М.Ж.Көшкінбаева

АҚПАРАТТЫҚ ҚАУІПСІЗДІК НЕГІЗДЕРІ

оқу құралы

ШЫМКЕНТ
2015

УДК 519.683(075.8)
ББК 32.973я73

М.Ж.Көшкінбаева
Ақпараттық қауіпсіздік негіздері: оқу құралы 5В070400-«Есептеу техникасы мен бағдарламалық қамтамасыз ету» мамандығының студенттеріне арналған. – Мирас университеті, Шымкент, 2015 ж. – 104 б.

Пікір жазғандар:
Е.Т.Теңізбаев – т.ғ.к., доцент, «Экономика және ақпараттық технологиялар» кафедрасының меңгерушісі, М.Сапарбаев атындағы ОҚГИ.
А.О.Оспанова –т.ғ.д., «Есептеу техникасы және бағдарламалық қамтамасыз ету» кафедрасының профессоры, М.Әуезов атындағы ОҚМУ.

ISBN 9965-737-73-8

Бұл оқу құралы “Ақпараттық қауіпсіздік негіздері” пәнін оқытуға практикалық көмекші. Оқу құралында «Ақпараттық қауіпсіздік негіздері» пәні бойынша теориялық материалдар, лабораториялық жұмыстар, студенттің өзіндік жұмысына арналған тапсырмалар, тест сұрақтары берілген. Оқу құралы 5В070400 - «Есептеу техникасы мен бағдарламалық қамтамасыз ету» мамандығы студенттеріне арналған.

Мирас университетінің Оқу-әдістемелік Кеңесімен қаралып, баспаға тапсырылған.
Хаттама № _____

КІРІСПЕ

Қазіргі заманғы қоғамдағы өмірде берілгендерді өңдеуде автоматтындырылған жүйені күнделікті қолдану барысында берілгендерді енгізу, сақтау және шығару қажет болады. Жалпылама компьютерлендіру, пайдасымен бірге көптеген мәселелерді алдына қояды, соның ішінде ең қиыны ақпараттың қауіпсіздігі болып табылады. Адамдардың автоматтындыруда ең жоғарғы деңгейге ұмтылуы, көп қолданылатын арзан компьютерлік жүйелерге деген сұранысы берілгендердің қауіпсіздігін қамтамасыз ету тәуелділігіне әкеліп соғады. Дербес компьютерлердің пайда болуы тек қана қолданушылардың ғана мүмкіндігін кеңейтіп қана қоймай сонымен қатар жүйе бұзушыларғада кең жол ашып отыр. Компьютерлік жүйенің қауіпсіздігі әлден ғылыми зерттеуде өзіндік бағытқа ие болды. Бірақта осыған қарамастан шешілмеген мәселелер саны азаймай отыр. Мұның себебін ең алдымен ғылыми техникалық прогресстің өте үлкен жылдамдықпен даму барысымен түсіндіруге болады. Жаңадан пайда болған компьютерлік технологиялар шешілген мәселенің шешілмеген жаңа қырын ашады.

Бүкіл дүние жүзі бойынша компьютерлік қылмыс тек құқық қорғау орындарының ғана емес, сонымен қатар мемлекеттік, коммерциялық және қоғамдық ұйымдардың да назарын аударуда. Бұл мәселе бизнес саласына өте үлкен қауіп төндіруімен қатар, тағы бір жағынан оның компьютерлендіру және ақпараттандандыру деңгейінің көрсеткіші. Сол сияқты компьютерлік технологияларды жетілдіру және жаңа бағыт – есептеуіш техникаларда өңделетін ақпаратты қорғау бағытын дамытуға қозғаушы күш болып отыр.

Ұсынылып отырған оқу құралында компьютерлік жүйелердегі ақпараттарды қорғау туралы теориялық материалдар, лабораториялық жұмыстар жүйесі, өзіндік жұмыстар нұсқалары, тест сұрақтары берілген. Лабораториялық жұмыстарда толығымен орындалу реті көрсетіліп, студенттерге арналған нұсқаулар берілген. «Ақпараттық қауіпсіздік негіздері» пәні бойынша студенттің өзіндік жұмысына арналған тапсырмалар және де теориялық материал түгелімен қамтылған тест сұрақтары берілген.

1 АҚПАРАТТАРДЫ ҚОРҒАУ

1.1 Ақпаратты қорғау және оның мәселелері

Өндірісте ЭЕМ базасының тиімді ақпараттық құрылымын құру мәселесі ақпаратты қорғауды ұйымдастыру мәселесінің бірі болып саналады. Бұл мәселе деректерді тұлғалық қорғау және жеке қорғау, жүйелік бағдарламаны арнайы бағдарламалармен қорғау сияқты сұрақтар жиынын құрайды. Сонымен деректерді қорғаудың бірінші түсінігі деректерді толық қорғау және оларға байланысты басқару сұрақтарын қамту. Толық деректерді сақтау мәселесі ұйымдастыру және техникалық аспектерден тұрады. Ұйымдастыру аспектісі келесі ережелерді құрайды:

- ақпарат басқалардың байланысы жоқ жерде сақталуы тиіс;
- өте керек ақпарат бірнеше жинақтауыштарда сақталуы тиіс;
- әр-түрлі есептерге жататын деректер бөлек атпен сақталуы тиіс;
- магнитті жинақтауштармен ережелерге сай байланыс жасалуы керек.

Техникалық аспект әр-түрлі шектеулердің түрімен байланысты. Бұл аспект деректер базасын басқару жүйесінің құрылымына сай келуі және қолданушыға қолайлы болуы тиіс. Оларға:

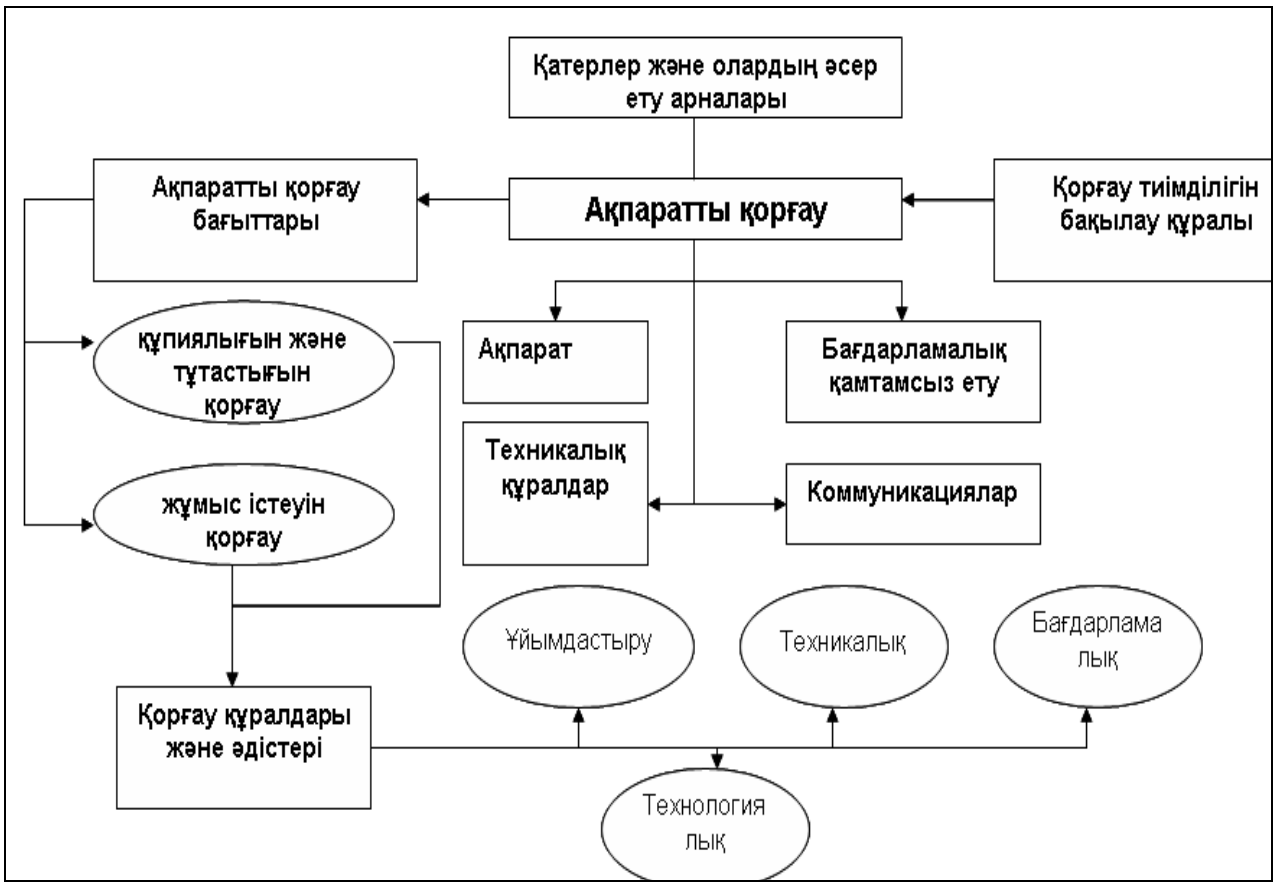
- ескі және жаңа мәндер арасындағы байланысты сақтау мақсатында белгілі атрибуттарды жаңалау шектеулі;
- әлдебір диапазонда кеңістік көрсеткішінің мәнін сақтау шектеулі.

Электрондық есептеуіш техниканың дамуы және кең қолданылуы - өндірісте, басқаруда, байланыста, ғылыми зерттеулерде, білім саласында, коммерциялық, қаржылық, және өзге де адам қызметі сфераларында ғылыми-техникалық прогрестің қазіргі кездегі маңызды бағыты болды. Баспасөзде, техникалық әдебиеттерде, күнделікті өмірде - ақпаратқа, оның таралу қауіпсіздігі мен қорғалуына көп көңіл бөлінетін болды.

«Ақпараттық қауіпсіздік негіздері» пәнінің мақсаты компьютерлік жүйелердегі және желілердегі тәжірибелік қолданудағы ақпаратты қорғау және теориялық негізін құруды үйрену болып табылады. Сонымен қатар, ақпаратты қорғаудағы құру құрылғылары және жүйелендірілген мақсатты білімгерлерге оқыту, ақпараттық жүйедегі ақпаратты қорғаудың тәжірибелік талаптарын қанағаттандыру болып табылады. Ақпаратты қорғаудың құрамдас бөліктері 1 сұлбада ашық келтірілген.

Пәннің мәселелері: компьютерлік жүйенің санкцияланбаған рұқсат етулерін қорғауды және ақпараттық ресурстарды басқару әдістерін білімгерлерге үйрету. Пәннің негізгі аумағында білімгер криптожүйенің симметриялық және асимметриялық құрылуларын, қазіргі таңдағы симметриялық және асимметриялық шифрлық жүйесін және олардың бағдарламалық құрылуындағы ерекшеліктерімен танысады.

Қазақстан Республикасының ұлттық ақпараттық инфрақұрылымын қорғау жүйесінің қызметіне жалпы талап. Ақпараттық қауіпсіздік саясаты стратегияны ақпараттайды және құрамдас бөлігінің ақпаратық қауіпсіздігін басқаруға қатынасын сипаттайды.

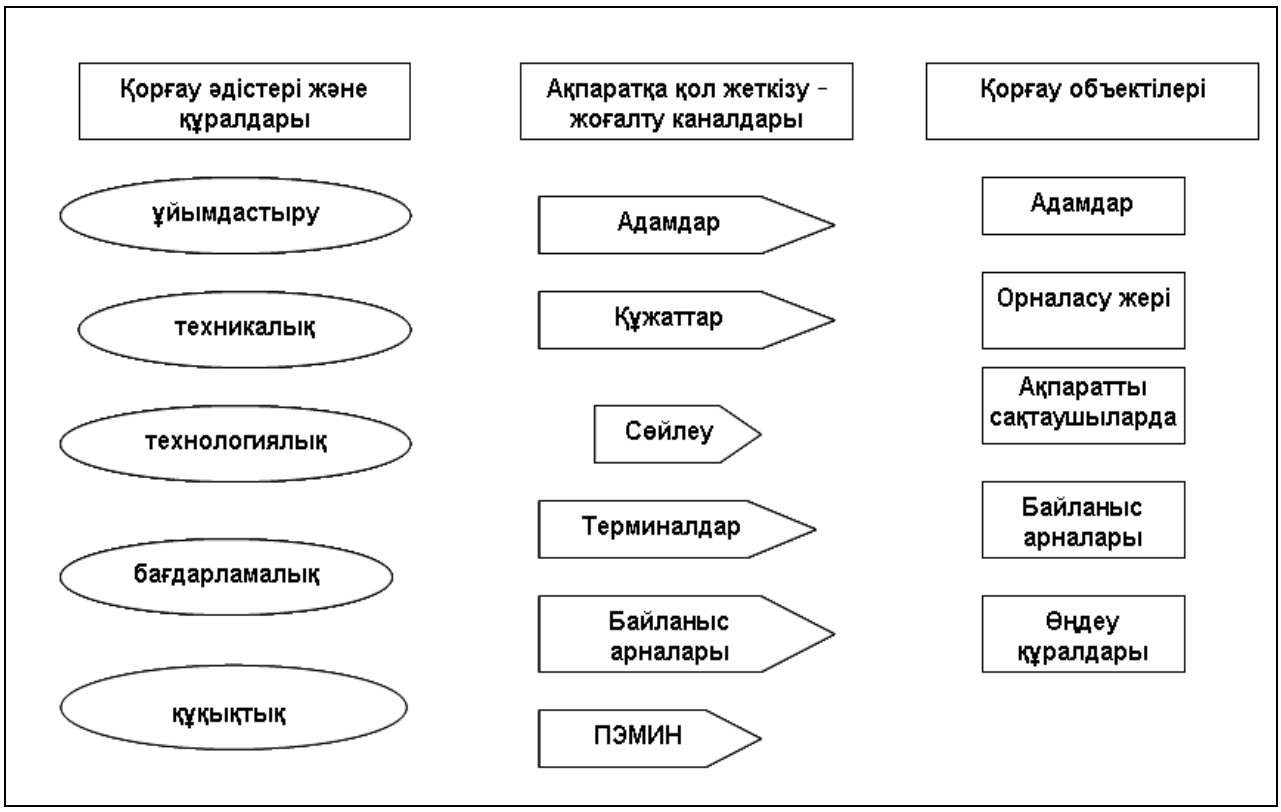


Сурет 1 Ақпаратты қорғаудың құрамдас бөліктері

Ақпараттық қауіпсіздік саясаты ұстану тиіс:

- ақпараттық қауіпсіздікті, оның негізгі мақсаттарын, ақпаратты бірлесіп пайдаланудың кепілдік механизмі ретінде қауіпсіздіктің маңыздылығын анықтайды;
- шешілген міндеттерге сәйкес ақпараттық қауіпсіздіктің мақсаттары мен ұстанымдарын қолдау жөніндегі шаралар;
- мақсаттарға және басқару құралдарына, оның ішінде тәуекелдерді бағалау, сондай-ақ тәуекелдерді басқару құрылымдарына жетістікке жету жөніндегі іс-шаралар;
- нормативтік, құқықтық, шарттық актілердің талаптарына сәйкес ұстанымдарды, стандарттарды түсіндіру;
- ақпараттық қауіпсіздікті басқару, оның ішінде ақпараттық қауіпсіздіктің қақтығысы туралы хабарлау жөніндегі жалпы және арнаулы міндеттерді анықтау;
- қауіпсіздік саясатын қолдай алатын құжаттамаларға сілтеме.

Ақпаратты қорғау жүйесіндегі пәннің орыны төменгі 2-сұлбада көрсетілген.



Сурет 2 Пәннің ақпаратты қорғау жүйесіндегі орыны

1.2 Ақпараттық қауіптер. Ақпараттық қауіптерге қарсы әрекет.

Ақпарат қауіпсіздігі - бұл ақпаратты өңдеуші жүйенің берілген уақыт аралығында мәліметтерді жоғалтпай, қойылған талапқа сай қажетті орынға жетуді толығымен қамтамасыз етуі.

Ақпарат шығыны (утечка информации) қандай да бір құпияны: мемлекеттік, әскери, қызметтік, коммерциялық және т.б. ашу болып табылады. Тек құпия ақпарат ғана қорғауға жатпайды. Сонымен қатар, құпия емес мәліметтерді де қорғау қажет, өйткені, құпия емес мәліметтерді жоғалтудың өзі құпия мәліметтер шығынына ұшыратуы мүмкін. Мәліметтерді өңдеу жүйелерінің жұмыс жасау сферасы мен аумағына қарай ақпаратты жоғалту немесе шығындау әр түрлі ауырлықтағы нәтижелерге алып келеді: күнәсіз әзілден бастап өте үлкен экономикалық немесе саяси шығынға дейін. Баспасөздер мен техникалық әдебиеттерде дәл осы мәселелерге көптеген мысалдар келтіріледі. Әсіресе мұндай үлкен қылмыстар банктік және сауда құрылымдарына қызмет етуші автоматтандырылған жүйелерде кең етек алып отыр. Шетелдік мәліметтер бойынша компьютерлік қылмыстар нәтижесінде банктердің көретін шығыны жыл сайын 170 млн.-нан 41 млрд. долларды құрайды екен. Сонымен, қазіргі кезде көптеген адамдардың игілігі мен бақ-берекесі және өмірі, ақпаратты өңдеуші компьютерлік жүйелердің қауіпсіздігін қамтамасыз етуден және әртүрлі объектілерді бақылап, басқарудан тәуелді болуда. Мұндай обьектілерге телекоммуникация жүйелер, банк жүйелері, атом станциялары,

ауа және жер асты транспортын бақылау жүйелері, сол сияқты құпия және өте құпия ақпаратты өңдеу мен сақтау жүйелері жатады. Бұл жүйелердің жақсы және қауіпсіз жұмыс жасауы үшін, олардың қауіпсіздігі мен тұтастығын қамтамасыз ету қажет.

Ақпараттық қауіпсіздіктің негізгі түсініктері

Ақпаратқа қол жеткізу мүмкіншілігі. Қол жеткізуді басқару саясаты қол жеткізудің басқару ережесі және әрбір пайдаланушының немесе пайдаланушылар тобының құқықтары нақты анықталуы тиіс. Қол жеткізуді логикалық және физикалық басқару құралы бірге қаралуы тиіс.

КЖ қауіпсіздік деңгейі – жүйенің шынайы қорғалған деңгейі және пайдалану барысында қауіп төнетін жағдайларды болжау компонентері

Қауіпсіздік шарасы – жағдайдың немесе процестің мүмкін болу іс-әрекеті, КЖ басқа компоненттеріне не ақпаратқа субъект қызығушылығының тікелей не жанама әсері болуы мүмкін

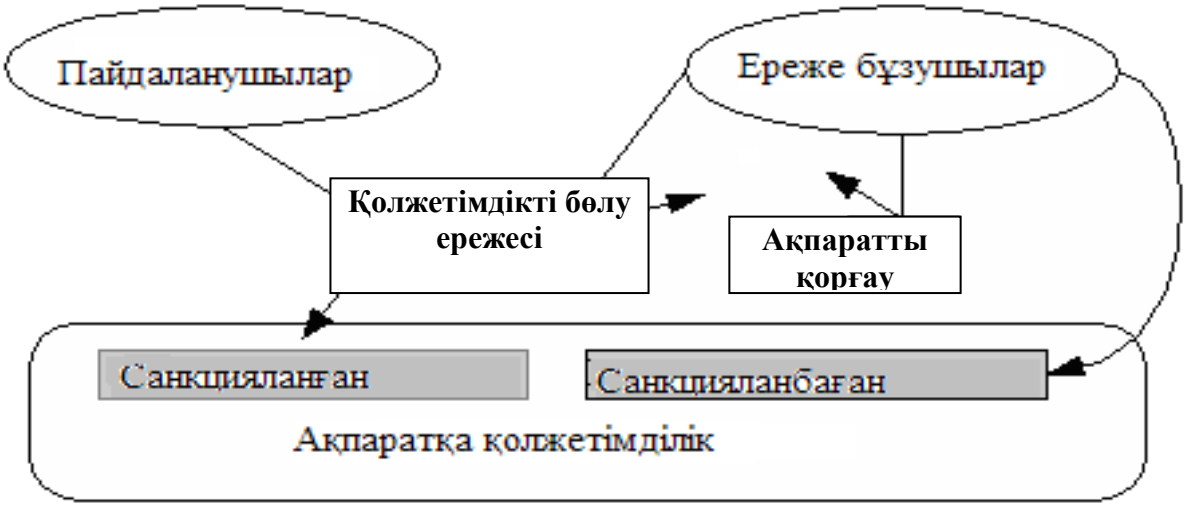
Ақпаратқа қолжетімділік – ақпаратпен танысу, ақпарат модификациясын көшіру, өңдеу және ақпаратты жою (сурет 3).

Қолжетімділікті шектеу ережесі – ережелер жиынтығы, субъектінің объектіге қолжетімділік құқығының регламентті

Ақпаратқа санкциялық қолжетімділік – бұл ақпаратқа қол жетімділік, қолжетімділікті шектеу ережесін бұзбау

Ақпаратқа санкциялық емес қолжетімділік – ақпаратқа қолжетімділік, қолжетімділікті шектеу ережесін ЕТ штатты құралдарын пайдалануда бұзбау

Ақпаратқа санкциялық емес қолжетімділіктен қорғау – ақпараттағы болатын қиындықтарды алдын-ала қарастыру



Сурет 3 Ақпаратқа қол жетімдікпен байланысты түсініктер

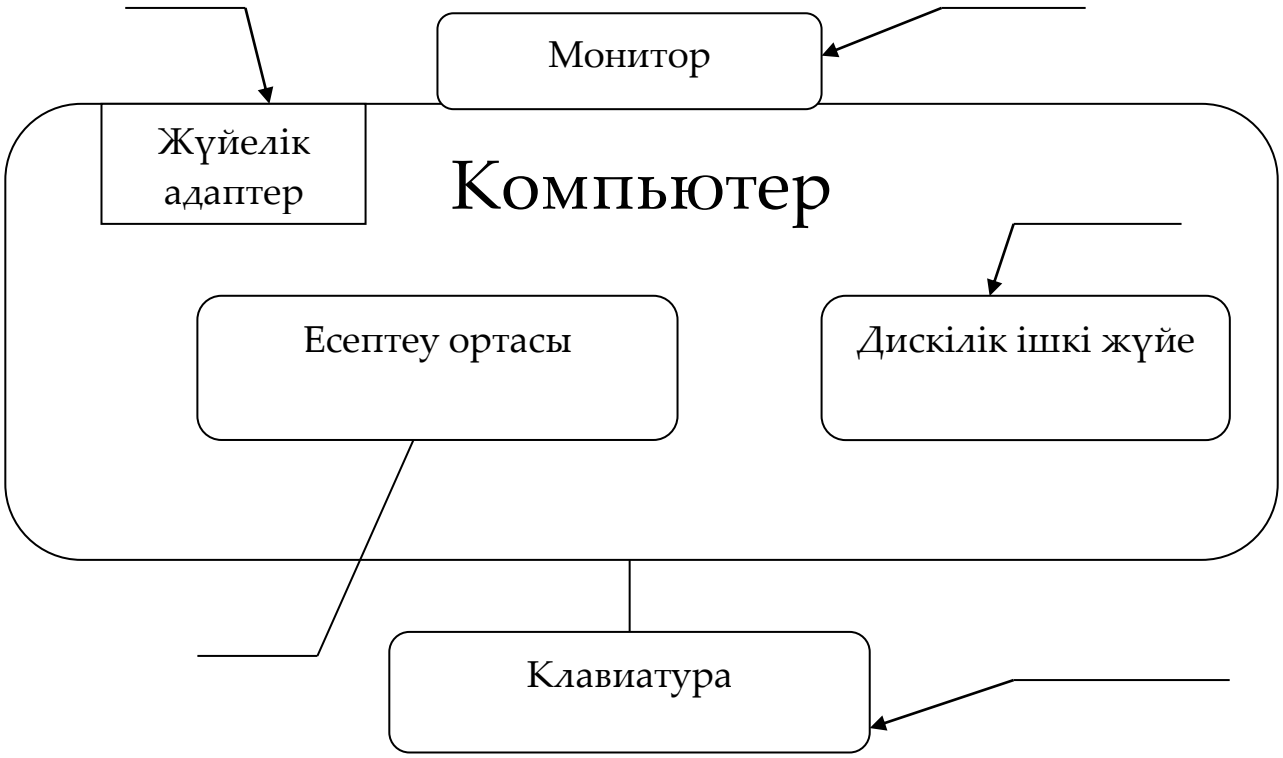
Қауіп төну каналы – КЖ қауіп физикалық ортадан келуі, ол санкциялық емес іс-әрекеттерден пайда болу қаупі. *Қауіп төну* тәсілі *(алгоритм)* – белгілі бір әдістерді пайдалана отырып КЖ құралдар каналдары арқылы субъектінің мақсатқа жетуінің алдын алу шаралары.

Есептеуіш жүйелерінің қауіпсіздігіне есептеуіш құралдары арқылы жасалатын қауіп түрлерін қарастырайық (сурет 4).

1. Есептеуіш жүйелер жұмысына адамның араласуы. Бұл топқа есептеуіш жүйелер қауіпсіздігін бұзушы ұйымдастырушылық құралдар (ақпарат тасымалданушы, ақпарат сақталушы дискеттер, өзге де құрылғыларды ұрлау, жарамсыздандыру) және есептеуіш жүйелердің программалық өнімдеріне рұқсатсыз ену жатады. Мұндай қауіпті іс-шараларға қарсы қолданылатын тәсілдер ұйымдастыру-шылық түрде (күзет қою, есептеуіш жүйелерге ену режимін белгілеу) болады.

2. Есептеуіш жүйелердің жұмысына аппаратты-техникалық араласу. Бұл сөз мағынасы есептеуіш жүйелердегі ақпараттың қауіпсіздігі мен тұтастығын техникалық құралдар көмегімен бұзу, мысалы: есептеуіш жүйелер құрылғыларынан электромагниттік сәулелену арқылы ақпарат қабылдау, ақпарат жіберуші каналдарға электромагниттік әсер ету, т.б. Мұндай қауіптерден сақтану үшін ұйымдастырушылық шаралардан басқа, аппараттық (аппарат экранын сәулеленуден сақтау, ақпарат жіберуші каналдарды жасырын тыңдалудан сақтау) және бағдарламалық тәсілдер қолданылады.

3. Бағдарламалық өнімдер көмегімен есептеуіш жүйелер бағдарламаларының компоненттеріне жоюшы әсер көрсету. Мұндай өнімдерді - бұзушы бағдарламалық өнімдер деп атауға да болады. Оларға компьютерлік вирустар, троян аттары, жергілікті және ауқымдық желілерді пайдалану арқылы алыстағы жүйелерге ену өнімдері. Мұндай шабуылдарға қарсы бағдарламалық және аппараттық қорғау жүйелері қолданылады.



Сурет 4 Есептеуіш жүйелер қауіпсіздігіне төнетін қатер түрлері

Ақпаратты қорғаудың әдістеріне төмендегілер жатады:

- енуді шектеу;
- енуді анықтау;
- енуді бөлу;
- ақпаратты криптографиялық түрлендіру;
- енуді бақылау және есепке алу;
- заңдық шамалар.

Ақпаратты өңдеу автоматтандырылғаннан кейін, оны өңдеудің техникалық құралдары күрделіленді. Физикалық тасымалдаушы құралдардың жаңа түрлері пайда болды. Ақпарат көлемінің көбейуі, жинақталуы, пайдаланушылар санының арта түсуі және өзге де себептерден ақпаратқа әдейі ену ықтималдығы да арта түсуде. Осыған байланысты есептеуіш жүйелердегі ақпараттарды қорғаудың жаңа түрлері пайда болды:

- функционалдық бақылау әдістері;
- авариялық жағдайлардан ақпаратты қорғау;
- аппаратураның ішкі құрылысына, байланыс желісіне және басқару органдарына технологиялық енуді бақылау әдістері;
- ақпаратқа енуді бақылау және анықтау әдістері;
- пайдаланушыларды, техникалық құралдарды ақпарат тасымалдаушы және құжаттарды идентификациялау және аутентификациялау әдістері.

Ақпаратты қорғаудың негізгі мағынасы ақпараттық объектіге ену тек бір ғана «күзетілуші өткел» арқылы жүзеге асырылу. Мұндағы «күзетшінің» қызметіне пайдаланушының пароль кодын тану және оң нәтиже болған жағдайда оны ақпаратпен жұмыс жасауға рұқсат беру. Бұл процедуралар пайдаланушы жүйеге жұмыс жасау үшін енген сайын қайталанып отырады. Сондықтан, әрбір жолы пароль теріп отырмау үшін, берілетін парольді арнайы физикалық тасымалдау-шыда (кілт, карта) сақтаған дұрыс.

Қазіргі кезде пароль кодтарын сақтаушы тасымалдаушылардың бірнеше түрлері бар. Мұндай тасымалдаушылар жататындар:

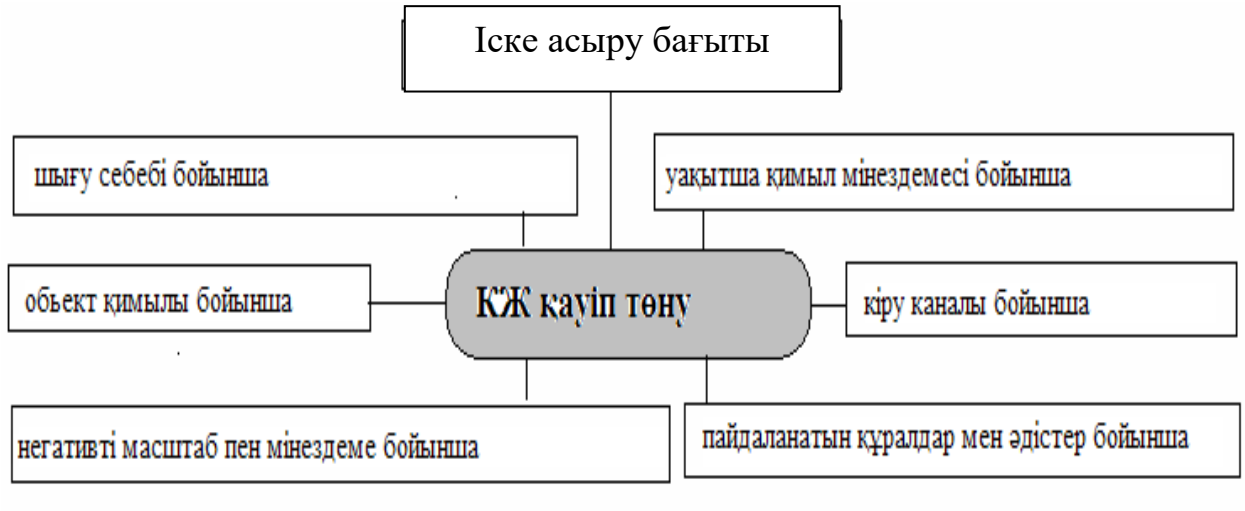
- пропусклер (access contzol);
- телефон карталары (phonecazd);
- визит карталары (business cazd);
- жеке куәлік (pass contzol);
- сатып-алушы карталары (shopping cazd);
- банк карталары (bank cazd);
- банкоматтар үшін карталар (ATM - Cazd).

Банк карталары дебеттік және кредиттік карталар болып бөлінеді. Дебет карталары чектерді және ақшаны алмастырады. Олар сатып алынған заттармен есеп-айырысу үшін, банк бөлімінде ақша алу үшін пайдаланылады.

Кредит карталары қажетті сумманы алдын-ала қандай да бір уақыт аралығына алу үшін пайдаланылады.

Смарт-карталар 70-жылдарда жасалып шығарылған, бірақ тек 1985 жылдан бастап Францияда қолданыла бастады. Мұндай карталар жалған жасап алу және көшірмесін түсіру мүмкін емес. Смарт-карталар операциялық жүйеден және қауіпсіздік жүйесінен тұрады.

КЖ қауіп төну келесі жағдайлар бойынша бөлінуі мүмкін (сурет 5).

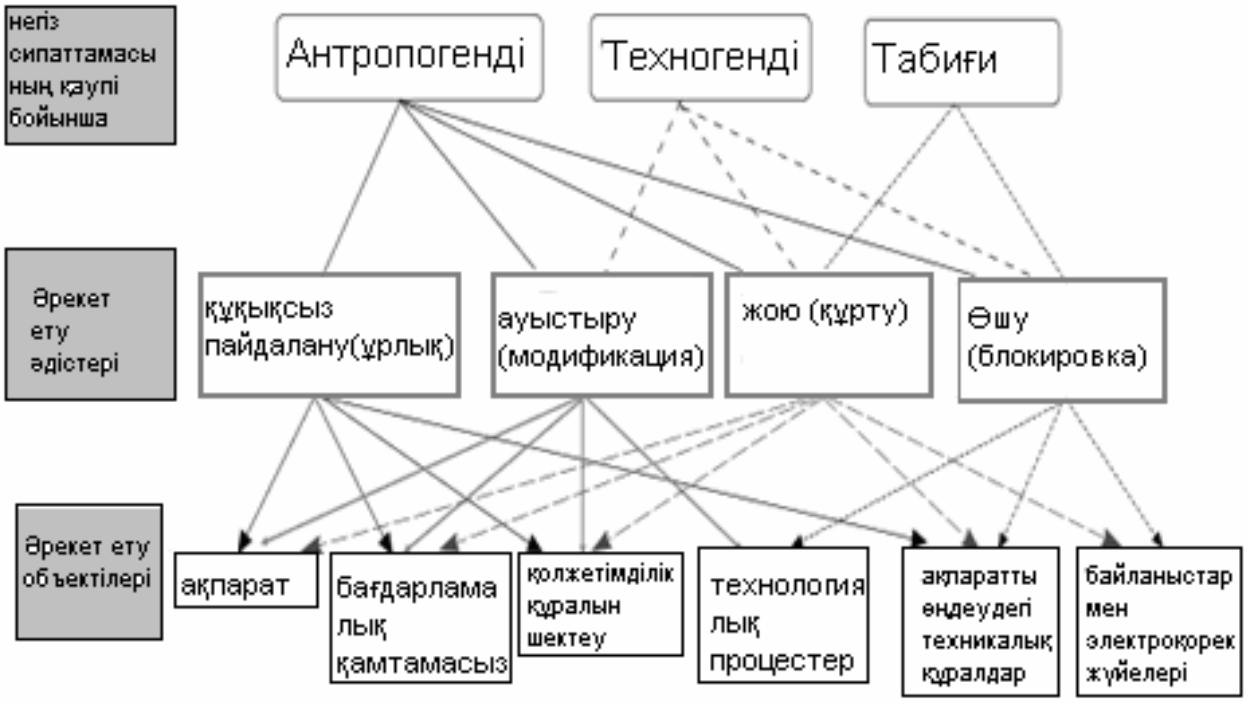


Сурет 5 Ақпараттық қауіптер классификациясы

АЖ қауіптері қайнарлары ішкі және сыртқы болады. Физикалық табиғат позицияларынан және "ақылдылықтың" дәрежесі бойынша болады (сурет 6):

- адамның әрекеттерімен байланысты қауіптер (жасанды қауіптер);
- техникалық құралдар процестері қауіптері (техногендік қауіптер);
- табиғи құбылыстармен (апаттармен) байланысты қауіптер.

