Ақпаратты қорғау негіздері

- Ақпараттық жүйелердің қауіпсіздігі. Ақпаратты қорғау негіздері.
- Компьютерлік вирустар.
- Компьютерлік вирустардан қорғау әдістері.
- Антивирус қорғау құралдары.
- АЖ-ді қорғаудың криптографиялық құралдары

Ақпаратты қорғаудың мақсаты ақпаратиесіне, меңгерушіге және пайдаланушыға келетін зиянды әрекеттерді болдырмау.

Ақпаратты қорғаудың *тиімділігі* ақпаратты қорғау нәтижелерінің қойылған мақсатқа сай келу дәрежесімен бағаланады.

Ақпаратты жүйелерді қорғаудың мақсаты (ақпаратты өңдеу жүйесі) қауіп-қатерге қарсы әрекеттер:

-өңделген ақпараттың жасырын бұзылу қатері;

-өңделген ақпараттың бүтіндігінің бұзылу қатері;

-жүйенің жұмыс істеуінің бұзылу қатері.

Сурет 1. Қорғаныс жүйесін құру кезеңдері

1. Мүмкін болатын қауіп-қатердің талдауы келесі қауіп-қатерден қорғанудың негізгі түрлерін зерттеумен айналысады:
- Ақпараттың конфиденциалдығының бұзылуының қауіп-қатері;
- Ақпараттың бүтіндігінің бұзылуының қауіп-қатері.

Бұл кезең шындығында да барлық қауіп-қатердің жиынтығынан байсалды зиян (вирус, ұрлық) келтіретіндерін таңдаумен аяқталады.

2. Қорғаныс жүйесін жоспарлау кезеңі қорғалатын құрылымдар тізімінен және оларға мүмкін болатын қауіп-қатерден тұрады. Бұл кезде қорғанысты қамтамасыз етудің келесі бағыттарын назарға алу қажет:
- құқықтық-этикалық;
- моральды-этикалық;
- қорғанысты қамтамасыз етудің әкімшіліктік шаралары;
- қорғанысты қамтамасыз етудің аппараттық-программалық шаралары.

3. Қорғаныс жүйесін іске асыру ақпаратты өңдеудің жоспарланған ережелерін іске асыруға қажетті құралдарды орнату мен баптауды қамсыздандырады.

4. Қорғаныс жүйесін сүйемелдеу кезеңі жүйенің жұмысын бақылау, ондағы болып жатқан оқиғаларды тіркеу, қорғанысты бұзуды айқындау мақсатымен оларды талдау және қажетінше қорғаныс жүйесін түзетумен сипатталады.

Ақпараттық жүйе деп ақпараттық үрдістерді жүзеге асырушы құжаттардың, құжаттар топтамасының және ақпараттық технологиялардың реттелген жиынтығын атайды, яғни объектіні басқаруға қажетті ақпаратты беру мен жаңарту, сақтау, жинақтау жүйесі.

Ақпараттарды қорғау дегеніміз қорғалған ақпараттарға санкцияланбаған және алдын ала ойластырылмаған әрекеттердің жасалуынан олардың ағып кетуіне тосқауыл қою.

Санкцияланбаған ену – қызығушылық тудырған субьектінің ену ережесін бұз арқылы қорғалған ақпараттарды алуы. у

Ақпараттың сапасы дегеніміз ақпараттың орындалуына қарай, оны қолданушының белгілі бір қажеттілігін қанағаттандыратын ақпараттың жарамдылығын көрсететін қасиеттердің жиынтығы. Ақпарат сапасының бір көрсеткіші оның

Сорғалдуы дегеніміз белгілі бір деңгейде ақпараттардың сақталуын, өңделуін пайдалануын қамтамасыз ету.

Қорғалған ақпараттың негізгі сипаттамаларына, оның дығы, бүтіндігі конфиденциаль- және жатады. қол жетімділігі

Ақпараттың конфиденциальдығы – бұл оның мазмұнының тек иеленуші субьектіге ғана белгілілігі.

Конфиденциальдық ақпаратқа қолжетімділіктің бұзылуынан қызығушылығын қорғайтын, обьективті қажеттілікпен байланысты, ақпараттың субьективті сипаттамасы болып табылады.

