bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі:
KZ45VPY00102718
2022

БӨЛІМ: ИНФОРМАТИКА

Ақпараттық қауіпсіздік және ақпаратты қорғау

ЖАРИЯЛАНДЫ
19.05.2022

СІЛТЕМЕ
https://bilimger.kz/121416/

Тақырып: Кіріспе.

Дәріс сұрақтары:

- Ақпараттық жүйелерде ақпаратты қорғау мәселесін талқылау.
- Ақпаратты қорғау тәсілдерін классификациялау.
- Қорғау тәсілдерінің тиімділігін бағалау принциптері мен әдістері.

Электронды есептеуіш техниканың адам қызметінің барлық жұмыс салаларында кең қолданылуы қазіргі заманда ғылыми-техникалық прогресстің маңызды бағыты болып табылады. Сонымен қатар ақпарат өңдеу масштабы кең көлемде ұлғаюда, яғни мүмкіндігінше үлкен көлемді мәліметтердің ақпараттық жүйелер көлеміндегі концентрациясы мен олардың өңделу процессі. Бұндай жүйенің сенімділігі мен функционалдау тұрақтылығы мәселелерімен қатар, ондағы ақпаратты циркуляциялайтын қауіпсізідікті камтамасыз ету мәселесі туындайды. Ақпарат қауіпсіздігі – жүйенің бұл берілген уақыт аралығында, яғни ақпаратты өңдеу кезінде мәліметтердің жоғалуы мен модификациясының минималды ықтималдылығын қамтамасыз ету әдісі.

Күрделі ақпараттық жүйелердің дамуы мен ұйымдастырылуы маманға мынадай талаптар қояды: мәліметтердің үлкен массивтерімен жұмыс істеу технологиясын білу, ыңғайлы қолданбалы интерфейсті құра алуы, ақпараттың қауіпсіздігін қамтамасыз ету. Ақпарат қауіпсіздігінің матақырыбытикалық, программалық және ұйымдастырушылық әдістерінің қажеттілігі және сол әдістердің мемлекеттік және муниципалды мекемелерде, ұйымдарда және басқа да қызмет салаларында өңделуі мен қолданылуын жүзеге асыратын мамандарға сұраныс үнемі артуда.

Ақпарат қауіпсіздігінің ұымдастырылуы мен технологиясы – ол қазіргі ақпараттық технологияларын қолдана отырып ақпарат алмасу, өңдеу және сақтауда оның қауіпсіздігін қамтамасыз ету әдістерінің; программалық-аппарттық, криптографиялық

және ұйымдық-құқықтық әдістердің жиынтығын қамтитын ғылым мен техника саласы.

Ақпараттық қауіпсіздіктің кешенді сипаттамасыбар және ол мыналарды қамтамасыз ету керек:

- ақпараттың жинау, сақтау және байланыс каналдарымен тасымалдану этаптарындағы қауіпсіздігі;
- криптографиялық әдістерді қолдана отырып, байланыс каналдарындағы ақпараттың қауіпсіздігі;
- ақпараттың жинау, сақтау және байланыс каналдарымен тасымалдану этаптарындағы ақпараттың бүтіндігі мен түп-нұсқасы(имитозащита);
- ақпарат алмасатын жақтардың аутентификациясы(электорнды цифрлық жазуды қолданып ақпаратты алущы мен жіберушінің ақпарат түп-нұсқасын куәландыру);
- ақпараттық жүйелер мен деректер базасына жолды бақылау;
- ақпараттың каналдар бойынша жоғалуы мен ондағы қапарат алатын электронды құрылғылардың болу мүмкіндігін көрсететін техникалық әдістердің қорғалуы;
- ақпараттық жүйелердің есептеуіш техникасының программалық өнімдерінің прпограммалық «вирустардан» қорғалуы.

Сабақтың мақсаты: мемлекеттік, өндірістік және коммерциялық объектілердің кешенді қорғалу жүйесін меңгеру, ақпараттық жүйелерге, кәсіптік және коммерциялық қызмет объектілеріне түсетін түрлі қауіптерді меңгеру, объектілер, ақпараттық жүйелер мен ақпараттың қорғалу әдістері мен тәсілдерін меңгеру.

Сабақтың тапсырмасы: студенттердің ақпарат өңдеу қауіпсіздігін қамтамасыз ету мәселелерімен танысу, құрылу принципі мен теорияларын, компьютер жүйелеріндегі ақпараттың қауіпсіздік жүйесінің эффектілік бағасы мен есебінің әдіістерін меңгеру.

Ақпарат қауіпсіздігі мәселесі адамзат жазуды үйренген кезеңнең бастап пайда болды. Бәрі білугісі келетін ақпарат әрқашан да болды. Мұндай ақпараты бар адам оны әртүрлі тәсілдермен қорғауға тырысты. Оған белгілі мысалдар келтірсек: құпияжазу(арнайы сиямен жазылған хат), шифрлеу(«тарабарлық жазу», Цезарь шифрі, басқа да ыңғайлы алмастыру шифрлері, қойылымдар).

Қазіргі жалпы компьютеризация заманында көптеген адамдардың жұмысы, тіпті өмірлері де ақпарат өңдейтін компьютерлік жүйелерінің ақпарт қауіпсіздігін қамтамасыз ету мен әртүрлі объктілерді бақылау мен басқаруға тәуелді. Мұндай объектілерге(оларды критикалық деп атайды) телекоммуникация жүйелерін, банктік жүйелерді, атом станцияларын, әуе және жердегі транспортты басқару жүйелерін, сонымен қатар құпиялы ақпартты өңдеу және сақтау жүйелерін жатқызуға болады. Бұл

жүйелердің бірқалыпты және қауіпсіз функционалдануы үшін олардың қауіпсіздігі мен бүтіндігін сақтау қажет. Қазіргі кезде құпиялы ақпаратқа кірудің мынадай мүмкіндіктері бар:

- бөлмедегі немесе автомашинадағы әңгімелесулерді алдынала орнатылған «радиожучок» пен магнитофондар арқылы тындау;
- телефондық, телекстік және телефакстық байланысты, радиотелефондар мен радиостанцияларды бақылау;
- әртүрлі техникалық құрылғылардан ақпартты дистанциялық алу, бірінші кезекте монитордан, компьютердің баспаға шығару құрылғыларынан және басқа да электронды техникалардан;
- «қызықты әңгімелер» болып жатқан бөлме терезелерінің лазерлік сәулеленуі, мысалы, телевизор, радиоқабылдағыш немесе басқа да техника детальдарының қосылып кетуіне мәжбүр ететін бағытталған радиосәулелену.

Ақпарат әлсіздігінің үш аспектісі белгіленген:

1. физикалық түрде жойылу немесе бүліну;
2. санкцияланбаған(әдейі немесе абайсызда) модификацияның мүмкіндігі;
3. ақпаратты санкцияланбаған түрде алудың қауіптілігі.

ЭЕМ-де ақпарат қорғау мәселесін қарастырып отырып, бірін-бірі толықтыратын үш негізгі бағытты бөліп көрсетуге болады:

1. ЭЕМ-дегі ақпарат өңдеу технологиясының ұйымдық және ұйымдық-техникалық әдістерінің іске асуы;
2. ЭЕМ-дегі өңделетін ақпаратты санкцияланбаған түрде алу жолын блоктау;
3. Ақпаратты санкцияланбаған түрде алу жолын техникалық әдіспен блоктау.

ЭЕМ-де ақпарат қорғау мәселесін шешуде қиындық тудыратын негізгі факторлар болып мыналар табылады:

- кең көлемде қолданылуы;
- функциялау қиындығының әрдайым өсіп отыруы;
- дербес компьютерлердің программалық қамтамаларының әртүрлілігі, қолданушылардың әртүрлі есептеулерінің жеңіл адаптациясы.

Иілгіш магнитті дискілерді қолдану әдейі істерге(ауыстыру, ұрлап кету, жүйеге “компьютерлік вирусты” енгізу, ақпаратты санкцияланбаған түрде көшірмесін алу, ЭЕМ желілерін заңсыз қолдану) жол беретінің айтып өту жөн. Бұл бағыттағы ақпарат қорғаудың негізгі өлшемі – иілгіш магнитті дискілерді қолдануды бақылау және ұйымдастыру.

Кез келген ЭЕМ-нің жұмыс уақыты кезінде ақпаратты санкцияланбаған түрде қабылдап алатын электромагниттік аймақ пайда болады. ДК-де бұл өте қауіпті, себебі ондағы өңделетін ақпарат құрылымдық болып келеді.

Сонымен қатар ЭЕМ-де ақпарат қорғау әдістерінің бірі болып криптографиялық әдіс табылады. Олардың негізгі мақсаты – ақпартты байланыс желілерімен тасымалданған кезінде, магнитті дискілерде сақталған кезінде қорғау және жалған ақпараттың енуіне жол бермеу.

Ақпарат қорғаудың практикалық жүзеге асуы программалық, яғни шифрлеу арнайы программамен жүзеге асады, және техникалық бола алады, яғни шифрлеу алгоритмі техникалық әдістермен жүзеге асады.

Қорғау жүйесі пайдаланушыларға ресурстарды қолдану кезінде ыңғайсыздық тудырмауы керек.

Ақпарат қауіпсіздігі үшін қорғау жүйесі әрдайым мынадай қорғанысты қамтамасыз етуі керек:

- мәліметтерді өңдеу жүйесін бөтен адамдардан;
- мәліметтерді өңдеу жүйесін пайдаланушылардан;
- пайдаланушыларды бір-бірінен;
- әр пайдаланушыны өз-өзінен;
- мәліметтерді өңдеу жүйесін өз-өзінен.

