади.

Internetда оммавий тус олган дастур бу Sendmail электрон почтасидир. Sendmail томонидан жунатилган хабарлар боскинчи хакер ахборот шаклида фойдаланиши мумкин.

Тармок номлари хизмати (Domain Name System — DNS) фойдаланувчилар номи ва хост-компьютерини - манзилини курсатади. DNS компаниянинг тармок тузилиши хакида маълумотларни саклайди. DNSнинг муаммоларидан бири шундаки, бундаги маълумотлар базасини муаллифлаштирилмаган фойлаланувчилардан яшириш анча кийин. Бунинг натижасида, хакерлар DNS ни купинча хост-компьютерларнинг ишончли номлари хакида маълумотлар манбасидан фойдаланиш учун ишлатиши мумкин.

Узок, терминаллар эмуляцияси химати узок, тизимларни бир-бирига улаш учун хизмат килади. Бу сервердан фойдаланувчилар TELNET серверидан руйхатдан утиш ва уз номи ва паролини олиши лозим. TELNET серверига уланган хакер дастурни шундай урнатиши мумкинки, бунинг натижасида у фойдаланувчининг номи ва паролини ёзиб олиш имконига эга булади.

World Wide Web — WWW бу тизим Internet ёки интратармоклардаги хар хил серверлар ичидаги маълумотларни куриш учун хизмат килади. WWW нинг асосий хоссаларидан бири — Тармокларо экран оркали аник протокол ва манзилларни фильтрлаш зарурлигини тармокнинг химоялаш сиёсати карори билан хал этилишидир.

Электрон почта билан ишлаш жараёнида куйидаги хавфлар мавжуд:

1. Жунатувчининг калбаки манзили. Кабул килинган хатни E-mail манзили аниклигига тулик ишонч хосил килиш кийин, чунки хат жунатувчи уз манзилини калбакилаштириши мумкин.

2. Хатни кулга киритиш. Электрон хат ва унинг сарлавхаси узгартирилмасдан, шифрланмасдан жунатилади. Шу боис, уни йулда кулга киритиш ва мазмунини узгартириши мумкин.

3. Почта «бомба»си. Почга тизимига куплаб электрон хатлар жунатилади, натижада тизим ишдан чикади. Почта серверининг ишдан чикиш холатлари куйидагилардир:

• диск тулиб колади ва кейинги хатлар кабул килинмайди. Агар диск тизимли булса, у холда тизим тамомила ишдан чикиши мумкин;

• киришдаги навбатда турган хатлар сонининг ошиб кетиши натижасида кейинги хатлар умуман навбатга куйилмайди;

• олинадиган хатларнинг максимал сонини узгартириш натижасида кейинги хатлар кабул килинмайди ёки учирилади;

• фойдаланувчига ажратилган дискнинг тулдирилиши натижасида кейинги хатлар кабул килинмайди ва дискни тозалаб булмайди.

4. «Куркинчли» (нохуш) хат. Internet оркали олинадиган электрон хатларнинг умуман номаълум шахслар томонидан жунатилиши ва бу хатда фойдаланувчиларнинг шахсиятига тегувчи сузлар булиши мумкин.

Электрон почтани химоялаш

Юкорида келтирилган хавфларга нисбатан куйидаги химояланиш усуллари ишлаб чикилган:

- калбаки манзилдан химояланиш, бу холда шифрланган электрон имзоларни куллаш таклиф килинади;

- хатни кулга киритишдан химояланиш, бу холда хабарни ёки жунатиш каналини шифрлаш таклиф килинади.

Ушбу химоялаш усуллари бевосита колган хавфларнинг улушини камайтиради.

Такрорлаш учун саволлар

1. Электрон почтадан фойдаланиш хусусиятларини кўрсатинг.

2. E-mail адресларидан фойдаланишда қандай ахборот хавфсизлиги муаммолари мавжуд.

3. Электрон почтада мавжуд хавфлар.

4. Электрон почтага рухсатсиз киришнинг қандай усуллари мавжуд.

5. Электрон почтани химоялаш усуллари ҳаида гапириб беринг.

9 – МАВЗУ: ЭЛЕКТРОН ТУЛОВЛАР ТИЗИМИДА АХБОРОТЛАРНИ ХИМОЯЛАШ

1. ***Электрон туловлар тизими асослари;***
2. ***Идентификацияловчн шахсий номерни химоялаш;***
3. ***Банкоматлар хавфсизлигини таъминлаш;***
4. ***Internetда мавжуд электрон туловлар хавфсизлигини таъминлаш;***

Электрон туловлар тизими асослари

Электрон туловлар тизими деб банк пластик карталарини тулов воситаси сифатада кулланилишидаги усуллар ва уларни амалга оширувчи субъектлар мажмуасига айтилади.

Пластик карта — шахсий тулов воситаси булиб, у мазкур воситадан фойдаланадиган шахсга товар ва хизматларни накдсиз пулини тулаш, бундан ташкари банк муассасалари ва банкоматлардан накд пулни олишга имкон беради.

Пластик картани тулов воситаси сифатида кабул килувчилар, савдо ва хизмат курсатувчи корхоналар, банк булимлари хамда бошкалар шу пластик карталарга хизмат курсатувчи кабул килувчилар тармогини ташкил этади.

Электрон туловлар тизимини яратищда пластик карталарга хизмат курсатиш конун-коидаларини ишлаб чикиш ва уларга риоя килиш асосий масалалардан бири булиб хисобланади. Ушбу коидалар нафакат техникавий (маълумотларни стандартлаш, ускуналар ва бошкалар), балки молиявий масалалар (корхоналар билан хисобларни бажариш тартиби)ни хам камраб олади.

Электрон туловлар тизимининг фаолиятини куйидагидек тасаввур килиш мумкин:

Электрон туловлар тизими билан биргаликда фаолият курсатадиган банк икки, яъни **банк-эмитент ва банк-эквайер** тоифасида хизмат курсатади:

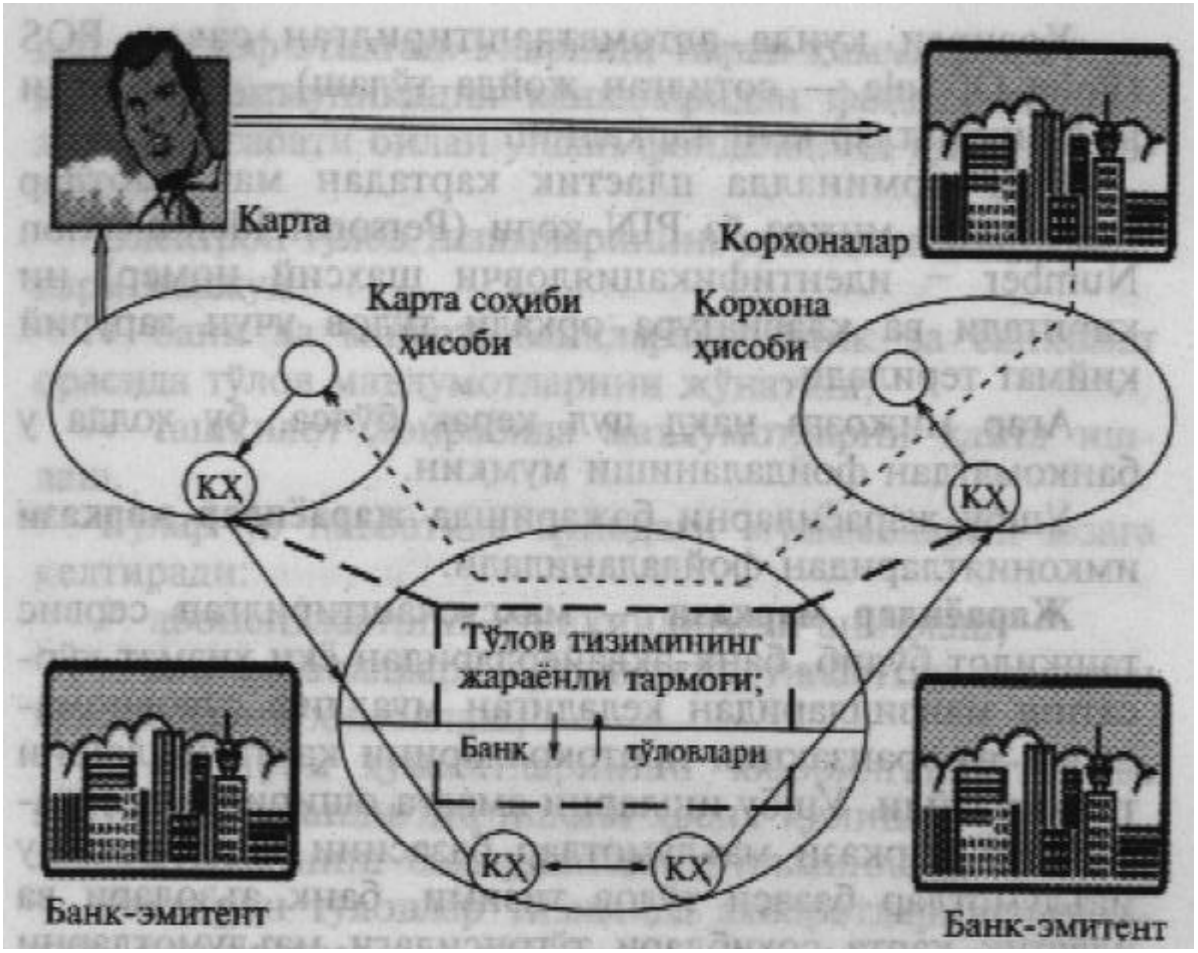
Банк-эмитент пластик карталарни ишлаб чикаради ва уларнинг тулов воситаси сифатида кулланилишига кафолат беради.

Банк-эквайер савдо ва хизмат курсатувчи ташкилотлар томонидан кабул килинган туловларни банк булимлари ёки банкоматлар оркали амалга оширади.

Хозирги кунда автоматлаштирилган савдо POS (Point-Of-Sale — сотилган жойда тулаш)— терминали ва банкоматлар кенг таркалган.

PQS-терминалда пластик картадан маълумотлар укилади ва мижоз уз PIN-коди (Personal Identification Number • идентификацияловчи шахсий номер)ни киритади ва клавиатура оркали тулов учун зарурий киймат терилади.

Агар мижозга накд пул керак булса, бу холда у банкоматдан фойдаланиши мумкин.



Ушбу жараёнларни бажаришда **жараёнлар маркази** имкониятларидан фойдаланилади.

Жараёнлар маркази – махсуслаштирилган сервис ташкилот булиб, банк-эквайерларидан ёки хизмат курсатиш манзилларидан келадиган муаллиф суровномаларни ва транзакция протоколларини кайта ишлашни таъминлайди. Ушбу ишларни амалга ошириш учун жараёнлар маркази маълумотлар базасини киритади. Бу маълумотлар базаси тулов тизими, банк аъзолари ва пластик карта сохиблари тугрисидаги маълумотларни уз таркибига олади.

Пластик карталар тулов буйича **кредитли ёки дебетли** булиши мумкин.

Кредитли карталар буйича карта сохибига купинча мухлати 25 кунгача булган вакганча карз берилади. Буларга Visa, Master Card, American Express карталари мисол була олади.

Дебетли карталарда карта сохибининг банк-эмитентидаги хисобига олдиндан маълум микдорда маблаг жойлаштиради. Ушбу маблагдан харид учун ишлатилган маблаглар суммаси ошиб кетмаслиги лозим.

Ушбу карталар факатгина шахсий эмас, балки корпоратив хам булиши мумкин.

Хозирги кунда **микропроцессорли карталар** ишлаб чикилмокда. Ушбу карталарнинг олдингиларидан асосий фарки бу мижознинг барча маълумотлари унда акс эттирилган булиб, барча **транзакциялар,** яъни маълумотлар базасини бир холатдан иккинчи холатга утказувчи суровномалар, off-line режимда амалга оширилади, шу боис, улар юкори даражада химояланган деб эътироф этилган. Уларнинг нархи кимматрок булса-да, телекоммуникация каналларидан фойдаланилмаслик муносабати билан ундан фойдаланиш киймати арзондир.

Электрон тулов тизимларининг куйидаги заиф кисмлари мавжуд:

• банк ва мижоз, банклараро, банк ва банкомат орасида тулов маълумотларини жунатиш;

• ташкилот доирасида маълумотларни кайта ишлаш.

Булар уз навбатида куйидаги муаммоларни юзага келтиради:

• абонентларнинг хакикийлигини аниклаш;

• алока каналлари оркали жунатилаётган электрон хужжатларни химоялаш;

• электрон хужжатларининг юборилганлигига ва кабул килинганлигига ишонч хосил килиш;

• хужжатнинг бажарилишини таъминлаш.

Электрон туловлар тизимида ахборотларни химоялаш функцияларини таъминлаш максадида куйидагилар амалга оширилиши керак:

- тизимнинг четки бугинларига киришни бошкариш;
- ахборотларнинг яхлитлигини назорат килиш;
- хабарларнинг махфийлигини таъминлаш;
- абонентларни узаро аутентификациялаш;
- хабарнинг муаллифлигидан воз кеча олмаслик;
- хабарнинг етказилганлигини кафолатлаш;
- хабар буйича бажариладиган чора-тадбирлардан воз кеча олмаслик;
- хабарлар кетма-кетлигини кайд килиш;
- кетма-кет хабарлар яхлитлигини таъминлаш.

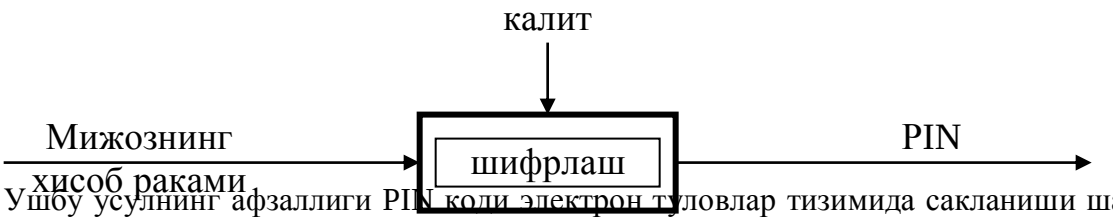
Идентификацияловчн шахсий номерни химоялаш

PIN-кодларини химоялаш тулов тизими хавфсизлигини таъминлашда асосий омилдир. Шу боис у факатгина карта сохибига маълум булиб, электрон туловлар тизимида сакланмайди ва бу тизим буйича юборилмайди.

Умуман олганда, PIN банк томонидан берилиши ёки мижоз томонидан танланиши мумкин. Банк томонидан бериладиган PIN куйидаги икки вариантдан бири буйича амалга оширилади:

1) мижоз хисоб раками буйича криптография усули билан ташкиллаштирилади;

Ушбу жараённи куйидагича тасвирлаш мумкин:



Ушбу усулнинг афзаллиги PIN коди электрон туловлар тизимида сакланиши шарт эмаслигидадир, камчилиги эса ушбу мижоз учун бошка PIN берилиши лозим булса, унга бошка хисоб раками очилиши зарурлигида, чунки банк буйича битта калит кулланилади.

2) банк ихтиёрий PIN кодни таклиф килади ва уни узида шифрлаб саклайди. PIN кодни хотирада саклаш кийинлиги ушбу усулнинг асосий камчилиги булиб хисобланади.

Мижоз томонидан танланиладиган PIN код куйидаги имкониятларга эга:

• барча максадлар учун ягона PIN кодни куллаш;

• харфлар ва ракамлардан ташкил этилган PIN кодни хотирада саклашнинг енгиллиги.

PIN коди буйича мижозни идентификациялаштиришнинг икки усули билан бажариш мумкин: **алгоритмлашган ва алгоритмлашмаган.**

Алгоритмлашмаган текшириш усулида элемент киритган PIN код маълумотлар базасидаги шифрланган код билан таккосланилади.

Алгоритмлашган текшириш усулида эса мижоз киритган PIN код, махфий калитдан фойдаланган холда, махсус алгоритм буйича узгартирилади ва картадаги ёзув билан таккосланилади.

Ушбу усулнинг афзалликлари:

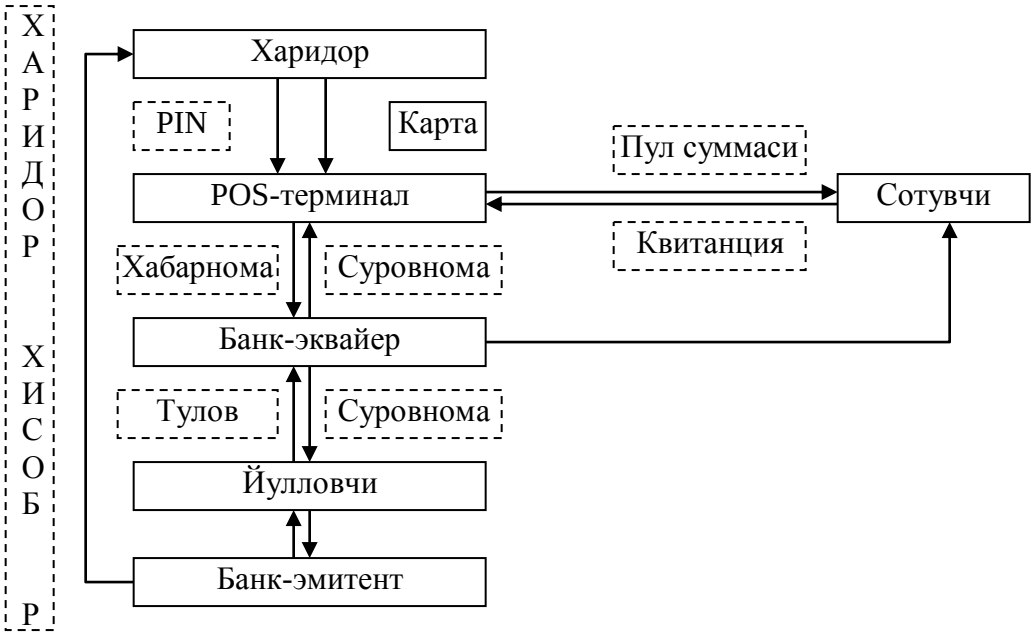
• асосий компьютерда PIN сакланмайди ва натижада персонал томонидан угирланмайди;

• PIN код телекоммуникация оркали жунатилмайди.

POS тизимини аник тасаввур килиш учун чизмани келтирамиз. Ушбу чизма буйича харидор уз пластик картасини урнатиб, PIN кодини киритади.

Сотувчи уз навбатида пул суммасини киритади. Шундан сунг, банк-эквайерга (сотувчи банки) пулни кучириш учун суровнома юборилади.

Банк-эквайер, уз навбатида, картанинг хакикийлигини аниклаш учун суровномани банк-эмитентга жунатади. Натижада, банк-эмитент пулни банк-эквайерга сотувчи хисобига кучиради. Пул кучирилгандан сунг, банк-эквайер томонидаи POS-терминалга хабарнома жунатилади. Ушбу хабарда транзакция бажарилганлиги хакида маълумот булади.



Шундан сунг, сотувчи харидорга махсулот ва квитанциясини такдим этади.

Уз-узидан куриниб турибдики, ушбу жараёнда хар хил вокеалар содир булиши мумкин.

POS тизимининг энг заиф кисми бу POS-терминалдир. Бундаги асосий хавф булиб терминалдаги махфий калитнинг угирланиши хисобланади.

Бунинг окибатлари куйидагилар булиши мумкин:

• олдинги транзакцияларда ишлатилган PIN кодни тиклаш;

• кейинги транзакцияларда кулланиладиган PIN кодни тиклаш.

Ушбу хавфлардан химояланишнинг 3 та усули таклиф этилади:

- хар бир транзакциясидан сунг калитни узгартириш;
- POS-терминал ва банк-эквайер орасидаги маълумотларни махсус калит билан шифрлаш хамда калитни хар бир транзакциядан сунг узгартириш;
- очик калитлар усули ёрдамида узатиладиган маълумотларни шифрлаш.

Банкоматлар хавфсизлигини таъминлаш

Банкоматлар накд пул олиш, хисоб ракамнинг холати ва пул кучириш имкониятларига эга.

Банкомат икки режимда ишлайди, off-line ва online.

Off-line режимда банкомат банк компьютерларидан мустакил ишлайди ва бажариладиган транзакциялар хакидаги ёзувларни уз хотирасида саклайди хамда принтерга узатиб, уларни чоп килади.

On-line режимда банкомат бевосита банк компьютерлари билан телекоммуникация оркали уланган булади. Транзакциясини амалга ошириш максадида банкомат банкдаги компьютер билан куйидаги хабарлар билан алмашади:

- банкомат суровномаси;

- банкнинг жавоб хабари;
- банкоматнинг туловни бажарганлиги хакидаги хабарни бериш.

Хозирги кунда банкоматлар тармокларидан бир неча банкларгина фойдаланади. Бу ерда мавжуд булган асосий муаммо бу банкларнинг махфий ахборотларини (масалан, махфий калит) бир-биридан химоялашдир.

Ушбу муаммонинг ечими сифатида PIN кодни, марказлаштирилган холда, хар бир банк томонидан текшириш таклиф килинади.

Бундан ташкари банкоматлар тармоги зоналарга таксимланади ва хар бир зонада ZCMK (Zone Control Master Key) калитлари, уз навбатида, компьютер тармогидаги калитларни шифрлашда кулланилади. Маьлумотларни шифрлашда эса IWK (Issuer Working Key) калитлар ишлатилади.

Internetда мавжуд электрон туловлар хавфсизлигини таъминлаш

Хозирги кунда Internetда купгина ахборот марказлари мавжуд, масалан, кутубхоналар, куп сохали маълумотлар базалари, давлат ва тижорат ташкилотлари, биржалар, банклар ва бошкалар.

Internetда бажариладиган электрон савдо катта ахамият касб этмокда. Буюртмалар тизимининг купайиши билан ушбу фаолият яна кескин ривожланади. Натижада, харидорлар бевосита уйдан ёки офисдан туриб, буюртмалар бериш имконига эга булишади. Шу боис хам, дастурий таьминотлар ва аппарат воситалар ишлаб чикарувчилар, савдо ва молиявий ташкилотлар ушбу йуналишни ривожлантиришга фаол киришишган.

Электрон савдо — глобал ахборот тармоклари оркали махсулотларни сотиш ва пулли хизматлар курсатиш демакдир.

Электрон савдонинг асосий турлари куйидагилардир:

• ахборотлар сотуви;

• электрон дуконлар;

• электрон банклар.

Ахборотлар сотуви асосан маълумотлар базасидан On-line режимда фойдаланиш учун такдим этилиши мумкин.

Электрон дуконлар Internetда Web-site оркали ташкиллаштирилади. Бунда товарлар руйхати, тулов воситалари ва бошкалар келтирилади. Харид килинган махсулотлар оддий почта оркали жунатилиши ёки агар улар электрон махсулот булса, бевосита Internetдан манзилга етказилиши мумкин.

Электрон банкларни ташкил этишдан асосий максад банкнинг доимий харажатларини камайтириш ва кенг оммани камраб олишдир. Шу боис, электрон банклар уз мижозларига юкори фоиз ставкаларини таклиф килишлари мумкин.

Харидор, кредит картаси сохиби, бевосита тармок оркали туловларни бажариш учун ишончли ва химояланган воситаларга эга булиши лозим.

Хозирги кунда SSL (Secure Socket Layer) ва SET (Secure Electronic Transactions) протоколлари ишлаб чикилган:

• SSL протоколи маълумотларни канал даражасида шифрлашда кулланилади;

• SET хавфсиз электрон транзакциялари протоколи якинда ишлаб чикилган булиб, факатгина молиявий маълумотларни шифрлашда кулланилади.

SET протоколининг жорий этилиши бевосита Internetда кредит карталар билан туловлар сонининг кескин ошишига олиб келади.

SET протоколи куйидагиларни таъминлашга кафолат беради:

- ахборотларнинг тулик махфийлиги, чунки фойдаланувчи тулов маълумотларининг химояланганлигига тулик ишонч хосил килиши керак;
- маълумотларнинг тулик сакланиши, яъни маълумотларни узатиш жараёнида бузилмаслигини кафолатлаш. Буни бажариш омилларидан бири ракамли имзони куллашдир;

• кредит карта сохибининг хисоб ракамини аудентификациялаш, яъни электрон (ракамли) имзо ва сертификатлар хисоб ракамини аудентификациялаш ва кредит карта сохиби ушбу хисоб ракамининг хакикий эгаси эканлигини тасдиклаш;

• тижоратчини уз фаолияти билан шугулланишини кафолатлаш, чунки кредит карта сохиби тижоратчининг хакикийлигини, яъни молиявий операциялар бажаришини билиши шарт. Бунда тижоратчининг ракамли имзосини ва сертификатини куллаш электрон туловларнинг амалга оширилишини кафолатлайди.

Такрорлаш учун саволлар

1. ***Электрон туловлар тизимининг асосий элементларини таърифлаб беринг.***

2. ***Идентификацияловчн шахсий номерини химоялашда андай амаллар бажарилади.***

3. POS тизими хавфсизлигини таъминлаш хусуиятларини кўрсатиб утинг.

4. Банкоматлар хавфсизлигини таъминлаш ҳақида айтиб беринг.

5. Электрон тўлов тизимларида ахборотларни химоялашнинг асосий восаталари нимадан иборат?

10 – МАВЗУ: КОМПЬЮТЕР ТИЗИМЛАРИНИНГ ХИМОЯЛАНГАНЛИК ДАРАЖАСИНИ АНИКЛАШ ВОСИТАЛАРИ

1. Компьютер тизимларига нисбатан дастурий хавфларнинг йуналишлари.

2. SSS (System Security Scanner) дастури хакида

3. Internet Scanner SAFEsuite дастури хакида

Корхоналарда жорий этилаётган автоматлаштирилган ахборот тизимининг хавфсизлигини таъминлаш, биринчи навбатда, ушбу тизимни лойихалаш боскичида кузда тутилган булиши лозим. Корхона микёсида кабул килинган хавфсизлик сиёсатининг ахборот тизимида кандай даражада акс эттирилиши мухим масалалардан бири хисобланади. Лекин, ахборот-коммуникациялар технологияларининг кескин ривожланиши, ахборот окимлари хажмининг ошиши. Internet ва intranet технологияларининг кенг микёсда кириб келиши бевосита автоматлаштирилган ахборот тизимларининг ахборот захираларини химоялашга йуналтирилган воситаларнинг мавжудлигини таъминлаш хамда тизимда мавжуд булган химоя воситаларини ривожлантиришини такозо этади.

Автоматлаштирилган ахборот тизимларига нисбатан мавжуд булган хавфларни учта йуналиш буйича ажратиш мумкин:

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

Амалий дастурларни текшириш буйича хозиргача ягона восита мавжуд эмас. Тармок хизматлари ва операцион тизим хизматларида кулланиладиган технологиялар умумий асосларга эга булганлиги учун уларни текшириш воситалари ишлаб чикилган.

Замонавий операцион тизимларда ахборот захираларини химоялаш воситаларининг мавжудлиги таъкидлаб келинмокда. Буларга аутентификациялаш, идентификациялаш, рухсатсиз киришни таъкиклаш, мониторинг ва аудит, криптография усулларининг мавжудлиги мисол була олади. Албатта, ушбу воситаларнинг операцион тизимларда мавжуд булганлиги корхонанинг хавфсизлик сиёсатига мос келади. Аммо, операцион тизимнинг нотугри конфигурацияланиши ва унинг дастурий таъминотидаги мавжуд хатолар окибатида ахборот тизимларига хужумлар уюштирилиши имконияти пайдо булади.

Шу боис, операцион тизимни танлашда ундаги камчиликларни тахлил килиш, ишлаб чикарувчи фирма томонидан йул куйилган хатоларнинг тан олиниши ва уларни зудлик билан тузатишга киришилиши талаб этилади.

Операцион тизимнинг параметрларининг тугри урнатилганлигини ёки уларнинг узгармаганлигини текшириш учун «тизим хавфсизлигини сканерлаш» деб номланувчи 10 га якин махсус дастурлар ишлаб чикарилган. Масалан, Solaris операцион тизими учун мулжалланган ASET, Netware ва NT учун KSA, Unix учун SSS дастурлари мавжуд.

SSS (System Security Scanner) дастури хакида

Ушбу дастур Unix операцион тизими урнатилган компьютерларда хавфсизлик холатини текшириш ва операцион тизимнинг ташки хамда ички заиф кисмларини аниклашга йуналтирилган. Бундан ташкари у кириш хукукларини, файлларга эгалик килиш хукукларини, тармок захираларини конфигурациялашни, аутентафикациялаш дастурларини ва бошкаларни текшириши мумкин.

Дастурнинг куйидаги имкониятлари мавжуд:

- **конфигурацияни текшириш**, яъни рухсатсиз киришларнинг олдини олиш максадида конфигурацияни текшириш. Бунга куйидагилар киради: конфигурация файллари, операцион тизим версияси, кириш хукуклари, фойдаланувчиларнинг захиралари, пароллар;
- **тизимдаги хавфли узгаришларни текшириш.** Рухсатсиз киришлар окибатида тизимда содир булган узгаришларни кидиришда кулланилади. Бундай узгаришларга куйидагилар киради: файллар эгаллаган хотира хажмининг узгариши, маълумотларга кириш хукуки ёки файлдаги маълумотларнинг узгариши, фойдаланувчиларнинг захираларга кириш параметрларининг узгариши, файлларни рухсатсиз бошка бир ташки компьютерларга узатишлар;
- **фойдаланувчи ннтерфейсининг кулайлиги.** Бу интерфейс ёрдамида нафакат дастур билан кулай ишлаш таъминланади, балки бажарилган ишлар буйича хисоботлар хам яратилади;
- **масофадан сканерлаш.** Тармокдаги кампьютерларни текшириш ва алока жараёнида маълумотларни шифрлаш имконияти таъминланади;
- **хисоботлар тузиш**. Бажарилган ишлар буйича тулик, хисоботлар яратилади. Ушбу хисоботларда тизимнинг аникланган заиф бугинларининг изохи келтирилади ва уларни тузатиш буйича курсатмалар берилади. Хисобот HTML ёки оддий матн куринишида булиши мумкин.

Тармок хизматларининг химояланганлигини тахлил килиш буйича биринчи булиб ишлаб чикарилган дастурлардан бири бу SATAN дастуридир. Бу дастур 20 га якин тармок хизматларидаги заифликларни аниклай олади.

Internet Scanner SAFEsuite дастури хакида

Агар текширувлар доимий равишда ва тулик амалга оширилиши талаб килинса, у хакда internet Scanner SAFEsuite дастурлар пакети таклиф килинади. Бу дастурлар пакети ёрдамида 140 та маълум булган заифликлар ва тармок воситалари, яъни тармоклараро экранлар, Web-серверлар, Unix, Windows 9.x, Windows NT тизимли серверлар ва ишчи станциялар, умуман TCP/IP протоколи кулланиладиган барча воситалар текширилади.

Internet Scanner SAFEsuite пакетинииг умумий имкониятлари куйидагилардан иборат:

1. Автомятлаштирилган ва конфигурацияланган сканерлаш:

• автоматлашган идентификациялаш ва заиф кисмлар буйича хисобот тузиш;

• доимий режа буйича сканерлаш;

• IP манзилларни сканерлаш;

• фойдаланувчи урнатган параметрларни сканерлаш;

• заиф бугинларни автоматик равишда тузатиш;

• ишончлилик ва такрорланувчанликни таъминлаш.

2. Хавфсизликни таъминлаш:

• тармок воситаларини инвентаризациялаш ва мавжуд асосий заиф бугинларни идентификациялаш;

• асосий хисоботларни таккослаш ва келгусида улардан фойдаланиш учун тахлил килиш.

3. Фойдаланишнинг оддийлиги:

• фойдаланувчининг график интерфейси;

• HTML туридаги тартибланган хисоботларни яратиш;

• сканерлашни марказлаштирилган холда бажариш, бошкариш ва мониторинг утказиш.

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

Web Security Scanner бевосита Web-серверларда мавжуд заиф кисмларни аниклашга мулжалланган булиб, бу дастурнинг имкониятлари куйидагилардан иборат:

• Web-сервер урнатилган операцион тизимни аудитлаш;

• Web-серверда мавжуд дастурларни аудитлаш;

• Web-файлларда мавжуд скриптларни аудитлаш;

• Web-сервер конфигурациясини тестдан утказиш;

• асосий файллар тизимининг хавфсизлик даражасини аниклаш;

• скриптларда мавжуд хатоларни аниклаш;

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

FireWall Scanner дастури бевосита тармокларо экранда мавжуд булган заиф кисмларни аниклашга мулжалланган булиб, у куйидаги амалларни бажаради:

• тармокларо экранга хужумлар уюштириб, уни тестдан утказиш;

• тармокларо экран оркали утадиган тармок, хизматларини сканерлаш.

Intranet Scanner дастури компьютер тармогида мавжуд камчиликларни тармокка рухсатсиз киришларини амалга ошириш оркали тестдан утказиш ёрдамида аниклашга йуналтирилган. Тармокнинг хир хил кисмлари (хост-компьютерлар, йулловчилар, Web-серверлар, Windows 9.x/NT тизимида ишлайдиган компьютерлар) ни текширишни хам амалга оширади.

Юкорида келтирилганлардан ташкари компьютер тизимларига рухсатсиз киришларни доимий равишда назорат килувчи дастурлар, масалан, Internet Security Systems компанияси томонидан ишлаб чикилган **Real Secure** дастури хам мавжуд. Бу дастур тармокда содир этилаётган ходисалар, масалан, хакерларнинг хужумларини кайд килиш билан биргаликда фаол химоя чора-тадбирларини ташкиллаштириши мумкин. Real Secure дастури йирик ташкилотлар учун мулжалланган булиб, хар куни тинимсиз ишлашга мулжалланган.

Real Secure дастури икки кисмдан иборат: **фильтрлаш** ва фойлаланувчининг **график нтерфейси.**

Фильтрлаш кисми тармокда содир этилаётган ходисаларни фаол кузатиш ва бошкариш учун хизмат килади. Дастурнинг иккинчи кисми ёрдамида фойлаланувчи руй берган ходисалар хакидаги маълумотларни кабул килади, уларни бошкаради ва тизим конфигурациясини узгартира олади. Натижада, фильтрлаш ва содир этилаётган ходисаларга нисбатан химоя тадбирларини автоматик равишда амалга ошириш мумкин булади, масалан, кайд килиш, дисплейга чикариш, ходисани ман этиш ва бошкалар.

Булардан ташкари барча кайд этилган ходисалар хакидаги маьлумотларни кейинчалик реал масштабда ёки тезкор ёки секинлашган режимларда куриб чикиш мумкин булади.

Real Secure дастури бевосита Sun OS, Solaris ва Linux операцион тизимларида ишлаш учун мулжалланган.

Такрорлаш учун саволлар

1. Корхона хавфсизлик сиёсатининг ахборот тизимида кандай акс эттирилиши керак.
2. Операцион тизимни танлашда қандай муаммоларни ҳисобга олиш керак.
3. Қандай диагностика дастурларини биласиз?
4. SATAN дастури қандай вазифаларни бажаради.
5. Real Secure дастури қайси операцион тизимлар остида фаолият кўрсатиб билади?

Адабиётлар:

1. Р.Х. Алимов, Б.Ю. Ходиев, К.А. Алимов, С.У. Усмонов, Б.А. Бегалов, Н.Р. Зайналов, А.А. Мусалиев, Ф. Файзиева, «Миллий иқтисодда ахборот тизимлари ва технологиялари», Ўқув қўлланма, Т. Шарқ, 2004 йил.
2. М.Т. Гафурова, Д.Ч. Дурсунов, В.И. Рапопорт, Б.Ю. Ходиев. Проектирование современных информационных технологий. Учебное пособие.-Тошкент, ТДИУ, 1994.-96 с.
3. Информационные системы в экономике: Учебник/Под ред. проф. В.В. Дика.-М.:Финансы и статистика,1996.-272 с.
4. Информатика: Учебник/Под ред. Н.В. Макаровой. -М.: Финансы и статистика, 1997.-768с.
5. Ғуломов С.С. ва бошқ. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик. —Т.: «Ўзбекистон», 1999. —528 б.
6. Козырев А.А. Информационные технологии в экономике и управлении: Учебник, 2-е изд. .—СПб.: Изд-во Михайлова В.А., 2001. —360 с.
7. Ходиев Б.Ю., Мусалиев А.А., Бегалов Б.А. Введение в информационные системы и технологии. Учебное пособие /Под ред. акад. С.С. Гулямова. —Т.:ТГЭУ, 2002. —156 с.
8. Шафрин Ю.А. Информационные технологии. —М.: Лаборатория Базовых Знаний, 1998. —704 с.
9. Петров Б.Н. Информационные системы. – СПб.: Питер, 2003. – 688с.:ил.

Кушимча адабиётлар:

1. Коутс Р., Влейминк И. Интерфейс "человек-компьютер": Пер. с англ.-М.: Мир, 1990.-501 с.
2. Гафурова М.Т., Дадабаева Р.А. Персонал компьютерларнинг программ системалари.- Тошкент, ТДИУ, 1992.-100 бет.
3. Р.Персон Windows 95 в подлиннике: Пер. с англ.-СПб: BHV- Санкт-Петербург, 1996.-736 с.
4. А.И. Марченко, В.П. Пасько Word 7.0 для Windows 95: К.: Торгово-издательское бюро BHX, 1996.-464 с.
5. Компьютерлаштиришни янада ривожлантириш ва ахборот коммуникацион технологияларини жорий этиш туғрисида \\Хабарнома. –2002, №2.
6. Гафурова М.Т., Дурсунов Д.Ч. Стандартизация оформления дипломных, курсовых проектов и лабораторных работ: Методические указания.—Т.: ТДИУ,1988.—80 б.
7. Острейковский В.А. Информатика. М.: Высшая школа, 1999.
8. IBM PC для пользователя. Фигурнов В.Э. М.: Инфра, 2001.
9. Рахмонқулова С.И. Шахсий компьютерда ишлаш. Тошкент - “Шарк”, 1998.
10. Джой Крейнак. Интернет. Санкт-Петербург, Питер, 1999.
11. www.piter.com
12. www.intuit.ru
13. www.it-study.ru
14. www.informatika.ru
15. www.edu.uz
16. www.ref.uz

6.2. Маъруза машғулотлари дарс ишланмаси

Самарқанд Давлат университети

“Ахборотлаштириш технологиялари” кафедраси

Ахборотларни ҳимоялаш фанидан

маъруза машғулотлари ишланмаси

20 соат

10 маъруза

САМАРҚАНД – 2019

1 - МАЪРУЗА: ЗАМОНАВИЙ АХБОРОТЛАШГАН ЖАМИЯТ ВА АХБОРОТ ХАВФСИЗЛИГИ. АСОСИЙ ТУШУНЧАЛАР ВА ТАЪРИФЛАР	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга ахборот хавфизлигининг асосий тушунчалари билан таништириш; предметнинг мақсад ва вазифалари ҳақида маълумот бериш, ахборот хавфсизлигига хавф-хатарларни таснифлаш, хавфсизликни назорат қилиш воситалари бўйича маълумот бериш.
Таянч иборалар	Ахборот хавфсизлиги**,** ахборот ҳимояси, ахборотларга нисбатан хавф хатарлар; ёвуз ниятли шахс, ахборотларга рухсатсиз кириш, бузғунчи.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут

Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Ахборот хавфсизлиги мақсад ва вазифалари нимадан иборат?
2. Предметнинг асосий тушунчаларини таърифлаб беринг.
3. Ахборотларга нисбатан хавф-хатарларни таснифлаб беринг.
4. Қайси тармок хавфсизлигини назорат килиш воситаларини биласиз?