АЖ компоненттері:

- Аппараттық жасақтама: ЭЕМ және құрама бөліктер (процестер, мониторлар, терминалдар, периферийлік құрылғылар, дисководтар, принтерлер, контроллерлар, кабелдер, байланыс линиялары) және т.б.;
- Бағдарламалық жасақтама: алынған бағдарламалар, негізгі, объектілі, жүктелетін модулдер, амалдық жүйелер және жүйелік программалар (компиляторлар, құрастырушылар және басқалар), утилиттер, диагностикалық программалар;
- мәліметтер – магниттік тасымалдаушылардағы тұрақты және уақытша сақталатындар, баспа архивтері, жүйелік журналдар және т.б.;
- персонал – қызмет етуші персонал және қолданушылар.

АЖ-ДІҢ ҚАУІПСІЗДІК ҚАТЕРІН ОНЫҢ КОМПОНЕНТТЕРІНЕ ЫҚПАЛЫ РЕТІНДЕ ЖҮЗЕГЕ АСЫРУДЫҢ НЕГІЗГІ ЖОЛДАРЫ

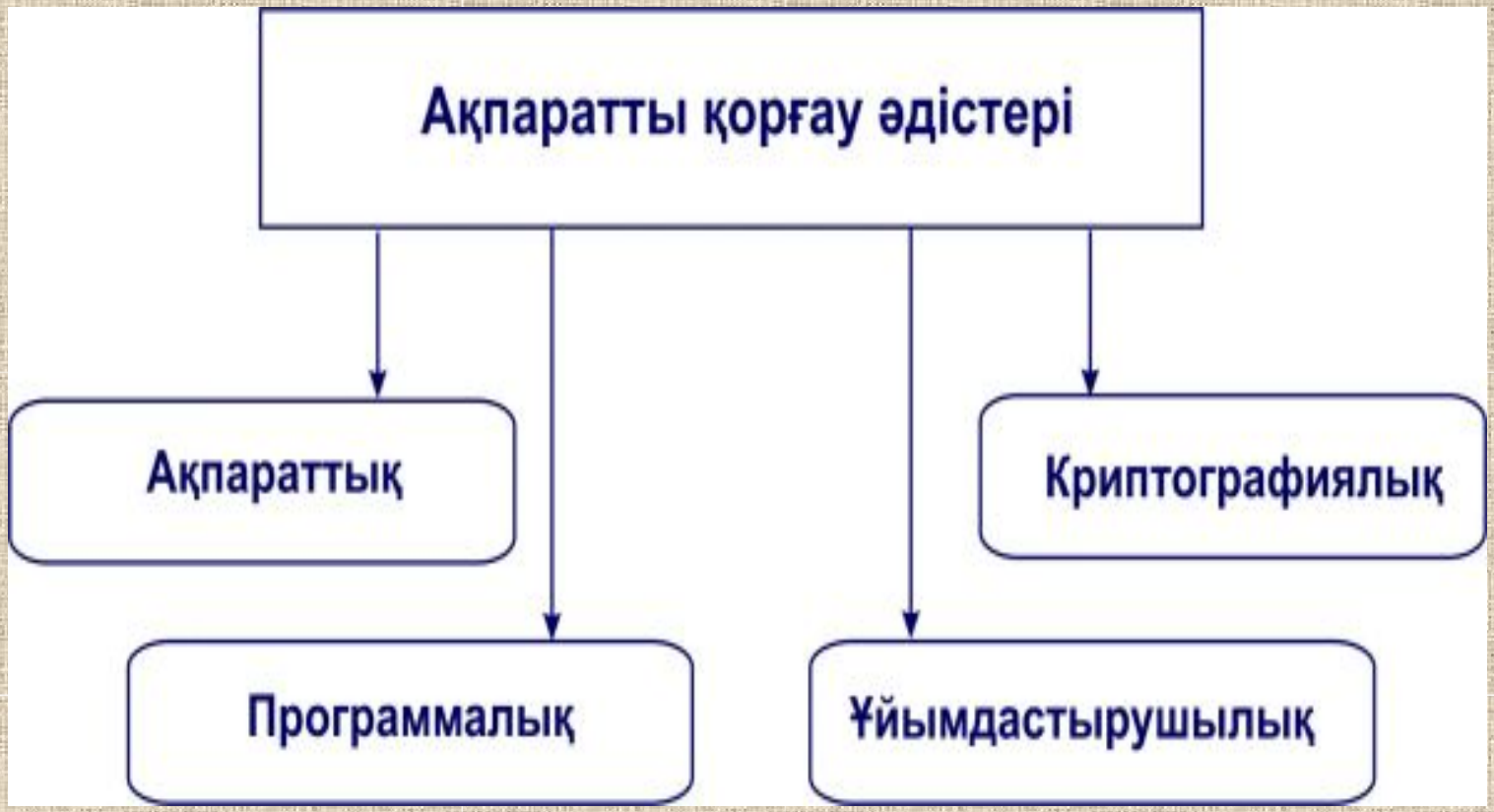
Ықпал ететін объектілер	Ақпараттың құпиялылығының бұзылуы	Ақпараттың бүтіндігінің бұзылуы	Жүйенің жұмыс істеу қабілетінің бұзылуы
Аппараттық жасақтама	РҚ – қосу, ресурстарды қолдану, тасымалдаушыларды тонау.	РҚ – қосу, ресурстарды қолдану, модификация, режимнің өзгеруі.	РҚ – режимдердің өзгеруі.
Программалық жасақтама	РҚ – көшіру; тонау; ұстап қалу.	РҚ, «троян аты», «вирустарды», «құрттарды» ендіру.	РҚ – бұрмалау; өшіру; айырбастау.
Мәліметтер	РҚ - көшіру; тонау; ұстап қалу.	РҚ – бұрмалау; модификация.	РҚ – бұрмалау; өшіру; айырбастау.
Персонал	Жариялау; қорғау жайлы мәлімет беру; ұқыпсыздық.	«Маскарад»; тарту; персоналды сатып алу.	Жұмыс орнынан кету; физикалық ауытқуы.