_

Ақпараттық қауіпсіздіктің қазіргі замандағы жағдайы.

Ақырғы кездері ақпаратқа шабуыл, хакерлер және компьютерлік бұзу туралы мәліметтер бұқаралық ақпарат құралдарын толтыра бастады. “Ақпаратқа шабуыл” дегеніміз не? Бұған анықтама беру өте қиын, себебі ақпарат, әсіресе электронды түрдегі ақпарат, жүздеген түрде беріледі. Ақпарат деп жеке файлды, деректер базасын, ондағы бір жазбаны және толық программалық кешенді айтуға болады. Осы барлық объектілер белгілі бір әлеуметтік топтар тарабынан шабуылға кезікті және кезігеді.

Кез келген ақпараттық объектіні сақтау, қолдау және оған жолды көрсету үшін иесі немесе сенімді адамы онымен жұмыс істеу ережелерін құрады. Оны әдейі бұзу ақпаратқа шабуыл болып табылады.

Адамзат қызметінің барлық салаларына компьютерлердің енуімен электронды түрде сақталған ақпарат көлемі мың есе өсті. Сондықтан өндірістің өнімділік жоспарының бар дискетаның көшірмесін жарты минутта алу – көп қағазды көшіріп жазу немесе көшірмесін алудан оңайырақ. Компьютерлік желілердің пайда болуымен ақпарат

қауіпсіздігіне сенім азайды.

Ақпаратқа шабуылдың қандай зардаптары болуы мүмкін? Бірінші кезектегі мәселе, әрине, экономикалық жоғалтулар:

1. коммерциялық ақпаратты бұзу нарықта үлкен шығындарға әкеліп соғуы мүмкін;
2. ақпаратты үлкен көлемде ұрлау фирма репутациясына зардабын тигізеді;
3. бәсекелес фирмалар ұрланған ақпаратты қолданып, басқа фирманы толық шығынға отырғызу үшін жалған келісім шарттар жасауы мүмкін;
4. ақпаратты сақтау немесе тасымалдау кезінде ауыстыру фирманы үлкен шығындарға әкеліп соғуы мүмкін;
5. ақпараттық қызмет көрсететін фирмаға көп шабуыл жасау фирма клиенттерінің сенімділігін азайтады, сол рақылы оның кіріс көлемі азаяды.

Компьютерлік шабуылдар үлкен зардабын әкеледі. Компьютер жүйелерінің кез келген пайдаланушысы оның хаттарын алушы адамнан басқа да 5-10 адамның оқуын немесе ЭЕМ клавиатурасында терілген мәтін буферге көшіріліп, кейін Интернет арқылы белгілі бір серверге жіберілуін қаламайды. Мыңдаған және он мыңдаған жағдайларда тура осылай болады.

2, 3 дәріс.

Тақырып: Ақпаратты енгізу, шығару, беру, өңдеу және сақтаудың ақпараттық процесін жетілдіру кезінде ақпаратты қорғау

Дәріс сұрақтары:

- Қорғау объектілерін классификациялау.
- Иілгіш магнитті дисктерде, «винчестер» тәрізді сыртқы есте сақтау құрылғыларында, дисплейде, баспа құрылғысында, тартылыс арналарында қорғау элементтерін классификациялау.
- Қорғау объектілерін классификациялау.
- Иілгіш магнитті дисктерде, «винчестер» тәрізді сыртқы есте сақтау құрылғыларында, дисплейде, баспа құрылғысында, тартылыс арналарында қорғау элементтерін классификациялау.

Ақпарат қорғаныс объектісі ретінде

Қазіргі кезде «ақпарат» ұғымы философиялық тұрғыдан тұрмыстыққа дейін зерттеледі.

В.И.Шапалов мынадай анықтама береді: «Объект туралы ақпарат дегеніміз – бақылаушы мен объект арасындағы қарым-қатынастан туатын параметрлердің өзгеруі».

Сонымен қатар ақпарат ұғымы жайлы Шеннон да санаулы өлшемдер жасап, айтқан. Олар ақпарат теориясында көрсетілген, онда «ақпарат хаттамалардың ықтимал қасиеттерімен анықталады. Барлық басқа қасиеттері, мысалы бір немесе басқа да әрекеттер үшін пайдалылығы, бір неемсе басқа да авторға иемделінуі ескерілмейді».

Ақпарат ұғымы деп фактілер,оқиғалар, процесстер мен құбылыстар, кейбір пәндік облыстағы объектілер(қасиеттері мен сипаттамалары) туралы мәліметтер деп түсінуге болады.

Немесе, **ақпарат** – бұл тұлғалар, заттар, фактілер, оқиғалар, құбылыстар мен процесстердің олардың формаларына қатыссыз мәліметтер. Ақпарат әртүрлі формадаәр типті сақтау құрылғыларындағы кейбір белгілердің(символдар, сигналдар және т.б.) жиыны ретінде болуы мүмкін.Дамып келе жатқан қоғамның ақпараттандыру процессіне байланысты үлкен көлемді ақпараттар қазіргі есептеуіш техникасы мен байланыс негізінде құрылған автоматтандырылған жүйелерде жинақталады, сақталады және өңделеді. Келешекте автоматтандырылған өндірісте қолданылатын ақпарат формалары ғана қарастырылады.

Қорғанысқа ішкі, конфиденциалды және құпиялы ақпарат жатады.

Ішкі ақпарат – компания туралы әлі баспаға шықпаған ақпарат(ішкі ақпаратты келісімсіз қолдану заңсыз деп саналады).

Конфиденциалды ақпарат – құқықтық режимі коммерциялық және қызметтік құпия, мемлекеттік қызмет жәнебасқа да заңды актілер негізінде құрылған қызметтік, өндірістік, коммерциялық немесе басқа да бір ақпарат.

Коммерциялық құпия деп мемлекеттік құпия болып табылмайтын, өндіріске, технологиялық ақпаратқа, басқаруға қаржыға және мекеменің басқа да бір салаларына байланысты мәліметтер табылады.

Құпиялы ақпаратқа – мемлекеттік құпиясы бар ақпарат жатады. *Мемлекеттік құпия* болып санкцияланбаған таралуы мемлекеттік органдарға, ұйымдарға, субъектілерге және толығымен мемлекетке зардабын тигізетін ақпарат жатады.

Ақпараттың зерттеу объектісі ретінде келесідей сипаттамалары бар:

- масса, өлшем, энергия сияқты параметрлердің физикалық әдістер мен приборлармен өлшенбеуі;

- сақтау құрылғысына жазылған ақпарат сақталып, өңделіп және түрлі байланыс каналдарынан тасымалданады;
- кез келген материалды объектте өзі немесе басқа бір объект туралы ақпарат болады.

Ақпаратсыз өмір жоқ, адам қолымен жасалған жүйелер де функциалдана алмайды, ақпаратсыз өмірдің өзі және адам жаратқандарының барлығы да тек химиялық /физикалық элементтер тобы ғана.

Ақпарат қорғау ұғымын көбінесе сол ақпаратқа түсу жолын бақылау деп түсінеді. Ақпаратты қорғау оның бірқатар қасиеттерімен анықталады. Олардың негізгілері:

1. Ақпарат *тасымалдау құрылғысында* болса ғана оны пайдалануға болады;

Ақпарат тасымалдаушылар:

- тасымалдаушы – ақпарат көзі(сызба – бұл негіз, ал ол салынған қағаз – тасымалдаушы, алайда сурет салынбаған таза қағаз оның физикалық және химиялық қасиеттері туралы ақпарат болып табылады);
- тасымалдаушы – ақпарат тасушы;
- тасымалдаушы – ақпарат алушы.

2. Ақпарат құндылығы оның пайдаланушы(алушы, иесі) үшін пайдалық дәрежесімен бағаланады.

Ақпарат біреулер үшін пайдалы, біреулер үшін зиян болады. Сол үшін қорғау процессінде алдымен оған қатысатын субъектілерді(мемлекеттер, фирмалар, адамтар тобы) анықтайды, себебі олардың арасында қастандық жасаушылар ды болуы мүмкін.

Ақпарат қорғау процессінде ақпарат тасымалдау құрылғысына пайдалықтың шартты белгісі – құпиялық және конфиденциалдық грифін енгізеді. Ақпарат конфиденциалдылығының грифін анықтайтын критерийлер болып бәсекелес немесе қастандық жасаушы субъектінің қолына түскен ақпарат табылады:

- мекемеге тиген экономикалық немесе моральдә зардап көлемі;
- ұйым қызметіндегі апатты жағдайлар(банкрот және т.б.) салдары.

1. Ақпарат алушыға пайдалы не зиянды болып табылуынан оны *тауар* ретінде қараструға болады.

Ақпарат құны, басқа да тауарларға сияқты, түпкілікті құны(өз құны) мен қосымша құннан(пайда) тұрады.Өз құны ақпаратты мынадай жолдармен алуға кеткен шығындармен анықталады:

- лабораториялардағы, аналитикалық орталықтар, топтар және т.б.-дағы зерттеулер;
- ақпарат сатып алу;
- ақпаратты заңсыз жолдармен алу.

Ақпараттан мынадай жолдармен пайда алуға болады:

- нарықта ақпараттың сатылуы;
- жаңа қасиеттері бар немесе пайда әкелетін технологияларға қажет ақпарат;
- маңызды шешімдер(ресурстарды экономдау) қабылдау үшін ақпарат қолдану.

