Ақпаратты қорғау әдістері

10.6.2.2 Деректерді шифрлау қажеттілігін бағалау

- Компьютерлік жүйені пайдаланатын кез келген адамға деректер қауіпсіздігі әсер етеді.
- Компьютер жүйесіндегі деректер ***бүлінген, жоғалған*** немесе ***ұрланған*** болса, онда оны қалпына келтіру мүмкін емес.

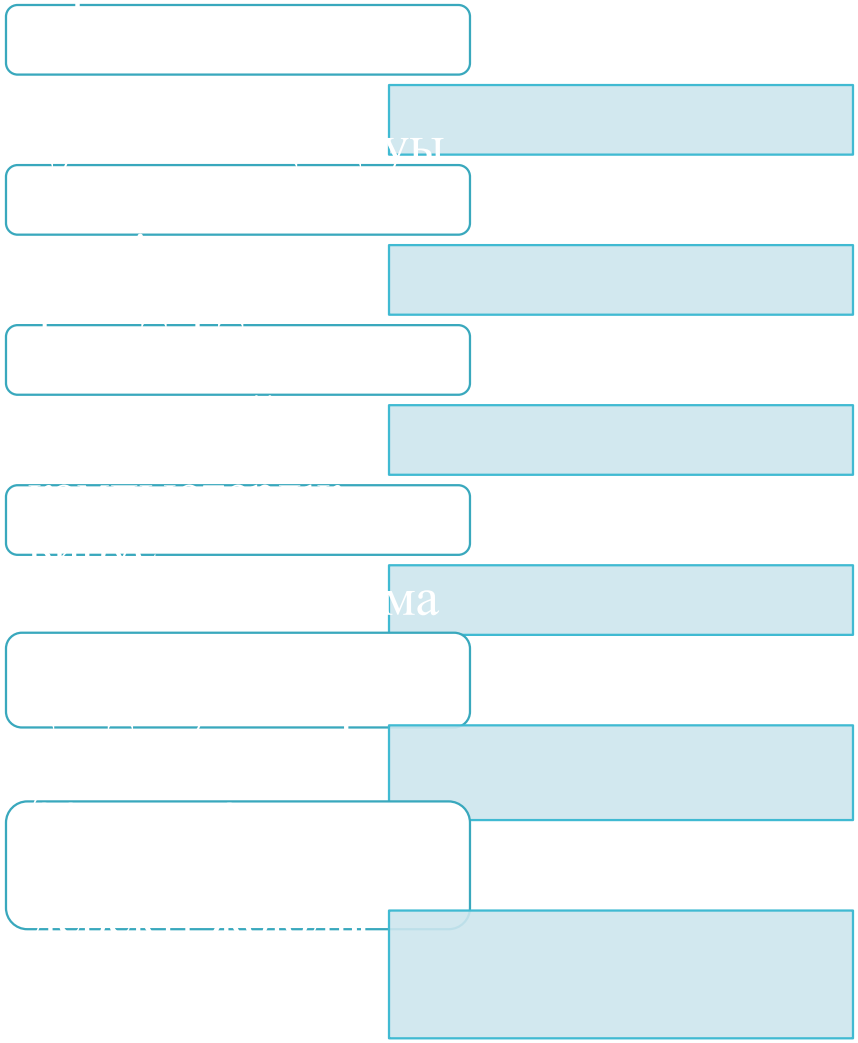
Анықтама

Ақпаратты қорғау– информациялық қауіпсіздікті (информацияның бүтіндігін, ену көздерін, шектулілігін, ақпарат және оның ресурста-рын қолдану барысында) қамтамасыз етуге бағытталған іс-шаралар комплексі.

Ақпарат қауіпсіздігі деп – оның оған түрлі қарсылық білдіруші әсері кезінде жүйенің иеленушілері мен қолданушыларына зиян келтіру әрекетіне қарсы әрекет жасау қабілетінен көрінетін қасиетін түсінеміз.