“Маскарад” – бір қолданушының басқа қолданушының атынан сәйкес өкілеттікпен қандай да бір әрекетті орындауы. “Маскарад” мысалдары – жүйеге басқа қолданушының атымен және паролімен кіру – торапта басқа қолданушының атымен хабар беру.

РҚ – рұқсатсыз қатынау.

АЖ қорғау әдістері:

- басқару;
- кедергілер;
- бүркемелеу;
- регламенттеу;
- талаптану;
- мәжбүрлеу.


Ақпаратты қорғау әдістері
Ақпараттық
Криптографиялық
Программалық
Ұйымдастырушылық

Ақпараттық қауіпсіздікке төнетін қауіптер және ақпараттар ағып кететін арналар

(Угрозы информационной безопасности и каналы утечки информации)

Компьютерлік жүйедегі (КЖ) ақпараттардың қауіпсіздігіне төнетін қауіп дегеніміз оларда өңделген ақпараттардың қорғалуының бұзылуынан КЖ-дің қызмет етуінің өзгерісін тудыратын оқиғалар немесе әрекеттер.

«Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының Заңына ЖАДЫНАМА

Жарияланған күні: 26 желтоқсан 2016 - 19:05

Жаңартылған күні: 26 желтоқсан 2016 - 19:06

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ЗАҢНАМА ИНСТИТУТЫ

«Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының Заңына ЖАДЫНАМА

*Құқық берілген тұлғалар – **ақпарат жайында алынатын***

«Әркімнің заң жүзінде тыйым салынбаған кез келген тәсілмен еркін ақпарат алуға және таратуға құқығы бар».

Қазақстан Республикасы Конституциясының 20 бабының 2 тармағы

*Міндетті тұлғалар – мемлекеттік органдар, мекемелер және т.б. – **ақпарат иеленушілер** болып табылады*

«Әрбір адамның ақпаратты еркін алуға және тарату құқығы адам құқықтар

Адам құқықтарының жалпыға бірдей декларациясы;

Азаматтық және саяси құқықтар туралы халықаралық пакті (Қазақстан 2006 жылы ратификациялады)

«Ақпаратқа қол жеткізу туралы» Заң

«Ақпаратқа қол жеткізу туралы» Заң (бұдан әрі – Заң) мемлекет істерін басқарудағы қоғам қатысуының маңызды құралы және салық т

Бұл заң мемлекетке, қоғамға және адамға қандай пайда әкеледі?