Мустақил иш топшириқлари:

1. Ахборот хавфсизлигининг асосий тушунчалари луғатини тузинг.
2. Ахборотларга нисбатан хавф-хатарларга мисоллар кўрсатинг?
3. Ташкилот ва муассасаларда ахборотларга нисбатан хавф-хатарлардан кўрилган зарарга мисоллар кўрсатинг?
4. Маълумотларга рухсатсиз киришда вирусдан қандай фойдаланиш мумкин?
5. Ахборот хавфсизлигини назорат қилиб турувчи воситаларга мисол кўрсатинг.

Мавзуга доир тестлар:

1. Ахборот химояси деганда куйидагилар тушунилади:

*a) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён

b) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси

c) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуби

d) Барча жавоблар тугри

2. Тармок даражасида химояланишнинг техник усуллари куйидагиларга булинадилар:
*a) аппаратли, дастурли, аппарат-дастурли
b) ташкиллаштирилган, тизимли, аппаратли
c) аппарат-дастурли, тизимли, дастурли
d) тугри жавоб йук

3. Кайси тизимлар максад ёмон ниятли кишиларни алдаш учун псевдо-сервислар билан ишлайди.
*a) алмаштириш тизими
b) регистрацион тизим
c) хужумларни ушлаш тизими
d) бутунлигини назорат килиш тизимлари

Адабиётлар:

1. Абдувоҳидов А. М., Позилов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. Ғуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
3. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

2 – МАЪРУЗА: АХБОРОТ ХАВФСИЗЛИГИНИНГ АСОСИЙ ХАВФЛАРИ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга ахборот химоялаш тизими, ташкилотлардаги ахборотларни химоялаш тизимининг комплекслилиги; ахборотларни ташкилий ҳимоялаш элементлари; ахборот тизимларида маълумотларга насбатан хавф-хатарлар бўйича маълумот бериш.
Таянч иборалар	Ахборотларга нисбатан хавф хатарлар; ҳимоя тизими, ҳуқуқий, техник-мухандис, дастурий-математик, ташкилий, чоралар мажмуаси.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут

Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Автоматлаштирилган ахборот тизимларида химоялаш зарурияти.
2. Ахборотни химоялаш тизими элементларини айтиб утинг.
3. Ташкилотлардаги ахборотларни химоялаш мухимлигини тушунтириб беринг.
4. Химоялаш тизимининг комплекслилигига андай эришилади.
5. Ахборотларни ташкилий ҳимоялаш элементлари вазифаси.
6. Ахборот тизимларида маълумотларга насбатан хавф-хатарлар

Мустақил иш топшириқлари:

1. Ташкилот ва муассасаларда ахборот алмашуви хажмига нисбатан қандай ахборот химояси чоралари қўрилиши мақсадли?
2. Ахборот хавсизлиги тизимининг ҳуқуқий чора-тадбирларга мисоллар кўрсатинг.
3. Ахборот хавсизлиги тизимининг техник-мухандис чора-тадбирларга мисоллар кўрсатинг.
4. Ахборот хавсизлиги тизимининг ташкилий чора-тадбирларга мисоллар кўрсатинг.
4. Ахборот хавсизлиги тизимининг дастурий чора-тадбирларга мисоллар кўрсатинг.

Мавзуга доир тестлар:

1. Фойдаланувчиларни идентификация килиш қуйидагиларни аниқлайди
*a) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш шкаласини
b) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш графигини
c) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш паролини
d) турли хил маълумотлар базаси ва маълумотлар базасининг қисмига кириш кодини

2. Маълумотларни физик ҳимоялаш кўпроқ
a) ташкилий ва ноташкилий чораларга қарашлидир
*b) ташкилий чораларга қарашлидир
c) ноташкилий чораларга қарашлидир
d) туғри жавоб йўқ

3. Ахборотга кириш ҳуқуқини узатиш ва ҳимоя қилиш воситалари қуйидаги
a) Файллар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
b) Браузерлар мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
c) Диференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди
*d) Маълумотлар билан диференциаллашган мунособатида бўлиш характерли хусусиятини қатъий қилиб қўяди

4. Ҳимоя қилишнинг асосий муаммолари қуйидагилардан иборат
*a) Ахборотга киришга йўл қўймаслик
b) Файлга киришга йўл қўймаслик
c) Шифрга киришга йўл қўймаслик
d) Кодга киришга йўл қўймаслик

Адабиётлар

1. Абдувоҳидов А. М., Позилов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. А.Ортиқов, А. Маматқулов. «IBM PC компютерларидан фойдаланиш». Т.: 1992 й.
3. Ғуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
4. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998
5. Трубачев А.П. и др. Оценка безопасности информационных технологий СИП РИА, 2001
6. Допильченко И.А. И др. Автоматизированные системы управления предприятиями. М. Машиностроение 1984.
7. Карминский А. М., Нестеров П.В. «Автоматизация бизнеса». Москва «Финансы и статистика». 1997 год
8. «Информатика» / Под ред. Проф. Н. В. Макаровой./ Москва: Финансы и статистика. 1997 й.
9. Russel D., Gangemi G.T. Sr.Computer Security Basics O'Reilly, 1992
10. Гайкович В., Першин А. Безопасность электронных банковских систем Единая Европа, 1994.

3 – МАЪРУЗА: ВИРУС ВА АНТИВИРУСЛАР ТАСНИФИ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга ахборот хавфизлигининг асосий тушунчаларидан бўлган вирус, уларнинг пайдо бўлиш йўллари ва турлари ҳақида маълумот бериш; эркин фикрлаб, вирусга қарши қўлланадиган воситалар бўйича маълумотга эга бўлиб, асосий антивирус дастурлар турларини таҳлил қилишни ўргатиш, ҳусусий холларга мос дастурларни танлаб билиш ва уларни аниқ холатларда қўллай билиш кўникмаларни ҳосил қилиш.
Таянч иборалар	Ахборотларга нисбатан хавф хатарлар; вирус, файлли, юкловчи, зарарли, ахборотларни ҳимоялаш, рухсат этилган кириш, маълумотларни ўқиб олиш, антивирус, диск, фаг, доктор, ревизор..
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут

Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун назорат саволлари

1.Вирус тушунчасини таърифлаб беринг.

2. Компьютернинг вируслар билан зарарланиш йулларинпи айтиб утинг.

3. Компьютер вирусларидан ахборотларга рухсатсиз кириш қандай ташкил қилинади?

4. Антивирус дастурларини таснифлаб беринг.

5. Вирусларга қарши қандай чора-тадбирлар самарали ҳисбланади.

Мустақил иш топшириқлари:

1. Вируслар билан зарарланиш натижасидаги оқибатларга мисоллар кўрсатинг.
2. Оҳирги 5 йилда кенг тарқалган вирус даструлар номлари ва уларнинг зарарли функцияларига мисоолар кўрсатинг?
3. Маълумотларга рухсатсиз киришда вирусдан қандай фойдаланиш мумкин?
4. Ҳозирги кунда оммавийлашган антивирус дастурларидан бирига мисол кўрсатинг ва унинг имкониятларини таҳлил қилиб беринг.
5. Вирусни шахсий компьютерга туширмаслик учун энг самарали чора-тадбирлар кетма-кетлигини кўрсатиб беринг.

Мавзуга доир тестлар:

1. Антивирус дастурларини синовдан ўтказиш билан қандай ташкилот шуғулланади?
   a) Intel, Celeron
   b) Celeron, IBM
   c) Компьютер хавфсизлиги миллий ассоциацияси NCSA (National Computer Security Association)
   d) IBM, INTEL

2. Бутликни назорат килиш тизими
   a) Команда файлларини, качонки ёвуз ниятли уларга узгартиришлар киритилгалигини аниклаш учун текширади
   b) Тизим файлларини, качонки ёвуз ниятли уларга узгартиришлар киритилгалигини аниклаш учун текширади
   c) Модул файлларини, качонки ёвуз ниятли уларга узгартиришлар киритилгалигини аниклаш учун текширади
   d) тугри жавоб тугри

3. Руйхатга олинган файллар монитори
   a) Тармокдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган файлларни назорат килади
   b) Тармокдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган тизимли файлларини назорат килади
   c) Тармокдаги серверлар ва ишчи станцияларда яратиладиган руйхатга олинган буйрук файлларини назорат килади
   d) Автоматик юклаш файлларини

Адабиётлар:

1. Абдувоҳидов А. М., Позилов Б. К. Замонавий ахборот технологияси. - Т.: 1999.
2. Ғуломов С.С. ва бошқалар. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик.
3. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

4 – МАЪРУЗА: АХБОРОТЛАРНИ СТЕГАНОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ ВА КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ		
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга ахборот хавфизлигининг асосий қисмларидан бўлган замонавий компьютер стеганографияси, конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш, стенографик дастурлар тўғрисида кисқача маълумот, криптография ҳақида асосий тушунчалар, симметрияли криптотизим асослари ҳақида маълумот бериш.	
Таянч иборалар	Стеганографик усуллар, сув ҳимоя белгиси, инверслаш, маълумотни қуриш, криптографик ҳимоялаш, очиқ калит, махфий калит.	
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.	
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат	
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.	
Дарснинг хронологик харитаси – 80 минут		
Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Замонавий компьютер стенографияси истикболлари.

2. Компьютер стенографиясининг асосий вазифалари.

3. Конфиденциал ахборотларни рухсатсиз киришдан ҳамоялаш учун андай йўналишлар мавжуд?

4.. *Криптографиянинг асосий тушунчаларини таърифлаб беринг.*

5. *Ахборотларни криптографияли ҳимоялаш тамойиллари.*

6. *Уринларни алмаштириш ва алмаштириш усуллари қандай криптотизиларга тегишли?*

Мустақил иш топшириқлари:

1. Дастурий таъминотни ниқоблаш алгоритмларини ўрганиб, энг самаралисини танлаш усулини таклиф қилинг?
2. Муаллифлик ҳуқуқларни ҳимоялашда стеганографиядан қандай фойдаланилади?

3. Windows операцион муҳитида ишловчи стеганография дастурларининг ишлаш принципларини, модуллари таркибини тавсифлаб беринг?
4. Симметрияли криптографик тизимдаги ўринларни алмаштириш усулларига мисоллар кўрсатинг.
5. Симметрияли криптографик тизимдаги алмаштириш усулларига мисоллар кўрсатинг.
6. Симметрияли криптографик тизимдаги гаммалаш усулларига мисоллар кўрсатинг.
7 Симметрияли криптографик тизимдаги тахлилий ўзгартириш усулларига мисоллар кўрсатинг.

Мавзуга доир тестлар:

1. Криптомустаҳкамлик – бу
*A. Шифрнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
B.Идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
C. Коднинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
D. Код ва идентификаторнинг дешифрлашга нисбатан мустаҳкамлигини аниқловининг тавсифидир
2. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда таалуқли?
A. Ахборотни чиқаришнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
B. Ахборотни киритишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
*C. Ахборотни қайта ишлашнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
D. Ахборотни ёзишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади
3. Очиқ калитли тизимда шифрлаш ва дещифрлаш учун қандай калит ишлатилади?
A. очиқ
*B. очиқ ва ёпиқ
C. ёпиқ
D. барча жавоблар нотўғри

4. Криптомустаҳкамликнинг қанақа кўрсаткичлари мавжуд
A. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли бошланғич вақт;
*B. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли ўртача вақт;
C. –мумкин бўлган калитлар сони; –крипто таҳлил учун керакли охирги вақт;
D. барча жавоблар тўғри

5. Ахборотни ҳимоялаш мақсадида шифрлашнинг эфективлиги қуйдагилардан боғлиқ
A. Тўғри жавоблар йўқ
B. Шифрни криптомустаҳкамлиги ва идетификаторларнинг сирини сақлашдан
*C. Шифрни криптомустаҳкамлиги ва калитнинг сирини сақлашдан
D. Шифрни криптомустаҳкамлиги ва коднинг сирини сақлашдан

6. Шифрланган маълумот ўқилиши мумкин фақат
*A. Калити берилган бўлса
B. Коди берилган бўлса

C. Идентификатори берилган бўлса
D. Шифри берилган бўлса

7. Шифрланган ахборотни шарҳлаб беришда мумкин бўлган калитларни танлаш йўли учун зарур жараёнлар сони қуйидагиларни ўз ичига олади

A. Юқоридан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

B. Қуйидан баҳолаш қаттиқ талаб қилинмайди; замонавий компьютерлар имконият чегарасидан чиқади

*C. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқади

D. Қуйидан баҳолаш қаттиқ талаб қилинади; замонавий компьютерлар имконият чегарасидан чиқмайди

8. Калитларни сезиларсиз ўзгартириш қуйдагиларга олиб келиши мумкин

A. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ўзгариш олади

B. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларли ва сезиларсиз ўзгариш олади

C. Хато бир хил калитни ишлатганда шифрланган маълумот кўриниши сезиларсиз ўзгариш олади

*D. битта ва бир хил калитдан фойдаланганда ҳам шифрланган хабарлар сезиларли даражада ўзгаришга эга бўлади

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

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

3. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).

5 – МАЪРУЗА: МАЪЛУМОТЛАРНИНГ ТАРКАЛИБ КЕТИШИ ВА МАЪЛУМОТЛАРГА РУХСАТСИЗ КИРИШ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга маълумотларнинг таркалиб кетиши ва маълумотларга рухсатсиз киришдан химоя қилиш чора-тадбирлари ва воситалари ҳақида маълумот бериш. Ахборот химоя тизимларини ташкил қилиш долзарблиги, ахборот тизимларнинг таъсирчан кисмлари, маълумотларга рухсатсиз киришнинг дастурий ва техник воситаларини ўргатиш.
Таянч иборалар	Маълумот тарқалиши, рухсатсиз кириш, таъсирчан кисм, протокол, дастурий ва техник воситалар.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут

Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

4. Протоколлар ижобий имкониятлари билан бирга кандай камчиликларга хам эга?
5. Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари.
6. Маълумотларга рухсатсиз эгалик килиш учун зарур булган дастурларни татбик этиш усулларини айтиб утинг.

Мустақил иш топшириқлари:

1. Ахборот химояси тизимини ташкил қилиш долзарблигини Ўзбекистон Республикасидаги корханалар мисолида кўрсатинг.
2. Ахборот тизимларининг асосий таъсирчан кисмлари руйхатини кенгайтиринг.
3. Windows операцион муҳитида маълумотлага рухсатсиз киришдан қанчалик даражада химоялангани ҳақида маълумот беринг.
4. Маълумотларга рухсатсиз киришнинг дастурий воситаларига мисоллар келтиринг

Мавзуга доир тестлар:

1. Шифрлаштириш сузининг маъноси нима ?

*A. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн шифрланган матн билан алмаштирилади.

B. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн жадвал билан алмаштирилади.

C. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн лотинча матн билан алмаштирилади.

D. Шифрлаштириш – алмаштирилган жараён бўлиб, берилган матн инглизча матн билан алмаштирилади.

2. Дешифрлаштириш сўзининг маъноси нима?

A. Дешифрлаштириш – бу матн маълумотларини ўзгартириш учун иккилик коди.

*B. Дешифрлаштириш – шифрлаштиришга тескари жараён. Калит асосида шифрланган матн ўз ҳолатига узгартирилади.

C. Шифрлаштириш – бу график маълумотларни ўзгартириш учун саккизлик коди.

D.Шифрлаштириш – бу график ва матнли маълумотларни ўзгартириш учун саккизлик коди

3. Калитларни тақсимлаш ва калит билан бошқариш терминлари қайси жараёнда таалуқли?

A. Ахборотни чиқаришнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

B. Ахборотни киритишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

*C. Ахборотни қайта ишлашнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

D. Ахборотни ёзишнинг шундай жараёники, бунда калитлар тузилади ва фойдаланувчиларга тарқатилади

4. Мумкин бўлган тўпламлардан олинган ҳар қандай калитлар қуйидагини таъминлайди

*a) ахборотни ишончли ҳимоялаш

b) компьютерни ишончли ҳимоялаш

c) файлни ишончли ҳимоялаш

d) ахборот ва файлни ишончли ҳимоялаш

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

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

3. Коблиц. Н. Курс теории чисел и криптографии - М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).

6 – МАЪРУЗА: КОМПЮТЕР ТАРМОҚЛАРИДА ЗАМОНАВИЙ ҲИМОЯЛАШ

УСУЛЛАРИ ВА ВОСИТАЛАРИ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга компьютер тормокларининг заиф кисмлари, тармок химоясини ташкил килиш асослари ва таъминлаш усуллари, компьютер телефониясидаги химоялаш усуллари хақида тушунча бериш.
Таянч иборалар	Компьютер тармоғи, тармоқ ҳимояси, операцион тизим, маълумот тарқалиши, рухсатсиз кириш, протокол, дастурий ва техник воситалар.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут		
Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Компьютер тормокларининг заиф кисмлари нимадан иборат?

2.Тармок химоясини ташкил килишда нималарга эътибор бериш зарур?

3. ***Компьютер телефониясида қандай хавсизлик муаммолари мавжуд?***

4. Компьютер тармокларида маълумотларни химоялашнинг асосий йуналишларини айтиб утинг.

Мустақил иш топшириқлари:

1. Компьютер тормокларининг заиф кисмлари руйхатини тузинг.
2. Компьютер телефониясидаги химоялаш усулларига мисоллар кўрсатинг.
3. Компьютер тармокларида химояни таъминлаш учун қуланадиган усуллар руйхатини келтиринг.
4. ЭХМ химоясини таъминлашнинг техник воситаларини таснифлаб беринг.
5. Компьютер жиноятларини камайтиришда кандай чора-тадбирларни утказиш керак?

Мавзуга доир тестлар:

1. Автоматик кайта чакирув усули гояси куйдагидан иборат

a) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилади

*b) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – идентификацион код талаб этилади

c) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – шифр талаб этилмайди

d) марказий базадан узоклашган фойдаланувчи базага бевосита мурожаат килолмайди – парол ва шифр талаб этилади

2. Узок (олис)лаштирилган масофадан бузиш нима?

a) Хаваскорлик фаолияти

b) Абонентлик фаолияти

*c) Хакерлик фаолияти

d) Фойдаланувчи фаолияти

3. Хакер (hacker) нима?

*a) хакер – бу булаётган ходисаларга кушилишни истайдиган одам учун умумий таъриф

b) хакер – ШК фойдаланувчиси

c) хакер – бу Интернет абоненти

d) хакер – бу булаётган ходисаларга кушилишни истамайдиган одам учун асосий таъриф.

4. Бузувчи (взломщик) нима?

a) cracker - хакер

*b) cracker – intruder (коида бузувчи)

c) cracker - Ping

d) cracker - domain

Адабиётлар

1. Гуломов С.С. ва бошк. Иктисодий информатика: Олий укув юртларининг иктисодий мутахассисликлари учун дарслик.

2. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

3. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

7 – МАЪРУЗА: INTERNETДА АХБОРОТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ АСОСЛАРИ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга Internetда рухсатсиз кириш усуллари, рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши, тармокларо экран, унинг вазифалари ва асосий компонентлари хақида тушунча бериш.
Таянч иборалар	Глобал тармоқ, манзил, рухсат этилган, рухсатсиз кириш, тармоқ ҳимояси, тармоқлараро экран, шлюз, амалий даража, тармоқ даражаси.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут		
Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Хар кандай ташкилот Intenetга уланганидан сунг андай муаммоларни хал этиши шарт?
2. Рухсат этилган манзилларнинг рухсат этилмаган вактда уланишни тушунтириб беринг.
3. Қайси хавф глобал тармокларнинг бир канча сохаларини камраб олади?
4. Тармокларо экран ва унинг вазифалари
5. Тармокларо экраннинг асосий компонентлари

Мустақил иш топшириқлари:

1. Internetда ахборот хавфсизлиги нуқтаи назаридан мавжуд булган муаммоларни кўрсатинг.
2. Локал тармокларнинг глобал тармокарга кушилиши учун тармоклар химояси администратори кандай масалаларни хал килиши лозим:
3. Рухсат этилган манзилларнинг рухсат этилмаган вактда уланиши хавфи глобал тармокларнинг қайси сохаларини камраб олади?

4. Тармокларарo экранниг вазифаларини таърифлаб беринг.

5. Амалий ва тармоқ даражадаги шлюзларнинг ишлаш принципларини кўрсатиб беринг.

Мавзуга доир тестлар:

1. “Instruction Detection System” нима?

a) Хужумни аниклаш дастури

b) Хужумни аниклаш модули

*c) Хужумни аниклаш тизими

d) Хужумни аниклаш пакети

2. Тармок даражасидаги аниклаш тизими куйидагиларни текширади?

*a) Тармок доирасидаги пакетлар ва ёвуз ниятлининг химояланадиган тизим ичига кириш холатини аниклайди

b) Тармок доирасидаги дастур ва ёвуз ниятлининг химояланадиган тизим ичига кириш холатини аниклайди

c) Тармок доирасидаги модул ва ёвуз ниятлининг химояланадиган тизим ичига кириш холатини аниклайди

d) барча жавоблар тугри

3. Тармок даражасида химояланишнинг техник усуллари куйидагиларга булинадилар:

*a) аппаратли, дастурли, аппарат-дастурли

b) ташкиллаштирилган, тизимли, аппаратли

c) аппарат-дастурли, тизимли, дастурли

d) тугри жавоб йук

Адабиётлар

1. Гуломов С.С. ва бошк. Иктисодий информатика: Олий укув юртларининг иктисодий мутахассисликлари учун дарслик.

2. Галатенко В.А., Под ред. Бетелина В.Б. Информационная безопасность: практический подход. Наука, 1998

3. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

8 – МАЪРУЗА: ЭЛЕКТРОН ПОЧТАДА АХБОРОТЛАРГА НИСБАТАН МАВЖУД ХАВФ-ХАТАРЛАР ВА УЛАРДАН ХИМОЯЛАНИШ АСОСЛАРИ		
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга электрон почтадан фойдаланишда ахборот хавфсизлигига нисбатан мавжуд бўлган хавфлар ва уларни бартараф этиш усуллари, чора-тадбирлари воситалари хақида тушунча бериш.	
Таянч иборалар	Глобал тармоқ, электрон почта, протокол, шахсий маълумот, спам, рухсат этилган манзил, апплет, динамик дастур тармоқ ҳимояси.	
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.	
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат	
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.	
Дарснинг хронологик харитаси – 80 минут		
Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Электрон почтадан фойдаланиш хусусиятларини кўрсатинг.

2. E-mail адресларидан фойдаланишда қандай ахборот хавфсизлиги муаммолари мавжуд.

3. Электрон почтада мавжуд хавфлар.

4. Электрон почтага рухсатсиз киришнинг қандай усуллари мавжуд.

5. Электрон почтани химоялаш усуллари ҳаида гапириб беринг.

Мустақил иш топшириқлари:

1. Internetда ахборот хавфсизлиги нуқтаи назаридан мавжуд булган муаммоларни кўрсатинг.
2. Электрон почта ишини таъминлайдиган протоколлар руйхатини келтиринг.
3. Бирон-бир электрон почта протоколининг ишлаш принципини тавсифлаб беринг.
4. Электрон почта билан ишлаш жараёнида мавжуд хавфлар руйхатини келтиринг.

5. Электрон почтада ахборот хавфсизлигига нисбатан хавфларга қандай химояланиш усуллари ишлаб чикилган:

Мавзуга доир тестлар:

1. Ахборот химояси деганда куйидагилар тушунилади:

*a) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён

b) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси

c) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуби

d) Барча жавоблар тугри

2. Ахборотлар таркалиш канали – бу:

a) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

*b) Манбаларнинг очиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

c) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

d) Тугри жавоблар йук

3. Ахборотлар таркалиш техник каналлари – бу:

a) Акустик ва вироакустик, электрик, телеканаллар, оптик

b) Акустик ва вироакустик, электрик, серверлар, оптик

*c) Акустик ва вироакустик, электрик, радио каналлар, оптик

d) Акустик ва вироакустик, электрик, теле каналлар, провайдерлар

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

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

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

4. Браунли Н., Гатмэн Э., Как реагировать на нарушения информационной безопасности (RFC 2350, BCP 21)

9 – МАЪРУЗА: ЭЛЕКТРОН ТУЛОВЛАР ТИЗИМИДА АХБОРОТЛАРНИ ХИМОЯЛАШ		
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга электрон почтадан фойдаланишда ахборот хавфсизлигига нисбатан мавжуд бўлган хавфлар ва уларни бартараф этиш усуллари, чора-тадбирлари воситалари хақида тушунча бериш.	
Таянч иборалар	Глобал тармоқ, электрон почта, протокол, шахсий маълумот, спам, рухсат этилган манзил, апплет, динамик дастур тармоқ ҳимояси.	
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.	
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат	
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.	
Дарснинг хронологик харитаси – 80 минут		
Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. ***Электрон туловлар тизимига таъриф беринг.***
2. ***Идентификацияловчн шахсий номери схемасини кўрсатинг.***
3. ***Банк томонидан бериладиган PIN қандай амалга оширилади:***
4. ***Банкоматлар иши режимлари қандай бўлиши мумкин?***

Мустақил иш топшириқлари:

1. Электрон туловлар тизимининг асосий элементларини таърифлаб беринг.
2. Идентификацияловчн шахсий номерини химоялашда андай амаллар бажарилади.
3. POS тизими хавфсизлигини таъминлаш хусуиятларини кўрсатиб утинг.
4. Банкоматлар хавфсизлигини таъминлаш ҳақида айтиб беринг.
5. Электрон тўлов тизимларида ахборотларни химоялашнинг асосий восаталари нимадан иборат?

Мавзуга доир тестлар:

1. Ахборот химояси деганда куйидагилар тушунилади:

*а) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини,

фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик жараён

b) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик процедураси

c) Бошкариш ва ишлаб чикариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлигини, ишончлилигини, фойдаланиш осонлигини ва махфийлигини таъминловчи катъий регламентланган динамик технологик услуби

d) Барча жавоблар тугри

2. Ахборотлар таркалиш канали – бу:

a) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

*b) Манбаларнинг очиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

c) Манбаларнинг ёпиклиги, инсонлар, техник воситалар, бузук электрон нурланишлар ва йуналишлар хисобланадилар

d) Тугри жавоблар йук

3. Ахборотлар таркалиш техник каналлари – бу:

a) Акустик ва виброакустик, электрик, телеканаллар, оптик

b) Акустик ва виброакустик, электрик, серверлар, оптик

*c) Акустик ва виброакустик, электрик, радио каналлар, оптик

d) Акустик ва виброакустик, электрик, теле каналлар, провайдерлар

Адабиётлар

1. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. – М.:СИНТЕГ, 2000, 248 с.

2. Ғуломов С.С. ва бошқ. Иқтисодий информатика: Олий ўқув юртларининг иқтисодий мутахассисликлари учун дарслик. —Т.: «Ўзбекистон», 1999. —528 б.

10 – МАЪРУЗА: КОМПЬЮТЕР ТИЗИМЛАРИНИНГ ХИМОЯЛАНГАНЛИК ДАРАЖАСИНИ АНИҚЛАШ ВОСИТАЛАРИ	
Дарснинг ўқув ва тарбиявий мақсади:	Талабаларга электрон почтадан фойдаланишда ахборот хавфсизлигига нисбатан мавжуд бўлган хавфлар ва уларни бартараф этиш усуллари, чора-тадбирлари воситалари хақида тушунча бериш.
Таянч иборалар	Глобал тармоқ, электрон почта, протокол, шахсий маълумот, спам, рухсат этилган манзил, апплет, динамик дастур тармоқ ҳимояси.
Дарс ўтиш воситалари:	Синф доскаси, плакатлар, фундаментал фан дарсликлари, ўқув ва услубий қўлланма, тарихий маълумотлар, информатика ва техника атамалари луғатлари ва копмьютердан самарали фойдаланилади.
Ўқитиш усуллари	Диалогик ёндошув, муаммоли таълим. Поғона, Венна диаграммаси, Т-схемаси, ўз-ўзини назорат
Дарс ўтиш усуллари:	Такрорлаш, сухбат, ва савол-жавоб ҳамда, мунозара (мавзуни ўзлаштиришни мустаҳкамлаш) тарзида жонли мулоқот ўтказилади (талабанинг мустақил, эркин фикрлаш ва сўзлашишга ўргатган ҳолда фикр мулохазаларини баён қилдириш, бунинг учун ҳар бир талабага ўтилган мавзулар, таянч иборалардан саволлар ташланади, улар ўз фикрини баён қилади, ҳамма ўқувчи жавобни баён қилиб бўлгандан сўнг ўқитувчи билан биргаликда жавоблар якун қилинади); тарқатма материаллар асосида амалий мисоллар ечилади, ибораларга изоҳлар берилади.

Дарснинг хронологик харитаси – 80 минут

Ташкилий қисми:	Аудиториянинг жихозланиши ва санитар шароитлари, талабалар давоматини аниқлаш	2 минут
Билимларни баҳолаш	Янги мавзуни ўрганиш учун зарур бўлган материал бўйича сухбат	10 минут
Янги мавзуни баён этиш	55 минут	
Мавзу ўзлаштирилган даражасини аниқлаш	10 минут	
Уйга вазифа	3 минут	

Такрорлаш учун саволлар

1. Корхона хавфсизлик сиёсатининг ахборот тизимида кандай акс эттирилиши керак.
2. Операцион тизимни танлашда қандай муаммоларни ҳисобга олиш керак.
3. Қандай диагностика дастурларини биласиз?
4. SATAN дастури қандай вазифаларни бажаради.

Мустақил иш топшириқлари:

1. Автоматлаштирилган ахборот тизимларига нисбатан мавжуд булган хавфларни қандай йуналишларга ажратиш мумкин?
2. SSS (System Security Scanner) дастурнинг имкониятлари ҳақида маълумот беринг.
3. Internet Scanner SAFEsuite пакетиниг умумий имкониятлари ҳақида маълумот беринг.
4. FireWall Scanner дастури тармокларарo экранда бажарадиган амаллар ҳақида маълумот беринг.
5. Маърузада кўрилган дастурлардан бошқа компьютер тизими ҳимояланганлик даражасини аниқловчи дастур ҳақида маълумот беринг.

Мавзуга доир тестлар:

1. “Instruction Detection System” нима?
   a) Хужумни аниклаш дастури
   b) Хужумни аниклаш модули
   *c) Хужумни аниклаш тизими
   d) Хужумни аниклаш пакети

2. Тизимни бузишнинг мохияти нима?
   a) Хакерлик фаолиятининг шундай куринишики, бунда фойдаланувчи юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
   *b) Хакерлик фаолиятининг шундай куринишики, бунда бузувчи юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
   c) Хакерлик фаолиятининг шундай куринишики, бунда абонент юкори махоратга эга булмаган абонент сифатида тизимда руйхатдан утган булади.
   d) Барча жавоблар тугри.

3. Маълумотларни ҳимоя қилиш тушунчасига
   *a) маълумотларнинг тўлиқлигини сақлаш ва маълумотга киришини бошқариш киради
   b) файлнинг тўлиқлигини сақлаш киради
   c) шифрнинг тўлиқлигини сақлаш киради
   d) коднинг тўлиқлигини сақлаш киради

Адабиётлар

1. Гуломов С.С. ва бошк. Иктисодий информатика: Олий укув юртларининг иктисодий мутахассисликлари учун дарслик.
2. Гафурова М.Т., Дадабаева Р.А. Персонал компьютерларнинг программ системалари.- Тошкент, ТДИУ, 1992.-100 бет.
3. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.

7. Амалиёт (семинар ва лаборатория) машғулотларнинг ишланмалари, уларни ўтказиш ва қўллаш бўйича услубий тавсиялар

Алишер Навоий номидаги
Самарқанд Давлат университети

“Ахборотлаштириш технологиялари” кафедраси

Ахатов А.Р.

Ахборотларни ҳимоялаш фанидан

амалиёт машғулотлари ишланмаси

САМАРҚАНД – 2019

№1-Лаборатория иши

Мавзу: Бевосита ўрин алмаштириш бўйича шифрлаш

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Симметрик криптотизимни асосий усулларини ўрганиш ва тадқиқ етиш.

Таянч иборалар: шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок, калит.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

Қисқача назарий маълумот:

Ўрин алмаштиришга мисол тариқасида дастлабки ахборот блокини матрисага қатор бўйича ёзишни, ўқишни еса устун бўйича амалга оширишни кўрсатиш мумкин. Матриса қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптотурғунлиги блок узунлигига (матриса ўлчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матриса ўлчами 8x8) учун калитнинг $1,6 \circ 10^9$ комбинасияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матриса ўлчами 16x16) калитнинг мумкин бўлган комбинасияси $1,4 \bullet 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЕҲМлар учун ҳам мураккаб ҳисобланади.

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

Масалан, «Ахборот хавфсизлиги жадвали» матни шифрлансин.

T_0=Ахборот хавфсизлиги жадвали;

К = 5x5; В=5;

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

T_1=АОФИД_ХТСГВ_БХИИА_ОАЗЖЛ_РВЛАИ

Биринчи бўлиб, шифрлаш жадвалидан (ХИВ асрнинг охирларида) дипломатик муносабатларда, харбий соҳаларда ахборотни муҳофазалашда фойдаланилган.

Оддий ўрин алмаштириш усулидан ташқари калит ёрдамида ўрин алмаштириш усули ҳам мавжуд. Шифрлаш жадвалидан калит орқали фойдаланилади.

Бу ерда калит символларига мос ҳолда жадвалнинг ўлчамига қараб НхМ жадвали тузилади ва очиқ матнни (T_0) устун бўйича жойлаштирилиб чиқилади. Сўнгра калит символлари алфавит тартибида тартибланиб, устун бўйича ўрин алмаштирилади, қатор бўйича ўқилиб шифрланган матнга (T_1) ега бўлинади ва блокларга бўлинади.

T_0= Ўзбекистон келажаги буюк давлат;

К = Тошкент;

В=4;

Матнда 28-та ва калитда 7-та ҳарфлар борлиги учун 7х7 жадвал тузамиз.

Ў	К	О	Л	Г	Ю	В
З	И	Н	А	И	К	Л
Б	С	К	Ж	Б	Д	А
Е	Т	Е	А	У	А	Т

Енди калит орқали 7х6 жадвал тузиб калитдаги ҳарфларни алфавит бўйича рақамлаб чиқамиз.

Т	о	ш	к	е	н	т
5	4	7	2	1	3	6
Ў	К	О	Л	Г	Ю	В
З	И	Н	А	И	К	Л
Б	С	К	Ж	Б	Д	А
Е	Т	Е	А	У	А	Т

Рақам бўйича устунларни ўзгартириб чиқамиз .

е	к	н	о	Т	т	ш
1	2	3	4	5	6	7
Г	Л	Ю	К	Ў	В	О
И	А	К	И	З	Л	Н
Б	Ж	Д	С	Б	А	К
У	А	А	Т	Е	Т	Е

Қатор бўйича 4 тадан блокларга бўлиб, символлар кетма-кетлигидаги шифрланган матнни оламиз. Шуни еътиборга олиш керакки, агар қаторда кетма-кет иккита бир хил ҳарф келса, чап тарафдан келаётган ҳарф биринчи рақамланади, кейин еса иккинчиси рақамланади ва шифрланган матн ҳосил қилинади.

T_1= ГЛЮК УВОИ АКИЗ ЛНБЖ ДСБА КУУА ТЕТЕ”;

Шифрни очишда тескари жараён амалга оширилади. Шифрланиш жараёни қадамма – қадам амалга оширилса мақсадга мувофиқ бўлади.

Икки томонлама ўрин алмаштириш усули. Бу усулда калит сифатида устун ва қатордаги ҳарфлар тартибидаги сонлардан фойдаланилади. Аввалам бор калит

символларига қараб жадвал тузилади, ва очиқ T_0 матн жойлаштирилиб чиқилади, сўнгра еса рақамлар навбатма – навбат тартибланиб, аввал устун, сўнгра еса қаторлар ўрни алмаштирилади ва жадвалдаги маълумот қатор бўйича ўқилиб T_1га ега бўлинади. Масалан: «Интилганга толе ёр» очиқ матни шифрлаш талаб етилсин. Бу ерда калит бўлиб 1342 ва 2314 хизмат қилади. Яхшироқ изоҳланиши учун $К_1$=1342 ва $К_2$=2314, В=4 деб белгилаб оламиз.

4х4 жадвал яратиб T_0 қатор бўйича ёзамиз:

	2	3	1	4
1	И	Н	Т	И
3	Л	Г	А	Н
4	Г	А	Т	О
2	Л	Е	Ё	Р

$К_2$

Енди қатор ва устунла $К_1$ бўйича ўринлари алмаштирилади.

	2	3	4	1
1	И	Н	Т	И
2	Л	Е	Ё	Р
3	Л	Г	А	Н
4	Г	А	Т	О

	2	3	4	1
1	И	И	Н	Т
2	Р	Л	Е	Ё
3	Н	Л	Г	А
4	О	Г	А	Т

Охирги жадвалга асосан шифрланган матнни ёзамиз ва блокларга бўлиб чиқамиз.

T_1 =ИИНТ_РЛЕЁ_НЛГА_ОГАТ

Икки томонлама алмаштиришда жадвал катталигига қараб вариантлар ҳам ортиб боради. Жадвал ўлчамининг катталиги шифр чидамлилигини оширади: 3х3 жадвалда 36 та вариант, 4х4 жадвалда 576 та вариант, 5х5 жадвалда 14400 вариант;

Мураккаб алмаштиришли шифр. Мураккаб алмаштиришли шифр кўп алфавитли бўлиб, шифрлашда келувчи матннинг хар бир ҳарфи ўзининг оддий алмаштириш шифри каби шифрланади. Кўп алфавитли алмаштиришда алфавит кетма-кетлиги ва сиклидан фойдаланилади.

А-алфавитли алмаштиришда кирувчи ахборотнинг $Х_0$-ҳарфи $В_0$-алфавитнинг $Й_0$-ҳарфи билан алмаштирилади, $Х_1$-харфи еса $В_1$-алфавитнинг $Й_1$-ҳарфи билан алмаштирилади, $Х_{р-1}$-харфи $В_{р-1}$-алфавитнинг $Й_{р-1}$-харфи билан алмаштирилади ва ҳоказо.

Кўп алфавитли алмаштиришнинг р=4 бўлган ҳол учун умумий кўриниши қуйидаги жадвалда келтирилган.

Кирувчи ҳарфлар	Х0	Х1	Х2	Х3	Х4	Х5	Х6	Х7	Х8	Х9
Алфавит алмаштириш	Б0	Б1	Б2	Б3	Б0	Б1	Б2	Б3	Б0	Б1

Бу усул билан шифрланган матнни очишда етарли қийинчиликлар туғдиради, енди к-калит бир-неча маротаба ўзгаради. Бунда душман ҳар бир матн бўлагини қандай

қилиб очишни бундай шифрлашда химояланганлик даражаси фойдаланиётган $B_ж$-алфавит кетма-кетлигига боғлиқдир. Кўп алфавитли алмаштириш шифрини Леон Батист Алъберт криптографияга киритди. 1566-йилда унинг “Трактат о шифре” китоби чиққан. Бутун дунёда кириптология (криптотаҳлил) асосини Л. Алъберт назарияси ташкил қилади.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларидан бирида шифрлансин ва қадамма – қадам изоҳлансин. Шунингдек **Делпи, ВБА, С++** ва **С#** дастурлаш тизимларидан бирида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

Иш мавзуси.

Ишдан мақсад.

Шифрлаш алгоритмини блок-схемаси.

Дастур матни.