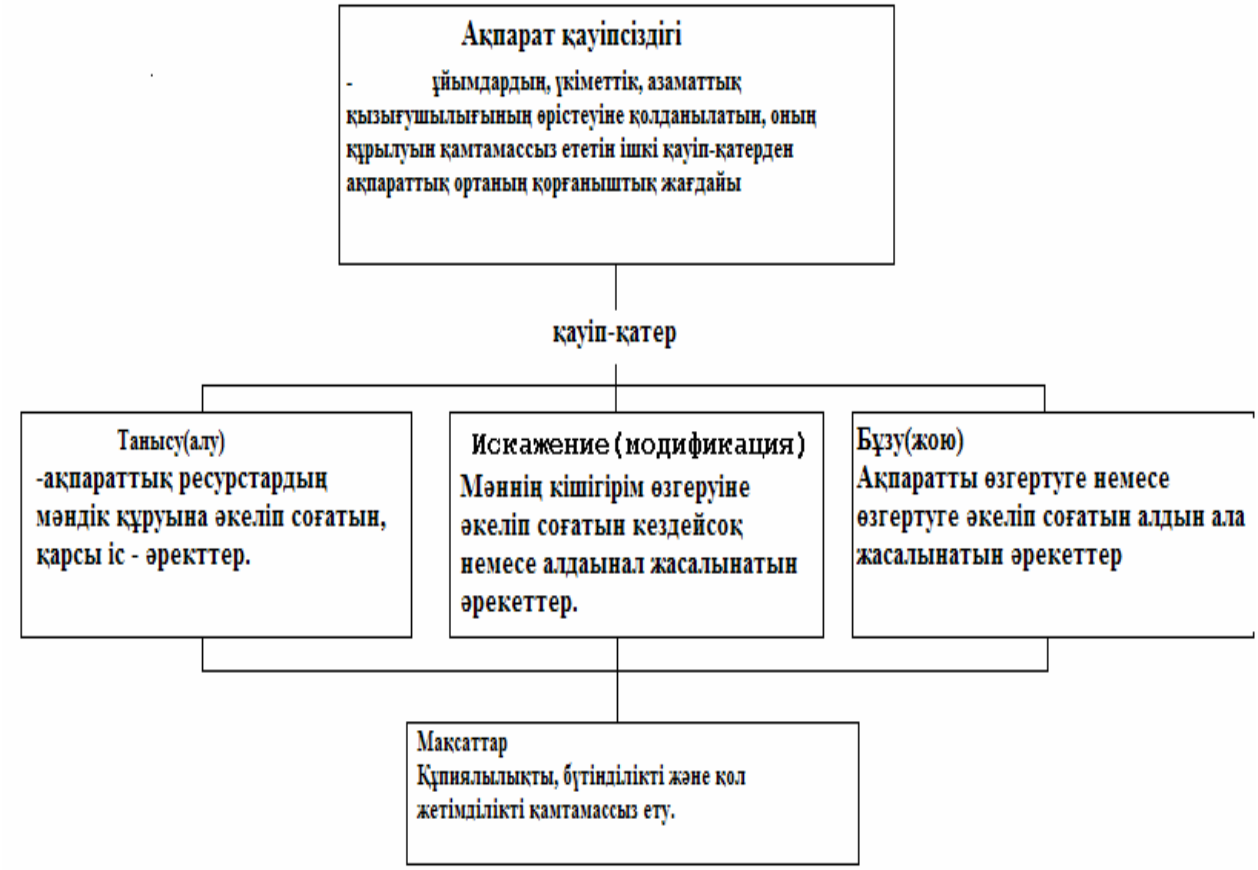
Сыртқы және ішкі субъектілер сияқты ақпаратты қорғау бірінші топты ұйымдастыру ең үлкен назарда ұстанылады.



Сурет 6 Қауіптердің пайда болу себептері бойынша классификациялау

1.3 Ақпаратты қорғау жүйелерінің сипаттамалық қасиеттері

Ақпараттық қауіпсіздік қатерлері және мақсаттары сурет 7-де, ал олардан ақпаратты қорғауды қамтамасыз ету іс-шаралары сурет 8-де көрсетілген.



Сурет 7 Ақпараттық қауіпсіздік қатерлері

Сурет 8 Ақпаратты қорғауды қамтамасыз ету іс шаралары

Объект қимылының қаупі байынша классификациялау төменгі сурет 9-да бейнеленген.

Сурет 9 Объект қимылының қаупі бойынша классификациялау

Жоғарғы тәуекелдер жағдайында мәжбүрленудің іс-қимылы туралы хабарлауды пайдалану қажеттігі тууы мүмкін, мәжбүрленуде тұрған адам үшін осынадай проблемаларды бар екенінін көрсете алады. Мәжбүрленуде тұрған туралы хабарлауға елеу рәсімдері жоғарғы тәуекелдерімен барабар жағдайымен болуы тиіс, ондайға мынадай хабарлау көрсетеді.

Болуы мүмкін ақпараттық қауіпсіздіктегі оқиғалар мен қақтығыстар:

- қызметтерді, құралдарды немесе жұмыс істеуін жоғалту;
- жүйенің дұрыс емес жұмыс жасауы немесе артық жүктелуі;
- адамдық қателер;
- ережелерді немесе нұсқаманы сақтамау;
- физикалық қауіпсіздікті сақтамау;
- бақылау жүргізілмейтін жүйенің өзгеруі;
- бағдарламалық қамтамасыз етудің немесе аппараттық құралдардың істен шығуы;
- қол жеткізудің бұзылуы;
- ақпараттық жүйенің істен шығуы және қызметтерді берудің тоқтатылуы;
- арам ниетті бағдарламалық код;
- қызметтерді беруде бас тарту;
- өндірістік дерктердің толық еместігіне немесе дәлдік еместігіне байланысты болатын қателер;
- құпиялығының және тұтастығының бұзылуы;
- ақпараттық жүйелерді дұрыс емес пайдаланылуы.

Қол жетімді ақпараттың тұтастығы рұқсатсыз өзгертуден қорғалуы тиіс. Ақпараттық жүйеде жалпыға қол жетімді жасалған тұтастықты талап ететін, бағдарламалық қамтамасыз ету, деректер, басқадай ақпарат сәйкестендірілген механизмдермен қорғалуы тиіс. Жалпы пайдаланатын

жүйе ақпаратын пайдаланар алдында онда осал орынның бар болуына және тұрақтылықтан бастартуға тестіленуі тиіс. Соған дейін, ақпарат жалпы қолжетімді болғанда, осы қол жетімділіктің рұқсат етілетін нысандық үдерісі орындалуы тиіс.

1.4 Ақпараттық қауіпсіздендіруді қамтамасыз ету жүйелерінің сипаттамалық қасиеттері

Ақпараттық қауіпсіздендіру келесі жүйелік қағидаларда құрылу тиісті:
- жинақтылық;
- қорғаудың үздіксіздігі;
- ақылды жеткіліктілік;
- басқару және қолдану иілгіштігі;
- қорғау алгоритмдерінің және механизмдарының ашықтығы;
- қорғау шараларын және құралдарын қолдану қарапайымдылығы.

Жинақтылық қағидасы. Қорғау тұтас жүйелері құру жанында әдістердің және құралдарды комплексті қолдану АЖ қорғау әр текті құралдардың келісілген қолдануын болжайды, қауіптерді орындау маңызды каналдары барлық қайта жабушының және компоненттердің оның бөлек жапсарларда әлсіз орындарды ұстаушының еместің. Есепке ала тек қана емес қорғау жүйесі тиісті салып алу, сонымен қатар қауіпсіздік қауіпларының орындау принципшіл жаңа жолдарының көріну мүмкіншілігі есепке ала.

Үздіксіздік қағидасы. Ақпаратты қорғау - бір жолғы шара емес және өткізілген шаралардың айқын жиынтық емес тіпті және анықталған қорғау құралдары, ал толассыз мақсатқа бағытталған процес, АЖ барлық тіршілік циклы кезеңдерінде лайықты шараларды қабылдау. Қорғау жүйесін өңдеу қорғайтын жүйені өңдеумен паралельді жасалу тиісті.

Ақылды жеткіліктілік қағидасы. Абсолютті қорғау жүйесін жасау принципиалды мүмкін емес. Уақыттың және құралдарды жеткілікті саны жағдайында кез-келген қорғауды жеңуге болады. Сондықтан тек қана қауіпсіздік қабылдауға болатын деңгейінде әңгіме қозғау мәні бар.

Қорғау иілгіштік қағидасы. Қорғау жүйесін жасау белгісіздік жағдайында жиі кездеседі. Сондықтан, қабылданған шаралар және анықталған қорғау құралдары, бастапқы дәуірге әсіресе оларды пайдалану, шамадан тыс сияқты, дәл осылай қорғау жеткіліктісіз деңгейін қамсыздандыра алады. Қамтамасыз етуге арналған түрлендіру мүмкіншіліктері қорғанушылық деңгейімен, қорғау құралдары айқын иілгіштікке ие болу тиісті.

Алгоритмдердің және қорғау механизмдарының ашықтық қағидасының мәні тек қана ұйымдық құрылымның және оның ішкі жүйелерінің жұмыс жасау алгоритмдері құпиялығынан қорғау қамтамасыз етілмеу тиісті. Қорғау жүйесінің жұмыс алгоритмдерін білу оны жеңуге мүмкіндік туғызу тиісті емес.

Қорғау құралдарын қолдану қарапайым қағидасы. Қорғау механизмдары интуициялық мәлім болуға тиісті және қолдануда қарапайым. Қорғау

құралдарын қолдану арнайы тілдерді білу немесе әрекеттердің орындалуымен байланысты болу тиісті емес, көп әрекетті талап ететін маңызды қосымшалар ресми пайдаланушылары әдеттегі жұмысына, сонымен қатар ескішіл түсініксіздеу операциялардың орындалу пайдаланушыларынан талап ету тиісті емес (бірнеше пароль және аттарды енгізу және т.б.).

Компьютерлік жүйеге ойластырылған қатерлердің типтік тәсілдері және әсер ететін каналдары келесі болады:

- Қолжетімдік объектілеріне тікелей қатынасы;
- Қорғау құралдарын айналып қол жетімдік объектілеріне қатынас жасайтын бағдарламалық және техникалық құралдарды жасау;
- Қол жетімдік жасауға мүмкіндік беретін қорғау құралдарын өзгерту;
- Компьютерлік жүйенің техникалық құралдарына, функцияларын және құрылымын бұзатын және қол жетімдікті жүзеге асыруға мүмкіндік беретін бағдарламалық және техникалық механизмдерді енгізу.

Ақпаратты алу тәсілі бойынша қол жетімдік каналдарды мыналарға бөлуге болады: физикалық; электромагниттік (сәулелерді ұстап алу); ақпараттық (бағдарламалық - математикалық). Қол жеткізу әдістері: ақпаратты жазу; ақпаратты оқу; ақпаратты жоюға немесе оны өңдеу және сақтау ережелерін бұзуға әкеліп соғатын КЖ элементтеріне физикалық әсер ету.

Ең көп таралған белгілі әдістер және әсер ететін каналдар мыналар:

- Өңдеуден кейін қалған ақпаратты жинау;
- АЖ-ге оның интерфейстері арқылы біреудің паролін алу жолымен ену;
- «Люк» деп аталатын компьютер мүмкіндіктерін жасырын, құжатталмаған өңдеушілерді қолдану;
- АЖ-ге ақпаратты тасымалдау құралдары арқылы (дискета, CD-ROM) немесе желі арқылы (ЭП, FTP...) бағдарламаларды енгізу;
- Жүйені зерттеуге арналған дизассемблерлер мен отладчиктерді қолдану;
- Қоректену көзін және АЖ компоненттерінің схемасын желі бойынша жоғары күшті импульстерді беру арқылы істен шығару;
- Қосымша электромагниттік сәулелер мен нысаналаулардың (ПЭМИН) эфир немесе комуникация сызықтары бойынша ұстап алу;
- Intranet және Internet желілері арқылы желілік шабуылдарды жүргізу.

Әкімшілік аутентификациясының мәліметтерін табуға арналған каналдар маниторингі және ақпараттық ағындардың келесі мүмкіндіктері бар желі протоколдардың анализаторлары:

- Желі ресурстарын қашықтықтан басқару, торабтарға қол жетімдік;
- Желілік трафик жайлы статистикалық мәліметтерді жинау;
- Желі бойынша жіберілетін пакеттерді декодтау.
- Ақпаратты талдау үшін ұстап қалу кезінде мәліметтерді іріктеу.
- Жасырын тыңдау - желілік ағынды ұстау және оны талдау ("sniffing")
- TCP sequence number (IP-spoofing) болжау;
- "десинхрониздік жағдайда" қосуды енгізу

- Пассивті сканерлеу: демондардың қандай TCP-порттарда жұмыс істейтінін анықтау;
- ICMP-пакеттермен ("ping flood") басылу;
- SYN-пакеттермен ("SYN flooding") басылу.
- Жіберушінің жалған адрестері: Интернеттің электрондық поштасында жіберушілердің адрестеріне сенуге болмайды. Хатты ұстап алу. Пошталық бомба – электрондық пошта арқылы шабуыл жасау:
- Пошталық ақпаратламалар диск толғанша қабылдана береді
- Кіріс кезек тағы өңдеу және беру керек хаттамалармен толады
- Қолданушыға диск квотасы шектен шыққан болуы мүмкін

Желілерді қорғау

Бір компьютерде жұмыс істеуден бірнеше компьютерлер желісінде жұмыс істеуге көшу барысында ақпаратты қауіпсіздендіруді қиындататын келесі себептері бар:

- желіде бірнеше пайдаланушылардың жұмыс істеуі және олардың күнделікті ауысып отыруы, пайдаланушының аты мен пароль арқылы ақпаратты бөтен пайдаланушылардан қауіпсіздендіру жеткіліксіз;
- желіге көптеген потенциалдық каналдардың кіріп кетуі;
- эксплуатациялық процесте туындайтын аппараттық және бағдарламалық қамтамасыз етудің жеткіліксіздігі.

Кез-келген қосымша байланыстар басқа сегменттермен немесе Интернет желісіне қосылу жаңа проблемаларды туындатады, оған қоса компьютерлік вирустармен зақымдау мүмкіншілігін көбейтеді. Әрбір құрылғы желіде, сәйкес өрістерді идеалдық емес экрандаудан электромагниттік сәулендірудің потенциалдық көзі болып табылады, әсіресе жоғары жиіліктерде. Электромагниттік сәулелендіруден басқа потенциалдық қауіпті кабелдік жүйеге контактілі емес электромагнит әсер етеді. Бірақ коаксиалдық кабелдер немесе “витых пар”, оларды “медные кабелы” деп атайды. Проводтық қосудың бұл типтерін физикалық жалғаудағы кабелдік жүйеге қолдану мүмкін. Егер желіге кіру үшін пароль белгілі болса, онда мұндай пайдаланушыларға желіге кіру файл-сервер арқылы, немесе жұмыс орындарының бірінен іске асуы мүмкін. Сол себепті желіден тыс орналасқан ақпаратты сақтайтын құрылғылардан ақпарат жоғалу мүмкін.

Желідегі ақпаратты қорғауды арнайы “шуыл генераторын” қолдану арқылы жүзеге асыруға болады. Оптоволокондық кабелдер электромагниттік өрістің әсерінен оқшауланған, және бұлар санкционирленбеген қосуларды таба алады. Ақпаратты қорғауды қамтамасыз ететін құралдарды үш топқа бөлуге болады:

1. **Техникалық құралдар**, бұлар физикалық кіруге кедергі жасайды (кілттер, терезедегі решеткалар, сигнализация және т.б.). Техникалық құралдың құндылығы субъектілік факторлардан тәуелсіздігімен және жоғары модификацияға беріктігімен байланысты. Кемшіліктері – жеткіліксіз сапасы, қымбат тұратындығы және т.б.

2. **Бағдарламалық құралдар**, бұған қоса пайдаланушыларды идентификациялауға арналған бағдарламалар, ақпаратты шифрлау, уақытша файлдарды жою, жүйені қауіпсіздендіретін текстік бақылау және т.б. Бағдарламалық құралдың құндылығы – универсалдығы, беріктігі, орнатудың қарапайымдылығы, модификациялауға мүмкіншілігі. Кемшіліктері – желінің физикалық мүмкіншілігін шектеуі, файл-сервердің және жұмыс орындардың жарты ресурстарын қолдану, кездейсоқ немесе келісілген өзгертулерге жоғары сезімталдығы, компьютердің типіне (аппараттық құралына) тәуелді мүмкіндігі.

3. **Ұжымдық құралдар**, бұған қоса ұжымдық-техникалық және ұжымдық-құқықтық құралдар. Ұжымдық құралдардың құндылығы - әр түрлі мәселелерді шешуге мүмкіншілігі, құрудың қарапайымдылығы, желідегі өзгерістерге тез сезімталдығы, модификациялауға мүмкіншілігінің шексіздігі. Кемшіліктері – субъектік факторларға жоғары тәуелдігі және нақты бөлімшелердің жалпы ұжымдық жұмыстармен байланысы.

Мәліметтерді шифрлау ақпаратты қауіпсіздендіруге арналған әр түрдегі бағдарламалық құралдардан тұрады. **Шифрлау түсінігі -"Криптография Firewalls"** ұғымымен байланысты жиі қолданылады. Криптография - шифрлау және шифрлық мәліметтерді ауыстыруға байланысты қосымша мәселені шешу жолдарын қарастырады. Шифрлауға арналған бағдарламалар саны шектеулі және олардың жартысы де-факто немесе де-юре стандарттары болып табылады. Бірақ шифрлау алгоритмін білмей дешифрлауды жүргізу қиын.

Ақпаратты қорғаудың бағдарламалық мүмкіншіліктері

Желілік операциялық жүйелерде орнатылған қауіпсіздік құралдары жеткіліксіз, себебі олар тәжірибе жүзінде пайда болатын жағдайларды толық шеше алмайды. Мысалыға, NetWare 3x, 4x желілік операциялық жүйелері аппараттық бүліну және құртылудан ақпараттардың эшалондаған қауіпсіздігінің беріктігін қамтамасыз ете алады.

Novell фирмасының SFT (System Fault Tolerance) бағдарламасы үш негізгі деңгейді қарастырады:

- SFTLevel I. Бірінші деңгей FAT және Directory Entries Tables-тің қосымша көшірмелерін жасауды қарастырады. Сонымен қатар файлдық серверге жаңадан жазылған берілгендердің блогын тездетіп верификациялауды және де кез-келген қатты дискіде 2% көлемді резервтеуді ұйымдастырады. Бүліну табылған жағдайда, берілгендер дискінің резервтелген облысына бағытталады, ал бүлінген блок "нашар" блок ретінде белгіленіп, келесіде ол қолданылмайды.
- SFTLevel II. Екінші деңгейдің "Арнайы дискілер" құру мүмкіндігі бар. Одан басқа қосымша дискілік бақылаушылар, ток көзін және интерфейстік кабельдерді дубльдеу мүмкіншіліктері бар.
- SFTLevel III. Үшінші деңгей локалды желіде серверлердің көшірмесін пайдалануға мүмкіндік береді. Олардың біреуі - "негізгі",

екіншісі – “барлық” ақпараттың көшірмесін сақтайды. Егер “негізгі” сервер істен шықса, екіншісін қолдануға болады.

NetWare желілеріндегі басқару және кіру құқығын шектеу жүйесі де бірнеше деңгейден тұрады:

- бастапқы кіру деңгейі пайдаланушы аты мен паролінен, жұмысқа рұқсат беру және бермеу типіндегі есептік шектеудің жүйесінен тұрады.
- пайдаланушылар құқығының деңгейі.
- файлдар мен каталог атрибуттарының деңгейі.
- файл-сервердің консолдық деңгейі.

Бірақ NetWare-дің операциялық жүйедегі бұл ақпаратты қорғау жүйесіне сену барлық кезде дұрыс емес. Өйткені, Интернеттің көптеген ережелері және дайын бағдарламалары санкциясыз кіруге болмайтын кейбір элементтерін бұзуға мүмкіндік береді. Мұндай ескерту сонымен қатар орнатылған ақпаратты қорғау құралдары бар мықты желілік операциялық жүйелерге де қатысты (Windows, Unix). Себебі, бұл желілік операциялық жүйелерінің шешетін есебі көптеген есептердің тек бір бөлігі ғана болып табылады. Бір функцияны алға шығарып, басқа функцияларға көңіл аудармау желілік операциялық жүйелерінің дамуының магистралды бағыты бола алмайды. Бірақ та, NetWare 4.1 желілік операциялық жүйесінде “ашық кілт” принципі негізінде RSA-алгоритмі көмегімен берілгендерді кодтау мүмкіндігі қарастырылған.

Ақпаратты қорғаудың арнайы бағдарламалық құралдарының санкциясыз кіруден қауіпсіздігі орнатылған желілік операциялық жүйелерге қарағанда мүмкіндіктері көп және мағыналы сипатталған. Шифрлау бағдарламаларынан басқа ақпаратты қорғау құралдары өте көп. Олардың ішінен екі жүйе көп қолданыс тапқан. Олар ақпараттық ағынды шектеуге көмектеседі.

1. Firewalls - *брандмауэрлер* (Firewalls – ағылшын тілінен аударғанда – “отты дуал”). Жергілікті және аумақты желі арасында арнайы аралық серверлер құрылады. Олар өзі арқылы өтетін желілік-транспорттық деңгейлер трафигін бақылап, фильтрлейді. Бұл жүйе корпоративтік желідегі санкциясыз кіруді азайтады, бірақ оны тіптен жоя алмайды. Бұдан қауіпсіз түрі – ол маскарад әдісі (masquerading). Бұл әдісте жергілікті желіден өтетін трафик firewall-сервері атынан жіберіледі. Сондықтан жергілікті желі тәжірибе жүзінде көрінбей қалады.

2. Proxy-servers. Жергілікті және аумақты желі арасындағы барлық желілік-транспорттық деңгейлер трафигі толығымен шектеледі, яғни маршрутизация типті болмайды, ал жергілікті желі аумақты желімен арнайы делдал-серверлер арқылы байланысады. Бұл жағдайда жергілікті және аумақты желілер арасындағы байланыс тіпті мүмкін емес. Сонымен қатар бұл әдіс жоғары деңгейлі қауіпсіздікті қамтамасыз ете алмайды.

Ақпаратты қорғаудың әкімшілік-ұйымдастыру қорғаныс құралы

Әкімшілік-ұйымдастыру қорғаныс құралдарына ақпаратты және мәліметтерді өңдеу жүйелерінің функциялық процестеріне енуді

регламенттеу, қызметкерлердің іс-әрекеттерін регламенттеу және т.б. жатады. Олардың мақсаты қауіптің іске асуын мейілінше болдырмау. Ең көп тараған әкімшілік-ұйымдастыру қорғаныс құралдарына мыналар жатады:

- ЭЕМ және басқа ақпаратты өңдеу құралдары орналасқан жерде кіріп шығуға бақылау - рұқсат беру әдісін қолдану;
- арнайы рұқсат қағаздарын дайындау және онымен өз адамдарын қамтамасыз ету;
- мәліметтерді өңдеуге қатысатын қызметкерлерді таңдауға байланысты іс-шаралар өткізу;
- құпия ақпараттарды беруге немесе өңдеуге тек қызмет бабымен рұқсаты бар адамдарды ғана жіберу;
- өзіндік құпиясы бар магниттік және басқалай ақпарат тасымалдағыштарын және тіркеу журналдарын сейфте немесе басқа адамдар кіре алмайтын жерлерге сақтау;
- ақпараттарды өңдеуге арналған бөлмеге тыңдағыш құралдар қойылуына қарсы қорғаныс ұйымдастыру;
- құпия ақпараттардың құжаттарының қолданылуы мен жойылуының есепке алынуын ұйымдастыру;
- компьютер құралдарымен және ақпарат тасымалдағыш жүйелерімен жұмыс істеуге арналған қызмет бабына байланысты ережелер жасау;
- ақпараттық және есептеу қорларына енуге тек қана өз қызметіне байланысты функционалдық міндетін атқаратын адамдарға ғана рұқсат беруі.

Техникалық құралдар

Техникалық объектілер мен қорғаныс элементтері физикалық тұйық ортаны құруға арналған. Бұл үшін төмендегідей іс-шаралар іске асырылады:

- ақпараттар өңделетін бөлмеге физикалық тосқауыл құралдарын орналастыру, кодтық құлыптар, сигнализациялар орнату;
- ақпарат өңделетін бөлмеден электромагнит сәулесінің таралуын жұқа металдармен немесе арнайы пластмассалармен экрандау арқылы болдырмау;
- құнды ақпараттарды өңдеуге арналған құрал-жабдықтардың электр тогын арнайы бөлек алуын немесе жалпы электр жүйесімен арнайы желілік фильтрлер арқылы алуын қамтамасыз ету;
- ақпараттарды алыс қашықтықтан рұқсатсыз жазып алуын болдырмас үшін сұйық кристалданған дисплейлер, ағындық және лазерлік принтерлерді қолданылуын қамтамасыз ету;
- автоматтық қорғаныс құралдары аппараттың сыртқы қабаты штопка түрінде қолдану және аппараттың ашылғаны туралы бақылау орнату.

Бағдарламалық қорғаныс құралдары мен әдістері

Бағдарламалық қорғаныс құралдары мен әдістері ақпараттарды қорғау үшін жеке компьютерлер мен компьютер желілерінде кеңінен қолдануды және мынандай қорғаныс функцияларын іске асырады:

- ақпараттық қорларға енуді бақылау және шектеу;
- болып жатқан процестердегі оқиғаларды тіркеу және анализ жасау;

▪ақпараттардың криптографиялық жолмен қорғалуы, яғни мәліметтердің шифрлануы;

▪қолданушылар мен процестердің ұқсастығы, аутентивтігі және т.б.

Қазіргі кезде экономикалық ақпараттарды өңдеу жүйелерінде осы іс-шаралар топтамаларының ішіндегі ең салмақтысы, ол арнайы бағдарламалар бумасы. Бұл бағдарламаларға ақпараттарды қорғау тапсырмалары кіреді.

Операциялық жүйелерді парольмен жабдықтау

Операциялық жүйелерді парольдік қорғау компьютерлік тораптардағы ақпараттарды қорғаудың негізгі деңгейі болып саналады. Бұл қорғау жүйесі барлық операциялық жүйелерде қолданылады. Компьютермен жұмыс бастағанда, қолданушы операциялық жүйелерге кірерде өзін тіркеу тиіс, яғни аты мен паролін енгізу керек. Аты операциялық жүйелерге қолданушыны идентификациясы үшін керек етіледі. Ал пароль енгізілген идентификацияның дұрыстығын дәлелдейді. Диалогтық режимде қолданушының енгізген ақпараты операциялық жүйелерінің үкімінде бар ақпаратпен салыстырылады. Егер салыстыру сәтті аяқталса, онда қолданушы операциялық жүйелердің барлық ресурстарымен жұмыс жасауына болады. Қазіргі таңдағы операциялық жүйелердегі қолданушылардың парольдарын шифрлауға арналған криптографиялық алгоритмдер көп жағдайда өте берік келеді. Мұндай парольдарды бұзу үшін арнайы бағдарламалар – парольды бұзу бағдарламалары жасалынған. Парольды бұзу бағдарламалары операциялық жүйелерге қойылған парольді сол криптографиялық алгоритмдердің көмегімен кері шифрлау арқылы тауып, табылған сөзді жүйелік файлдағы жазылған сөзбен салыстырады. Белгілі бір символдар жиыны мен автоматты реттелген символдар тізбегін парольдық бұзу бағдарламалары варианттар есебінде қолданады. Бұл әдіс барлық парольдарды бұзуға мүмкіндік береді. Егер парольдық шифрланған түрі белгілі болып және ол осы жиын символдарынан тұратын болса, парольды бұзуға кететін максимальді уақытты келесі формуламен есептеуге болады:

$$T = \frac{1}{S}\sum_{i=1}^{L} N^i;$$

Мұндағы N – жиындағы символдар саны;

L - әр секундтағы тексеру саны;

S – парольдың шектік ұзындығы;

S – парольдың қауіпсіздігін бұзатын компьютердің жылдам істеуі мен операциялық жүйеге тәуелді. Операциялық жүйелердің парольдық қауіпсіздігін бұзуға арналған бұл әдіс өте көп уақытты алады.

Windows NT операциялық жүйесінің парольдық қауіпсіздігі

Windows NT қауіпсіздік жүйесінің негізгі бір компоненті қолданушылардың жазу тіркегіш диспетчері болып табылады. Ол қауіпсіздік жүйенің басқа компьютермен байланысын қамтамасыз етеді. Парольдар туралы мәлімет **SAM** берілгендер қорында сақталады. (SAM – “Security Acconnt Management Database”). Бұл база кез-келген компьютерде Windows

NT операциялық жүйесінде болады. Онда Windows NT қолданушыларының аутентификациясы үшін қолданатын, жүйеге кірердегі барлық ақпараттар сақталады. SAM берілгендер қоры Windows NT жүйесінде жүйелік реестрдің бір бұтағы болып саналады. SAM берілгендер қорындағы ақпарат негізінде екілік формада сақталады. Оған рұқсатты қатынас жазу тіркегіш диспетчері арқылы іске асырылады. Ол SAM берілгендер қорындағы жазылған ақпаратты өзгертуге жол бермейді. SAM берілгендер қорына енгізілген парольдық тізбек DES алгоритмі арқылы шифрланады.

Windows NT жүйесінде парольдарды пайдалану

Парольдар туралы мәлімет SAM берілгендер қорында сақталған. Олар Windows NT қолданушының аутентификация қызметін атқарады. Интерактивті немесе желіге кіру кезінде жүйеге енгізілген қолданушы парольдары бірінші хэшифрланады, содан кейін екінші шифрланады. SAM берілгендер қорында жазылған 16 байттық тізбекпен салыстырылады. Егер олар сәйкес келсе қолданушы жүйеге кіруге қол жеткізеді. SAM берілгендер қорының мәліметтері шифранған түрде немесе хэшифрлаған пароль түрінде сақталынады. Бірақ кейбір жағдайларда операциялық жүйе олардың біреуін ғана есептейді. Мысалыға: қолданушы Windows for Workgroups компьютерінде жұмыс істеп отырған Windows NT домені қолданушысы паролін өзгертетін болса, онда оның есептік тізімінде тек Lan Manager паролі ғана қалады. Ал, егер, қолданушылық пароль 14 символдан көп болып немесе бұл символдар көмекші құралдардың жиынтығына кірмейтін болса, онда SAM берілгендер қорына Windows NT паролі енгізіледі.

Жүйені заңсыз, яғни тіркеуден өтпеген қолданушылардан қорғау үшін біріншіден есептік тізімді орнату керек. Қолданушылар өзінің паролін енгізген жағдайда есептік тізім парольді тексереді. Егер пароль дұрыс болмаған жадайда, қолданушы жүйеге кіре алмайды. Мысалы: Windows жүйесінде кез-келген қолданушыға арнайы дербес есептік тізім және сонымен қатар ішкі сақтау коды SID тағайындалады (Security Identifier), ал кез-келген қолданушыға идентивті және оперативті түрде қолдануға мүмкіндік береді.

Windows жүйесінде бұл анықтамаға сай келмейтін есепті тізім бар. Ол Guect (гость). Бұл тізімге кіру жолы оңай, өйткені оның паролі бәріне ортақ болады. Бұл тізімнің кемшілігі, ол тек шектелген қол жеткізу жүйесінде жұмыс істей алады. Ішкі сақтау коды берілгендер жүйесінде қолданушы қандай қызмет атқара алатындығы анықталады.

Идентивті қолданушыларға жай пароль емес, арнайы пароль қойылады. Бұл заңсыз тұлғалардың есептік тізімді білген жағдайда да жүйеге кіруге жол бермейді.

2 Компьютерлік қылмыстар. Компьютерлік вирус. Антивирустық бағдарламалар

2.1 Компьютерлік вирус

Компьютерлік вирус – арнайы жазылған шағын көлемдегі (кішігірім) бағдарлама. Ол өздігінен басқа бағдарламалардың соңына немесе алдына қосымша жазылады да, оларды ″бүлдіруге″ кіріседі, сондай-ақ компьютерде тағы басқа келеңсіз әрекеттерді істеуі мүмкін. Ішінен осындай вирус табылған бағдарламалар ″ауру жұққан″ немесе ″бүлінген″ деп аталады. Мұндай бағдарламаны іске қосқанда алдымен вирус жұмысқа кірісіп, бағдарламаның негізгі функциясы орындалмайды немесе қате орындалады.

Вирус іске қосылған бағдарламаларға да кері әсер етіп, оларға да ″жұғады″ және басқа да зиянды іс әрекеттер жасай бастайды. Мысалы, файлдардың немесе дискідегі файлдардың орналасу кестесін бүлдіреді, жедел жадтағы бос орынды жайлап алады және т.с.с.

Өзінің жабысқанын жасыру мақсатында вирустың басқа бағдарламаларды бүлдіруі және оларға зиян ету әрекеттері көбінесе сырт көзге біліне бермейді.