2. Ақпарат құндылығы *уақыт бойынша өлшенеді*.Ақпаратты тарату және қолдану оның бағасы мен құнының өзгеруіне әкеледі. Уақыт бойынша құндылығының өзгеруі ақпарат түріне байланысты.
3. Ақпарат мөлшерін объективті түрде(пайдаланушыға пайдалығының есебінсіз) бағалау мүмкін емес.

Кей жағдайда ақпарат пайдалығын оның сапасымен байланыстырады, «сапа» ұғымының ақпаратқа қатысты өз мағынасы жоқ, себебі ол «көлем» ұғымымен көрінбей қалады.

Ақпарат көлемі оның сапасына байланысты: фотосурет неғұрлым сапалы болса, соғұрлым онда көп түстер болады, соғұрлым онда кедергілер аз болады.

Ақпаратты көшіру кезінде оның көлемі өзгермейді, ал бағасы төмендейді.

Барлық айтылған қасиеттер ұйымның, мемлекеттің, адамдар тобының – кез келген ақпараттық жүйелер субъектілерінің ақпараттық қауіпсіздік саясатын құру процессінің құрамдас бөлігі болып табылады.

Ақпараттық қауіпсіздік тарапынан алғанда ақпараттың келесідей категориялары бар:

- **Құпиялылығы** – белгілі бір ақпараттың белгілі бір адамдарға ғана тиімді екеніне сенімділік; бұл категорияны бұзу – ақпаратты бұзу немесе ұрлау деп атлады;
- **Бүтіндіг**і – ақпараттың сақталуы немесе таралуы кезінде санкцияланбаған өзгерісиердің болмағанына сенімділік; бұл категорияны бұзу – мәліметтің фальсификациясы деп аталады;
- **Аутентичность** – ақпараттың көзі – оның авторы болып табылатынына сенімділік; бұл категорияны бұзу – автордың тарапынан мәліметтердің фальсификациясы деп аталады;
- **Апелляциялануы** — өте күрделі категория, бірақ электронды коммерцияда жиі қолданылады. Қажет уақытында белгілі бір адам сол мәліметтің авторы өзі

екенін дәлелдей алады. Алдыңғы категориялардың ерекшелігі – автордың ауысуы кезінде, басқа біреу өзін сол мәліметтің авторы депайтуы мүмкін; ал апелляцияда – автордың өзі бір кездегі «сөздерінен» бас тартуы мүмкін.

Ақпараттық жүйелер қатынасында басқаша категориялар қолданылады:

- **Сенімділік** – жүйенің жоспарланғандай қалыпты және штаттан тыс режимде болуына сенімділік;
- **Нақтылық** – барлық командалардың толық және нақты орындалуына сенімділік;
- **Ақпаратқа жолды бақылау** — әртүрлі адамдардың объектілерге әртүрлі жету жолдарының болуына сенімділік; бұл жолдардың шектелуі әрқашан орындалып отырады;
- **Бақылануы** – кез келген уақытта программалық кешеннің кез келген компоненттеріне толық тексеріс болу мүмкіндігі;
- **Идентификация бақылауы** – жүйеге қосылған пайдаланушының онда болған қателіктерді мойындауы.

Технология – қайта өңдеу әдістерінің жиынтығы(бастапқы шикізаттың қандай да бір әдістермен соңғы өнімге түрленуі).

Қауіпсіз технологиялар — өздеріне тура немесе жанама қатынасы бар субъектілерге материалдық зардабын тигізетін технологиялар(субъектілер болып мемлекет, жеке тұлғалар, т.б. табылады).

Қорғаныс жүйесінің дұрыс құрылуы үшін мыналарды анықтау керек:

- Ақпаратқа әсер ету түрлері;
- Автоматтандарылған жүйе түсінігі;
- Автоматтандарылған жүйеге түсетін қауіп түрлері;
- Қауіптерге қпрсы тұру шаралары;
- Қорғаныс жүйелерінің құрылу принциптері.

Ақпаратқа әсер ету түрлері:

Ақпаратты блоктау – қолданушы ақпаратты ала алмайды. Ақпаратқа жол болмаса, ол өзі жоғалып кетпейді. Себептері: құрылғылардың, мамандардың, программалық қамсыздандырудың болмауы;

Бүтіндігінің бұзылуы:

- сақтау құрылғыларынан жоғалуы;
- бүлінуі;

- мәндік мазмұнының бұзылуы;
- логикалық байланыстың бұзылуы;
- дұрыстығының бұзылуы(қолда бар ақпараттың негізгі жағдайына сәйкес келмеуі).

Құпиялылығының бұзылуы – ақпаратпен бөтен адамдардың танысуы. Ақпаратты алу жолының деңгейін оның иесі анықтайды. Құпиялылығының бұзылуы қапаратқа жолдың шектелу жүйесінің жұмысы дұрыс емес болу немесе ақпаратты алудың жанама жолының болуы салдарынан болады;

Санкцияланбаған таралым – ақпараттың меншіктелу және авторлық құқық қорғанысы.

Қорғаныс объектілері:

- барлық жұмыс станциялары;
- белгіленген серверлер және орталық компьютер;
- локальді байланыс каналдары;
- ақпарат алу жолының реквизиттері.

4, 5 дәріс.

Тақырып: Ақпаратты қорғаудың теориялық әдістері

Дәріс сұрақтары:

- Ақпаратты қорғау жүйелерінің жалпы анализі мен классификациясы.
- Тақ жиындар теориясының негізгі көрінісі.
- Ықтималдылық-автоматты модельдеудің негізгі көрінісі.
- Формальды емес жүйелер теориясының негізгі көрінісі.

6 дәріс.

Тақырып: Ақпаратты қорғаудың практикалық әдістері

Дәріс сұрақтары:

- Басқару.
- Бөгет.
- Маскировка.
- Регламентация.

- Талап.
- Еріксіз көндіру.

_

7, 8, 9 10 дәріс.

Тақырып: Компьютерлер мен желілерде ақпаратты қорғаудың программалық құралы

Дәріс сұрақтары:

- Вирустардан қорғау. Компьютерлік вирустар классификациясы.
- Вирусты белсендендіру әдістері. Вирустардың деструктивті әрекеті.
- Маскировка тәсілдері. Вирустың болу симптомы. Басқа қауіпті программалар.
- Антивирустық құралдардың классификациясы.
- Төмендеңгейлі редакторлар. Вирустармен күресудің перспективті бағыттары.
- Санкцияланбаған кіруден программалық қамтамасын қорғау.
- Пайдаланушының идентификациясы мен аутентификациясы.
- ДЭЕМ идентификациясы. Орындалатын модуль идентификациясы.
- Программаның жасырын бөлігін пайдалану және санкцияланбаған көшірулерден қорғау кезінде ақпаратты физикалық тасымалдау ерекшеліктері.
- Ашық желілерден ақпаратты қорғау. Интернетке қосылу кезінде ақпараттық қауіпсіздікті қамтамасыз ету: құру сатылары мен басқару.
- Клиент-сервер архитектурасын қорғау. Деректер базасын басқару жүйесін қорғау.
- Зерттеуден программалық қамтамасын қорғауды ұйымдастыру.
- Отладчик жұмысының спецификалық ерекшеліктерін пайдалану.
- Қорғалған программалардың программалау тілдері.

Есептеу техникасында қауіпсіздік ұғымының ауқымы кең болып табылады. Оған компьютердің жұмыс істеу сенімділігі, құнды деректердің сақталуы, қатысы жоқ ақпаратты қорғау, электрондық байланыстағы өзара хабар алысу құпиясын сақтау сияқты көптеген мәселелер кіреді. Әрине барлық өркениетті елдерде азаматтардың қауіпсіздігін қорғауға заңдар бар, бірақ есептеу техникасының қатысты құқықты қолдану практикасы әлі толық дамымаған, ал шығару процесі технология дамуынан

қалып отыр, сондықтан компьютерлік жүйелер жұмысының сенімділігі өзін-өзі қорғау шараларына келіп тіреледі.

Компьютерлік вирустар – бұл жұмыс істейтін компьютерде рұқсат етілмеген іс-әрекеттерді орындауға арналған программа коды. Ол кодта басқа программаға немесе құжатқа деректер тасымалдаушылық белгілі бір аумақтарына ендіріледі.

Компьютерлік вирустардың негізгі түрлеріне мыналар жатады:

- Программалық вирустар
- Жүктелетін вирустар
- Макро вирустар

Программалық вирустар. Программалық вирустар- басқа қолданбалы программаның ішіне мақсатты түрде ендірілетін программалық кодтардың блогы вирусы бар программа жұмыс атқарғанда ондағы вирустық код іске асырылады. Бұл код қатты дискіде және басқа программа файлдық жүйесінде пайдаланушыға көрінбейтін өзгерістер жасайды. Мысалы., вирустар, коды басқа программалар денесінде өзін-өзі қайталайды. Бұл процестің көбейуі деп атайды. Белгілі бір уақыт өткеннен соң көшірмелердің белгілі бір санын құрған соң, программалық вирусты бұлдіру әрекетіне көшеді: — программа мен ОЖ-ның жұмысын бұзады, қатты дискідегі ақпаратты жояды.

Ең нашар бүлдіру вирустары қатты дискіні форматтауға дейін барады. Дискіні форматта — ұзақ процесс, оны пайдаланушы міндетті түрде байқайды, сондықтан көп жағдайда программалық вирус қатты дискідегі деректер сол қалпында қалады, бірақ арнайы құралдар көмегімен ғана пайдалануға болады. Өйткені дискідегі қай файл, қай секторға жататынын анықтау қиындық келтіреді. Теориялық тұрғыдан деректерді қалпына келтіруге болады, бірақ оған кететін еңбек өте хор.