Топшириқ вариантлари

- **ВАРИАНТ №1. «Самарқанд давлат университети»** сўзи оддий ўрин алмаштириш усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №2. «Самарқанд давлат университети»** сўзи Сезар усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №3. «Самарқанд давлат университети»** сўзи силжитиш ва кўпайтиришга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №4. «Самарқанд давлат университети»** сўзи кўпайтириш ва силжитишга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №5. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Жадвал устунлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №6. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Жадвал сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №7. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери силжитиш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №8. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери кўпайтириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №9. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери айириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №10. «Самарқанд давлат университети»** матни каррали силжитишга (силжитишлар символнинг жойлашган ўринлари номерига боғликда, масалан, калит к=3 да «Фан» сўзидаги «Ф» символи 3+1 га, «а» символи 3+2 га, «н» символи еса 3+3 га силжийди) асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №11. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №12. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда кўпайтириш алгоритми асосида шифрлансин ва шифр очилсин;

- **ВАРИАНТ №13. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда кўпайтириш ва силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №14. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Сатрлар ўрнига устунларни ёзиш орқали янги жадвал ҳосил қилинсин. Кейин еса сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №15. «Самарқанд давлат университети»** матни «сеҳирли квадрат» жадвали асосида шифрлансин ва шифр очилсин;

Назорат саволлари

1. Криптография мақсади ва вазифаси.
2. Оддий ўрин алмаштириш усули ва калит сўзли ўрин алмаштириш усули.
3. Икки марталик қайта қуйиш усули ва сеҳрли квадрат усули.
4. Сезар усули ва калит сўзли Сезар тизими.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компютера. М.: АБФ, 1997. – 336с.
2. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издателский дом «Вилямс», 2005г.-424с.
3. Петров А.А. «Компютерная безопасност. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблис Н. Курс теории чисел в криптографии. – М., Научное издателство ТВП, 2001й.
5. Масленников А. Практическая криптография БҲВ – СПб 2003й.
6. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
8. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

№2-Лаборатория иши

Мавзу: Полиалфавитли вижинер жадвалини (матрисасини) қўллаган ҳолда шифрлаш

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Симметрик криптотизимни асосий усулларини, жумладан, полиалфавитли вижинер жадвалини, ўрганиш ва дастурини ишлаб чиқиш.

Таянч иборалар: Вижинер, Сезар, жадвал, матриса, шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок. калит.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари *– 5 минут.*

Уйга вазифалар бериш *- 3 минут.*

Мавзу баёни

Қисқача назарий маълумот

Вижинернинг шифрлаш тизими. Биринчи бўлиб Вижинер тизими 1586-йилда чоп етилган ва у кўп алфавитли тизимга нисбатан юқорироқ ўринда туради. Блеза Вижинера ўзини ХВИ асрнинг француз дипломати деб ҳисоблайди. У криптография тизимига, яъни унинг ривожланишига ўз ҳиссасини қўшган. Вижинер тизими Сезар шифрлаш тизимига қараганда мукаммалроқ ҳисобланиб, унда калит ҳарфидан ҳарфга алмаштирилади. Бундай кўп алфавитли алмаштириш шифрини шифрлаш жадвали орқали ифодалаш мумкин. Қуйидаги биринчи жадвалда Вижинернинг инглиз алфавити учун мос келувчи жадвал кўрсатилган. Бу жадвалдан матнни шифрлаш ва уни очиш учун ишлатилади. Жадвалнинг иккита кириши бўлиб:

- Юқори қатордаги харфлардан кирувчи очиқ ёзув учун фойдаланилади.
- Чап устундан еса калит ҳарфларидан фойданилади.

Мисол учун калит кетма-кетлигини р-деб олайлик, у холда калит р-алфавитли р-сатрдан иборат бўлади.

$$\pi=(\pi_0, \pi_1,\ldots,\pi_{р-1});$$

Вижинернинг шифрлаш тизимида очиқ матн $х=(х_0,х_1,\ldots,х_{н-1})$ ва шифрланганн матн $й=(й_0,й_1,\ldots,й_{н-1})$ кўринишга ега. $\pi=(\pi_0, \pi_1,\ldots,\pi_{р-1})$ калит ёрдамида қуйидагича муносабатда бўлади.

$$х=(х_0,х_1,\ldots,х_{н-1}) \qquad й= (й_0,й_1,\ldots,й_{н-1});$$

$$(й_0,й_1,\ldots,й_{н-1})=(\pi_0(х_0),\pi_1(х_1),\ldots,\pi_{н-1}(х_{н-1}));$$

Юқоридаги ифодадан маълумки Вижинер жадвали орқали шифрлашда матннинг (ахборотнинг) хар бир ҳарфига мос келувчи калитнинг ҳар бир ҳарфи орқали уларнинг устун ва сатрлари кесишмасига мос келувчи ҳарфлар олинади.

Агар ўзбек алфавити ишлатилса, Вижинер матрисаси [36х36] ўлчамга ега бўлади (2.1. -расм).

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

2.1.- расм. Вижинер матрисаси.

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

1-қадам. Узунлиги М символли калит К ни танлаш.

2-қадам. Танланган калит К учун [(М+1),Р] ўлчамли шифрлаш матрисаси $Ц_х=(б_{иж})$ ни қуриш.

3- қадам. Дастлабки матннинг ҳар бир символи $с_{0р}$ тагига калит символи $к_м$ жойлаштирилади. Калит кераклича такрорланади.

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

1) К калитнинг алмаштирилувчи $с_{0р}$ символга мос $к_м$ символи аниқланади;
2) шифрлаш матрисаси $Ц_х$ даги $к_м = б_{ж1}$ шарт бажарилувчи и қатор топилади.
3) $с_{ор} = б_{и1}$ шарт бажарилувчи ж устун аниқланади....
4) $с_{ор}$ символи $б_{иж}$ символи билан алмаштирилади.

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

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

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

2-қадам. Шифрматндан $с_{1р}$ символлари ва мос калит символлари $к_м$ кетма-кет танланади. $Ц_х$ матрисада $к_м = б_{иж}$ шартни қаноатлантирувчи и қатор аниқланади. и-қаторда $б_{иж}= с_{1р}$ елемент аниқланади. Расшифровка қилинган матнда р - ўрнига $б_{иж}$ символи жойлаштирилади.

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

Агар калит сифатида <ВАЗА> сўзи танланган бўлса, шифрлаш матрисаси бешта қатордан иборат бўлади. (2.2. - расм)

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХСЧШЪЕЮЯЎҚҒҲ_
ВГДЕЁЖЗИЙКЛМНОПРСТУФХСЧШЪЕЮЯЎҚҒҲ_АБ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХСЧШЪЕЮЯЎҚҒҲ_
ЗИЙКЛМНОПРСТУФХСЧШЪЕЮЯЎҚҒҲ_АБВГДЕЁЖ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХСЧШЪЕЮЯЎҚҒҲ_

2.2. - расм. «Ваза» калити учун шифрлаш матрисаси.

Мисол. К= <ВАЗА> калити ёрдамида Т=<БАЙРАМ КУНИ> дастлабки матни шифрлансин.

Шифрматн $Т_1$ қуйидагича бўлади: ГАСРВМЖКХНП

Сезарнинг шифрлаш тизими. Алмаштириш усуллари сифатида қуйидаги усулларни келтириш мумкин: Сезар усули, Аффин тизимидаги Сезар усули, таянч сўзли Сезар усули ва бошқалар.

Сезар шифри оддий силжитиш шифрининг бир қисми ҳисобланади. Бу шифрни римлик олим Голе Юлий Сезар ўйлаб топган. Шифрлашда матннинг ҳар бир ҳарфи бошқа ҳарф билан қуйидаги қоида асосида алмаштирилади. Ҳарфларни алмаштиришда келаётган

ёзув ҳарфларини К-га силжитиб алмаштирилади. Бу ерда К–бутун сон ҳисобланиб уни қуйидагича ифодалаш мумкин. **К=Кмод(м), м** -алфавит сони . **Сезар усули**да алмаштирувчи харфлар к ва силжиш билан аниқланади. Юлий Сезар бевосита к = 3 бўлганда ушбу усулдан фойланган.

к = 3 бўлганда ва алифбодаги ҳарфлар м = 26 та бўлганда қуйидаги жалвал ҳосил қилинади:

Силжимаган алфавит	Силжиган алфавит	Силжимаган алфавит	Силжиган алфавит	Силжимаган алфавит	Силжиган алфавит
А	Д	Ж	М	С	В
В	Е	К	Н	Т	W
С	Ф	Л	О	У	Х
Д	Г	М	П	В	Й
Е	Ҳ	Н	Қ	W	З
Ф	И	О	Р	Х	А
Г	Ж	П	С	Й	Б
Ҳ	К	Қ	Т	З	С
И	Л	Р	У		

Масалан, матн сифатида КОМПУТЕР сўзини оладиган бўлсак, Сезар усули натижасида қуйидаги шифрланган ёзув ҳосил бўлади:

T_1 = НРПСХWҲУ.

Сезар усулининг камчилиги бу бир хил ҳарфларнинг ўз навбатида, бир хил ҳарфларга алмашишидир.

Аффин тизимидаги Сезар усулида ҳар бир ҳарфга алмаштирилувчи ҳарфлар махсус формула бўйича аниқланади: ат+б (мод м), бу ерда а, б - бутун сонлар, 0≤а, б<м.

м=26, а=3, б=5 бўлганда қуйидаги жадвал ҳосил қилинади:

Т	3т+5
0	5
1	8
2	11
3	14
4	17
5	20
6	23
7	26
8	29
9	32
10	35
11	38
12	41
13	44
14	47
15	50
16	53
17	56
18	59
19	62
20	65
21	68
22	71
23	74

Шунга мос равишда ҳарфлар қуйидагича алмашади:

А	Ф
Б	Ъ
В	Ь
Г	Э
Д	Ю
Е	Я
Ж	З
З	Қ
И	Ғ
Й	Ҳ
К	П
Л	Т
М	Х
Н	Б
О	Ф
П	Ж
Р	Н
С	Р
Т	В
У	З
Ф	Д
Х	Ҳ
Ц	Л
Ч	П
Ш	Т

24	77
25	80
26	83

Ў	Х

Натижада юқорида келтирилган матн қуйидагича шифрланади:

T_1=ПФХЖДЗСР

Калит сўзли Сезар тизими. Сезарнинг калит сўзли шифрлаш тизими битта алфавитли алмаштириш тизими ҳисобланади. Бу усулда калит сўзи орқали ҳарфларнинг суришда ва тартибини ўзгартиришда фойдаланади. Калит сўзини танлашда такрорланмайдиган ҳар хил ҳарфлардан иборат бўлган сўзни танлаш мақсадга мувофиқдир. Бу усул амалётда қўлланилмайди. Чунки калит сўзли Сезар шифрини кириптотаҳлил асосида очиш мумкин.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларидан бирида шифрлансин ва қадамма – қадам изоҳлансин. Шунингдек **ВБА** ёки **С++** дастурлаш тизимида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компютера. М.: АБФ, 1997. – 336с.
2. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издателский дом «Вилямс», 2005г.-424с.
3. Петров А.А. «Компютерная безопасност. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблис Н. Курс теории чисел в криптографии. – М., Научное издателство ТВП, 2001й.
5. Масленников А. Практическая криптография БҲВ – СПб 2003й.
6. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
8. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

Қўшимча адабиётлар

9. фтп://фтп.киае.су/мсдос/срйпто/пгп
10. ҳттп://драго.сентерлине.ком:8080/франл/пгп/…
11. Яҳоо - Компутерс, Сесуритй-анд-Енсрйптион

№3-Лаборатория иши

Мавзу: Гамилтон маршрутларига асосланган шифрлаш

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Компютердаги маълумотлар ҳимояси ва уларни қайта тиклаш.

Таянч иборалар: маршрутлар, символнинг тартиб рақами, шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок. Калит, дешифрлаш.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80+80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2+2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20+20 минут.*

Янги мавзу баёни: *-30+30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20+20 минут.*

Синов саволлари *– 5+5 минут.*

Уйга вазифалар бериш *– 3+3 минут.*

Мавзу баёни

Қисқача назарий маълумот:

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

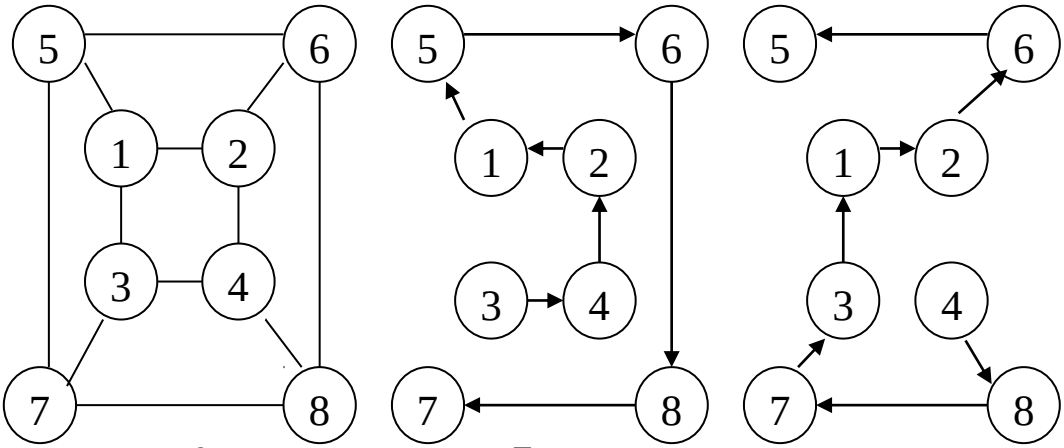
1-қадам. Дастлабки ахборот блокларга ажратилади. Агар шифрланувчи ахборот узунлиги блок узунлигига каррали бўлмаса, охирги блокдаги бўш ўринларга махсус хизматчи символлар-тўлдирувчилар жойлаштирилади (масалан, *).

2-қадам. Блок символлари ёрдамида жадвал тўлдирилади ва бу жадвалда символнинг тартиб рақами учун маълум жой ажратилади. (1 - расм)

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

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

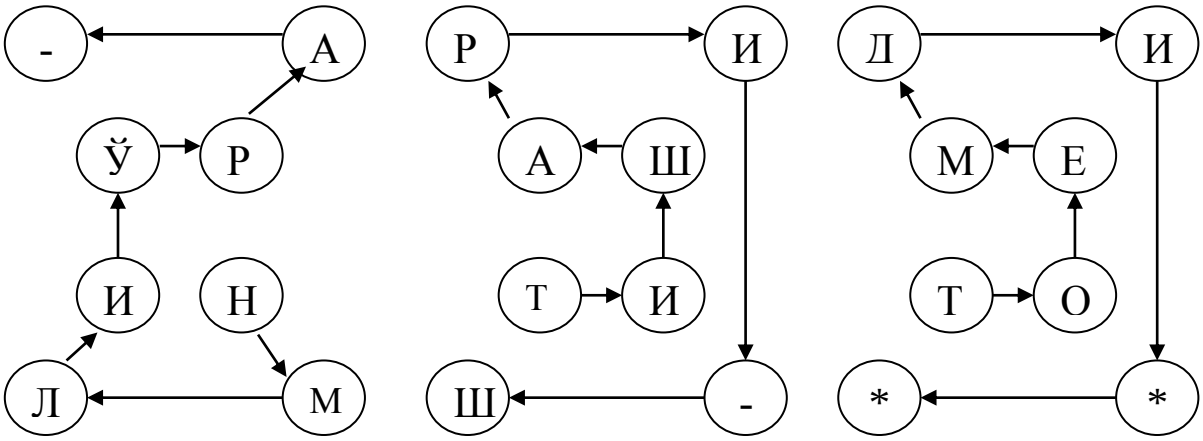
Дешифрлаш қилиш тескари тартибда амалга оширилади. Калитга мос ҳолда маршрут танланади ва бу маршрутга биноан жадвал тўлдирилади.



1-расм. 8-елементли жадвал ва Гамилтон маршрутлари вариантлари.

Жадвалдан символлар елемент номерлари келиши тартибида ўқилади.

Мисол. Дастлабки матн T_0 «Ўрин алмаштириш усули»ни шифрлаш талаб етилсин. Калит ва шифрланган блоклар узунлиги мос ҳолда қуйидагиларга тенг: К=<2,1,1>, Л=4. Шифрлаш учун 2.5-расмда келтирилган жадвал ва иккита маршрутдан фойдаланилади. Берилган шартлар учун матрисалари тўлдирилган маршрутлар 2.6-расмда келтирилган кўринишга ега.



2 - расм. Гамилтон маршрути ёрдамида шифрлаш мисоли.

1-қадам. Дастлабки матн учта блокка ажратилади. Б1=<Ўрин_алм>, Б2=<аштириш->, Б3=<усули**>;

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

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

T_1=<НМЛИЎРА_ТИШАРИ_ШТОЕМДИ**>

4-қадам. Шифрматнни блокларга ажратиш.

T_1=<НМЛИ ЎРА_ ТИША РИ_Ш ТОЕМ ДИ**>

3.Қўйилган вазифа:

Назарий келтирилган маълумот учун дастур ишлаб чиқилсин. Дастур **ВБА, С++** ёки С# дастурлаш тизимидан фойдаланган ҳолатда яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компютера. М.: АБФ, 1997. – 336с.
2. Нилс Фергюсон, Брюс Шнаер «Практическая криптография», М.: Издателский дом «Вилямс», 2005г.-424с.
3. Петров А.А. «Компютерная безопасност. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
4. Коблис Н. Курс теории чисел в криптографии. – М., Научное издателство ТВП, 2001й.
5. Масленников А. Практическая криптография БҲВ – СПб 2003й.
6. Шнаер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
7. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.

№4-Лаборатория иши
Мавзу: Очиқ калитли шифрлаш тизимлари
РСА, Эл-Гамал, Мак-Элис тизимлари

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади: Ассимметрик криптотизимлар дастурини ишлаб чиқиш.

Таянч иборалар: Очиқ калит, қайтарилмас ёки бир томонли функсиялар, маршрутлар, символнинг тартиб рақами, шифр ва шифрлаш, ўрин алмаштириш, блок, криптотурғунлик, ахборот, блок, калит, дешифрлаш, РСА, Эл-Гамал, Мак-Элис.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш – *3 минут.*

Мавзу баёни

Қисқача назарий маълумот: Очиқ калитли шифрлаш тизимларида иккита калит ишлатилади. Ахборот очиқ калит ёрдамида шифрланса, махфий калит ёрдамида дешифрлаш қилинади.

Очиқ калитли тизимларини қўллаш асосида қайтарилмас ёки бир томонли функсиялардан фойдаланиш ётади. Бундай функсиялар қуйидаги хусусиятларга ега. Маълумки x маълум бўлса у=ф(x) функсияни аниқлаш осон. Аммо унинг маълум қиймати бўйича x ни аниқлаш амалий жихатдан мумкин емас. Криптографияда яширин деб аталувчи йўлга ега бўлган бир томонли функсиялар ишлатилади. z параметрли бундай функсиялар қуйидаги хусусиятларга ега. Маълум z учун $Е_з$ ва $Д_з$ алгоритмларини аниқлаш мумкин. $Е_з$ алгоритми ёрдамида аниқлик соҳасидаги барча x учун $ф_з$ (x) функсияни осонгина олиш мумкин. Худди шу тариқа $Д_з$ алгоритми ёрдамида жоиз қийматлар соҳасидаги барча y учун тескари функсия x=$ф^{-1}$(y) ҳам осонгина аниқланади. Айни вақтда жоиз қийматлар соҳасидаги барча z ва деярли барча, y учун хатто $Е_з$ маълум бўлганида ҳам $ф^{-1}$(y)ни ҳисоблашлар ёрдамида топиб бўлмайди. Очиқ калит сифатида y ишлатилса, махфий калит сифатида x ишлатилади.

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

Очиқ калитли криптотизимлари бир томонли функсиялар кўриниши бўйича фарқлаш мумкин. Буларнинг ичида РСА, Эл-Гамал ва Мак-Элис тизимларини алохида тилга олиш ўринли. Ҳозирда енг самарали ва кенг тарқалган очиқ калитли шифрлаш алгоритми сифатида РСА алгоритмини кўрсатиш мумкин. РСА номи алгоритмни

яратувчилари фамилияларининг биринчи харфидан олинган (Ривест, Шамир ва Адлеман).

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

1-қадам. Иккита 200дан катта бўлган туб сон п ва қ танланади.

2-қадам. Калитнинг очиқ ташкил етувчиси н ҳосил қилинади

н=п қ.

3-қадам. Қуйидаги формула бўйича Ейлер функсияси ҳисобланади:

ф(п,к)=(п-1)(к-1).

Ейлер функсияси н билан ўзаро туб, 1 дан н гача бўлган бутун мусбат сонлар сонини кўрсатади. Ўзаро туб сонлар деганда 1 дан бошқа бирорта умумий бўлувчисига ега бўлмаган сонлар тушунилади.

4-қадам. ф(п,к) қиймати билан ўзаро туб бўлган катта туб сон д танлаб олинади.

5-қадам. Қуйидаги шартни қаноатлантирувчи е сони аниқланади

е д=1(модф(п,к)) .

Бу шартга биноан $e \cdot d$ кўпайтманинг ф(п,к) функсияга бўлишдан қолган қолдиқ 1га тенг. е сони очиқ калитнинг иккинчи ташкил етувчиси сифатида қабул қилинади. Махфий калит сифатида д ва н сонлари ишлатилади.

6-қадам. Дастлабки ахборот унинг физик табиатидан қатъий назар рақамли иккили кўринишда ифодаланади. Битлар кетма-кетлиги Л бит узунликдаги блокларга ажратилади, бу ерда Л – Л $\geq$ лог$_2$(н+1) шартини қаноатлантирувчи енг кичик бутун сон. Ҳар бир блок [0, н-1] оралиққа тааллуқли бутун мусбат сон каби кўрилади. Шундай қилиб, дастлабки ахборот Х(и), и=$\overline{1,I}$ сонларнинг кетма-кетлиги орқали ифодаланади. И нинг қиймати шифрланувчи кетма-кетликнинг узунлиги орқали аниқланади.

7-қадам. Шифрланган ахборот қуйидаги формула бўйича аниқланувчи Й(и) сонларнинг кетма-кетлиги кўринишида олинади:

$$Y(i) = (X(i))^e \pmod n.$$

Ахборотни дешифрлаш қилишда қуйидаги муносабатдан фойдаланилади:

Х(и)=(Й(и))^д (мод н).

Мисол. <ГАЗ> сўзини шифрлаш ва дешифрлаш қилиш талаб етилсин. Дастлабки сўзни шифрлаш учун қуйидаги қадамларни бажариш лозим.

1-қадам. п=3 ва қ=11 танлаб олинади.

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

3-қадам. Ейлер функсияси аниқланади.

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

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

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

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

000100 000001 001001.

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

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

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

У(1)=(4^7)(мод 33)=16384(мод 33)=16

У(2)=(1^7)(мод 33)=1(мод 33)=1

У(1)=(9^7)(мод 33)=4782969(мод 33)=15

Шифрланган сўз У(i)=<16,1,15>

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

$$У(1)=(16^3)(мод\ 33)=4096(мод\ 33)=4$$
$$У(1)=(1^3)(мод\ 33)=1(мод\ 33)=1$$
$$У(1)=(15^3)(мод\ 33)=3375(мод\ 33)=9$$

Дастлабки сон кетма-кетлиги дешифрлаш қилинган Х(и)=<4,1,9> кўринишида дастлабки матн <ГАЗ> билан алмаштирилади.

Эл-Гамал тизими чекли майдонларда дискрет логарифмларнинг ҳисобланиш мураккаблигига асосланган. РСА ва Эл-Гамал тизимларининг асосий камчилиги сифатида модул арифметикасидаги мураккаб амалларнинг бажарилиши заруриятини кўрсатиш мумкин. Бу ўз навбатида айтарлича ҳисоблаш ресурсларини талаб қилади.

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

Барча очиқ калитли шифрлаш методлари учун НП-тўлиқ масалани (тўлиқ саралаш масаласи) ечишга асосланган криптотахлил методидан бошқа методларининг йўқлиги қатъий исботланмаган. Агар бундай масалаларни ечувчи самарали методлар пайдо бўлса, бундай хилдаги криптотизим обрўсизлантирилади.

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

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

Шифрлашнинг ўзгарувчан алгоритмларини қўллаш тавсия қилинади. Бунда шифрлаш калити шифрлашнинг муайян алгоритмини танлаш учун ҳам ишлатилади.

Очиқ калитлардан фойдаланувчи шифрлаш методларининг афзаллиги, аввало, махфий калитларни тарқатиш заруриятининг йўқлигидир. Катта масофаларда тарқалган компютер тизимлари учун махфий калитларни тарқатиш айтарлича мураккаб масала ҳисобланади. Очиқ калитли тизимларнинг оммалашувига махфий калитларнинг фақат уларни тўлиқ саралаш орқали олинишидан бошқа йўл билан олиб бўлмаслиги исботининг йўқлиги тўсқинлик қилади.

Стеганогрфия ахборотни криптоҳимоялашнинг истиқболли йўналишларидан ҳисобланади. Стеганография билан шифрлашни биргаликда (комплекс) ишлатилиши махфий ахборот криптотурғунлигини айтарлича оширади.

3. Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларидан бирида шифрлансин ва қадамма – қадам изоҳлансин. Шунингдек **ВБА** ёки **С++** дастурлаш тизимида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Шифрлаш алгоритмини блок-схемаси.
4. Дастур матни.

Назорат саволлари

1. Очиқ калитли шифрлаш тизимлари.
2. РСА криптотизимининг моҳияти.
3. Ел-Гамал ва МакЕлис криптотизимининг моҳияти.
4. Шифрлаш стандартлари.

Фойдаланилган адабиётлар

1. Желников В. Криптография от папируса до компютера. М.: АБФ, 1997. – 336с.
2. Зубанов Ф. WИНДОWС НТ-выбор “профи”. – М.: Издателский отдел “Русская Редаксия” ТОО “Чанел Трединг Лтд.”, 1996.
3. Баричев С. Криптография без секретов. М.: "ДИАЛОГ-МИФИ", - 1995.

№5-Лаборатория иши

Мавзу: Компютер тизимларининг вируслар билан заҳарланиш профликаси

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади: Компютер тизимларида вирувслар ва уларнинг ҳимояси.

Таянч иборалар: тармоқ, вирус, махсус дастур, анитвируслар, детекторлар, фаглар, ваксиналар, прививкалар, ревизорлар, мониторлар, Аидстест, Достор Wеб, НОД, КАВ.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

Компютер вируси – бу махсус ёзилган дастур бўлиб, бошқа дастурлар таркибига ёзилади, яъни зарарлайди ва компютерларда ўзининг ғаразли мақсадларини амалга оширади.

Компютер вируси орқали зарарланиш окибатида компютерларда қуйидаги узгаришлар пайдо бўлади:

- айрим дастурлар ишламайди ёки хато ишлай бошлайди;
- бажарилувчи файлнинг хажми ва унинг яратилган вақти узгаради;
- екранда англаб бўлмайдиган белгилар, турли хил тасвир ва товушлар пайдо бўлади;
- компютернинг ишлаши секинлашади ва тезкор хотирадаги буш жой хажми камаяди;
- диск ёки дискдаги бир неча файллар зарарланади (баъзи холларда диск ва файлларни тиклаб бўлмайди):
- винчестер орқали компютернинг ишга тушиши йўқолади.

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

Детекторлар — вируснинг сигнатураси (вирусга тааллуқли байтлар кетма-кетлиги) бўйича тезкор хотира ва файлларни кўриш натижасида маълум вирусларни топади ва хабар беради. Янги вирусларни аниқлаб олмаслиги детекторларнинг камчилиги хисобланади.

Фаглар — ёки докторлар, детекторларга хос бўлган ишни бажарган ҳолда зарарланган файлдан вирусларни чиқариб ташлайди ва файлни олдинги холатига кайтаради.

Ваксиналар — юқоридагилардан фарқли равишда ҳимояланаётган дастурга урнатилади. Натижада дастур зарарланган деб ҳисобланиб, вирус томонидан ўзгартирилмайди. Фақатгина маълум вирусларга нисбатан ваксина қилиниши унинг камчилиги ҳисобланади. Шу боис хам, ушбу антивирус дастурлари кенг тарқалмаган.

Прививка — файлларда худди вирус зарарлагандек из қолдиради. Бунинг натижасида вируслар «прививка қилинган» файлга ёпишмайди.

Филтрлар — қуриқловчи дастурлар куринишида бўлиб, резидент ҳолатда ишлаб туради ва вирусларга хос жараёнлар бажарилганда, бу ҳақда фойдаланувчига хабар беради.

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

Детектор дастурлар компютер хотирасидан, файллардан вирусларни қидиради ва аниқланган вируслар хақида хабар беради.

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

Филтр дастурлар компютер ишлаш жараёнида вирусларга хос бўлган шубҳали ҳаракатларни топиш учун ишлатилади.

Бу харакатлар қуйидагича бўлиши мумкин:

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

Текширувчи (ревизор) дастурлари вирусдан ҳимояланишнинг енг ишончли воситаси бўлиб, компютер зарарланмаган ҳолатидаги дастурлар, каталоглар ва дискнинг тизим майдони ҳолатини хотирада саклаб, доимий равишда ёки фойдаланувчи ихтиёри билан компютернинг жорий ва бошлангач ҳолатларини бир-бири билан солиштиради. Бунга АДИНФ дастурини мисол қилиб келтириш мумкин.

Компютер тизимларида хавф-хатарсиз ишлашнинг амалда синаб кўрилган ва юқори самара берган асосий қоидалари қуйидагилар.

Биринчи қоида. Қонуний расмий йўл билан олинган программ маҳсулотлардан фойдаланиш.

Иккинчи қоида. Ахборотни иккилаш. Аввало программ таъминотнинг дистрибутив елтувчиларини сақлаш лозим. Ишчи ахборотнинг сақланишига катта еътибор бериш лозим.

Учинчи қоида. Вирусга қарши воситалардан мунтазам равишда фойдаланиш лозим. Ишни бошламасдан аввал программа-сканерлар ва программа-тафтишлар ишлатилиши керак. Вирусларга қарши воситаларнинг мунтазам равишда янгиланиб турилиши шарт.

Тўртинчи қоида. Айниқса ахборотнинг янги елтувчиларидан ва янги файллардан фойдаланишда еҳтиёт бўлиш лозим. Янги дискеталар уларда юклама файлли вирусларнинг йўқлиги нуқтаи назаридан сўзсиз текширилиши шарт.

Бешинчи қоида. Тақсимланган тизимлар ёки жамоа фойдаланувчи тизимлар билан ишлаганда янги алмаштириладиган ахборот елтувчилар ва тизимга киритилувчи файллар махсус ҳисоблаш машинасида текширилиши лозим.

Вирусга қарши ҳар томонлама текшириш амалга оширилганидан кейингина дисклар ва файллар тизимдан фойдаланувчиларга узатилиши мумкин.

Олтинчи қоида. Елтувчига ахборот ёзиш кўзда тутилмаган бўлса, бу амални бажарилишига йўл қўйиш керак емас. Бунинг учун 3,5 дюмли дискетларда квадрат тешик очиш кифоя.

Юқорида келтирилган тавсияларга риоя қилиш программ вируслар билан захарланиш ехтимолини айтарлича камайтиради ва фойдаланувчини ахборотни йўқотишдан сақлайди.

Компютер вирусларига карши курашнинг қуйидаги турлари мавжуд:

- вируслар компютерга кириб бузган файлларни ўз ҳолига қайтарувчи дастурларнинг мавжудлиги;
- компютерга парол билан кириш, диск юритувчиларнинг ёпиқ туриши;
- дискларни ёзишдан ҳимоялаш;
- лисензион дастурий таъминотлардан фойдаланиш ва ўғирланган дастурларни қўлламаслик;
- компютерга кириталаётган дастурларнинг вирусларнинг мавжудлигини текшириш;
- антивирус дастурларидан кенг фойдаланиш;
- даврий равишда компютерларни антивирус дастурлари ёрдамида вирусларга қарши текшириш.

Антивирус дастурларидан ДрWеб, Адинф, АВП, ВоотСҲК ва Нортон Антивирус, Касперскй Сесуритй кабилар кенг фойлаланилади.

НАЗОРАТ САВОЛЛАРИ

1. Компютер вируслари қандай аломатлари бўйича классификасияланади?
2. «Стелс»-вируслар ва полиморф вирусларнинг таъсири принсипини тушунтиринг.
3. Файл вируси ва унинг таъсири алгоритмини тушунтиринг.
4. Макровирус ва юклама вируслар таъсири алгоритми қандай?
5. Вирусларни аниқлаш методлари.
6. Вируслар таъсири оқибатларини йўқотиш методлари.
7. Компютер системаларининг вируслар билан захарланишининг олдини олувчи профилактик чоралар кетма-кетлигини санаб ўтинг.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Завгородний В.И. Комплексная защита информасии в компютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
2. Столинс, Вилям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.- М.: Издателский дом «Вилямс», 2002. 432 с.
3. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

№6 - Лаборатория иши

Мавзу: Тармоқни бошқариш қисм тизимида ахборотни ҳимоялаш

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Тармоқни бошқариш қисм тизимида ахборотни ҳимоялашнинг асосий усулларини ўрганиш ва тадқиқ етиш.

Таянч иборалар: тармоқ, ҳалқаро стандарт-ТСП/ИП ва Х.25 протоколлар, протоколларнинг сатҳ моделлари.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

1.Ишдан мақсад: Компютердаги маълумотлар ҳимояси ва уларни қайта тиклаш.

2.Қисқача назарий маълумот:

Ахборотларни узатиш бошқариш протоколлари деб аталувчи маълум қоидалар бўйича амалга оширилади. Ҳозирда компютер тармоқларида тармоқнинг узоқлаштирилган елементлари ўртасидаги алоқа иккита ҳалқаро стандарт-ТСП/ИП ва Х.25 протоколлари ёрдамида амалга оширилади.

ТСП/ИП протоколи асосида Интернет тармоғи қурилган. Х.25 протоколига пакетларни коммутасиялаш асосида қурилган маълумотларни узатиш технологиясининг ривожи сифатида қараш мумкин. Х.25 протоколи очиқ тизимларнинг ўзаро алоқаси модели ОСИ га мувофиқ ҳалқаро стандартлаш ташкилоти ИСО томонидан яратилган. Х.25 моделида тармоқнинг барча вазифалари 7 сатҳга ажратилса, ТСП/ИП моделида 5 сатҳ мавжуд.

Х.25 протоколи узоқлаштирилган жараёнлар ўртасида юқори ишончли алоқани таъминлай олади. ТСП/ИП протоколининг афзаллиги сифатида тармоққа уланишнинг соддалигини ва нархининг пастлигини кўрсатиш мумкин.

OSI модели

Татбиқий
Тақдимий
Сеанс
Транспорт
Тармоқ

TCP/IP модели

Татбиқий
Транспорт
Тармоқ

Каналли
Физикавий

Каналли
Физикавий

1 - расм. Протоколларнинг сатҳ моделлари.

Тармоқда ахборотни ҳимоялашни таъминлаш масаласи барча сатҳларда амалга оширилади. Протоколларнинг бажарилиши бошқариш қисм тизими томонидан ташкил етилади.

3.Қўйилган вазифа:

1. Ахборот хавфсизлиги масалалари ҳам ечиладиган тармоқни бошқарувчи ягона бошқариш марказини яратиш.
2. Тармоқнинг барча обектларини рўйхатга олиш ва уларнинг ҳимоясини таъминлаш. Идентификаторларни тақдим етиш ва барча тармоқдан фойдаланувчиларни ҳисобга олиш.
3. Тармоқ ресурсларидан фойдаланишни бошқариш.
4. Калитларни шакллантириш ва уларни компютер тармоқ абонентларига тарқатиш.
5. Трафикни (тармоқдаги ахборотлар оқимини) мониторинглаш, абонентларнинг ишлаш қоидаларига риоя қилишларини назоратлаш, бузилишларга тездан ўз муносабатини билдириш.
6. Тармоқ елементларининг ишлаши бузилганида уларнинг ишлаш қобилиятини тиклашни ташкил етиш.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Назарий қисм.

4. Назорат саволлари

1. Тармоқ қандай қисм тизимларига ажратилади.?
2. Коммуникасион қисм тизимининг таркиби.
3. Тармоқда информасияни ҳимоялаш тизимини яратишда нималарни ҳисобга олиш зарур?
4. Фойдаланувчи қисм тизимида информасия ҳимоясини таъминлаш қандай амалга оширилади?
5. Ихтисослаштирилган коммуникасион компютер тизимларида информасия ҳимояси қандай таъминланади.
6. Тармоқни бошқариш қисм тизимида информасияни ҳимоялаш.
7. Тармоқлараро екранлашнинг моҳиятини тушунтиринг.
8. Ўзаро алоқада бўлган жараёнларнинг ҳақиқийлигига қандай ишонч ҳосил қилинади?
9. Коммуникасион қисм тармоқ орқали олинувчи информасиянинг сохта емаслигининг тасдиғига қандай еришилади?

Фойдаланилган адабиётлар

1. Гук М. Аппаратные средства ИБМ ПС. Енсиклопедия. - СПб.: Питер, 2002, - 928 с.
2. Мииаси М. Модернизасия и обслуживание персоналного компютера. Базовый курс. - М.; Век, 2000. - 592 с.
3. Завгородний В.И. Комплексная защита информасии в компютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
4. Столинс, Вилям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.-М.: Издателский дом «Вилямс», 2002. 432 с.
5. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информасия ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77

№7 Лаборатория иши
Мавзу: Компютер вирусларининг таснифланиши

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Компютер вируслари ва улардан ҳимояланиш тизимларини таҳлил етиш ва ўрганиш.

Таянч иборалар: вирус, тармоқли, файлли, юкланадиган ва файлли-юкланадиган, чувалчанг, резидентли ва резидентли бўлмаган.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80+80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2+2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20+20 минут.*

Янги мавзу баёни: *-30+30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20+20 минут.*

Синов саволлари – *5+5 минут.*

Уйга вазифалар бериш – *3+3 минут.*

Мавзу баёни

Ҳозирги вақтда 60000 тадан ортиқ дастурли вируслар маълумдир. Уларни қуйидаги белгилар бўйича таснифлаш мумкин:

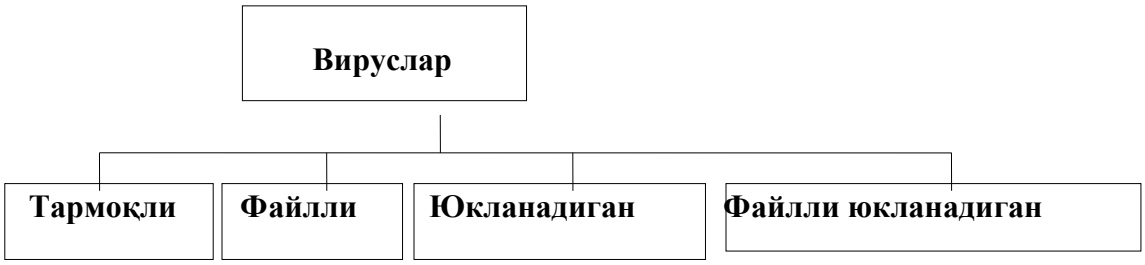
а) яшаш муҳити бўйича;

б) зарарлантириш усули бўйича;

в) таъсир етиши бўйича;

г) алгоритмнинг хусусиятлари бўйича;

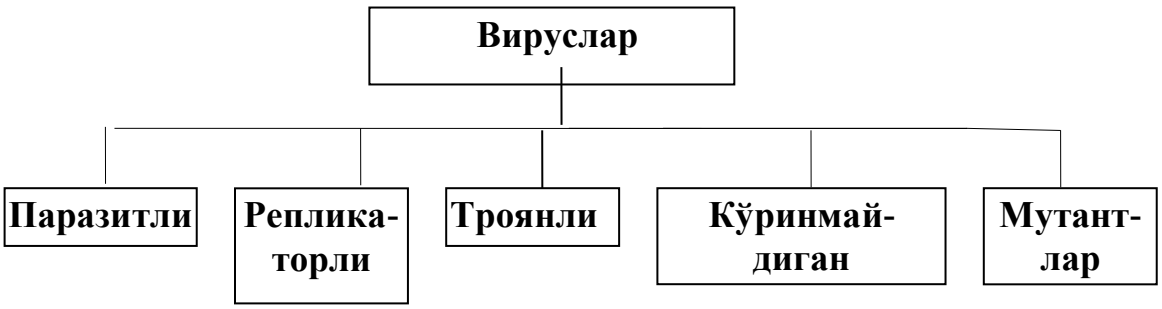
А) Яшаш муҳити бўйича вирусларнинг таснифлаши



Б) Зарарлантириш усули бўйича вирусларнинг таснифланиши

В) Таъсир етиш даражаси бўйича вирусларнинг таснифланиши

Г) Алгоритмларнинг хусусиятлари бўйича вирусларнинг таснифланиши



Яшаш муҳитига боғлиқ равишда вирусларни тармоқли, файлли, юкланадиган ва файлли-юкланадиган турларга бўлиш мумкин.