Оның кері әсері белгілі бір шарттарды орындағанда ғана іске асады. Вирус өзіне қажетті бүлдіру әрекеттерін орындаған соң, жұмысты басқаруды негізгі бағдарламаға береді, ал ол бағдарлама алғашында әдеттегідей өз жұмысын істей алмайды, тоқтап қала беруі мүмкін, немесе қателер жіберуі, өшіп қалуы. Сөйтіп, ол бағдарлама бұрынғы қалпынша жұмысын жалғастырып, сырт көзге ″вирус жұққандығы″ бастапқы кезде байқалмай қалады.

Компьютерлік вирустар ″таза″ компьютерлерге вирус жұққан иілгіш дискеттер арқылы таратылады. Егер компьютер жергілікті желіге қосылған болса, онда вирустың таралуына бұрынғыдан да кең жол ашылады.

Айта кететін жайт, вирустардың кейбір түрлері компьютерге келісімен зиянды істеріне кірісіп кетеді, ал олардың кейбірі файлдар құрамына енсе де жұмысына кіріспей, біраз уақыт тым-тырыс жасырынып жатады, бұл уақытты *″инкубациялық мезгіл″* деп атайды. Бұл мезгіл аралығында олар екпінді күйде файлдар арасына таратылып, зақым келтіруді белгілі бір уақыт мөлшері өткен соң немесе ол өзінен-өзі белгіленген мөлшерде көбейтіп болған соң ғана бастайды.

Вирустан сақтану үшін мынадай шаралар қолдануға болады:

- ақпаратты қорғаудың жалпы шаралары – дискіні физикалық зақымданудан сақтау, дұрыс жұмыс істемейтін бағдарламаларды қолданбауға және жұмыс істеп отырған адам қателіктер жібермеуге тырысу;
- профилактикалық шараларды пайдалану, яғни вирустарды жұқтыру мүмкіндігін азайту тәсілдерінің орындалуын қарастыру;
- вирустан сақтайтын арнайы бағдарламаларды қосымша пайдалану;
- вирустардың кейбір түрлерінің кері әсері тіпті одан да терең болады.

Барлық *.com және *.exe типті файлдар үшін – каталогтағы файлдың алғашқы мәлімет көрсетілген орынға вирус жазылған қате орын көрсетіліп, ал дұрыс көрсеткіш – таңбаланған (кодталған) түрде каталогтың пайдаланылмайтын бөлігіне жасырылады. Сол себепті кез-келген бағдарламаны іске қосқанда дискіден бірінші вирус оқылады да, ол тұрақты ЭЕМ жедел жадында сақталып файлдарды өңдейтін DOS бағдарламаларына жабысады.

Вирустың көптеген түрлері ЭЕМ жадында DOS-ты қайта жүктегенше тұрақты сақталып, оқтын-оқтын өзінің зиянын тигізіп отырады.

Вирустың зиянды іс-әрекеттері алғашқы кезде жұмыс істеп отырған адамға байқалмайды, өйткені ол өте тез орындалып, әсері білінбеуі мүмкін, сондықтан көбінесе адамдардың компьютерде әдеттегіден өзгеше жағдайлардың болып жатқанын сезуі өте қиынға соғады.

Компьютерлерде ″вирус жұққан″ бағдарламалар саны көбеймей тұрғанда, онда вирустың бар екені сырт көзге ешбір байқалмайды. Бірақ біраз уақыт өткен соң, компьютерде әдеттегіден тыс, келеңсіз құбылыстар басталғаны білінеді, олар, мысалы, мынадай іс-әрекеттер істеуі мүмкін:

- кейбір бағдарламалар жұмыс істемей қалады немесе дұрыс жұмыс істемейді;
- экранға әдеттегіден тыс бөтен мәліметтер, символдар, әріптер және т.с.с. шығады;
- компьютердің жұмыс істеу жылдамдығы баяулайды және нашарлайды;
- көптеген файлдардың бүлінгені байқалады және т.с.с.

Компьютерге вирус жұққанын байқаған кезде кейбір файлдар мен каталогтар, дискідегі мәліметтер бұзылып үлгереді. Оның үстіне пайдаланылған дискеттер арқылы немесе жергілікті байланыс желілері бойымен компьютердегі вирус, басқа компьютерлерге таралып кеткені байқалмай қалады.

Вирустардың кейбір түрлерінің кері әсері тіпті одан да терең болады. Олар бастапқы кезде өзінің жұққанын білдіртпей, көптеген бағдарламалар мен дискілерге үндемей таралып кетеді де, сонан соң бірден бел шешіп зиянкестік жасауға кіріседі. Мысалы, компьютердегі қатты дискті форматтап шығады. Ал зиянкестік әсерлерін бағдарламаларға өте аз тигізіп, бірақ қатты дисктегі мәліметтерді іштен ″мүжіп″, құртып жататын вирустарға не істеуге болады?!

Осының бәрі вирустан дер кезінде құтылмасақ, оның келешектегі әсері керекті мәліметтерді жоғалтуға душар ететіні талас тудырмаса керек.

Вирус бағдарламасының байқалмау себебі олардың көлемі кішігірім ғана болады да, өздері ассемблер тілінде жазылады. Кез-келген жағдайда вирус бағдарламасы қай компьютерге арналып жазылса да, ол мәлімет алмасып жұмыс істейтін басқа компьютерлерге де тез тарап кетеді және өте көп зиянкестік әрекеттер жасауы мүмкін.

Қазіргі кездегі вирустар негізгі екі топқа бөлінеді:

- резиденттік(компьютер жадында тұрақты сақталатын) вирустар.
- резиденттік емес вирустар.

Вирус жұққан бағдарлама іске қосылғанда резиденттік вирустар әсерлене әрекет етеді, олар жедел жадқа көшіріліп жазылып, алғашқы бірсыпыра уақытта әсері сезілмегенмен, соңынан іске бірден қатты кіріседі. Бұл вирустарды тез анықтау ісін қиындатады.

Дискілерге мәлімет жазу кезінде вирус өзінің жабысуына қолайлы сәт іздеп, негізгі операциялар орындалып жатқанда солармен қосылып дискіге жазылып алады да, оның қалай жұққанын адамдар білмей де қалады. Ал, резиденттік емес вирустар жедел жадқа тұрақты күйде жазылмайды, бірақ вирустың әсері тиген бағдарлама іске қосылғанда ол екпіндене түседі де, өзі жұмыс істеп тұрған каталогтан немесе PATH командасында көрсетілген каталогтардан өзі ішіне байқаусыз еніп кететін файл іздейді. Ондай файлды тауып алып, оның ішіне кіріп алып, ол кейін жұмыс істейтін кезде соған зиянды әрекетін тигізеді.

Бүлінген және вирус жұққан файлдар

Вирус дискідегі кез-келген файлды бүлдіре алады, бірақ кейбір файлдарға ол бірден жабысады, яғни ол файлдың ішкі көлемінен орын алып, оның қызметін түрлендіріп, қолайлы жағдай туғанда, зиянды әрекетін бастап кетеді. Дегенімен, көптеген бағдарламалар тексті мен құжаттарға мәліметтер қоймасының ақпараттық файлдарына электрондық кестелердегі мәліметтерге вирустар онша әсерін тигізе алмайды, тек оларды аздап қана зақымдауы мүмкін.

1. Бірден орындалатын файлдар, белгілі-бір іс-әрекет орындайтын кеңейтілулері *.com және *.exe болып келген файлдар, сондай-ақ басқа бағдарламаларға қажет кезінде қосылатын оверлейлік файлдар. Файлдарды зақымдайтын ондай вирустарды **файлдық вирустар** деп атайды. Вирус жұққан файлдар өздерінің кері әсерін жұмыс істеген сәттерде жасайды. Ең қауіпті вирустарға резиденттік түрде жедел жадта сақталып, орындалатын әрбір бағдарламаны зақымдап отыратындары жатады. Ал, егер де, олар AUTOEXEC.BAT және CONFIG.SYS арқылы іске қосылатын бағдарламаларға жұқса, онда компьютер өшіріліп қайта іске қосылған сайын вирустар өз әсерлерін тұрақты қайталап отырады.

2. Операциялық жүйенің жүктеуші мен қатты дискінің ең басты мәлімет жіктеу жазбасы. Бұл аумақтарды зақымдайтын вирустар **жүктегіш** немесе **Boot-вирустар** деп аталады.

Бұндай вирустар өз қызметін компьютерді іске қосқанда, яғни операциялық жүйені жүктегенде бірден бастайды және әрдайым компьютердің жедел жадында тұрақты сақталады. Бұлардың таралу тәсілі – компьютерге салынған дискеттердің алғашқы жолдарына жазылған жүктегіш мәліметіне зақым келтіру болып табылады. Әдетте мұндай вирустар екі бөліктен тұрады, өйткені дискеттің жүктеуіш жазбасы мен операциялық жүйенің басты жазбасы өте шағын көлемнен тұрады, сондықтан вирус бірден түгелдей олардың ішіне орналаса алмайды. Вирустың екінші бөлігі дискінің түпкі каталогының соңына немесе мәліметтер кластерлеріне жазылып қалады.

3. Құрылғылар драйверлері, яғни CONFIG.SYS файлының шеткері құрылғылар көрсетілетін **devise** деген сөз тұрған қатарында жазылған файлдар. Ондай файлдағы вирус сол құрылғыны іске қосқан сайын, қызметке кіріседі. Бірақ драйверлерді бір компьютерден екінші компьютерге көшіру өте сирек болатындықтан, мұндай вирустар көп тарала қоймаған. DOS жүйелік файлдарына (MS-DOC.SYS және IO.SYS) да вирус жұқтырылуы теория жүзінде мүмкін болғанымен, олардың таралуы іс жүзінде өте сирек кездеседі.

Әдетте әрбір вирус түрлі файлдың бір немесе екі типіне (түріне) ғана жұғады. Көбінесе бірден орындалатын файлдарға жұғатын вирустар жиі кездеседі. Дискінің жүктегіш аймағын зақымдайтын вирустар екінші орында деп алуға болады. Шеткері құрылғылар драйверлерін зақымдайтын вирустар сирек кездеседі, әдетте олар бірден орындалатын файлдарға да зиянын тигізеді.

4. Файлдық жүйені өзгертетін вирустар. Соңғы кезде вирустың жаңа түрлері – дискідегі файлдық жүйені өзгертетін вирустар көбейіп таралуда, олардың қысқаша **DIR вирустар** деп атайды. Мұндай вирустар өз текстін дискінің белгілі бір бөлігіне (әдетте дискінің соңғы кластеріне) жасырын жазып қояды да, оны дискінің файлды орналастыру кестесіне FAT файлдың соңы ретінде белгілейді.

Барлық *.com және *.exe типті файлдар үшін – каталогтағы файлдың алғашқы мәлімет көрсетілген орынға вирус жазылған қате орын көрсетіліп, ал дұрыс көрсеткіш – таңбаланған (кодталған) түрде каталогтың пайдаланылмайтын бөлігіне жасырылады. Сол себепті кез-келген бағдарламаны іске қосқанда дискіден бірінші вирус оқылады да, ол тұрақты ЭЕМ жедел жадында сақталып файлдарды өңдейтін DOS бағдарламаларына жабысады. Бірақ жалпы көрініс каталог дұрыс жұмыс атқарған сияқты болып сырт көзге мұның әсері білінбей тұрады. Тек вирусы бар дискеттерден барлық бағдарламалық файл оқитын сәттерде оның нақты көлемі небәрі 512 немесе 1024 байт қана болып қалады. Бірақ атқарылуға тиіс вирусы бар әрбір бағдарлама іске қосылғанда оның дұрыс бағдарламаларына жабысады. Бірақ жалпы көрініс каталог дұрыс жұмыс атқарған сияқты болып сырт көзге мұның әсері байқалмайды. Міне осылай ауырған дискілерді дұрыс қалпына келтіру үшін тек арнайы антивирустық бағдарламалар қажет (мысалы, Aidstest бағдарламасының соңғы нұсқалары).

5. "Көрінбейтін" және өздігінен өрбитін вирустар. Өзін жәй көзге сездірмес үшін кейбір вирустар жасырынудың қилы-қилы тәсілдерін пайдаланып жүр. Осындайлардың екі түрін – көрінбейтін және өздігінен өрбейтін вирустарды қарастырайық.

Көрінбейтін вирустар.

Көптеген резиденттік вирустар былай жасырынуды әдетке айналдырған, олар DOS жүйесінің вирус жұққан файлдарды шақыруын өзгертпей дұрыс күйінде қалдырады. Бірақ бұл эффект тек вирус жұққан компьютерде ғана байқалады, ал вирус жұға қоймаған компьютерлерде файлдар мен дискілерді жүктеуіш аймақтарының өзгеруін байқау қиын емес.

Өздігінен өрбитін вирустар

Вирустардың жасырыну жолының екінші тәсілі - өзін өзі аздап өзгертіп, өрбіп толықтырылып отыруы. Көптеген вирустар жасайтын кері әсерін байқатпас үшін өз көлемінің бірсыпырасын кодталған (таңбаланған) жасырын күйде сақтайды. Бірте-бірте өрби отырып олар таңбалану тәсілін де, таңбаланбаған алғашқы бөлігін де аздап өзгертіп отырады. Осының арқасында вирусты іздеп табатын тұрақты байттар тізбегі болмай, оларды ұстайтын детектор-бағдарламалар жұмысы қиындайды.

Компьютерлік вирустардың қысқаша жіктелуі

Қазіргі кезде 10 000 шамасында компьютерлік вирустар белгілі. Оларды әдетте әсер етуіне, логикасына байланысты және көлеміне қарай топтарға жіктейді (1-кесте).

Логикасына және мақсатына қарай оларды шартты түрде төмендегідей жіктеуге болады:

1. **″Ұстауыш вирустар″** - бағдарламалық құралдар кешеніндегі қателіктер мен дәлсіздіктерді пайдаланады. Көлемді бағдарламаларды түзету кезіндегі белсенділік көрсетіп бағдарламаға жабысады. Әр түрлі зиянды әрекеттері бар қауіпті вирус.

2. ″Логикалық бомбалар″ (баяу әсер ететін ″бомбалар″**)** – қарапайым бағдарламаларға кіріп алып білінбей тұрады. Тек белгілі бір шарттар (көрсетілген күн, ай мерзімінде немесе уақытта, бағдарлама орындалуының белгілі кезеңінде) орындалғанда ғана әсер ете бастайда. Сол шарт орындалар мезетке дейін неғұрлым көп бағдарламаларға ″жұғуға″ тырысады.

3. ″Құрттар″ - жүйелік бағдарламалаушылардың ақпараттық – есептеу желілерінің бос тұрған ресурстарын анықтау бағдарламаларына кіріп алып, сол бос құрылғыларды тектен-тек жұмыс істеуге мәжбүр етеді. Мысалы, оларды шексіз циклге енгізіп, құрдан-құр жүргізіп қояды немесе қажетсіз мәліметтерді баспаға шығартады және т.с.с.

4. ″Троян аттары″ - қарапайым қолданбалы бағдарламаларға еніп алып, соларға рұқсат етілмеген әрекеттерді (жасырын ақпаратты оқып жария етеді, жедел жадтағы ақпаратты ″басқа жаққа″ жіберуге дайындалады) орындатады. Мысалы, Word-та тексттерді теретін болсаңыз әр пернені басқан сайын және сол әріп немесе сол символдың артына сөз немесе символдар жазуы мүмкін. Жасалу құрылымы мен көбею жолы оңай болғандықтан, көбінесе компьютер желілерін жайлап алады. ″Троян аттары″ - интернет желілерінде өте тез көбейіп компьютерге қауіп төндіреді.

Кесте 1 Компьютерлік вирустардың қысқаша жіктелуі

Көлемі бойынша	Логикасы бойынша	Әрекетіне байланысты	Мақсатына қарай
"А"648 байт	"Ұстауыштар"	ДЭЕМ-дерде	
"В"1701 байт			"бей сауыт"
"С"1808 байт	"Логикалық	көп машиналы	"шантаж

	бомбалар"	кешендерде ақпараттық	жасаушы"
"D" n байт	"Құрттар"	Есептеу желілерінде	
"E"1800 байт	"Троян аттары"	Есептеу желілерінде	
"N" n байт	"Жолбарыстар"	Ақпараттық желілерінде	
"Z" n байт	ЭЕМ желілерінде		"мағынасыз" "насихатшы"

Мақсатына қарай вирустар мынадай 4 бөлікке бөлінеді:

1. ″Бейсауат″ (гуманда) – онша қатты зиянын тигізбейтін вирустар.
2. ″Шантаж жасаушы″ - мысалы, белгілі төлемақы берсе, вирус әсері жоғалатынын анонимді түрде хабарлайтын ″баяу әсер ететін бомбалар″.
3. ″Насихатшы″ - ″өзін көрсету″ мақсатында жасалған.
4. ″Мағынасыз″ - атынан-ақ әсері түсінікті.

2.2 Антивирустық бағдарламалар

Жалпы, ақпаратты қорғау тәсілдері тек вирустан сақтануда ғана емес, басқа жағдайда да пайда болатынын есте сақтаған жөн. Ондай тәсілдің негізгі екі түрі белгілі.

1. **Ақпараттың көшірмесін** алып отыру – файлдарды және дискінің жүйелік мәліметтерін көшіріп сақтау.

2. Керекті ақпаратыңызды басқалардың жиі пайдалануына **тосқауыл қою** – ол ақпаратты рұхсатсыз (санкциясыз) көшіріп алуды, яғни бағдарламамен дұрыс жұмыс істемейтіндерден және қателігі бар бағдарламалардан қашық жүруді және мәліметтерді өзгертуді, вирустар енгізуді болдырмауды қамтамасыз етеді.

Жалпы ақпаратты сақтаудың ортақ тәсілдерінің қажеттілігіне қарамастан, қазіргі кезде тіптен олардың өзі жеткіліксіз болып отыр. Вирустан сақтану үшін арнайы бағдарламалар қажет, және оларды тұрақты түрде қолдана бастау керек. Мұндай бағдарламаларды бірнеше түрлерге бөлуге болады:

- **детекторлар**;
- **докторлар** (фаг-бағдарламалар);
- **ревизорлар** (файлдардағы және дискінің жүйелік аумақтарындағы өзгерістерді бақылайтын бағдарламалар);
- **доктор-ревизорлар**;
- **сүзгі бағдарламалар (**вирустан сақтайтын резиденттік бағдарламалар**)**;
- **вакциналар (**иммунизаторлар**).**

Вирустың әсерін жоятын антивирустік бағдарламаларды негізгі үш топқа бөлуге болады:

▪файл мәліметтерінің бақылауға арналған олардың қосындыларын есте сақтауға негізделген бағдарламалар;

▪бағдарламаға немесе операциялық жүйеге вирус жұққан сәтте оларды анықтайтын резиденттік бағдарламалар;

▪вирустар жұқтырылғаннан кейін олардың бар екенін анықтайтын бағдарламалар.

Файлдағы мәліметтердің белгілі бір сипаттамаларын есте сақтайтын антивирустық бағдарламалардың негізгі жұмысы – сол файлдардың жаңа сипаттамаларын бұрын белгіленіп жазылып қойылған мәндерімен салыстыру. Егер файл ішіне вирус енсе, онда олар бір-біріне сай келмейді де, бағдарлама ол туралы экранға ескертпе хабар шығарады. Осы тәсілмен бұрын белгісіз жаңадан шыққан вирус түрін де анықтауға болады. Бірақ бұрын белгіленіп жазылып қойылған сипаттамаларды вирустан мұқият сақтау қажет. Ал кейде сол сипаттамалардың өзгеруі вирустың әсерінен емес, тексергеннен кейін өзіңіздің өзгертуіңізден де болуы ықтимал. Оның үстіне, сіз тексеру сипаттамаларын жазу кезінде компьютерде вирус жоқ екеніне сенімді күйде болуыңыз қажет, әйтпесе бұл тәсіл дұрыс нәтиже бере алмайды.

Сондай-ақ, бұл бағдарламалардың тағы бір кемшілігіне тексеруге көп уақыттың кетуі мен бақылау сипаттамаларының файл көлемін шектен тыс үлкейтетінін жатқызуға болады. Оған қоса, ол мәліметтерді көшіру немесе аттарын өзгерту қажет болса, тағы да сипаттамаларын өзгертіп жазу керек.

Детектор-бағдарламалар тек бұрыннан белгілі вирус түрлерінен ғана қорғай алады, жаңа вирусқа ол дәрменсіз болып келеді.

Доктор-бағдарламалар немесе "**фагтар**" вирус жұққан бағдарламалар мен дискілерді "вирус" әсерін алып тастау, яғни "жұлып алу" арқылы емдеп оларды бастапқы қалпына келтіреді.

Ревизор-бағдарламалар да алдымен бағдарламалар мен дискінің жүйелік аймағы туралы мәліметтерді есіне сақтап, содан соң оны кейінгісімен салыстыра отырып сәйкессіздікті анықтаса, оны дереу бағдарлама иесіне хабарлайды.

Доктор-ревизорлар – доктор-бағдарлама мен ревизорлар арасынан шыққан гибрид. Бұлар тек файлдағы өзгерістерді ғана анықтап қоймай, оларды автоматты түрде "емдеп" бастапқы қалыпты жағдайға түзеп келтіреді.

Сүзгі бағдарламалар – компьютердің оперативтік (жедел) жадында тұрақты (резиденттік) орналасады да, вирустардың зиянды әрекетіне әкелетін операцияны ұстап алып, бұл туралы жұмыс істеп отырған адамға дер кезінде хабарлап отырады. Одан әрі шешім қабылдау әр адамның өзіне байланысты болады.

Вакцина-бағдарламалар (иммунизаторлар) компьютердегі бағдарламалар жұмысына әсер етпей, оларды вирус "жұққан" сияқты етіп модификациялайды да, вирус әсерінен сақтайды, бірақ бұл бағдарламаларды пайдалану онша тиімді емес.

Ең көп тараған антивирус – Д.Лозиннскийдің **Aidstest** бағдарламасы. Ол әрбір жаңадан шыққан вирустан хабардар болып, соларға қарсы шара

қолдану жолдарын анықтап, үнемі өзгертіліп отырады. Бұл бағдарламаны пайдаланып компьютерді вирустан сақтау үшін жиі-жиі дискілерді (мысал с:) мынадай командамен тексеріп отыру керек: **Aidstest c:**

Ал егерде компьютерде вирус бар деген күмән болса, онда оны мына командамен емдеу қажет:

Aidstest c:\f

Тек бағдарлама файлдарды ғана емес, қалған мәліметтерді де түгел тексеру үшін мына команда орындалады:

Aidstest c:\f\g

Бұдан басқа И.Даниловтың қуатты полифаг-антивирустар тобына жататын Doctor Web бағдарламасы да жиі қолданылып жүр, оның бұрынғы нұсқаларын іске қосу үшін **Web c:\f** жолын пайдалану қажет немесе соңғы шыққан нұсқаларын **DrWeb** командалық жолы арқылы бағдарламалық ортаға кіріп, мәзір жүйесі бар терезеде қандай дискілері, қалай тексеретінімізді енгізу, оның бар мүмкіндігін (F1 пернесі көмекші мәлімет ала отырып) толық қолдана аламыз.

Бағдарлама-фильтрді қолдану.

Aidstest, Dr.Web, ADinf Cure Mobule бағдарламаларға қосымша бағдарлама – күзетші (фильтрлі) қолдану болып табылады, яғни компьютерлерге салынатын дискеттердің, енгізілетін файлдардың бәрін тексеріп тұратын арнайы фильтрі бар бағдарлама.

Компьютерлерге дискеттерді салғаннан кейін бірден сізге вирус кіргенін немесе кірмегенін хабарлап тұрады және сіздің ол вирусты емдеуіңізге болады. Егер оны білмей, дискета компьютерге вирус жұқтырғанда, кейін ол бүкіл компьютерді зақымдап құртуы мүмкін болар еді.

Сол үшін, Norton AntiVirus (Windows үшін) кешенінің NAVTSR.EXE бағдарламма – күзетшіні (фильтрді) қолдануға болады. Бұл бағдарламаны іске қосу үшін AUTOEXES.BAT файлына NAVTRS.EXE шақыру командасын енгізу керек. Файлдары бар Norton AntiVirus каталогы PATH командасын көрсету керек. Бұдан кейін NAVTRS.EXE бағдарламасы автоматты түрде белгілі бағдарламадағы файлдық вирустарды бақылап, қадағалап, тексеріп отырады.

NAVTRS.EXE бағдарлама режимдерін басқару үшін Norton AntiVirus (Windows үшін) іске қосып, Options түймесін басып және Auto-Protect Settings пунктін таңдау керек.

Norton AntiVirus (Windows үшін) – ескі бағдарлама болғанымен, ол вирустардың ең жаңа түрлерін анықтап, емдей алады: Symantec фирмасы әр ай сайын берілген база файлдарын жаңартып тұрады (VIRSCAN.DAT және VIRSCAN.INF файлдары), және осы файлдарды қолданушыларға Интернет арқылы тегін көшіріп алуға болады. Адресі: WWW_сервер WWW.SYMANTEC.COM.

Вирустардың жаңа түрлері күнбе-күн пайда болып жатыр, сондықтан антивирустық бағдарламалардың да тексеру-емдеу қабілеттері жоғары соңғы шыққандарын қолданған дұрыс.

Компьютерге вирус енгенін сезсеңіз мына ережелерді мұқият орындаған абзал:

1. Вирустың зиянды әрекеттерін әрі жалғастырмас үшін компьютерді бірден өшіру қажет.
2. Егер компьютерде "жұққан" вирусты емдей алатын детектор-бағдарламаларыңыз болса, дискілерді тексеру мақсатында соларды дереу іске қосыңыз.
3. Біртіндеп вирус жұғуы мүмкін болған барлық дискілерді тексеріп шығу қажет.
4. Егер дискідегі барлық файлдарыңыздың архивтік көшірмелері болса онда дискіні қайта форматтап, мәліметтеріңізді бұрынғы қалпына келтіруге тырысыңыз.

Енді компьютерге вирус жұқтыру мүмкіндігін азайтатын және жұққан жағдайда оның зиянкесті әрекеттерін барынша болдырмайтын шараларды қарастырайық, оларды бірнеше топтарға жіктеуге болады:

1. Ақпараттың жиі пайдалануын шектеу және оның көшірмесін сақтау.
2. Сырттан келген мәліметтерді мұқият тексеруден өткізу.
3. Вирустан "емдеу аспаптарын" дайындап қою.
4. Белгілі бір уақыт сайын компьютерді вирусқа тексеріп отыру.

3 АҚПАРАТТЫ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ

Криптография – ақпараттың, деректердің мағынасын құпия түрде қалай сақтау керектігін оқытатын ғылым.

Криптология – ақпаратты өзгеріске келтіре отырып, оны қорғау мәселесімен айналысатын ғылым.

Криптоанализ – ешқандай да кілтсіз ақпараттың шифрін ашу мүмкіндіктерін зерттейтін ғылым.

3.1 Ақпаратты қорғаудың математикалық негіздері

1. Санақ жүйелері

Санақ жүйелері - сандарды цифрлық белгілермен жазу ережелері мен тәсілдерінің жиынтығы. Барлық санақ жүйелері позициялық, позициялық емес болып бөлінеді.

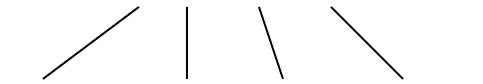
Позициялық емес санақ жүйесінде символдың мәні оның сандағы тұрған орнына тәуелді болмайды. Мысалы: римдік санақ жүйесі

I	1	L	50	M	1000
V	5	G	100		
X	10	D	500		

88_{10} ⟶ LXXXVIII 52_{10} ⟶ LII
91_{10} ⟶ LXXXXI

Позициялық санақ жүйелерінде цифр мәні оның сандағы тұрған орнымен анықталады:

Мысалы: 3 2 4 5



Кез-келген позициялық санақ жүйесі негізбен сипатталады - яғни берілген жүйедегі цифрларды бейнелеу үшін пайдаланылатын белгілер немесе символдар санымен сипатталады. Позициялық санақ жүйелері үшін келесі өрнек орындалады.

$$A_{(p)}=a_{n-1}P^{n-1}+\ldots+a_1P^1+a_0P^0+a_{-1}P^{-1}+\ldots+a_{-m}P^{-m}$$

мұндағы, P- санақ жүйесінің негізі;

A_p – кез келген сан;

a_i – санақ жүйесінің цифры;

m, n – бүтін және еселі разрядтар саны.

Мысалы: $86{,}54_{10}=8*10^1+6*10^0+5*10^{-1}+4*10^{-2}$

Ақпаратты компьютерде бейнелеу кезінде 0 және 1 - лерден тұратын кодтар қолданылады. Санақ жүйелері екілік, сегіздік, ондық, он алтылық болып бөлінеді.

Санақ жүйелеріндегі сандардың сәйкес келуі:

10-дық	16-лық	8-дік	2-лік
0	0	0	0
1	1	1	1
2	2	2	10
3	3	3	11
4	4	4	100
5	5	5	101
6	6	6	110
7	7	7	111
8	8	10	1000
9	9	11	1001
10	A	12	1010
11	B	13	1011
12	C	14	1100
13	Д	15	1101
14	E	16	1110
15	F	17	1111

Санақ жүйелерінің бірінен- біріне өтуге болады.

№1.

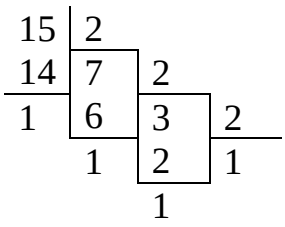
$$(123_{10})_2=11011011$$

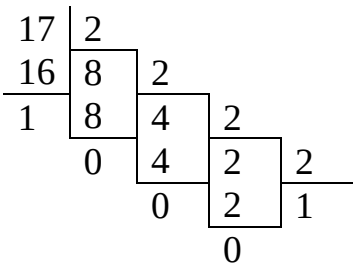
$$1111011=1\cdot 2^6+1\cdot 2^5+1\cdot 2^4+1\cdot 2^3+1\cdot 2^1+1\cdot 2^0=123$$

123	2					
122	61	2				
1	60	30	2			
	1	30	15	2		
		0	14	7	2	
			1	6	3	2
				1	2	1
					1	

Қосу	Айырма	Көбейту
0+0=0	0-0=0	0*0=0
0+1=1	1-0=1	0*1=0
1+0=1	1-1=0	1*0=0
1+1=10	10-1=1	1*1=1
1+1+1=11		

Мысалы: 1) $15_{10}+17_{10}=32_{10}$





$$\overset{5\,4\,3\,2\,1\,0}{100000_2} = 0\cdot 2^0 + 0\cdot 2^1 + 0\cdot 2^2 + 0\cdot 2^3 + 0\cdot 2^4 + 1\cdot 2^5 = 32_{10}$$

2) $x_1=10110_2$

$x_2=1011_2$ $\quad$ x_1*x_2-?

		*	1	0	1	1	0
				1	0	1	1
			1	0	1	1	0
		1	0	1	1	0	
	0	0	0	0	0		
1	0	1	1	0			
1	1	1	1	0	0	1	0

$$\overset{4\,3\,2\,1\,0}{10110} = 1\cdot 2^1 + 1\cdot 2^2 + 1\cdot 2^4 = 22_{10}$$

$$\overset{3\,2\,1\,0}{1011} = 1\cdot 2^0 + 1\cdot 2^1 + 1\cdot 2^3 = 1+2+8 = 11_{10}$$

$$\overset{7\,6\,5\,4\,3\,2\,1\,0}{11110010_2} = 1\cdot 2^1 + 1\cdot 2^4 + 1\cdot 2^5 + 1\cdot 2^6 + 1\cdot 2^7 = 2+16+32+64+128 = 242$$

3) $x_1=1111101_2=125_{10}$

$x_2=101_2=5_{10}$

-	1111101	101
	101	$11001_2=1\cdot 2^4+1\cdot 2^3+2^0=25_{10}$
	101	
	101	
	000101	
	101	
	000	

Екілік жүйеден сегіздікке өту үшін солдан оңға қарай үш-үштен топтап бөліп, сәйкестік кестесіндегі мәндерді орнатамыз.

Мысалы: $11011001_2=11\ \ 011\ \ 001_2=331_8$

Екілік жүйеден 16-қа өту үшін 4 саннан топтаймыз.

1 1000 1101 $1001_2 = 18$ Д 9_{16}

2. Хемминг кодын анықтау

Мысалы:

1) 100110- коды берілген болсын

$$\underset{6\ 5\ 4\ 3\ 2\ 1}{100110}$$ -разряд саны к=6

$L=\log_2 k=\log_2 6=\log_2 2^3=3\log_2 2=3\cdot 1=3$; - разряд саны ең жақын үлкен санға дейін дөңгеленеді.

Разрядты түрде мәні 1-ге тең шифрланушы разрядтар номерлерін қосамыз:

\+ 010
\+ 011
110
111

Алынған нәтижені кері ауыстырамыз, яғни 111 = 000 – бұл қосымша код, яғни негізгі кодпен бірге қосымша код беріледі.

10011000- Хемминг коды.

2) 11101- коды берілген болсын

x=5 $l=\log_2 k=\log_2 2^3=3$

001
011
100
101

011 100

11101100- Хемминг коды.