1.Мемлекеттік басқаруды реформалау (ашықтық және есептілік);

Ақпараттық қауіпсіздікк қауіп төндіруді мынандай түрлерге бөлуге болады:

- адамның іс әрекетінен тәуелсіз (табиғат құбылыстарының ақпараттарға әсер ететін табиғи физикалық қауіптері);
- адамның іс әрекеті арқылы туындайтын (жасанды қауіптер), олар алдынғыларына қарағанда аса қауіпті болып саналады.

Жасанды қауіптер өздерінің туындау жағдайларына байланысты алдын- ала ойластырылмаған (кездейсоқ) және алдын -ала ойластырылған (қасақана) болып бөлінеді.

Алдын-ала ойластырылмаған қауіпке жататындар:

- КЖ –ні жобалау кезіндегі қателіктер;
- КЖ-нің бағдарламалық құрылымын жасау кезіндегі қателіктер;
- КЖ-нің аппараттық қондырғыларының, байланыс желілерінің, энергиямен қамтушылардың жұмысы кезіндегі кездейсоқ апаттар;
- КЖ-ні пайдаланушылардың қателіктері;
- КЖ-нің аппараттық қондырғыларына басқа да электрондық қондырғылардың физикалық өрістерінің әсері (олардың электромагниттік үйлесімділік шарттарының сақталмауы) және т.б.

ҚАСАҚАНА ҚАУІПТЕРГЕ ЖАТАТЫНДАР:

- КЖ-ге қызмет көрсетуші тұлғалардың санкцияланбаған әрекеттері (мысалға, КЖ-нің қауіпсіздігіне жауапты әкімшілік қызметкерінің қауіпсіздік саясатын әлсіретуі);
- КЖ-нің ресурстарына КЖ-ні пайдаланушылар мен бөгде адамдардың санкцияланбаған енуі, мұндағы келтірілген зиян тәртіп бұзушының іс-әрекетімен анықталады.

КЖ-ДЕГІ АҚПАРАТТЫҢ ҚАУІПСІЗДІГІНЕ ЖАСАЛЫНҒАН АЛДЫН-АЛА ОЙЛАСТЫРЫЛҒАН ҚАУІПТЕР МАҚСАТЫНА БАЙЛАНЫСТЫ НЕГІЗГІ ҮШ ТОПҚА БӨЛІНУІ МҮМКІН:

- Бүтіндіктің бұзылуына жасалынған, яғни КЖ-де сақталған немесе КЖ-лер арасында берілген ақпаратқа алдын-ала ойластырылған қауіп;
- Бүтіндіктің бұзылуына жасалынған, яғни КЖ-де сақталған немесе КЖ-лер арасында берілген ақпаратқа алдын-ала ойластырылған қауіп;
- Ақпараттың қол жетімділігінің бұзылуына жасалынған, яғни КЖ-ні пайдаланушылардың біреуінің (тәртіп бұзушының) алдын-ала ойластырылған әрекетінен туындайтын қызметт етуден бас тарту, бұл жағдайда КЖ-нің кейбір ресурстарына КЖ-ні басқа пайдаланушылар тарапынан ену жабылып қалады.

Компьютерлер мен желілердегі ақпаратты қорғаудың ұйымдық және техникалық құралдары

Ақпаратты қорғауды қамтамасыз ету үшін өткізілетін шаралар бірнеше бөліктерге бөлінеді. Соның ішінде негізгілерге мыналар жатады: ақпаратты қорғаудың құқықтық, ұйымдық, административті, инженерлік және техникалық қамтамасыздандыру.

Ұйымдық шаралар мыналардан тұрады:

- Қорғалушы кәсіпорынның ортақ аумағы мен қорғаныс шекарасын бөлу маскатымен әр корпусты жекелей және қорғалу деңгейі бойынша аумақты дамытуды жоспарлау;
- Қызметкермен жұмыс (жұмысқа қабылдау үшін сұхбаттасу, жұмыстан шығару, қызметкердің көңіл-күйі мен психологиялық жағдайын бақылау);
- Бейнебақылау жүйесін, күзеттің өткізу режимін, сонымен қатар құжаттарды/қағаз және электронды тасымалдаушыларда сақтау үшін сенімді сақтау орнын қамтамасыз ету.