Тармоқли вируслар турли компютер тармоқлари бўйича тарқаладилар. Дискетадан емас, балки локал ёки глобал тармоқдан тарқатиладиган бу вируслар бажарадиган дастурларни зарарлантирмайдилар. Улар ҳимоя қилишнинг тармоқ воситалари орқали кириб олиш учун мослашганлар ва тармоқда юқори тарқалиш тезлигига егадир.

Тармоқли вирусларнинг енг кенг тарқалган тури компютер “чувалчанглари” ҳисобланади, улар дастурли коднинг “бошқа жинсли” қисми бўлиб, компютер тармоғини барча участкаларида юқори тезликда тарқаладилар.

Компютер “чувалчанглари” тизимнинг жиддий бузилишларига олиб келмайди. Вирус “чувалчанг” сифатида Worm дастурини келтириш мумкин, у ўзининг нусхаларини тарқатиш учун ўзининг дастурли кодини Интернет тармоғи бўйича електрон хабарларга иловалар кўринишида жўнатади. Бу вирус бажариладиган HAPPУ99. EXE файлида жойлашади.

Файлли вируслар асосан бажариладиган модулларга, яъни .COM ва .EXE кенгайтмаларга ега бўлган файлларга, татбиқ қилинади. Файлли вируслар бошқа турдаги файлларга ҳам татбиқ қилиниши мумкин, лекин бунда улар бошқаришни узатадилар, ва,

демак, кўпайиш қобилиятини йўқотадилар. Файлли вируслар компютердан компютерга файлларда кўчиб ўтадилар ва юқори зарарлантириш хоссасига ега.

Зарарланган дастурни ҳар сафар ишга туширилганда вируснинг ўз-ўзини нусхалаши бўлиб утади.

Юкланадиган вируслар- дискнинг юкланадиган секторига (Воот сектор) ёки тизимли дискни юклаш дастурини ўз ичига олган секторга (Мастер Боот Ресорд) татбиқ қилинади. Улар файлли вируслардан шуниси билан фарқланадики, тизимдан тизимга юкланадиган сектор орқали кўчиб ўтади ва дискеталарни ва қаттиқ дискларни фақат Боот-секторларини зарарлантиради. Бу вирусли дастурлар кичик ўлчамларга ега (512 байтдан ошиқроқ).

Файлли юкланадиган вируслар - файлларни ҳам, дискларнинг юкланадиган секторларини ҳам зарарлантиради. Бу турдаги вирусларни яратиш учун одатда, мураккаб алгоритмлар ва технологиялар ишлатилади.

Зарарлантириш усули бўйича вируслар резидентли ва резидентли бўлмаган бўлади.

Резидентли вирус компютерни зарарлантирганда тезкор хотирада ўзининг резидентли қисмини қолдиради, бу қисм кейин операсион тизимни зарарланган обектларга (файлларга, дискларнинг юкланадиган секторларига) мурожаатини ушлаб олади ва уларга татбиқ қилинади. Резидентли вируслар хотирада жойлашади ва компютерни ўчиргунгача ёки қайта юклагунгача фаол ҳисобланади.

Резидентли бўлмаган вируслар компютер хотирасини зарарлантирмайдилар ва чегараланган вақт ичида фаол ҳисобланади.

Таъсир етиш даражаси бўйича вирусларни қуйидаги кўринишларга бўлиш мумкин

1. Хавфсиз - улар компютер ишлашига тўсиқ бермайдилар, лекин бўш тезкор хотирани ва дисклардаги хотираларни сиғимини камайтиради, бундай вирусларнинг ишлаши бирорта графикли ёки товушли самараларда намоён бўлади.

2. Хавфли - улар компютер ишлашида турли бузилишларга олиб келиши мумкин.

3. Жуда хавфли - уларнинг таъсирида дастурлар йўқолади, маълумотлар ўчиб кетади, дискнинг тизимли соҳаларидаги ахборотлар ўчирилиб юборилади.

Алгоритмнинг хусусиятлари бўйича вирусларни уларнинг турли-туманлигини катталиги туфайли таснифлаш мушкулроқдир.

Паразитли вируслар оддийроқдир, улар файлларнинг ва диск секторларининг мазмунини ўзгартирадилар, ва етарлича енгил пайқалиши ва йўқотилиши мумкин.

Чувалчанглар деб аталадиган вирус репликаторларни таъкидлаш керакки, улар компютер тармоқлари бўйича тарқаладилар, тармоқ компютерларининг манзилларини ҳисоблайдилар ва бу манзиллар бўйича ўзларининг нусхаларини ёзадилар.

Стелс-вируслар деб аталадиган кўринмайдиган вируслар мавжуд бўлиб, уларни пайқаш ва зарарлантириш жуда мушкулдир, чунки улар операсион тизимни зарарланган файлларга ва дискларнинг секторларига мурожаат қилишни ушлаб оладилар ва ўзининг танасини ўрнига дискнинг зарарланмаган қисмларини қўяди.

Шифрлаш-қайта шифрлаш алгоритмларини ўз ичига олган вирус-мутантларни пайқаш жуда мушкулдир, шу алгоритмлар ҳисобига бир хил вируснинг нусхалари битта ҳам такрорланмайдиган байтлар занжирига ега емас.

Квазивирусли ёки “троянли” дастурлар деб аталадиган вируслар ҳам мавжуддир, улар ўз-ўзидан тарқалиш хоссасига ега бўлмасада, лекин жуда хавфлидир, чунки улар фойдали дастур остида ниқобланиб, юкланадиган секторни ва дискларнинг файлли тизимини бузадилар.

Компютер вирусларидан ҳимоя қилиш усуллари

Компютер вирусларидан ҳимоя қилишнинг учта чегараси мавжуддир:

- вирусларни кириб келишини бартараф етиш;
- агар вирус барибир компютерга кирган бўлса, вирус ҳужумини бартараф етиш;
- агар ҳужум барибир амалга ошган бўлса, бузувчи оқибатларни бартараф етиш.
- ҳимоя қилишни амалга оширишни учта усули мавжуддир:
- ҳимоя қилишнинг дастурли усуллари;

- ҳимоя қилишнинг аппаратли усуллари;
- ҳимоя қилишнинг ташкилий усуллари.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: “касалликни даволагандан кўра унинг олдини олган яхшироқ”. Афсуски, айнан у енг бузувчи оқибатларни келтириб чиқаради. Компютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустахкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум - бу муҳим маълумотларни йўқотишни ягона бўлмаган ва хаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операсион тизимни ишдан чиқариши мумкин, ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқациз қилиб қўйиш қобилиятига егадирлар. Ўғирлаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда компютерни йўқотиш еҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда “охиридан” бошлаш керак - исталган таъсирни, у вирус ҳужуми, хонада ўғрилик ёки қаттиқ дискни физик ишдан чиқиши бўлишидан қатъий назар, бузувчи оқибатларини бартараф етишдан бошлаш керак.

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

Вирусга қарши ҳимоя қилиш воситалари

Ахборотни ҳимоя қилишнинг асосий воситаси енг муҳим маълумотларни захирали нусхалаш ҳисобланади. Юқорида санаб ўтилган сабабларнинг исталгани бўйича ахборотни йўқотиш ҳолатида қаттиқ дисклар қайта форматланади ва янгидан ишлатишга тайёрланади. ”Тоза” форматланган дискка дистрибютив ихчам-дискдан операсион тизим ўрнатилади, кейин еса унинг бошқаруви остида барча керакли дастурли таъминот ўрнатилади, уларни ҳам дистрибютив ташувчилардан олинади. Компютерни тиклаш захирадаги ташувчилардан олинадиган маълумотларни тиклаш билан якунланади.

Маълумотларни захиралашда яна шуни инобатга олиш керакки, барча рўйхатдан ўтган ва паролли маълумотларни, Интернетнинг тармоқли хизматларига мурожаат қилиш учун, алоҳида сақлаш керак. Уларни компютерда сақламаслик керак. Одатдаги сақлаш жойи - бўлим рахбарининг сейфидаги хизмат кундалигидир. Ахборотни захирали нусхалаш бўйича тадбирлар режасини тузиб олиб захирали нусхалар компютерда алоҳида сақланиш кераклигини инобатга олиш керак. Яъни масалан, ўша компютернинг алоҳида қаттиқ дискида ахборотни захиралаш фақатгина хавфсизлик иллюзиясини яратади.

Муҳим, лекин махфий бўлмаган маълумотларни нисбатан янги ва етарлича ишончли усули уларни Интернетда узоклашган серверларда Web-папкаларда сақлаш ҳисобланади. Фойдаланувчи маълумотларини сақлаш учун бўш жойни (бир неча Мбайтгача) текинга берадиган хизмат турлари мавжуддир.

Ахборотни ҳимоя қилишнинг ёрдамчи воситалари вирусга қарши дастурлар ва аппаратли ҳимоя қилиш воситалари ҳисобланади. Масалан, бош платада уланиш жойини оддийгина ўчириб қўйиш ДЕҚҚ сини қайта дастурланадиган (флеш - БИОС) микросхемасини ўчиришни амалга ошириш имконини бермайди, бунда бу ишни ким амалга оширишига: компютер вирусими, ёмон ниятли кишими ёки тартибсиз фойдаланувчими бунга боғлиқ емасдир.

Вирусга қарши ҳимоя қилишнинг етарлича кўп дастур воситалари мавжуддир.

Вирусдан ҳимоя қилиш учун ишлатиш мумкин:

- ахборотни ҳимоя қилишнинг умумий воситалари, улар магнит дискларини физик бузишдан кафолатлаш, каби, нотўғри ишлайдиган дастурлар ёки фойдаланувчиларнинг нотўғри ҳаракатлари каби фойдалидир;
- вирус билан зарарланиш еҳтимолини камайтириш имконини берадиган профилактик чоралар;

- вируслардан ҳимоя қилиш учун махсус дастурлар.

Ахборотни ҳимоя қилишни умумий воситалари вирусдан ҳимоя қилиш учун фойдали емас. Бу воситаларнинг иккита асосий тури мавжуддир:

-**ахборотни нусхалаш** - файллар ва дискларнинг тизимли соҳаларини нусхаларини яратиш;

-**мурожаат қилишни чеклаш** -тақиқланган ахборотни ишлатишни бартараф етиш, хусусан, вируслардан дастурларни ва маълумотларни ўзгаришлардан ҳимоя қилишдан, нотўғри ишлайдиган дастурлардан ва фойдаланувчиларнинг нотўғри ҳаракатларидан ҳимоя қилишдан.

Ахборотни ҳимоя қилишни умумий воситалари вируслардан ҳимоя қилиш учун жуда муҳимлигига қарамасдан, уларнинг ўзлари етарли емас. Вируслардан ҳимоя қилиш учун махсус дастурларни қўллаш ҳам керакдир.

Бу дастурларни бир нечта турларга бўлиш мумкин: детекторлар, ваксина (иммунизаторлар), докторлар (ораш), тафтишчилар (файлларда ва дискларнинг тизимли соҳаларида ўзгаришларни назорат қилиш дастурлари), доктор-тафтишчилар ва филтрлар (вируслардан ҳимоя қилиш учун дастурлар).

Вируслардан компютерларни ва маълумотларни хавфсизлигига хисса қўшиш бўйича биринчи ўринда, шубхасиз, маълумотларни нусхалаш, ҳисобланади. Вирус билан компютер зарарланганда ҳали ҳам ҳеч бўлмаганда маълумотларнинг бир қисмини тиклаш мумкин, лекин агар компютерда қаттиқ диск бузилса, унда нима қилмоқ керак? Бундан ташқари, нусхалари архивда мавжуд бўлган дастурлар ва маълумотлар исталганча бузилганда, қўшимча уларни турли “докторлар” билан даволашни амалга оширишга интилмасдан, архивдан тўғри нусхаларни нусхалаш мақсадга мувофиқдир.

Хавфсизликка ҳисса қўшиш бўйича иккинчи ўринга маълумотларга мурожаат қилишни чеклашни қўйиш мумкин. Агар аксарият кўпчилик ишлатиладиган дастурлар тўплами ёзишдан ҳимоя қилинган мантиқий дискда жойлашган бўлса, унда вирус билан зарарланганда бу тўпламлар бузилмайдилар ва зарарланиш оқибатларини бартараф етиш учун нисбатан кам уринишлар талаб етилади.

Тафтишчилар дастури- (вирус билан зарарланишни олдиндан пайқаш) учинчи ўринда турадилар, улар дастурларнинг ва маълумотларнинг бутунлигини аниқлайдилар. Бундай текшириш вируснинг борлигини, у ҳам кўп нарсаларни бузишга улгурмасдан олдин, енг бошланғич босқичда пайқаш имконини беради.

Филтрлар дастури тўртинчи ўринда туради. Бу дастурлар кўплаб вирусларни (ҳаммасини бўлмаса ҳам), улар хали кўп нарсаларни бузишга ёки зарарлантиришга улгурмасдан олдин, енг бошланғич босқичда пайқаш имконини беради. Антивирус ва Флу Шот Плус туридаги дастурлар филтрлар дастурига тегишлидир.

Детекторлар дастури - бешинчи ўринда турадилар, улар янги олинган дастур таъминотида вирусларнинг мавжудлигини текшириш учун ишлатилади.

Докторлар дастури- (фаглар) олтинчи ўринда (умуман биринчида емас) жойлашган. Уларни, бузилган дастурни нусхаси архивда бўлмаганда, ва уни бошқа усул билан олиш қийин бўлган ҳоллардагина қўллаган маъқулроқ. Бундан ташқари, агар дастур-фаг ишлатилаётган бўлса, унда кейин тикланган файлни дастур-тафтишчи билан албатта текшириш керак бўлади (тушунарлики, агар бу файл тўғрисидаги ахборот олдиндан сақланган бўлса), лекин ҳар доим ҳам дастур-доктор тўғри даволайвермайди.

Ва ниҳоят, енг охирги ўринда **ваксиналар доктори** жойлашган. Дунёда минглаб вируслар мавжуд бўлган шароитларда айнан компютер зарарланадиган вирусдан файлни ҳимоя қилиш ехтимоли жуда ҳам кичкинадир. Бундан ташқари, дастурни ёзувдан ҳимоя қилинган дискетага жойлаштириш янада самаралироқдир.

Жуда кўп фойдаланувчилар таъкидламоқдаларки, вируслардан ҳимоя қилиш учун вирусларни пайқайдиган ва уларни йўқотадиган дастурларни иложи борича кўпроқ (яъни детекторлар дастурини ва докторларни) йиғиш керак, ҳимоя қилишнинг бошқа чораларини инобатга олмаслик мумкин: вирус қачон пайдо бўлса, унда бу дастурлардан тўғри келадиган “дорини” танлаш балки мумкин бўлади. Шу билан бирга вирусдан

келадиган зарарни камайтириш учун тиббиёт ходимлари қадимдан гапириб келаётган қоидага риоя қилиш керак: «касални даволагандан кўра унинг олдини олган яхшироқ».

Вирус билан зарарланишга қарши профилактика

Бу параграфда компютерни вирус билан зарарланиш еҳтимолини камайтириш, ҳамда, агар барибир вирус билан зарарланиш бўлиб ўтган бўлса, ундан келадиган зарарни минимумга олиб келиш чоралари кўриб чиқилади. Албатта, вирус билан зарарланишга қарши профилактика учун кўриб чиқилган барча воситаларни емас, балки фақатгина сиз керакли деб ҳисоблаган воситаларнигина ишлатиш керак.

1. Ўзгартирмайдиган файлларни ўзида сақлаган дискеталарда ёзувдан ҳимоя қилувчи кесилган жойини елимлаб қўйиш керак. Қаттиқ дискда ёзувдан ҳимоя қилинган мантиқий дискни яратиш ва унга ўзгартирилмасдан, фақат ишлатиладиган дастурларни ва файлларни жойлаштириш керак.

2. Вирусдан ҳимоя қилиш учун резидентли филтрлар дастурини доимо, мумкин бўлган ҳамма вақтда ишлатиш мақсадга мувофиқдир.

3. Дискеталарнинг юкланадиган секторлари орқали тарқаладиган вирус билан зарарланишдан халос бўлиш учун қаттиқ дискдан компютерни қайта юклашдан олдин А: дисководда бирорта дискета йўқлигига ишонч ҳосил қилинг. Агар у ерда дискета бор бўлса, унда қайта юклашдан олдин дисковод ешигини очиб қўйинг.

4. Агар сиз компютерни дискетадан қайта ишлашни хохласангиз, фақатгина операсион тизимли ёзишдан ҳимоя қилинган “еталон” дискетадан фойдаланинг.

5. ДОС бошланғич юкланганда бажариладиган АУТОЕХЕС.ВАТ буйруқли файлига, параметр сифатида файлларнинг унча катта бўлмаган рўйхатини кўрсатган ҳолда, файлларда ўзгаришларни текшириш учун тафтишчи-дастурни чақиришни қўйиш мақсадга мувофиқдир.

6. Сиз яратган ёки ўзгартирган файлларни даврий равишда архивлаш керак. Файлларни архивлашдан олдин, компютерда вирус йўқлигига ишонч ҳосил қилиш ва архивга бузилган ёки зарарланган файлларни жойлашишидан халос бўлиши учун, вирус борлигини аввалроқ диагностика қилиш учун дастурни бажариш мақсадга мувофиқдир.

7. Бошқа компютерлардан дастур таъминотини кўчириб ёзиш керак емас, чунки у вирус билан зарарланган бўлиши мумкин.

8. Сиз бирорта дастур маҳсулотини ёки ҳужжатни олганингиздан ёки ишлаб чиққанингиздан кейин мос файлларнинг еталонли архивли нусхасини яратишингиз керак, унинг ёрдамида бу файлларни компютер вирус билан зарарланганда енгилгина тиклаш мумкин бўлади.

9. Ташқаридан олиб келинган дискеталарни ишлатишдан олдин детектор -дастур ёрдамида вирус борлигига текшириш керак. Буни хаттоки, сиз бу дискеталарда фақатгина маълумотли файлларни ишлатишни истаган ҳолатларингизда ҳам фойдалидир - сиз вирусни қанчалик тез пайқасангиз, шунчалик яхшидир.

10. Компютерда ишлашга бегона шахсларни, айниқса агар улар ўзларининг дискеталарига ега бўлмасалар, қаровсиз қолдирмасдан рухсат бермаслик керак. Жуда кўп ҳолларда компютерни вирус билан зарарланиш сабаби дискетада олиб келинган, кимдир уни компютерда 10-15 минут ўйнаган компютер ўйини ҳисобланади. Агар компютерга тасодифий шахсларни мурожаат қилишдан халос бўлишнинг имкони бўлмаса (масалан, ўқув марказида), компютернинг қаттиқ дискида жойлашган барча ёки деярли барча дастурларни ёзишдан ҳимоя қилинган дискда жойлаштирилган мақсадга мувофиқдир.

11. Агар компютер қаттиқ дискка ега бўлса, ҳар доим ишончли жойда “тизимли” дискетага, яъни ДОС операсион тизимини юклаш мумкин бўлган дискетага ега бўлиш керак.

12. Турли компютер вирусларини пайқаш ва йўқотиш учун дастурларни йиғиб бориш керак. Бу дастурларни ишончли жойда сақланиш керак бўлган дискетага жойлаштириш керак. Бу дискета билан биргаликда уни ишлатиш бўйича йўриқномани сақлаш мақсадга мувофиқдир. Дастурларни танлаб олишда “миқдор сифатни алмаштирмайди” деган қоидани ёддан чиқармаслик керак ва фақатгина:

- ўзига яхши тавсиянома берган;
- вирусларнинг кенг диапазонига ёки бошқа дастурлар билан “ушлаб олинмайдиган” вирусларга мўлжалланган;
- ўзларида вируслар йўқлигига текширилган дастурларни йиғиш керак

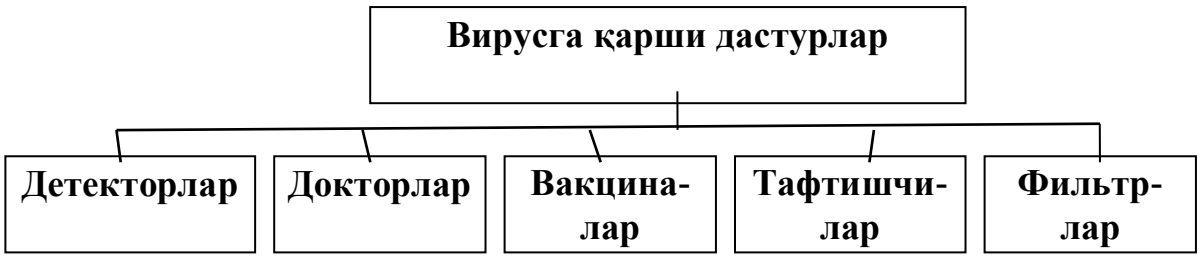
Вирусларни пайқаш ва улардан ҳимоя қилиш дастурлари ва уларнинг тавсифлари

Компютер вирусларини пайқаш, ўчириш ва улардан ҳимоя қилиш учун махсус дастурларнинг бир нечта турлари ишлаб чиқилган, улар вирусларни пайқаш ва йўқотиш имконини беради. Бундай дастурлар **вирусга қарши** дастурлар деб аталади.

Вирусга қарши дастурларнинг қуйидаги турлари мавжуд:

1) детекторлар дастури;
2) докторлар дастури ёки фаглар;
3) тафтишчилар дастури;
4) филтрлар дастури;
5) ваксиналар дастури ёки иммунизаторлар.

Вирусга қарши дастурларнинг турлари



Детекторлар дастури маълум бир вирус учун тавсифли бўлган байтлар кетма-кетлигини (вирус сигнатуралари) тезкор хотирада ва файлларда қидиришни амалга оширилади, ва вирусни пайқаганда мос хабарни беради. Бундай вирусга қарши дастурларнинг камчилиги шундаки, улар фақат бундай дастурларнинг ишлаб чиқувчиларига маълум бўлган вирусларнигина топа оладилар.

Докторлар дастури ёки **фаглар,** ҳамда **ваксиналар дастури** нафақатгина вируслар билан зарарланган файлларни топмасдан, балки уларни “даволайди” ҳам, яъни файлдан вирус-дастур танасини ўчирадилар, файлларни бошланғич ҳолатга қайтарадилар. Фаглар ўзининг ишини бошида тезкор хотирада вирусларни қиди-ради, уларни йўқотади ва фақат кейингина файлларни “даволашга” ўтади. Фаглар орасида **ярим фагларни** ажратиш мумкин, улар катта миқдордаги вирусларни қидириш ва йўқотиш учун мўлжалланган докторлар дастуридир. **Аидстест, Ссан, Нортон Антивирус** ва **Достор Web** енг машҳур полифаглар ҳисобланадилар. Янги вируслар доимо пайдо бўлиб боришини инобатга олиб, детекторлар дастури ва докторлар дастури тезда ескирадилар, ва уларнинг версияларини доимо янгилаб бориш талаб етилади.

Тафтишчилар дастури вируслардан ҳимоя қилишнинг енг ишончли усулларига тегишлидир. Тафтишчилар, компютер вирус билан зарарланмаганда, каталогларнинг дастурларини ва дискнинг тизимли соҳаларини бошланғич қийматини еслаб қоладилар, кейин еса даврий равишда ёки фойдаланувчининг хохиши бўйича жорий ҳолатни бошланғич ҳолат билан таққослайди. Пайқалган ўзгаришлар видеомонитор екранига

чиқарилади. Қоидага кўра, ҳолатларни тақ-қослаш опкрасион тизим юклангандан кейин бирданига амалга оширилади. Таққослашда файл узунлиги, циклик назорат қилиш коди (файлнинг назорат йиғиндиси), ўзгартириш санаси ва вақти, бошқа параметрлар текширилади. Тафтишчилар дастури етарлича ривожланган алгоритмларга ега, стелс-вирусларни пайқайдилар, ва ҳаттоки текширилаётган дастурдаги версияларини ўзгаришларини вирус томонидан киритилган ўзгаришлардан фарқини пайқайдилар.

Россияда кенг тарқалган **“Диалог-Наука”** фирмасининг **Адинф** дастури тафтишчилар дастури қаторига киради.

Филтрлар дастури ёки “қоровуллар”- компютер ишлашида вируслар учун тегишли бўлган шубҳали ҳаракатларни пайқаш учун мўлжалланган, унча катта бўлмаган резидентли дастурлардир. Бундай ҳаракатлар бўлиши мумкин:

1) .COM ва .EXE кенгайтмали файлларни тўғрилашга интилишлар;

2) файллар атрибутларини ўзгартириш;

3) абсолют манзил бўйича дискка тўғридан-тўғри ёзиш;

4) дискнинг юкланадиган секторларига ёзиш;

5) резидент дастурни юклаш.

Бирор дастур томонидан кўрсатилган амалларни бажаришга интилиш бўлганда “қоровул” фойдаланувчига хабар юборилади ва мос амалларни таъқиқлашни ёки рухсат беришни таклиф етади. Филтрлар дастури жуда фойдалидир, чунки улар вирусни уни пайдо бўлишини бошланғич босқичларида, кўпайгунга кадар пайқаш қобилиятига егадир. Аммо улар файлларни ва дискларни “даво-ламайдилар”. Вирусларни йўқотиш учун бошқа дастурларни, масалан фагларни, қўллаш талаб етилади. Дастур-қоровулларнинг камчиликларига уларнинг жонга тегишини “(масалан, улар бажарилаётган файлни нусхалашга ихтиёрий интилиш тўғрисида доимо огоҳлантириб турадилар), ҳамда бошқа дастур таъминоти билан мумкин бўлган келишмовчиликларни келтириш мумкин. Дастур-филтрга мисол тариқасида МС ДОС операсион тизимининг утилитларини тўпламини таркибига кирувчи **Всафе** дастурини келтириш мумкин. [25; 112-119]

Ваксиналар ёки иммунизаторлар - файлларни зарарланишини бартараф етувчи резидентли дастур ҳисобланади. Ваксиналарни вирусни “даволайдиган” дастур докторлар йўқ бўлганда қўлланилади. Ваксиналаш фақатгина маълум бўлган вируслардан мумкиндир. Ваксина дастурни ёки дискни шундай ўзгартирадики, бу уларнинг ишлашида акс еттирилмайди, вирус еса уларни зарарланган деб қабул қилади ва шунинг учун татбиқ етилмайди. Ҳозирги вақтда ваксиналар дастури чекланилган қўлланишга ега.

Вируслар билан зарарланган файллар ва дискларни ўз вақтида пайқаш, ҳар бир компютерда пайқалган вирусларни тўлиқ йўқотиш вирус епидемиясини бошқа компютерларга тарқалишини олдини олиш имконини беради.

Компютер вирусларидан ҳимоя қилиш учун асосий чоралар

Компютерни компютер вируслари билан зарарланишини олдини олиш ва дискларда ахборотларни ишончли сақлашни таъминлаш учун қуйидаги қоидаларга риоя қилиш керак:

- компютерни замонавий вирусга қарши дастурлар, масалан Аидстест ёки Достор Web, билан таъминланг ва уларнинг версияларини доимо янгилаб боринг;

- бошқа компютерларда ёзилган ахборотларни дискетадан ўқишдан олдин ўзингизни компютердаги вирусга қарши дастурни ишга тушириб бу дискеталарни вирус борлигига доимо текширинг;

- ўзингизни компютерингизга архивланган кўринишдаги файлларни кў-чириб ўтишда, текшириш соҳасини ҳозиргина ёзилган файллар билан чеклаган ҳолда, уларни қайта архивлангандан кейин тезда қаттиқ дискда текширинг;

- олдиндан ОТ ни ёзишдан ҳимоя қилинган тизимли дискетадан юклаб, файлларни, хотираларни ва тизимли соҳаларни ёзишдан ҳимоя қилинган дискетадан вирусга қарши

дастурларни ишга тушириб компютернинг қаттиқ дискларини вируслар борлигига даврий равишда текшириб боринг;

- бошқа компютерда ишлаганда ўзингизни дискетани, агар уларга ахборотни ёзиш амалга оширилмаса, ёзишдан ҳар доим ҳимоя қилинг;

- Сиз учун муҳим бўлган ахборотларни архивли нусхаларини дискеталарда албатта ишлаб чиқинг;

- компютерни юкланадиган вируслар билан зарарланишини олдини олиш учун операсион тизимни қайта юклашда ёки компютерни улашда А: дисководда дискетани қолдирманг;

- компютер тармоқларидан олинадиган барча бажарадиган файлларни назорат қилиш учун вирусга қарши дастурларни ишлатинг.

- Аидстест ва Достор Web дастурларини қўллашни юқори хавф-сизлигини таъминлаш учун **Адинф** диск текширувчисини ҳар куни ишлатиб бориш керак.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Компютер вирусларидан ҳимоя қилиш учун асосий чоралар, Ваксиналар ёки иммунизаторлар, Филтрлар дастури ёки “қоровуллар”, Тафтишчилар дастури, Докторлар дастури, Детекторлар дастури, Вирус билан зарарланишга қарши профилактика мавзуларини ўрганиг ва улар ҳақида маълумотлар тўпланг.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Асосий маълумотлар.
4. Умумий хулосалар.

Назорат саволлари

1. Компютер вируси нима ва унинг табиати қандай?
2. Вирусларни компютерга кириб боришини асосий йўллари қандай?
3. Компютер вирусларини зарарлари нималарда намоён бўлади?
4. Сизларга компютер вирусларини қандай асосий кўринишлари маълум?
5. Вирусларни пайқаш ва улардан ҳимоя қилиш учун дастурларнинг қандай турлари мавжуд?
6. Детекторлар дастури ва докторлар дастурининг фарқлари ва ўхшаш жойлари нимада?
7. Тафтишчилар дастурининг ва филтрлар дастурининг афзалликлари нималарда намоён бўлади?
8. Компютер вирусларидан ҳимоя қилиш бўйича асосий чораларни айтиб беринг.
9. Дастур маҳсулотларини ҳимоя қилиш нима учун керак?

№8 Лаборатория иши
Мавзу: Антивирус дастурлари ва уларнинг вазифалари

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади:

Антивирус дастурлари, уларнинг вазифалари билан танишин ва уилардан фойдаланиш.

Таянч иборалар: Аидстест, Достор Web полифаг дастури, мураккаб вируслар мутантлар, Евристик таҳлил, Адинф, Адинф Суре Модуле даволовчи блоки

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

A. Аидстест дастури - полифаг

Аидстест - бу жуда ҳам кенг тарқалган 1300 дан ортиқ компютер вирусларини пайқаш ва йўқотиш имкониятига ега бўлган дастурдир. Аидстест версиялари янги вируслар тўғрисидаги ахборот билан доимий равишда янгиланиб ва тўлдирилиб бормоқда.

Аидстест ни ишга тушириш учун қуйидаги буйруқни бериш керак:

Аидстест <патҳ>[<оптионс>]

бу ерда: **патҳ** - диск номи, тўлиқ ном, файл спесификасияси, файллар гуруҳининг ниқоби:

*- қаттиқ дискнинг барча бўлимлари

**- тармоқ ва СДРОМ дискларини қўшган ҳолда барча дисклар.

Оптионс - қуйидаги калитларнинг исталган комбинасияси:

F- зарарланган дастурларни тўғрилаш ва бузилганларини ўчириш;

G- барча файлларни кетма-кет текшириш (фақатгина .COM, .EXE ва СЙС ларни емас);

H- бузилган вирусларни қидириш учун секин ишлаш;

X- вирус таркибида бузилишлар бўлган барча файлларни ўчириш;

Q- бузилган файлларни ўчиришга рухсат сўраш;

R- кейинги дискектани қайта ишлашни таклиф етмаслик.

Мисол 1. **АИСТЕСТ В: /Ф/Г/Қ**

B: дискни “даволаш” ва текшириш учун вирусга қарши Аидстест дастурини ишга тушириш, пайқалган зарарланган дастурлар тўғриланади. Агар файлни тўғрилашга имкон бўлмаса, унда дастур уни ўчиришга рухсат сўрайди.

Достор Web полифаг дастури

Бу дастур, енг аввало, компютер оламида нисбатан яқинда пайдо бўлган полиморфли вируслар билан курашиш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун мўлжалланган. Дискларни текшириш ва пайқалган вирусларни ўчириш учун Др.Web ни ишлатиш Аидстест дастурига тўлиқ ўхшашдир. Бунда текширишни дублаш деярли бўлмайди, чунки Аидстест ва Др.Web дастурлари вирусларнинг турли тўпламлари билан ишлайди.

Др.Web дастури Аидстест кучи етмайдиган мураккаб вируслар мутантлар билан самарали курашиши мумкин. Аидстест дан фарқли равишда Др.Web дастури хусусий дастурли коддаги ўзгаришларни пайқаш, ҳамда “ваксинали беркитишни” енгиб ўтган ҳолда шифрланган ва ихчамлаштирилган файлларга кириб янги, нўмалум вируслар билан зарарланган файлларни самарали аниқ-лаш қобилиятига егадир. Бу кучли евристик таҳлилчи мавжудлиги ҳисобига еришилади.

Евристик таҳлил режимида Др.Web дастури вируслар учун характерли бўлган янги ёки унга номаълум вирусларни пайқашга интилиб файлларни ва дискларнинг тизимли соҳаларини тадқиқот етади. Агар шундай вируслар топилса, унда обект номаълум вирус билан зарарланганлиги тўғрисида огоҳлантириш берилади.

Евристик таҳлилни учта даражаси кўзда тутилган. Евристик таҳлил режимида ёлғон ишлашлар, яъни зарарланмаган ҳисобланмаган файлларни детекторлаш мумкиндир. “Евристика” даражаси ёлғон ишлаш мавжуд бўлмаган кодни таҳлил қилиш даражаси кўринишига егадир. Евристик таҳлилчининг ишлашини биринчи иккита даражаси тавсия етилади.

Евристик таҳлилни учинчи даражаси файлларни яратилишини “шубхали” вақтига уларни қўшимча текширишни кўзда тутади. Файллар зарарланишида баъзи бир вируслар ушбу файлларнинг зарарганлик белгиси каби яратилишнинг нотўғри вақтини ўрнатади. Масалан, зарарланган файллар учун секундлар 62 қийматга ега бўлиши мумкин, яратилиш йили еса 100 йилга кўпайтирилиши мумкин.

Вирусга қарши Др.Web дастурини етказиб бериш таркибига яна унинг имкониятларини кенгайтирадиган дастурнинг асосий вирусли тўпламига файл қўшимчалар ҳам кириши мумкин.

Др.Web дастури билан икки режимда ишлаш мумкин:

- меню ва мулоқот ойнасини ишлатиб тўлиқ екранли интерфейс режимида;
- буйруқ қатори орқали бошқариш режимида.

Доимий бўлмаган бир марталик қўллаш учун биринчи режим қулайроқдир, лекин дискеталарнинг доимий киришини назорат қилиш мақсадида доимий қўллаш учун яхшиси иккинчи режимини қўллаган маъқулдир.

Иккинчи режимни ишлатганда Др.Web нинг мос ишга тушириш буйруғи Нортон Соммандер операсион қобиғини фойдаланувчисини менюсига ёки махсус буйруқли файлга киритилган бўлиши мумкин.

Др.Web ни ишга тушириш учун буйруқ қатори қуйидаги кўринишга ега:

Др.Web [диск:] [йўл] [калитлар]

бу ерда **диск:** - қаттиқ дискни мантиқий қурилмаси ёки егилувчан дискни физик қурилмаси, масалан, Ф: ёки А:

*- қаттиқ дискдаги барча мантиқий қурилмалар;

йўл - бу талаб етилаётган файлларнинг йўли ёки ниқоби.

Енг муҳим калитлар:

/ АЛ-берилган қурилмадаги барча файлларнинг диагностикаси;

/ СУ [П] - дискларни ва файлларни “даволаш”, топилган вирусларни ўчи-риш;

Р- фойдаланувчининг тасдиқлаши билан вирусларни ўчириш;

/ ДЛ-тўғрилаб даволашни имкони бўлмаган файлларни ўчириш;

/ НА [даража]- файлларни евристик таҳлил қилиш ва уларда номаълум вирусларни қидириш, бу ерда [даража] 0,1,2 қийматларни қабул қилиш мумкин;

/ СЛ - буйруқли қатор режимида дастурни ишга тушириш, файлларни ва тизимли соҳаларни тестлашда тўлиқ екранли интерфейс ишлатилмайди;

/ ҚУ- тестлашдан кейин тезда ДОС га чиқиш.

Агар Др.Web нинг буйруқли қаторида бирорта ҳам калит кўрсатилмаган бўлса, унда жорий сўров учун барча ахборот ДРWЕБ. ЕХЕ жойлашган каталогда жойлашган ДРWЕБ.ИНИ конфигурасия файлидан ўқилади. Конфигурасия файли тестлаш учун зарур бўлган параметрларни сақлаш буйруғи ёрдамида Др.Web дастури билан ишлаш жараёнида ишлатиладиМисол-2: **ДрWеб Б: / АЛ/ СУП/ ҲА1/ҚУ/СЛ**

В: дискни текшириш ва даволаш учун Др.Web вирусга қарши дастурини ишга тушириш.

Тўлиқ екранли интерфейс режимида Др. Web дастури билан ишлаш технологияси

Тўлиқ екранли интерфейс режимида ишга тушириш учун буйруқ қаторига фақат дастур номини киритиш етарлидир. Дастур юкланган кейин компютернинг тезкор хотирасини тестлаш, агар у компютернинг олдинги ўрнатилишида ўчирилмаган бўлса, бошланади. Тестлашнинг бориши тестлаш ойнасида акс еттирилади. Хотирани унинг тугагандан кейин тўхташ амалга оширилади. Дастур ишлашини, агар екраннинг юқори қаторида жойлашган асосий менюдан фойдаланилса, давом еттириш мумкин. Менюни фаоллаштириш учун Ф10 клавишини босиш керак. Асосий меню қуйидаги режимларга ега:

Др.Web ТЕСТ НАСТРОЙКИ ДОПОЛНЕНИЯ

Исталган режимни танлашда мос қисмменю очилади.

Др.Web қисмининг менюси ДОС га вақтинчалик кириш, Др.Web дас-тури ва унинг муаллифи тўғрисида қисқача ахборотни олиш ёки дастурдан чиқиб кетиш имконини беради.

ТЕСТ қисм менюси файлларни тестлашни ва “даволашни” асосий амалларини бажариш, ҳамда бажарилган ишлар тўғрисида ҳисоботларни кўриб чиқиш имконини беради.

Настройки қисмининг менюси мулоқот ойналари ёрдамида дастурни созлаш параметрларини ўрнатиш, қидиришни йўлларини ва ниқобларини ўрнатиш ва параметрларни ДРWЕБ.ИНИ конфигурасия файлида сақлаш учун хизмат қилади.

ДОПОЛНЕНИЯ қисмининг менюси дастурнинг асосий вирусли базасига, унинг имкониятларини кенгайтирадиган файл-қўшимчаларни қўшиш учун ишлатилади.