3.2 Криптография элементтері

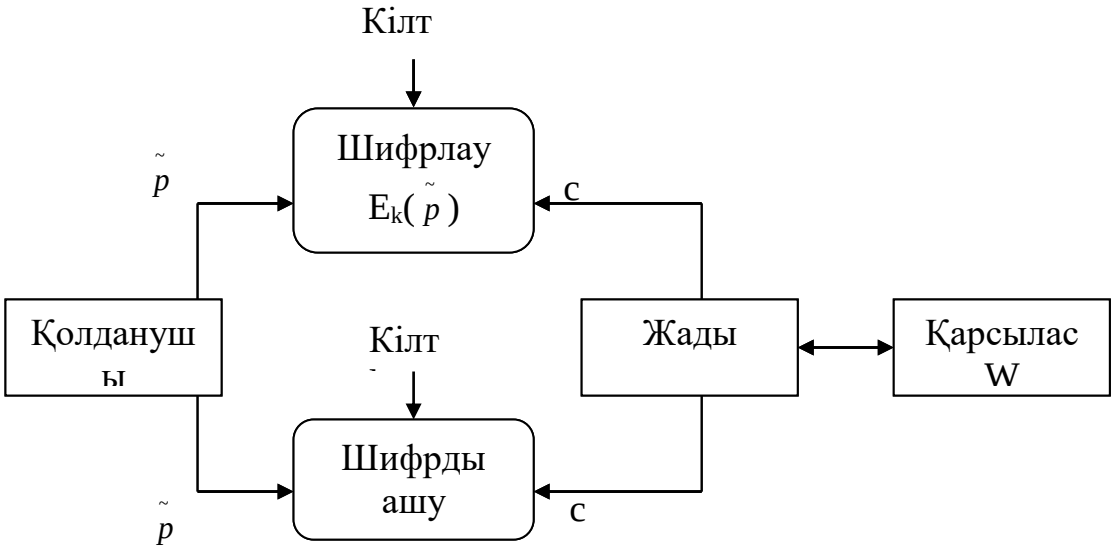
Ақпаратты қорғау мәселесін шешуде келесілерге әкеліп соғады:

- компьютерлік техникамен өңделетін, сақталатын және жиналатын ақпараттар көлемінің үлкеюіне;
- түрлі қолданыстағы және мақсаттағы ақпараттарды бірегей берілгендер қорына жинақтауға;
- компьютерлік жүйенің ресурстарына мүмкіндігі бар қолданушылар тобын кеңейтуге;
- компьютерлік жүйенің қызмет режимінің қиындауына;

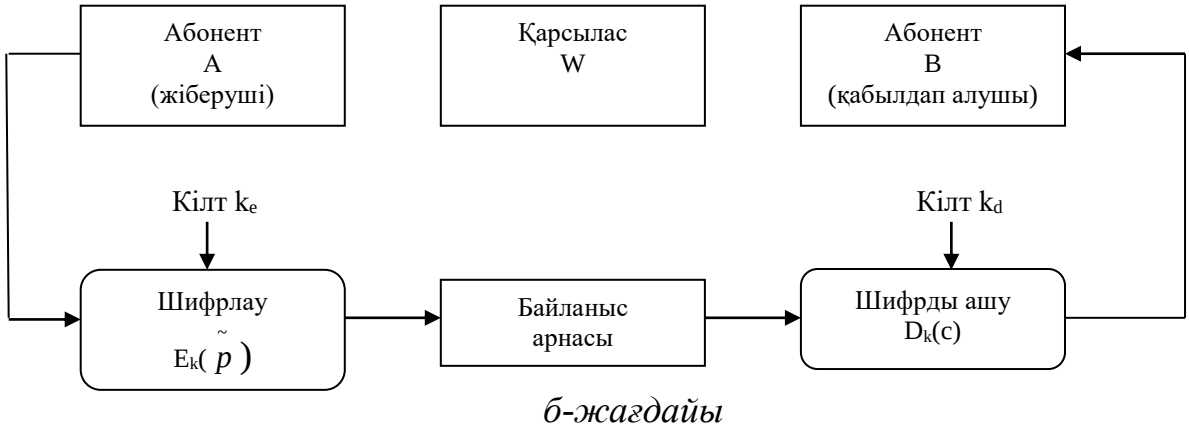
- шетелдік бағдарламамен және техникамен қамтамасыздандыруға;
- желілік технологияны таратуға, локальдық желіні глобальдық желіге біріктіруге;
- берілгендерді өткізу үшін жаңа технологияларды пайдалануға;
- қауіпсіздіктің ең төменгі дәрежесіне жауап бере алмайтын бағдарламалық қамтамасыздандырудың көбеюі;
- берілгендерді өңдеу барысында қолданушыны шеттету;
- бағдарламалаудың түрлі стильдерінің болуымен қолданыстағы бағдарламалық өнімнің сапасын анықтауды қиындатуы және т.б;

Ақпаратты шифрлау әдістері

Төмендегі суретте классикалық криптографияның негізгі обьекттері қарастырылған. Мұндағы А және В – заңды қолданушылар, W- қарсылас немесе криптоаналитик. Суреттегі *а* жағдайын дербес ретінде қарастыра отырып *б* жағдайын В=А болғанда ары қарай тек осы жағдай қарастырылады.



а-жағдайы



б-жағдайы

Сурет 10 Криптоқорғаныс: *а*-сақтау кезінде; *б*-байланыс арнасы арқылы ақпаратты өткізу кезінде

Шифрлау (encryption) және шифрды ашу (decryption) процедурасын келесі түрде көрсетуге болады:

$$c = E_k(\tilde{p});$$

$$\tilde{p} = D_k(c)$$

мұндағы $\tilde{p}$ және c – ашық (plaintext) және шифрланған (ciphertext) мәтіндер; k_e және k_d – шифрлау және шифрды қайта ашу кілттері; E_k және D_k - k_e кілті бойынша шифрлау және k_d кілті бойынша шифрды қайта ашу функциясы және кез-келген ашық мәтінді $\tilde{p}$ үшін $D_k(E_k(\tilde{p})) = \tilde{p}$ орындалады.

Келесі суретте ақпаратты шифрлаудың класификациялық әдістері келтірілген. Шифрлау алгоритмінің екі түрі бар: симметриялық (құпия кілтпен) және ассиметриялық (ашық кілтпен). Бірінші жағдайда шифрды қайта ашу кілті шифрлау кілтімен сәйкес болады, яғни $k_e=k_d=k$, немесе шифрлау кілтін жақсы білу шифрды қайта ашу кілтін табуға пайдасы тиеді. Ассиметриялық алгоритмдерде мұндай мүмкіндік жоқ: шифрлау және шифрды қайта ашу үшін әртүрлі кілт қолданылады және бір кілтті білгенмен екінші кілтті білуге немесе есептеп табуға ешқандай мүмкіндік жоқ. Сондықтан егер қаблдап алушы В шифрды қайта ашу кілтін $k_{dB}=k_B^{(secret)}$ құпия ұстаса шифрлау кілтін $k_{eB}=k_B^{(public)}$ ашық түрде ұстауға болады.

Сурет 11 Ақпаратты шифрлау әдістерінің классификациясы

Шифрлау процесінде ақпарат бір биттен жүз битке дейінгі өлшемдерге бөлінеді. Ереже бойынша топтық шифр ашық және жабық мәтіндермен жұмыс жасайтын болса, блоктық шифр белгіленген ұзындықтағы шифрлармен жұмыс жасайды. Бұл екі әдістің арасындағы ең басты мәселе блоктық шифрлауда барлық бөлікті шифрлау үшін тек бір кілт қолданылады, ал топтық шифрлауда әр бөліктің өзіндік бір өлшемді кілті болады.

Топтық шифрлаудың артықшылығына шифрлаудың жоғары жылдамдығын жатқызуға болады, ол оның берілгендерді шифрлауды қолдану аясын анықтап, мысалы дыбыстық немесе бейне ақпараттарды тұтынушыға оперативті түрде жеткізіп береді.

Шифрлау әдісі екіге бөлінеді, блоктық және ағымдық шифрлар. Кілтке байланысты оларды симметриялық және ассиметриялық криптожүйеге бөлуге болады.

Вижинер шифрлары

Ең танымал ретінде Вижинер шифрлары болып саналады. Оның ерекшелігі ашық мәтіндегі символдарды сәйкес шифромәтіндегі алфавиттің символдарымен ауыстырады. Вижинердің бір алфавиттік және көп алфавиттік деген екі түрі бар. Бір алфавиттік шифрды ашу негізі жеке әріптердің немесе олардың қосындысының пайда болу жиілігін есептеуге бағытталған. Көп алфавиттік шифрлық ауыстыру мысалына Вижинер жүйесін келтіруге болады. Шифрлау тәсілі *n x n* өлшемді алфавиттік кесте бойынша жүзеге асырылады. Төмендегі суретте Вижинер кестесі келтірілген. Бірінші қатарда алфавиттің барлық символы бар. Әр келесі қатар алфавиттегі әріптерді оң жаққа жылжытқандағы екінші әріптерінен басталып отырады.

Алдымен кілт немесе кілттік сөз таңдалып алынады. Одан кейін шифрлау әдісі келесі түрде орындалады. Ақпараттың әр әрпінің астына тізбектелген түрде кілттің әріптері жазылады, егер кілт ақпаратт сөзінің ұзындығынан қысқа болса, онда ол бірнеше рет қайталанып жазылады. Шифрмәтіннің әр әрпі ашық мәтіннің әріптерін анықтайтын кесте бағанының, кілт әріптерін анықтайтын қатар қиылысында орналасады. Мысалы:

МЕН УНИВЕРСИТЕТТЕ ОТЫРМЫН НКТ ДИПЛОМ ЖАЗУДАМЫН НКТ сөзін АСЕЛАЙЫМ кілті арқылы шифрлайтын болсақ, онда ақпараттың астына кілттік сөздің әріптерін жазып шығамыз:

МЕН УНИВЕРСИТЕТТЕ ОТЫРМЫН НКТ ДИПЛОМ ЖАЗУДАМЫН НКТ
АСЕЛАЙЫМАСЕЛАЙЫМАСЕЛАЙЫМАСЕЛАЙЫМАСЕЛАЙЫМАСЕЛА

Шифрлау нәтижесінде төмендегідей шифрмәтінді аламыз:

МЦТКУЦГОНЩЬУЮТ_АХРАЕСЖГФЖЬИЖПЫБЖНМЯСГЛНЬМЙЦЖЩ

Вижинер әдісі полиалфавиттік шифрлау әдісі болып табылады. Оны математикалық жолмен беретін болсақ:

m Є Z_n – белгілі сан болсын.

Анықтама:

P = C = K = $(Z_n)^m$. K = (K_1, K_2, …, K_m) кілті үшін келесілерді анықтаймыз:

$E_x(x_1, x_2,…, x_m) = (x_1 + K_1, x_2 + K_2, …, x_m + K_m)$

$D_k(y_1, y_2,…, y_m) = (y_1 - K_1, y_2 - K_2, …, y_m - K_m)$

Барлық операциялар Z_n арқылы орындалады. Мүмкін болатын кілттер саны 256^m.

Вижинер әдісімен шифрлау процесін келесі түрде өрнектеуге болады:

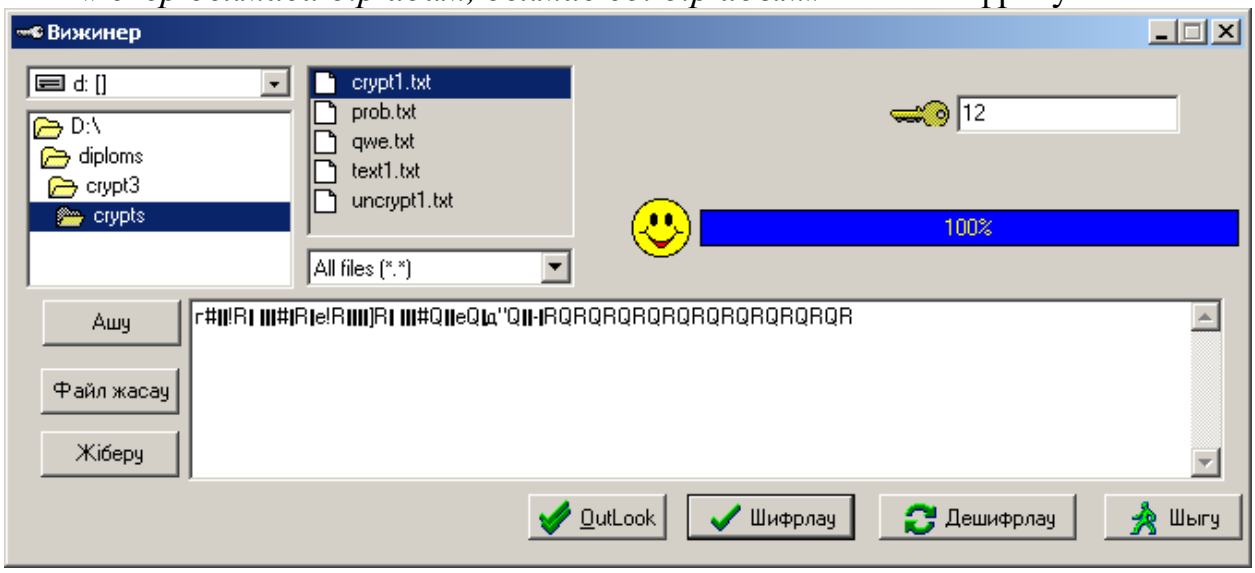
Ашық типті файл болсын, яғни құрамында кез-келген ақпарат болатын мәтіндік файл. Бұл файл Вижинер әдісі алгоритмі бойынша шифрланады. Нәтижесінде шифр мәтінді файл құрылады.

Шифрды қайта ашу процесі келесі түрде болады:

Шифрланған мәтіндік файлы Вижинер әдісінің шифрды қайта ашу алгоритмі бойынша ашылады. Нәтижесінде ашық мәтінді файл құрылады.

Сурет 12 Бағдарламаның бас формасы

«Іскер болмаса бір адам, болмас еді бір адым» сөзін шифрлау нәтижесі:



Сурет 13 Вижинер терезесі

Шифрлау коды:

```
buf := Length(trim(Edit1.Text));
s := trim(Edit1.Text);
 AssignFile(F,'crypts\text1.txt');
    Reset(F);
 AssignFile(G,'crypts\crypt1.txt');
  rewrite(G);
 While not EoF(F) do
 begin //2
 for i:=1 to buf do
 begin
 if eof(f) then exit;
 read(f,c);
 p := chr((ord(c) + ord(s[i])) mod 256);
 write(g,p);
 end;
 end;
 closefile(f);
  closefile(g);
```

Дешифрлау коды:

```
k := Length(trim(Edit1.Text));
s := trim(Edit1.Text);
if k<1 then exit;
 AssignFile(F,'crypts\crypt1.txt');
    Reset(F);
 AssignFile(G,'crypts\uncrypt1.txt');
  rewrite(G);
```

```
While not EoF(F) do
begin //2
for i:=1 to k do
begin
if eof(f) then exit;
read(f,c);
p := chr((ord(c) - ord(s[i])) mod 256);
write(g,p);
end;
end;
closefile(f);
 closefile(g);
```

Орын ауыстыру арқылы шифрлау

Орын ауыстыру арқылы шифрлау немесе транспозициялау дегеніміз ағымдағы мәтіннің тек символдардың немесе элементтердің ретін өзгертеді. Мұндай шифрлаудың классикалық мысалы ретінде Кардано тор жүйесін қарастыруға болады. Парақ бетіне жазғанда оның кейбір бөліктерін бос қалдырып отырады. Шифрлау кезінде ақпараттың әріптері осы бос бөліктерге толтырылады. Шифрды ашу үшін ақпарат қажетті өлшемдегі диаграммаға жазылып, оның үстіне торды қойса ашық мәтіннің әріптері көрініп тұрады.

Торды екі түрлі әдіспен қолдануға болады. Бірінші жағдайда шифрланатын мәтін тек ағымдағы ақпараттың әріптерінен ғана тұрады. Торды қатарынан түрлі жағадайда қолданғанда астында жатқан парақтағы әр тор бос болмауы керек болатындай етіп жасалынады. Мұндай торға мысал ретінде бұрылатын торды көрсетуге болады (сурет 14). Егер мұндай торды қатарынан 90^0 бұратын болсақ ашық торлардың барлығын толтырғаннан кейін тор өзінің ағымдық орнына қайтып келгеннен кейін барлық тор бөліктері толтырылған болып шығады. Тор бөліктеріндегі сандар торды дайындауды оңайлатады. Әр бөліктен бірдей саны бар тор бөліктерінен тек біреуі ғана кесіп алынып отырады. Екінші әдіс, стеганографиялық әдісі құпия ақпаратты беру фактісін жасыруға мүмкіндік береді. Бұл жағдайда парақ бетінің тек бір бөлігі ғана толтырылып, қалған бөлігі жалған ақпаратпен толтырылады.

Кесте бойынша күрделендірілген орын ауыстыруды қарастырайық. Бұл шифрлау әдісін іс-жүзіне асыру кесте мысалы төмендегі суретте көрсетілген (сурет 15). Кесте 6х6 өлшемді матрица түрінде берілген. Оған қатар бойымен ақпарат жазылып шығады. Ақпаратты баған бойымен кілт сандар тізбегі бойынша оқығанда шифрмәтінді аламыз. Мұның қиындығы кестенің кейбір ұяшықтары қолданылмайды.

1	*2*	*3*	*4*	*5*	*1*
5	1	2	3	1	2
4	3	1	1	2	3
3	2	1	1	3	4
2	1	3	2	1	5
1	5	4	3	2	1

Сурет 14 Бұрылатын тор

Кілт					
2	**4**	**0**	**3**	**5**	**1**
К	І		Т	А	П
Х	1	Х	А	Н	А
4	*Д*	А		О	Т
3	Ы	1	Р	Ғ	А
Н		Ж	О	1	Қ
П	5	4	Ы	Н	1

Сурет 15 Кесте бойынша күрделендірілген орын ауыстыру әдісімен шифрлау

КІТАПХАНАДА ОТЫРҒАН ЖОҚПЫН сөзін шифрлайтын болсақ, онда келесі шифрмәтінді аламыз:

ІХАПАТАҚКХНПТА РОЫІДЫ АНОҒН

Шифрды ашу үшін шифрмәтіннің әріптерін кілт сандарының тізбегі бойынша баған бойымен жазып шығады да, одан кейін мәтін қатар бойымен оқылады.

Математикалық жолмен жазатын болсақ, онда $P=C=Z_nK$ n-символдарынан тұратын барлық мүмкін орын ауыстырулардан тұратын болсын. Мұндағы n=0,1,2,... n-1.

$\pi \in K$ әр орын ауыстыруы үшін, $e_\pi(x) = \pi(x)$ және $d_\pi(y) = \pi^{-1}(y)$ анықтаймыз. Мұндағы π^{-1} – кері орын ауыстыру. Бұл әдісте мүмкін болатын кілттер саны **n!.** Ал біздің жағдайда, мен бағдарламада ASCII код символдарын қолданғандықтан мүмкін болатын кілттер саны 256!. ($8{,}6*10^{506}$ саны аралас әдісімен ашу үшін өте үлкен сан және мүмкін емес).

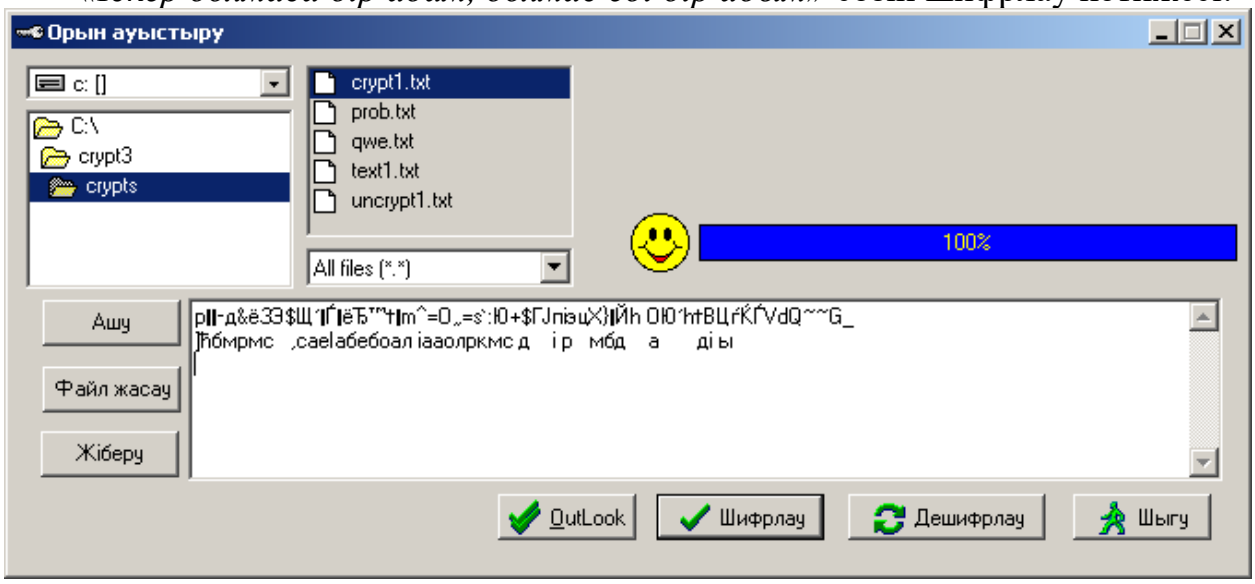
Орын ауыстыру әдісімен шифрлау процесін келесі түрде өрнектеуге болады:

Ашық типті файл болсын, яғни құрамында кез-келген ақпарат болатын мәтіндік файл. Бұл файл орын ауыстыру әдісі алгоритмі бойынша шифрланады. Нәтижесінде шифр мәтінді файл құрылады.

Шифрды қайта ашу процесі келесі түрде болады:

Шифрланған мәтіндік файлы ауыстыру әдісінің шифрды қайта ашу алгоритмі бойынша ашылады. Нәтижесінде ашық мәтінді файл құрылады.

«Іскер болмаса бір адам, болмас еді бір адым» сөзін шифрлау нәтижесі:



Сурет 16 Орын ауыстыру терезесі

Шифрлау коды:

```
 AssignFile(F,'crypts\text1.txt');
      Reset(F);
AssignFile(G,'crypts\crypt1.txt');
  rewrite(G);
  k := (FileSize(F) mod 32);
  if k<>0 Then
  for i:=1 to 32-k do
```

```
  begin //2
  seek(F,FileSize(F));
  c := chr(32);
  Write(f,c);
  end; //2
  CloseFile(f);
   randomize;
For i:=1 to 64 do
 s := s + chr(random(255));
 Reset(F);
For i:=1 to 64 do
Write(G,s[i]);
While not EoF(F) do
begin //3
  str := '';
 For i:=1 to 32 do
 begin //4
 If EoF(F) Then Exit;
 Read(f,c);
 Str := str + c;
 end; //4
for i:=1 to 63 do
 begin //5
 m := ord(s[i+1]) mod 32;
 n := ord(s[i]) mod 32;
 if n>m Then
   begin  //6
   buf := m;
   m := n;
   n := buf;
 end; //6
 str := copy(str,m+1,32-m) + copy(str,n+1,m-n) + copy(str,1,n);
    end;//5
 for i:=1 to Length(str) do
 write(g,str[i]);
  end; //4
   CloseFile(F);
     CloseFile(G);
image1.Picture.LoadFromFile('c:\crypt3\ico\face03.ico');
```

Дешифрлау коды:

```
AssignFile(F,'crypts\crypt1.txt');
    Reset(F);
AssignFile(G,'crypts\uncrypt1.txt');
  rewrite(G);
```

```
s := '';
for i:=1 to 64 do
begin //2
read(f,c);
s := s + c;
  end; //2
 while not EoF(f) do
  begin //3
  str := '';
for i:=1 to 32 do
  begin //4
  if eof(f) then exit;
  read(f,c);
  str := str + c;
    end; //4
  for i:=length(s) downto 2 do
  begin //5
  n := ord(s[i-1]) mod 32;
  m := ord(s[i]) mod 32;
  if n>m then
  begin //6
  buf := m;
  m := n;
  n := buf;
  end; //6
  str := copy(str,32-n+1,n) + copy(str,32-m+1,m-n) + copy(str,1,32-m);
  end; //5
for i:=1 to 32 do
write(g,str[i]);
  end; //3
   CloseFile(F);
     CloseFile(G);
```

Ауыстыру шифрлары

Ауыстыру шифрлары модульдік арифметикаға негізделген.

Анықтама:

P=C=K=Z_m болсын делік. K $(0 \le K \le m)$ үшін e_k шифрлау ережесін және d_k шифрды қайта ашу ережесін анықтаймыз.

Мұндағы:

$e_k(x) = x + K \bmod m$

және

$d_k(y) = y - K \bmod m$

$(x,y \in Z_m)$

Ауыстыру әдісі қарапайым шифрлау әдісі және оны компьютерде бағдарламалық жолмен оңай көрсетуге болады. Бағдарламаны іс-жүзіне асыру үшін ASCII код символдары қолданылды. Сондықтан бұл әдіс 256 мүмкін болатын кілті бар.

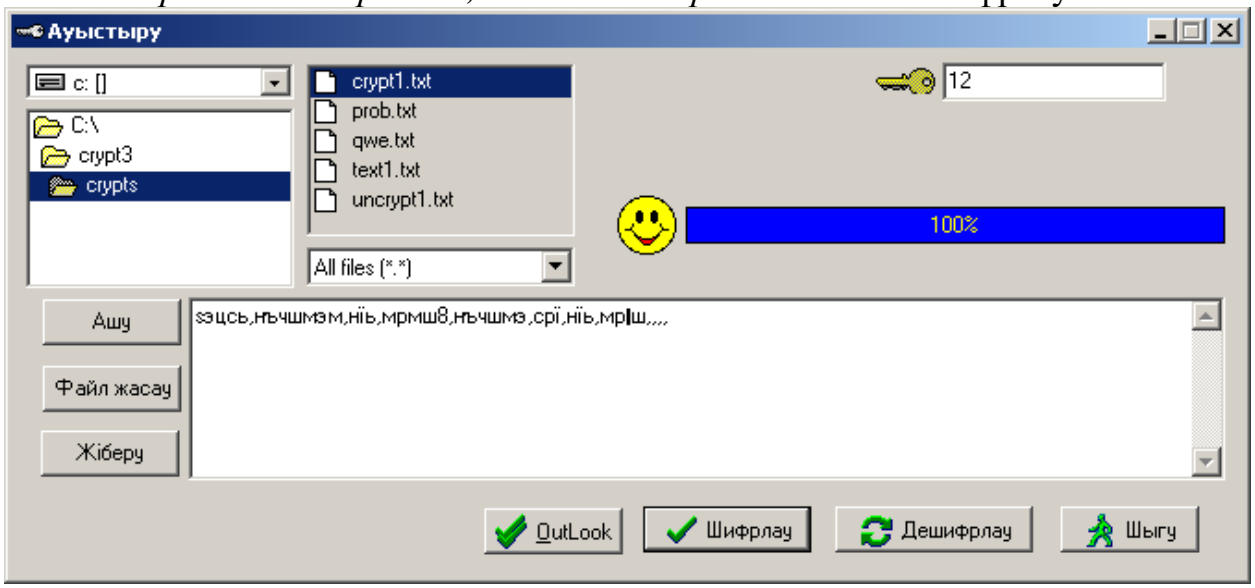
Ауыстыру әдісі үшін шифрлау процесін келесі түрде қарастыруға болады:

Кез-келген типтегі ашық файл болсын, яғни құрамында кез-келген ақпарат болатын мәтіндік файл. Бұл файл ауыстыру әдісі алгоритмі бойынша шифрланады. Нәтижесінде шифр мәтінді файл құрылады.

Шифрды қайта ашу процесі келесі түрде болады:

Шифрланған мәтіндік файлды аламыз, және бұл файл ауыстыру әдісінің шифрды қайта ашу алгоритмі бойынша ашылады. Нәтижесінде ашық мәтінді файл құрылады.

«Іскер болмаса бір адам, болмас еді бір адым» сөзін шифрлау нәтижесі:



Сурет 17 Ауыстыру терезесі

Шифрлау коды:

```
s := Edit1.Text;
If s = '' Then
  ShowMessage('Àëäûìåí ê³ëòò³ åíã³ç !!!') else
   k := StrToInt(s);
  AssignFile(F,'c:\crypt3\crypts\text1.txt');
        Reset(F);
 AssignFile(G,'c:\crypt3\crypts\crypt1.txt');
   rewrite(G);
   Seek(F,0);
     Seek(G,0);
   While not EoF(f) do
```

```
  begin //3
  read(f,c);
 p := chr((ord(c)+k) mod 256);
  Write(G,p);
   end; // 3
image1.Picture.LoadFromFile('c:\crypt3\ico\face03.ico');
   CloseFile(F);
     CloseFile(G);
```

Дешифрлау коды:

```
k := StrToInt(Edit1.Text);
 AssignFile(F,'crypts\crypt1.txt');
    Reset(F);
 AssignFile(G,'crypts\uncrypt1.txt');
  rewrite(G);
   Seek(F,0);
    Seek(G,0);
  While not EoF(f) do
  begin //2
  read(f,c);
 p := chr((ord(c) - k) mod 256);
  Write(G,p);
   end; //2
   CloseFile(F);
     CloseFile(G);
```

Affine шифры

Affine шифры үшін:

P=C=K=Z_n және K = {(a,b) Є Z_n x Z_n:ҮОБ (a,n) = 1} болсын делік. К = (a,b) Є K үшін e_k шифрлау ережесін және d_k шифрды қайта ашу ережесін анықтаймыз.

Мұндағы:

$e_k(x) = ax + b \bmod n$

және

$d_k(y) = a^{-1}(y - b) \bmod n$

(x,y Є Z_n)

Теорема.

$a \cdot x \equiv b \pmod m$ – ң x Є Z_m барлық b Є Z_m егер және тек егер ҮОБ(a,m) = 1 болса өзіндік шешімі бар.

Анықтама:

$a \geq 1$ және $m \geq 2$ $a,m \in Z$ деп аламыз. Егер УОБ(a,m) = 1, болса, онда a және m шамалас қарапайым деп айтуға болады. m санына шамалас қарапайым Z_m бүтін сандары φ(m). (бұл функция Эйлердің фи-функциясы деп аталады).

Теорема:

Егер $m = \prod_{i=1}^{n} p_i^{e_i}$ болса, онда $\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1})$

Осы теореманы қолдана отырып шамалас қарапайым сандар санын анықтауға болады. Ол менің бағдарлама құруда осы әдісті іс-жүзіне асыруыма көмектеседі, мұндағы m = 256 (ASCII).

$m = 256 = 2^8$ демек $\varphi(m) = 2^8 - 2^7 = 128$.

Яғни, мүмкін кілттер саны 128*256 = 32768.

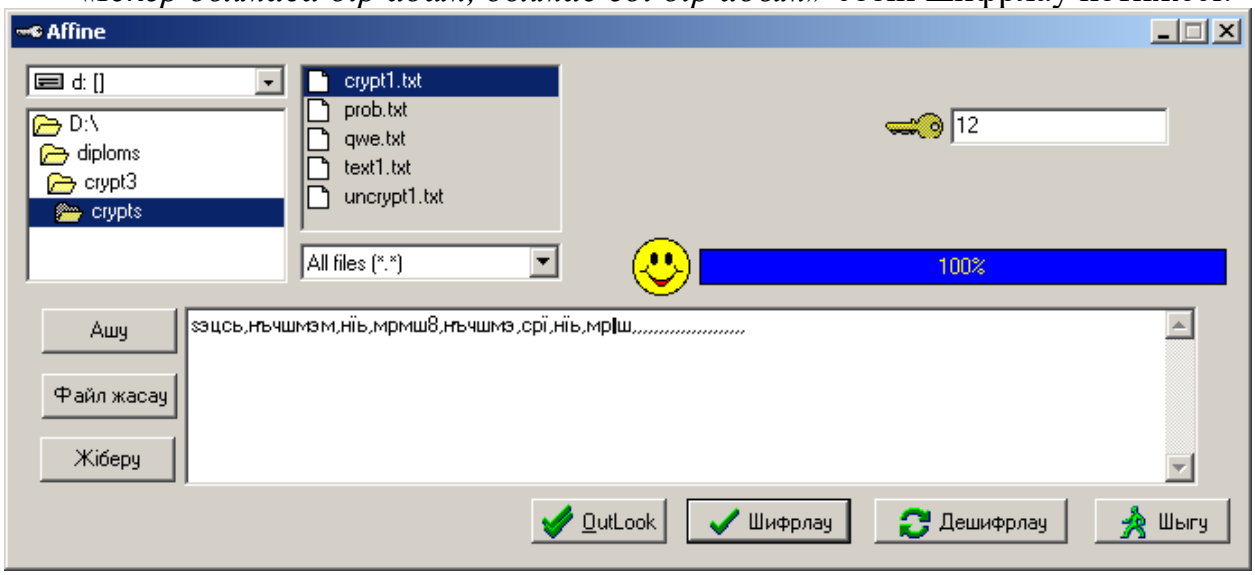
Affine әдісі үшін шифрлау процесін келесі түрде қарастыруға болады:

Ашық типтегі кез-келген файл болсын, яғни құрамында кез-келген ақпарат болатын мәтіндік файл. Бұл файл Affine әдісінің алгоритмі бойынша шифрланады. Нәтижесінде шифр мәтінді файл құрылады.

Шифрды қайта ашу процесі келесі түрде болады:

Шифрланған мәтіндік файлды бағдарлама арқылы көрсетіп және бұл файлды Affine әдісінің шифрды қайта ашу алгоритмі бойынша ашамыз. Нәтижесінде ашық мәтінді файл құрылады.

«Іскер болмаса бір адам, болмас еді бір адым» сөзін шифрлау нәтижесі:



Сурет 18 Affine терезесі

Шифрлау коды:

k := StrToInt(Edit1.Text);

s := Edit2.Text;

```
AssignFile(F,'crypts\text1.txt');
    Reset(F);
AssignFile(G,'crypts\crypt1.txt');
  rewrite(G);
 While not EoF(F) do
begin //2
read(f,c);
m := ord(c);
n := (strtoint(trim(s))* m + k) mod 256;
c := chr(n);
write(g,c);
 end; //2
    CloseFile(F);
     CloseFile(G);
```

Дешифрлау коды:

```
k := StrToInt(Edit1.Text);
  s := edit2.Text;
  //copy(edit2.Text, length(edit2.Text)-2, 3);
 // s := copy(trim(Edit2.Text), 1, 3);
  buf := StrToInt(trim(s));
  if k<1 then exit;
  begin //2
 AssignFile(F,'crypts\crypt1.txt');
    Reset(F);
 AssignFile(G,'crypts\uncrypt1.txt');
   rewrite(G);
while not EoF(f) do
begin //3
read(f,c);
m := ord(c);
n := (buf * (m - k)) mod 256;
c := chr(n);
write(g,c);
end; //3
 CloseFile(F);
     CloseFile(G);
```

RSA шифры

Бірінші болып және ең көптараған ашық кілтті криптографиялық жүйе 1978 жылы RSA деп аталатын жүйе ретінде ұсынылған. RSA жүйесінің атауы жүйені құрушылардың авторларының бас әріптерінен алынған, олар Р. Ривеста, А. Шамира, Л. Адлеман. Ол өте көп қиын бүтін сандарды қарапайым көбейткіштерге негізделген. Көбейту нәтижесінде шифрлау ашық кілтті элементі қолданыла алады. Ағымдық қарапайым сандар шифрды қайта

ашу үшін қолданылады, бірақ оны орнына қайта келтіру мәселесі криптоаналитиктердің шифрды бұзу жұмысына қарсы тұрып келеді. Осылайша біржақты құпия функцияны құруға болады. Мысал ретінде авторлардың шифрлау принципін көрсетейік.