Техникалық қорғау келесі құралдарды қолданады [1]:

- Физикалық құралдар;
- Аппараттық құралдар;
- Программалық құралдар;
- Криптографиялық құралдар

Компьютерлік желілердегі ақпаратты қорғау бойынша ұйымдық шаралар келесі аспектілерден тұрады:

- Желінің дұрыс физикалық ұйымдастырылуы.
- Қауіпсіздік критериіне сүйене отырып, желінің аппараттық қамтамасын таңдау.
- Логиндерді беру менесеп берудің орталықтандырылған саясатына кіріспе.
- Қолданылатын программалық қамтаманың корпоративті стандартын өңдеу және ендіру.
- Ақпаратты қорғаумен тікелей немесе жанама айналысатын қызметкерлерді өндіріс штатына енгізу.
- Қауіпсіздік критериіне сүйене отырып, қолданушының жұмыс орнын дұрыс ұйымдастыру.
- Жүйенің қорғалғандығын (аудиттің) желінің әлсіз қорғалған аумақтары мен ақауларды шығару мақсатымен жиі тексеруден өткізіп отыру.

Компьютерлік желілердегі ақпаратты қорғау бойынша негізгі техникалық шаралар болып:

- Жұмыс тобы немесе доменнің парольдік қорғалуын енгізу мен жақтау.
- Программалық жамауларды өз уақытында орнату, қолданылатын программалық қамтаманың (ПҚ) жаңа версиялары мен жаңартулар.
- Желіаралық экрандар мен антивирустық ПҚ-ны орнату.
- Қолданушының идентификациялары/аутентификацияларының қосымша жүйелерін орнату.
- Жүйелік блоктың ішкі құрамына қатынауды қиындататын қорғау механизмдерін орнату.
- Техникалық арна бойынша ақпараттың азаюынан қорғаудың аппараттық құралдарын орнату.

Компьютерлік вирустар.

Программалық вирустар.

Макровирустар.

Компьютерлік вирустардан қорғау әдістері.

Антивирус қорғау құралдары.

Программалық вирус – бұл автоматтандырылғанжүйелерде сақталатын және программалық қамтаманы жою немесе өзгерту мақсатымен телекоммуникациялық желілер мен автоматтандырылған жүйелердегі өзіндік туындау мен рұқсатсыз таралу қасиетіне ие болатын орындаушы немесе интерпретацияланатын программалық код.

Компьютерлік вирустардың өмірлік циклі

Биологиялық вирустар тәрізді компьютерлік вирустардың өмірлік циклі әдеттегідей келесі фазалардан тұрады:

- Вирусқа ешқандай әрекет қолданылмайтын белгісіз кезең;
- Вирус тек қана көбейетін инкубациялық кезең;
- Көбеюмен қатар қолданушымен рұқсатсыз әрекет орындалатын көрініс кезеңі.

Компьютерлік вирустардың негізгі түрлеріне мыналар жатады:

- программалық вирустар;
- жүктелетін вирустар;
- макровирустар.

Программалық вирустар. Программалық вирустар – басқа қолданбалы программаның ішіне мақсатты түрде ендірілетін программалық кодалардың блогы вирусы барпрограмма жұмыс атқарғанда ондағы вирустық кода іске қосылады. Бұл кода қатты дискіде және басқа программаның файлдық жүйесінде пайдаланушыға көрінбейтін өзгерістер жасайды. Мысалы, вирустық кода басқа программалар денесінде өзін - өзі қайталайды. Бұл процесті *көбейу* деп атайды. Белгілі бір уақыт өткенне соң көшірмелердің белгілі бір санын құрған соң, программалық вирусты бүлдіру әрекетіне көшеді: - программамен ОЖ –ның жұмысын бұзады, қатты дискідегі ақпаратты жояды. Бұл процесті
вирустік шабуыл деп атайды.

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

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

Макровирустар. Вирустың бұл түрі макроклманданы орындауға арналған құралдары бар қолданбалы программалардағы құжаттардыбүлдіреді. Мысалы, мұндай құжаттарға Microsoft Word (dos кеңейтуі бар) мәтіндік процессорының құжаттары жатады. Егер макрокоманданы орындалу мүмкіндігі өшірілмесе, онда құжат файл ашқанда жұқтыру басталады. Шабуыл нәтижесі арқылы болуы мүмкін, өте қауіпсіз еместей қалпына келтіруі қиын бүлдіруге дейін апара алады.