Дискнинг вирусга қарши тафтишчиси Adinf

Адинф тафтишчиси стелс-вирусларни, вирус-мутантларни ва бугунги кунгача номаълум вирусларни қўшган ҳолда исталган вирусларни пайдо бўлишини пайқаш имконини беради.

Адинф дастури еслаб қолади:

- юкланадиган секторлар тўғрисидаги ахборотни;
- бузилган кластерлар тўғрисидаги ахборотни;
- файлларнинг узунлиги ва назорат йиғиндиларини;
- файлларни яратилиш санаси ва вақтини.

Компютерни бутун ишлаши давомида Адинф дастури бу тавсифларни сақланганлигини кузатиб боради. Ҳар кунги назорат қилиш режимида Адинф дастури

компютер биринчи марта уланганда автоматик равишда ишга туширилади. Айниқса вирусга ўхшаш ўзгаришлар кузатиб борилади, улар тўғрисида тезда огоҳлантириш берилади. Файлларнинг бутунлиги назорат қилишдан ташқари Адинф дастури қисм каталогларни яратишни ва ўчиришни, файлларни яратишни, силжитишни ва қайта номлашни, янги бузуқ кластерларни пайдо бўлишини, юкланадиган секторларини сақлаганлигини ва кўплаб бошқа нарсаларни кузатади. Вирусни тизимга татбиқ қилиш учун мумкин бўлган барча жойлар ёпиб қўйилади. Адинф дастури, ДОС ни ишлатмасдан БИОС га тўғридан-тўғри мурожаат қилиб дискни секторлари бўйича ўқиган ҳолда текширади.

Adinf Scype Module даволовчи блоки

Adinf Scype Module - бу компютерни янги вирусдан “даволашга” ёрдам берадиган дастур бўлиб, у вирус маълум бўлган Аидстест ёки Др.Веб полифагларни янги версияларини кутиб турмайди. Адинф Суре Модуле дастури, вирусларни кўплаб турлари борлигига қарамасдан уларни файлларга татбиқ қилишни унчалик кўп бўлмаган турлича усуллари мавжудлиги далилини ишлатади. Меъёрий ишлаш вақтида, доимий равишда ишга туширишда Адинф тафтишчиси Адинф Суре Модуле дастурига охирги марта ишга туширилгандан бери қайси файллар ўзгарганлиги тўғрисида хабар беради. Адинф Суре Модуле дастури бу файлларни таҳлил қилади ва ўзининг жадвалларига, вирус билан зарарланганда файлларни тиклаш учун керак бўладиган, ахборотни ёзиб қўяди. Агар зарарланиш бўлиб ўтган бўлса, унда Адинф тафтишчиси ўзгаришларни пайқайди ва Адинф Суре Модуле дастурини яна чақиради, у зарарланган файлни таҳлил қилиш ва уни ёзиб қўйилган ахборот билан таққослаш асосида файлнинг бошланғич ҳолатини тиклашга ҳаракат қилади.

Дастур маҳсулотларини ҳимоя қилиш

Дастур маҳсулотлари бир қатор сабабларга кўра ҳимоя қилишнинг муҳим обекти ҳисобланади.

Биринчидан, улар юқори малакали мутахассисларнинг, баъзида ўнлаб ҳаттоки юзлаб кишиларнинг интеллектуал меҳнати маҳсулоти ҳисобланади.

Иккинчидан, бу маҳсулотларни лойиҳалаш жараёни моддий ва меҳнат ресурсларини сезиларли ҳаракатлари билан боғлангандир, қимматбахо компютер жиҳозларини ва илмий-техникавий технологияларни ишлатишга асосланган.

Учинчидан, бузилган дастур таъминотини тиклаш анчагина меҳнат сарфини талаб етади, ҳисоблаш техникаси жиҳозларини ишламай туриб қолиш еса ташкилотлар ва жисмоний шахслар учун нохуш натижаларга олиб келиши мумкин.

Дастур маҳсулотларини ҳимоя қилиш қуйидаги мақсадларни кўзда тутади:

- фойдаланувчиларнинг алоҳида тоифаларини дастур маҳсулотлари билан ишлаш учун тақиқланган мурожаат қилишни чеклаш;
- маълумотларни қайта ишлашни меъёрда олиб бориш мақсадида дастурларни олдиндан режалаштирилган бузилишини инкор қилиш;
- дастур маҳсулотини ишлаб чиқарувчиларни нуфузини бузиш мақсадида дастурларни олдиндан режалаштирилган ўзгартирилишни инкор қилиш;
- дастурларни тақиқланган ададлашни (нусхалашни) инкор қилиш;
- дастурларни мазмунини, таркибини ва ишлаш механизмини тақиқланган ўрганишни инкор қилиш.

Дастур маҳсулотлари турлича обектларнинг кишини, техник воситаларни, махсус дастурларни, атроф муҳитни ва бошқаларни тақиқланган таъсирларидан ҳимоя қилиниши керак.

Кишилар дастур маҳсулотига шу дастур маҳсулотини ҳужжатларини ёки машина ташувчисининг ўзини ўғрилаш ёки физик йўқотиш, дастур воситаларини ишлаш қобилиятини бузиш йўли билан таъсир етиши мумкин.

Техник воситалар (аппаратура) компютерга ёки узатувчи муҳитга уланиш йўли билан дастурларни ўқиш, қайта шифрлаш, ҳамда уларни физик бузишни амалга ошириши мумкин.

Махсус дастурлар ёрдамида дастур маҳсулотини вирус билан зарарлантириш, уни тақиқланган нусхалаш, унинг маъносини рухсациз ўрганиш ва амалга ошириши мумкин.

Ва нихоят, **атроф-муҳит** аномал ҳодисалар ёрдамида (електромагнит нурланишни кўпайиши, ёнғин, сув тошқини ва бошқалар.) дастур маҳсулотини физик бузиш амалга оширилиши мумкин.

Дастур маҳсулотларини ҳимоя қилишни енг оддий ва мумкин бўлган усули уларга қуйидаги усуллар билан мурожаат қилишни чеклаш ҳисобланади:

- дастурлар ишга тушганда уларни парол билан ҳимоя қилиш;
- калит дискетани ишлатиш;
- компютернинг киритиш - чиқариш портига уланадиган махсус техник қурилмани (електрон калитни) ишлатиш.
- дастурларни тақиқланган нусхалашдан сақлаш мақсадида ҳимоя қилишнинг махсус дастурли воситалари:
- дастур ишга тушириладиган муҳитни идентификасиялаш;
- рухсат етилган инсталлясияларни ва нусхалашларни бажарилишини миқдорини ҳисобини олиб бориш;
- тизимларнинг ишлаш алгоритмларини ва дастурларини ўрганишга қарши туриш (хаттоки ўз-ўзини бузишгача) керак.
- дастур маҳсулотлари учун самарали ҳимоя қилиш чоралари қуйидагилар ҳисобланадилар:
- ишга туширадиган дискетани ностандарт шакллантириш;
- қаттиқ дискда дастурларни жойлашган жойини қатъий белгилаш;
- киритиш-чиқариш портига қўйиладиган електрон калитга боғланиш;
- БИОС номерига боғланиш ва бошқалар.
- Дастур маҳсулотларини ҳимоя қилиш ҳуқуқий усуллар билан ҳам албатта амалга оширилиши керак, уларнинг қаторига келишувлар ва шартномаларни, патентли ҳимоя қилишни, муаллифлик ҳуқуқини, технологик ва ишлаб чиқариш махфийлигини ва бошқаларни киритиш мумкин.

Компютер тизимларини ривожланиши билан янада янги компютер вируслари пайдо бўлмоқда, шунга мос равишда турли хил антивирусли тизи,млар ва воситалар ҳам пайдо бўлмоқда. Одатда вируслар компютер тизимида сақлаётган дастур таъминотини маълумотларни ўзгартиради ёки йўқ килади. Зарар келтирадиган дастурларга биологик вирусларнинг хоссалари киради.

Компютер вирусларини шаклларини ва турли - туманлигини кўп қирралилиги тавсифли схемаларда турли хил белгилар бўйича келтирилгандир. Айниқса «мантиқий бомбалар», «троян отлари», «чувалчанглар» каби вирусларни таъкидлаш жоиздир.

Шак-шубхасиз, махсус антивирусли воситаларни ишлаб чиқиш ва ишлатиш долзарбдир. Антивирусли воситалар вирусдан зарарланиш окибатларини аниқлаш (сканерлаш, ўзгаришларни пайқаш усули, евриетик тахлил етиш, аппарат - дастурли антивирусли воситалар ва хакозо) ва юк килиш масалаларини ечади, шу билан бир каторда файлларни ва хотира сохаларини, юкланиш секторларини тиклайди.

Антивирусли дастурлардан детектор, ревизор (тафтишли) ва «коровул» дастурларини таъкидлаб утиш мумкин.

Компютер вирусларидан ҳимоя қилишнинг асосий чораларидан дастур маҳсулотларини расмий йўл билан ишлатишни келтириш мумкин. Алоҳида таъкидлаш керакки, антивирусли воситалар доимо янгиланиб бориши керак, бунда ташқаридан келадиган янги дастурларга ва файлларга алоҳида еътиборни қаратиш керак.

Таъкидлаб ўтамизки, дастур маҳсулотларини вируслардан ҳимоя қилишнинг ахамияти жуда каттадир. Бундай ҳимоя, оддий вируслардан ташқари, албатта ҳуқуқий усуллар билан амалга оширилиши керакдир.

Асосий атамалар

Вирусга қарши дастур, юкланадиган вирус, компютер вируси, вирус-мутант, кўринмайдиган вирус (стелс-вирус), хавфсиз вирус, резидент бўлмаган вирус, хавфли вирус, жуда хавфли вирус, паразит (текинхур) вирус, резидент вирус, вирус-репликатор (чувалчанг), тармоқли вирус, троян вируси, файл вируси, зарарланган дастур, зарарланган диск, дастур-ваксина, дастур-доктор (фаг), дастур-детектор, дастур-тафтишчи, дастур-филтр (қоровул), Аидстест ва Достор Web полифаг дастурилари.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Компютер вирусларга қарши курашадиган антивирус дастурлари, жумладан, Аидстест, Достор Web, НОД 32, КАВ, Адинф, Адинф Суре Модуле ларни компютерга ўрнатинг, уларнинг параметрларини созланг, ишлатинг, натижаларини таҳлил етинг.

Ҳисобот мазмуни:

1. Иш мавзуси.
2. Ишдан мақсад.
3. Дастурий воситани ўрнатиш алгоритми.
4. Дастур параметрларини созлаш.
5. Базаларини ўрнатиш.
6. Дастурни ишга тушириш ва унинг натижасини таҳлил қилиш.

Назорат саволлари

1. Компютер вируси нима ва унинг табиати қандай?
2. Вирусларни компютерга кириб боришини асосий йўллари қандай?
3. Компютер вирусларини зарарлари нималарда намоён бўлади?
4. Сизларга компютер вирусларини қандай асосий кўринишлари маълум?
5. Вирусларни пайқаш ва улардан ҳимоя қилиш учун дастурларнинг қандай турлари мавжуд?
6. Детекторлар дастури ва докторлар дастурининг фарқлари ва ўхшаш жойлари нимада?
7. Тафтишчилар дастурининг ва филтрлар дастурининг афзалликлари нималарда намоён бўлади?
8. Компютер вирусларидан ҳимоя қилиш бўйича асосий чораларни айтиб беринг.
9. “Диалог-Наука” ХЖ нинг вирусга қарши дастурлар тўпламини таркибини ва вазифасини айтиб беринг.
10. Вирусларни пайқаш ва йўқ қилиш учун Аидстест дастурини қандай қўллаш керак?
11. Др.Web вирусга қарши дастурини Аидстест дастуридан фарқи нимада?
12. Др.Web дастурини қандай режимларда ишлатиш мумкин?
13. Қаттиқ дискни вируслар мавжудлигига даврий равишда текшириш технологиясини айтиб беринг.
14. Дастур маҳсулотларини ҳимоя қилиш нима учун керак?

№9 Лаборатория иши

Мавзу: Тақиқланган мурожаат қилишдан ахборотни ҳимоя қилишнинг КРИПТОН - ВЕТО криптографик тизими

Режа:

1. Қисқача назарий маълумот
2. Ишни бажарилиш тартиби ва қўйилган вазифа:

Дарснинг мақсади: Тақиқланган мурожаат қилишдан ахборотни ҳимоя қилишнинг КРИПТОН - ВЕТО криптографик тизимини ўрганиш ва ундан фойдаланиш кўникмасини ҳосил қилиш

- **Таянч иборалар: КРИПТОН -** ВЕТО , ахборотни “шаффоф” шифрлаш, КРИПТОН-ЗАМОК, Secret Disk, абонентлик шифрлаш (АШ), пакетли шифрлаш (ПШ), Kripton Sign дастури.

Дарс ўтиш воситалари: синф доскаси, ўқув-услубий қўлланмалар, компютер, машғулотга доир слайдлар, машқ ва масалалар тўплами.

Дарс ўтиш усули: суҳбат, мустакамлаш, намойиш, амалий ишлаш.

Дарснинг технологик харитаси:*-80 минут.*

Ташкилий қисм: *хонанинг тозалиги, жиҳозланиши, санитария ҳолати, талабаларнинг давомати-2 минут.*

Талабалар билимини баҳолаш: *ўтилган мавзуни қисқача такрорлаш, талабалар билан савол – жавоб ўтказиш ва баҳолаш- 20 минут.*

Янги мавзу баёни: *-30 минут.*

Мавзуни ўзлаштириш даражасини аниқлаш ва мустаҳкамлаш-*20 минут.*

Синов саволлари – *5 минут.*

Уйга вазифалар бериш - *3 минут.*

Мавзу баёни

Қисқача назарий маълумот:

КРИПТОН-ВЕТО тизими MS ДОS 5.0 ва ундан юқори, Windows 3.1 ОТ лари бошқаруви остида ишлайдиган, 386 просессордан паст бўлмаган ШК ларни ҳимоя қилиш учун мўлжалланган. Бунда ШК абонентлик пункти, пакетларни коммутасиялаш маркази, калитларни ишлаб чиқариш маркази сифатида ишлатиши мумкин.

Тизим шахсларни ва уларнинг ҳуқуқларини ШК даги ахборотга мурожаат қилиш ҳуқуқини чеклайди. Унинг амалга оширилиши ГОСТ 28147-89 алгоритми бўйича мантиқий дискларни “шаффоф” шифрлаш ва ГОСТ 34.10ғ11-94 бўйича електрон рақамли имзо технологияларига асосланган.

КРИПТОН-ВЕТО тизимининг асосий функсиялари таркибига қуйидагилар киритилган:

- ШК ни ёки “винчестр” ни ўғрилаб кетилганда ахборот махфийлигини таъминлаш;
- компютер ресурсларига мурожаат қилиш бўйича фойдаланувчининг ваколатларини чеклаб қўйиш;
- дастурнинг яхлитлигини уни бажаришга ишга тушириш вақтида текшириш;
- тизимда пайдо бўладиган ҳодисаларни қайд қиладиган тизимли журнални олиб бориш;
- ҳимоя қилинган дискка мурожаат қилишда ахборотни “шаффоф” шифрлашни таъминлаш;

- вируслар, фойдаланувчи хатолари, техник ишдан чиқишлар ва ёмон ниятли киши ҳаракатлари келтириб чиқарган бузилишларни пайқаш.

Компютерга мурожаат қилишни чеклаш учун
КРИПТОН-ЗАМОК комплекси

КРИПТОН-ЗАМОК комплекси компютерга мурожаат қилишни чеклайдиган аппарат-дастурли воситаларни, КРИПТОН сериясидаги маълумотларни криптографик ҳимоя қилиш қурилмасини (**МКҲҚҚ**) ишлатган ҳолда, қуриш учун мўлжалланган. Комплекс ШК асосида, ундаги мавжуд бўлган ахборотга мурожаат қилишга ега бўлган шахслар доирасини чеклаган ҳолда, иш жойини ташкил қилиш имконини беради.

КРИПТОН-ЗАМОК комплексини ишлаши учун MS ДОS, Windows 95/98/NT, Unix операсион тизимли, просессори 386 дан паст бўлмаган ИБМ ПС туридаги ШК керакдир, улар учун МС ДОС бошқаруви остида компютерга ўрнатилган файлли тизим шаклини тушуниш имконини берадиган мос драйвер мавжуддир.

Комплекс F**AT 12, FAT 32, NTFS, Unix** ва ҳ.к. шакллардаги файлли тизимли, қаттиқ дискли компютерларни ҳимоя қилиш учун хизмат қилади. КРИПТОН-ЗАМОК комплексининг иккита кўриниши чиқарилган:

- сиғими 8 Гбайтдан камроқ қаттиқ дисклар учун;
- сиғими 8 Гбайтдан кўпроқ қаттиқ дисклар учун.

ШК га ўрнатилган, мурожаат қилишни чеклайдиган КРИПТОН -ЗАМОК комплекси қуйидаги функсияларни бажаради:

- фойдаланувчиларнинг компютерга мурожаат қилишини, уларни иденти-фикасиялаш йўли билан, чеклаб қўяди;
- фойдаланувчиларни компютер ресурсларига мурожаат қилишини уларнинг ваколатларига мос равишда бўлиб чиқади;
- комплексни, операсион муҳит дастурларини, амалий дастурларни ва хотира соҳаларини ўзакларини яхлитлигини назорат қилади;
- ҳимоя қилинган електрон журналда ҳодисаларни қайд қилади;
- бошқаришни ва фойдаланувчи параметрларини маъмурият кўрсатган дастур таъминотига (РУН -файлларга) узатади.

Бажарадиган функсияларига мос равишда КРИПТОН-ЗАМОК комплекси қуйидаги асосий қисмтизимларни ўз ичига олади:

- КРИПТОН қурилмасидан ва хизмат кўрсатадиган CPLOCK. EXE дас-туридан ташкил топган мурожаат қилишни бошқарадиган қисмтизим;
- 2 та журнални ўз ичига олган қайд қилиш ва ҳисобга олиш қисмтизими **(1-журнал - аппаратли** - компютерга, унинг ОТ ишга тушгунча, киришга интилишларни қайд қиладиган КРИПТОН қурилмасида, **2-журнал - тўлиқ** - қаттиқ дискда, унда комплексга муваффақиятли киргандан кейин барча воқеалар, шу жумладан аппаратли журнал мазмуни, акс еттирилади), журналларни бошқариш комплексга хизмат кўрсатадиган CPLOCK.EXE дастури билан амалга оширилади;
- КРИПТОН қурилмасидан ва комплекс ишлашида асосий ОТ нинг яхлит-лигини текширадиган CHECKCOS.EXE дастуридан ташкил топган яхлитликни таъминлайдиган қисм тизим. [25;138-141]

КРИПТОН-ЗАМОК комплекси қуйидаги вазифаларни бажаришни таъминлайди:

- компютерга фақатгина рухсат етилган фойдаланувчи кириши мумкин.
- комплекснинг ишончли ядроси юкланади;
- ишончли ОТ юкланади;
- маъмурият томонидан кўрсатилган амалий дастур таъминотининг яхлит-лиги текширилади;
- маъмурият томонидан кўрсатилган дастурларни ишга тушириш амалга оширилади.

Махфий ахборотни ҳимоя қиладиган Secret Disk тизими

Махфий ахборотни ҳимоя қиладиган **Secret Disk** тизими АНКАД фирмаси иштирокида Алладдин компанияси томонидан ишлаб чиқилган ва компютерлардан

фойдаланувчиларнинг кенг доираси: раҳбарлар, бошқарувчилар, бухгалтерлар, адвокатлар, яъни шахсий ёки касбий ахборотни ҳимоя қилиш тўғрисида қайғуриши керак бўлган барча учун мўлжалланган.

Secret Disk тизимини ўрнатишда компютерда янги мантиқий дисклар яратилади, уларга ёзишда ахборот автоматик равишда шифрланади, ўқишда еса - қайта шифрланади. Махфий дисклар билан ишлаш мутлақо сезиларсиздир ва барча ишга туширилаётган иловаларга шифрлашни созлашга тенг кучлидир.

Secret Disk тизимининг муҳим хусусияти шундаки**,** ҳимоя қилинган ахборотга мурожаат қилиш учун нафақатгина фойдаланувчи киритадиган парол, балки яна електрон идентификатор керак бўлади. Бундай идентификатор сифатида параллел порт учун оддий електрон калит, ноутбуклар учун РСМСИА карточкаси ёки смарт-карточкалар ишлатилиши мумкин.

Secret Disk тизими фақатгина фойдаланувчи парол киритгандан ва тизим мос идентификаторни пайқагандан кейингина уланади. Шунинг учун, агар фойдаланувчи компютердан електрон калитни чиқариб олса, ёмон ниятли кишиларга хаттоки паролни билганлиги ҳам ёрдам бермайди.

ТМҚ дан ҳимоя қилишнинг асосий усулларига тармоқ томонидан қуйидаги криптографик усуллар тегишлидир:

- абонентлик шифрлаш (АШ);
- електрон рақамли имзо (ЭРИ);
- пакетли шифрлаш (ПШ);
- абонентларни криптографик аутентификасиялаш.

Абонентлик шифрлашни (АШ) ва електрон рақамли имзони (ЭРИ) амалга ошириш учун ҳужжатларни узатишга бевосита тайёрлашдан олдин ёки уни қабул қилгандан кейин ишга тушириладиган алоҳида дастур ёки дастур-аппаратли тизим қўлланилиши мумкин. АШ ва ЭРИ ни ишлатишни иккинчи варианти коммуникасия дастурларига мос модулларни қўшишни кўзда тутади. Иккала вариантларда ҳам тизим тахминан бир хил функсияларни бажаради.

MS-DOS учун АШ ва ЭРИ дастурлари

Абонентли шифрлашнинг ва Kripton сериясидаги електрон рақамли имзонинг дастур воситаларига қуйидаги дастурлар тегишлидир:

- симметрик шифрлаш ва Kripton Tools калитлари билан ишлаш дастурлари;
- електрон рақамли имзонинг Kripton Tools дастури;
- асимметрик шифрлаш ва ЭРИ ёрдамида файллар-ҳужжатларни ҳимоя қилиш учун **Срйптон Сигн**
- Бу дастурлардан ҳар бирининг муваффақиятли ишлаши учун компютер қуйидаги талабларга жавоб бериши керак:
- 386 ва ундан юқори микропросессор;
- 4.0 ва ундан юқори версияли MS ДОС ОТ;
- 350 Кбайтдан кам бўлмаган тезкор хотира;
- КРИПТОН шифрлаш платаси ёки **Kripton Lite** дастури.

Електрон рақамли имзонинг Kripton Sign дастури

Kripton Sign дастури, електрон ҳужжатларнинг муаллифлигини ўрнатишни ва електрон ҳужжатларнинг яхлитлигини текширишни таъминлайдиган електрон ҳужжатларнинг електрон рақамли имзосини шакллантириш ва текшириш учун мўлжалланган.

Електрон рақамли имзо (ЭРИ) имзоланаётган ҳужжат охирига ёки алоҳида файлга жойлаштириладиган байтлар кетма-кетлиги кўринишига егадир. **ЭРИ** ҳужжат мазмуни, махфий калит ва ҳужжатни имзолаётган шахснинг пароли асосида шакллантирилади. Ҳар бир махфий калитнинг имзосини текшириш учун очиқ калит яратилади.

Имзоланадиган електрон ҳужжат сифатида дастурда исталган файл ишлатилиши мумкин.

Срйптон Сигн дастурини бошқариш учун Norton Commander интерфейсига ўхшаш интерфейс фойдаланувчига керак бўлади.

Срйптон Сигн дастурининг асосий менюси иккита қисмга (панелга) ажратилган. Менюнинг чап қисмида дастур бажарадиган буйруқлар номлари жойлашган, ўнг қисмида еса файллар ва бу файллар жойлашган бўлимлар рўйхати жойлашгандир. Буйруқларни ва файлларни танлаш учун маркер ишлатилади.

Срйптон Сигн дастури ёрдамида **ЭРИ** ни яратиш ва текшириш схемаси 6.2-расмда кўрсатилган. Имзони шакллантириш ва кейинчалик текшириш учун иккита калит-имзони: махфий ва очиқ, яратиш керак. Калитлар дискетадаги оддий файллар ёки електрон карточкадаги байтлар кетма-кетлиги кўринишига егадир.

Калитларни яратиш учун тасодифий кодни ҳосил қилиш (ишлаб чиқариш) КРИПТОН сериясидаги **МКҲҚҚ** лардан бири билан аппарат нуқтаси назардан бажарилади. Агар **МКҲҚҚ** компютерда йўқ бўлса, тасодифий кодни **Kripton Lite** дастури ёки тасодифий сонлар генератори ёрдамида дастур нуқтаи назаридан олиш мумкин.

Калитларни ишлаб чиқариш учун “Калитларни яратиш” буйруғини бажариш етарлидир. Файлни имзолаш учун имзоланадиган файлни ўзини ва махфий калитни танлаш, кейин еса “Имзони қўйиш” буйруғини бажариш керак.

“Имзони кўрсатиш” ва “Имзони текшириш” буйруқлари файлдаги имзоларни борлигини ва ҳақиқийлигини текшириш, ҳамда имзо тўғрисида қўшимча ахборотларни олиш учун ишлатилади. Бу буйруқларни бажариш учун текширилаётган файлларни танлаш ва очиқ калитли каталогларни кўрсатиш керак бўлади.

Windows 95/98/NT учун АШ ва ЭРИ дастурлар пакети.

Windows 95/98/NT учун КРИПТОН/Kripton сериясидаги абонентли шифрлаш ва електрон рақамли имзонинг дастур воситаларига қуйидаги дастурар пакетини келтириш мумкин:

- “КРИПТОН Р Шифрлаш” пакети;
- “КРИПТОН Р Имзо” пакети;
- Windows 95/98/NT 4.0 учун Kripton Arc Mail дастурлар пакети.

Бу дастурлар пакетларини муваффақиятли ишлаши учун компютер ега бўлиши керак:

-Windows 98 ёки Windows NT 4.0 ОТ;

-1.3 ва ундан юқори версияли Windows – Kripton Emulator учун мос драйверли КРИПТОН серияли МКҲҚҚ;

-2.2 ва ундан юқори версияли Windows 95/NT учун Kripton API;

-сичқонча монипулятори.

Янада ишончлироқ ҳимоя қилишни амалга ошириш учун Kripton Emulator дастури ўрнига КРИПТОН сериясидаги МКҲҚҚ сини ишлатиш тавсия етилади.

Ишни бажарилиш тартиби ва қўйилган вазифа:

Юқорида келтирилган тизимларни, жумладан, КРИПТОН-ВЕТО тизими, КРИПТОН-ЗАМОК комплекси, Махфий ахборотни ҳимоя қиладиган Сесрет Диск тизими, Срйптон Тоолс калитлари билан ишлаш дастури, Срйптон Сигн дастурини компютерга ўрнатинг. Уларнинг ишлаш принспларини ўрганинг. Параметрларини созланг.

Ҳисобот мазмуни:

Иш мавзуси.

Ишдан мақсад.

Ишни бажариш алгоритми.

Дастур ишининг натижаси.

Назорат саволлари

1. Интернетда ахборотни ҳимоя қилишнинг обектив шарт-шароитлари қандай?
2. Бузғунчи Интернет орқали нималар қилиши мумкин?
3. Интернетнинг кенг тарқалган хизматлари қандай «туғма» заифликларга ега?

4. Тармоқли номлар хизмати ДНС нинг муаммоси нима ҳисобланади?
5. Ахборот хавфсизлиги учун WWW нинг қайси хоссаси заиф буғин ҳисобланади?
6. Интернетнинг тармоқ хавфсизлиги сиёсатининг моҳияти нимада?
7. Интернетнинг тармоқ сервисларига мурожаат қилиш сиёсатининг асосий принсиплари қандай?
8. Интернет учун маълумотларни ҳимоя қилишнинг қайси стандартлари қўлланилади?
9. Интернетда ахборотни ҳимоя қилишнинг қайси усуллари қўлланилади?
10. Електрон почтани ҳимоя қилиш учун қайси стандартлар қўлланилади?
11. Интернетда мулкчилик ҳуқуқлари қандай?
12. Интернетнинг ахборот хавфсизлигини режимини шакллантиришнинг қонуний даражаси ўз ичига нималарни олади?
13. Интернет хавфсизлик сиёсатининг тармоқли аспектларини ишлаб чиқишда қандай принсиплар ишлатилади?
14. Интернетда қайси енг кўп тарқалган ахборотни ҳимоя қилиш тизимлари ишлатилади?
15. КРИПТОН-ВЕТО тизимининг асосий функсиялари қандай?
16. Мурожаат қилишни чекловчи КРИПТОН-ЗАМОК комплекси қандай функсияларни бажаради?
17. Сесрет Диск тизими нима?
18. Срйптон Сигн дастури нима учун мўлжалланган?
19. Срйптон Сигн ёрдамида електрон рақамли имзо қандай яратилади ва текширилади?
20. Wиндowc 95/98/НТ учун АШ ва ЕПИ нинг қайси дастурлар пакети қўлланилади?
21. Брандмауер нима? Унинг тавсифларини келтиринг.
22. Филтрловчи маршрутловчи нима?
23. Тармоқ даражасидаги шлюзлар тавсифларини келтиринг.
24. Електрон рақамли имзо нима?

Тавсия этиладиган адабиётлар:

1. Ю.В. Романес, П.А. Тимофеев, В.Ф. Шангин. Защита информасии в КС и С. – М.: “Радио и связ”, 2001.
2. Хорошко В.А. Чекатков А.А. Методы и средства защиты инфор-масии. – К.: Издателство Юниор, 2003. – 504 с.
3. Щеглов А.Ю. Защита компютерной информасии от несанксионированного доступа. – СПб.: Наука и техника, 2004. – 384 с.
4. Завгородный В.И. Комплексная зашита информасии в ком-пютерных системах. – М.: Логос, 2001.
5. Камилов Ш.М., Машарипов А.К., Закирова Т.А., Ерматов Ш.Т., Мусаева М.А. Компютер тизимларида ахборотни ҳимоялаш. Маъруза матнлари. – Т.: ТДИУ, 2003.

8. Тарқатма материаллар (реферат мавзулари, адабиётлар рўйхати, баҳолаш мезонлари, ҳорижий манбалар)

Реферат (мустақил таълим топшириқлари) мавзулари ва уларни бажариш учун тавсия қилинган адабиётлар рўйхати:

№	*Мавзу номи*	Топшириклар	Хисо-бот шакли	Адабиёт лар
1	2	3	4	5
1	Ахборот ҳавфсизлигининг асосий тушунчалари ва уларни аниқлаштириш.	Ахборот хавфсизликнинг асосий мақсад ва вазифаларини ёритиб бериш	Ёзма	[1-12, 15-25]
2	Ҳавфсизликнинг мавжуд барча хилма-хил чораларидан фойдаланиш.	Ахборот хавфсизлигини таъминлаш чораларининг босқичлари ва даражалари	Ёзма	[1-12, 15-25]
3	Ахборот ҳимоясининг бузулиши, ҳимоя механизими ва ҳимоя турлари.	Ахборот хавфсизлигига хавфларни ва хавфсизлик тизимлилигини таъминлаш усулларини ўрганиш	Ёзма	[1-12, 15-25]
4	**Ахборот ҳавфсизлиги моделлари** Ҳавфсизлик моделлари. Ахборот хавфсизлиги тизимининг архитектураси.	Ҳавфсизлик моделлари бажарадиган вазифалари. Тизимнинг яшовчанлигини асослаш, унинг архитектураси, қурилишида фойдаланадиган асосий принциплар.	Ёзма	[1-12, 15-25]
5	**Криптографиянинг асосий қоидалари ва таърифлари.** Симметрик шифрлаш тизими. Асимметрик шифрлаш тизими	Симметрик ва асимметрик шифрлаш тизимларнинг хусусиятлари. Шифрлаш усуллари.	Ёзма	[3-21]
6	Хэшлаш функцияси. Электрон рақамли имзо.	Хешлаш функциясини қуриш принцип ва моделлари. Рақамли имзо файлини яратиш.	Ёзма	[3-21]
7	Криптографик калитларни бошқариш	Очиқ, махфий, бир ва икки калитли тизимлар асосида криптографик алгоритмларни ишлаб чиқиш	Ёзма	[3-11, 21-30]
8	**Идентификация ва аутентификация**. Асосий тушунчалар ва туркумланиши. Пароллар ва сертификатлар асосида аутентификациялаш	Оддий ва мураккаб пароллар. Идентификация ва аутентификация усуллари ривожланиши ва истиқболлари.	Ёзма	[3-11, 21-30]
9	**Internet ва Intranetда ахборот ҳавфсизлиги** Internet тармоғи орқали узоқдаги ҳужумдан ҳимояланиш усуллари ва муҳитлари.	Локал ва глобал тармоқларда ички ва ташқи хавфлар таснифи. Глобал тармоғи орқали хужумлардан ҳимояланиш усуллари	Ёзма	[3-11, 21-30]
10	**Тармоқлараро экранлар** Тармоқлараро экранларини функцияларининг хусусиятлари.	FireWall тизимларини ташкил қилиш принцип-лари, турлари, вазифалари, дастурий таъминоти	Ёзма	[3-11, 21-30]

11	**Тармоқлараро экранларини асосий компоненталари.** Маршрутлаштириш ва шлюзалар турлари. Кучлантирилган аутентификация.	Филтрлайдиган маршрутлаштиришлар. Тармоқ даражасининг шлюзи. Амалий даражасининг шлюзаси. Кучлантирилган аутентификация принципи	Ёзма	[3-11, 21-30]
12	Тармоқлараро экранлар асосий схемалари. Экранлашган кўприк. Экранлашган қисм тармоқ..	Тармоқлараро экранлар базасида тармоқ ҳимоясининг асосий схемалари. Филтрлайдиган маршрутлаштириш кўприкларининг асоси. Экранлашган кўприк асосида тармоқлараро экран.	Ёзма	[1-5, 10-11,15,19 20]
13	Тармоқлараро экранларни ҳимоялашнинг дастурли усуллари.	Тармоқлараро экран вазифасини бажарувчи дастурий таъминот риволаниш тарихи, мавжуд дастурлар шарҳи	Ёзма	[1-5, 10-11,15,19 20]
14	Компьютер вируслари, уларнинг классификацияси ва курашиш механизмлари	Компьютер вируслари ва уларнинг классификацияси. Вируслар билан курашиш. Компьютер тизимларнинг вируслар билан захарланиш профилактикаси.	Ёзма	[1-5, 10-11,15,19 20]
15	Операцион тизимлар ва тармоқлардаги ахборот ҳавфсизлиги усуллари ва воситалари.	Операцион тизимлар фаолиятига хавф хатарлар. Компьютер тармоқларида ахборот хавфсизлигини таъминлаш хусусиятлари	Ёзма	[1-5, 10-11,15-30]
16	Компьютер тармоқларида ахборот ҳимоясининг хусусиятлари	Ахборот ҳимояси нуқтаи назаридан компьютер тармоқларини корпоратив ва умумфойдаланувчи тармоқларга ажратиш	Ёзма	[1-5, 10-11,15-19, 25-30]
	Жами			

Рефератнинг режаси:

Мустақил топшириқлар бўйиша ёзилгар реферат қуйидаги бўлимлардан ташкил топиши лозим:

-рефераснинг мавзуси;

- рефератнинг мақсади (масалинг қўйилиши);

- асосий қисм;

- хулосалар.

Рефератни ёзиш, топшириш ва ҳимоя қилиш:

Танланган мавзу бўйича ёзиладиган реферат:

- *режада кўрсатилган бўлимлардан ташкил топиши;*
- *унинг елестрон варианти тайёрланиши;*
- *елестрон варисnти илмий раҳбари билан муҳокама қилиниши;*
- *муҳоламада баъзи бир камчиликлар фниқланган бўлба, улар тузатилиши;*

- *тайёр реферат принтерда босмадан чиқарилиб, унунг електрон ва қоғоз вариантлари кафедрага топширилиши;*
- *белгиланган санада реферат ҳимоя қилиниши керак.*

Рефератни баҳолаш:

Танланган мавзу бўйича ёзилган реферат ҳимоя қилинганда қуйидагича баҳоланади:
Максимал балл – 3.0; Саралаш бали – 1,7.

ТАВСИЯ ҚИЛИНГАН АДАБИЁТЛАР

1. С.С.Свириденко. Современные информационные технологии. М., : Радио и связь, 1989, 304 бет;
2. Ғуломов С.С., А.Т.Шермуҳаммедов, Б.А.Бегалов. Иқтисодий информатика. Тошкент, Ўзбекистон,1999й., 528 бет ";
3. Симонович С., Евсеев Г., Алексеев А. Специальная информатика. М.,:АСТ-ПРЕСС, 2002, 480 бет;
4. С.С. Қобилов, И.И. Жуманов. СУБД и информационные системы. Самарканд, СамДУ нашри, 1997, 97 бет;
5. М.Арипов. Internet ва электрон почта алоқаси. Т., "Университет", 2000, 132 бет;
6. Е. Шафрин. Работа на E-mile. М., 1996, 330 бет;
7. А.Девид, Дж. Уорл. Пользование WWW. М., 1997, 426 бет;
8. Жуманов И.И., Мингбоев Н.С. Ҳисоблаш системаларининг информацион асослари. Самарқанд,: СамДУ нашри, 2002, 107 бет;
9. Мингбаев Н.С., Жуманов И.И. Информатика.- Самарканд,: СамДУ нашри, 2002, 107 бет;
10. Жуманов И.И., Мингбоев Н.С. Ахборот технологиялари (1-қисм: ахборот технологияларининг қурилмавий ва дастурий таъминоти), Самарқанд,: СамДУ нашри, 2005, 148 бет;
11. Жуманов И.И., Мингбоев Н.С. Ахборот технологиялари (2-қисм: ахборот технологияларининг информацион таъминоти), Самарқанд,: СамДУ нашри, 2005, 70 бет;
12. Мингбоев Н.С., Сайдуллаев У.Ж. Turbo Pascal дастурлаш тилидан лаборатория ишларини бажариш бўйича услубий кœрсатмалар. Самарқанд: СамДУ нашри, 98 бет, 2007;
13. Файсман А. Профессиональное программирование на языке Паскаль. М.,: Наука, 2000, 524 бет;
14. Зуев Е.А. Язык программирование Turbo Pascal 6.0. М.,: Радио и связь, 1996 йил, 486 бет;
15. Россияда нашр қилинаётган «Компьютер Пресс», «Мир ПК», «Компьютерра», «Компас», «Hard and Soft» ва республикамизда нашр қилинаётган «ПрессТИЖ» журналлари, 2000-2005 йиллар.
16. Завгородний В.И. Комплексная защита информации в компьютерных системах. Учебное пособие.-М.:Логос; ПБОЮЛ Н.А.Егоров, 2001. 264 с.
17. Столинс, Вильям. Основы защиты сетей. Приложения и стандарты: Пер. С англ.- М.: Издательский дом «Вильямс», 2002. 432 с.
18. Ғаниев С.К.,Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув қулланма.- Тошкент давлат техника университети, 2003. 77 б.
19. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. Защита информации в компьютерных системах и сетях.
20. Ю. В. Нестеренко. Алгоритмические проблемы теории чисел (глава 4 из книги "Введение в криптографию" под ред. В. В. Ященко) | 29.10.2001
21. "Введение в криптографию" под редакцией В.В.Ященко | 15.11.2001

22. "Введение в криптографию" /Под общ. ред.В.В.Ященко --- М., МЦНМО, 1998, 1999
23. В. А. Носов. Краткий исторический очерк развития криптографии. Из материалов конференции "Московский университет и развитие криптографии в России" (МГУ, 17--18 октября 2002 г.).
24. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.: Горячая линия - Телеком, 2000. 452с.
25. Устинов Г.Н. Основы информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия «безопасность». – М.:СИНТЕГ, 2000, 248 с.
26. Широчин В.П. Мухин В.Е., Кулик А.В. Вопросы проектирования механизмов защиты информации в компьютерных системах и сетях.- К.:, «ВЕК+», 2000. 112 с.
27. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.- М.: Издательство ТРИУМФ, 2003 – 816 с.
28. Н. Коблиц. Курс теории чисел и криптографии. М., Научное издательство ТВП, 2001 г., 260 стр. (перевод с английского).
29. В. В. Яшенко. Криптография, которая раньше была засекречена (интервью для журнала "Компьютера" от 25.05.1998)
30. М. Е. Масленников. Практическая криптография. Фрагмент книги, вышедшей в издательстве " bhv -Петербург" 2002 г. 120 с.