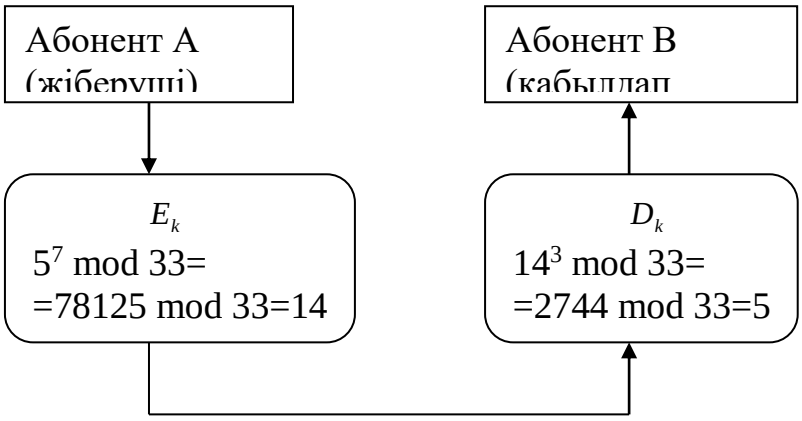
- Шифрлау ашық кілті: n және e саны
- Шифрды ашу жабық кілті: p,q және d саны
- $\tilde{p}$ ақпаратын шифрлау алгоритмі:

$$E_k(\tilde{p}) = \tilde{p}^{\,e} \pmod{n} = c.$$

- c жабық ақпаратын қайта ашу алгоритмі:

$$D_k(c) = c^{\,d} \pmod{n} = \tilde{p}.$$

D_k қайта ашу алгоритмін табудың жалғыз әдісі, және e сандары белгілі болғанда, n санын қарапайым көбейткіштерге көбейтіп, p және q сандарының мәнін, сонымен бірге d санының мәнін табу керек. p және q сандарының разрядтығын дұрыс таңдау есептің n факторизациясын іс-жүзінде мүмкін емес етеді (RSA авторлары бірінші 40-разрядтан төмен емес ондық сандарды қолдануды ұсынған). Келтірілген схема бойынша шифрлау келесі суретте көрсетілген (сурет 19), мұндағы e=7, d=3 және n=33.



Сурет 19 RSA схемасы бойынша шифрлау мысалы

RSA авторлары өздерінің жүйелерінің жұмыс істеу принциптерін жазғанда мысал үшін төмендегі сөзді таңдап алды:

ITS ALL GREEC TO ME (Мен үшін мұның бәрі түсініксіз)

Бұл мәтінді үлкен санға айналдыру үшін сөздің арасындағы бос аралықты 0, A әрпін – 1, B әрпін – 2, C әрпін – 3, ... , Z әрпін – 26 деп кодтап алды. Әр символды көрсету үшін әрқайсысына 5 екілік разряд бөлді. Нәтижесінде келтірілген мәтінге келесі сан тең болды: $\tilde{p}$ = 09201900011212000718050511002015001305.

Шифрлау үшін авторлар e=9007 және n=1143816257578888676692357799761466420102182967212423625626518429357069352457338978305971235639587050589890751475992900268795435 41 сандарын таңдап алды.

Шифрлағаннан соң

$$c = \tilde{p}^{e} \pmod{n} =$$

1999351314678051004523171227402606474232040170583914631037037174062597160894862750439920962672582675012893554461353823769748026 санын алды. Кездейсоқ таңдап алынған n саны 64 және 65 дәрежелі p және q сандарының көбейтіндісі. Егер мәтін өте үлкен болған жағдайда онымен бір сан ретінде жұмыс жасау үшін оны блоктарға бөлу керек, әр блокты жеке сан ретінде қарастырып және шифрлау барысында блоктар байланысын қолдану қажет.

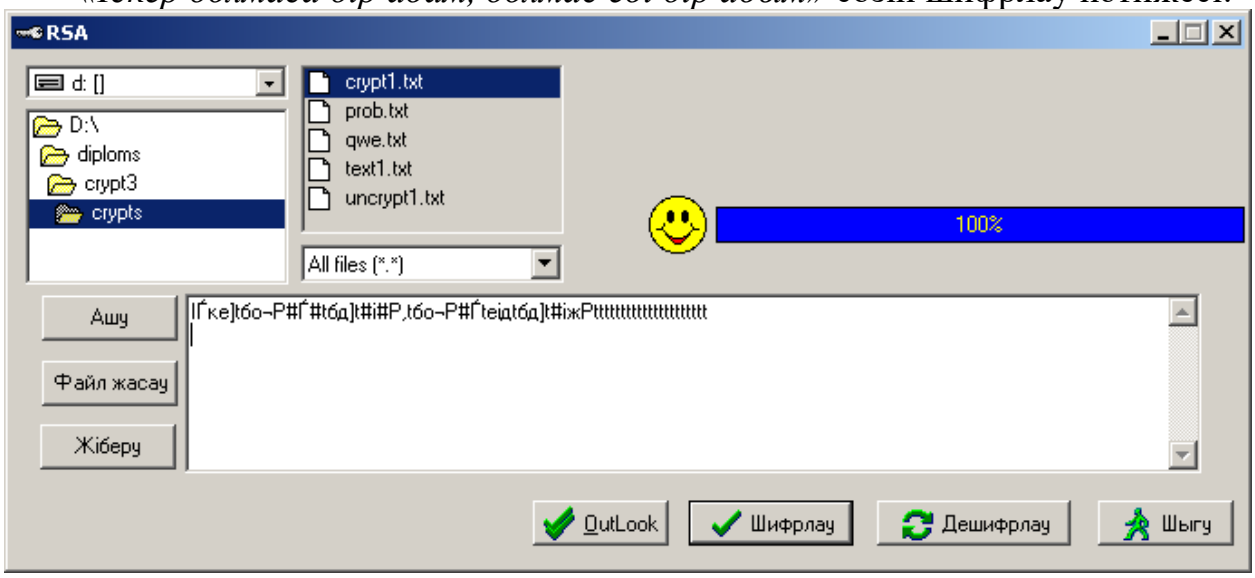
RSA әдісімен шифрлау процесін төмендегіше келтіруге болады:

Ашық типтегі кез-келген файл болсын, яғни құрамында кез-келген ақпарат болатын мәтіндік файлды таңдап аламыз. Бұл файл RSA әдісінің алгоритмі бойынша шифрланады. Нәтижесінде шифр мәтінді файл құрылады.

Шифрды қайта ашу процесі келесі түрде болады:

Шифрланған мәтіндік файлды бағдарлама арқылы көрсетіп және бұл файлды RSA әдісінің шифрды қайта ашу алгоритмі бойынша ашамыз. Нәтижесінде ашық мәтінді файл құрылады.

«Іскер болмаса бір адам, болмас еді бір адым» сөзін шифрлау нәтижесі:



Сурет 20 RSA терезесі

Шифрлау коды:

```
AssignFile(F,'crypts\text1.txt');
    Reset(F);
 AssignFile(G,'crypts\crypt1.txt');
   rewrite(G);
```

```
  While not EoF(F) do
 begin //2
  read(f,c);
  m := ord(c);
  d := 19;
  n := 259;
  ot1 := 1;
for i := 1 to d do
begin
ot2 := ((m*ot1) mod n);
ot1 := ot2;
  end;
  c1 := chr(ot1);
  write(g,c1);
  end;
    CloseFile(F);
      CloseFile(G);
```

Дешифрлау коды:

```
AssignFile(F,'crypts\crypt1.txt');
     Reset(F);
 AssignFile(G,'crypts\uncrypt1.txt');
   rewrite(G);
  While not EoF(F) do
 begin //2
  read(f,c);
  m := ord(c);
  d := 91;
  n := 259;
  ot1 := 1;
for i := 1 to d do
begin
ot2 := ((m*ot1) mod n);
ot1 := ot2;
  end;
  c1 := chr(ot1);
  write(g,c1);
  end;
    CloseFile(F);
      CloseFile(G);
```

Нақты бір ақпарат жүйесі үшін таңдау қорғаныс әдісінің күшті және әлсіз жақтарын тереңінен талдауды қажет етеді. Таңдап алынған қандай да бір қорғаныс жүйесі тиімділік критерилерін қанағаттандыруы керек. Бірақ, өкінішке орай қазіргі уақытқа дейін криптографиялық жүйенің тиімділігін

анықтауға және бағалауға мүмкіндік беретін сәйкес әдістеме жасалмаған. Мұндай тиімділіктің ең қарапайым түрі – кілтті ашу ықтималдылығы немесе кілттің көптілігі. Негізі бұл да крипто тұрақтылыққа жатады. Оны бағалауға барлық мүмкін кілттерді теру немесе ашу қиындығын қолдануға болады. Бірақ та бұл критерий крипто жүйеге қойылатын басқа да маңызды талаптарды ескермейді:

* Ашудың мүмкін еместігі немесе әдейі модификацияланған ақпарат;
* қолданылатын қорғаныс протоколдарының кең мүмкіндігі;
* қолданылатын кілттік ақпараттың ең кіші көлемі;
* іс-жүзіне асырудағы қолайлық және құндылығы;
* жылдам жұмыс жасауы.

Орын алмастырулар шифрлары

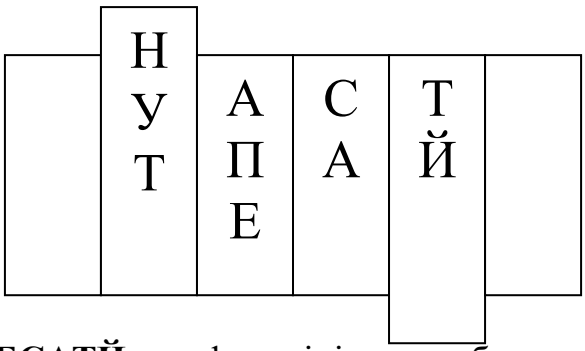
Орын алмастырулар шифрларын пайдалану кезінде мәтіннің белгілі бір бөлігі анықталған ереже бойынша ауыстырылып қойылады. Орын алмастырулар шифрлары ең қарапайым, ең ежелгі шифрлар болып табылады.

«Скитала» орны алмастыру шифры

Біздің эрамызға дейінгі V ғасырда Спарта басқарушылары жақсы ойластырылған әскери байланыс жүйесімен жұмыс жасаған және өз хабарламаларын ең алғашқы криптографиялық құрылғы «скитала» көмегімен шифрлаған.

Шифрлау келесі әдіспен жүргізіледі. Цилиндрлік түрдегі серіппеге пергаменттер орап, оған мәтін жазған. Сонан соң серіппеден пергаментті жазылған мәтінмен бірге шешкен. Пергамент бетінде жазулар шашырай орналасады.

Мысалы: **«НАСТУПАЙТЕ»** сөзін серіппе шеңбері бойымен жазсақ



«НУТАПЕСАТЙ» шифрмәтінін алуға болады. Шифрмәтінді қайта ашу үшін шифрлау ережесін және серіппе диалектрін білу қажет.

Шифрлаушы кестелер

Қайта өрлеу дәуірі басталғаннан бастап криптография да қайта дами бастады. Сол заманғы орын алмастыру шифрлары ретінде шифрлаушы кестелер пайдаланылған.

Шифрлаушы кестелерде кілт ретінде :

1) кесте өлшемі ;
2) орын алмастыруды беретін сөз;
3) кесте құрылымы ерекшеліктері пайдаланылады.

Ең көп тараған түрі - кесте өлшемі кілт болатын қарапайым орын алмастыру. Мысалы: **«СЕГОДНЯ В ПОЛНОЧЬ В РЕСТОРАНЕ ЧАЙКА»** хабарламасын баған бойынша жазамыз.

С	Н	Л	В	О	Ч
Е	Я	Н	Р	Р	А
Г	В	О	Е	А	Й
О	П	Ч	С	Н	К
Д	О	Ь	Т	Е	А

Кесте 6 бағаннан, 5 жолдан тұрады. Шифрмәтін алу үшін жазуларды жол бойымен 5 әріптен бөлейік.

«СНЛВО ЧЕЯНР РАГВО ЕАЙОП ЧСНКД ОЬТЕА» хабарламасы алынады.

Хабарламаны жіберуші мен алушы алдын-ала жалпы кілт ретінде кесте өлшемін пайдалануды келісіп алуы тиіс. Алынған шифрмәтінді қайта ашу үшін кері қарай амалдар орындалады.

Келесі орын алмастыру **<u>кілт бойынша бірлік орын алмастыру</u>** деп аталады. Бұл әдістің айырмашылығы кесте бағандары кілттік сөзге не сандар жиынына байланысты орын ауыстырылады. Мысалы: **«ПЕЛИКАН»** кілттік сөзін алып, **«ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛЬНОЧЬ»** мәтінін шифрлайық. Осы сөздің алфавит бойынша орналасуын қарастырайық.

А-1 Л-5
Е-2 Н-6
И-3 П-7
К-4

Алғашқы кесте

П	Е	Л	И	К	А	Н
7	2	5	3	4	1	6
Т	Н	П	В	Е	Г	Л
Е	А	Р	А	Д	О	Н
Р	Т	И	Е	Ь	В	О
М	О	Б	Т	М	П	Ч
И	Р	Ы	С	О	О	Ь

Шифрланған кесте

А	Е	И	К	Л	Н	П
1	2	3	4	5	6	7
Г	Н	В	Е	П	Л	Т
О	А	А	Д	Р	Н	Е
В	Т	Е	Ь	И	О	Р
П	О	Т	М	Б	Ч	М
О	Р	С	О	Ы	Ь	И

Демек, сандарды өсу реті бойынша орналастырдық. Алынған кестедегі әріптерді жол бойымен 5-ден топтап келесі шифрмәтінді аламыз:

ГНВЕП ЛТОАА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЫЬИ.

Жіберілетін хабарламаны бұдан да толығырақ жасауы қажет болса, бір рет шифрлағаннан кейін, тағы да қайта шифрлауға болады. Мұндай шифрлау **екілік орын алмастыру** деп аталады. Бұл жағдайда орын алмастырулар бағандар және жолдар үшін жеке-жеке анықталады. Алдымен, кестеге хабарлама мәтіні жазылады, содан соң бағандар, кейін жолдар орын ауыстырылады. Мысалы: **«ПРИЛЕТАЮ ВОСЬМОГО»** сөзін шифрлау қажет. Ескілік орын алмастыруларда кілт ретінде берілген кестенің бағандар номерлері және жолдар номерлері тізбегі қолданылады.

а)	4	1	3	2
3	П	Р	И	Л
1	Е	Т	А	Ю
4	В	О	С	Ь
2	М	О	Г	О

б)	1	2	3	4
3	Р	Л	И	П
1	Т	Ю	А	Е
4	О	Ь	С	В
2	О	О	Г	М

в)	1	2	3	4
1	Т	Ю	А	Е
2	О	О	Г	М
3	Р	Л	И	П
4	О	Ь	С	В

а) берілген кесте; б) бағандардың орын алмасуы; в) жолдардың орын алмасуы.

Егерде алынған мәтінді 4 әріптен топтайтын болсақ,
«ТЮАЕ ООГМ РЛИП ОЬСВ» хабарламасы шығады.
Екілік орын алмастырулар варианттары саны кесте өлшемі өсуіне қарай көбейтіп отырады.

-3*3 кесте үшін 36 вариант;
-4*4 кесте үшін 576 вариант;
-5*5кесте үшін 14400 вариант.

Сиқырлы квадраттарды пайдалану

Сиқырлы квадраттар деп 1-ден бастап өзге де сандармен толтырылған, әр бағанның, жолдың, диагональдың қосындысы бір санды беретін квадрат кестелерді атайды. Шифрланатын мәтінді ұяшықтар номерлеріне сәйкестендіріп сиқырлы квадраттарға жазады. Соңынан, осы кестенің мазмұны жол бойынша жазып алса, қажетті шифрмәтін алынады.

Мысалы: **«ПРИЛЕТАЮ ВОСЬМОГО»** хабарламасы үшін

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

О	И	Р	М
Е	О	С	Ю
В	Т	А	Ь
Л	Г	О	П

Пайда болған шифрмәтін: **ОИРМ ЕОСЮ ВТАЬ ЛГОП**

- 3*3 өлшемді сиқырлы квадраттар саны біреу ғана;
- 4*4 өлшемді сиқырлы квадраттар саны 880;
- 5*5 өлшемді сиқырлы квадраттар саны 250000.

Қарапайым ауыстыру шифрлары

Орын алмастыру шифрларында мәтіннің символдары алдын-ала орнатылған ереже бойынша сол және өзге алфавит символдарымен алмастырылады. Ал қарапайым ауыстыру шифрында берілген мәтіннің әрбір символы дәл сол алфавиттің символдарымен бүкіл мәтін бойында бірдей ауыстырылады. Көбінесе қарапайым ауыстыру шифрларын бір алфавитті орынға қою шифрлары деп те атайды.

Полибиан квадраты

Қарапайым ауыстыру шифрларының ең алғашқысы полибиан квадраты болып есептеледі. Б.э.д. 2 ғасыр бұрын грек жазушысы және тарихшысы Полибий шифрлау мақсатында 5*5 өлшемді грек алфавиті әріптерімен толтырылған кестені ойлап шығарды.

λ	ε	ϑ	ω	γ
ρ	ς	δ	σ	ο
μ	η	β	ξ	τ
ϕ	π	θ	α	κ
χ	ν	_	φ	ι

Полибиан квадраты әйтеуір орналасқан 24 әріптен және бос орыннан (пробел) тұрады. Шифрлау кезінде осы полибиан квадратынан ашық мәтіннің кезекті әріпін тауып және шифрмәтінге осы әріптен төмен тұрған сол бағандағы әріпті жазып отырған. Егер ашық мәтіннің әріпі кестеде ең соңғы жолда тұрған болса, онда шифрмәтін үшін дәл сол бағандағы ең жоғарғы әріп алынған.

Трисемус шифрлаушы кестелері

1508-жылы Германиялық Аббат Иоганн Трисемус «Полиграфия» деп аталатын криптология туралы жұмысын басып шығарды. Бұл кітапта ол алғаш рет кездейсоқ ретпен толтырылған алфавитті шифрлаушы кестелерді қолдануды жүйелік түрде сипаттап шықты. Мұндай ауыстыру шифрын алу үшін әдетте кесте және кілттік сөз қолданылады. Кестеге алдымен сөз жол бойымен жазылады, қайталанатын әріптері алынып тасталады. Сонан соң, бұл кесте алфавиттің ондағы жоқ әріптермен рет-ретімен толтырылады. Кілттік сөзді есте сақтау оңай болғандықтан, мұндай қадам шифрлау және шифрлауды ашу процестерін жеңілдетеді. Орыс алфавиті үшін шифрлаушы кестенің өлшемі 4 х 5. Кілттік сөз ретінде **БАНДЕРОЛЬ** сөзін алайық. Нәтижелік кесте:

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Ж	З	И	Й	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

Полибиан квадраты секілді, шифрлау кезінде ашық мәтіннің әріпін кестеден тауып, орнына сол баған бойындағы төмен тұрған әріпті жазу қажет. Егер мәтін әріпі кестенің ең соңғы жолында тұрса, оның орнына сол бағандағы ең жоғарғы әріп жазылады. Мысалы:

ВЫЛЕТАЕМ ПЯТОГО
ПДКЗЫВЗЧ ШЛЫЙСЙ

Мұндай кестелік шифрлау көпграммды деп аталады, өйткені шифрлау бір әріппен орындалады. Шифрлаушы кестелер екі әріптен шифрлауға мүмкіндік беретінін Трисемус алғашқы болып байқаған. Мұндай шифрлар биграммдық шифрлар деп аталады.

Плейфейр биграммалық шифрлары

Плейфейр шифры 1854 жылы жасалған және орын ауыстырудың биграммалық шифрларының ең көп тараған түрі. Бұл шифр Ұлыбританияда бірінші дүниежүзілік соғыс кезінде қолданылған. Плейфейр шифрының негізі ағымдағы хабарлама алфавиті әріптері кездейсоқ орналасқан шифрлаушы кесте болып табылады. Шифрлаушы кестені жіберуші және алушының есте сақтауы оңай болуы үшін кілттік сөз пайдалануға болады. Жалпы алғанда, Плейфейр жүйесінің шифрлаушы кестелері толығымен Трисемус шифрлаушы кестелері құрылымына сәйкес. Сондықтан, Плейфейр жүйесінде шифрлау және кері шифрлауды үшін Трисемус кестесін пайдаланамыз.

Шифрлау процедурасы келесі қадамдардан тұрады:

1. Ағымдық хабарламаның ашық мәтіні жұпталған әріптерге бөлінеді. Мәтіндегі әріптер саны жұп болуы керек және екі бірдей әріптен тұратын биграмма болмауы тиіс;
2. Ашық мәтіннің биграммалар тізбегі шифрлаушы кесте көмегімен келесі ереже бойынша тізбекке бөлінеді:
   2а) егер биграмманың екі әріпі де бір жолда немесе бір бағанда жатпайтын болса, онда осы жұп әріптерден анықталған тіктөртбұрыштың бұрышындағы әріптер табылады;
   2б) егер биграмманың екі әріпі де кестенің бір бағанында жататын болса, онда шифртекст әріптері ретінде олардан төмен тұрған әріптер алынады;
   2в) егер биграмманың екі әріпі бір жол бойында жатса, онда шифртекст әріптері ретінде олардың оң жағында орналасқан әріптер алынады. Егер, мұнда әріп шеткі оң жақтағы бағанда орналасса, онда шифр ретінде сол жолдағы сол жақ бағандағы сәйкес әріп алынады.

Мысалы: **ВСЕ ТАЙНОЕ СТАНЕТ ЯВНЫМ**

Биграммаларға бөлеміз:

ВС ЕТ АЙ НО ЕС ТА НЕ ТЯ ВН ЫМ

Шифрлаушы кесте бойынша келесі шифрмәтін алынады:

ГП	**ДУ**	**ОВ**	**ДЛ**	**НУ**	**ПД**	**ДР**	**ЦЫ**	**ГА**	**ЧТ**
2а	**2а**	**2а**	**2в**	**2а**	**2а**	**2в**	**2а**	**2а**	**2а**

Б	А	Н	Д	Е	Р	О	Л
Ь	В	Г	Ж	З	И	Й	К
М	П	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ы	Ъ	Э	Ю	Я

Шифрлауды ашу кезінде кері іс-әрекеттер орындалады.

Вижинер шифрлау жүйесі

Вижинер жүйесі алғаш рет 1586 жылы жарық көрді және ең көне көп алфавиттік жүйелердің бірі болып табылады. Өз атын ол XVI ғасырдың француз дипломаты Блез Вижинер құрметіне алған. Вижинер сол заманғы криптографиялық жүйелерді жетілдіріп, дамытқан.

Вижинер жүйесі орын алмастыру кілті әріптен әріпке ауысатын Цезарь шифрлау жүйесіне ұқсас. Бұл шифрді **Вижинер кестесі** деп аталатын кестемен сипаттауға болады.

Вижинер кестесі шифрлау және кері шифрлау үшін қолданылады. Кесте екі ену жолынан тұрады:

- жоғарғы жолда асты сызылған символдары. Олардың көмегімен ашық мәтіннің әріпі есептеледі;
- сол жақ шеткі кілт бағаны.

Кілттер тізімі әдетте кілттік сөздің әріптерінің сандық мәнінен алынады.

Шифрлау кезінде хабарламаны жол бойынша жазады. Ал оның астына кілттік сөз жазылады. Егер кілт қысқа болса, онда ол циклдық түрде қайталанады. Шифрлау процесі барысында кестенің жоғарғы жағынан әріп табылады және сол жақ бағаннан кілттің мәні алынады. Шифртекст әріпі осы жол мен баған қиылысында анықталады.

Мысалы: кілт сөзі ретінде **АМБРОЗИЯ** сөзі алынсын және **ПРИЛЕТАЮ СЕДЬМОГО** хабарламасын шифрлау қажет .

Хбарлама: **П Р И Л Е Т А Ю С Е Д Ь М О Г О**
Кілт: **А М Б Р О З И Я А М Б Р О З И Я**
Шифртекст: **П Ъ Й Ы У Щ И Э С С Е К Ь Х Л Н**

Күрделі ауыстыру шифрлары

Күрделі ауыстыру шифрлары көп алфавитті деп аталады, өйткені ағымдық хабарламаның әрбір символын шифрлау үшін өзіндік қарапайым ауыстыру шифры қолданылады.

Ауыстырудың көп алфавитті шифрларын тәжірибе жүзінде криптографияға Леон Батист Альберти ұсынды және енгізді. Оның **«Шифр туралы трактат»** кітабы 1566 жылы жазылып, Европадағы криптология бойынша ең алғашқы ғылыми еңбек болды. Бүкіл әлемдегі криптологтар Л.Альбертиді криптологияның негізін қалаушы деп біледі.

Гронсфельд шифры

Гронсфельд шифры деп аталатын күрделі ауыстыру шифры Цезарь шифрының бір түрі болып келеді. Ағымдық хабарламаның төменгі жағына сандардан тұратын кілт цифрлары жазылады. Егер кілт хабарламадан қысқа болса, онда жазба циклдық түрде қайталанады. Шифрмәтін алу үшін алфавиттегі әріптен кілт цифрына сәйкес орынға жылжыған әріпті сәйкестендіреді.

Мысалы: **ВОСТОЧНЫЙ ЭКСПРЕСС** хабарламасы және **2718** кілті берілген болсын. Келесі шифрмәтінді аламыз:

Хабарлама: **В О С Т О Ч Н Ы Й Э К С П Р Е С С**
Кілт: **2 7 1 8 2 7 1 8 2 7 1 8 2 7 1 8 2**
Шифрмәтін: **Д Х Т Ь Р Ю О Г Л Д Л Щ С Ч Ж Щ У**

Яғни хабарламаның алғашқы әріпі В-ны шифрлау үшін кілттің 2 цифрын пайдаланып алфавиттегі В-дан кейін тұрған Д әріпі алынады.

Цезарьдің шифрлау жүйесі

Цезарь шифры қарапайым ауыстыру шифрының дербес жағдайы болып табылады. Бұл шифрдың аты Рим императоры Гай Юлий Цезарь құрметіне қойылған. Өйткені, аталған император бұл шифрды цицеронмен хабарлама алмасу кезінде пайдаланған (б.э.д. 50жыл).

Ағымдағы мәтінді шифрлау кезінде әрбір әріп дәл сол алфавиттің өзге әріпімен келесі ереже бойынша ауыстырылып отырған. Алынған әріпті алфавит бойымен к әріпке жылжу арқылы ауыстырылатын әріп анықталып отырған. Алфавит соңына жетіп қалған жағдайда циклдық түрде оның басына ауысу орындалған. Цезарь к=3 жылжу шифрын қолданған. Мұндай ауыстыру шифры үшін ашық мәтін мен шифрмәтін әріптерін сәйкестендіруші орын ауыстырулар кестесі қажет. К=3 үшін мүмкін болатын орынға қоюлар жиынтығы келесі кестеде көрсетілген:

К=3, m=26

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

Мысалы: Цезарь жолдамасы: **VENI VIDI VICI** жоғарыдағы кестемен шифрланған жағдайда **YHQL YLGL YLFL** түріне айналады.

Қарапайым ауыстыру шифрына математикалық анализ жасайық.

Zm алфавитіндегі орынға қою **Zm**-нен **Zm**-ге өзара бірмәнді бейнелеу **П** болып табылады: **П: t →П(t).**

Яғни, ол ашық мәтіннің t әріпін шифрмәтіннің П(t) әріпіне алмастырады. **Zm**-дегі барлық орынға қоюлардың жиыны **Zm симметриялы тобы** деп аталады және **SYM(Zm)** белгіленеді. SYM(Zm) симметриялы тобы келесі қасиеттерге ие:

1. **Тұйықтылық:** П1 П2 орынға қоюлардың көбейтіндісі де орынға қою болады: П2 П2

$$П: Zm \rightarrow Zm \rightarrow Zm$$

$$П: t \rightarrow П1(П2(t))$$

2. **Ассоциативтілік:** П1П2П3 орынға қоюлардың көбейтіндісі.

«Бұрылмалы торкөздер» шифрлары

Бұрылмалы торкөздер деп аталатын шифрды пайдалану үшін торкөзді қағаздан **2m**х**2к** торкөздерден тұратын трафарет дайындалады. Трафаретте **m, к** торкөздері оны таза параққа төрт түрлі әдіспен қойғанда оның барлық торкөздері жабылатындай етіп қиылған. Хабарлама әріптері трафарет қиындыларына орнатылған ретпен жазылады. Шифрлау процесін мысалмен қарастырайық. Кілт ретінде 10х6 торкөзі алынсын.

Сурет 1.

Келесі мәтін шифрланатын болса:

ШИФР РЕШЕТКА ЯВЛЯЕТСЯ ЧАСТНЫМ СЛУЧАЕМ ШИФР МАРШРУТНОЙ ПЕРЕСТАНОВКИ.

Торкөздерді параққа қойып алғашқы 15 әріпті жазамыз. Торкөзді 180 бұрамыз. Жаңа толтырылмаған торкөздер пайда болады, келесі 15 әріп жазылады. Сонан соң торкөзді кері жаққа бұрып, қалған мәтінді дәл осылайша шифрлаймыз. Хабарламаны қабылдаушыда дәл осындай торкөз бар бола, онда еш қиындықсыз ағымдық мәтінді оқи алады.

Сурет 2.

	Ш								
И				Ф		Р	Р		
	Е				Ш				Е
			Т				К		
	А								
		Я			В	Л			Я

Сурет 3.

Е	Ш		Т	С			Я		
И				Ф		Р	Р	Ч	
	Е	А			Ш	С			Е
Т				Н			К	Ы	
	А	М	С		Л				У
		Я			В	Л		Ч	Я

Сурет 4.

Е	Ш	А	Т	С	Е	М	Я		Ш
И	И			Ф		Р	Р	Ч	
	Е	А	Ф		Ш	С	Р		Е
Т	А		Т	Н	М		К	Ы	А
Р	А	М	С	Ш	Л	Р	У		У
	Т	Я			В	Л		Ч	Я

Сурет 5.

Е	Ш	А	Т	С	Е	М	Я	Н	Ш
И	И	О	Й	Ф	П	Р	Р	Ч	С
Р	Е	А	Ф	Е	Ш	С	Р	С	Е
Т	А	Т	Т	Н	М	А	К	Ы	А
Р	А	М	С	Ш	Л	Р	У	Н	У
О	Т	Я	В	К	В	Л	И	Ч	Я

Уитстон «Екілік квадрат» шифры

1854 жылы ағылшын Чарльз Уитстон «Екілік квадрат» деп аталатын биграммалармен шифрлаудың жаңа әдісін жасады. Өз атауына бұл шифр полибиан квадраты секілді ие болды.

Уитстон шифры криптографияның дамуы тарихында жаңа кезеңді ашты. Бұл шифрдың Полибиан квадратынан айырмашылығы «Екілік квадрат» бірден екі кестені пайдаланады. Кестелер бірінің қасына бірі жол бойымен орналасады, ал шифрлау Плейфейр шифрларі секілді биграммалар бойынша жүргізіледі. «Екілік квадрат» шифры өте тиімді және ыңғайлы болды, екінші дүниежүзілік соғыс кезінде Германияда қолданылды.

Мысалы: орыс алфавиті әріптері кездейсоқ орналасқан екі кесте берілген болсын. Шифрлау алдында ағымдық хабарлама биграммаларға бөлінеді. Әрбір биграмма жеке шифрланады. Биграмманың алғашқы әріпін сол жақтағы кестеден, екінші әріпін оң жақтағы кестеден табамыз. Сонан соң, ойша осы әріптер бұрыштары болатын тіктөртбұрыш тұрғызамыз. Бұл тіктөртбұрыштың өзге екі бұрышы шифрмәтін биграммалары әріптерін береді.

Ж	Щ	Н	Ю	Р
И	Т	Ь	Ц	Б
Я	М	Е	.	С
В	Ы	П	Ч	
:	Д	У	О	К
З	Э	Ф	Г	Ш
Х	А	,	Л	Ъ

И	Ч	Г	Я	Т
,	Ж	Ь	М	О
З	Ю	Р	В	Щ
Ц	:	П	Е	Л
Ъ	А	Н	.	Х
Э	К	С	Ш	Д
Б	Ф	У	Ы	

Ағымдық хабарлама биграммасы **ИЛ** шифрланып жатқан болсын. **И** әріпі 1-баған, 2-жол сол жақтағы кестеде, **Л** әріпі 5-баған, 4-жол оң жақтағы кестеде орналасқан. Яғни, тіктөртбұрыш 2-ші және 4-ші жолдардағы, 1-ші және 5-ші бағандары арқылы тұрғызылған, сондықтан **ОВ** биграммасын аламыз.

Егер биграмманың екі әріпі де бір жолда жататын болса, онда шифрмәтін әріптері де дәл сол жолдан алынады.

Шифрмәтін биграммасының алғашқы әріпін хабарлама биграммасының екінші әріпі орналасқан бағанаға сәйкес келетін сол жақ кестеден алады. Екінші әріп хабарлама биграммасының алғашқы әріпі орналасқан бағанаға сәйкес оң жақ кесте бағанынан алынады. Сондықтан хабарлама биграммасы **ТО** шифрмәтін биграммасы **ЖБ** айналады. Осылайша хабарламаның биграммалары шифрланады.

Хабарлама: **ПР ИЛ ЕТ АЮ _Ш ЕС ТО ГО**

Шифрмәтін: **ПЕ ОВ ЩН ФМ ЕШ РФ БЖ ДЦ**

«Екілік квадрат» әдісімен шифрлау енуге тұрақты және қолдануда қарапайым шифрды береді. «Екілік квадрат» шифрмәтінін бұзу өте үлкен күш жұмсауды қажет етеді, мұның өзінде хабарлама ұзындығы кем дегенде отыз жолдан тұруы тиіс.