Программалық вирус компьютерге иілгіш дискілерден, немесе интернеттен алынған тексерілмеген программаларды іске қосқанда енеді. *«Іске қосу»* деген сөзге ерекше көңіл аудару қажет. Вирус жұқтырған файлдарды көшіргенде компьютерге вирус жұқпайды.

Сондықтан интернеттен алынған барлық деректер қауіпсіздікке тексеруден өтуі қажет, ал егер қай жерден алынғаны белгісіз болса, оларды қарап шықпай-ақ көзін құрту керек.

Жүктелетін вирустар – программалық вирустардың жүктелетін вирустардан ерекшелігі тарату әдістерінің басқаша болуы. Олар программалық файлдарды емес, магниті тасушы иілгіш және қатты дискілер белгілі бір жүйелік аумақтарды бұзады. Сонымен бірге іске қосылып тұрған компьютерде олар уақытша жедел жадыда орналасады.

Әдетте, жүйелік аумағын да жүктелетін вирус бар компьютер іске қосылғанда оның магниттік тасушыдан жұғу басталады. Мысалы компьютерді иілгіш дискіден іске қосқанда вирус алдымен жедел жадыға, содан соң қатты дискінің жүктеме секторына барады, одан ары қарай компьютердің өзі, вирусты ары қарай тарату көзі болады.

Макровирустар. Вирустың бұл түрі макро команданы орындауға арналған құралдары бар қолданбалы программалардағы құжаттарды бүлдіреді. Мысалы, мұндай құжаттарға Microsoft Word мәтіндік редакторының құжаттары жатады. Шабуыл нәтиже сі арқылы юоуы мүмкін, өте қауіпсіз еместей қалпына келтіруі қиын бүлдіруге дейін апара алады.

Компьюетрлік вирустардан қорғану әдістері. Антивирус қорғау құралдары.

Компьютерлік жүйенің қауіпсіздену қаупі – бұл потенциалды мүмкін болу жағдайы, жүйенің өзінде кездейсоқ болуы мүмкін, сондай-ақ бұр жерде сақталған ақпаратта. Компьютерлік жүйенің бұзылуы –қауіпке әкелетін дұрыс емес сәтсіз мінездеме. Басқа сөзбен айтқанда, компьютерлік жүйенің бұзылуынан жағдайлар орындалады.

Қорыта келгенде, компьютерлік жүйеге шабуыл жасау – сол немесе басқа бұзылу орындалғанда және ізделгенде жаман ойлаушының атқаратын қызметі Сондықтан шабулы дегеніміз қауіп төндіруді орындау .

Шабуылды қарастыру — қауіп элементін кездейсоқ анықта уды болдырмау, яғни тәжірибеден білеміз кездейсоқ немесе алдын ала жасалған қауіптерді білу мүмкін емес, бұған қорғаушы жүйе тез жұмыс істеуі қолайлы.

Зерттеушілер қауіпсіздену қалпының ұш негізгі түрін анықтаған – бұл қауіпті ашу, толықтыру немесе қызмет көрсетуден бас тарту.

Вирустар жұмыс амалдарына байланысты екі типті болады: резидентті және резидентсіз

Егер программа өшсе вирус та жұмысын аяқтайды. Резидентті вирустар бұдан да қауіпті мұндай вирустар бұзылған программа қосылғанда іске асады, бірақ бұл вирус компьютер жадысында өзінің резиденттік бөлігін қалдырады. Компьютер жадысында қалған вирус операциялық жүйенің және басқа программалардың ішіне енеді. Резиденттік вирустар жедел жадыда жүйе тоқтағанша шейін жұмыс атқарады.

Вирус программасы программа жұмыс істеп отырған уақытта қауіпті. Резидентсіз вирус бұзылған программа қосылғанда жұмыс атқарады.

Резидентсіз вирус бұзылған программа қосылғанда жұмыс атқарады. Вирус программасы программа жұмыс істеп отырған уақытта қауіпті.

Компьютерлік вирустан қорғайтын үш аралықты қарап кетуге болады:

- Вирустың келуін тоқтату

- Егер вирус тауып компьютерге енсе, онда вирустық шабуылдарды тоқтату
- Шабуыл егер болса, онда одан кейін болатын қатерлерден сақтау.

Қорғау әдістерін таратудың үш түрі бар:

- Программалық қорғау әдістері
- Аппараттық қорғау әдістері
- Ұйымдастырылған қорғау әдістері.

Вирусқа қарсы қорғау құралдары.

Компьютерлік вирустардан қорғау үшін қолдануға болады:

- Ақпаратты қорғаудың жалпы құралдары
- Вируспен бұзылудың жағдайларын азайтатын қорғау профилактикалық шараларды;
- Вирустан қорғауға арналған арнайы программалар.

Компьютерлік вирустан және вирустан қорғау құраларының түрлері:

- Ақпаратты көшіру –дискінің жүйелік аймақтарын және файл көшірмесін құру;
- Сұранысқа тосқауыл – ақпаратты санкцияланбаған қолданудан тосқауылдау, яғни дұрыс жұмыс істемейтін программалар мен пайдаланушылардың қате қимылдарынан деректер мен программаға өзгерістер енгізуге тосқауыл қою.

Вирустан қорғауға арналған арнайы программалар

1. Детекторлар программалары бірнеше әйгілі вирустарды табу үшін қолданылады.
2. Флаги немесе доктор дискілерді немесе бұзылған программаларды «жазады» (тазалайды), бұзылған программалардан вирус денесін «тістеп алу» арқылы программаларды вируспен бұзылмаған кездегідей қалыпқа келтіреді.
3. Ревизор (тексеруші) программалар –бірінші дискінің жүйелік аймақтары және программа күйі жайлы ақпараттарды есіне сақтап, содан кей ін оны бастапқы күйімен салыстыра отырып тексереді. Олардың салыстыруында келіспеушіліктер болса, онда ол туралы пайдаланушыға хабарлайды.
4. Ревизор докторлар – ревизорлар мен докторлардың қызметін атқарады, яғни программалар тек өзгерулерден автоматты түрде бастапқы күйге келтіруге бар жағдай жасайды.
5. Фильтр программалары резидентті түрде компьютердің жедел жадысында орнатыла ды да көбею және қауіп төндіру үшін вирустар қолданатын операциялық жүйеге түсетін хабарламаларды жолдарынан ұстап алып ол

туралы пайдаланушыларға хабарлайды.

6. Вакцина – программалары, дискілерді немесе программаларды оның жұмыс нәтижесінде көрінбейтіндей етіп модификациялайды, яғни вакцинацияланған программаны вирусталған екен деп түсінеді.

Вирустың классификациясы.

Қазіргі уақытта 5000 астам вирустық программалар бар оларды келесі белгілеріне байланысты бөлуге болады:

- өмір сүру мекені
- өмір сүру мекенін жұқтыру
- қарым қатынас
- алгоритмінің ерекшелігі

Вирус мекеніне байланысты желілік, файлдық, жүктеуші және файлдық-жүктеуші болып бөлінеді. Желілік вирустар әртүрлі компьютерлік желілер арқылы таралады. Файлдық вирустар атқарушы модульдерге басшылық негізде енеді, яғни COM және EXE типті файлдарға. Файлдық вирустар басқа типті файлдарғада енуі мүмкін бірақ бұл жағдайда олар басшылықты ала алмайды, демек көшірме жасау қабілетін жоғалтады. Жүктеуші вирустар систақырыбылық дискінің жүктеушілік программалары бар (Master Boot Record) дискінің жүктеуші секторларына (Boot — сектор) енеді. Файлдық-жүктеуші вирустар файлдық және дискінің жүктеуші секторларында аурумен жұқтырады.

Ауруды жұқтыруына байланысты вирустар екі түрге: резидентті және резидентті емес болып бөлінеді. Резидентті вирустар компьютерді инфицирлеу кезінде жедел жадыда қараушылықты операциялық жүйенің объектілеріне (файлдар, жүктеуші секторлар және т.б) беретін және оларға енетін өзінің резиденттік бөлігін қалдырады. Резиденттік вирустар компьютердің жадысында болады, олар компьютердің өшкенінше белсенді болады. Резиденттік емес вирустар жадыны жұқтырмайды, белгілі бір шектеулі уақыт аралығында ғана белсенді болады.

Қатынасына байланысты вирустарды келесі ттүрлерге бөлуге болады:

қауіпсіз, компьютердің жұмысына бөгет жасамайтын, бірақ компьютердің жадысының және дискінің жадысының көлемінің бос орындарын азайтады, мұндай вирустар дыбыстық немесе графикалық эффектлерде білінеді.

қауіпті, мұндай вирустар компьютердің жұмыстарына әртүрлі бұзулар әкеледі.

өте қауіпті, олардың қатынасы программалардың құруына, деректемелердің құруына, дискінің систақырыбылық бөлігінде информацияның өшіуіне әкеледі.

Алгоритм ерекшеліктеріне байланысты вирустарды классификациялау қиын.

Қарапайымы – паразиттіктер, олар файлдардың немесе дискінің секторлардың мазмұнын өзгертеді, олар тез табылып тез өлтірілуі мүмкін. Вирус-репликатор деген вирусты айта кетсек, ол компьютерлік желілер арқылы жүріп, компьютерлік адрестерді есептейді және онда өзінің көшірмелерін жазады.