Компьютерлік вирустардың классификациясы

Компьютерлік вирустар келесі белгілерге сәйкес классификацияланады:

- Тіршілік ортасы;
- Тіршілік ортасын зақымдау тәсілі;
- Активтеу тәсілі;
- Көрсету тәсілі;
- Маскировка тәсілі.

Вирустарды активтеу тәсілдері

Активтеу тәсілінен тәуелді бөлінеді:

- Резидентті емес вирустар;
- Резидентті вирустар.

Вирустардың деструктивті әрекеттері

- Вирустардың пайда болуы (деструктивті әрекеттермен):
- ДЭЕМ-ның жұмысына әсер ету;
- Программалық файлдардың бұзылуы;
- Мәліметтері бар файлдардың бұзылуы;
- Дискі немес оның бөлігін форматтау;
- Дискідегі немесе оның бөлігіндегі ақпаратты ауыстыру;
- BR немесе MBR дискінің бұзылуы;
- FAT бұзылу жолымен файлдар байланысының бүлінуі;
- CMOS-жадыдағы мәліметтердің бұзылуы.

Вирусты маскировкалау тәсілдері

Маскировкалау тәсілдеріне сәйкес бөлінеді:

- Маскировкаланбайтын вирустар;
- Өзіндік шифрленетін вирустар;
- Стелс-вирустар.

Стелс-вирустармен қолданылатын маскировкалау әдісі кешенді сипаттан тұрады және екі категорияға бөлінуі мүмкін:

- Вирустасымалдаушы-программада вирустың болуын маскировкалау;
- ОЖСҚ(ОЗУ)-да резидентті вирустың болуын маскировкалау.

Вирустардың бар болу белгілері

- Дискідегі файлдар санының ұлғаюы;
- Бос оперативті жады көлемінің азаюы;
- Файлды құру уақыты мен мерзімінің өзгеруі;
- Программалық файл өлшемінің ұлғаюы;
- Программаның дұрыс жұмыс жасамауы;
- Программа жұмысының бәсеңдеуі;
- Дискіге айналу болмау керек кезде дисководта лампочканың жануы
- Қатты дискіге қатынау уақытының айрықша өсуі;
- ОЖ жұмысындағы ақаулар, әсіресе, оның тұрып қалуы;
- Файлдық құрылымның бүлінуі (файлдардың жоғалуы, каталогтардың бұзылуы).

Желі құрттары

Берілген категорияға төмендегі мақсатпен жергілікті немесе ауқымды желілер арқылы өзінің көшірмелерін тарататын программалар жатады:

- өшірілген компьютерлерге ену;
- өшірілген компьютерге өзінің көшірмесін жіберу;
- желімен басқа компьютерлерге таралу.

Өзінің таралуы үшін желілік құрттар әртүрлі компьютерлік және мобильді желілерді қолданады: электронды пошта, лездік хабарлармен алмасу жүйесі, файл алмастырулар (P2P) және IRC желілер, LAN, мобильді құрылғылар арасында мәліметтер алмастыру желісі (телефондармен, қалта компьютерлерімен) және т. б. Белгілі құрттардың көбісі файлдар түрінде тарайды: электронды хаттарға салу, қандай да веб- немесе FTP ресурста ICQ- және IRC-хабарларда зақымдалған файлға сілтеме, P2P алмасу каталогындағы файл және т. б.

Троянды программалар

Берілген категорияға қолданушымен әртүрлі рұқсатсыз әрекеттерді іске асыратын программалар кіреді: ақпаратты жинау және оны қаскүнемге беру, оның бұзылуы немесе арам ниетті модификацияны, компьютердің жұмысістеу қабілетінің бұзылуы, лайықсыз мақсаттардағы компьютер ресурстарын қолдану.

Троянды программалардың жеке категориялары зақымдалған компьютердің жұмыс істеу қабілетін бұзбай, өшірілген компьютерлер мен желілерге нұқсан келтіреді (мысалы, желінің өшірілген ресурстарындағы массирленген DoS-шабуылдар үшін жасалған троянды программалар).