№ 1

ПР ИГ ЛА ШЕ НИ ЕН АБ АН КЕ Т.
ЕП ЖЬ ОФ _Ш ЖГ РУ ХФ ДУ _. МД

№ 2

ОД НО РА ЗО ВЫ ЕС ИС ТЕ МЫ ШИ ФР ОВ АН ИЯ
ХГ ТЬ ЧК ИД ЕХ РФ ЬЗ МЫ АВ РЭ ЕС .. ДУ ЖМ

Ашық кілтті криптографиялық жүйелер.

RSA шифрлау жүйесі

Криптографиялық қорғау жүйелерінің ең маңыздылары ашық кілтті жүйелер болып табылады. Мұндай жүйелерде мәтінді шифрлау үшін бір кілт, ал кері шифрлау үшін өзге кілт қолданылады. Бірінші кілт құпия болмайды және мәліметтерді шифрлайтын өзге де пайдаланушылар үшін жария етіледі. Ал, шифрланған мәліметтерді алу үшін құпия сақталатын екінші кілт қолданылады.

Қазіргі кезде ақпаратты қорғаудың криптографиялық әдістері арасында ең ең дамыған әдіс RSA әдісі болып табылады. (RSA- әдісті ойлап

табушылардың тегінің бастапқы әріптерімен аталған Rivest, Shamir және Adleman). RSA әдісін құрастыру үшін кейбір мектептегі ұғымдарды еске түсіру қажет.

Жай сан деп - тек өзіне және 1-ге бөлінетін санды айтамыз. Өзара жай сандар деп 1-ден өзге артық бөлгіші жоқ сандарды айтамыз. I mod j амалының нәтижесі ретінде і санын j- ге бөлгендегі қалдығы алынады.

RSA алгоритімін пайдалану үшін ашық және құпия кілттер генерациясы жасалады. Келесі қадамдарды орындаймыз:

1. Өте үлкен жай сан таңдалады: p және q.
2. p және q көбейтіндісі мен n саны анықталады. (n=p*q)
3. Үлкен кездейсоқ d саны таңдалады. Бұл сан (p-1)*(q-1) көбейтіндісінің нәтижесімен өзара жай сан болуы тиіс.
4. e*d mod ((p-1)*(q-1))=1 қатынасы орындалатындай e саны анықталады.
5. e және n сандарын ашық кілттер, ал d және n сандрын құпия кілттер деп атайды.

Ары қарай, {e,n} белгілі кілті бойынша мәліметтерді шифрлау үшін берілген мәтінде бөліктерге бөледі. Әр бір бөлік M(i)=0,1,…n-1 саны түрінде бейнеленеді. M(i) сандарының тізбегі түрінде берілген мәтінді $C(i)=M(i)^e$ mod(n) формуласымен шифрлайды. Бұл мәліметтерді шифрлау үшін {dn} құпия кілтін пайдаланып, $M(i)=C(i)^d$ mod(n) есептеулерін орындайды. Нәтижесінде M(i) сандарының жиыны алынады. Ал, бұл сандар ағымдық мәтінді береді.

Қарапайым мысал қарастырайық: **<<EDA>>** хабарламасын RSA әдісімен шифрлайық.

1. p=3 және q=11 деп таңдап аламыз.
2. n=3*11=33 екенін анықтаймыз.
3. (p-1)*(q-1)=(3-1)*(11-1)=2*10=20

d саны ретінде 20-ға өзара жай болатын сан таңдалады. Мысалы, d=3.

4. e санын таңдаймыз. e*3 mod(20)=1; мысалы, e=7.

5. Шифрланатын хабарламаны 0..32 аралығындағы бүтін сандар тізбегі түрінде жазамыз.

A=1 D=5 E=6

EDA-651

Мәтінді {7,33} кілті көмегімен шифрлаймыз.

$C_1=6^7 \text{mod}(33)=279936 \text{ mod}(33)=30$;

$C_2=5^7 \text{mod}(33)=78125 \text{ mod}(33)=14$;

$C_3=1^7 \text{mod}(33)=1 \text{ mod}(33)=1$;

Алынған шифрмәтін: {30,14,1}.

Кері шифрлау жүргізейік. {30,14,1} шифр мәтінін ашу үшін {3,33} құпия кілті қолданылады:

$M_1=30^3 \text{mod}(33)=27000 \text{ mod}(33)=6$

$M_2=14^3 \text{mod}(33)=2744 \text{ mod}(33)=5$

$M_3=1^3 \text{mod}(33)=1 \text{ mod}(33)=1$

{6,5,1} сандары алынады. Бастапқы хабарлама <<EDA>>.

RSA алгоритмінің криптотұрақтылығы құпия кілтті анықтаудың мүмкін еместігіне негізделеді. Алғашқы, белгілі кілт бойынша құпия кілтті анықтау

үшін осы санның бөлгіштерін анықтау туралы есепті шешу қажет болады. Мұндай есептің осы уақытқа дейін тиімді (полиномды) шешімі табылмаған.

3.3 К.Шеннон қағидасының негіздері

Хабарламаның бастауы **X** ашық мәтінін туғызады. Кілттің бастауы **Z** кілтін түрлендіреді.

Шифрлаушы **Z** кілтінің көмегімен, **X** ашық мәтінін шифртекстке түрлендіреді:

$$\mathbf{Y:\ Y=TzX\ .}$$

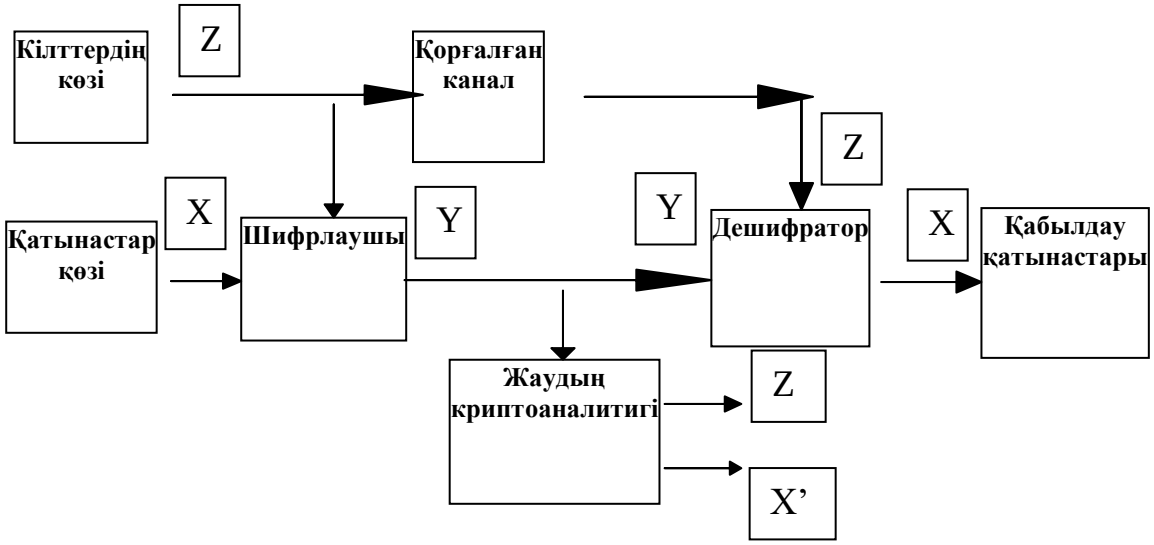
Дешифратор, **Y** шифрланған хабарламасын ала , $\mathbf{X=Tx(-\ 1)\ Y}$ қарама-қарсы операциясын орындайды.

Қарсыластың негізгі мақсаты криптоаналитика қарсыластың ашық мәтіннің және кілттің шифртекст талдауының мақсаты болып табылады.

Шеннон қағидалы және практикалық құпиялықтың сұрақтарын қарады. Теориялық құпиялықты анықтау үшін Шеннон келесі сұрақтарлы қалыптастырды:

1. Егер жаудың криптоаналитігі уақытпен шектелмесе және криптограммаларды талдау үшін барлық құралдармен жабдықталған болса онда жүйе қаншалықты төзімді?
2. Криптограмма жалғыз шешім алады ма?
3. Бір ғана шешім алу үшін криптоаналитикке шифрмәтіннің қандай көлемін ұстап алу керек.

Бұл сұрақтарға жауап үшін Шеннон келесі шарт көмегімен мүлтіксіз құпиялықтың ұғымын енгізді: апостериорлық ықтималдықтар тәжірибеден бұрын ықтималдықтарға тең барлық **Y** үшін, яғни шифрланған қатынасты ұстап қалу криптоаналитика жауына ешқандай мәлімет бермейді. Байес теоремасы бойынша.



Сурет 21 Шифрланған хабарламаларды жіберудің жалпы сұлбасы

Бұл жерде P(X) - X хабарламасының – априорлы ықтималдығы; P(Y) – X хабарламасы таңдалғанда (яғни X хабарламасы Y криптограммаға аударатын барлық кілттердің ықтималдылығының суммасы) Y криптограммасының шартты ықтималдылығы, *Y шартты белгісінің – шартты ықтималдығы, немесе X хабарламасы таңдалған, яғни барлық кілттің мүмкіндігінің сомасы, нешінші X хабарламасын Y шартты белгісіне аударады;* P(Y) - Y криптограмманы алу ықтималдылығы; P(X) –Y криптограмма ұсталған жағдайда (шарты орындалғанда) X хабарламасының апостериорлық ықтималдығы. $P_Y(X)$ және P(X) -нің құпиялығы үшін X және Y мәндері барлығы үшін тең болуы қажет.

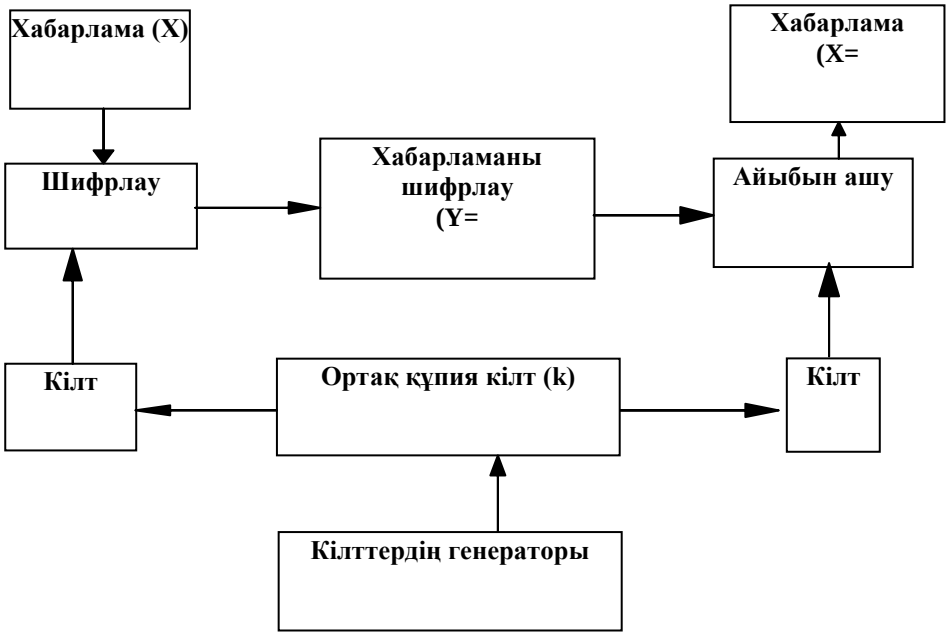
Криптограммаларды статикалық талдауға қарсы әрекеттер үшін Шеннон екі әдісті қолдануды ұсынды: ыдырау және кедергі жасау.

3.4 Шифрлаудың симметриялы әдістері

Симметриялы криптожүйенің негізгі кластары

Симметриялық крифтографиялық жүйелердің астарында шифрлау және кері шифрлау ашу үшін құпия сақталған ылғи бір кілтті қолданылатын криптожүйелер тығылады.

Пайдаланушылар үшін бұл жүйені қолданудан алдын, оған потенциалды қаскүнемге рұқсат бермеу мақсатында жалпы құпия кілтті алу қажет екенін білдіреді. Симметриялық криптожүйелердің барлық алуантүрлігі келесі негізді кластарда жіктелінген.



Сурет 22 Симметриялық шифрлау әдісін қолдану

Моноалфавитті алмастырулар - бұл бастапқы мәтіннің символдарын сол алфавиттің басқа символдарымен ереже бойынша алмастыруға негізделген ең қарапайым түрлендіру әдісі. Моноалфавитті шифрлауда бастапқы мәтіннің әрбір символы бір заңдылық бойынша шифрланған мәтін

символына алмасады. Көп алфавитті алмастыруда түрлендіру заңы символдан символға алмасу (мүлдем басқа алфавиттің символына).

Орын ауыстырулар - нақты бір ереже бойынша бастапқы мәтіннің символдарының орнын аумастыруға негізделген криптографиялық түрлендірудің қарапайым әдісі. Қазіргі уақытта алмастырулар жиі қолданылмайды, өйткені оларды криптотөзімділігі жеткіліксіз.

Блоктық шифрлар – берілген мәтіндердің блоктарын кері түрлендірулері. Негізінде блоктық шифр – бұл блоктар алфавитінде алмастырулар жүйесі. Қазіргі уақытта блоктық шифрлар іс-жүзінде (тәжірибеде) кеңінен таралған. Ресейлік және американдық шифрлаудың стандарттары дәл осы шифрлардың кластарына жатады (ГОСТ 28147-89-шы, DES).

3.5 Кілттерді басқару

Кілттерді басқарудың қарапайым жүйесі

Нақты бір ақпараттық жүйеде криптографиялық қорғау құралы үшін кілттерді басқару өзекті мәселе болып табылады. Криптожүйе канша күрделі және сенімді болса да ол кілттерді қолдануға негізделген. Егер екі пайдаланушы арасында ақпарат алмасуда конфиденциальдылықты қамтамасыз ету қажет болса кілттермен алмасу үрдісі көптік болады, онда жүз немесе мың пайдаланушыдан тұратын ақпараттық жүйеде басқару - өзекті мәселеге айналады.

Кілттік ақпарат деп АЖ-дегі барлық істеп тұрған кілттердің жиыны түсініледі. Егер кілттік ақпаратты басқару жеткілікті сенімділікте қамтамасыз етілмесе, онда қаскүнем оған қол жеткізіп, барлық ақпаратқа шексіз қол жетімділікке ие болады.

Кілттерді басқару – үш элементтен тұратын ақпараттық үрдіс: кілттерді генерациялау, кілттерді жинақтау, кілттерді тарату.

Кездейсоқ емес кілттерді оларды есте сақтау оңайлығы үшін қолдануға болмайды. Күрделі АЖ-лерде кілттерді генерациялау үшін арнайы аппараттық және бағдарламалық әдістер қолданылады. Ереже бойынша кездейсоқ сандар көрсеткіштерін (КСК) қолданады. Дегенмен олардың генерациясының кездейсоқтық деңгейі жеткілікті дәрежеде жоғары болуы қажет. «Табиғи» кездейсоқ үрдістерге негізделген құрылғылар идеалды генераторлар болып табылады. Мысалы, ақ радиошумға негізделген кілттерді генерациялаудың сериялық үлгісі пайда болды. Кездейсоқ сандарды физикалық көрсеткіші Pentium III процессорының ядросына кірістірілген. Трансцендентті сандардың ондық таңбалары басқа математикалық кездейсоқ объект болып табылады. Мысалы, стандартты математикалық әдістермен есептелінетін π немесе e.

Орташа қауіпсіздікті талап ететін АЖ-де пайдаланушы енгізген ағымдық уақыт және (немесе) саннан КСК–ін күрделі жүйе ретінде есептейтін бағдарламалық кілттер генераторын қолдануға болады.

Кілттерді жинақтау дегенде олардың сақталуын, есепке алынуын және жойылуын ұйымдастыру түсініледі.

Кілт қаскүнем үшін конфиденциалды ақпаратқа жол ашатын ең жағымды объект болғандықтан құпия кілттерді оқуға немесе көшіруге мүмкіндіксіз жинақтауыштарда ашық жазылмауы кажет.

Жеткілікті күрделі АЖ-де бір пайдаланушы кілттік ақпараттың үлкен көлемімен жұмыс істеуі мүмкін, кейде кілттік ақпарат бойынша мини деректер қорын ұйымдастыру қажеттілігі туады. Мұндай деректер қоры қолданылатын кілттердің қабылдануына, сақталуына, есепке алынуына және жойылуына жауап береді.

Қолданылатын кілттер туралы барлық ақпарат шифрланған түрде сақталуы тиіс. Кілттік ақпаратты шифрлайтын кілттер шебер кілттер деп аталады. Мүмкіндігінше, шебер кілтті әрбір пайдаланушы жатқа білгені және оларды материалдық тасушыда сақтамағаны жөн. Ақпарат қауіпсіздігінің өте маңызды шарты болып АЖ-дегі кілттік ақпараттың жүйелі түрде жаңартылып тұруы саналады. Мұнда қарапайым кілттер де, шебер кілттер де қайта тағайындалуы қажет. Жауапкершілігі ерекше АЖ-де кілттік ақпаратты мүмкіндігінше күн сайын жаңартып тұру керек.

Алгоритм және әдістерді сипаттау үшін бұл тарауда келесі белгілеулер қажет:

I_A – А тараптың идентификаторы

D_A – А тараптың құпыя криптотүрлендірілуі (ассиметриялық криптожүйенің құпыя кілтін қолдана отырып)

E_A – А тараптың ашық криптотүрлендірілуі (ассиметриялық криптожүйенің ашық кілтін қолдана отырып)

T_A – А тараптың уақытша штампы

R_A - А тарап таңдаған кездейсоқ сан

Кілттерді тарату - бұл кілттерді басқарудағы ең жауапты үрдіс. Оның екі талабы бар:

1. таратудың жеделдігі және дәлдігі
2. таратылған кілттерді құпиялығы

Симметриялық шифрлау жүйесі қоршауында өзара қауіпсіз іс-әрекетті орнатуды қалайтын екі пайдаланушы алдымен қауіпсіз жалпы кілтті орнатулары қажет. Мұның бір жолы болып үшінші тараптың қолданылуы болып табылады, мысалы куръер.

Тәжірибеде қауіпсіздікті қамтамасыз ету үшін жүйелі түрде кілттерді алмасытырп тұру керек. Бұл күрделі немесе соған ұқсас сұлбаны бағасын қымбаттатуы және эффективсіз етуі мүмкін.

Бұған альтернатива болып екі пайдаланушының кілттерді тарату орталығы (КТО) орталық органынан - өзара жұмыс істеуге мүмкіндік беретін жалпы кілтті алуы қажет.

КТО және пайдаланушы арасында берілгенмен алмасуды ұйымдастыру үшін олардың арасында берілетін хабарламаны шифрлайтын арнайы кілті ерекшеленеді. әрбір пайдаланушыға жеке кілт берілгендіктен, оның компрометациясы ерекше ешқандай жағымсыз нәтижеге әкелмейді.

Бұл тәсілдің әлсіз жері келесідей: кілттерге қолжетімділігі бар қаскүнемнің КТО-ға қол жеткізуі. Нәтижеде қауіпсіздіктің бір рет бұзылуы

бұл жүйеге қауіп төндіреді. Оған қоса, КТО ұзақ уақыт бойы пассивті тыңдалуда болуы да мүмкін, дегенмен бұны дәлелдеу қиын.

Үлкен желілерде бұл процедура өте маңызды орын алады, өйткені кілтке қажет болған әрбір пайдаланушылар жұбы кем дегенде бір рет орталық түйінге қатынас жасау керек. Одан басқа орталық органның істен шығуы кілттерді тарату жүйесін бұзуы мүмкін.

Парақтарда және орталық түйіндердегі кілттерді басқару орталығындағы пайдаланушылардың иерархиялық жүйесі бұл мәселені оңайлатудың бір тәсілі болып табылады. Бірақ, бұл қауіпсіздіктің жаңа проблемасын тудырады, өйткені қаскүнем үшін көптеген кіру нүктесі құрылады. Оған қоса, егер жиі өзара іс-әрекет жасайтын жұп бір ішкі түйінде (поддеревада) болмаса, берілген жүйе эффективсіз болады, өйткені ағаштың түбірі жаңадан әлсіз жер болып қалады.

Осы кемшіліктердің кейбіреулерін ашық кілттік жүйелерге негізделген кілттерді тарату тәсілін қолданып жөндеуге болады.

Ашық кілтті жүйелерде негізделген кілттерді басқару

Ашық кілтті криптожүйені қолданудан алдын А және В пайдаланушылары қарапайым құпыя кілттерімен алмасу үшін өздерінің ашық кілттерімен алмасу қажет. Бұл проблема құпыя кілт алмасуға қарағанда оңайрақ, өйткені ашық кілттерді сақтауда және жіберуде құпиялықты талап етпейді.

Ашық кілттерді басқару жедел немесе автономды каталогтар қызметінің көмегімен ұйымдастырылуы мүмкін, пайдаланушылардың өздері де өзара кілт алмасуы мүмкін. Бірақ, бұл жердегі проблема – аутентивтілік. Егер А E_C –ны шын мәнінде E_B деп ойласа, онда А хабарламаны E_C –ның көмегімен шифрлайды және С-ға D_C –ны қолданып кері шифрлауға байқамай (әдейі емес) мүмкіндік беруі мүмкін.

Екінші проблема толықтылық болып табылады: ашық кілттің жіберілуіндегі кез-келген қателік оны тиімсіз етеді. Сондықтан қателерді табатын (жөндейтін) қандай да бір қалып (форма/жүйе) болғаны жөн. Ашық кілттерді тарату үшін таңдалған сұлбадан тәуелсіз қандай да бір кезеңде орталық орган қатысады. Дегенмен, пайдаланушылардың өзара ашық кілттермен алмасуы орталық органның талап етпейді, өйткені негізгі проблема болып аутетификация саналады. Демек, орталық органның компрометациясының зардабы (нәтижесі) қарапайым кілттік жүйедегі сияқты онша ауыр болмайды.

Проблеманың тағы бір аспекті болып сенімділік (анықтылық) саналады: пайдаланушының ашық кілті сәйкес құпыя кілттің компрометациясының нәтижесінде немесе қандай да бір басқа себептермен, мысалы, жарамдылық мерзімі бітіп қалса, сенімсіз болып табылады.

Егер ашық кілттер каталогта сақталса немесе оларға қатынау (доступ) каталогы арқылы болса, онда ескірген берілгендер (мәліметтер) проблемасын (мәселесін) тудырады.

Мысал ретінде Диффи-Хеллманның кілттермен алмасу хаттамасын келтіруге болады бұл хаттаманы жүйелік параметрлері болып GF(p) нің

примитивті элементтері болып табылатын p және g қарапайым (жай) сандары саналады.

Енді А және В пайдаланушылар жалпы (ортақ) құпия кілтті алғысы келсін (алуды қаласын). Алдымен А a құпыя кездейсоқ санын генерацияласын, ал В b санын генерацияласын. Кейін олар g^a mod және p g^b mod p –ны сәйкесінше есептейді және есептелген мәнді бір –бірлеріне жібереді. Бұны байланыстың ашық каналы арқылы жүзеге асыруға болады. Содан соң А $K_{ab}=(g^b \bmod p)$, ал В $K_{ba}=(g^a \bmod p)$–ны есептейді. $K_{ab}=K_{ba}=K$ болғандықтан А және В –да К жалпы (ортақ) құпыя кілті бар.

Дегенмен, Диффи-Хеллманның хаттамасы «ортадағы адам» деп аталатын шабуылға әлсіз. С қаскүнем А-дан В-ға жіберілне ашық мәнді ұстап алып, оның орнына өзінің ашық мәнін жіберуі мүмкін. Кейін ол В-дан А-ға жіберілген ашық мәнді ұстап алып, оның орнынан да өзінің ашық мәнін жіберуі мүмкін. Сонымен С А және В-ның ортақ құпыя кілтін алуы және бір тараптан екінші тарапқа жіберілген хабарламаны оқуы және/немесе өзгенртуі мүмкін.

Құпия кілттермен алмасу хаттамасы

Алдынғы параграфта қарастырылған шабуылдан қорғану үшін төменде сипатталған хаттаманы қолдануға болады. Мұнда А және В бір –бірлерінің ашық кілттерінің аутентивтілігін тексеру мүмкіндігіне ие болады.

Айталық, А және В жалпы құпыя кілттерін анықтауды қаласын. Мұнда егер олар бір-бірлерімен ашық кілттерін алған болса, онда үш кезеңдік қол алысу хаттамасын қолдануға болады.

А –В-ға $C=E_B$ (R_A,I_A) хабарламасын жіберуі мүмкін, бұл жерде E_B - В ашық кілтімен шифрлау процедурасы, I_A - А идентификаторы және R_A - кездейсоқ саны. Енді В С –ны кері шифрлап, I_A –ны біле алады. Енді В R_B кездейсоқ санын таңдайды және $C'=E_A(R_A,I_B)$ –ны А-ға жібереді. С' –кері шифрланғаннан кейін А нақты уақытта В R_A –ны алғанын тексере алады. өтйкені тек В С-ны кері шифрлай алады.

Демек, А В-ға $C''=E_B(K_B)$ –ны жібереді, және В С''-ны кері шифрлағанда ол нақты уақытта А R_B –ны алғанын тексере алады, өйткені тек А С' –ны кері шифрлай алады. Сонымен А және В бір-бірлерін аутентивтілікке тексерді, яғни олар бір-бірлерімен байланыста отырғандарын нақты біледі.

Енді А В-ға $E_B(D_A(K))$ –ны жібереді, В хабарламаны кері шифрлайды және К-ны алады. Бұл процедура К кілтімен алмасу кезінде құпиялықты сақтайды да, аутентивтілікті де қамтамасыз етеді.

Жоғарыда қарастырылған «сұрақ-жауап» механизмі деп аталатын процедура контрагенттің аутентивтілігі үшін пайдаланушы оған ол хабарлама-сұранысқа алдын ала келісілген операцияны орындап жауап қайтару үшін алдын ала қандайда бір хабарламаны жіберуге негізделген нұсқа болып табылады.

Пайдаланушы жауап алған соң байланыс сеансының шындығына сенімді болады. Бұл әдістің кемшілігі болып сұраныс және жауап арасында заңдылықты орнату қиындығы табылады.

Сертификаттарды қолдану

Ашқ кілттерді таратқанда бір уақытта аутентивтілік және толықтылыққа қол жеткізу әдісі сертификаттарды қолдануға негізделген. Сертификаттарды қолдануға негізделген жүйе құпыя кілттерді тарату сиқты орталық орган (ОО) бар деп болжамдайды. Одан кейін әрбір пайдаланушы ОО-мен қауіпсіз өзара іс-әркет жасай алады деп есептейді. (болжам жасайды)

Бұл үшін әрбір пайдаланушының E_{OO} – ОО-ның ашық кілті болуы қажет. Сонда әрбір А пайдаланушы ОО-да өзінің E_A ашық кілтін тіркеуі мүмкін. $E_д$ ашық болғандықтан бұны пошта бойынша, электр байланысының ашық каналы бойынша немесе тағы басқа жолмен істеуге болады.

ОО-ға тіркелу кезінде А анықталған аутентификация процедурасы бойынша іс-әркет жасайды. Ағаш тәрізді құрылымғаие болған жүйе арқылы тіркеудің өңделуі альтернативті нұсқа болуы мүмкін: ОО жергілікті өкілдерге иерархияның төменгі сатысындағы пайдаланушыларды тіркеу үрдісінде делдал ретінде жұмыс істеуі үшін сертификаттар береді .

Кез-келген жағдайда А ОО қол қойған және E_A –сы бар сертификат алады, яғни ОО E_A сертификаттың жарамдылық мерзімінде $A(I_A)$ үшін идентиифкациялық ақпараттан тұратын М хабарламасын қалыптастырады.

Содан кейін ОО А-ның сертификаты болатын $CERT_A=D_{OO}(M)$ –ді есептейді. $CERT_A$ E_A –сы бар және ОО сертификатқа қол қойғандықтан бір уақытта оны аутентификациялайтын жаплы қол жетімді құжат болып дайындалады. Сертификаттарды ОО, пайдаланушылар таратуы немесе иерархиялық жүйеде қолданылуы мүмкін. Жарамдылық мерзімінің қосылуы скомпроментированный кілттерді қолданудан қорғануды қамтамасыз ету үшін уақытша штамптың жалпылануы болып табылады.

Бірақ, ескірген мәліметтердің проблемасы тек қана уақытша штамптың көмегімен шешілуі мүмкін емес, өйткені сертификат компрометация нәтижесінде немесе әкімшілік себептер бойынша оның жарамдылық мерзімі бітіп қалып жарамсыз болып қалуы мүмкін. Сондықтан, егер сертификаттар пайдаланушыларда сақталса, (оларды әрбір қолданғанда ОО бермесе) ОО жүйелі түре жарамсыз сертификаттар тізімін публикациялауы (жариялауы) қажет.

Қарастырылған сұлбалардың кейбір қасиеттері сертификаты бар жұмсақ диск сияқты электрондық эквивалентті қолданатын «телефондық анықтама» деп аталатын танымал (подходқа) тәсілге біріктірілуі мүмкін.

Бұл қолдануды оңайлатады, өйткені пайдаланушы соңғының сертификатына өте жылдам қол жеткізіп, басқалармен өте жылдам байланысқа шыға алады.

Аутентификация хаттамасы

Айталық, А В-мен байланыс орнатуды қалады, А дан В-ға дейін сертификатталған жолды алды, мысалы, каталогқа қатынас жасап, және бұл жолды В-ның ашық кілтін алу үшін пайдаланды. I_A – А тараптың идентиификаторы, D_A – тараптың құпыя криптотүрлендірілуі (құпия кілт), E_A – А тараптың ашық криптотүрлендірілуі (ашық кілт), T_A – А тараптың

уақытша штампы, R_A – А тарап таңдаған кездейсоқ сан, C_A – А тараптың сертификаты болсын.

I_B – В тараптың идентиификаторы, D_B – тараптың құпыя криптотүрлендірілуі (құпыя кілт), E_B – В тараптың ашық криптотүрлендірілуі (ашық кілт), T_B – В тараптың уақытша штампы, R_B – В тарап таңдаған кездейсоқ сан.

Идентиифкаторлар – бұл А және В уникальді (қайталанбайтын) атаулар. М хабарламаға қосылатын уақытша штампы М-ның жарамдылық мерзімінің датасын да сақтайды. Кездейсоқ сандар осы байланыс сеансында уақытша штампта көрсетілген жарамдылық мерзімінде қайталанбайтын тізбектелген сандармен алмастырылуы мүмкін.

Онда бір жақты аутентификация хаттамасы келесідей болады:

А пайдаланушы

1. R_A – ны таңдайды
2. $M=(T_A,R_A,I_A,$ <берілгендер>)- хабарламаны қалыптастырады.

Бұл жерде <берілгендер> кез-келген мәлімет. Берілгендер құпиялық үшін E_B көмегімен шифрлануы мүмкін, мысалы, А В-ға шифрланған берілгендердің кілтін жіберсе.

3. В пайдаланушыға (C_A D_A (M)) жібереді.

В пайдаланушы:

1. C_A –ны кері шифрлайды және E_A –ны алады. Сертификаттың жарамдылық мерзімінің аяқталу датасын тексереді.
2. D_A(M) –ді кері шифрлау үшін А қолының шындығын және қол қойылған ақпараттың толықтылығын тексере отырып E_A-ны пайдаланады.
3. М құрамындағы I_B –ны дәлдікке тексереді.
4. М-дегі T_a-ны тексереді.
5. қосымша М құрамындағы R_A-ны тексереді.

Әртүрлі қосымшалар үшін (азамттық/әскері) интеллектуалды карталарға негізделген қол жеткізу жүйелерінің кеңінен таратылуы субъекттің аутентификациясын қамтамасыз ететін сұлбаларды құруды талап етті.

Мұнда карта қожайынының құпия кілті оның тұлғалығының ажырамас белгісі болып қалады, және бұл кілттің мүмкін болған компрометациясынан қорғауды қамтамасыз ету үшін құпыя кілттің мәнін ашпай субъектінің құқығын (мүмкіндігін/өкілеттігін) растайтын нөлдік жариялаумен немесе нөлдік мәндік (zero knowledge proofs) дәлелдеу хаттамалары деп аталатын бір қатар сұлбалар ұсынылған.

Мұндай типтегі бірінші сұлбаны 1986 ж. Фейге, Фиат және Шамир ұсынған. Оның мәні келесідей.

Өзінің шындығын растауға тура келетін пайдаланушылар тобы үшін екі жай санның көбейтіндісі болып табылатын үлкен (512 биттен ұзын) n кездейсоқ бүтін саны таңдалынады. Аутентификация процесінде екі тарап

қатысады: өзінің шындығын дәлелдеуші А тарап, және оны растаушы В тарап.

Сенімді төреші (КТО) n модулі бойынша квадраттық болатын кездейсоқ болатын v санын таңдайды, яғни $\exists x : x^2 = v(\mathrm{mod}\, n)$, және n менен өзара дара сан. Бұл v мәні А-ға ашық кілт ретінде жіберіледі. Содан кейін $S = (v^{-1})^{1/2}(\mathrm{mod}\, n)$ арқылы S –тің ең кіші мәні есептелінеді. Бұл А тараптың құпыя кілті болады. әрі қарай аутентификация келесідей болады:

1. А тарап екі кездейсоқ санын таңдайды, 0<r<n. Кейін $x = r^2 \bmod n$-ді есептейді және оны В тарапқа жібереді.

2. В тарап А-ға b кездейсоқ санын жібереді.

3. егер $b = 0$ болса, онда А В-ға r санын жібереді. Егер $b = 1$ болса, онда А В-ға : $y = rv(\mathrm{mod}\, n)$-ді жібереді.

4. Егер $b = 0$ болса, онда В $x = r^2(\mathrm{mod}\, n)$-ді А х-тың квадрат түбірін білетіндігіне көз жеткізу үшін тексереді. Егер b=1 болса, онда В тарап $x = y^2 v(\mathrm{mod}\, n)$-ді А v^{-1}-дің квадрат түбірін білетіндігіне көз жеткізу үшін тексереді.