Деректер қауіпсіздігінің қауіпсіздік-қатерлері

Деректер төмендегідей жағдайды шешу мүмкін:



Ақпаратты қорғау әдістері

- Ақпаратты қорғау әдістері
- Программалық
- Ұйымдастыру-шылық
- Криптографиялық
- Техникалық

Ақпаратты қорғаудың техникалық әдісі

Ақпаратты қорғаудың техникалық шараларына бейнебақылау, дабыл беру жүйелері, сондай-ақ ақпараттарды таратуға жол бермейтін және бұғаттайтын басқа да құралдарды пайдаланумен байланысты болады.

Қорғаныстың аппараттық әдістерін қолдану мынадай техникалық құралдарды пайдалануды ұсынады:

1. Тыңдалатын және жазылатын құрылғылардан қорғайтын TRD-800 категориялы радиохабарлағыштар мен магнитофондар детекторы;
2. Жасырын бейне бақылау құратын модульдік нөмірлер;
3. Ақпаратты жеткізудің дұрыстылығын қамтамасыз ететін ақпаратты анықтылыққа тексеру сызбалары;
4. Құпиялы құжаттарды жіберуге арналған SAFE-400 категориялы факстік хабардың скремблері.

Ақпаратты қорғаудың программалық әдісі

- Ақпаратты қорғаудың бағдарламалық шаралары: мәтінді шифрлау, файлдарды уақытша жою, құпия сөздерді бір деректерге енгізу үшін пайдалану, зиянды бағдарламалардан қорғау мүмкіндіктері.

Программалық әдістер келесі функцияларды іске асырады:

1. Идентификация, аутентификация, авторизация (Pin кодтар, парольдер жүйелері арқылы);
2. Резервті көшіру және қалпына келтіру процедуралары;
3. Антивирустық программаларды белсенді қолдану және антивирустық қорларды жиі жаңартып отыру;
4. Транзакцияны өңдеу.

Ақпаратты қорғаудың ұйымдастыру-шылық әдісі

Ақпаратты қорғаудың ұйымдастырушылық шараларына ұйымдардың қауіпсіздік саясаты және оларды қол жеткізуді қиындататын байланыс арналарының орналасуы ұйымдастырылды.

Ақпаратты қорғаудың криптографиялық әдісі

Бұл ақпаратты шифрлаудың, кодтаудың немесе басқаша түрлендірудің арнайы әдісі, Мұның нәтижесінде ақпарат мазмұнына криптограмма кілтінсіз және кері түрлендірмей шығу мүмкін болмайды. Криптографиялық қорғау – ең сенімді қорғау әдісі, өйткені ақпаратқа шығу емес, оның тікелей өзі қорғалады, (мысалы, әуелі тасуыш ұрланған жағдайдың өзінде ондағы шифрланған файлды оқу мүмкін емес).

Анықтама

Шифрлау дегеніміз - арнайы кодтау. Бөгде қызмет ету туралы түсініксіз, ашық ақпарат түрлендіру. Ол екі бөлімнен тұрады: криптография және криптоталдау. Криптография 4 мыңжылдық тарихы бар ғылым. Криптография - ақпаратты шифрлау әдістері туралы ғылым. Криптоталдау - шифрланған түсіндірудің қажеттіліктері мен әдістері туралы ғылым.

Криптографиялық шифрлау әдістері шифрлау кілтіне және оларды қайта ашу белгісі бойынша симметриялық және ассиметриялық деп 2-ге жіктеледі.

- Симметриялық әдістер:

- DES, IDEA, ГОСТ
- Симметриялық әдісте жіберуші мен қабылдаушыда тек бір ғана кілт қолданылады (құпия кілт).

- Ассиметриялық әдістер:

- RSA, Diffi-Hellman
- Ал ассиметриялық әдісте 2 кілт қолданылады: құпия және ашық кілт.