Белгілі көрінбейтін вирустар, оларды көпшілік жағдайда стелс-вирустар деп атайды, оларды табып, істен шығару өте қиын. Олар операциялық жүйенің қарауын жұқтырылған файлдарға немесе секторларға қаратады және өзі ретінде дискінің сау жерлерін ұсынады. Ең қиыны вирус-мутанттарды табу, олар кодталған алгоритмнен тұрады, олардың көшірмелерінде бірде бір қайталанып келетін тізбек болмайды. Тағыда квазивирустар немесе «троянские» деп аталатын программалар бар, олар көшірме жасай алмасада өте қауіпті. Олар қажетті программаның ішінде тығыладыда жүйелік секторды бұзады.

Полиморфты вирустар – жұқтырылған программаларда бір вирус өзінің екі экземпляры бірде бір битта кодтары сәйкес келмейтіндей жасалады. Мұндай вирустар әртүрлі кодтау амалдарын пайдаланып өз кодын тек қана кодтамайды, олар кодтаушының генерациялық кодын пайдаланады.

Полиморфты вирустар кодтаушымен өзіндік модифицияланатын вирустар. Мұндай кодтаудың мақсаты: сіз жұқтұрылған және сау файлды ала тұрып оның кодына жай диассембрлеу арқылы оның кодын таба алмайсыз. Бұл код кодталған, сондықтан текке қажеті жоқ командалардың жиынтығын береді. Кодтау жұмыс істеу кезінде вирустың өзімен жүргізіледі. Бұл жағдайдың ек түрі бар: біріншісі, ол өзін толық кодтау мүмкін немесе екінші жағдай бөлініп кодталуы мүмкін және жұмыс кезінде қайтадан кодталуы мүмкін.

Вирусқа қарсы программалар компьютерді тексеру кезінде операциялық жүйенің және BIOS кіру/шығу базалық жүйенің көмегімен облыстық жүйедегі және файылдағы деректерді санайды. Кейбір вирустар жұмысты бастағаннан кейін жедел жадыда арнайы модульдерді қалдырады. Егер осындай модуль табылса программа жұқтырылған файлдарды немесе облыстық жүйені оқимын деген кезде сау файлдармен ауыстырып, вирус жоқ сияқты қылып көрсетеді.

Стелс-вирустар вирусқа қарсы вирустарды алдап көрінбей қалады. Бірақ оларды табудың қарапайым жолы бар, ол үшін жүйелік дискета арқылы компьютерді жүктеп басқа программаларды қоспай тұрып вирусқа қарсы программамен компьютерді тексеру керек. Жүйелік дискета арқылы компьютерді жүктеген кезде стелс-вирус басқаруды өзіне қарата алмайды, сондықтан жедел жадыда резиденттік модульдің орната алмайды, сондықтан вирусқа қарсы программа дискда вирусты оқып, тез таба алады.

Вирустардың кіруі

Компьютер вирусты жұқтырған кезде оны табу керек. Ол үшін оның ең басты көрінетін белгілерін білу керек. Оларға келесі белгілерді жатқызуға болады:

- компьютердің ақырын жұмыс істеуі
- операциялық жүйенің жүктелмеуі
- файлдардың және каталогтардың жоғалуы немесе олардың мазмұнының өзгеруі
- файлдың күнінің немесе уақытының өзгеруі
- файлдардың мөлшерінің өзгеруі
- файлдардың белгісіз бір себептен компьютерде көбейіп кетуі
- жедел жадының бос орынының азайуы
- экранда қаралмаған бейнелердің немесе сөздердің шығуы
- қаралмаған дыбыстардың берілуі
- компьютердің жиі жұмысын тоқтатып қалуы

Жоғарыда айтылған барлық жағдай вирус бар дегенді білдіреді.

Вирустан қорғану тәсілдері

Вирус қандай болмасын, қолданушы одан қорғанудың негізгі тәсілдерін білуі қажет. Вирустан қорғану үшін мынаны қолдануға болады:

- винчестер қорғалып тұрған сияқты файлдардыңда жалпы қорғаушы түрлері
- профилактика
- вирусқа қарсы программаларды орнату

Жалпы қорғаушы түрлері дегеніміз:

1. информацияның және дискінің облыстық жүйелерінің көшірмесін жасау.
2. информацияға шектеулі қолдану қою.

ВИРУСҚА ҚАРСЫ ҚҰРАЛДАР

Вирустардың жіктелуі. Компьютерлік вирустардың әртүрлі типтері бар: жүктелетін, файлдық, макровирустар және желілік.

Жүктелетін вирустар дискеттердің немесе винчестердің жүктеуші секторларын

зақымдайды. Жүктелетін вирустармен зақымдалған жүйені қайта қосқанда басқаруды операциялық жүйенің жүктеуші программалық кодына емес, вирус кодына береді.

Файлдық вирустар өзінің көбеюі үшін операциялық жүйенің файлдық жүйесін пайдаланады. Файлдық вирустар әртүрлі форматтағы (EXE, COM, BAT, SYS және т.б.) орындалушы файлдарды зақымдайды.

Барлық жүктелетін және файлдық вирустар резидентті, яғни компьютердің оперативті жадында орналасады және пайдаланушының жұмыс істеу процесінде қауіпті жағдайлар (дискеттегі мәліметтерді өшіріп тастау, аттарын және басқа да атрибуттарын өзгерту және т.б.) тудырады. Резиденттік вирустардан емдеу қиын, зақымдалған файлдарды дискіден өшіргенмен олар компьютердің оперативті жадында қалып қояды және файлдарды қайта зақымдауы мүмкін.

Макро-вирустар мәліметтерді өңдеуге арналған жүйелерге (мәтіндік редакторлар, электрондық кестелер және т.б.) орнатылған тілдерде жазылған программалар болады. Өзінің көбеюінде мұндай вирустар макро-тілдер мүмкіндіктерін қолданады және олардың көмегімен зақымдалған файлдың (құжаттың немесе кестенің) біреуінен басқаларына көшеді. Макро-вирустар көбінесе Visual Basic for Application тілінің мүмкіндіктерін қолданатын Microsoft Office-те кең таралды.

Пайдаланушы құжатпен жұмыс істеу барысында әртүрлі әрекеттер орындайды: құжатты ашады, сақтайды, баспаға шығарады, жабады және т.б. Мұндай кезде қосымшалар сәйкес келетін стандартты макростарды іздейді және орындайды. Макро-вирустар стандартты макростардан тұрады, олардың орнына шақырылады және әр ашылған және сақталынған құжаттарды зақымдайды. Макро-вирустардың жағымсыз әрекеті түзілген макростар (мәтіндерді орналастыру, меню қосымшасының орындалуына тиым салу және т.б.) көмегімен таралады.

Макро-вирустар шектелген резидентті болып табылады, яғни олар оперативті жадыда болады және құжаттарды қосымша ашық тұрғанда зақымдайды. Сондай-ақ, макро-вирустар құжат шаблондарын зақымдайды және сол себепті зақымдалған қосымша жүктелуінде-ақ іске қосылады.

Желілік вирустар жергілікті және ауқымды желі хаттамаларын пайдалану барысында таралады. Желілік вирустардың негізгі жұмыс принципі — өз кодын алыста орналасқан компьютерге беріп, тасымалдай алуы.

Вирусқа қарсы программалар

Вирустардан қорғау және зақымдалған компьютерлерді емдеу үшін антивирустық программалар қолданылады, оларды әрекеттеріне қарай блоктаушы, ревизорлар және полифагтар деп бөлуге болады.

Вирусқа қарсы блоктаушылар — «вирусты-қауіпті» жағдайларды қармап және ол туралы пайдаланушыға хабар жеткізетін резиденттік программалар. Мысалы, дискінің жүктеу секторына жазылған жазба «вирусті-қауіпті» болып табылады, оларды BIOS Setup пограммасы арқылы тоқтатуға болады.

Ревизорлар. Ревизорлардың жұмыс істеу принципі дискіде сақталған файлдардың бақылау қосындыларын есептеуге негізделген. Бұл қосынды, сонымен бірге бұдан да басқа ақпараттар (файл ұзындығы, олардың соңғы өзгертілген уақыты және т.б.) вирусқа қарсы құралдың мәліметтер қорында сақталады. Келесі жүктеген кезде ревизорлар соңғы санаған мәндермен мәліметтер қорындағы мәндерді салыстырады. Егер мәліметтер қорындағы файл туралы мәлімет қазіргі уақыттағы мәнге сәйкес келмесе, онда ревизор файлдың өзгертілгендігі немесе вируспен зақымдалғаны туралы белгі береді. **Полифагтар.** Полифагтардың жұмыс істеу принципі файлдарды, секторларды және жүйелік жадыны және олардағы белгісіз және жаңа (полифагқа белгісіз) вирустарды тексеруге негізделген. Белгілі вирустарды іздеу үшін вирустардың маскасы (әрбір вирусқа тән, тұрақты програмалар кодының тізбегі) қолданылады.

Сонымен бірге көптеген полифагтарда эвристикалық сканерлеу алгоритмі қолданылады, яғни тексерілетін объекттің командалар тізбегін, кейбір статистикалық мәліметерді талдап, әр объект үшін шешім (зақымдалған ба, жоқ па) қабылдайды.

Полифаг-мониторлар барлық уақытта компьютердің оперативті жадында орналасады да, барлық файлдарды осы уақыт режимінде тексереді. Полифаг-сканерлер жүйені қолданушының командасынан кейін ғана тексереді.

Вирустан қорғау, ұстау және емдеу. Вирусқа қарсы программалар көмегімен өз компьютеріңізде вирустың бар жоқтығын тексеріп, бар болған жағдайда емдеңіз.

Вирустан қорғау, ұстау және емдеу.