1-4 қадамдар хаттаманың бір циклын құрастырады. Тараптар бұл циклды r және b –ның әртүрлі мәндері үшін t рет қайталайды. Егер А тарап s –тің мәнін білмесе, ол В-ны $b = 0$ немесе b=1 жағдайында (осы екі жағдайдың тек біреуінде) оған В-ны алдауға мүмкіндік беретін r-ді таңдауы мүмкін. Бір циклдағы алдау ықтималдығы 0.5 –ке тең. t циклдағы ықтималдылық 2^{-t}-ға тең.

Бұл сұлбаның кемшілігі болып талап етілген ықтималдықпен (егер бұл ықтималдық өте кіші болса) дәлелдеуге қажет болған хаттамадағы цикл санының үлкен болуы табылады.

Алмасудың бір раундын талап ететін, бірақ өте көп есептеулерді қажет ететін тәсіл Гиллоу және Кискатер тарапынан ұсынылған.

I – А тараптың идентификациялық ақпараты (немесе оның хэш функциясының мәні), n –екі құпыя қарапайым сандардың ашық туындысы, v - ашық мән (дәреже көрсеткіші).

А тараптың g құпыя кілті былай анықталады: $\lg^{v} = 1(\mathrm{mod}\, n)$. А тарап В- ға өзінің I идентиифкациялық берілгендерін жібереді. Дәлелдеу хаттамасы келесідей болады:

1. А r бүтін кездейсоқ санын (0<r<n-1) таңдайды, $T = r^{v}(\mathrm{mod}\, n)$-ді есептейді және бұл мәнді В тарапқа жібереді.

2. В d бүтін кездейсоқ санын (0< d <n-1) таңдайды және бұл санды А тарапқа жібереді.

3. А $D = rg^{d}(\mathrm{mod}\, n)$-ді есептейді және бұл мәнді В-ға жібереді.

4. В $T' = D^{v} I^{d}(\mathrm{mod}\, n)$-ді есептейді және $T' = T$ теңдігін орындалуын тексереді. Егер ол орынды болса, онда тексеру сәтті аяқталған деп саналады.

Кілттерді анонимді тарату

Егер біз пайдаланушылар өздерінің кілттерін өздері таңдай алмайды деп болжамдасақ, онда олар кілттерді тарату орталығының қызметін пайдаланулары қажет. Мұндағы басты мәселе кім қандай кілтті алғанын

ешкім анықтай алмауы тиіс. Бұл жағдайда тарату процедурасы келесідей болады:

1. А <ашық кілт, құпыя кілт> жұбын таңдайды. (бұл хаттама үшін ол екеуін де құпыя сақтайды)

2. КТО кілттердің үзіліссіз ағымын генерациялайды.

3. КТО өзінің ашық кілтімен кілттерді бірінен соң бірін шифрлайды.

4. КТО шифрланған кілттерді бірінен соң бірін желіге жібереді.

5. А кілтті кездейсоқ таңдайды.

6. А таңдалған кілтті өзінің ашық кілтімен шифрлайды.

7. А біраз уақыт күтеді (кідірту) және екі рет шифрланған кілтті КТО – ға қайта жібереді.

8. КТО А-ның ашық кілтімен бір рет шифрланған кілтті қалдыра отырып екі рет шифрланған кілтті өзінің құпыя кілтімен кері шифрлайды.

9. КТО шифрланған кілтті А пайдаланушыға қайтадан жібереді.

10. А кілтті өзінің құпыя кілтімен кері шифрлайды.

№1 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Шифрлеудің классикалық жүйелерін зерттеу
Орын ауыстыру әдістері

Жұмыстың мақсаты:

Орын ауыстырудың криптографиялық әдісімен танысу және оны іс жүзінде қолдана білу.

Теориялық мәліметтер

Орын ауыстыру әдісі бойынша мәтіннің белгілі бір бөлігі анықталған ереже бойынша ауыстырылып қойылады.

Орын ауыстырудың қарапайым мысалы ретінде матрицаларды қарастыруға болады. Ағымдық мәтін белгілі бір ұзындықтағы бөліктерге бөлінеді және әріптерді оқу матрицаның жолы бойынша, ал жазу баған бойынша орындалады. Мысалы, 8х8 өлшемді матрица үшін мүмкін болатын кілттер саны $1{,}6 \times 10^{9}$. Бірақта, қазіргі ЭЕМ үшін бастапқы мәліметтің шешімін осы кілттердің арасынан іздеп табуға болады. 16х16 өлшемді матрицалар үшін (блоктың ұзындығы 256 символ) 1,4х1026 кілттер болады. Мұнша кілттерді қарап шығу біршама қиындықтар тудырады. Бағдарламалық және аппараттық жолдармен іске асыруға болатын басқа да орын ауыстырудың әдістері бар. Мысалы, аппараттық жолмен орын ауыстырылған блок, ақпаратты түрлендіру үшін электр тізбектерін қолданады және сол арқылы ақпарат параллельдік әдіспен беріледі. Текстi түрлендіру үшін блок ішіндегі электрлік монтаж схемасын өзгерту арқылы цифрлық код бағдарламадағы қатарлық разрядтар санын шатастыру арқылы жасалады. Қабылдау пунктінде шатасқан шифрларды реттеу үшін және тізбекті реттеу үшін басқа блок қойылады.

Орын ауыстырудың ерекшеліктері

Орын ауыстыру әдістері үшін алгоритм және бағдарламаны іске асыру мүмкіндігі жеңіл болу керек, әрі қорғаныс күші төмен, себебі берілген текстің ұзақтығына байланысты шифрланған тексте кілттің статистикалық заңдылықтары орын алады және бұл оның тез ашылуына мүмкіндік жасайды. Бұл әдістің басқа кемшіліктері – егер жүйеге шифрлау үшін бірнеше арнайы таңдап алынған мәліметтер жіберілген болса, сонда олар тез ашылады. Егер ашық тексте блок ұзындығы К символға тең болса, онда текстi ашу үшін ашық текстің К-1 блогын шифрлау жүйесінен өткізу жеткілікті, мұндағы бір символдан басқасы бірдей. Ақпаратты шифрлаудағы орын ауыстыру әдісін қолданғанда, берілген текстің символдары белгілі бір ережелер арқылы ауысады.

Тапсырманы орындау нұсқасы

Мысал 1. Ашық текст: **“ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ”**. Кілт (алмастыру ережесі): 8 әріптен тұратын 1,2,…,8 реттегі топты келесі рет бойынша ауыстыр: **3 – 8 – 1 – 5 – 2 – 7 – 6 – 4.**

Шифртекст: **“ФНШОИАВР_СИЕЕЕРПННТВАОКО”.**

Бұдан басқа күрделілеу ауыстыруды қолдануға болады. Ол үшін ашық текстi анықталған к1 кілті бойынша матрицаға бөліп жазамыз. Шифртекст осы матрицаның к2 кілті бойынша оқығанда пайда болады.

Мысал 2. Ашық текст: **“ШИФРОВАНИЕ_ПЕРЕСТАНОВКОЙ”.**
Төрт бағаннан тұратын матрицаға бөлеміз.
Кілттер: к1: **5 – 3 – 1 – 2 – 4 – 6**; к2: **4 – 2 – 3 – 1.**
Бастапқы матрица:

Ш	**И**	**Ф**	**Р**
О	**В**	**А**	**Н**
И	**Е**	**_**	**П**
Е	**Р**	**Е**	**С**
Т	**А**	**Н**	**О**
В	**К**	**О**	**Й**

Енді бастапқы матрицаның жолдарын к1 кілті бойынша орналастырамыз: **1-5, 2-3, 3-1, 4-2, 5-4, 6-6.**
Шифрланған матрица алынады:

	1	**2**	**3**	**4**
1	**И**	**Е**	**_**	**П**
2	**Е**	**Р**	**Е**	**С**
3	**О**	**В**	**А**	**Н**
4	**Т**	**А**	**Н**	**О**
5	**Ш**	**И**	**Ф**	**Р**
6	**В**	**К**	**О**	**Й**

Бұдан кейін шифрланған матрицаның бағандарын к2 кілтіне сәйкес жазамыз, яғни бірінші 4-бағанды жолға, сосын 2-бағанды жолға жалғастырып, 3-бағанды жолға жалғастырып, 1-бағанды жолға жалғастырып жазып, нәтижесінде аламыз:
Шифртекст: **“ПСНОРЙЕРВАИК_ЕАНФОИЕОТШВ”.**

№2 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Симметриясыз шифрлеу жүйелерін зерттеу
Алмастыру әдісі

Жұмыс мақсаты:

Криптографиялық алмастыру әдісімен танысу және оны қолдана білу.

Теориялық мәліметтер.

Алмастыру әдісі бойынша бір алфавитте жазылған бастапқы мәтін символдары белгілі кілт бойынша өзге алфавит символдарымен алмасады. Қарапайым алмастыру әдістерінің бірі ретінде бастапқы символды алмастырулар векторы бойынша символ эквивалентіне тікелей алмастыруды қарастыруға болады.

Шифрлаудың алмастыру әдісі алгебралық амалдарға негізделген. Криптографияда алмастыру әдісінің 4 түрі бар: моноалфавиттік, гомофеникалық, полиалфавиттік және полиграммдық.

Вижинер шифрлау жүйесі моноалфавиттік түріне жатады.

Жалпы формуласы: $y_i = k1 * x_i + k2$ ***(mod N)***

Мұндағы: y_i – алфавит символы, $k1, k2$ – тұрақтылар, x_i – ашық мәтін символы, *N* – алфавиттегі символдар саны.

Мысалы: ашық мәтін **«Замена»**

Кілт: **«Ключ»**

З	А	М	Е	Н	А
К	Л	Ю	Ч	К	Л

$У_1$=8 + 11 (mod 33) = 19 Т

$У_2$=1 + 12 (mod 33) = 13 М

$У_3$=13 + 31 (mod 33) = 11 К

$У_4$=6 +24 (mod 33) = 30 Э

$У_5$=14 + 11 (mod 33) = 25 Ш

$У_6$=1 +12 (mod 33) = 13 М

Шифрмәтін: **ТМКЭШМ**

Ашық мәтіннің өзі немесе шифрмәтін «кілт» ретінде қолданылатын шифр – автокілттік шифр деп аталады. Шифрлау үшін ағымдық мәтін символдарының реттік номерлері кілт символдарының реттік номерлерімен қосылады, осыдан код алынады. Мысалы:

Мәтін:
Кілт:

З	А	М	Е	Н	А
К	Л	Ю	Ч	К	Л

Нәтиже - код: **18 13 44 30 25 13**

№3 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Кодтау әдісі

Жұмыстың мақсаты:

Кодтау әдістерімен танысу және қолдана білу.

Теориялық мәліметтер.

Кодтау дегеніміз ағымдық мәтін әріптерін кодтармен алмастыру. Кодтау символдық және мәндік болады. Символдық кодтау кезінде ашық мәтіннің әрбір әріпі сәйкесінше кодқа алмастырылады.

Символдық кодтау әдісін Рябко ұсынған. Мысалы, А алфавитімен берілген Х хабарламаны жіберу қажет болсын. Алфавиттің әріптері 1,2,3, ... сандарымен сәйкестендірілген. Әрбір әріпке $К_i$ коды сәйкес келеді. Х хабарламасының әріпі $Х_j$ болғанда, оның коды j позициясының реттік кодымен көрсетіледі. Кері жағдайда j позициясының реттік коды арқылы $Х_j$ әріпін анықтауға болады.

Бөліп/тарату әдісі бойынша бір файл ішіндегі ақпарат бірнеше блоктарға бөлінеді. Осы блоктар бірнеше файлдарға жазылады. Бұл файлдар таратылған түрінде ешқандай ақпарат бермейді. Мысалы, ашық мәтінді 8 блокқа бөліп тастайық. Ол үшін 2 қатар және 4 баған таңдалады. S_j бағандары {4,1,3,2} ретінде, қатарлар {2,1} ретінде таңдалады. Ашық мәтіннің келесі символы жазылатын блок келесі формуламен анықталады:

$$K = (r_i - 1) * n + S_i$$

мұндағы n – баған саны.

№1, №2, №3 зертханалық жұмыстарға тапсырмалар нұсқалары

Нұсқа №	Ағымдағы мәтін	Код
1.	Защита информации	12386574
2.	Компьютерная преступность	72165438
3.	Государственная тайна	18534672
4.	Общественная организация	12465387
5.	Электронные средства	34512678
6.	Банковские платежи	67432158
7.	Организованная преступность	56731482
8.	Компьютерное мошенничество	85724631
9.	Компьютерный подлог	15876432
10.	Повреждение информации	38152764
11.	Уголовноправовые отношения	72154836
12.	Частное учреждение	13267548
13.	Экономические преступления	15843762
14.	Коллективная безопасность	28364571
15.	Навигационный комьютер	38467125
16.	Компьтерная махинация	32415687
17.	Несанкциоированный доступ	14287653
18.	Компьютерная программа	23658741
19.	Финансовые документы	18532476
20.	Личная безопасность	74523861

Тапсырманы орындау нұсқасы

1. Есептің берілгені:
Вариант бойынша мәтінді шифрлау қажет.

2. Кез-келген бағдарламалау тілінде немесе бағдарламалау ортасында берілген мәтінді ширфлайтын бағдарлама құру.

3. Бағдарлама нәтижесін ауызша есептеген нәтижемен салыстыру.

№4 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Симметриялы емес шифрлау

Жұмыстың мақсаты:

Симметриялы емес шифрлау және дешифрлау әдістерін қолдана білу.

Теориялық мәліметтер.

Симметриялы емес жүйелер ашық кілтті жүйелер деп те аталады. Мұндай жүйелерде шифрлау үшін 1 кілт, ал дешифрлау үшін өзге кілт пайдаланылады. Қазіргі кезде ең дамыған ашық кілтті жүйе RSA шифрлау жүйесі болып табылады. RSA алгоритімін пайдалану үшін келесі қадамдарды орындау қажет.

1. p және q екі жай сандары таңдалады.
2. n саны p мен q көбейтіндісі ретінде анықталады. **(n=p*q)**
3. Кездейсоқ d үлкен саны таңдалады. Ол сан **(p-1)*(q-1)** көбейтіндісімен өзара жай болуы тиіс.
4. Келесі қатынас ақиқат болатындай e саны таңдалады:

e*d*mod((p-1)*(q-1))=1

5. e, n сандарын ашық кілт, d, n сандарын құпия кілт деп атайды.

Ары қарай {e, n} кілті бойынша берілгендерді шифрлау үшін ағымдық мәтін блоктарға бөлінеді. Блоктардың әрқайсысы

M(i)=0, 1, ..., n-1 саны түрінде көрсетілуі тиіс.

Мәтінді $C(i)=M(i)^e * mod(n)$ формуласы бойынша шифрлайды. Дешифлау үшін $M(i) = C(i)^d * mod(n)$ формуласы қолданылады.

Тапсырмалардың нұсқалары

RSA шифрлау жүйесі бойынша келесі мәтіндерді шифрлау қажет. Тапсырма варианты студенттік билеттің соңғы санымен анықталады. (i – алдыңғы сан, j - соңғы сан).

i – номері бойынша шифрланатын сөз таңдалады, j – номері, (p, q) сандарында осы алгоритмді жүзеге асыру.

i:	0.	БЕДА	6.	БЕГ
	1.	ДЕВАК	7.	ГИВ
	2.	ЗАБАВА	8.	ЕДА
	3.	КАБАК	6.	ГАД
	4.	БАГАЖ		
	5.	БИВАК		
j:	0.	(7,17)	6.	(5,11)
	1.	(5,7)	7.	(7,13)
	2.	(3,11)	8.	(11,17)
	3.	(11,13)	6.	(5,13)
	4.	(13,17)		
	5.	(3,7)		

Тапсырманы орындау нұсқасы

Студенттік билеттің соңғы саны j = 2, яғни p = 3; q = 11; ал соңғыдан алдыңғы сан i = 6, демек шифрланатын мәтін БЕГ. n санын есептейік:

$n = p * q = 3 * 11 = 33$

$(p - 1) * (q - 1) = (3 - 1) * (11 - 1) = 2 * 10 = 20$

d = 3 деп таңдап алып, e санын табамыз;

$e * d * \text{mod}((p - 1) * (q - 1)) = 1$

$e * 3 * \text{mod}(20) = 1, \quad e = 7.$

Шифрланатын мәтін 2 6 4 сандарының тізбегі ретінде көрсетеміз. Өйткені БЕГ сөзінде алфавиттегі әріп номерлері 2 6 4. Ашық кілт бойынша шифрлаймыз:

$C(i) = M(i)^e * \text{mod}(n);$

$C_1 = 2^7 * \text{mod}(33) = 128 \text{ mod}(33) = 29$

$C_2 = 6^7 * \text{mod}(33) = 279936 \text{ mod}(33) = 30$

$C_3 = 4^7 * \text{mod}(33) = 16\,384 \text{ mod}(33) = 16$

Алынған шифрмәтін: 29 30 16

Шифрмәтінді ашу үшін { 3, 33 } жасырын кілтті пайдаланамыз:

$M(i) = C(i)^d * \text{mod}(n);$

$M_1 = 29^3 * \text{mod}(33) = 24389 \text{ mod}(33) = 2;$

$M_2 = 30^3 * \text{mod}(33) = 27\,000 \text{ mod}(33) = 6;$

$M_3 = 16^3 * \text{mod}(33) = 4096 \text{ mod}(33) = 4;$

Нәтижесінде келесі хабарлама алынады: 2 6 4

Б Е Г

№5 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Кілт бойынша бірлік орын алмастыру.
Трисемус шифрлаушы кестелері

Мақсаты: Мәтіндерді шифрлаудың кілт бойынша бірлік орын алмастыру, Трисемус шифрлаушы кестелерін пайдалану.

Тапсырмалардың нұсқаулары.

1. ТАБЛИЧНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ сөзін ФОРМУЛА кілтімен кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
2. ВСПОМАГАТЕЛЬНЫЕ И ВСТРОЕННЫЕ ПРИЛОЖЕНИЯ ИНТЕРНЕТА сөзін ФАЙЛ кілтімен кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
3. РАДИУС кілттік сөзі бойынша ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МИКРОЭВМ мәтінін кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
4. СТОП кілттік сөзі бойынша СТРОИТЕЛЬСТВО ПИРАМИДЫ ИЗ ШАРОВ мәтінін кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
5. ЦИКЛ С ПРЕДВАРИТЕЛЬНЫМ УСЛОВИЕМ мәтінін Трисемус шифрлаушы кестелері бойынша шифрлаңыз.
6. ОПЕРАЦИОННАЯ СИСТЕМА мәтінін Трисемус шифрлаушы кестелері бойынша БАЯН кілттік сөзі арқылы шифрлаңыз.
7. ВИРУС кілттік сөзі арқылы КОМПЬЮТЕРНАЯ - ПРЕСТУПНОСТЬ мәтінін кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
8. УШНИК кілттік сөзімен СКРЫТОНОСИМЫЙ МИКРОФОН ЭКМ9 мәтінін кілт бойынша бірлік орын алмастыру көмегімен шифрлаңыз.
9. КЛАСС кілттік сөзімен ЕДИНОЕ НАЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ мәтінін кілт бойынша бірлік орын алмастыру әдісімен шифрлаңыз.
10. АДМИНИСТРАТИВНЫЙ ПРЕССИНГ мәтінін БАЯН кілтімен кілт бойынша бірлік орын алмастыру арқылы шифрлаңыз.
11. КОМПЬЮТЕРНАЯ И ВЕКТОРНАЯ ГРАФИКА мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
12. ТАБЛИЧНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
13. ЛИТЕРАТУРНОЕ РЕДАКТИРОВАНИЕ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
14. ОПРЕРАТОР ПРИСВАЕВАНИЯ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
15. АППАРАТНОЕ ОБЕСПЕЧЕНИЕ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
16. МАТЕМАТИЧЕСКАЯ ФОРМУЛИРОВКА ЗАДАЧИ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
17. НЕСООТВЕТСТВИЕ КОНСТРУКЦИИ В ПРОГРАММЕ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
18. ТАБЛИЧНЫЕ ПРОЦЕССОРЫ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері арқылы шифрлаңыз.

19. ЭКОНОМИЧЕСКАЯ ИНФОРМАТИКА мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.
20. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ мәтінін БАЯН кілтімен Трисемус шифрлаушы кестелері көмегімен шифрлаңыз.

№6 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Плейфейр биграммалық шифрлау жүйесі.
Гронсфельд шифры

Мақсаты: Мәтіндерді шифрлаудың Плейфейр биграммалық шифрлау жүйесін және Гронфельд шифрларын қолдана білу.

Тапсырмалардың нұсқаулары.

1. АЛГОРИТМ СУММИРОВАННИЯ И ТАБУЛИРОВАНИЯ АСТ мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
2. МАТЕМАТИЧЕСКАЯ ФОРМУЛИРОВКА ЗАДАЧИ мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
3. АСПЕКТЫ РЕШЕНИЯ ЗАДАЧ НА ЭВМ мәтінін 79683 кілті бойынша Гронсфельд шифры көмегімен шифрлаңыз.
4. НЕСООТВЕТСВИЕ КОНСТРУКЦИИ В ПРОГРАММЕ мәтінін 82591 кілті бойынша Гронсфельд шифры көмегімен шифрлаңыз.
5. ПРЕКТИРОВАНИЯ ИС мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
6. ОПЕРАТОР ПРИСВАИВАНИЯ мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
7. ОПЕРАЦИОННАЯ СИСТЕМА мәтінін 83679 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
8. ТАБЛИЧНОЕ ПРЕДСТАВЛЕНИЕ ДАННЫХ мәтінін 29787 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
9. ЛИТЕРАТУРНОЕ РЕДАКТИРОВАНИЕ мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрмәтінге айналдырыңыз.
10. ВСПОМАГАТЕЛЬНЫЕ И ВСТРОЕННЫЕ ПРИЛОЖЕНИЯ ИНТЕРНЕТА мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
11. КОМПЬЮТЕРНАЯ И ВЕКТОРНАЯ ГРАФИКА мәтінін 62973 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
12. ЭКОНОМИЧЕСКАЯ ИНФОРМАТИКА мәтінін 921578 кілтімен Гронсфельд шифрлау жүйесі көмегімен шифрлаңыз.
13. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрмәтінге айналдырыңыз.
14. МЕТОДИЧЕСКОЕ УКАЗАНИЕ мәтінін 6453279 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
15. СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА мәтінін 182937 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
16. КЛЮЧ НА ПЕРВОЙ ЯЧЕЙКЕ СПРАВА мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
17. ПРОГРАММИРОВАНИЕ ИГР мәтінін БАЯН кілтімен Плейфейр биграммалық шифрлау жүйесі бойынша шифрлаңыз.
18. ВСПОМАГАТЕЛЬНЫЕ И ВСТРОЕННЫЕ ПРИЛОЖЕНИЯ ИНТЕРНЕТА мәтінін 148765 кілтімен Гронсфельд шифрлау жүйесімен шифрлаңыз.

19. СТАТИСТИЧЕСКИЕ И ЛОГИЧЕСКИЕ ФУНКЦИИ мәтінін 873659 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.
20. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ мәтінін 443785 кілтімен Гронсфельд шифрлау жүйесі бойынша шифрлаңыз.

№7 ЗЕРТХАНАЛЫҚ ЖҰМЫС
Дешифрлауды орындау

Мақсаты: Белгілі бір шифрлау жүйесі көмегімен жасалған шифрмәтінді кері қарай дешифлау әрекетін орындай білу.

Тапсырмалардың нұсқаулары.

1. НОДЙИФУПТФЬФОЛПВРГКЭДПЕМРКОЛПВРГКЭРК шифрмәтінінен Плейфейр жүйесін қолданып бастапқы хабарламаны анықтаңыз.
2. БПДУБПЖФБЪГЦЛШРХБФЯЦФИАЙЛВЕВЕНЬЭ шифрмәтінінен Плейфейр жүйесін қолданып бастапқы хабарламаны анықтаңыз.
3. ЗЬХННЩДЦНПМЦОЗКЗНЖЯРЗЖИФ шифрмәтінінен 76683 кілтімен Гронсфельд шифрын қолданып бастапқы шифрмәтінді анықтаңыз.
4. ХЗЦТЦФЗЙЬУЧЖРЗПТХУЧФЫМЫМРДФФЦЕХДФОК шифрмәтінінен 8254 кілтімен Гронсфельд шифрын пайдаланып, ағымдық мәтінді анықтаңыз.
5. НИДИЕВТНЕСЧПЛАЫДТНРЕБХААОЕНЛ шифрмәтінінен ФОРМУЛА кілті бойынша бірлік орын алмастыру арқылы ағымдық мәтінді анықтаңыз.
6. ФЗКУОЩФЧНХТМНЩШВЙФНУКМНИУПВНЮ ширфмәтінін 27986 кілтін пайдаланып Гронсфельд шифрф көмегімен ағымдық мәтінге айналдырыңыз.
7. ВЕТИРСЫРНИЛЬОГЛОНЕЕОМЫНРЖОЕННЕГИЫЕНАВЕТИТСПАЯ шифрмәтінін ФАЙЛ кілтімен кілт бойынша бірлік орын алмастыру көмегімен шифрлаңыз.
8. ГХЧФУУДОЬЛТЯОЯНОЙЦУФЦЛФТЪЙЧЦПРПКНУПДЙСЬЛЧТЖЦИ шифрмәтінін 148675 кілтімен Гронсфельд шифры көмегімен ағымдық мәтінге айналдырыңыз.
9. ЯФЦКЩШИЗЖПВИФПЗКМПДЧЪЩКЙПФЗЧ шифрмәтінінен Трисемус шифрлаушы кестелері көмегімен ағымдық мәтінді анықтаңыз.
10. АХРОПЛОАФГФПВЙГНДКЭ шифрмәтінінен Трисемус шифрлаушы кестелері көмегімен ағымдық мәтінді анықтаңыз.
11. ЦРКЧЙЮЙУФИАЦПЬЬЖСЗ шифрмәтінін 148765 кілтімен Гронсфельд шифры көмегімен ағымдық мәтінді анықтаңыз.
12. АЕППРИМОЕРОЕМБЧОЭМНЕЕГВИОСНРМК шифрмәтінін РАДИУС кілті бойынша кілтпен бірлік орын алмастыру арқылы бастапқы хабарламаға айналдырыңыз.
13. ИИСЛРЗТЬАШОСМАОТИРИВДОТОЫВЕП шифрмәтінін СТОП кілтімен кілт бойынша бірлік орын алмастыру арқылы дешифрлаңыз.
14. САЕВТДСНРМСЫАИИЙТННПИИГР шифрмәтінін БАЯН кілтімен кілт бойынша бірлік орын алмастыру арқылы дешифрлаңыз.
15. АЕНОТЛДАВЕЬИЦАСННИНТОООИИЕЕНЕР шифрмәтінін КЛАСС кілтімен кілт бойынша бірлік орын алмастыру арқылы дешифрлаңыз.
16. КНМСОРЭЫКНОКИРОФММЫСО9ИТИ шифрмәтінін УШНИК кілтімен кілт бойынша бірлік орын алмастыру арқылы дешифрлаңыз.
17. РУХРЮДЧООСЖДСГИРЧЧССЖДМСДЬНУБ шифрмәтінін 65914 кілтімен Гронсфельд шифры бойынша дешифрлаңыз.
18. ПЕНЮЧКЗЩТБ : : ГЖЗНС . шифрмәтінін Уистон “Екілік квадрат” шифры бойынша дешифрлаңыз.

19. БЮМЫЧКЬАГК.ЧЯ_АДХРЬЕ . . шифрмәтінін Уистон “Екілік квадрат” шифры бойынша дешифрлаңыз.
20. ХГТЬЧКИДЕХРФЬЗМЫАВРЭЕС . . ДУЖМ шифрмәтінін Уистон “Екілік квадрат” шифры бойынша дешифрлаңыз.

Өзіндік жұмыстарға арналған тапсырмалар

Тақырып: Қарапайым ауыстыру шифрлары

Вариант №1.

А бөлімінде шифрланған хабарлама Б бөліміне 12 символдан тұратын кесінділерге бөлініп жіберіледі. Хабарлама қарапайым ауыстыру шифры бойынша шифрланған және орыс тілі алфавитінің әріптері мен бос орыннан (_) тұрады. Хабарламаны жіберген кезде алдымен жұп орындарда тұрған символдар, кейіннен тақ орындарда тұрған символдар жіберіледі. В бөлімінде алынған хабарлама дәл сол алфавиттегі өзге қарапайым ауыстыру шифрымен шифрланады. В бөлімінде алынған кесінділер:

С	**О**	**_**	**Г**	**Ж**	**Т**	**П**	**Н**	**Б**	**Л**	**Ж**	**О**
Р	**С**	**Т**	**К**	**Д**	**К**	**С**	**П**	**Х**	**Е**	**У**	**Б**
_	**Е**	**_**	**П**	**Ф**	**П**	**У**	**Б**	**_**	**Ю**	**О**	**Б**
С	**П**	**_**	**Е**	**О**	**К**	**Ж**	**У**	**У**	**Л**	**Ж**	**Л**
С	**М**	**Ц**	**Х**	**Б**	**Э**	**К**	**Г**	**О**	**Щ**	**П**	**Ы**
У	**Л**	**К**	**Л**	**__**	**И**	**К**	**Н**	**Т**	**Л**	**Ж**	**Г**

бойынша бастапқы хабарламаны анықтаңыз.

Вариант №2.

Орыс алфавиті әріптері мен бос орыннан тұратын (_) хабарлама сандық түрге ауыстырылды, мұндағы әрбір әріп сандар жұбына келесі кесте бойынша сәйкестендірілген:

А	**Б**	**В**	**Г**	**Д**	**Е**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**
01	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
	2	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Р	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ь**	**Ы**	**Э**	**Ю**	**Я**	**_**
1	**1**	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**3**	**3**	**3**
7	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**

Шифрлау кезінде хабарламаның әрбір саны кесіндінің сәйкес санымен қосылады және алынған қосындының соңғы санына ауыстырылады. Хабарламаны анықтаңыз:

233986721645816067061731558 8

Вариант №3.

12 2 24 5 3 21 6 29 28 2 20 18 20 21 5 10 27 17 2 11 2 16
19 2 27 5 8 29 12 31 22 2 16, 19 2 * 19 5 17 29 8 29 6
2916:
8 2 19 19 29 10 19 29 14 19 29 29 19 10 2 24 11 216
10 14 18 21 17 2 20 2 28 29 16 21 29 28 6 29 16.

Криптограммасы әріптерді сандарға (1-ден 32-ге дейін) ауыстыру арқылы алынған, мұндағы әртүрлі әріптерге әртүрлі сандар сәйкестендіріледі. Жеке сөздер бірнеше бос орындар арқылы, әріптер 1 бос орын арқылы бөлінген. «е» және «ё» әріптері бір болып есептеледі. **В.Высоцкийдің өлеңін оқыңыздар.**

Вариант №4.

А Б В Г Д Е Ё Ж З И Й К Л М М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я орыс алфавитінің әріптерін басатын телетайпты тексеру үшін 9 сөзден тұратын хабарлама берілген. Телетайптың дұрыс істемеуінің арқасында қабылдау бөлімінде келесі сөздер алынған:

ГЪЙ АЭЕ БПРК ЕЖЩЮ НМЬЧ СЫЛЗ ШДУ ЦХОТ ЯФВИ. Бастапқы мәтінді анықтаңыз. Мұнда әрбір әріп алфавиттегі өзінен кейін тұрған 2 әріппен алмастырылған. Мысалы, Б әріпі {А,Б,В,Г} әріптерінің біріне ауыстырылған болуы мүмкін.

Шифрлаушы кестелер

Вариант №1.

6х10 тор көздерден тұратын тіктөртбұрышты трафарет шифрдың кілті болып табылады. Трафареттің 15 тор көзі, оны 6х10 өлшемі параққа 4 түрлі әдіспен қойғанда барлық кесінділер толығымен жабылатындай етіп кесілген.

Хабарламаның әріптері (бос орынсыз) трафарет кесінділеріне әрбір оның мүмкін әдісіне сәйкес тізбектеліп жазылады. Шифрлаудан кейін парақ бетінде келесі мәтін жазылған болса, бастапқы мәтінді оқыңыз:

Р	**П**	**Т**	**Е**	**Ш**	**А**	**В**	**Е**	**С**	**Л**
0	**Я**	**Т**	**А**	**Л**	**_**	**Ь**	**З**	**Т**	**_**
_	**У**	**К**	**Т**	**_**	**Я**	**А**	**Ь**	**_**	**С**
Н	**П**	**_**	**Ь**	**Е**	**У**	**_**	**Ш**	**Л**	**С**
Т	**И**	**Ь**	**З**	**Ы**	**Я**	**Е**	**М**	**_**	**О**
_	**Е**	**Ф**	**_**	**_**	**Р**	**0**	**_**	**С**	**М**

Вариант №2

Хабарлама 20 бағаннан тұратын кестеге жол бойымен жазылған. Мұнда әрбір тор көзге хабарламаның бір әріпі жазылған, бос орындар алынып тасталған, ал үтір орнына ЗПТ, нүкте орнына ТЧК белгілеулері енгізілген. Сонан соң кесте бағандары қандай да бір әдіспен орын ауыстырылған, нәтижесінде келесі мәтін алынған:

Я	**Н**	**Л**	**В**	**К**	**Р**	**А**	**Д**	**О**	**Е**	**Т**	**Е**	**Р**	**Г**	**О**	**М**	**И**	**З**	**Я**	**Е**
Й	**Л**	**Т**	**А**	**Л**	**Ф**	**Ы**	**И**	**П**	**Е**	**У**	**И**	**О**	**О**	**Г**	**Е**	**Д**	**Б**	**О**	**Р**
Ч	**Р**	**Д**	**Ч**	**И**	**Е**	**С**	**М**	**О**	**Н**	**Д**	**К**	**Х**	**И**	**Н**	**Г**	**И**	**К**	**Е**	**О**
Н	**У**	**Л**	**А**	**Е**	**Р**	**Е**	**Б**	**Ы**	**Ы**	**Е**	**Е**	**З**	**И**	**О**	**Н**	**Н**	**Ы**	**Ч**	**Д**
Ы	**Т**	**Д**	**О**	**Е**	**М**	**П**	**П**	**Т**	**Щ**	**В**	**А**	**Н**	**И**	**П**	**Т**	**Я**	**З**	**С**	**Л**
И	**К**	**С**	**И**	**_**	**Т**	**Ч**	**Н**	**О**	**_**	**_**	**Е**	**_**	**Л**	**У**	**Л**	**_**	**Т**	**_**	**Ж**

Бастапқы хабарламаны оқыңыз.