Брандмауэр, Резервтік көшіру

- **Брандмауэр** (Firewall) - бағдарламалық-аппараттық кешеннің бағдарламалық жасақтамасын орнатуға мүмкіндік береді. Басқаша жауап - ол сүзгі ретінде желі мен компьютерлер арасындағы кедергілерді қамтамасыз ету, жүйені компьютерлік операциялардан қорғау үшін қажет. Жұмыс, бағдарлама пайдаланушының өзін басқарған нәрсені ғана өткізеді.

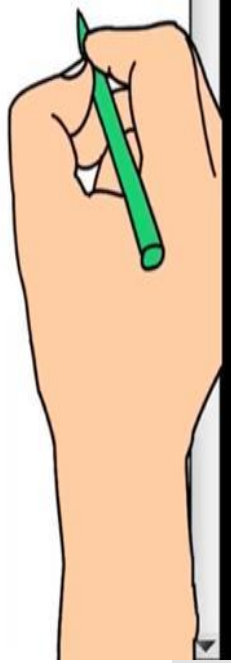
- **Резервтік көшіру** - деректердің бұзылған немесе жойылған жағдайдағы деректері, оларды өзгертуге арналған көшірмелерін жасауға арналған ережелер.

Оқу тапсырмасы 1 (сәйкестендіру)

Тапсырма. Қауіп көзі мен ақпарат объектісіне (мысалы, 1-А) қауіпті әсердің алдын алатын немесе әлсіретететін ақпаратты қорғау әдісінің сәйкестігін орнатыңыз.

	Ақпараттық қауіпсіздікке қауіп төндіретін көздер
1	Ақпараттық ресурстарға рұқсатсыз қол жеткізу.
2	Ақпаратты ұрлау мақсатында серверлік бөлмеге заңсыз кіру.
3	Кітапханалардың, мұрағаттардың, банкілердің және деректер базасының ақпараттық жүйелерінен ақпаратты жою.
4	Компьютерді бағдарламалық қамтамасыз етуге вирустарды енгізу.
5	Электрондық кілттер мен парольдерді бұзу әрекеті.
6	Ақпарат тасығыштарды жоюға немесе ұрлауға әрекет жасау.
7	Ақпараттық жүйелер қызметкерлерінің байқаусызда жіберілген қателіктері.
8	Маңызды ақпаратты жоғалтуға әкелетін компьютердің бұзылуы.
9	Қызметкерлердің ақпаратты өңдеу, беру және пайдалану ережелерін сақтамауы.

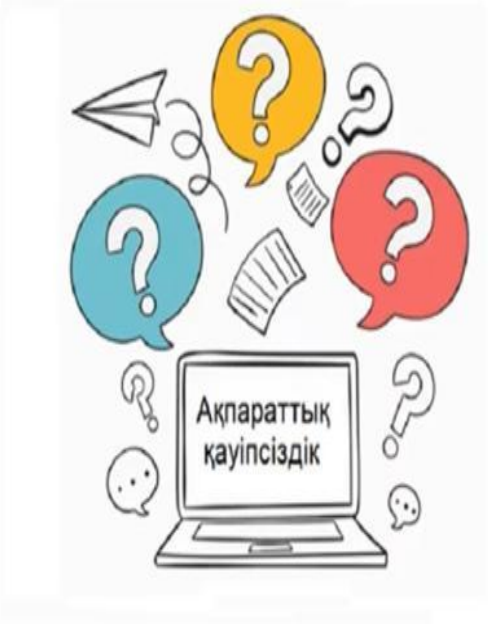
	Ақпаратты қорғау әдістері
A	Қатынасты басқару
B	Кедергілер
C	Сақтық көшірме
D	Мамандандырылған бағдарламалар
E	Бүркемелеу
F	Кедергілер
G	Регламенттеу
H	Сақтық көшірме
I	Ояту



Оқу тапсырмасы 2

Қалай қорғау?

Нені қорғау?



Кімнен қорғау?