Хакерлік утилиттер және басқа зиянды программалар

Берілген категорияға жататындар:

- вирустарды, құрттар мен троянды программаларды (конструкторлар) құруды автоматтандырудың утилиттері;
- зиянды ПҚ-ны құруға арналып жасалған программалық кітапханалар;
- антивирустық тексеруден зақымдалған файлдар кодын жасырудың хакерлік утилиттері (файлдарды шифрлеушілер);
- компьютер жұмысын қиындататын «қатал әзілдер»;
- қолданушыға өзінің жүйедегі әрекеттері жайлы жалған ақпарат беретін программалар;
- мәліметтерге немесе өшірілген компьютерлерге әр түрлі тәсілмен әдейі тікелей және жанама нұқсан келтіретін басқа да программалар.

Антивирустық құралдар классификациясы

Антивирустық құрал деп келесі функциялардың біреуін немесе бірнешеуін орындайтын құрылғы немесе программалық өнімді айтады:

- Бүлінуден мәліметтерді қорғау (файлдық құрылымды);
- Вирустарды табу;
- Вирустарды нейтрализациялау.

АЖ-ДІ ҚОРҒАУДЫҢ КРИПТОГРАФИЯЛЫҚ ҚҰРАЛДАРЫ

- *Ақпаратты шифрлеу* оны жасау кезінде қолданылатын, ақпараттың мазмұны басқа қолданушы субьектіге түсініксіз болатын үрдіс. Ақпаратты шифрлеу нәтижесі *шифрлі мәтін* немесе *криптограмма* деп аталады. Шифрлі мәтінннен ақпаратты қалпына келтіретін кері үрдіс ақпараттың *шифрін шешу* (расшифровка) деп аталады. Ақпаратты шифрлеу және шифрді шешу кезінде қолданылатын алгоритмдер конфиденциальды емес, шифрлі мәтінің конфиденциальдығы шифрлеу кезінде қолданылатын қосымша параметрлердің, *шифрлеу кілтінің* көмегімен жүзеге асырылады. Шифрлеу кілтін білу шифрлі мәтінді дұрыс шешуге көмектеседі.

Мәліметтердің криптографиялық өзгеру әдістері:

- Шифрлеу.
- Кодтау.
- Басқа түрлері.

Шифрлеу – қорғалатын хабардың әрбір символы өзгеруге ұшырайды.

Шифрлеу тәсілдері:

- ауыстыру;
- алмастыру;
- аналитикалық өзгеру;
- гаммирлеу;
- аралас шифрлеу.

Кодтау – қорғалған элементтердің кейбір элементтері (жеке символдар міндетті емес) алдын ала таңдалған кодтармен ауыстырылады.

Кодтау тәсілдері:

- мағыналық кодтау;
- символдық кодтау.

Басқаларға (жеке түрлеріне) – кесу, тарату және мәліметтерді қысу әдістері кіреді.

- ***Кесу*** – мәліметтерді тарату, қорғалатын мәліметтер массиві әрқайсысы қорғалатын ақпараттар мазмұнын ашуға мүмкіндік бермейтін элементтерге бөлінеді және осындай тәсілмен ерекшеленген элементтер есте сақтау құрылғысының әртүрлі аумағында орналасады.

Криптожүйелер екі класқа бөлінеді:

- Симметриялық (біркілтті) криптосистемалар.
- Асимметриялық (ашық кілті бар екікілтті криптосистемалар).

Криптожүйелерге қойылатын талаптар:

- Шифрленген хабар тек кілт болғанда ғана оқылуы тиіс.
- Шифрленген хабар фрагменті бойынша шифрлеудің қолданылған кілтін анықтау үшін қажетті операциялар саны және оған сәйкес ашық мәтін мүмкін болатын кілттердің жалпы санынан аз болмауы керек.
- Барлық мүмкін болатын кілттерді артық таңдау жолымен ақпараттарды шифрлеуді ашу үшін қажетті операциялар саны қатал төмен бағамен болуы тиіс және қазіргі компьютерлердің мүмкіндіктерінің (тораптық есептеу мүмкіндіктерін ескере отырып) шегінен шығуы керек.
- Шифрлеу алгоритмін білу қорғау сенімділігіне әсер етпеуі тиіс.
- Кілттің аздап өзгеруі бір кілтті ғана қолданғанның өзінде шифрленген хабар түрінің елеулі өзгеруіне әкелуі тиіс.