ТАВСИЯ ҚИЛИНГАН ИНТЕРНЕТ САЙТЛАРИ

1. IXBT (http://www.ixbt.com);
2. Multimedia Dayjest (http://www.tpcdigest.ru);
3. Virtualnыy kompyuternыy muzey (http://computer-museum.ru);
4. Novosti mira kompyuternoy texnologiy (http://www..lgg.ru /-ru-technews/);
5. Kompyuternыye novosti ZDNet (http://www.zdnet.ru/zdreviews/);
6. Kompyuternaya ensiklopediya Kirilla i Mefodiya (http://www.km.ru);
7. Bazы dannыx po senam na komplektuyushiye (http://www.price.ru).
8. Softkey.Ru (http://www.softkey.ru);
9. Softodrom.Ru (http://www.softodrom.ru);
10. ListSoft (http://www.listsoft.ru);
11. Server Besplatnыx Programm (http://www.freeware.ru);
12. Freeware.Ru (http://www.freeware.ru);
13. Download.com (http://www.download.com);
14. Winfiles (http://www.winfiles.com);
15. Freeware Home (http://www.freewarehome.com);
16. SoftNews (http://www.fcenter.ru/softnews.htm).

17. Virusnaya ensiklopediya «Laboratoriya kasperskogo» (http://www.viruslist.com/index.htm);
18. Antivirus Kasperskogo (http://www.kav.ru);
19. DrWeb (http://www.drweb.ru);
20. Trojan Remover (http://www. simplesup.com/tremover/);
21. Trauscan (http://www.agnetum.com/ru/products/ /tauscan/index.htm).

9. Мустақил иш мавзулари ва уни бажариш бўйича услубий тавсиялар

Мустақил иш мавзулари

№	Мустақил машғулот мавзулари	Берилган топшириқлар	Бажариш муддати	Ҳажми, соат
VII семестр				
1	Ахборотларга нисбатан хавф-хатарлар таснифи.	Реферат таёрлаш	1,2,3 хафталар	4
2	Тармоқ хавфсизлигини назорат қилиш воситалари	Реферат таёрлаш		
3	Ахборотни ҳимоялаш усулларининг тизимлилиги	Реферат таёрлаш		
5	Ахборотларни ташкилий ҳимоялаш елементлари	Реферат таёрлаш		4
6	Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар	Реферат таёрлаш		
7	Компютер вирусларидан ахборотларга рухсациз кириш ва улардан фойдаланиш.	Вируслардан ҳимояланиш тизимини ташкил қилиш бўйич тавсиялар ишлаб чиқиш	4 хафта	2
8	Антивирус дастурлари			2
9	Вирусларга қарши чора-тадбирлар			2
10	Замонавий компютер стенографияси	Реферат таёрлаш	5,6 хафталар	4
11	Конфиденсиал ахборотларни рухсациз киришдан ҳимоялаш	Реферат таёрлаш		
12	Ахборотларни ҳимоялашнинг криптографик усуллари	Реферат таёрлаш		4
13	Симметрияли криптотизимлар	Реферат таёрлаш		
14	Ўринларни алмаштириш усуллари	Реферат таёрлаш		
15	Електрон почтага рухсациз киришдан ҳимояланиш	Реферат таёрлаш	7,8,9 хафталар	4
16	Маълумотларга рухсациз киришнинг дастурий ва техник воситалари	Реферат таёрлаш		
17	Компютер тармоқларининг заиф қисмлари. Тармоқ ҳимоясини ташкил қилиш	Реферат таёрлаш		
18	Компютер телефониясидаги ҳимоялаш усуллари	Реферат таёрлаш		4
19	ЕҲМ ҳимоясини таъминлашнинг техник воситалари	Реферат таёрлаш		
20	Интернет тармоғида мавжуд алоқанинг хавфсизлигини таъминлаш	Реферат таёрлаш	10,11 хафталар	6
21	Интернетда рухсациз кириш усулларининг таснифи. Рухсат етилган манзилларнинг рухсат етилмаган вақтда уланиши	Реферат таёрлаш		
22	Тармоқлараро екран ва унинг вазифалари. Тармоқлараро екраннинг асосий компонентлари.	Екранни тизимда уланиши ва созлаш бўйича тавсиялар ишлаб чиқиш		

23	Электрон почтада мавжуд хавфлар. Електрон почтани ҳимоялаш	Екранни тизимда уланиши ва созлаш бўйича тавсиялар ишлаб чиқиш		
24	Електрон туловлар тизимида идентификасия-ловчн шахсий номерни ҳимоялаш.	Реферат таёрлаш	12, 13 хафталар	6
25	Банкоматлар хавфсизлигини таъминлаш	Реферат таёрлаш		
26	Интернетда мавжуд електрон туловлар хавфсизлигини таъминлаш	Реферат таёрлаш		
27	Дастурларни ваксинасия усули билан вируслардан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш	14-17 хафталар	8
28	Мавжуд ехе-файлларни ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш		
29	Антивирус Касперский 6.0. дастури	Дастурни ШЕҲМда ўрнатиш ва созлаҳ бўйича ҳисобот таёрлаш		
30	Дастурларни норасмий нушалашдан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш		
31	Дастурларни трассировкадан ҳимоялаш	Мавзудаги усул бўйича дастур тузиш Ҳисобот таёрлаш		
32	Шифрлаш жадваллари. Сеҳрли квадратларни қўллаш	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш	18-20 хафталар	6 соат
33	Оддий алмаштириш шифрлари. Сезар шифрлаш тизими	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш		
34	Ўрнига қўйиш Афина тизими. Трисемус шифрлаш жадвали	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш		
35	Плейфейр биграмма шифри. Ҳилл криптотизими	Мавзудаги усул бўйича дастур тузиш. Ҳисобот таёрлаш		
			Жами	56

Мустақил таълимни ташкил этишнинг шакли ва мазмуни

«Телекоммуникация тизимлари ва компютер тармоқларида ахборот хавфсизлиги» фани бўйича талабанинг мустақил таълими шу фанни ўрганиш жараёнининг таркибий қисмидир.

Талабалар айрим мавзуларни кенгроқ ўрганиш мақсадида қўшимча адабиётларни ўқиб, рефератлар тайёрлайдилар ва машғулот режаси бўйича қуйилган масала ечимини моделлаштириш, алгоритмларини тузиш ва дастурий воситаларини қўллаш билан боғлиқ саволларни ёритадиган лойиҳалар тайёрлашади.

Мустақил таълим натижалари рейтинг тизими асосида баҳоланади. Бунинг учун берилган вазифаларни текшириш ва баҳолаш амалий машғулот олиб борувчи ўқитувчи

томонидан амалга оширилади. Конспектларни ва мавзуларни ўзлаштириш даражасини баҳолаш эса, маъруза дарсларини олиб борувчи ўқитувчи томонидан бажарилади.

Талабанинг мустакил иши бажариш турлари

1. Реферат
2. Электрон дастур
3. Электрон дарслик
4. Презентация
5. Демонстрацион материал

Мустакил ишларни бахолаш мезонлари

№	Ўзлаштириш (%) ва балларда	Баҳо	Талабанинг билим даражаси
1.	86-100	Аъло «5»	Хулоса ва қарор қабул қилиш Ижодий фикрлай олиш Мустақил мушохада юритиш Амалда қўллай олиш Моҳиятини тушуниш Билиш, айтиб бериш Тасаввурга эга бўлиш
2.	71-85	Яхши «4»	Мустақил мушохада юритиш Амалда қўллай олиш Моҳиятини тушуниш Билиш, айтиб бериш Тасаввурга эга бўлиш
3.	55-70	Қониқарли «3»	Моҳиятини тушуниш Билиш, айтиб бериш Тасаввурга эга бўлиш
4.	0- 54	Қониқарсиз «2»	Аниқ тасаввурга эга эмаслик Билмаслик

Талаба мустақил ишининг ташкилий шакллари

Талаба мустақил ишини ташкил этиш муайян фаннинг хусусиятларини, шунингдек, ҳар бир талабанинг академик ўзлаштириш даражаси ва қобилиятини ҳисобга олган холда қуйидаги шакллардан фойдаланилади:

1. айрим назарий мавзуларни ўқув адабиётлари ёрдамида мустақил ўзлаштириш;
2. берилган мавзу бўйича ахборот (реферат) тайёрлаш;
3. семинар ва амалий машғулотларга тайёргарлик кўриш;
4. лаборатория ишларини бажаришга тайёргарлик кўриш;
5. малакавий битирув иши ва магистрлик диссертациясини тайёрлаш;
6. режавий материал қисмини мустақил ўрганиш бўйича қандай маъруза машғулотлари чегарасида бўлса, худди шундай лаборатория ишлари ёки амалий машғулотларга тайёргарликда ахборотни электрон ўқув адабиётлари, Интернет ва бошқаларни қўллаш;
7. фаннинг бўлимлари ёки мавзулари устида махсус ёки илмий адабиётлар (монографиялар, мақолалар) бўйича ишлаш;
8. квалификацион амалимёт ўтаётган вақтда мутахассислар раҳбарлигида янги техника ва асбобларни, илмий технология ва жараёнларни ўрганиш;
9. илмий мақола, анжуманга маъруза тезисларини тайёрлаш.

Талаба мустақил ишини назорат қилиш ва бахолаш

1. Хар бир фан бўйича талаба мустақил ишига раҳбарлик қилиш юкламаси (ўқитувчи шахсий иш режасининг ташкилий-услубий бўлимида - 15 соат, 1540 соат доирасидан) қайд этилади.
2. Талаба мустақил ишига рахбарлик қилиш кафедрада тузиладиган ва факультет декани томонидан тасдиқланадиган консультациялар жадвали асосида амалга оширилади.
3. Талаба мустақил ишини назорат қилиш ўқув машғулотларини бевосита олиб борувчи ўқитувчи томонидан амалга оширилади.
4. Талабанинг мустақил иши ТМИ учун ажратилган балл ҳисобидан бахоланади ва натижаси фан бўйича талабанинг умумий рейтингига киритилади.
5. Талабанинг рейтинг кўрсаткичлари, шу жумладан мустақил иши бўйича, анъанавий гурух рейтинг ойнасида ва (ёки) факультетнинг махсус электрон тармоғида ёритиб борилади.
6. Талаба мустақил ишини назорат қилиш турлари ва уни бахолаш мезонлари тегишли кафедра томонидан белгиланади ва факультет Илмий кенгашида тасдиқланади. Мустақил ишларни бахолаш меъзонлари талабаларга ўқув йили (семестри) бошланиш олдидан методик материаллар билан биргаликда тарқатилади.
7. Мустақил иш бўйича белгиланган максимал рейтинг баллининг 55%дан кам балл тўплаган талаба фан бўйича якуний назоратга қўйилмайди.
8. Фанлар кесимида талабаларнинг мустақил ишлари бўйича ўзлаштириши мунтазам равишда талабалар гурухларида, кафедра йиғилишлари ва факультет Илмий кенгашларида муҳокама этиб борилади.
9. Талабанинг мустақил иши кафедра архивида рўйхатга олинади ва икки йил мобайнида сақланади.

10. Курс ишлари мавзулари ва уларни бажариш бўйича тавсиялар

Курс иши учун тавися қилинган мавзулар

Ташкилотнинг ҳимоялаш системасига бўлган ҳақиқий эҳтиёжини аниқлаш ва хавфсизликнинг чораларини танлаш.
Хавфсизлик моделлари асосида тизимнинг яшовчанлигини ошириш.
Белла-Ла Падула, Деннинг ва Ландвер моделлари ва уларнинг қўлланилиши.
Internet тармоғи орқали узоқдан хужумдан химоя усуллари ва муҳитлари.
Тармоқлараро экран асосида ахборот ҳимоя тизимини ишлаб чиқиш.
Тармоқлараро экранлар базасида кучлантирилган аутентификацияни ташкил қилиш.
Филтрлайдиган маршрутлаштириш кўприклари асосида тармоқлараро экранни амалга ошириш.
Тармоқлараро экран - экранлашган қисм тармоқ.
Виртуал корпоратив тармоқларни ташкиллаштириш учун тармоқлараро экранларни қўллаш.
Ҳимоянинг дастурли усуллари таснифланиши.
Операцион тизимлар ва тармоқлардаги ахборот хавфсизлиги усуллари ва воситаларини ўраганиб чиқиш
Ахборот ҳимояси нуқтаи назаридан компьютер тармоқларини корпоратив ва умумфойдаланувчи тармоқларга ажратиш ва уларни кўриб чиқиш
Фойдаланувчининг идентификацияси ва аутентификациясини турлаш схемалари.
Алоқа каналларида ахборотни ҳимоялашнинг ишончли ва универсал усулларини кўриб чиқиш.
Узоқлаштирилган жараёнларда ўзаро алоқа қилиш ҳимоясини таъминлаш.
Алоқадаги жараёнларнинг ҳақиқийлигини текшириш усуллари.
Электромагнит нурланиш ва таъсирланишлардан (наводкалардан) ҳимояланиш усуллари ва воситалари.
Актив ва пассив усуллар ва уларнинг турлари.
Компьютер вируслари ва уларнинг классификацияси.
Вируслар билан курашиш усуллари ва воситалари.
Тизимда рухсатсиз кириш хавфсизлигини таъминлаш.
Internet ва Intranetда ахборот хавфсизлиги.
Корпоратив ва умумфойдаланувчи тармоқлардаги ахборот хавфсизлиги.
Тармоқни бошқариш қисм тизимида ахборотни ҳимоялаш.
Арифметик алгоритмларни дастурлаш.
Алгебраик алгоритмларни дастурлаш.
Web-серверларнинг ҳимояси.

Амалий математика ва информатика таълим йўналишида билим олаётган 3-курс талабалари учун «Ахборотларни ҳимоялаш» фанидан курс ишини бажариш бўйича услубий қўрсатмалар ва тавсиялар

Курс ишининг мақсади, вазифалари ва талаблари.

Курс иши ўқув жараёнининг муҳим шаклларидан бири бўлиб, у талабани амалий фаолиятга тайёрлаш учун йўналтирилган.

Курс иши мақсади:

а) олинган назарий ва амалий билимларни кенгайтириш, чуқурлаштириш ва мустаҳкамлаш;

б) мустақил иш куникмаларини махсус адабиётлар ва бошқа манбалар орқали ўрганиш;

в) фикр ва мулоҳазаларни изоҳлаш, мантиқий кетма-кетликлар ва исботларни келтира олиш;

г) чиқишларга тайёргарлик қилиш ва дискуссияларда қатнашиш;

д) битирув малакавий ишига тайёргарлик қилиш

Курс иши мавзуси назарий курснинг талабларига жавоб бериш керак.

Фанлар бўйича мулжалланган курс ишлари мавзуларини ва уларни бажариш вақти кафедра мажлисида ишлаб чиқилади ва тасдиқланади.

Курс ишига талабларни уч хил гуруҳ - структурасига, мазмунига (асосий бўлим) ва шакллантиришга талабларга ажратиш мумкин.

Курс ишининг структураси танланган мавзуни очиш қобилятига ега бўлиши керак ва курс ишининг структураси: титул варағи, мундарижаси, кириш, асосий қисм, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат бўлиши керак.

Курс ишини шакллантириш учун талаб етиладиган шартлар:

Киришда танланган мавзунинг долзаблиги асосланади, курс ишининг умумий мақсади, уни аниқ масаласи ва тадқиқот усули аниқланади.

Тадқиқот масаласи ва унинг мақсадини аниқлашда уларни тўғри ифодалаш зарур. Масаланинг мақсали сифатида “қилади” кабилардан фойдаланмаслик керак. Қуйидагилардан фойдаланиш тўғрироқ бўлади: очиш, аниқлаш, яратиш, кўрсатиш, урганиш ва шу кабилар.

Ишнинг асосий қисми икки ёки уч бобдан иборат бўлиб, улар қисмларга ва бўлимларга ажратилади. Ҳар бир боб киришда шакллантирилган масалани ёчишга ва бобнинг охирида кичик хулосага ега бўлади.

Курс иши номи ва унинг бирор бобининг номи мос келиши каби, мантиқий хатоларга йўл қўймаслик керак.

Курс иши ўқув – тадқиқот характерига ега бўлиб, худди шу вақтнинг ўзида у ўзининг фан соҳасида янги ютуқлардан фойдаланиш лозим.

Ишнинг мазмуни жадваллар, график материаллар ва шу кабилар билан иллюстрасия қилиниши керак.

Назарий таҳлил усулининг мазмунини тўғри тушунтириш керак ва ҳамма саҳифаларни ёритишда фақатгина иккита ёки учта адабиётлардан фойдаланмаслик керак. Иш плагиат шаклида бўлмаслиги учун фойдаланилган адабиётлар рўйхатини кўрсатиб ўтиш зарур. Фан бўйича фойдаланиладиган дарсликда келтирилган маълумотларни кўчирмаслик

керак. Курс ишида ёритилган мавзу танланган мавзуни чуқур урганишни назарда тутади.

Ишни бажаришда нуфузли назарий нашриётларда чоп етилган мақолалар билан тўлдирмаслик лозим. Масалан, таърифни беришда қайси олимлар қайси манбада бу таърифни берганлиги улар ишлатган иборалар сизникидан қандай фарқ қилиши, бунга ҳар хил нуқтаий назарлар, уларнинг мос келиши ва келмаслиги, шунингдек олимларнинг енг яхши тўғри келадиган фикрларини ўз сўзларингиз билан ифодаланг.

Назарий характерга ега ишларда тадқиқот мавзуси бўйича адабиётлар таҳлили, кузатилган ҳодисалар урганилиб, муаллиф албатта бу муаммога нисбаттан ўз фикрини ёритади.

Хулоса, фойдаланилган адабиётлар ва иловалар қисмини шакллантиришда, ДТС га мос келиши ва таъминланиши зарур.

Курс ишининг ҳажми қўлёзма шаклида 35, 40 саҳифадан ёки 25, 30 саҳифа печатланган шаклда (Тимес Hew Роман 14 пт) 1,5 см. интервалдаги матндан иборат бўлиши керак. Бажарилган курс иши муқоваланади.

Ёзилаётган курс иши ўқитувчи раҳбарлиги остида амалга оширилади. Раҳбарлик масалани берилишидан бошлаб унинг талаба томонидан амалга оширилиши учун маслаҳат бериш билан давом еттирилади.

Талаба маслаҳатлар давомида – урганиладиган мавзуни, тадқиқот режасини, иш структурасини, ишнинг босқичма-босқич бажарилиш даврини, зарурий адабиётларни ва бошқа материалларни, шунингдек ишдаги раҳбар кўрсатган камчиликларни бартараф етади.

Талаба томонидан бажарилган иш текшириш учун топширилгандан сунг, унинг раҳбари томонидан 10 кун муддат ишида текширилиб ёзма ҳулоса - тақриз берилади.

Ишни баҳолашда унинг мазмунини, долзарблигини, мустақиллик даражасини, хулоса ва таклифларнинг аниқлилигини, фойдаланилган материалларнинг сифатини, шунингдек хатолик даражаларини ҳисобга олади. Бир вақтнинг ичида тақризчи ишнинг яхши томонларини, камчиликларини ва қилиниши керак булган ишларни кўрсатади. Тақриз – ишни ҳимояга қўйилиши ёки қўйилмаслиги ҳақидаги хулоса билан якунланади.

Ишни ва тақризни кўриб чиқиш ва тўғрилаш учун талабага қайтарилади. Агар курс иши тақризчининг хулосаси асосида қониқарсиз ва қайта ишлашга берилган бўлса, у ҳолда иш талаба толмонидан қайта кўриб чиқилиб яна тақризга берилади.

Курс иши ҳимояси кафедра томонидан ҳимоягача 10, 15 кун қолганда тасдиқланган икки – уч киши, уларнинг бири курс иши раҳбаридан иборат бўлган комиссия аъзоларидан ташкил топади.

Курс иши сессия бошлангунга қадар ҳимоя қилиниши шарт.

Ҳимояда талаба курс ишининг мазмунини қисқача ёритиши, курс иши учун берилаган тақризнинг саволларига ва комиссия аъзоларининг саволларига тўлиқ жавоб бериши керак. Ҳимоя хулосаси бўйича комиссия аъзолари курс иши охирги баҳони қўяди.

Илмий тугаракларда талаба томонидан бажарилган курс иши ва комиссия мажлисида кўриб чиқилган сўнг уни курс иши сифатида ҳисоблаш мумкин.

Курс ишини бажариш бўйича тавсиялар

Курс иши – реферат, доклад, назорат ишларига қараганда юқори даражада туради. Енг аввало, курс иши бу каби ишлардан фарқ қилиб, билимларни текширишнинг ёрдамчи шаклига кирмайди. Агар реферат ёки назорат ишларига қўйилган баҳо фақат ЖН,ОН, ЯН га таъсир еца, курс ишига қўйилган баҳо рейтинг дафтарчасига қўйилади. Бошқача айтганда курс ишининг баҳоси ЖН,ОН, ЯН статусига ега.

Курс ишини ёзиш таълим стандартида кўрсатилган махсус фанлардан амалга лширилади. Ўқув йили давомида битта курс иши топширилади. Биринчи курсда талаба бу фаолиятга тайёр бўлмаганлиги учун курс ишини ёзиш иккинчи курсидан бошланади.

Курс иши – бу талабанинг ҳақиқий илмий тадқиқот иши ҳисобланиб, у махсус фан бўйича ёзилади ва талабанинг мустақил илмий фаолиятини баҳолайди. Шунинг учун талаба учун курс иши ёзиш чегараланмаган.

Курс иши раҳбарининг маслаҳатлари ва танланган адабиётлардан фойдаланиб, талаба бир неча ой мобайнида тайёрланиш босқичидан ўтади ва матнини ёзади, шундан сунг ўзининг илмий раҳбарига ўқиш ва баҳолаш учун топширади. Иккинчи ва учинчи курсларда курс учун қўйилган баҳо рейтинг дафтарчасига қўйилади. Туртинчи курсда еса барча курс ишларининг ҳимояси махсус кафедраларда бажарилади. Бу каби ҳимоялар БМИ ҳимоясига тайёргарлик сифатида кўрилади.

Курс иши бу мустақил илмий тадқиқот бўлганлиги учун унинг мавзуси долзарб бўлиши керак(замонавий фаннинг ҳолатини ҳисобга олган ҳолда).

Ҳар хил турдаги курс ишлари учун унинг турига қараб талаб ҳар хил бўлади. Агар курс иши назарий характерда бўлса яъни амалиёт натижалари бўлмаса, у ҳолда унинг структурасинии шунга мос ҳолда ишлаб чиқиш зарур. Бунда мавзуга бағишланган чет ел ва мамлакатимизда чоп етилган адабиётлар таҳлили ва уларни услубий солиштириш ҳақидаги бобларни жойлаштирилади.

Амалий характердаги ишларда еса, иш икки қисмга ажратилади, биринчиси, назарий услубий қисми ва иккинчиси еса амалий қисм бўлиб, унда графиклар, чизмалар, блок схемалар, жадваллар ва шунга ухшаш зарурий маълумотлар билан ёритилади.

Тажрибавий – експрементал характерга ега бўлган курс иши ҳам назарий услубий ва шундан сунг експрементни ўтказиш, унинг усули ва ёритиш шартлари, умумлаштириш ва олинган натижаларнинг ёритилиши кўрсатилади.

Курс ишлари ҳар хил турга мансуб бўлишига қарамасдан ихтиёрий турдаги курс иши мундарижа, кириш, асосий қисм, хулоса, фойдаланилган адабиётлар рўйхати ва иловадан иборат бўлади, курс иши ҳажмига нисбатан 10% кириш, 5% хулоса ва қолган қисмлардан таркиб топган бўлади.

Кириш қисми албатта қисқа ва мавзунинг долзаблилигини ифодалаб, унда жуда кўп сўз ва ҳар хил мантиқсиз иборалардан фойдаланмаслик зарур.

Шундан сўнг курс иши масаласи ва мақсадини шакллантириш керак. Бу шакллантириш қасқа ва мазмунли бўлиши зарур. Унинг вазифаси – иш ёзилишининг тактикасини аниқлаш керак. Курс ишининг асосий мақсади бу қўйилган масалани ечими ва мақсадини ифодалашдир. Охирида, услубияти ва тадқиқот усули ёритилади.

Курс ишини асосий қисми кириш қисмида ёритилган масалани ечишга бағишланади. Одатда асосий қисми икки булимга ажратилади, айрим ҳолларда уч қисмга ажратилади. Бу бўлимларда масалани ечилиши мантиқан кетма-кет жойлаштирилади.

Хулоса муаллиф томонидан бажарилган ишлар ва тадқиқот натижалари ёритилади. Бу мавзу бўйича бажарилган ишнинг истиқболда кутиладиган натижалари кўрсатилади. Бу кейинги БМИ ва башқа илмий тадқиқот ишларини танлашда кўмаклашади.

Хулоса ёритилгандан сўнг талаб етилган кўрсатма билан фойдаланилган адабиётлар рўйхати келтирилади, агар курс ишида илова мавжуд бўлса, у алоҳида охирги саҳифаларда кўрсатилади ва номерланади.

Шуни есдан чиқармаслик керакки, рефератлар, докладлар ва назоарт ишларидан курс ишини фарқи ҳеч бўлмаганда унинг мустақил бажарилиши билан ажралиб тўриши керак. Бу ерда мустақил иш деганда илмий мустақил ишни бажариш назарда тутилмоқда.

Курс ишида талаба қанчалик даражада бошланғич илмий фикрлашга кўникма ҳосил қилганлигини кўрсатиш керак. Шунинг учун талабага муаммони аниқ, равон ва мутахассислик даражасида қўйиш керак. Муаммони қўйиш – фандаги биринчи қадамдир.

Бундан ташқари курс иши ўқиш даврида бир марта ёзилмайди. Шунинг учун, бирор мавзуни олиб уни кетма – кет равишда чуқурлаштириб бориш ва бу муаммони ривожлантириб келажакда шу муаммо бўйича нафақат БМИ мавзусини бажаришга балки, магистрлик диссертасия мавзусини танлашга тайёрлаб бориш мақсадга мувофиқдир.

Тайёрланган курс иши кафедрага топширилади. Мос қонун қоидалар асосида курс ишининг илмий раҳбари ёзма тақризида унга қўйилган баҳони асослаб бериш керак. Курс иши кафедрада ҳимоядан ўтгач унинг натижаси муҳокама қилинади ва қўйилган баҳо кафедра протоколига киритилади.

Курс ишининг баҳолаш меъзонига танланган мавзунинг долзарблиги, материалларни чуқур ўзлаштирганлиги, маънбани танлаш ва улардан фойдаланганлиги, қизиқарли иловалар ва ёзишнинг умумий кўриниши кабилар киради.

Курс иши ҳимоясига тайёрланиш

Курс иши ҳимоясига тайёрланишни ҳимоя жараёнлари кунинг санаси аниқ бўлгандан сунг дарҳол бошлаш керак. Бунда нутқ сўзлаш учун матн тайёрлаш ва шу каби бир қанча тайёргарлик ишларини бажариш лозим бўлади. Ҳимояга тайёрланишнинг муҳим ишларидан бири бу ҳимояга шахсан тайёргарлик кўриш, шунингдек ёзма ишга тақриз ва хулосалар тайёрлашлар

киради.

Ҳимояга тайёргарлик кўриш. Чиқиш вақтини тақсимлаш курс иши ҳимоясини ташкил етишга ва қолган бошқа барча ҳимоя қилиш жараёнлари ҳамда ҳимояни ўзида муҳим ўрин тутади. Вақт тайёрланишда ва ҳимоя қилишда енг муҳим омил ҳисобланади. Қоида бўйича ҳимоя учун 1 ҳафтадан 4 ҳафтагача вақт кетади.

Ҳимояни давомийлигини ҳисобга олиш, ҳимоя вақтида қайси енг муҳим омилларга еътибор бериш кераклигини билиш талаб етилади. Ҳимоянинг умумий давомийлиги 10 минутдан 20 минутгача чузилиши мумкин.

Ҳимоя матнини тайёрлаш. Демак, чиқиш учун қанча вақт кетишини ва қайрда бўлиб утишини билгандан сўнг талаба курс ишининг матнини тайёрлайди.

Тайёрланиш ўз ичига қўйидагиларни олади:

- чиқиш мазмунини ўйлаб кўриш;
- чиқиш режаси ва ишланмаларини тайёрлаш;
- чиқишнинг асосий матнини тайёрлаш;
- унинг оҳанги ва айтилишига тайёргарлик.

“Ҳимоядаги” матн устида ишнинг бошланғич босқичи ҳақида чиқишни ташкил етиш зарур.

Комиссия аъзоларини нимани ешитишни олдиндан билиш. Чиқишни шундай ташкил етиш керакки, қатнашчилар кутган саволларнинг натижасини олсин. Бош мавзудан четга чиқмаслик керак. Чиқишда қаттиқ овозда аниқ ва равон сўзлаш зарур.

11. БМИ мавзулари банки ва уни бажариш бўйича услубий тавсиялар

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ
АМАЛИЙ МАТЕМАТИКА ВА ИНФОРМАТИКАФАКУЛТЕТИ
«Тадбиқий математика ва информатика» йўналиши бўйича
«Ахборотлаштириш технологиялари» кафедраси талабаларининг битирув ишлари мавзулари банки

№	Мавзу
1	Информацияни узатиш ишончлигини назорат қилишнинг шартли эҳтимолли модел, алгоритм ва программавий воситаларини ишлаб чиқиш
2	Информацияни узатиш ишончлигини назорат қилишнинг нейротармоқли модел, алгоритмлари ва программавий воситаларини ишлаб чиқиш
3	Параллел ҳисоб услублари асосида ўзбек тилидаги электрон матнлар орфографиясини назорат қилиш модел, алгоритмлари ва программавий воситаларини ишлаб чиқиш
4	Ўзбек тилидаги электрон матнларнинг орфографиясини назорат қилиш тизимининг графематик модели, алгоритмлари ва программавий воситаларини ишлаб чиқиш
5	Корхоналар кўрсаткичларини таҳлил ва башорат қилиш алгоритм ва программавий воситаларини нотиниқ мантиқ моделлар асосида ишлаб чиқиш
6	ОЎЮ кадрларининг сонли ва сифатли кўрсаткичларини тахлил қилувчи нейронотиниқ тизим модели, алгоритмлари ва программавий воситаларини ишлаб чиқиш
7	Олий таълимда ўқув жараёни сифатини бошқариш ахборот тизимининг модел, алгоритм ва программавий воситаларини яратиш
8	Масофавий таълимда ўқитиш жараёнини бошқариш ахборот тизимининг дастурий таъминотини яратиш
9	Имкониятлари чекланган шахслар учун мўлжалланган мултимедиали електрон ўқув қўлланма яратиш
10	Эллиптик тенгламаларга асосланган очиқ калитли крипто тизим алгоритми ва унинг дастурий воситаларини яратиш
11	Антивирус программалар яратиш механизмларини ишлаб чиқиш ва уларни қўллаш
12	Ностационар жараённи башорат қилишда кўп ўлчамли маълумотларнинг корреляция функцияси бўйича информатив белгиларни танловчи алгоритмларни ишлаб чиқиш
13	Маълумотларга нейротармоқли ишлов берувчи тизимни ўргатишда параболик сплайн-функсиялар бўйича идентификация ва муаянлаштирувчи алгоритмларни ишлаб чиқиш
14	Кўп факторли башорат модели асосида ностасионар жараён маълумотларига ишлов берувчи тизим учун информатив белгиларни танлаш алгоритмлари
15	Таҳлил ва башоратловчи нейронотиниқ тизими учун ностасионар обектлар динамик таснифларининг тегишлилик функсияларини шакллантирувчи алгоритмларни ишлаб чиқиш
16	Нотиниқ семантик гипертармоқ модели бўйича Электрон матнлардаги хатоларни аниқловчи ва тузатувчи тизим алгоритмларни ишлаб чиқиш

Битирув малакавий ишни бажариш бўйича услубий тавсиялар

Битирув малакавий ишни бажаришдан мақсад талабанинг институтда олган назарий ва амалий билимларини мустаҳкамлаш ва кенгайтириш ҳамда олинган билимларини ишлаб чикаришга тавсия этишдан иборат. Олий ўқув юртларида битирув малакавий ишни бажаришга қўйиладиган талаблар Ўзбекистон Республикаси Олий ва Ўрта махсус таълим вазирлигининг 2010 йил 9 июндаги 225 - сонли буйруғи билан тасдиқланган.

Битирув малакавий ишларининг мавзуси илмий раҳбар томонидан белгиланиб кафедра ва факультетнинг илмий кенгаши томонидан тасдиқланади. Талабаларга малакавий ишларини мавзуларини танлаш ҳуқуқи берилади. Ишнинг раҳбари малакавий ишнинг мавзусига мувофиқ талабага малакавий ишга тегишли материалларни тўплаш бўйича (жумладан малакавий амалиёт ўтказиш даврида ҳам) топшириқ беради. Малакавий иш раҳбари ишниг бажарилишини режалаштиради. Асосий адабиётлар, маълумотлар, мавзу бўйича қилинган илмий ишлар ҳақида манбаъларни тавсия этади. Ишнинг ҳар бир бўлими қарор ва хулосалар билан ёритилади. Малакавий ишда бажарилган ишларнинг натижалари ёки бошқа муаллифларнинг (илмий мақолалари, илмий ишлари, жадвал, графиклар асосида, диаграмма, схема, расмлар шаклида) ишлари акс эттирилиши ёки улардан фойдаланиш мумкин. Асосий қисмида малакавий ишнинг мазмунини қисқа ва муайян шаклида ифодалаши лозим. Унда расмлар гарафиклар диаграммалар схемалар илова этилади. Асосий қисми қўлёзма тарзида расмийлаштирилган бўлиб 10 - 15 минг сўз ҳажмда белгиланади. Малакавий ишни олий ўқув юртининг ўқув тажриба лабораторияларида, ишлаб чиқариш корхоналарида ва илмий тадқиқот институтларида бажариш мумкин. Малакавий ишнинг бажарилишини раҳбар назорат қилиб, талаба кафедра мудири ва раҳбар олдида малакавий битирув иши ҳакида қисқача ҳисобот бериб боради.

Малакавий ишни ҳимоя қилиш. Белгиланган тартибда расмийлаштирилган малакавий иши талаба томонидан раҳбарга тақдим этилади. Раҳбар малакавий ишини талаб даражасида бажарилганлигига ишонч билдиргач ўз тақризи билан бирга у кафедра мудирига тақдим этилади. Тақризда малакавий ишнинг янгилиги ва ижобий томонлари тавфсифланади. Кафедра йиғилишида тақдим этилган материаллар асосида малакавий ишни талаба томонидан ДАК да ҳимоя қилишга киритиш ҳақида қарор қабул қилинади. Агар кафедра талабаниг малакавий ишини ҳимояга киритиш мумкин эмас деб ҳисобласа кафедра мажлисида раҳбар иштирокида муҳокама этилади. Ҳимояга киритилган малакавий иш тақризчига юборилади. Битирув малакавий ишлари ҳимоя қилингач олий ўқув юртида сақланади.

Бакалавриат талабаларнинг битирув малакавий иши реферотив ва илмий тадқиқотлар асосида бажарилиши мумкин.

Реферотив шаклдаги битирув малакавий ишини қуйидаги шаклда бажариш тавсия этилади:

- **Титул варағи;**
- **Кафедрадаги муҳокама қароридан кўчирма;**
- **Битирув малакавий ишниг топшириғи;**
- **Мундарижа;**
- **Асосий қисм 2-3 та бобни ичига олади (50-60 бет);**
- **Адабиётлар шаҳри;**
- **Хулоса ва таклифлар (3-5 бет);**
- **Фойдаланилган адабиётлар рўйхати;**

Касбий таълим йўналиши талабалари кўрсатилганлардан ташқари яна 1 та боб “Мавзуни ўқитиш услуби” ни қўшимча тайёрлайдилар.

Титул варағида Ўзбекистон қишлоқ ва сув хўжалик вазирлиги ҳамда олийгоҳнинг номи, кафедра номи, битирувчи талабанинг исми шарифи ва фамилияси, мутахассислик шифри, йўналиш номи, битирув малакавий ишининг мавзуси (катта шрифда), битирув ишига раҳбарлик қилган илмий раҳбарнинг исми ва фамилияси ёзилади. Кафедрада

кўриб чиқилгач уни ҳимояга тавсия этиш учун кафедра мудири кўриб чиқилган санани ёзиб имзо билан тасдиқлайди. Сўнгра иш деканатга топширилади. Факультет декани ишни кўриб чиқилган санани имзо билан тасдиқлаб тақриз ёзиш учун бошқа кафедрага жўнатади (1 - илова).

Кафедранинг муҳокама қароридан кўчирма. Битирув иши кафедрада кўриб чиқилгач ҳимояга тавсия этилади. Кафедра қароридан кўчирма кафедрада битирув иши бўйича талабаниг маърузаси эшитилганлиги асосида берилади. Талаба ўз маърузасида битирув ишининг моҳиятини аниқ ва равон тушунтириб берилса ва кафедра аъзолари ҳамда илмий раҳбарнинг фикрига кўра асосий ҳимояга тавсия этилади. Кўчирма кафедра мудири ва котиб томонидан тасдикланади. (3 - илова).

Битирув малакавий ишнинг топшириғида (4 - илова) олийгоҳ номи, факультет, йўналиш шифри ва номи, кафедрани номи ёзилган бўлиб талабанинг исми фамилияси, битирув иши мавзуси институт илмий кенгашининг қарор билан тасдиқланган бўлиши, мавзунинг долзарблиги, назарий ва амалий аҳамияти битирув ишини бажариш учун тавсия қилинадиган илмий, ўқув услубий ва бошқа ахборот манбалари, иш бўйича маълумотларни тўплаш ҳамда тадқиқот ишлари олиб бориш манбалари ва жойлари кўрсатилади. Шунингдек, битирув ишини тайёрлаш бўйича амалга ошириладиган ишлар режасида ишнинг мазмуни мавзу бўйича маълумотларни тўплаш ва таҳлил қилиш, олинган натижаларнинг назарий ва амалий аҳамияти бўйича хулоса бериш, ҳамда тадбиқ соҳалари ва усулларига оид таклифлар тайёрлаш, битирув ишини расмийлаштириш ва унинг ҳимояси учун зарурий кўргазмали воситаларни (жадвал, расм, график, диаграмма стенд ва ҳ.к) тайёрлаш. Бундан ташқари, ҳимояга чиқиш учун матн тайёрлаш кўрсатилади. Таҳминий ҳажми (бет) ижро муддати (сана), рақамлар билан кўрсатилган бўлиши керак. Топшириқ варақаси илмий раҳбар ва кафедра мудири томонидан имзо билан тасдиқлангач олийгоҳ ўқув ишлари бўйича ректор муовини томонидан имзо ва муҳр билан тасдиқланади (тасдиқланган сана, ой ва кун ёзилади).

Рефератив шаклдаги битирув иши учун қуйидаги қисмлар бўлиши тавсия этилади.

Мундарижада ишнинг мазмуни ёритилган боб ва бўлимлар кўрсатилади (2 - илова).