1.BIOS Setup программасының көмегімен жүйелік дискінің жүктеу секторына қорғаныс орнатуға болады.

2. ADinf32 ревизорының көмегімен компьютердегі күдікті өзгерістер туралы мәлімет ала аламыз. Бірінші жүктелуінде кестеде оперативті жадының көлемі, басты жүктеу секторының, жүктеу секторының бейнесі, қате беріп тұрған кластерлердің тізімі, каталогтардың бұтақ тәрізді құрылымы, файлдардың ұзындығы мен олардың бақылау қосындысы туралы мәлімет сақталады. Ревизорды іске қосу үшін:
3. ADinf32 ревизорын іске қосыңыз.
4. Терезеде тексерілетін дискіні таңдап, Старт батырмасын шертіңіз.
5. Таңдалған дискілерге кестелер құрылады.

1-сурет. ADinf32 ревизорының терезесі.

Вирус компьютерді зақымдағанда, ол ендірілетін объектілерді (файл немесе жүктеу секторы) өзгертеді. ADinf32 ревизорын жүктеу вируспен зақымдалғандығын куәландыратын өзгерістерді табу мүмкіндігін береді.

Тексеру нәтижелерін көру үшін:

1.Терезеде тексерілетін дискілерді таңдап, Старт батырмасын шертіңіз.

2. Кестеде сақталған мәліметтермен қазіргі уақыттағы мәліметтер салыстырылады.
3. Нәтиже батырмасын шертіңіз және алынған мәліметтерге талдау жасаңыз.

2-сурет. ADinf32 ревизорының Тексеру нәтижелерін көру терезесі.

Adinf ревизор кестесінде өзгерістер анықталған жағдайда және/ немесе компьютерде жұмыс істеу барысында қателерге ұрынса, онда компьютерді вирустан емдеу үшін антивирустық полифагты қолдану керек, мысалы, ntiViral Toolkit Pro.

3-сурет. AntiViral Toolkit Pro терезесі.

1. AntiViral Toolkit Pro полифаг-сканерді іске қосыңыз.
2. Облыс бөлімінен тексеруге қажет дискіні таңдаңыз.

3.Объектілер бөлігінде тексерілетін объектілердің типін (оперативті жады, жүктеу секторы, әртүрлі типтегі файлдар) таңдаңыз.

4-сурет. Объектілер (тексерілетін объектілерді таңдау) терезесі.

4. Әрекеттер бөлігінде вирус табылғандағы әрекеттерді (Тек есеп, Емдеуге сұраныс, Сұраныссыз емдеу, Сұраныссыз жою) таңдаңыз.

5.Пуск батырмасын шерту арқылы тексеруді бастаңыз.

6. Вирус табылған жағдайда емдеуге сұраныс пайда болады.
7. Тексеру аяқталғаннан кейін қосымшаның оң жақ төменгі шетінде табылған вирустар мен емделген файлдар туралы мәлімет пайда болады.

5-сурет. Статистика (табылған вирустар мен емделген файлдар туралы мәліметер) терезесі.

–

11, 12, 13, 14 дәріс.

Тақырып: Ақпаратты қорғаудың криптографиялық тәсілдері

Дәріс сұрақтары:

- Симметриялық криптожүйе. Симметриялық криптожүйелер көрінісі.
- Подстановка жүйесі. Гаммалау.
- Псевдокездейсоқ сандар датчигі.
- Блоктік шифрлеу стандарттарымен таныстыру.
- Ашық кілті бар жүйе. Ашық кілті бар жүйенің теориялық негізі.
- Тасымалданатын және сақталатын деректерді қорғау үшін ашық кілті бар криптожүйелер алгоритмін пайдалану.
- Кілтті бөлу үшін ашық кілті бар криптожүйені пайдалану.

Криптография занимается поиском и исследованием матақырыбытических методов преобразования информации.

Сфера интересов криптоанализа — исследование возможности расшифровывания информации без знания ключей.

Современная криптография включает в себя четыре крупных раздела:

Симметричные криптосистемы

Криптосистемы с открытым ключом

Системы электронной подписи

Системы управления ключами.

Основные направления использования криптографических методов — передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Итак, криптография дает возможность преобразовать информацию таким образом, что ее прочтение (восстановление) возможно только при знании ключа.

В качестве информации, подлежащей шифрованию и дешифрованию, будут рассматриваться тексты, построенные на некотором алфавите. Под этими терминами понимается следующее:

Алфавит — конечное множество используемых для кодирования информации знаков.

Текст — упорядоченный набор из элементов алфавита.

В качестве примеров алфавитов, используемых в современных ИС можно привести следующие:

* алфавит Z33 — 32 буквы русского алфавита и пробел;

* алфавит Z256 — символы, входящие в стандартные коды ASCII и КОИ-8;

* бинарный алфавит — Z2 = {0,1};

* восьмеричный алфавит или шестнадцатеричный алфавит;

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование — обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая систақырыбы представляет собой семейство T преобразований открытого текста. хлены этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей K — это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд букв алфавита.

Криптосистемы разделяются на симметричные и с открытым ключом.

В ***симметричных криптосистақырыбых*** и для шифрования, и для дешифрования используется один и тот же ключ.

В систақырыбых с ***открытым ключом*** используются два ключа — открытый и закрытый, которые матақырыбытически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины ***распределение ключей и управление ключами*** относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых:

* количество всех возможных ключей;

* среднее время, необходимое для криптоанализа.

Преобразование Tk определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Требования к криптосистақырыбым

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

* зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

* число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста,

должно быть не меньше общего числа возможных ключей;

* число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

* знание алгоритма шифрования не должно влиять на надежность защиты;

* незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

* структурные элементы алгоритма шифрования должны быть неизменными;

* дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

* длина шифрованного текста должна быть равной длине исходного текста;

* не должно быть простых и легко устанавливаемых зависимостью между ключами, последовательно используемыми в процессе шифрования;

* любой ключ из множества возможных должен обеспечивать надежную защиту информации;

* алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

15 дәріс.

Тақырып: Компьютерлер мен желілерде ақпаратты қорғаудың техникалық құралдары және ұйымдастыру

Дәріс сұрақтары:

- Ақпараттық жүйелерде қауіпсіздік деңгейін бағалау әдістері.
- Бақылау және ақпаратты қорғау бойынша ұйымдастыру шаралары.
- Ақпаратты қорғау бойынша құқықтық шаралар.
- Ақпаратты қорғаудың техникалық құралдары.

8.2. Тәжірибелік сабақ

1-2 зертханалық жұмыс. Құпия нөмірдің көмегімен ақпаратты қорғау.

Жұмыстың мақсаты құпия нөмірдің көмегімен қорғауды, сонымен қатар құпия нөмірге шабуыл жасауға қарсы әдістерді зерттеу.

Құпия нөмірге шабуыл.

Бүгінгі таңда құпия нөмір жиі қолданыста болғандықтан, рұқсат алу субъектілерінің негізінде түпнұсқаны орнату құралы көп қолданылады.

Кез-келген шектік жүйеде маман-оператордың жіберген қатесі қымбатқа соғады және ондай жағдай көп кездеседі. Криптожүйе жағдайында, тәжірибесі жоқ пайдаланушылардың іс-әрекеті ең мықты криптоалгоритмге және оның нақты жүзеге асырылып орындалуына әкеп соқтырады.

Біріншіден бұл құпия нөмірді пайдаланумен байланысты. Әрине, қысқа немесе мағынасыз құпия нөмірлер тез жатталады, бірақ оларды тез ашып алуғада болады. Криптожүйе көзқарасымен ұзын және мағынасыз құпия нөмірлерді пайдалану өте жақсы, бірақ әдетте пайдаланушы оны есінде сақтай алмағандықтан оны бір бетке жазып қояды, ал ол бет жоғалуы немесе басқа біреудің қолына түсуі мүмкін. Тәжірибелі пайдаланушылар қысқа немесе мағыналы құпия нөмірлерді пайдаланғандықтан, оларды ашып алудың екі әдісі бар: толық терумен және сөздікпен шабуыл жасау.

Құпия нөмірді таңдауда оның қорғалуы оны тексеру жылдамдығына және мүмкін болатын құпия нөмірдің ұзындығына тәуелді, ал ол құпия нөмірдің ұзындығына және қолданылатын алфавит символдарының өлшеміне тәуелді. Онымен қоса оның қорғалуына құпия нөмірді қорғау программасының жүзеге асуы ықпал етеді..

Есептеу қуатының аз уақыт аралығында тез өсуіне байланысты толық терумен шабуыл жасау бұрынғыға қарағанда сәтті болу ықтималдығы өте жоғары. Сонымен қатар кең таралған есептеулер белсенді пайдаланылады, яғни параллель жұмыс істейтін машиналардың көбіне есептеулердің біртекті таралуы. Бұл құпия нөмірді бұзуда уақытты қысқартуға мүмкіндік береді.

Толық теру үшін есептеу қуаты жетіспеген уақытта қайтып оралайық. Бұған қарамастан хакерлер жаңа әдіс ойлап шығарды, олар құпия нөмір ретінде маман сөздікте бар сөзді немесе өзі туралы ақпаратты және жақындары туралы ақпаратты пайдаланатынын білді (есім,туған күн және т.с.с). Ал, кез-келген тілде 100000 кем емес сөз болғандықтан оларды теру көп уақытты алмайды, сондықтан 40-тан 80%-ке дейін құпия сөздер қарапайым схемамен шешілуі мүмкін, ол «сөздікке шабуыл» деп аталады. Осындай әдіспен құпия нөмірдің 80%-ы 1000 сөзді ғана пайдаланып шешілуі мүмкін.