Алмастыру әдістері

Вариант №1.

ФН*6і=ФАФ
+ * -
ЕЕ+Е=НЗ
= = =
ИША+МР=ИМН

Криптограммасы берілген. Әріптердің берілген теңдіктер орындалатындай сандық мәндерін тұрғызыңыз.Әрбір әріпке әртүрлі сандар сәйкес келеді. Әріптерді олардың сандық мәндерінің өсу ретіне қарай орналастырыңыз және бастапқы хабарламаны оқыңыз.

Вариант №2.

Атақты математик Леонард Эйлер 1759 жылы шахмат тақтасының барлық торкөздерін «ат» жүрісі бойынша бір реттен жүріп шығудың түйық жолын тапты.

Д	Л	Р	И	Л	П	Н	Б
У	К	А	О	Т	У	С	Т
О	0	0	А	Н	0	И	Р
Т	Б	Г	К	Т	Т	У	К
К	О	Е	0	Р	А	В	0
К	Л	Г	П	В	Л	Е	Т
Т	А	Н	Р	М	А	Г	0
Е	А	О	В	И	Д	У	Л

Шахмат тақтасының тор көздеріне осы әдіспен жазылған мәтінді оқыңыз. Мәтіннің алғашқы әріпі а4 - тен басталады.

Вариант №3.

Хабарлама 20 бағаннан тұратын кестеге жазылған. Мұнда, әрбір торкөзге хабарламаның бір әріпі жазылады.Сөздер арасындағы бос орындар есепке алынбайды, ал тыныс белгілері шартты белгілермен ауыстырылған: нүкте -ТЧК, үтір-ЗПТ. Сонан соң кесте бағаналары қандай бір әдіспен орын ауыстырылған, нәтижесінде келесі мәтін алынған:

Я Н Л В К Р А Д О Е Т Е Р Г О М И З Я Е
Й Л Т А Л Ф Ы И П Е У И О О Г Е Д Б О Р
Ч Р Д Ч И Е С М О Н Д К Х И Н Г И К Е О
Н У Л А Е Р Е Б Ы Ы Е Е З И О Н Н Ы Ч Д
Ы Т Д О Е М П П Т Щ В А Н И П Т Я З С Л

И К С И _ Т Ч Н О _ _ Е _ Л У Л _ Т _ Ж
Бастапқы хабарламаны оқыңыз.

Желілерді қорғау

Вариант №1.

1997 абоненттен тұратын байланыс жүйесінде әрбір абонент N өзгелерімен байланысқан. N-ның мүмкін болатын мәндерін анықтаңыз.

Вариант №2.

Компьютерлік желіде цифрлардан тұратын парольдер қолданылады. Парольдерді ұрлаудан сақтау үшін дискте шифрланған түрде сақтайды. Пайдалану қажеттігі туған кезде сәйкес парольді бір мәнді кері шифрлау жасалады. Парольды шифрлауға, символдар бойынша, бір ғана түрлендіру қолданылады. Алғашқы цифр өзгеріссіз қалады, ал әрбір кейінгі цифрдың шифрлану нәтижесі тек өзіне және алдыңғы тұрған цифрға тәуелді болады.

Шифрланған парольдер тізімі белгілі:
4249188780319, 4245133784397, 5393511, 428540012393, 4262271910365, 4252370031465, 4245133784735 және осы тізімде шифрланған екі пароль 4208212275831, 4242592823026. Мұнан өзге парольдерді анықтауға бола ма? Егер болса, онда оларды құрастырыңыз.

Вариант №3.

АБВГДЖЗИКЛМНОПРСТУФЦХЧШЩЬЫЭЮЯ алфавитінде жазылған хабарлама осы алфавиттің әріптерінің тізімі көмегімен шифрланады. Тізбек ұзындығы хабарлама ұзындығына тең. Ағымдық хабарламаның әрбір әріпін шифрлау, оның алфавиттегі реттік номерін сәйкес шифрланушы тізбектің әрпінің реттік номеріне қосудан тұрады.

Тест сұрақтары мен жауаптары

1. Ашық текстің бөгде адамдарға мағынасын түсінбеу үшін жасалынатын өзгерту процесі қалай аталады ?
   а) шифрлау
   б) дешифрлау
   в) кері шифрлау
   г) криптография
2. Шифртекстті ашық текстке өзгерту процесі?
   а) дешифрлау
   б) шифрлау
   в) цифрлау
   г) решифрлау
3. Шифрлау нәтижесінде берілген хабар неге айналады?
   а) шифртекстке
   б) ашық текстке
   в) шифралфавитке
   г) ашық алфавитке
4. Шығысында C болу үшін E шифр функциясының кірісіне P берілсін. Математикалық тілде осы белгілеулер қалай жазылады?
   а) E(P)=C
   б) E(C)=P
   в) P(E)=C
   г) C(P)=E
5. Кері шифрлау жағдайында D кері ширлау функциясының кірісінде C, шығысында P болса, математикалық тілде осы белгілеу қалай жазылады?
   а) D(C)=P
   б) D(P)=C
   в) C(P)=D
   г) D(P)=C
6. Ақпараттың, деректердің мағынасын құпия түрде қалай сақтау керектігін оқытатын ғылым?
   а) криптография
   б) криптология
   в) криптоанализ
   г) криптожүйе
7. Ақпаратты өзгеріске келтіре отырып оны қорғау мәселесімен не айналысады?

а) криптология б) криптоанализ в) криптография
г) криптожүйе д) барлығы дұрыс

8. Ешқандай да кілтсіз ақпараттың шифрын ашудың мүмкіндіктерін қандай ғылым зерттейді?

а) криптоанализ б) криптография в) криптология
г) криптоберіктілік д) дұрыс жауабы жоқ

9. Криптография құрамына кіретін бөлім?

а) берілген жауаптың барлығы дұрыс б) симметриялықкриптожүйе
в) ашық кілттік криптожүйе г) электронды жазба жүйесі
д) кілттерді басқару
10. Криптографиялық әдістерді қолданудың негізгі бағыттары?
а) барлық жауабы дұрыс
б) құпия ақпараттардың байланыс каналдары арқылы берілуі
в) берілетін ақпараттың түпнұсқасын құру
г) түрлі тасымалдағыштарда ақпаратты шифрланған күйінде сақтау
д) электронды почта арқыла құпия ақпараттарының берілуі
11. Алфавит дегеніміз не ?
а) ақпараттарды кодтау үшін қолданылатын белгілер жиынтығы
б) кез-келген ретпен орналасқан белгілер жиынтығы
в) алфавит элементтерінің реттелген жиынтығы
г) символдар жиынтығы д) барлық жауабы дұрыс
12. Қазіргі кездегі жаңа ақпараттық жүйеде қолданылатын алфавит ?
а) барлық жауабы дұрыс б) алфавит z33 в) алфавит z256
г) бинарлық алфавит д) сегіздік және он алтылық алфавит
13. ASCII стандартты кодына кіретін символдар қай алфавиттің құрамына кіреді ?
а) алфавит z256-мың б) бинарлық алфавиттің в)алфавит z33-тің
г) сегіздік және он алтылық алфавиттің д) дұрыс жауабы жоқ
14. Алфавит элементтерінің реттелген жиынтығы ?
а) текст б) жүйе в) қатар
г) символдар д) барлық жауабы дұрыс
15. Классикалық криптографияда алмастыру шифрінің түрі ?
а) барлық жауабы дұрыс б) омофонды алмастыру
в) көп алфавитті алмастыру г) блоктап алмастыру
д) жай алмастыру
16. Ашық текстің әр әрпіне шифртексттен бірнеше символдың қойылуы алмастырудың қай түріне жатады ?
а) омофонды алмастыру б) көп алфавитті алмастыру
в) блоктап алмастыру г) жай алмастыру д) дұрыс жауабы жоқ
17. Ашықтексттің әр әрпінің шифртексттің сол символына алмастырылуы алмастырудың қай түріне жатады ?
а) дұрыс жауабы жоқ б) көп алфавитті алмастыру
в) орын ауыстыру г) блоктап алмастыру д) омофонды алмастыру
18. “АБА”- “РТК” шифрлану алмастырудың қай түріне жатады ?
а) блоктап алмастыру б) омофонды алмастыру
в) жай алмастыру г) орын ауыстыру д) көп алфавит алмастыру
19. “А” әрпіне – “5,13,25 немесе 57” алмастырылуы алмастырудың қай түріне жатады?
а) дұрыс жауабы жоқ б) орын ауыстыру в) блоктап алмастыру
г) көп цифрлы алмастыру д) көп алфавитті алмастыру
20. “Б”әрпіне- “7,19,31 немесе 43” алмастырылуы алмастырудың қай түріне жатады ?
а) омофонды алмастыру б) блоктап алмастыру

в) көп алфавитті алмастыру г) көп цифрлы алмастыру
д) дұрыс жауабы жоқ
21. Классикалық криптографияда алмастыру шифрінің неше түрі бар?
а) 4 б) 2 в) 3 г) 5 д) олардың түрі өте көп
22. Ашықтекстің әр әрпінің шифртекстің сол символына алмастырылуы алмастырудың қай түріне жатады ?
а) бір алфавитті алмастыру б) омофонды алмастыру
в) блоктап алмастыру г) көп алфавитті алмастыру
д) дұрыс жауабы жоқ
23.Орын ауыстыру дегеніміз не ?
а) ашықтекст әріптерінің орналасу ретінің ауысуы
б) ашықтекстің әр әрпінің шифртекстің сол символына ауыстырылуы
в) ашықтекстің блоктап шифрлануы г) барлық жауабы дұрыс
д) ашықтекстің әр әрпінің шифрланған тексттің символына орнын ауыстыру алгоритімдік шифры
24. Ашықтекст әріптерінің орналасу ретінің ауысуы қалай аталады ?
а) орын ауыстыру б) орын алмастыру в) жәй алмастыру
г) омофонды алмастыру д) көп алфавитті алмастыру
25. Симметриялық криптожүйеде шифрлау үшін қанша кілт қолданады?
а) 1 б) 2 в) 3 г) 4 д) кілтсіз ширланады
26. Ашық кілтті криптожүйеде шифрлау үшін неше кілт қолданылады?
а) 2 б) 1 в) 3 г) 4 д) бұл жүйеде шифрлау үшін кілт қолданылмайды
27. 2 кілтті қолданып шифрлау криптожүйенің қай түріне тән?
а) ашық кілтті криптожүйе б) симметриялық криптожүйе
в) жабық кілтті криптожүйе г) симметриялық емес криптожүйе
д) барлық жауабы дұрыс
28. Кілт дегеніміз не?
а) барлық жауабы дұрыс
б) ешқандай кедергісіз тексттердің шифрлауға қажетті ақпарат
в) ешқандай кедергісіз тексттерді дешифрлауға қажетті ақпарат
г) ешқандай кедергісіз тексттеуді кері шифрлауға қажетті ақпарат
д) алвавит әріптерінің тізбектелген реті
29. Ашық кілтті криптожүйеде ақпараттың шифрын ашу үшін қандай кілт қолданылады?
а) жабық кілт б) ашық кілт в) симметриялы кілт
г) цифрлық кілт д) дұрыс жаубы жоқ
30. Шифрдің кілтсіз дешифрлау әрекетіне шыдамдылығын анықтайтын мінездемесі?
а) криптоберіктілік б) электронды жазба в) криптожүйе
г) криптографя д) криптоанализ
31. Текстi қабылдаған өзге пайдаланушы арқылы ақпараттың авторлығын және түпнұсқасын тексеруге мүмкіндік беретін криптографиялық өзгерту?
а) цифрлық жазба б) криптоберіктілік в) криптоанализ
г) криптожүйе д) дұрыс жауабы жоқ

32. Қазіргі кезде жаңа ақпаратты қорғау криптожүйелері үшін қандай талап қойылады?
а) барлық жауабы дұрыс
б) кілт бар болған жағдайда ғана шифрланған текст оқылуға берілуі тиіс
в) шифрланған текст ұзындығы бастапқы тексттің ұзындығына тең болуы тиіс
г) шифрлау алгоритмнің құрылымдық элементтері тұрақты болуы тиіс
д) шифрлаудың алгоритмін білу ақпараты қорғаудың сенімділігіне әсер етпеуі тиіс
33. Қай әдіс криптографиялық әдістер классификацясына кіреді?
а) барлық жауабы дұрыс б) көп алфавитті қойылым
в) алмастыру әдісі г) гаммирование д) блоктық шифрлар
34. Бастапқы текстке кілт негізінде өзгерту үшін кейбір кездейсоқ тізбектерді қою әдісі?
а) гаммирование б) алмастыру в) блоктық ширлар
г) ауыстыру д) көп алфавитті қойылым
35. Ширланатын текстің блогы үшін қолданылатын негізгі өзгертулер әдістерінің қатары?
а) блоктық шифрлар б) гаммирование в) алмастыру әдісі
г) көп алфавиттік қойылым
36. Бастапқы текст символдарын қиын немесе қиын емес ереже бойынша басқа символдармен алмастыру әдісі?
а) көп алфавитті қойылым б) гаммирование
в) алмастыру әдісі г) блоктық ширлар
37. Криптографиялық өзгертулердің оңай тәсілі, бұл әдіс көбінесе басқа әдістермен қолданады?
а) алмастыру әдісі б) гаммирование в) блоктық шифрлар
г) көп алфавиттік қойылым
38. Көп алфавиттік қойылым дегеніміз не?
а) бастапқы текст символдарын қиын немесе қиын емес ереже бойынша басқа символдармен алмастыру әдісі
б) бастапқы текстке кілт негізінде өзгерту үшін кейбір кездейсоқ тізбектерді қою
в) шифрланатын тексттің блогы үшін қолданылатын негізгі өзгертулер әдістерінің қатары
г) криптографиялық өзгертудің оңай тәсілі, бұл әдіс көбінесе басқа әдістермен бірге қолданылады
39. Блоктық шифрлар-...
а) шифрланатын текстің блогы үшін қолданылатын негізгі өзгертулер әдістерінің қатары
б) бастапқы текстте кілт негізінде өзгерту үшін кейбір кездейсоқ тізбектерді қою
в) бастапқы текст символдарын ереже бойынша алмастыру
г) көбінесе басқа әдістермен бірге қолданатын әдіс
40. Гаммирование-...
а) бастапқы текстке кілт негізінде өзгерту үшін кездейсоқ тізбектерді қою

б) бастапқы текст символдарын басқа символдармен алмастыру
в) өзгертулер әдістерінің қатары
г) көбінесе басқа әдістермен бірге қолданылатын әдіс
41. Ресей және АҚШ шифрлау стандарттары шифрлаудың қай класына негізделген?
а) блоктық шифрлар б) алмастыру әдісі
в) көп алфавиттік қойылым г) гаммирование
д) дұрыс жауабы жоқ
42. Алмастыру әдісі-...
а) криптографиялық өзгертулердің оңай тәсілі, бұл әдіс көбінесе басқа әдістермен бірге қолданылады
б) бастапқы текст символдарын басқа символдармен алмастыру тәсілі
в) бастапқы текстке тізбектерді қою
г) шифрланатын тексттеу блогы үшін қолданылатын әдістер қатары
д) дұрыс жауабы жоқ
43. Ресей және АҚШ цифрлау стандарттары шифрлаудың қай класына негізделген?
а) блоктық шифрлар б) алмастыру әдісі в) көп алфавиттік қойылым
г) гаммирование д) дұрыс жауабы жоқ
44.Шифрлау -...
а) барлық жауабы дұрыс
б) бастапқы тексттің шифрланған текстпен алмастырылуы
в) өзгерту процесі
г) ашық тексттің бөгде адамдарға мағынасын түсінбеу үшін жасалынатын өзгерту процесі
д) ашық тексттің шифрланған текстпен алмастырылуы
45. Дешифрлау-...
а) барлық жауабы дұрыс
б) кілт арқылы шифрланған тексттің бастапқы қалпына келтірілуі
в) кері өзгерту процесі
г) шифртекстті ашық текстке өзгерту процесі
д) шифртекстті бастапқы текстке өзгерту процесі
46. Криптографияның қай бөлімінің мазмұны “кілттерді пайдаланушылар арасында құрастыру және жіктеу” болып табылады?
а) кілттерді басқару б) ашыққілтті криптожүйе
в) электронды жазба жүйесі г) симметриялық криптожүйе
д) дұрыс жауабы жоқ
47. Криптографияның қай бөлімі текстті қабылдаған өзге пайдаланушы арқылы ақпараттың авторлығын және түп-нұсқасын тексеруге мүмкіндік береді ?
а) электронды жазба жүйесі б) ашыққілтті криптожүйе
в) кілттерді басқару г) симметриялық криптожүйе
д) барлық жауабы дұрыс
48. Криптографияның қай бөлігінде шифрлау және дешифрлау үшін математикалық тұрғыдан бір-бірімен тығыз байланысты ашық және жабық кілттер қолданылады ?

а) ашық кілтті криптожүйеде б) симметриялық криптожүйеде
в) электронды жазба жүйесінде г) кілттерді басқаруда
д) барлық жауабы дұрыс
49. Криптографиялық алгоритмдер....
а) шифрлау немесе алгоритімдік шифрлау
б) ақпараттарды өңдеуге арналған құрал жабдықтар
в) шифрлауға қажетті математикалық амалдар
г) ақпараттарға физикалық тосқауылдар құру
д) дұрыс жауабы жоқ
50. Ашықтексті-Р, шифртексті-С, шифр функциясын- Е әрпімен белгілесек, Е(Р)=С математикалық белгіленуі нені білдіреді ?
а) Е- шифр функциясының кірісіне-Р, шығысына- С берілгенін
б) Е- шифр функциясының шығысына-Р, кірісіне- Р берілгенін
в) Е- шифр функциясының кірісіне де, шығысына да Р берілгенін
г) Е- шифр функциясының кірісіне-С, шығысына- С берілгенін
д) дұрыс жауабы жоқ
51. Криптография қандай ғылым ?
а) ақпараттың, деректердің мағынасын құпия түрде қалай сақтау керектігін оқытатын ғылым
б) ақпаратты өзгеріске келтіре отырып оны қорғау мәселесімен айналысатын ғылым
в) ешқандай да кілтсіз ақпараттың шифрын ашудың мүмкіндіктерін зерттейтін ғылым
г) шифрдің кілтсіз дешифрлау әрекетіне шыдамдылығын анықтайтын ғылым
52. Криптоанализ.....
а) ешқандай да кілтсіз ақпараттың шифрын ашудың мүмкіндіктерін зерттейтін ғылым
б) ақпаратты өзгеріске келтіре отырып, оны қорғау мәселесімен айналысатын ғылым
в) ақпаратты өзгертудің математикалық әдісін іздеумен және зерттеумен айналысытын ғылым
г) ақпараттың мағынасын құпия түрде қалай сақтау керектігін оқытатын ғылым
53. Криптология.....
а) ақпаратты өзгеріске келтіре отырып, оны қорғау мәселесімен айналысатын ғылым
б) ешқандайда кілтсіз ақпараттың шифрын ашудың мүмкіндіктерін зерттейтін ғылым
в) ақпаратты өзгертудің математикалық әдісін іздеумен және зерттеумен айналысытын ғылым
г) шифрдың кілтсіз дешифрлау әрекетіне шыдамдығын анықтайтын ғылым
54. Желіде бірнеше пайдаланушылардың жұмыс істеуі және олардың күнделікті ауысып отыруы неге алып келеді?
а) информайияны қауіпсіздендіруді қиындатады
б) ешқандай өзгеріске алып келмейді в) ЭЕМ істен шығады
г) ЭЕМ- де жұмыс істеу қиын болады

55. Желіде жұмыс істеуге көшу барысында информацияны қауіпсізденді қиындататын себептің бірі?
а) желіге көптеген потенциялдық каналдардың кіріп кетуі
б) желінің дұрыс қосылмауы в) компьютердің дұрыс жұмыс істемеуі
г) желіні дұрыс пайдаланбауы
56. Толық деректер сақтау мәселесі келесі аспектерден тұрады?
а) ұйымдастыру және технологиялық аспекттер
б) ұйымдастыру және бақылау аспекттер
в) информациялық аспект г) бағдарламалық аспект
57. Толық деректер сақтау мәселесі неше аспекттен тұрады?
а) 2 б) 1 в) 4 г) 8
58. Ережелердің қайсысы ұйымдастыру аспектісіне жатады?
а) барлық жауабы дұрыс
б) ақпарат басқалардың байланысы жоқ жерде сақтайды
в) өте керекті ақпарат бірнеше жинақтауыштарда сақталуы тиіс
г) әртүрлі есептерге жататын деректер бөлек атпен сақталады
д) магнитті жинақтаулармен ережелерге сай байланыс жасалынуы тиіс
59. Әр түрлі есептерге жататын деректер бөлек атпен сақталады, бұл ереже қай аспектке жатады?
а) ұйымдастыру б) бағдарламалау в) есептеу
г) жинақталу
60. Ұйымдастыру аспект ережесінің бірі?
а) өте керекті ақпарат бірнеше жинақтауыштарда сақталуы тиіс
б) ЭЕМ- ге бөтен пайдаланушыларды келтірмеу
в) пайдаланушылардың аты мен пароль арқылы информацияны бөтен пайдаланушылардың қауіпсіздандыру жеткіліксіз
г) әлде бір диапозонды кеңістікте көрсеткішінің мәнін сақтау шектеулі
61. Бұрыңғы және жаңа мәндер арасындағы байланысты сақтау мақсатындағы белгілі атрибуттарды жаңалау шектеулі, бұл ереже қай аспектке жатады?
а) технологиялық аспект б) ұйымдастыру аспектісі
в) бақылау аспектісі г) шектеу аспектісі
62. Технологиялық аспект неше шектеулерден тұрады?
а) 2 б) 10 в) 5 г) 7 д) дұрыс жауабы жоқ
63. Технологиялық аспект ережесінің бірі?
а) әлде бір диапозонда кеңістік көрсеткішінің мәнін сақтау шектеулі
б) ақпарат басқалардың байланысы жоқ жерде сақталады
в) әртүрлі есептерге жататын деректер бөлек атпен сақталады
г) желіге көптеген потенциялдық каналдардың кіріп кетуі
64. Ұйымдастыру аспект ережесінің бірі?
а) магнитті жинақталу мен ережелері сай байланыс жасалуы тиіс
б) әлде бір диапазонда кеңістік көрсеткішінің мәнін сақтау шектеулі
в) ЭЕМ- де пайдаланушылардың көп болуы
г) желіде бірнеше пайдаланушылардың жұмыс істеуі
65. Кез келген қосымша байланыстар басқа элементтермен келесі интернет желісіне қосылу қандай проблемаларға алып келеді?

а) компьютерлік вирустармен зақымдау мүмкіншілігін көбейтеді
б) ЭЕМ істен шығады в) клавиатура жұмыс істемейді
г) аналық плата істен шығады
66. Коаксиалдық кабельдердің басқаша атауы?
а) “мыстық кабель” б) жай кабель в) желілік кабель
г) сандық кабель
67. Желідегі информацияны қорғау не арқылы қауіпсіздендіруге болады?
а) “генератор шумы” б) пароль арқылы
в) желіні өшіру арқылыг) информацияны қорғау мүмкін емес
68. Информацияны қоғауды қамтамасыз ететін құралдар неше топқа бөлінеді
а) 3 б) 4 в) 1 г) 8 д) 10
69. Информацияны қорғауды қамтамасыз ететін құралдарды ата?
а) техникалық, программалық, ұжымдық құралдар
б) жүйелік, кодтық, математикалық құралдар
в) физикалық құрал г) шифрлық құрал
70. Технологиялық, программалық ұжымдық құралдар не үшін керек?
а) информацияны қорғауды қамтамасыз етеді
б) компьютердегі вирустарды жояды
в) жинақтауыштардағы вирустарды юояды
г) ешнәрсеге қолданбайды
71. Технологиялық құрал не үшін керек?
а) физикалық кіруге кедергі жасайды
б) вирустар кіруге кедергі жасайды
в) бөтен пайдаланушылардан қорғайды
г) информацияны қорғайды
72. Технологиялық құралдарға не жатады?
а) кілттер, решеткалар, сигнализациялар
б) шифрлар, кодтар в) пароль г) желілік
73. Технологиялық құралдардың кемшілігі?
а) құралдың қымбат тұруы б) құралдың тез істен шығуы
в) құралдың дұрыс істемеуі г) құралдардың көлемі үлкен болуы
74. Программалық құрал не үшін қолданады?
а) пайдаланушыларды идентификацияға арналған программалар, информацияны шифрлау
б) вирустарды жоятын программа в) желіні қорғайтын программа
г) компьютерлік информациянықорғауға арналған порграмма
75. Программалық құралдың құндылығы неде ?
а) универсалдығы, орнатудың қарапайымдылығы, модификацияға және жүзеге асыруына мүмкіншілігі
б) құралдың арзан тұруы
в) құралды бөтен пайдаланушының қолдана алмауы
г) құралдың өте қарапайымдылығы
76. Программалық құралдың кемшілігі ?
а) барлық жауабы дұрыс
в) желінің физикалық мүмкіншілігін шектеу
с) файл сервердің және жұмыс орындарының жарты ресурстарын қолдану

д) кездейсоқ және келісілген өзгертулерге жоғары сезімталдығы
е) компьютердің типіне тәуелді мүмкіндігі
77. Ұжымдық құралдың құндылығы неде ?
а) барлық жауабы дұрыс
в) әр түрлі проблемалардың мүмкіншілігі
с) құрудың қарапайымдылығы
д) желідегі өзгерістерге тез сезімталдығы
е) модификацияға мүкіншілігінің шексіздігі
78. Әр түрлі проблемалардың мүмкіншілігі құрудың қарапайымдылығы, желідегі өзгерістерге тез сезімталдығы, модификацияға мүмкіншіліктердің шексіздігі қандай құралға тән ?
а) ұжымдық құрал в) программалық құрал
с) технологиялық құрал д) математикалық құрал
79. Шифрлау түсінігі қандай ұғымымен байланысты ?
а) криптография в) микрография
с) кодтау д) түрлендіру
80. Криптография ұғымын аударғанда нені білдіреді ?
а) крипто- құпия, графия-жазу в) крипто-жазу, графия-құпия
с) крипто-жүбе, графия-құру д) крипто-ақпарат, графия-алу
81. Құпия жазу қай ұғымына тән ?
а) криптография в) кодтау с) түрлендірі
д) микрография
82. Криптография ұғымы нені қарастырады ?
а) шифрлау және цифрлық мәліметтерді ауыстыруға байланысты қосымша проблеманы шешу жолдарын қарастырады
в) информацияны біріктіруді с) программалық құралды
д) түрлендіруді
83. Универсалдығы орнатудың қарапайымдылығы, модификацияға және жүзеге асыру мүмкіншілігі қандай құралға тән ?
а) программалық құрал в) ұжымдық құрал
с) техникалық құрал д) математикалық құрал
84. Novell фирмасының SFT жүйесі неше негізгі деңгейді қарастырады?
а) 3 в) 4 с) 8 д) 2
85. Novell фирмасының SFT жүйесінің бірінші деңгейін көрсет ?
а) SFT level 1 в) SFT level 3 с) SFT level 2
д) SFT level 1.1
86. Novel фирмасының SFT жүйесінің екінші деңгейін көрсет ?
а) SFT level 2 в) SFT level 2.2 с) SFT level 2.2
д) SFT level 2.1
87. Novel фирмасының SFT жүйесінің үшінші деңгейін көрсет ?
а) SFT level 3 в) SFT level 3.3 с) SFT level 3.1
д) SFT level 3.3
88. Бірінші деңгей нені қарастырады ?
а) FAT және Directory Entries Tables қосымша көшірмелерін жасауды қарастырады
в) көшірмелерін жасауды қарастырады

с) жүйелерді қосуды қарастырады
д) вирустық бағдарламаларды қосуды қарастырады
89. Екінші деңгейдің SFT level 2 мүмкіндігі бар.
а) арнайы дискілер құру мүмкіндігі бар.
в) бағдарлама құру мүмкіндігі бар.
с) ЭЕМ-дегі вирустарды жою мүмкіндігі бар.
д) желіні қорғау мүмкіндігі бар.
90.SFT level 2 деңгейдің қосымша мүмкіндігі.
а) дискілік контролёрларды, ток көзін және интерфейстік кабельдерді дубілдеу. в) ЭЕМ-гі вирустарды жою мүмкіндігі бар.
с) желіні қорғау мүмкіндігі. д) бағдарлама құру мүмкіндігі.
91.SFT level 3 үшінші деңгей мүмкіндігі.
а) локальді желіде серверлердің көшірмесін пайдалануға мүмкіндігін береді.
в) арнайы дискілер құру мүмкіндігі
с) ток көзін және интерфейстік кабелдерді дубілдеу
д) желіні қорғау мүмкіндігі.
92.SFT жүйесін түрлендір
а) System. Fault. Tolerance в) System Fault Tables
с) System Firewalls Tolerance д) System Firewalls Tolerance
93. Локальді желіде серверлердің көшірмесін пайдалануға мүмкіндігі қай деңгейге тән?
а) SFT Level 3 б) SFT Level 2 в) SFT Level 1
г) SFT Level 4
94. Арнайы дискілер құру мүмкіндігі қай деңгейгк тән?
а) SFT Level 2 б) SFT Level 4 в) SFT Level 3
г) SFT Level 5
95. Novell фирмасының SFT жүйесінің үш негізгі деңгейін көрсет
а) SFT Level 1, SFT Level 2, SFT Level 3
б) SFT Level 2, SFT Level 4, SFT Level 5, SFT Level 3
в) SFT Level 2, SFT Level 3, SFT Level 4
г) SFT Level 1, SFT Level 2
96. FAT және Directory Entries Tables қосымша көшірмелерін жасауды қарастыратын деңгей?
а) SFT Level 1 б) SFT Level 2 в) SFT Level 4
г) SFT Level 3
97. Ақпаратты қорғау құралдары өте көп, олардың ішінен екі жүйе көп қолданыс тапқан, соны көрсет?
а) отты дуал Firewalls-брандмауэрлер, Droxy- servers
б) SFT Level 2 в) System Foult Tables, SFT Level1
г) SFT
98. Отты дуал Firewalls-брандмауэрлер қандай жұмыс атқарады?
а) локальді және глобальді желі арасында арнайы аралық серверлер құрады
б) компьютердегі вирустарды жояды
в) жинақтауыштардағы вирустарды жояды
г) информацияны қорғауды қамтамасыз етеді
99. Droxy- servers қандай жұмыс атқарады?

а) локальді және лобальді желі арасындағы барлық желілік транспорттық деңгейлер графигі бойынша шектеледі
б) локальді және глобальді желі арасында арнайы аралық серверлер құрады
в) компьютердегі вирустарды жояды
г) программа құруға көмектеседі
100. Ақпаратта қорғаудың административтік ұйымдастыру қорғаныс құрамының мақсаты?
а) қауіптің іске асуын мейлінше болдырмау б) желіні қорғау
в) ЭЕМ көп уақыт жұмыс істеуін г) информацияны қорғау

Тест сұрақтарының тек бірінші (а) жауаптары дұрыс.

ӘДЕБИЕТТЕР

1. Мельников В. Защита информации в компьютерных системах. - М.: ФиС, 1997.
1. Жельников В. Криптография от папируса до компьютера. - М.: АБФ, 1996.
2. Домарев В.В. Защита информации и безопасность компьютерных систем. - Киев, 1999.
3. Домарев В.В. Безопасность информационных технологий. - М., 2002.
4. Баричев С. Основы современной криптографий. – М., 2002.
5. Герасименко В.А. Защита информации в АСОД. - М.: Энергоиздат, 1994.
6. Введение в криптографию. Под.ред. Ященко В.В., - М.: МЦНМО, 2000.
7. Информатика. Под.ред Могилева. - М.: Академия, 2001.
8. Быстро и легко осваиваем работу в сети интернет. Под.ред. Резникова Ф.А. - М., 2000.
9. Защита программного обеспечения, пер. с анг.под.ред. Граукера Д.М. - Мир, 1992.
10. Коцюбинский Б. Экономическая информатика. - СПб., 2000.
11. Баричев С.В. криптография без секретов – М.: Наука, 1998.
12. Галатенко В.А. Информационная безопасность – М.: Финансы и статистика, 1997. – 158 с.
13. Ростовец А.Г., Михайлова Н.В. Методы криптоанализа классических шифров. – М.: Наука, 1995. – 208 с.
14. Герасименко В.А. Защита информации в автоматизированных системах обработки данных кн. 1.-М.: Энергоатомиздат, 1994.- 400с.
15. Вербицкий О.В.Вступление к криптологии.- Львов: Издательство науково-техничной литературы, 1998. – 300 с.
16. Диффи У. Первые десять лет криптографии с открытым ключом //ТИИЭР, 1988. - Т56. - с. 54-74.
17. Герасименко В.А., Скворцов А.А., Харитонов И.Е. Новые направления применения криптографических методов защиты информации.- М.: Радио и связь, 1989. – 360 с.
18. Галатенко В.А. Информационная безопасность. – М.: Финансы и статистика, 1997. – 158 с.
19. Грегори С. Смит. Программы шифрования данных // Мир ПК –1997. - №3. -С.58 - 68.
20. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. – 208 с.
21. Терехов А. Н., Тискин А. В. // Программирование РАН. –1994. -N 5 - С. 17-22.
22. Криптология – наука о тайнописи // Компьютерное обозрение. –1999. - №3. – С.10-17.
23. Баричев С.В. Криптография без секретов. – М.: Наука, 1998. – 120 с.

МАЗМҰНЫ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК НЕГІЗДЕРІ
оқу құралы

___ ___ 2012ж. баспаға қол қойылды.
Қағаз форматы $X^{x}Y$ 1/16
Типографиялық қағаз. Офсеттік баспа. Көлемі 6,5 б.п.
Тираж 50 дана. Тапсырыс №

Мирас университетінің баспа орталығы, Шымкент қаласы, 1 мамыр көшесі, 10