Кириш қисмида мавзунинг долзарблиги, янгилиги, аҳамияти қишлоқ хўжалик соҳасида республикамизда амалга оширилаётган ишлар, ҳукумат қарорлари битирув ишининг мақсад вазифалари ёритилади.

Асосий қисмда мавзу бўйича бир неча бўлим бўлиб унинг адабиётлар шарҳида битирув иши мавзусига оид илмий манбалар ва илмий тадқиқот ишлари қисқача баён этилиб муаллифларнинг исми шарифи келтирилади. Сўнги йилларда нашр этилган адабиётларда ва интернет маълумотларидан фойдаланилади. Шунингдек, тажрибаларда ўрганилган экиннинг етиштириш технологияси технологик хариталар, жадвал, расм, диаграмма кўринишларида ёритилади. Хулоса ва таклифлар қисмида ўрганилган адабиётлар маълумотлари асосида хулосалар қилинади.

Фойдаланилган адабиётлар рўйхатида битирув ишида фойдаланилган адабиётлар рўйхати ва илмий манбалар, муаллифларнинг исми шарифи мақола номи, нашр қилинган жойи ва вақти кўрсатилиб, алфавит шаклида дастлаб маҳаллий нашрлар, сўнгра ҳорижий манбалар кўрсатилади.

Илмий тадқиқотлар асосида бажарилган битирув малакавий иши.

Титул варағида Ўзбекистон қишлоқ ва сув хўжалик вазирлиги ҳамда олийгоҳнинг номи, кафедра номи, битирувчи талабанинг исми, шарифи ва фамилияси, мутахассислик шифри, йўналиш номи, битирув малакавий ишининг мавзуси (катта шрифда), битирув ишига раҳбарлик қилган илмий раҳбарнинг исми ва фамилияси ёзилади. Кафедрада кўриб чиқилгач уни ҳимояга тавсия этиш учун кафедра мудири кўриб чиқилган санани ёзиб имзо билан тасдиқлайди. Сўнгра иш деканатга топширилади. Факультет декани ишни кўриб чиқилган санани имзо билан тасдиқлаб тақриз ёзиш учун бошқа кафедрага жўнатади (1 - илова).

Кафедранинг муҳокама қароридан кўчирма. Битирув иши кафедрада кўриб чиқилгач ҳимояга тавсия этилади. Кафедра қароридан кўчирма кафедрада битирув иши бўйича талабанииг маърузаси эшитилганлиги асосида берилади. Талаба ўз маърузасида битирув ишининг моҳиятини аниқ ва равон тушунтириб берилса ва кафедра аъзолари ҳамда илмий раҳбарнннг фикрига кўра асосий ҳимояга тавсия этилади. Кўчирма кафедра мудири ва котиб томонидан тасдикланади (3 - илова).

Битирув малакавий ишнинг топшириғида (4 - илова) олийгоҳ номи. факультет. йўналиш шифри ва номи, кафедрани номи ёзилган бўлиб талабанинг исми, фамилияси, битирув иши мавзуси институт илмий кенгашининг қарор билан тасдиқланган бўлиши, мавзунинг долзарблиги, назарий ва амалий аҳамияти битирув ишини бажариш учун тавсия қилинадиган илмий, ўқув услубий ва бошқа ахборот манбалари, иш бўйича маълумотларни тўплаш ҳамда тадқиқот ишлари олиб бориш манбалари ва жойлари кўрсатилади. Шунингдек, битирув ишини тайёрлаш бўйича амалга ошириладиган ишлар режасида ишнинг мазмуни мавзу бўйича маълумотларни тўплаш ва таҳлил қилиш, олиб борилган тажрибалар, тадқиқот ишлари натижаларини таҳлил қилиш (боб, бўлим ёки қисмлар бўйича), олинган натижаларнинг назарий ва амалий аҳамияти бўйича хулоса бериш, ҳамда тадбиқ соҳалари ва усулларига оид таклифлар тайёрлаш, битирув ишини расмийлаштириш ва унинг ҳимояси учун зарурий кўргазмали воситаларни (жадвал, расм, график, диаграмма стенд ва ҳ.к) тайёрлаш. Бундан ташқари, ҳимояга чиқиш учун матн тайёрлаш кўрсатилади. Таҳминий ҳажми (бет) ижро муддати (сана), рақамлар билан кўрсатилган бўлиши керак. Топшириқ варақаси илмий раҳбар ва кафедра мудири томонидан имзо билан тасдиқлангач олийгоҳ ўқув ишлари бўйича ректор муовини томонидан имзо ва муҳр билан тасдиқланади (тасдиқланган сана, ой ва кун ёзилади).

Мундарижада ишнинг мазмуни ёритилган боб ва бўлимлар кўрсатилади (2 - илова).

Кириш (3 - 5 бет). Мавзунинг долзарблиги, илмий тадқиқот ишининг аҳамияти, мақсад вазифалари, илмий янгилиги ва ишлаб чиқаришдаги аҳамияти кўрсатилади.

Адабиётлар шарҳида мавзуга оид илмий манбалардан фойдаланилади. Олинган маълумотлар муаллифлари, йили кўрсатилиб баён этилади ва булардан ташқари интернет сайтлари маълумотлари ҳам келтирилади.

Тадқиқот ўтказиш шароити ва услублари. Бунда тадқиқот ўтказилган жой тупроғи, иқлими, ўрганилаётган экиннинг агротехникаси, тадқиқот мақсади, вазифалари ва объекти, тадқиқот услуби (тажриба схемаси, майдони, кузатиш ва ҳисоблаш усуллари) кўрсатилади.

Тадқиқот натижалари (15 - 20 бет) бир неча бўлимлардан иборат бўлиши мумкин, олинган маълумотлар жадваллар, расмлар, диаграммалар билан безатилади. Шунингдек тажрибада ўрганилган ўсимликнинг ўсув (вегетация) даври давомийлиги, ўсимликларнинг биометрик кўрсатикичлари маҳсулдорлик ва ҳосилдорлик кўрсаткичлари бўйича баҳоланади. Хулосалар тажриба мақсадидан келиб чиққан ҳолда олинган натижалар асосида баён қилинади. Бўлимни сўнгида хулоса берилади.

Хулоса ва таклифлар (3 - 5 бет). Мавзу бўйича муаллифнинг якуний хулосалар аниқ ва мантиқий ишнинг мазмунидан келиб чиққан бўлиши керак.

Фойдалаиилгаи адабиётлар руйхати. Алфавит шаклида, аввал маҳаллий нашрлар сўнгра хорижий ҳамда интернет сайтлари манбалари кўрсатилади. Бунда муаллиф фамилияси, исми, шарифи мақола номи, журнал номи, рақами, нашр қилинган вақти кўрсатилади.

Иловалар. Ҳосилдорлик кўрсаткичлари бўйича математик таҳлил маълумотлари, расмлар, интернет маълумотлари ва далолатномалар сингари қўшимача маълумотлар келтирилиши мумкин.

12. Глоссарий

Ўзбекистон Республикаси
Олий ва ўрта махсус таълим вазирлиги

Самарқанд Давлат университети

“Ахборотларни ҳимоялаш” фанидан атамалар лўғати

САМАРҚАНД - 2019

Амалий дастурлар - фойдаланувчиларга компютерда маълум амалларни бажаришга имкон берувчи дастурий воситалардир.
Антивируслар. Вирус-дастурларни излаб топувчи ва уларни зарарсизлантирувчи дастурий воситалардир.
Арифметик-мантиқий мослама - барча арифметик ва мантиқий амалларни бажаришга хизмат қилади. Қўшувчи сумматор ва маҳаллий бошқариш регистрларидан ташкил топган.
Архивлаш воситалари (ёки архиваторлар) - махсус усуллар билан файлларнинг ҳажмини қисиб, кичрайтиришга, яъни уларнинг архивларини ташкил қилишга хизмат қилувчи воситалардир.
Архивни янгилаш - архивдаги файлларнинг ескироқ версияси устига янги версиясини ёзиш.
Ахборот тармоғи - алоқа тизимларида компютерланинг бир-бири билан боғланиши.
Ахборот технологияси фани - ахборотларни жамлаш, сақлаш, узатиш ва шу жараёнларни амалга оширувчи техник воситаларни ишлатишни ўргатувчи фан.
Ахборот тизими - белгиланган мақсадга еришиш учун ахборотларни шакл ва мазмунига кўра турларга ажратиш, уларни сақлаш, излаш ва қайта ишлаш принсиплари, қайта ишлашда қўлланиладиган усуллар, шахслар ҳамда воситаларнинг ўзаро боғланган мажмуи.
Баённома (протокол) - компютерлар орасида маълумотларни узатиш тартиби ва форматини белгиловчи қоидалар мажмуи.
Белгили маълумот - алифбо-рақамли белгилар мажмуидан иборат маълумот тури.
Билимлар омбори - аниқ бир фан соҳасида тўпланган билимларни компютерда тасвирлаш ва қайта ишланган ахборотларни сақлашга мўлжалланган модел.
Билимлар омборини бошқариш тизими - маълумотлар омборини яратиш, юритиш ва фойдаланишга мўлжалланган дастур ва тил воситалари мажмуи.
Биологик бошқариш - ҳайвонот оламининг сақланиши, кўпайиши ва ривожланишини режали равишда тартибга солиш мақсадида биологик тизимларга ўтказиладиган таъсирдир.
Биологик модел - обектлар ва уларнинг қисмларига хос биологик тузилиш, функсия.
Бош калит - маълумотлар омборида саралаш ишларининг тез ва аниқ бажарилишига имкон берадиган жадвалнинг бир устуни.
Дастурий интерфейслар - компютер қурилмалари билан фойдаланувчи ишлатаётган дастурларнинг ҳамжиҳатликда ишлашини таъминловчи воситалардир.
Диагностика воситалари. Компютер қурилмаларининг ва магнит дискларининг ишлаш қобилиятларини ва ҳолатларини текширувчи ҳамда улардаги нуқсонли жойларни аниқлаб, иложи борича тузатувчи воситалардир.
Фойдаланувчи интерфейси - берилган масалага мос интерфейсни танлаш.
Фойдаланувчи муҳити - интерфейс тушунчасининг бошқача номланиши.
Информатика - ахборотлаштириш жараёнларини ҳамда шу жараёнларни автоматлаштириш усулларини ўргатувчи фан сифатида намоён бўлмоқда.
Интеллект - инсоннинг тафаккур юритиш қобилиятидаги (ақл, онг).
Интеллектуал ахборотли излаш тизимлари - иш жойидан туриб билимлар омбордаги керакли ахборотни излашга имкон берадиган тизимлар.
Интеллектуал интерфейс - интерфейс тушунчасини бошқача номланиши.
Интеллектуал китоблар - имтиҳон олувчи китобларга ўхшаш бўлиб, бунда ўқувчиларнинг қобилиятлари, билим даражалари махсус тестлар ёрдамида уларнинг компютер билан мулоқати жараёнида аниқланади ва баҳоланади.
Интеллектуал тизимлар - инсоннинг мантиқий фикрлаш усулини қўллаган ҳолда масалани ечадиган тизимлар.

Ишчи тизимлар - катта миқдордаги маълумотларни сақлаш, излаш, мураккаб ҳисоблашлар, моделлаштириш, дастурий таъминотни ривожлантиришга хизмат қиладиган воситалар.

Ишонтира олишлик хоссаси. Ҳар қандай информация бошқариш органи ишона оладиган даражада яъни бошқарилаётган объектнинг имконияти даражасида бўлиши керак. Имконият даражасидан четга чиқувчи ҳар қандай информация бошқариш жараёнининг бузилишига олиб келади.

Кодлаш - узлуксиз сигнални рақамлар орқали ифодалаш жараёни.

Компютерли моделлаштириш - ҳодиса ва жараёнларнинг моделини компютерда қуриш ва ўрганиш.

Маълумотлар базаси билан ишлаш воситалари. Турли маълумотлар базаларини ташкил қилиш, уларни бошқариш, улар устида турли амалларни бажариш (гуруҳлаш, тартибга солиш, нусха олиш ва ҳ.к.) ҳамда зарур маълумотларни турли мезонлар орқали (калит сўзлар, саналар, фан йўналишлари, мавзулар, муаллифнинг исми ва шарифи ва ҳ.к.) тезда излаб топиб беришга хизмат қилувчи воситалардир.

Маълумотлар модели - ахборотларни ифодаловчи воситалар мажмуи.

Маълумотлар омбори - компютернинг узоқ муддатли хотирасида сақланаётган берилганлар ва улар устида аниқ амалларни бажаришга имкон берадиган маълумотлар йиғиндиси.

Маълумотлар омборидаги доимий маълумотлар - маълумотлар омборининг узоқ муддат ўзгармай қоладиган елементлари.

Маълумотлар омборидаги ўзгарувчан маълумотлар - маълумотлар омборининг қиймати тез-тез ўзгартириб турадиган елементлари.

Маълумотлар омборини бошқариш тизими - маълумотлар омборидан фойдаланиш учун махсус яратилган дастур.

Маълумотлар омборини бошқаришнинг иерархик тизими - маълумотларнинг иерархик тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотлар омборини бошқаришнинг реляцион тизими - маълумотларнинг реляцион тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотлар омборини бошқаришнинг тармоқли тизими - маълумотларнинг тармоқли тизимини яратиш ва ундан фойдаланиш учун мўлжалланган маълумотлар омборини яратиш тизими.

Маълумотларни чегириш - ахборотлар тизимида кўрсатилган шартни қаноатлантирмаган элементларнинг маълумотлар омборига киритмай қолдириш ҳолати.

Маълумотларни тартиблаш - маълумотлар қиймати ва форматини фойдаланиш учун қулай ҳолатга келтириш жараёни.

Маъмурият тизимлари - тармоқни бошқарадиган тизимлар.

Математик модел - ўрганилаётган обектнинг математик формула ёки алгоритм кўринишида ифодаланган характеристикалари орасидаги функционал боғланиш.

Модел - бирор объект ёки объектлар тизимининг образи ёки намунаси.

Моделлаштириш - билиш объектларини уларнинг моделлари ёрдамида тадқиқ қилиш, мавжуд предмет ва ҳодисаларнинг моделларини ясаш ва ўрганиш.

Объект - ўзига ўхшашларидан ажралиб турадиган алоҳида олинган предмет.

Қимматлилик хоссаси. Бир мақсадга хизмат қилувчи бир нечта информация ичидан енг мақсадга мувофиқлари, яъни қимматлилари танлаб олиниши керак.

Қисқалик хоссаси. Информация қисқа ва мазмундор бўлиши, яъни унда ортиқча маълумотлар ёки такрорланишлар бўлмаслиги керак. Бу еса бошқаришни тез ва обектив кечишини таъминлайди.

Сонли маълумот - ихтиёрий сондан иборат маълумот тури.

Тўлалик хоссаси. Информациялар шароитга қараб, жаҳон фан ва техникасининг сўнги ютуқлари ҳамда бошқариш жараёнида тўпланган тажрибаларни ҳисобга олиб, узлуксиз равишда ўзгартирилиб, янгиланиб, тўлдирилиб борилиши керак. Бу еса бошқаришда замонавий усуллардан кенг фойдаланиш имконини беради ва объектнинг ҳар қандай ўзгаришларига бардошлиги, мослашиши даражасини оширади.

Тушунарлилик хоссаси. Информация - бошқариш органи (яъни ЕҲМ) тушуна оладиган ҳолатда (сараланган, кодлаштирилган, информация ташувчи воситаларга ёзилган) бўлиши, яъни дастлабки қайта ишлашдан ўтган бўлиши керак.

Ахборот манбаларига стратегик ҳужумлар - кўпинча, бир-бири билан уруш ҳолатида бўлган давлатларнинг бир-бирига нисбатан амалга оширилувчи ахборотий ҳужумларидир. Бундай ҳаракатларнинг асосий мақсади, рақиб давлатнинг ҳарбий аҳамиятга ега бўлган ахборот тизимларига кириб бориб, уларни ишдан чиқариш ёки уларда сақланаётган стратегик маълумотларни ўғирлаш ва йўқотишдир.

Бош калит - маълумотлар омборида саралаш ишларининг тез ва аниқ бажарилишига имкон берадиган жадвалнинг бир устуни.

Бошқариш мосламаси - енг мураккаб мослама бўлиб, барча қурилмалардан келувчи сигналларни қайта ишлайди ва бошқарувчи буйруқларни ишлаб чиқади, уларни керакли қурилмаларга узатади ҳамда шу буйруқларнинг бажарилишини назорат қилиб боради.

Бошқариш органи - системани қўйилган мақсадга мувофиқ бошқариш учун зарур тадбирлар, буйруқлар ишлаб чиқувчи ҳамда уларнинг бажарилишини назорат қилиб турувчи бўлимдир.

Бошқариш тизими - бошқариш субектлари - бошқарувчи тизимлар ва бошқариш обектлари - турли табиатли мураккаб динамик тизимлар мажмуи.

Чувалчанг («Черви») - бошқа дастурий воситаларни зарарламовчи, фақат ўзидан нусха олиб кўпаювчи вируслардир. Бундай вирусларнинг таъсири натижасида компютер хотираси бегона файллар билан (вирус-дастурларнинг нусхалари билан) тўлиб қолиб, унинг самарадорлиги кескин пасаяди.

Диагностика воситалари. Компютер қурилмаларининг ва магнит дискларининг ишлаш қобилиятларини ва ҳолатларини текширувчи ҳамда улардаги нуқсонли жойларни аниқлаб, иложи борича тузатувчи воситалардир.

Доктор ревизорлар - файл ва дискнинг тизимли соҳасидаги ўзгаришларни аниқлаш билан бирга, ўзгарган файлларни дастлабки ҳолатига қайтара оладиган вирусга қарши дастурлар.

Электрон котиблар. Бундай компютерлар - манзилгоҳлар, телефон рақамлари, жорий ишлар рўйхати, кун тартиби каби иш фаолиятида тез-тез зарур бўлиб турадиган електрон маълумотларни ташкил қилиш ва сақлашга хизмат қилувчи компютерлардир.

Электрон ёзув дафтарчалари. Електрон хотира дафтарчалари деб ҳам аталади. Електрон котиблар каби вазифаларни бажаради. Лекин улардан фарқи шундаки, бундай компютерларда айрим амалларни бажариш учун фойдаланувчи тамонидан дастур тузилмайди. Улар фақат хотирасига ёзилган стандарт амалларнигина бажариши мумкин.

Факс-серверлар - фойдаланувчиларга кўп адресли електрон факсимил алоқа хизматидан фойдаланишга имкон берувчи серверлар.

Фактографик тизим - содда ва қўйилган масалаларга ягона ҳамда аниқ ечимни кўрсата оладиган тизим.

ФАТ вируслари - ФАТ жадвалини ишдан чиқарувчи, яъни файлларнинг дискда жойлашувини кўрсатувчи жадвални ўзгартирувчи ёки йўқотувчи вируслар.

Файлли дискеталар - фойдаланувчининг файлларини сақловчи дискеталар.

Файл-менеджерлар - фойдаланувчининг МСДОС бошқарувида компютер билан

қулай ва кўргазмали равишда мулоқот олиб боришини таъминловчи дастурий воситалардир. Кўпинча *«қобиқ» дастурлар* деб ҳам айтилади.
Файл-серверлар - фойдаланувчиларга турли ахборот тизимларидаги файллар билан ишлашга имкон берувчи серверлар.
Филтр дастурлар ёки резидент дастурлар - вируслар томонидан зарарни кўпайтириш ва зиён етказиш мақсадида операцион тизимга қилинаётган мурожаатларни ушлаб қолиш ва улар ҳақида фойдаланувчига маълум қилиш вазифасини бажарувчи вирусга қарши дастурлар.
Гибрид вируслар - резидент файлли вирусларнинг ҳамда кўринмас вирусларнинг барча хусусиятларини ўзида мужассамлаштирган вируслар.

Ҳимоя филтрлари - фойдаланувчини мониторларнинг електрон-нурли трубкасидан тарқалаётган нурланишлардан (електромагнит, рентген, инфрақизил, ултрабинафша, радиочастотали) ҳимоя қилувчи воситалар.

Интернет - минглаб локал ва минтақавий компютер тармоқларини бир бутун қилиб бирлаштирувчи бутун дунё компютер армоғи.
Интернетнинг ахборотли қисми - Интернет тармоғида мавжуд бўлган турли електрон ҳужжат, график расм, аудиоёзув, ведеотасвир ва ҳоказо кўринишидаги ахборотлар мажмуи.
Интернетнинг дастурий таъминоти - тармоққа уланган компютерлар ва тармоқ воситаларини ягона стандарт асосида мулоқот қилиш, маълумотларни ихтиёрий алоқа канали ёрдамида узатиш даражасида қайта ишлаш, ахборотларни қидириб топиш ва сақлаш ҳамда тармоқда ахборот хавфсизлигини таъминлаш каби муҳим вазифаларни амалга оширувчи дастурлар мажмуи.
Интернетнинг техник таркибий қисми - турли русумдаги компютерлар, алоқа каналлари, тармоқ техник воситалари мажмуи.
Интранет - Интернет технологияси, дастур таъминоти ва баённомалари асосида ташкил етилган, маълумотлар омбори ва електрон жадваллар билан жамоа бўлиб ишлаш имконини беърувчи корхона ёки ташкилот миқёсидаги компютер тармоғи.
Кўринмас вируслар - резидент вирусларга ўхшайди, лекин улар ўзларининг борлигини сездирмасликка ҳаракат қилади яъни ўзларининг борлигини турли усуллар билан ниқобловчи вируслар.
Компютер вируслари - компютерда турли нохуш амалларни бажаришга мўлжаллаб ёзилган, ўлчами катта бўлмаган дастурлар.
Мантиқий «бомба» - махсус ўрнатилган санада ёки белгиланган шарт бажарилмаганда (масалан, вирус-дастур муаллифининг маоши оширилмаганда) ишга тушувчи вируслар.
Парол билан архивлаш - бегона фойдаланувчилар очмасликлари учун файлга парол қўйиб архивлаш.
Ревизор дастурлар - дастлаб дастур ва дискнинг тизимли соҳаси ҳақидаги маълумотларни хотирага олиб, сўнгра уларни дастлабкиси билан солиштирадиган ва мос келмаган ҳолларда фойдаланувчига маълум қиладиган вирусга қарши дастурлар.

Шифрланган вируслар - ҳар бир таъсир қилиш сиклидан кейин ўзининг кодланишини ҳам, жойлашишини ҳам ўзгартириб турувчи вируслар.

Шлюз - баённомани бир турдаги муҳитдан иккинчи турдаги муҳитга ўтказувчи тармоқ қурилмаси.

Тўлиқ ҳимоя филтрлари - енг юқори сифатли филтрлардан бўлиб, махсус қопламали ойнадан тайёрланган. Барча нурланишларнинг таъсирини 70-80% гача камайтиради.
Тўрли филтрлар - нурланишлардан яхши ҳимоя қила олмайди. Лекин улар кўзни ташқи ёритиш шуълаларидан ва екраннинг милтиллашидан ҳимоя қилиши мумкин.

Тозаловчи дискета - оддий дискетага ўхшаш бўлиб, фақат дискининг сатҳи махсус жилвир қоғоз билан қопланган дискета. Бундай дискета дисководнинг ўқувчи ва ёзувчи магнит каллакчасини турли ифлосликлардан, дисковод кўп ишлатилганда пайдо бўладиган оксидловчи қатламдан тозалашга хизмат қилади. Бунинг учун дискета дисководга ўрнатилиб, сунгра дисковод ишга туширилади.
Троя оти - ўзини оддий дастурлардек тутувчи, бузғунчилик фаолиятини еса фақат маълум амал бажарилгандагина (масалан, нусха олиш амали, файлни босмага чиқариш амали ва ҳ.к.) бошловчи вируслар.

Тузилган архив файлни текшириб кўриш - архив файлнинг зарарланган ёки зарарланмаганлигини ҳамда зарарланиш даражасини махсус буйруқ ёрдамида текшириш.

UnErase Wizard - тасодифан ўчириб юборилган файлларни қайта тиклашга имкон берувчи восита.

Утилитлар - тизим дастурлар сафига кирувчи дастурий воситаларлар. Компютернинг ҳамда унинг қурилмаларининг самарали ишлашини таъминлашга хизмат қилади.
Юкловчи сектор вируслари - дисклар ёки дискеталарнинг юкловчи секторини ишдан чиқаришга мўлжалланган, яъни шу секторларда жойлашган тизимли дастурларни зарарловчи вируслар.

Адабиётлар

1. Леонтьев В.. Новейшая энциклопедия персональгого компьютера. -М.: Олма пресс образование, Москва. -2005.
2. Қобулов В.Қ. Ақл мўжизаси. - Т,: Фан, Тошкент. - 1984.
3. Жуманов И.И., Мингбоев Н.С.. Информатика. Услубий қўлланма. – Самарқанд: СамДУ. - 2002.
4. Нурмуҳаммедов Т.А. ИБМ ПС ва МС ДОС билан ишлаш. - Т.: Фан, Тошкент – 1995.
5. Ғуломов С.С., Шермуҳаммедов А.Т., Бегалов Б.А. Иқтисодий информатика. – Т.: “Ўзбекистон”, Тошкент. – 1999.
6. Бройдо В.Л. Офис техникаси (бошқариш ва иш юритиш учун). – Т.: Меҳнат, Тошкент. - 2001.
7. Қобилов С.С., Жуманов И.И. СУБД и информасионние системи. – Самарқанд: СамДУ. - 1997.
8. Арипов М. Интернет ва електрон почта алоқаси. - Т.: «Университет».- 2000.
9. Жуманов И.И., Мингбоев Н.С. Ҳисоблаш системаларининг информацион асослари. – Самарқанд: СамДУ. – 2002.
10. Ғуломов С.С. ва бошқалар. «Иқтисодий информатика». - Т.: Фан - 1999.
11. Рахмонқулова С.И. ИБМ ПС шахсий компютерида ишлаш. - Т.: Фан, Тошкент – 1999.
12. Насретдинова Ш. Wиндowс учун Ехсел саҳифаларида. - Т.: Фан. – 1999.
13 Фигурнов В.Э. ИБМ ПС для пользователя. - М.: Инфра, 1996.
14 Шафрин Ю. Основы компьютерной технологии. - Б.: Туркистон, Бишкек. – 1998.

13. Илова

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

САМАРҚАНД ДАВЛАТ УНИВЕРСИТЕТИ

«Ахборотлаштириш технологиялари» кафедраси

“АХБОРОТ ХАВФСИЗЛИГИ”

фанидан бакалавр йўналишлари талабалари учун лаборатория ишларини бажариш бўйича

УСЛУБИЙ КЎРСАТМА

Тузувчи:
Холмонов С.М.

Самарқанд – 2010

КИРИШ

Компьютер технологияларининг, айниқса Интернетнинг жадал суръатлар билан кенг тарқалиши натижасида тармоқда маълумотларнинг кескин кўпайишига олиб келди. Бу маълумотларни тармоқда ҳимоялашда (маълумотлардан ижозатсиз фойдаланишнинг олдини олиш мақсадида) криптография усулларидан фойдаланиш ва уларнинг янги алгоритмларни ишлаб чиқиш замонавий ҳамда актуал муаммолардан бири бўлиб ҳисобланади.

Компьютер технологияларининг тараққиёти криптогафиянинг қўлланиш соҳасини кенгайтириб унга янги масалаларни қўйди.

Ҳозирги вақтда маълумотларни шифрлашда криптографик алгоритмларидан фойдаланиш мураккаб бўлмаган масалардан бири бўлиб ҳисобланади. Чунки замонавий юқори босқичли алгоритмик тилларда яратилган дастурлар орқали берилган маълумотларни шифрлаб керакли жойга тармоқда узатиш тизимлари кўплаб яратилган ва улар фойдаланувчиларга қўл келмоқда. Аммо тармоқдаги криптографик усуллар билан шифланган маълумотларни очиш ва уларни бузиш ҳоллари ҳам мовжуд. Буларни олдини олиш мақсадида криптографик усулларнинг янги динамик алгоритмларини ишлаб чиқиш мақсадга муофиқдир.

Ҳозирги вақтда криптографиянинг икки ишлатилиш соҳаси мовжуд: маълумотларни узатишда ҳимоялаш ва уларни сақлашда ҳимоялаш. Уларнинг ҳар бири криптографияга ўзининг хусусий талабларини қўяди ва муайян масалалар ечимида ўз тасдиғини топади.

I. Қисм. Назарий асослар

§1.1. Криптография

Маълумотларнидан ижозатсиз фойдаланишнинг олдини олиш мақсадида уни ўзгартириб ифодалаш қадимдан маълум. Унинг кўп сонли йўллари ва усуллари ишлаб чиқилган, такомиллаштирилган ҳамда улардан фойдаланиб келинмоқда. Информатика ва информацион технологияларнинг ривожланиши бу процесснинг тезлашига туртки бўлди. Бунинг асосий сабабларидан бири глобал тармоқларнинг пайдо бўлиши ва улардаги коммерцион (давлатлараро, харбий, иқтисодий, комерцион ва шахсий характерли) маълумотларни ўз вақтида ҳимоялаш, иккинчи томондан эса янги кучли компьютерларнинг ҳамда тармоқ технологияларининг ривожланиши натижасида кечаги очилиши мумкин бўлмаган криптографик тизимнинг ечими топилишидир.

Маълумотларни шакл ўзгартириш орқали ҳимоялаш муаммолари билан криптология (***krypt*os** - яширин, **l*ogos*** - фан) ўрганади. Криптологиянинг маълумотларни ўзгартириб ифодалашнинг янги математик усулларини топиш ва улар устида изланишлар олиб борувчи бўлими криптография дейилади.

Компьютер технологияларининг, айниқса Интернетнинг жадал суръатлар билан кенг тарқалиши натижасида тармоқда маълумотларнинг кескин кўпайишига олиб келди. Бу маълумотларни тармоқда ҳимоялашда (маълумотлардан ижозатсиз фойдаланишнинг олдини олиш мақсадида) криптография усулларидан фойдаланиш ва уларнинг янги алгоритмларни ишлаб чиқиш замонавий ҳамда актуал муаммолардан бири бўлиб ҳисобланади.

Компьютер технологияларининг тараққиёти криптогафиянинг қўлланиш соҳасини кенгайтириб унга янги масалаларни қўйди.

Ҳозирги вақтда маълумотларни шифрлашда криптографик алгоритмларидан фойдаланиш мураккаб бўлмаган масалардан бири бўлиб ҳисобланади. Чунки замонавий юқори босқичли алгоритмик тилларда

яратилган дастурлар орқали берилган маълумотларни шифрлаб керакли жойга тармоқда узатиш тизимлари кўплаб яратилган ва улар фойдаланувчиларга қўл келмоқда. Аммо тармоқдаги криптографик усуллар билан шифланган маълумотларни очиш ва уларни бузиш ҳоллари ҳам мовжуд. Буларни олдини олиш мақсадида криптографик усулларнинг янги динамик алгоритмларини ишлаб чиқиш мақсадга муофиқдир.

Ҳозирги вақтда криптографиянинг икки ишлатилиш соҳаси мовжуд: маълумотларни узатишда ҳимоялаш ва уларни сақлашда ҳимоялаш. Уларнинг ҳар бири криптографияга ўзининг хусусий талабларини қўяди ва муайян масалалар ечимида ўз тасдиғини топади.

Барча криптографик алгоритмлар симметрик ва асимметрик алгоритмларга бўлинади. Симметрик алгоритмларда маълумотларни шифрлаш ва уларни очиш битта калит сўзлари орқали содир этилади. Калит сўзларининг тез-тез янгиланиши маълумотларнинг кўпроқ ҳимояланганлигини кўрсатади. Калит сўзларининг тез-тез алмашинуви маълумотлар физик алмашинувига таъсир этганлиги сабабли амалида ҳар бир узатиш вақти учун алоҳида калит сўзлари ишлаб чиқилади ва улар орқали маълумотлар шифрланади ва аслига қайтарилади.

Асимметрик алгоритмлар яқинда пайдо бўлди ва криптографияда янги соҳа очди. Бу турдаги алгоритмлар икки қисмдан: шифрлаш учун калит ва шифрланган маълумотларни очиш учун калитдан иборат бўлади.

Асимметрик моделда ижозатсиз мурожаатларнинг олдини олиш мақсадида очиқ калитларни ҳақиқийлигини тасдиқлашнинг махсус усулларини (сертификация) ишлаб чиқиш талаб этилади. Бундан ташқари бу моделдан фойдаланилганда қўшимча маълумотлар алмашинувининг пайдо бўлиши ҳисобига тармоқнинг ишлаш тезлиги сезиларли даражада камаяди.

Юқоридагиларни ҳисобга олган ҳолда тармоқда маълумотларни ҳимоялашнинг криптографик усулларидан қайси бирини танлаш фойдаланувчининг ўзига ҳавола этилади.

Криптографикада маълумотларни шифрлашда ишлатиладиган кодларини

яширинлишини таъминлаш муҳим рол ўйнайди. Чунки тармоқдаги маълумотга рухсатсиз кирувчида барча информациялар (криптограмма матни ва алгоритм ҳақида маълумот) ва дастурий воситалар мавжуд. Унга фақат бир нарса – калит сўзи (калит рақамлар) етишмайди. Бундай ҳолда калит сўзи (калит рақамлар)ни топиш учун мумкин бўлган барча ҳолатларни қараган ҳолда матнни очиб уни таҳлил қилиш керак. Бу энг секин бажариладиган, лекин тўғри йўлдир. Калит сўзлар узунлиги мумкин бўлган ҳолатларнинг сонини оширади ва натижада криптографиянинг турғунлигини сақлаш критерияси бўлиб ҳисобланади.

§1.2. Шифрлаш ва шифрларни очиш

Фараз қилайлик, жўнатувчи олувчига бирор хабар юбормоқчи. У бу маълумотни олувчидан бошқа бирор кишининг ўқиимаслигини ҳохлайди. Хабар очиқ матндан иборат бўлади. Бу очиқ матнни бегоналар ўқий олмайдиган ҳолга келтириб шакл алмаштиришга шифрлаш дейилади. Натижада шифрли-матн хабар ҳосил қилинади. Шифр-матнли хабарни тескари алмаштириб ўз ҳолига келтириш шифрларни очиш дейилади.

Очиқ матнли хабарларни ижозатсиз фойдаланувчиларлад ҳимоя қилиш йўллари ва усулларини ўрганувчи фан криптография деб аталади.

Криптография билан шуғулланувчи кишиларни криптографлар дейишади.

Криптотаҳлил бу– шифрланган матнли хабарни очиш (оригиналига мос келадиган матнни топиш) муаммолари билан шуғулланиш бўлиб бунлай соҳада фаолият кўрсатидиган кишиларни криптоаналитиклар деб аташадилар.

Фаннинг криптография ва криптотаҳлилни бирлаштирувчи бўлими криптология бўлиб ҳисобланади.

Шифлаш ва шифрларни очишнинг математик содда моделини қуйидагича тушинтириш мумкин:

Очиқ матнни P ҳарфи (инглизча plaintext сўздан) билан белгилайлик. Очиқ матн матнли файл, битли тасвир, рақамлаштирилган мусиқа ва

бошқалар бўлиши мумкин. Шифрли-матнни С ҳарфи билан (инглизча ciphertext сўздан) белгилансин. Шифрли-матн ҳажми айрим ҳолларда асл матн ҳажмидан катта ёки кичик бўлиши мумкин. Шифрли-матн тармоқ орқали керакли жойга узатилиши ёки компьютер хотирасида сақланиши керак. Очиқ матнни шифрлаш ва шифрли-матнни олиш математикада қуйидаги функция билан аниқланади:

E(P) = C

Бу ерда E шифрлаш алгоритми функцияси.

Шифрли-матнни очишни қуйидагича кўрсатиш мумкин:

Д(C) = M

Шифрли-матнни очганда асл матн ҳосил бўлишини ҳисобга олиб қуйидаги ифодани кўрсатишимиз керак:

Д(E(P)) = P

§1.3. Аутентификация, яхлитлик ва ишончлилик

Тармоқларда маълумотларни шифрлаб узатишда аутентификация, яхлитлик ва ишончлилик тушинчалари катта роль ўйнайди.

Аутентификация. Маълумотни қабул қилувчи маълумот кимдан келганини билиши ва унга ишонч ҳосил қилиши керак. Бу а**утентификация** дейилади.

Яхлитлик. Хабарни қабул қилувчи хабар узатилиши пайтида унга ўзгартиришлар киритилганлигини ёки уни бошқа хабар Билан алмаштирганлигини аниқлаш хабарни яхлитлигини текшириш дейилади.

И**шончлилик.** Хабарни юборувчи шифпли-матнни ишончлигига кафил бўлади ва уни ишончоигини инкор этмайди.

Маълумотларни тармоқда узатишда юқорида келтирилган тушинчалар ката роль ўйнайди, чунки маълумот алмашинуви катта масофада иштирокчиларнинг бир-бирларини кўрмасдан ҳосил қилинади. Шунинг учун ҳар бир маълумот алмашинувида хабарнинг аутентификацияси, яхлитлиги ва ишончлилиги таъминланган бўлмоғи зарур.

§1.4. Шифрлар ва калитлар

Шифрлаш ёки шифрлаш алгоритми деб аталувчи криптографик алгоритм шифрлашда ва шифрни очишда ишлатиладиган математиканинг оддий ёки махсус функциялардир. Бу функцияларнинг бири ахборотларни (матнлар ёки белгиларни) шифрлашда ишлатилса иккинчиси уни очишда ишлатилади.

Криптографик алгоритмнинг ишончлилиги фойдаланилган алгоритмнинг сирлигига боғликда бўлса шифрлашнинг бундай алгоритми чегараланган дейилади. Чегараланган алгоритмли шифрлаш замонавий криптографиянинг талабларига жавоб бермайди. Чунки маълумот алмашинувчиларнинг ҳар бирининг ўз алгоритмлари мовжуд бўлишлари керак ва уларга мос келувчи дастурий воситалар яратилган бўлиб стандарт дастурларнинг тузилиши шарт эмас.

Замонавий криптография бу масаланинг ечими сифатида бир ёки бирнеча алгоритмларни яратиш ва уларнинг дастурий воситаларини ишлаб чиқиш, улар учун яширин калитлар ўрнатишни тавсия қилади.

Калитлар К ҳариф билан белгиланади ва калитлар соҳаси деб аталувчи фазога қарашли қийматларнинг бири бўлади. Бу ҳолда шифрлаш функцияси Е ва шифрлани очувчи функция D ҳам калит К га боғлик бўлади. Бу тушинчани қуйидаги ифодалар орқали ифодалаймиз:

Е к (Р) = С

Д к (С) = Р

Бу ерда ҳам қуйидаги тасдиқ ўринли бўлади:

Д к (Е к (Р)) = Р

Айрим криптографик алгоритмларда шифрлашда бир калит К1, шифрларни очишда бошқа калит К2 ишлатилади. Бу ҳолда ҳам юқоридагидек ифодаларни ёзиш мумкин:

Е к 1 (Р) = С

Д к2 (С) = Р

Д к2 (Е к1 (Р)) = Р

Калитлар ёрдамида шифрлаш алгоритмининг ишончлилиги

калитларнинг яширинлигига боғлик бўлиб алгоритмни яширишнинг ҳожати қолмайди.

§1.5. Шифрлашнинг симметрик алгоритмлари

Калитлар ёрдамида шифрлашнинг икки хили: симметрик ва асимметрик (очиқ калитлар) усули мовжуд.

Ахборотларни шифрлашда ва шифрларни очишда бита калитдан фойдаланиш, ёки шифрларниочишдаги калитни шифрлаш калитидан ҳосил қилиш симметрик алгоритмли криптография бўлиб ҳисобланади. У бир калитли алгоритм деб ҳам аталади.

Бир калитли алгоритмниг ишончлилиги калитнинг танланишига боғлик бўлади ва бу калит қаттик сир ҳолда сақланади.

