

М У Н Д А Р И Ж А

1. Фаннинг аннотацияси 6

2. Муаллифлар хакида маълумот 7

3. Норматив ҳужжатлар 8

3.1. Давлат таълим стандарти 8

3.2. Ўқув режа 43

3.3. Ишчи ўқув режа 45

3.4. Ўқув дастури 47

3.5. Ишчи ўқув дастури 51

3.6. Календар-тематик режа 63

4. Таълим технологияси 64

4.1. Машғулотларнинг педагогик технологияси 64

5. Назорат материаллари 68

5.1. Топшириқлар мазмуни 68

5.2. ОН, ЯН учун тестлар 69

5.3. Ёзма иш ва оғзаки назоратлар саволлари (вариантлар) 77

6. Ўқув материаллари 88

6.1. Маъруза матни 88

6.2. Маъруза машғулотлари дарс ишланмаси 137

7. Амалиёт (семинар ва лаборатория) машғулотларнинг ишланмалари, уларни ўтказиш ва қўллаш бўйича услубий тавсиялар 159

8. Тарқатма материаллар (реферат мавзулари, адабиётлар рўйхати, баҳолаш мезонлари, ҳорижий манбалар) 199

9. Мустақил иш мавзулари ва уни бажариш бўйича услубий тавсиялар 203

10. Курс ишлари мавзулари ва уларни бажариш бўйича тавсиялар 207

11. БМИ мавзулари банки ва уни бажариш бўйича услубий тавсиялар 213

12. Глоссарий 217

13. Илова 223

# 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:

1. Талабаларда компьютер тармоклари ва тизимларида ахборот хавфсизлиги тугрисидаги билимларни шакллантириш;
2. Ахборотни химоя килишнинг назарий, амалий ва услубий асосларини бериш;
3. Талабаларга компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллашни амалий жихатдан ургатиш;
4. 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;

1. компьютер тармоклари ва тизимларидаги ахборот хавфсизлигига тахдид солиши кутилаётган хавф хатарнинг мохиятини ва окибатларини тушуниши;
2. компьютер тармоклари ва тизимларида ахборотни химоя килиш буйича куйиладиган асосий талаблар ва асосларни узлаштириш;
3. компьютер тармоклари ва тизимларида ахборот хавфсизлигини таъминлашда кулланиладиган замонавий усуллар ва воситаларни билиш;
4. 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 эхтимолли- 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 cтр. (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"](http://security.aspu.ru/index.php?section=article&read=14) security.aspu.ru/index.
2. [Криптографические алгоритмы | Безопасность](http://lib.kbsu.ru/elib/disk/compress/2004/4/html/2003_03_algoritm/index.htm)  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:

1. компютер тармоқлари ва тизимларида ахборот хавфсизлиги тугрисидаги билимлар;
2. ахборотни ҳимоя қилишнинг назарий, амалий ва услубий асослари;
3. компютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашнинг замонавий усуллари ва воситаларини куллаш;
4. 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:

1. компютер тармоқлари ва тизимларидаги ахборот хавфсизлигига таҳдид солиши кутилаётган хавф хатарнинг моҳиятини ва оқибатларини тушуниши;
2. компютер тармоқлари ва тизимларида ахборотни ҳимоя қилиш буйича қуйиладиган асосий талаблар ва асосларни ўзлаштириш;
3. компютер тармоқлари ва тизимларида ахборот хавфсизлигини таъминлашда қулланиладиган замонавий усуллар ва воситаларни билиш;
4. тизимларда ахборот бутунлиги ва ишончлигини бузувчи вируслар ва бошқа манбалар мавжудлигини тизимли текширишни таъминлаш ва уларни зарарсизлантириш бўйича чораларни куриш;
5. 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 умумкасбийфанлар 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 ваксинация 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 | 1,2,3 хафталар | 4 |
| 2 | Тармоқ хавфсизлигини назорат қилиш воситалари | Реферат тайёрлаш |
| 3 | Ахборотни ҳимоялаш усулларининг тизимлилиги | Реферат тайёрлаш |
| 5 | Ахборотларни ташкилий ҳимоялаш елементлари | Реферат тайёрлаш | 4 |
| 6 | Ахборот тизимларида маълумотларга нисбатан хавф-хатарлар | Реферат тайёрлаш |
| 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 | 4 |
| 11 | Конфиденциал ахборотларни рухсатсиз киришдан ҳимоялаш | Реферат тайёрлаш |
| 12 | Ахборотларни ҳимоялашнинг криптографик усуллари | Реферат тайёрлаш | 4 |
| 13 | Симметрияли криптотизимлар | Реферат тайёрлаш |
| 14 | Ўринларни алмаштириш усуллари | Реферат тайёрлаш |
| 15 | Электрон почтага рухсатсиз киришдан ҳимояланиш | Реферат тайёрлаш | 7,8,9 хафталар | 4 |
| 16 | Маълумотларга рухсатсиз киришнинг дастурий ва техник воситалари | Реферат тайёрлаш |
| 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 | 6 |
| 21 | Интернетда рухсатсиз кириш усулларининг таснифи. Рухсат этилган манзилларнинг рухсат етилмаган вақтда уланиши | Реферат тайёрлаш |
| 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 | 6 |
| 25 | Банкоматлар хавфсизлигини таъминлаш | Реферат тайёрлаш |
| 26 | Интернетда мавжуд электрон туловлар хавфсизлигини таъминлаш | Реферат тайёрлаш |
| 27 | Дастурларни ваксинасия усули билан вируслардан ҳимоялаш | Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш | 14-17 хафталар | 8 |
| 28 | Мавжуд ехе-файлларни ҳимоялаш | Мавзудаги усул бўйича дастур тузиш. Ҳисобот тайёрлаш |
| 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  , 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 cтр. (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/артиcле19.1996.ҳтмл](http://www.jetinfo.ru/1996/19/1/article19.1996.html)
2. ҳттп[://www. жетинфо.ру /1997/4/1/ артиcле 1.4.1997.ҳтмл](http://www.jetinfo.ru/1997/4/1/article1.4.1997.html)
3. ҳттп[://www. жетинфо.ру/1999/1/1/ артиcле 1.1.1996.ҳтмл](http://www.jetinfo.ru/1999/1/1/article1.1.1996.html)
4. ҳттп://www. жетинфо.ру /2002/5/2/ артиcле 2.5.2002.ҳтмл
5. [ҳттп://www.интуит.ру](http://www.intuit.ru)