Қазіргі таңда пайдаланушылар ондай сөздерді таңдауға болмайтынын түсінсе де,

мұндай 34jXs5U@bTa!6;) түрдегі құпия нөмірлерді компьютерлік қауіпсіздікті қамтамасыз ететін мамандар да пайдаланбайды. Сондықтан тәжірибелі пайдаланушы мынандай құпия нөмірлерді таңдайды: hope1, user1997, pAsSwOrD, toor, roottoor, раго1, gfhjkm, asxz. Көріп отырғандай бұлардың барлығы мағыналы сөздерге негізделген, кейбір қарапайым ережеге сай оған сан, жыл қосуға болады, сонымен қатар сөзді керісінше жазуға, орыс тіліндегі сөзді латын әріптерімен жазуға немесе қатар тұрған пернелерден құпия нөмірді жазуға болады.

Егер мұндай құпия сөздің өзі шешіліп жатса, оған таң қалмаңыз, себебі хакерлер пайдаланушыдан да айласын асырып түсіреді, олар осы уақытта өз программаларын сөздің өзгеруіне сай қайта өңдеп алған. Ең жаңа программаларда (John The Ripper, Password Cracking library) бұл ережелер қайта программаланып және хакердің өзі ғана білетін арнайы тілде жүзеге асуы мүмкін.

Бұндай терудің эффектілігіне мысал келтірейік. Қауіпсіздікке байланысты көп кітаптарда сенімді құпия нөмір ретінде бір белгімен ажыратылған екі мағыналы сөз таңдау керек делінген (мысалы, good!password). Мұндай құпия нөмірлер қанша уақытта шешілетінін есептейік, егер мұндай ережелер хакердің программасына еңгізілген болса,(сөздік 10000 сөзден тұрады делік,ажыратқыш белгі ретінде 10 сан және 32 тыныс белгілері,сонымен қатар арнайы символдар алынсын, машина класы Pentium,жылдамдығы 15000 құпия нөмір/сек): 10000*(32+10)*10000/15000*2=140000 секунд немесе 1.5 күн!

Құпия нөмірдің өлшемі неғұрлым ұзын болса, оны шешуге ұзақ уақыт өтетіндіктен жүйе оның қауіпсіздігін ұзақ уақыт қамтамасыз етеді.Мұндай жағдайды құпия нөмірді шешудегі күтілетін уақыт немесе күтілетін қауіпсіз уақыт деген терминмен беруге болады. Күтілетін қауіпсіз уақыт($T_б$) — мүмкін болатын құпия сөздердің санының жартысы және уақыты, бұл әрбір сұрау болған сайын құпия нөмірді теру үшін. Мұны формула түрінде келтірейік: мұнда t— құпия нөмірді еңгізуге арналған уақыт, ол E/R-ға тең; E —рұқсат алу кезіндегі берілген хабарламадағы символдар саны (құпия нөмір мен қызметтік символдармен қоса); R — байланыс линиясында хабарлама беру жылдамдығы (символдар/мин); S — құпия нөмірдің ұзындығы; A — құпия нөмір құрылатын алфавиттегі символдар саны. Егер әрбір сәтсіз теру кезінде он секундтық кідіріс болса, онда қауіпсіз уақыт лезде ұлғаяды.

- Сондықтан аутентификацияны пайдалану кезінде жүйемен қорғалатын құпия нөмірдің негізінде келесі ережелер сақталу керек:

а) Құпия нөмір 6–8 символдан кем болмау керек;

б) Құпия нөмірлер контроллерлермен тексеріліп отыру керек;

в) Құпия нөмірді еңгізгенде оның символдары көрсетілмеуі керек;

г) Құпия нөмірді дұрыс еңгізгеннен кейін, соңғы рет жүйеге кірген туралы ақпарат шығады;

д) құпия нөмірді еңгізу мүмкіндігі шектеулі болады;

ж) Байланыс каналымен хабарлама берілгенде құпия нөмірлер шифирлену керек;

з) Құпия нөмірлер жадыда шифирленген түрде пайдаланушыға рұқсат етілмеген файлдарда сақталу керек;

и) пайдаланушының өзі құпия нөмірді өзгертуіне мүмкіндігі болуы керек;

к) администратор пайдаланушылардың құпия нөмірін білмеуі тиіс, бірақ оларды өзгерте алады;

л) құпия нөмірлер периодты түрде өзгеріп отыруы тиіс;

м) Құпия нөмірдің жұмыс істеу мерзімі орнатылады;

Құпия нөмірді таңдау мәселесі

Құпия нөмірдің ұзындығы көп жағдайда техникалық құрылғылардың дамуымен, олардың элементтік базасымен және жылдамдығымен анықталады. Қазіргі кезде көп символды құпия нөмірлер қолданылады, онда S>10. Осыған байланысты сұрақтар туады: қалай және қайда оны сақтау керек, оны пайдаланушының аутентификациясымен қалай байланыстыруға болады? Бұл сұрақтарға құпия нөмірдің аралас жүйесі жауап береді, ал ол екі бөлімнен тұрады. Бірінші бөлігі 3–4 ондық белгілерден тұрады, егер код сандық болса 3–4 белгіден артық емес, ал егер әріппен болса, онда оны есте сақтау оңай болады. Екінші бөлігі техникалық мүмкіндіктерді жүзеге асыру және қорғауға деген талапты анықтайтын белгілерден тұрады, ол физикалық тасмалдаушыда орналасады да құпия нөмір кілтін анықтайды, ал оның ұзындығы жоғарыдағы әдістеме бойынша есептелінеді. Бұл жағдайда құпия нөмірдің жарты бөлігін білуге бұзушыға рұқсат берілмейді.

Бірақ құпия нөмірдің ұзындығын есептей отырып, оның ұзындығын ұзартқан кезде оның периодтты түрде ауысып отыру уақытын ұзарту мүмкін емес екендігін естен шығармау керек. Құпия нөмірдің кодын міндетті түрде ауыстырып отыру керек, себебі оларды ұрлап алу, көшірмесін алу, күшпен алу ықтималдығы болуы мүмкін. Периодтылықты таңдау кезінде жүйе жұмысының нақты шарттарымен таныс болу керек, бірақ жылына 1-2 реттен кем емес. Ауыстырған уақыт және периодтылығы кездейсоқ болуы керек.

Құпия нөмірдің әлсіздігін тексеру үшін арнайы контроллерлер қолданылады. Мысалы, Кляйннің танымал контроллері , құпия нөмірді бұзу барысында пайдаланушының атын, инициалын және олардың комбинациясын пайдаланады, әртүрлі сөздіктердегі сөздерді қолдану арқылы, сөздердің орының ауыстыру арқылы тексереді, сонымен қатар шетел-

пайдаланушы тілінде тексереді. Құпия нөмірді Кляйн контроллерімен тексеру есептеуіш желілерінде жақсы нәтижелер көрсетті — пайдаланушылардың көп бөлігі қарапайым құпия нөмірлерді пайдаланатыны анықталды. Тексеру нәтижесінде мысалы, Кляйн контроллері 5 символдан тұратын 100 құпия нөмірді, 6 символдан тұратын 350 құпия нөмірді, 7 символдан тұратын 250 құпия нөмірді, 8 символдан тұратын 230 құпия нөмірді анықтады.

Құпия нөмірдің әлсіздігін және оларға деген шабуылды төмендету үшін келтірілген мысал төмендегі ережелерді қалыптастырды:

– алфавиттегі әріптердің көп мөлшерін, латын және орыс алфавитінің әріптерін, сандарын және белгілерін пайдаланыңыз;

– мағыналы сөздерді пайдаланбаңыз;

– символдар тобын қайта-қайта қайталамаңыз;

– 6–8 символдан кем емес құпия нөмірді пайдаланыңыз, себебі оны есте сақтау оңай болады, ал құпия нөмірді жазбай міндетті түрде есте сақтау керек. 15 немесе одан да көп символдан тұратын құпия нөмірлер керегі жоқ, себебі оларды есте сақтау мүмкін емес болады;

– Бір құпия нөмірді барлық жүйеге қолданбаңыз, себебі біреуін бұзса, барлық жүйеге зиян әкеледі;

– құпия нөмірді пайдаланар алдында оны арнайы контроллермен тексеріп алыңыз;

Құпия нөмірді құру үшін арнайы нұсқаулар беруге болады, бірақ оны абайлап пайдалану қажет:

– әннің немесе поэманың бірнеше жолын таңдаңыз (бірақ жиі қайталап жүретін әуен болмасын) және әрбір сөздің бірінші (немесе екінші) әрібін пайдаланыңыз — осымен қоса құпия нөмір ұзын болуы керек (15 символдан кем емес), әйтпесе әріптер регистрын ауыстыруға тура келеді;

– 7-8 әріптен тұратын сөздегі бір дауыстыны дауыссызға немесе санмен, белгілермен алмастырыңыз. Әдетте, мұндай құпия нөмірлер оңай есте сақталынады. Енді, қортындылайық:

«Нашар» құпия нөмір дегеніміз не:

- Пайдаланушының өз аты;
- Сөздікте бар сөз;
- Жүйемен белгіленген идентификатор;
- Туған күн;

- Қайталанған символ (мысалы: AAA);
- 6 символдан кем құпия нөмір;
- Бөтен адаммен қойылған құпия нөмір;
- Пернетақтада қатар орналасқан символдардан тұратын құпия нөмір (мысалы: QWERTY немесе ЙЦУКЕ);
- Жеке куәлік мәліметтері: жеке нөмір, жүргізуші куәлігінің нөмірі және т.б.