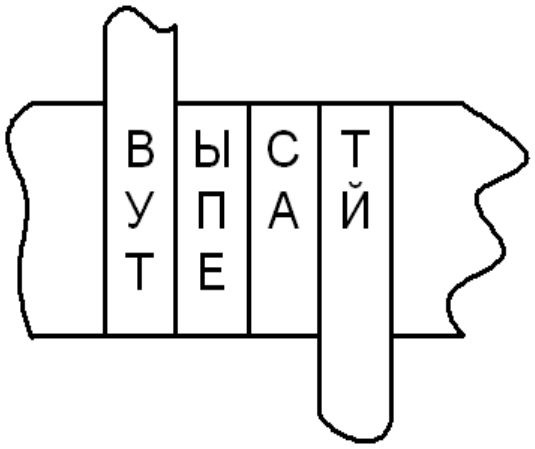
Симметрик алгоритмли шифрлашда юқорида келтирилган ифодалар ишлатилади:

Е к (Р) = С

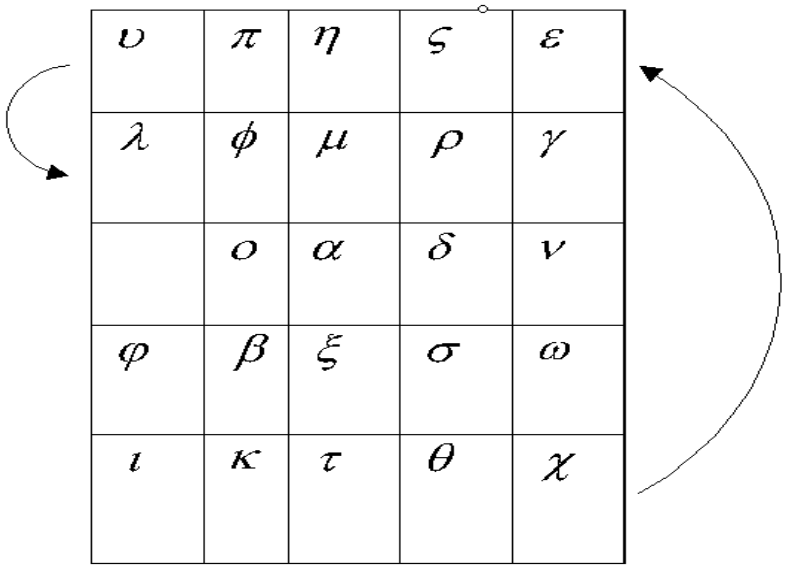
Д к (С) = Р

§1.6. Шифрлашнинг айрим алгоритмлари

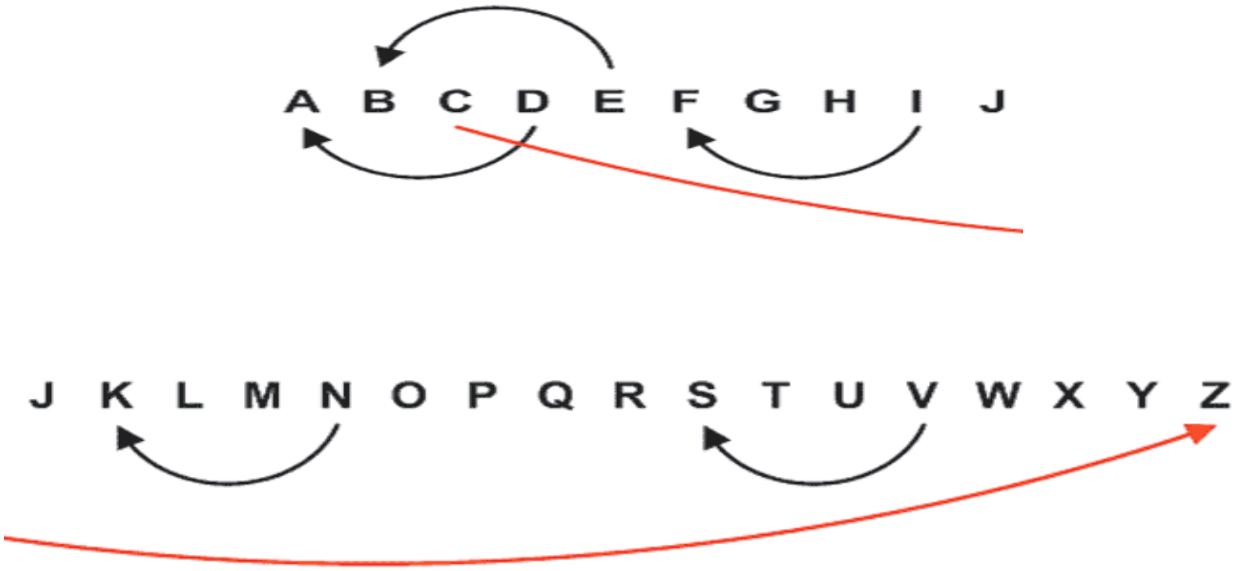
1. Қуйидаги шаклдаги алгоритмда бўйича шифрлашда ахборотлар бирор матрица шаклида ёзилади ва шифрланган матн матрицанинг устунлари бўйича ўқилади. Бундай алгоритмларни компьютерларда ижро этиш осон.



2. Бу алгоритмда ҳам маълумотлар жадвал кўринишида тасвирланиб шифрланиш пайтида берилган қоида асосида жадвалнинг элементлари танланади. Масалан, а(1,5), а(2,5), а(3,5) ва ҳакозо.



3. Матн сатри элементлари берилган қоида асосида шифрлаш пайтида ўз ўринларини алмаштиради. Масалан, 4-элемент 1-чи элемент ўрнига келади, 5-чи элемент 2-чи элемент ўрнига келади, 3-чи элемент эса охирги элемент ўрнига келади ва ҳакозо.



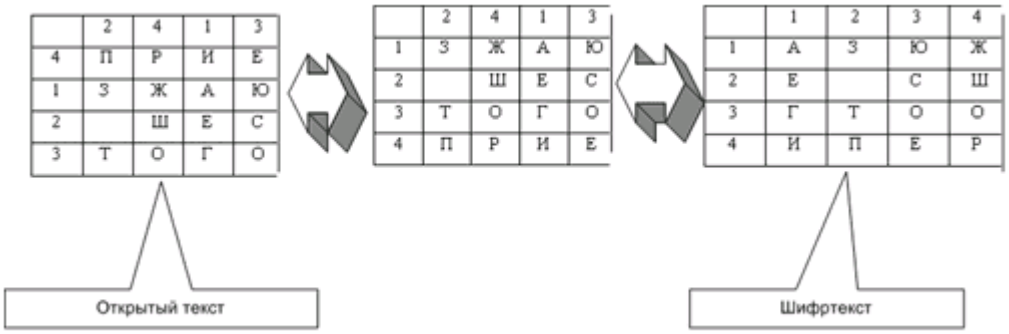
4. Шифрланадиган матн жадвалнинг устунлари бўйича тўлдирилади ва шифрлаш пайтида жадвал элементлари сатрлар бўйича ўқилади. Бу алгоритм дастурлашга қўлай бўладиган алгоритмлардан ҳисобланади.

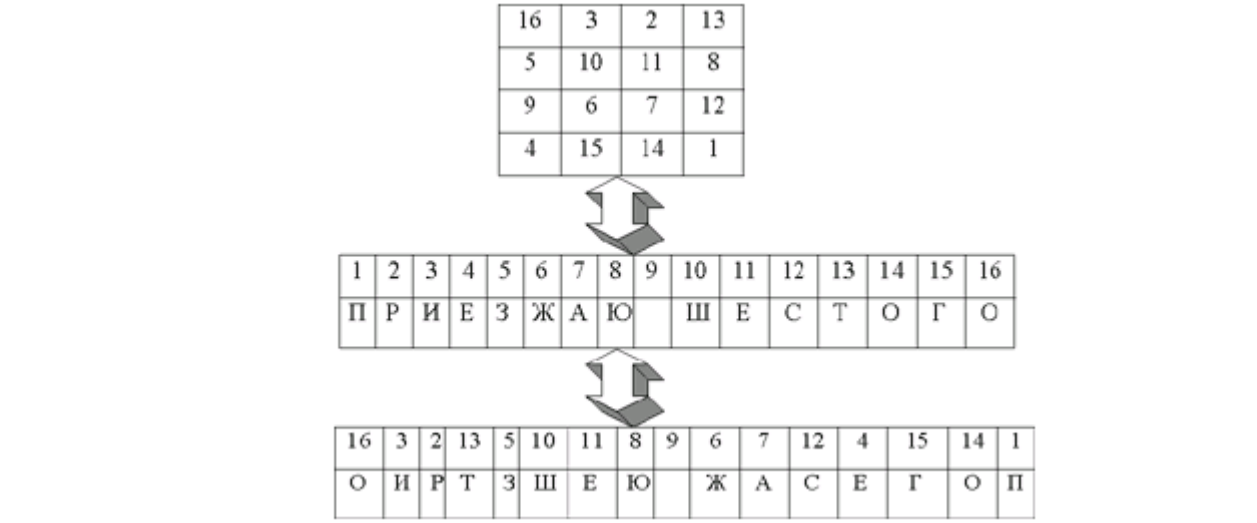
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Л	У	Н	А	Т	И	К
4	7	5	1	6	2	3
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

1	2	3	4	5	6	7
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

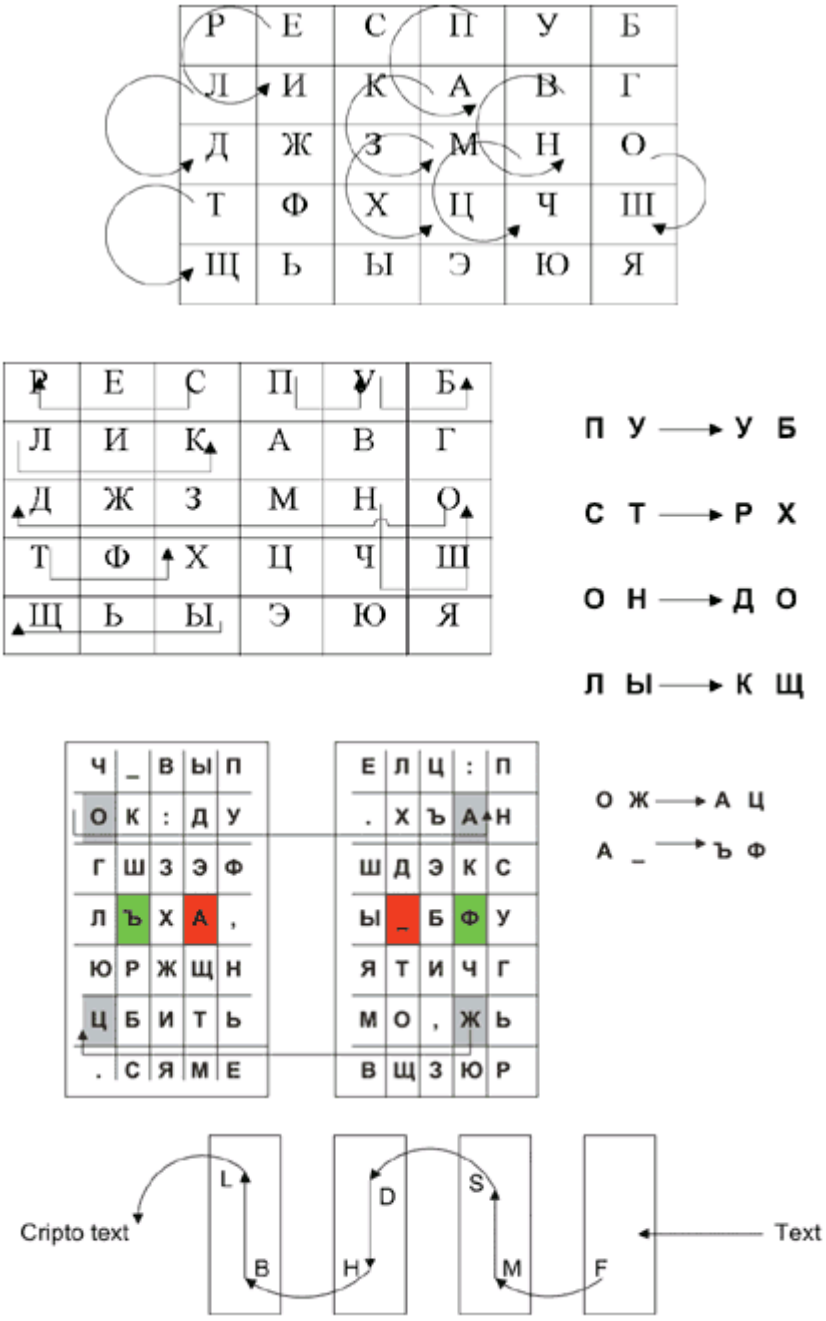
5. Шифрлаш алгоритми шакл орқали кўрсатилмокда.





6. Шифрланадиган матн саҳифаси жадвал (матрица)га жойлаштирилади ва уни шифрлаш жадвал устунлари ва сатрлар номерлари комбинацияларидан иборат сонлар кетма-кетлигига боғлик бўлади.

Қуйида шифрлашнинг бошқа алгоритмларининг тасвирлари келтирилмоқда. Бу алгоритмларнинг айримлари кейинги мавзуларда ёритилади.



§1.7. Очиқ калитли шифрлаш алгоритмлар

Очиқ калитли шифрлаш алгоритмлар (асимметрик алгоритмлар)ида шифрларни очишдаги калитлар шифрлашда ишлатиоган калитлардан тубдан фарқ килади ва уни сир сақлашнинг хожати йўқ.

Ҳозирги пайтда очиқ калитли критпографик алгоритмлар ичида энг яхши деб тан олнгани RSA (алгоритм яратувчиларининг номлари: Rivest, Shamir, Adelman) бўлиб ҳисобланади.

RSA алгоритмининг марказий қисмини бир жуфт очиқ калитни яратиш ташкил этади. Калитларни ҳосил қилиш қуйидагича содир этилади:

1. Тасодифий равишда иккита содда (фақат ўзига ва 1 га бутун бўлинадиган) сонлар танланади, p ва q, $p \neq q$.
2. Ҳисобланади $r=p*q$.
3. Ҳисобланади $\phi=(p-1)*(q-1)$.
4. Очиқ (Ко) ва яширин (Кс) калитлар танланади. Бу калитлар ϕ га нисбатан ўзаро содда бўлиб $(Ко*Кс) \bmod \phi = 1$ шартни қаноатлантиришлари керак.

Очиқ калит Ко ҳақидаги маълумотларни шифрлаш учун қуйидагилар бажарилади:

1) Берилган матн блокларга ажратилади, уларнинг ҳар бири M(i)=0, 1, …, n-1 сон шаклида тасвирланган бўлишлари мумкин;

2) M(i) кетма-кет сонларни қуйидаги формула бўйича шифрлаймиз $C(i)=(M(i)^{Ко}) \bmod n$, бу ердаги кетма-кет C(i) сонлар шифрланган матнни аниқлайди.

Ушбу шифрланган маълумотларни яширин Кс калит билан очиш учун қуйидаги ишларни бажарамиз:

$M(i)=(C(i)^{Кс}) \bmod n$.

Натижада берилган матнни ифодалайдиган M(i) сонлар тўплами ҳосил бўлади.

Мисол.

Қуйидаги “CAB” матнни очиқ калитли RSA алгоритми билан шифрлаш алгоритми келтирилади. Соддалик учун кичик сонлардан фойдаланамиз.

1. Танлаймиз p=3, q=11.
2. Ҳисоблаймиз r=3*11=33.
3. Ҳисоблаймиз $\phi=(p-1)*(q-1)=20$.

4. ϕ билан ўзаро содда бўлган махфий калит Кс ни танлаймиз, масалан Кс=3 бўлсин.

5. Кс ва ϕ асосида очиқ калит Ко ни ҳисоблаймиз.

Ко ни ҳисоблайдиган алгоритмнинг Паскаль алгоритмик тилдаги дастурини келтирамиз:

```
Program RSA;
Var
 I,k0,kc,f,y:integer;
g,u,v:array[0..50] of integer;
BEGIN
      Readln(kc,f);
      G[0]:=f; g[1]:=kc;
      U[0]:=1; u[1]:=0;
      V[0]:=0; v[1]:=1;
      i:=1;
            while g[i]<> 0 do
                  begin
                        g[i]:=u[i]*f+v[i]*kc;
                        y:=g[i-1] div g[i];
                        g[i+1]:=g[i-1]-y*g[i];
                        u[i+1]:=u[i-1]-y*u[i];
                        v[i+1]:=v[i-1]-y*v[i];
                  end;
      k0:=v[i-1];
      if k0<0 then k0:=k0+f; writeln(k0);
END.
```

Натижа: Ко=7.

6. Шифрланадиган матнни 2...28 диапазондаги бутун сонлар кетма-кетлиги каби тасаввур этамиз. А ҳарфига 2 сони, В ҳарфига 3 сони, С ҳарфига 4 сони мос келсин. У ҳолда “CAB” матинни

қуйидаги кетма-кетлик шаклида тасвирлаш мумкин {5, 3, 4}. Матнни очиқ калит Ко=7 орқали шифрлаймиз:

$C1 = (5^7) \bmod 33 = 78125 \bmod 33 = 14,$

$C1 = (3^7) \bmod 33 = 2187 \bmod 33 = 9,$

$C3 = (4^7) \bmod 33 = 16384 \bmod 33 = 16.$

7. Шифрни махфий калит Кс=3 билан очиш учун қуйидаги {14, 9, 16} сонлар тўплами ҳосил бўлди. Ҳисоблаймиз:

$M1 = (14^3) \bmod 33 = 2744 \bmod 33 = 5,$

$M1 = (9^3) \bmod 33 = 729 \bmod 33 = 3,$

$M1 = (16^3) \bmod 33 = 4096 \bmod 33 = 4.$

Натижада (“CAB”) матнига мос келувчи {5, 3, 4} сонлар тўплами ҳосил бўлди.

Ушбу алгоритмнинг мураккаблиги ва шифрни очишдаги қийинчилик танланадиган сонларнинг катталигига боғликда бўлади, масалан 200 та рақамдан иборат сон танланса махфий калитни ҳосил қилиш учун 10^{23} атрофидаги операцияларни бажариш талаб этилади.

§1.8. Криптотаҳлили ҳужумлар

Криптотаҳлил бу – шифрланган ахборотни қайта ишлаб унинг асл ҳолатини тиклашдан иборатдир. Муаффақиятли криптотаҳлил натижасида нафақат шифранган ахборотнинг асл ҳолатини балки унинг шифрлаш калитини ҳам ҳосил қилиши мумкин. Шунинг учун криптотаҳлилни шифрланган ахборотларга нисбатан қилинган ҳужум деб қабул қилинади.

Криптотаҳлилли ҳужумнинг 4 асосий типлари аниқланган:

1. Фақат шифрланган матнни билган ҳолда криптотаҳлилли ҳужум. Криптотаҳлилчида бир хил алгоритм билан шифрланган бир неча маълумотлар мавжуд. У шифрланган маълумотларни очиши ва

очиқ калитни топиб кейинги шифрланган маълумотларга қўллаши керак. Бу масаланинг математик моделини қуйидагича кўрсатиш мумкин:

Берилган

$C_1=E_{к1}(P_1),\ C_2=E_{к2}(P_{12}),\ ..,C_i=E_{кi}(P_i)$

Топиш керак

$P_1,\ P_1, . . . , P_n$ ёки $к_1, к_2, . . . , к_n$

2. Очиқ матнли билган ҳолда ҳужум. Криптотаҳлилчи шифранган маълумотларни ҳамда уларнинг очиқ матнларини билади. У шулар асосида калитни қўлга киритиш билан шуғулланади. Бу масаланинг математик ифодасини келтирамиз:

Берилган:

P1, C1 = Ек1(P1), P2, C2 = Ек2(P2),..., Ри, Си = Еки(Ри).

Топилиши керак:

К1, К2, . . , Ки .

3. Танланган очиқ матнли ҳужум. Криптоаналитик нафақат шифрланга ва очиқ матнли ахборотларни билади, балки бу ахборотларни маъносини ҳам чиқара олади. Бу ҳолда ҳам ундан калитни топиш талаб қилинади. Бу масаланинг математик модели ҳам юқорида келтирилганидек бўлади.
4. Танланган очиқ матнли адаптирлашган ҳужум. Бу ҳужум танланган очиқ матнли ҳужумнинг бир кўриниши бўлиб унда криптоаналитик шифрланган очиқ матнни танлабгина қолмайди, балки шифрлаш натижасига кўра танлашларни ҳам ўзгартириши мумкин.

§1.9. Шифрлаш алгоритмларининг мустаҳкамлиги

Ҳар хил криптографик алгоритмлар ҳар хил мустаҳкамликга эга бўлишади. Мустаҳкамлик криптоаналитикнинг шифрни қандай қийинчилик билан очишига боғлик. Шифрни очиш учун кетадиган вақт ва унга кетадиган

сарф-харажатлар катта бўлиб ахборотни сир сақлаш муддатидан кўп бўлса бундай алгоритмларни мустаҳкам деб ҳисобласа бўлади. Шифрланган ахборотлар ва уларнинг мустаҳкамлигига боғлик қуйидаги қоида мовжуд:

- ***Сир сақланадиган маълумотнинг баҳоси криптоаналитиклар томонидан шифрни очишга сарфланадиган харажатдан кам бўлмоғи керак.***

Криптоаналитик ҳужумнинг мураккаблиги

Криптоаналитик ҳужумнинг мураккаблигини уч катталик Билан характерлаш мумкин:

- Маълумотлар бўйича қийинлик. Муоффақиятли криптоаналитик ҳужум учун керакли маълумотларнинг етарлилиги.
- Ҳисоблашларнинг мураккаблиги. Муоффақиятли криптоаналитик ҳужум учун керакли вақтнинг етарлилиги.
- Хотиралар бўйича мураккаблик. Муоффақиятли криптоаналитик ҳужум учун керакли хотира майдонинг етарлилиги.

Криптоаналитик ҳужумнинг қийинлигини экспонентал функция кўринишда тасвирлаш қабул қилинган. Масалан, ҳужумнинг қийинлик даражаси2^{128} бўлсин. Демак, шифрни очиш учун 2^{128} та прерация бажарилиши керак экан.

§1.10. Шифрлашнинг алмаштириш ва ўрин алмаштириш алгоритмлари

Шифрлашнинг алмаштириш ва ўрин алмаштириш алгоритмлари кенг қўлланилади. Бунда элементлар бошқа элементлар билан алмаштирилади ёки элементлар ўз ўринларини алмаштириладилар.

§1.11. Алмаштирувчи шифрлар

Классик криптографияда алмаштирувчи шифрларнинг 4 хил кўриниши мовжуд:

1. Оддий алмаштириш ёки бир алфавитли алмаштириш (monoalphabetic). Очиқ матннинг ҳар бир ҳарифи бирор символ билан алмаштирилади.
2. Омофонли алмаштириш (homophonic). Бунда оддий

алмаштиришдан фарқли равишда ҳар бир ҳарифлар бир неча символлар билан алмаштирилади.

3. Блокли алмаштириш (polyalphabetic). Очиқ матн блокларга айлантирилади ва ҳар бир блок алоҳида символлар билан алмаштирилади.
4. Кўп алфавитли алмаштириш (polygram). Бунда очиқ матннинг бирор символи бир неча символлар ичидан танлангани билан алмаштирилади. Танланиш очиқ матн символининг ўрни билан аниқланади.

§1.12. Ўрин алмаштиришли шифрлаш

Бу алгоритмда очиқ матндаги символлар бошқалари билан алмаштирилмайди, балки уларнинг ўринлари алмаштирилади. Масалан, очиқ матн жалвалнинг сатрлари бўйича ёзилади ва ўқиш эса устунлари бўйича содир этилади.

Ўрин алмаштиришли шифрлашда икки карали ўрин алмаштиришлар ҳам содир этилиши мумкин. Бу ҳолат икки калитли шифрлаш дейилади.

Бевосита ўрин алмаштириш бўйича шифрлаш

Monoalphabetic синфига кирувчи тизимларда берилган матн символлари қатъий боғланган бошқа символлар билан алмаштирилади. Бундай тизимнинг криптографик калити жорий алфавитга мос келувчи янги ўрин алмаштириш жадвалидир. Бундай тизимнинг энг содда шифрлаш алгоритмида алфовитдаги ҳар бир ҳариф k позицияга сурилади, бу ерда k шифрлаш калитидир.

Цезарь алгоритми

Цезарь алгоритми ҳам шунга асосланган бўлиб уни қуйидаги ифода билан тасвирлаш мумкин:

$$E_k(i) = (i+k) \bmod 26.$$

Масалан, k=3 деб ҳисобланганда лотин алифбосида i=0 ўринда турадиган A ҳарфи i=3 ўринда турувчи D ҳарфи билан алмаштирилади, чунки,

$$(i+k) \bmod 26 = (0+3) \bmod 26 = 3$$

Ёки лотин алифбосида i=25 ўринда турадиган z ҳарфи i=2 ўринда турувчи C ҳарфи билан алмаштирилади, чунки,

$$(i+k) \bmod 26 = (25+3) \bmod 26 = 2$$

Мисол.

Берилган матн: CRYPTOGRAPHYANDDATASECURITY.

Шифротекст :FUBSWRJUDSKBDQSGDWDVHFXULWB.

Шифрни очиш алгоритми қуйидагичадир

$$D_k(i) = (i+26-k) \bmod 26.$$

Ўрин алмаштиришнинг мураккаблашган усули

Юқорида келтирилган шифрлаш алгоритмини такомиллаштирамиз. Бунда берилган матн символлари позициялари калит k га кўпайтирилади. Унинг алгоритмини қуйидагича ифодалаш мумкин:

$$E_k(i) = (i*k) \bmod n,$$

Бу ерда i – берилган матн символи номери, n – берилган алфовитдаги символлар сони (n=26 лотин алифбоси учун ва n=256 ASCII-кодлари учун). Силжитиш ва кўпайтиришга асосланган шифрлаш алгоритмининг ифодаси қуйидаги кўринишда бўлади:

$$E_k(i) = (i*k_1+k_0) \bmod n.$$

Криптографик тизимларнинг homophonic синифида бошланғич символни алмаштиришнинг бир нечита варианти аниқланган бўлади. Масалан, A ҳарфи 24, 35, 37 рақамлар билан, B ҳарфи эса 41, 17, 76 рақамлар билан алмаштирилиши мумкин.

Криптографик тизимларнинг polyalphabetic синфи бир қанча ҳар хил калитлардан фойдаланишга асосланган. Қуйидаги кўринишли берилган матн

$$X = x_1\ x_2\ x_3\ x_4 \dots x_p\ x_{p+1} \dots x_{2p} \dots$$

k1, k2, …, kp калитлар орқали :

$$E_k(X) = E_{k1}(x_1)\ E_{k2}(x_2) \dots E_{kp}(x_p)\ E_{k1}(x_{p+1}) \dots E_{kp}(x_{2p})$$

шакилда шифрланади.

Шундай алгоритмларнинг бирини XVI асрда француз Вигенер (Vigenere) таклиф этади.

Бу ерда калит K

$$K = k_1\ k_2 \dots k_p,$$

шакилда тасвирланади. Бу ерда ki (1 <= i <= p) берилган алфовитдаги силжишлардир.

Берилган матн символлари қуйидаги формула бўйича шифрланади

$$E_k(i) = (i + k_j) \bmod n,$$

бу ерда i –берилган матн символи номери, Kj - калит, $j \in \{1, \dots, n\}$.

Вижинернинг шифрлаш тизими.

Биринчи бўлиб Вижинер тизими 1586-йилда чоп этилган ва у кўп алфавитли тизимга нисбатан юқорироқ ўринда туради. Вижинер тизими Цезар шифрлаш тизимига қараганда мукаммалроқ ҳисобланиб, унда калит ҳарфидан ҳарфга алмаштирилади. Бундай кўп алфавитли алмаштириш шифрини шифрлаш жадвали орқали ифодалаш мумкин. Қуйидаги биринчи жадвалда Вижинернинг лотин алфавити учун мос келувчи жадвал кўрсатилган. Бу жадвалдан матнни шифрлаш ва уни очиш учун ишлатилади. Жадвалнинг иккита кириши бўлиб:

- Юқори қатордаги харфлардан кирувчи очиқ ёзув учун фойдаланилади.
- Чап устундан эса калит ҳарфларидан фойданилади.

Мисол учун калит кетма-кетлигини р-деб олайлик, у холда калит р-алфавитли р-сатрдан иборат бўлади.

$$\pi = (\pi_0, \pi_1, \dots, \pi_{r-1});$$

Вижинернинг шифрлаш тизимида очиқ матн $x = (x_0, x_1, \dots, x_{n-1})$ ва шифрланганn матн $y = (y_0, y_1, \dots, y_{n-1})$ кўринишга эга. $\pi = (\pi_0, \pi_1, \dots, \pi_{r-1})$ калит ёрдамида қуйидагича муносабатда бўлади.

$$x=(x_0,x_1,\ldots,x_{n-1}) \qquad y=(y_0,y_1,\ldots,y_{n-1});$$

$$(y_0,y_1,\ldots,y_{n-1})=(\pi_0(x_0),\pi_1(x_1),\ldots,\pi_{n-1}(x_{n-1}));$$

Юқоридаги ифодадан маълумки Вижинер жадвали орқали шифрлашда матннинг (ахборотнинг) хар бир ҳарфига мос келувчи калитнинг ҳар бир ҳарфи орқали уларнинг устун ва сатрлари кесишмасига мос келувчи ҳарфлар олинади.

Агар ўзбек алфавити ишлатилса, Вижинер матрицаси [36x36] ўлчамга эга бўлади.

АБВГД..... .....ЎҚҒҲ_
БВГДЕ..... ....ҚҒҲ_А
ВГДЕЖ..... .....ҒҲ_АБ
....._АБ
ВГ..... ....ЯЎҚҒҲ

Вижинер матрицаси.

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

1-қадам. Узунлиги М символли калит К ни танлаш.

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

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

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

5) К калитнинг алмаштирилувчи s_{0r} символга мос k_m символи аниқланади;

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

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

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

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

Расшифровка қилиш қуйидаги кетма-кетликда амалга оширилади.

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

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

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

Агар калит сифатида <ВАЗА> сўзи танланган бўлса, шифрлаш матрицаси бешта қатордан иборат бўлади.

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_
ВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_АБ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_
ЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_АБВГДЕЁЖ
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЬЪЭЮЯЎҚҒҲ_

«Ваза» калити учун шифрлаш матрицаси.

Мисол. К= <ВАЗА> калити ёрдамида Т=<БАЙРАМ КУНИ> дастлабки матни шифрлансин.

Шифрматн $Т_1$ қуйидагича бўлади: ГАСРВМЖКХНП

Ўринларни алмаштириш усулларига мисол сифатида яна қуйидагиларни келтириш мумкин:

— шифрловчи жадвал;

— сеҳрли квадрат.

Шифрловчи жадвал усулида калит сифатида қуйидагилар қўлланилади:

— жадвал ўлчовлари;

— сўз ёки сўзлар кетма-кетлиги;

— жадвал таркиби хусусиятлари.

Мисол.

Қуйидаги матн берилган бўлсин:

КАДРЛАР ТАЙЁРЛАШ МИЛЛИЙ ДАСТУРИ

Ушбу ахборот устун бўйича кетма – кет жадвалга киритилади:

К	Л	А	Л	И	Й	Т
А	А	Й	А	Л	Д	У
Д	Р	Ё	Ш	Л	А	Р
Р	Т	Р	М	И	С	И

Натижада, 4х7 ўлчовли жадвал ташкил қилинади.

Энди шифрланган матн қаторлар бўйича аниқланади, яъни ўзимиз учун 4 тадан белгиларни ажратиб ёзамиз.

КЛАЛ ИЙТА АЙАЛ ДУДР ЁШЛА РРТР МИСИ

Бу ерда калит сифатида жадвал ўлчовлари хизмат қилади.

Сеҳрли квадрат деб, катакчаларига 1 дан бошлаб сонлар ёзилган, ундаги ҳар бир устун, сатр ва диагонал бўйича сонлар йиғиндиси битга сонга тенг бўлган квадрат шаклидаги жадвалга айтилали.

Сеҳрли квадратга сонлар тартиби бўйича белгилар киритилади ва бу белгилар сатрлар бўйича ўқилганда матн ҳосил бўлади.

Мисол.

4х4 ўлчовли сеҳрли квадратни оламиз, бу ерда сонларнинг 880 та хар хил комбинацияси мавжуд. Қуйидагича иш юритамиз:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Бошлангич матн сифатида қуйидаги матнни оламиз:

ДАСТУРЛАШ ТИЛЛАРИ

ва жадвалга жойлаштирамиз:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Шифрланган матн жадвал элементларини сатрлар бўйича ўқиш натижасида ташкил топади:

ИСАЛ УТИА ШРЛЛ ТРАД

§1.13. Роторли машиналар

Роторли машиналар очиқ матннинг ҳар бир симолини маълум бир позицияга суришдан иборат. Бундай шифрлаш дастурлаш учун осон булсанидек криптоаналитиклар учун ҳам қийинчилик туғдирмайди.

§1.14. Бир марталик блокнотлар

Бир марталик блокнотлар энг мустаҳкам шифрлашлардан бири бўлиб ҳисобланади. Бу алгоритм бўйича шифрлашда узун тасодифий харфлар кетма-кетлигидан фойдаланилади. Тасодифий ҳарифлар кетма-кетлиги шифрлашда фақат бир марта ишлатилади. Шифрни очишда тасодифий

харфлар кетма-кетлигидан иборат блокнот нусхаси ишлатилади. Ҳар бир янги алоқада янги тасодифий харфлар кетма-кетлиги фойдаланилади.

§1.15. Шифрлашнинг компьютерли алгоритмлари

Информатика ва информацион технологияларнинг ривожланиши криптографияга ҳам ўз таъсирини ўтказмоқда. Мутахассислар томонидан бир қанча компьютерлашган алгоритмлар яратилган. Бу алгоритмлар сифатида қуйидагиларни келтириш мумкин:

- Data Encryption Standard (DES). АҚШ давлатининг стандари бўлиб ҳисобланадиган симметрик алгоритм.
- RSA (River, Shamir, Adiemam). Очиқ калитли шифрлаш алгоритми.
- ГОСТ 28147-89. Россиянинг давлат стандарти, симметрик шифрлаш алгоритми.

§1.16. Сир сақланадиган калит узунлиги

Симметрик криптосистемаларнинг мустаҳкамлиги унда ишлатилган алгоритм ва сир сақланадиган калитнинг узунлилиги боғлиқ бўлади. Фараз қилайлик, идеал алгоритм мовжуд, уни ижозатсиз очиш учун фақат мумкин бўлган барча калитларни бирма-бир кўриб чиқиш керак. Криптоаналитиканинг бу ҳужуми тотал кўздан кечириш дейилади.

Агар сир сақланадиган калитнинг узунлиги 64 битдан иборат бўлса, 1 секундда 1 млн. калитни текширадиган суперкомпьютер барча мумкин бўлган имкониятларни 5 минг йилда текшириб бўлади.

II. Қисм. Амалий топшириқлар

Лаборатория иши

Мавзу: Бевосита ўрин алмаштириш бўйича шифрлаш

Кириш. Ахборотларни қайта ишлаш жараёнларини автоматлаштириш воситалари, усуллари ва формалари мураккаблашуви ва ривожланиши бўйича уларни ахборот технологияларида уларни қўлланилиш хавфсизлик даражасидан ошиб бормоқда.

1.Ишдан мақсад: Симметрик криптотизимни асосий усулларини ўрганиш ва тадқиқ этиш.

2.Қисқача назарий маълумот:

Назарий маълумотлар услубий кўрсатманинг биринчи қисмида ҳамда мавзу бўйича ташкиллаштирилган адабиётларда келтирилган.

3. Ишни бажарилиш тартиби ва қўйилган вазифа:

Асосий матн шифрлаш усулларидан бирида шифрлансин ва қадамма – қадам изоҳлансин. Шунингдек **TP**, **Delpi** дастурлаш тизимларидан бирида дастурий таъминот яратилсин.

Ҳисобот мазмуни:

Иш мавзуси.

Ишдан мақсад.

Шифрлаш алгоритмининг блок-схемаси.

Дастур матни.

Илова ва натижа

Умумий хулосалар

4. Топшириқ вариантлари

- **ВАРИАНТ №1. «Самарқанд давлат университети»** сўзи оддий ўрин алмаштириш усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №2. «Самарқанд давлат университети»** сўзи Цезарь усули билан шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №3. «Самарқанд давлат университети»** сўзи силжитиш ва кўпайтиришга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №4. «Самарқанд давлат университети»** сўзи кўпайтириш ва силжитишга асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;

- **ВАРИАНТ №5. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Жадвал устунлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №6. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Жадвал сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №7. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери силжитиш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №8. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери кўпайтириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №9. «Самарқанд давлат университети»** матни блокларга ажратилсин. Ҳар бир блок номери айириш калити сифатида олиниб матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №10. «Самарқанд давлат университети»** матни каррали силжитишга (силжитишлар символнинг жойлашган ўринлари номерига боғликда, масалан, калит k=3 да «Фан» сўзидаги «Ф» символи 3+1 га, «а» символи 3+2 га, «н» символи эса 3+3 га силжийди) асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №11. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда силжитиш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №12. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда кўпайтириш алгоритми асосида шифрлансин ва шифр очилсин;
- **ВАРИАНТ №13. «Самарқанд давлат университети»** матни тескари ўқиш ҳамда кўпайтириш ва силжитиш алгоритми асосида шифрлансин ва шифр очилсин;

- **ВАРИАНТ №14. «Самарқанд давлат университети»** матни 6*6 жадвалга жойлаштирилсин. Сатрлар ўрнига устунларни ёзиш орқали янги жадвал ҳосил қилинсин. Кейин эса сатрлари ўринларини алмаштириш усулига асосланган шифрлаш алгоритми асосида матн шифрлансин ва шифрлар очилсин;
- **ВАРИАНТ №15. «Самарқанд давлат университети»** матни «сеҳирли квадрат» жадвали асосида шифрлансин ва шифр очилсин;

5. Назорат саволлари

1. Криптография мақсади ва вазифаси.
2. Оддий ўрин алмаштириш усули ва калит сўзли ўрин алмаштириш усули.
3. Икки марталик қайта қуйиш усули ва сеҳрли квадрат усули.
4. Цезар усули ва калит сўзли Цезар тизими.
5. Криптографиянинг симметирик ва асимметрик усуллари.
6. Электрон имзо.
7. Шифрлашнинг компьютерли алгоритмлари.
8. Шифрлаш алгоритмларининг мустаҳкамлиги
9. Криптотаҳлили ҳужумлар ва уларнинг типлари
10. Аутентификация, яхлитлик ва ишончлилик

Фойдаланилган адабиётлар

9. Жельников В. Криптография от папируса до компьютера. М.: ABF, 1997. – 336с.
10. Нильс Фергюсон, Брюс Шнайер «Практическая криптография», М.: Издательский дом «Вильямс», 2005г.-424с.
11. Петров А.А. «Компьютерная безопасность. Криптографические методы защиты», М.: ДМК, 2000г. -448с.
12. Коблиц Н. Курс теории чисел в криптографии. – М., Научное издательство ТВП, 2001й.
13. Масленников А. Практическая криптография BHV – СПб 2003й.
14. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Триумф-2002й.
15. Баричев С. Основы современной криптографии. Учебный курс. Горячая линия Телеком 2002й.
16. Ғаниев С.К., Каримов М.М. Ҳисоблаш системалари ва тармоқларида информация ҳимояси: Олий ўқув юрт.талаб. учун ўқув қўлланма.- Тошкент давлат техника университети, 2003. 77 б.

АХБОРОТЛАРНИ ҲИМОЯЛАШ