Компьютерлік желілерде ақпаратты қорғау

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 конфиденциалдығы – бұл оның мазмұнының тек иеленуші субьектіге ғана белгілілігі.

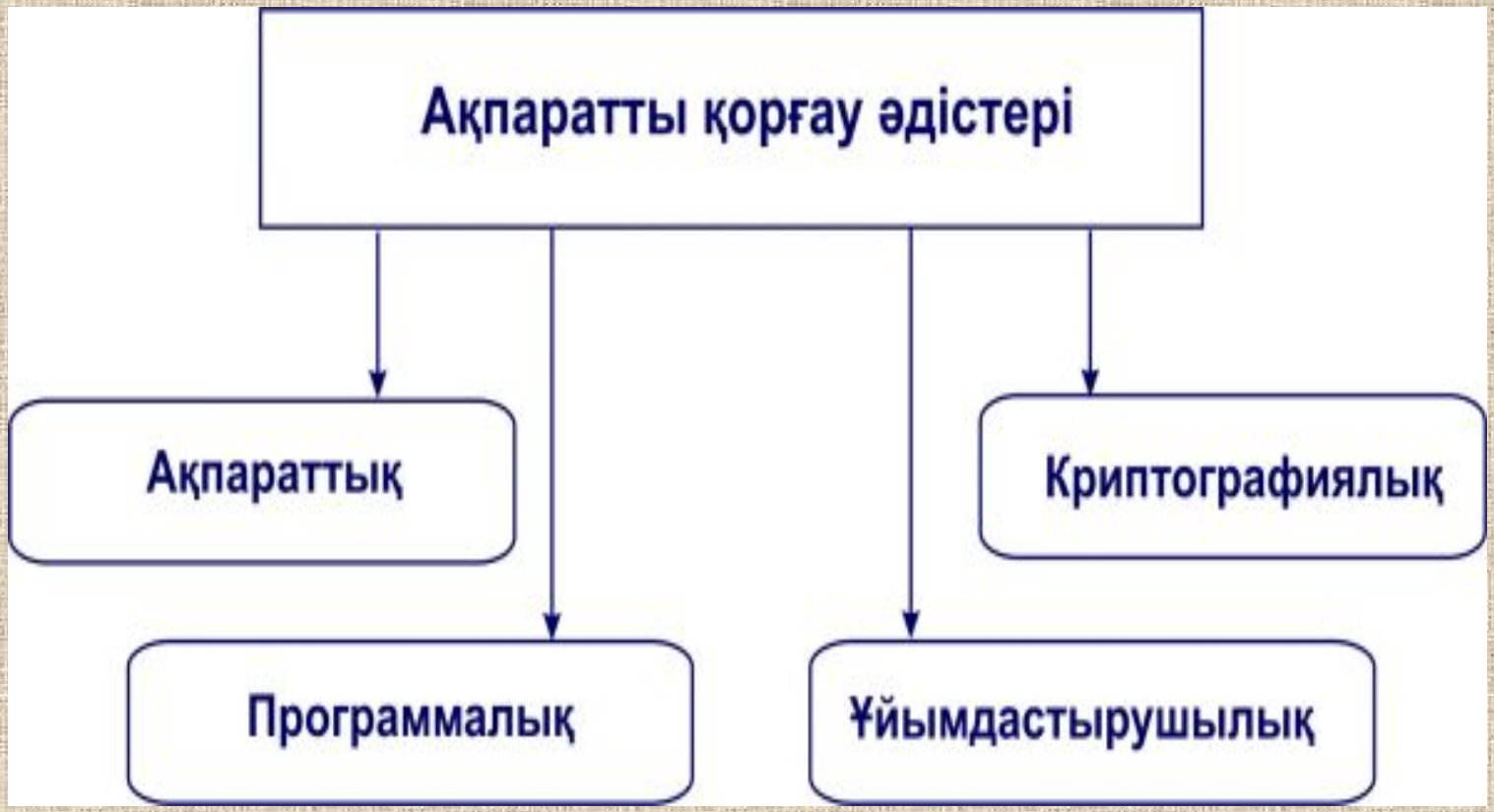
Конфиденциальдық – ақпараттың құқықтық қызығушылығын қорғайтын, обьективті қажеттілікпен байланысты, ақпараттың субьективті сипаттамасы болып табылады.

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 қорғау әдістері:

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


Ақпаратты қорғау әдістері
Ақпараттық
Криптографиялық
Программалық
Ұйымдастырушылық

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.

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.