- Шифрлеу алгоритмінің құрылымдық элементтері өзгеріссіз болуы керек.
- Шифрлеу процесінде хабарға енгізілетін қосымша биттер шифрленген мәтінде толық және сенімді жасырылуы тиіс.
- Шифрленген мәтіннің ұзындығы бастапқы мәтіннің ұзындығына тең болуы тиіс.
- Шифрлеу процесінде тізбектей қолданылатын кілттер арасында жай және жеңіл орнатылатын тәуелділіктер болмауы керек.
- Мүмкін болатын жиындардың ішіндегі кез келген кілт ақпаратты сенімді қорғауды қамтамасыз етуі тиіс.
- Алгоритм программалық тәрізді аппараттық іске асуды жіберуі тиіс, бұл жағдайда кілт ұзындығының өзгеруі шифрлеу алгоритмінің сапалы төмендеуіне әкелмеуі керек.

Ашық кілтті криптожүйелер

Ашық кілтті криптожүйелер классикалық және қазіргі кездегі алгебра негізінде өңделген (Диффи және Хеллман, 1975ж.)

Оның мәні: АЖ-ның әрбір адрес иесімен арнайы ереже бойынша өзара байланысқан екі кілт генерацияланады: 1-ші кілт – **ашық**, екіншісі – **жабық**.

Бір кілт ашық болып жарияланса, екіншісі жабық болады. Ашық кілт жарияланады және адрес иесіне хабар жібергісі келген кез келген адамға ашық. Жабық кілт адрес иесімен құпияда сақталады. Бастапқы мәтін ашық кілтпен шифрленеді және адрес иесіне беріледі. Хабардың шифрін ашу адрес иесінің өзіне ғана белгілі жабық кілтті қолдану арқылы жүзеге асуы мүмкін.

Симметриялық криптожүйелер. Алмастырулар

Хабарларды шифрлеу кезінде де, шифрлеуді ашқанда да бір құпия кілт қолданылады.

Қолданылатындар:

- алмастыру шифрлары;
- ауыстыру шифрлары;
- гаммирлеу шифрлары;
- шифрленген мәліметтердің аналитикалық өзгерулері негізіндегі шифрлар.

Практикада **аралас жүйелер** жиі кездеседі – бір шифрленген мәтінге қолданылатын криптографиялық өзгерулердің негізгі әдістер тізбегі. (Ресейлік және американдық шифрлеу стандарттары дәл осы аралас криптографиялық өзгерулерге негізделген).

Алмастыру шифрлары

Бастапқы мәтіннің $T=(T_1, T_2, T_3, \ldots, T_N)$, символдарын алмастыру дегеніміз - оның қайта реттеліп, символдың i позициясынан $\sigma(i)$ позициясына ауысуын атайды, мұндағы .

Мысалы, «Пришлите помощь» мәтіні 15, 2, 5, 7, 9, 1, 6, 13, 11, 4, 14, 3, 12, 10, 8 кілттер негізінде «ЬРЛТ - ПООШЩИМПЕ» хабарына шифрленеді.

Алмастырулар шифрленген кестелермен жиі беріледі. Кілт түрінде шифрленген кестелерде мыналар қолданылады:

- кесте көлемі
- алмастыруға берілетін сөз немесе сөйлем
- кесте құрылымының ерекшеліктері

Мысалы, 5*3 кестесі бойынша «завтра была война» мәтіні «ЗАВАБОВЫЙТЛНРАА» түрінде шифрленеді.

З	А	В	Т	Р
А	Б	Ы	Л	А
В	О	Й	Н	А

Мәтін: «АЗРВТБААЫЛОВАЙН »

Алмастырудың ең сенімді класы - төмендегі кілт негізіндегі жолды-баған алмастырулар:

З	А	М	О	К
2	1	4	5	3
З	А	В	Т	Р
А	Б	Ы	Л	А
В	О	Й	Н	А

А	З	К	М	О
1	2	3	4	5
А	З	Р	В	Т
Б	А	А	Ы	Л
О	В	А	Й	Н

Мысалы, «ЗАМОК» кілті бар «ЗАВТРА БЫЛА ВОЙНА» мәтіні «АЗРВТБААЫЛОВАЙН» түрінде шифрленеді.