«Жақсы» құпия нөмір дегеніміз не:

- Мағынасыз сөз;
- Кездейсоқ терілген әріптер қатары;

Құпия нөмірлерді ашу программасының жұмыс істеу реті.

Берілген лабораториялық жұмыста құпия нөмірмен жабылған архивті ашатын программалық өнім: Advanced ZIP Password Recovery

AZPR негізіндегі шабуыл жасау программаларымен жұмыс

AZPR программасы ұмытылып қалған құпия нөмірлерді қайтадан құру үшін арналған. Қазіргі кезде құпия нөмірді ашудың екі әдісі бар: теру арқылы (brute force) және сөздікпен шабуыл (dictionary-based attack).

Басқару панелі:

- Ашу және Сақтау батырмалары проектпен жұмыс істеуге мүмкіндік береді. Сонымен қатар ашу процесін тоқтата тұруға мүмкіндік береді.
- Старт және Стоп батырмалары құпия нөмірді теруді бастап және аяқтауға мүмкіндік береді.
- Набор батырмасы құпия нөмірдің қандай символдан тұратынын білетін болса өзінің көптеген символдарын қоюға рұқсат береді.
- Справка батырмасы программа туралы мәліметті береді.
- О AZPR программасы программа туралы ақпаратты шығарады.
- Выход батырмасы программадан шығуға мүмкіндік береді.

.

Программаның мүмкіндіктерін қарастырайық:

Шабуыл жасау типі және ашу үшін архив таңдалады.

Жұмыс параметрлері таңдалады:

- Набор закладкасы

Программа теру облысын таңдауға мүмкіндік береді (символдар тобы). Бұл теру уақытын біршама қысқартады.Набор батырмасымен берілген пайдаланушының наборын пайдалануға болады. Бастапқы құпия нөмірді беру арқылы терілетін құпия нөмір санын шектеуге болады. Ал егер құпия нөмірдің жартысы белгілі болса маскамен шабуыл өте тиімді. Сәйкес шабуыл типін таңдаса болғаны маска өрісі шығады. Онда белгілі құпия нөмірдің жартысын мынадай түрде еңгізуге болады P?s?W?r? , белгісіз символдардың орынына сұрақ белгісін қою керек. Кез-келген басқа символды да пайдалануға болады, тек оны маска өрісіне еңгіземіз.

- Ұзындық закладкасы

Құпия нөмір ұзындығын таңдауға мүмкіндік береді.

- Сөздік закладкасы

Файл-сөздікті таңдауға мүмкіндік береді.

- Автосохранение закладкасы

Жұмыс нәтижесін сақтау үшін файл атын және автосохранения закладкасын таңдауға мүмкіндік береді.

- Опции закладкасы

Жұмыс приоритеті таңдалады (фондық және жоғары), ағымдағы құпия нөмірді теру туралы ақпараттың жаңару интервалы.Интервалдың жоғарлығы жылдамдығын тездетеді, бірақ ақпараттығын төмендетеді.

Теру арқылы шабуыл (brute force attack)

1. Құпия нөмірді ашатын программаны пайдалана отырып кодталған файлға шабуыл жасау try_me.rar (try_me.arj, try_me.zip – нұсқаның қандай болуына байланысты). Теру облысы – барлық басылатын символдар, құпия нөмір ұзындығы 1-ден 4-ке дейін символ. Pentium класындағы компьютерде орындалу уақыты шамамен 3-4 минут. Pentium II класындағы компьютерде – 50 секунд. Анықталған құпия нөмірдің дұрыстығын тексеру файлды ашып, оның мазмұнымен танысу арқылы жүреді.
2. 1 пункті орындағаннан кейін теру облысын ұзарту арқылы қайтадан ашу және уақыт айырмашылығын тексеру (мысалы, егер құпия нөмір 6D1A – болса, онда оның орынына ағылшын әріптерін немесе сандарын таңдау арқылы).

Сөздікпен шабуыл жасау (dictionary attack)

1. Бір файлды қысып құпия нөмір ретінде 5 символдан тұратын ағылшын сөзін таңдаңыз (мысалы, love, god, table, admin және т.б.). Сөздікпен шабуыл жасау.

Ол үшін шабуыл түрін және Сөздік закладкасында English.dic файлын таңдаңыз. Ол құпия нөмір ретінде жиі пайдаланылатын ағылшын сөздерінен, символдарынан тұрады.

2. Құпия нөмірді тікелей теру арқылы ашып көріңіз. Кеткен уақытыңызбен салыстырыңыз.

3-4 зертханалық жұмыс. Ауыстыру әдісі.

1. Қарапайым ауыстыру шифры.
2. Күрделі ауыстыру шифры.
3. Көпалфавитті ауыстыру шифры.

5 зертханалық жұмыс. Алмастыру әдісі.

6 зертханалық жұмыс. Шифрлеудің биттік әдісі.

7 зертханалық жұмыс. Биттік манипуляция әдісі. Кодтау кітабы.

8 зертханалық жұмыс. Аналитикалық түрлендіру әдістері.

9 зертханалық жұмыс. Гаммалау.

10 зертханалық жұмыс. Комбинирленген әдістер. Ашық кілтпен шифрлеу.

11-12 зертханалық жұмыс. Электронды цифрлік қол.

13 зертханалық жұмыс. Криптожүйелер тұрақтылының анализі.

14 зертханалық жұмыс. Кодтау әдістері.

15 зертханалық жұмыс. Архивация әдістері.

8.3. СӨЖ және СОӨЖ.

8.3.1. СӨЖ сұрақтары

1. Санкцияланбаған кіруден қорғау әдістері.
2. Тасымалдауыштардағы ақпаратты қорғау.
3. Шифрлеу әдістері.
4. Псевдокездейсоқ сандар датчигінің негізгі сипаттамасы.
5. Операциялық орта құрамында криптографиялық функциялардың қазіргі өндірілуі.

6. Таралған операциялық жүйелерде қорғау подсистақырыбыларын ұйымдастыру.
7. Пайдаланушы идентификациясы мен аутентификациясы жүйесі.
8. Антивирустық қорғау әдістері мен тәсілдері.
9. Компьютерлік вирус жұмысының алгоритмі.

8.3.2. СОӨЖ тапсырмалары

СОӨЖ № 1.

Тақырыбы: Дискретті сигналды кодтау

1. Түзу кодтар.
2. Сигнал жиілігін ескеретін кодтар.
3. Грей коды.

СОӨЖ №2.

Тақырыбы: Дискретті сигналды криптографиялық кодтау

1. Қарапайым алмастыру әдісі.
2. Вижинер әдісі.

СОӨЖ №3.

Тақырыбы: Дискретті сигналды тиімді кодтау

1. Шеннон-Фано әдісі.
2. Хаффмен әдісі.

СОӨЖ №4.

Тақырыбы: Дискретті сигналды бөгеттен қорғай алатындай кодтау

1. Қатені табу үшін код құру.
2. Қатені түзету үшін код құру.

_

СОӨЖ №5.

Тақырыбы: Дискретті сигналды өлшеу. Кодтау тиімділігін талдау.

СОӨЖ №6.

Тақырыбы: Сандарты көрсету формасы. Кері кодтарда қосу.

8.4. Емтихан сұрақтары

1. Қорғау объектілерін жіктеу.
2. Иілгіш дискілеріндегі қорғау элементтерін жіктеу.
3. Компьютерлік вирустарды жіктеу, өмір сүру ортасына жұгу тәсілдері.
4. «Винчестер» типті сыртқы есте сақтау құрылғысындағы және дисплейдегі қорғау элементтерді жіктеу.
5. Ақпаратты қорғау жүйесін моделдеу әдістерін жіктеу және талдау.
6. Вирустарды белсенді ету тәсілдері.
7. Ақпаратты қорғаудың тәжірбиелік әдістері.
8. Желілердегі ақпаратты қорғаудың программалық құралдары.
9. Вирустардың бұзушылық әрекеттері.
10. Компьютерлердегі ақпаратты қорғаудың программалық құралдары.
11. Вирустардың болу белгілері.
12. ДЭЕМ идентификациялау.
13. Вирусқа қарсы антивирустық құралдарды жіктеу.
14. Рұқсатсыз көшіруден қорғау кезінде программалардың жасырын бөліктерінің ерекшеліктерін қолдану.
15. Ақпараттық қауіпсіздіктің қазіргі замандағы жағдайы.
16. Құпиялы ақпаратты.
17. Ақпараттардың физикалық тасымалдағыштарының ерекшеліктерін қолдану.
18. Шифрлау әдістері.
19. Программалық қамтаманы зерттеуден қорғауды ұйымдастыру.
20. Ақпарат қорғау.
21. Internet-ке қосу кезеңінде ақпарат қауіпсіздігін қамтамасыз ету, оның құру және басқару кезеңдері.

22. Ақпаратты қорғаудың криптографикалық құралдары.
23. Құпия нөмірдің көмегімен ақпаратты қорғау.
24. Ақпараттық қауіпсіздіктің кешенді сипаттамалары.
25. Ашық кілті жүйелері.
26. Операциялық жүйелердегі ақпаратты қорғау
27. Қауіпсіз технологиялар.
28. Ақпараттық жүйелерде қауіпсіздік деңгейін бағалаудың әдістері.
29. Компьтерлік вирустардың жіктелуі.
30. Алынатын тасушыларда ақпаратты қорғау.

ҚМ АА Куәлік нөмірі: **KZ45VPY00102718** — ҚР Мәдениет және Ақпарат министрлігі