ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Ш. ЕСЕНОВ АТЫНДАҒЫ КАСПИЙ МЕМЛЕКЕТТІК ТЕХНОЛОГИЯЛАР ЖӘНЕ ИНЖИНИРИНГ УНИВЕРСИТЕТІ
ПЕДАГОГИКАЛЫҚ ТЕХНОЛОГИЯЛАР ИНСТИТУТЫ

Қанатбаева Ж.Д.

«Компьютерлік ақпаратты қорғаудың құралдары мен тәсілдері»

Педагогикалық технологиялар институтының студенттеріне арналған әдістемелік нұсқау

АҚТАУ-2010

ӘОЖ 004.3 (073, 8)

Қанатбаева Ж.Д.

Компьютерлік ақпаратты қорғаудың құралдары мен тәсілдері: Әдістемелік нұсқау. – Ақтау қ. КМТжИУ,2010, 46 бет.

Пікір жазған: Педагогика ғылымдарының кандидаты С.Н. Идрисов

Бұл әдістемелік нұсқауда компьютерлік ақпаратты қорғауда пайдаланатын дағдыларын толық меңгеру үшін педагогикалық технологиялар институтының студенттеріне арналған қосымша дәрістер мәнжазбалары ұсынылған.

Ш.Есенов атындағы Каспий Мемлекеттік Технологиялар және Инжиниринг Университетінің Педагогикалық Технологиялар институтының оқу-әдістемелік кеңесінің шешімімен баспаға ұсынылды.

© Қанатбаева Ж.Д.,2010

Ш. Есенов атындағы Каспий мемлекеттік технологиялар және инжиниринг университеті

МАЗМҰНЫ **беті**

Компьютерлік ақпаратты қорғаудың құралдары мен тәсілдері.

Дәріс №1. Кіріспе. Ақпараттық қауіпсіздік..... 4
Дәріс №2. Ұлттық қауіпсіздік түсінігі және оның түрлері..... 7
Дәріс №3.. Ақпараттық қауіп..... 9
Дәріс №4. Ақпаратты қорғау амалдары мен тәсілдері..... 11
Дәріс №5. Қорғаныс саясаты және стандарттары..... 14
Дәріс №6. Қауіпсіздік жүйесін практикалық іске асыру..... 17
Дәріс №7.. Симметриялық криптожүйелер..... 21
Дәріс №8..... Симметриялық криптожүйелер..... 25
Дәріс №9.. Компьютерлік жүйені бұзу тәсілдері..... 28
Дәріс №10. Ақпаратты қорғау дұрыстығының әдістемесі..... 31
Дәріс №11. Ақпаратты қорғау жүйесіне баға беру..... 33
Дәріс №12. Ақпаратты қорғаудың компоненттері..... 36
Дәріс №13 Компьютерлік желілердің қауіпсіздік ерекшеліктері..... 37
Дәріс №14. Ауқымды желідегі ақпаратты қорғау..... 39
Дәріс №15. Компьютерлік жүйелер қауіпсіздігі..... 42

Пайдаланған әдебиеттер тізімі..... 46

Дәріс №1

Тақырыбы: Кіріспе. Ақпараттық қауіпсіздік

Мақсаты: Ақпараттық қауіпсіздік пәніне кіріспе, пән мақсатын түсіндіру.

Жоспар:

1.1. Ақпаратты қорғау-ақпараттық қауіпсіздік пәнінің объектісі

1.2 Ақпаратты және ақпараттық жүйені қорғау мәселелері

Кілттік сөздер: Ақпарат, ақпараттық қауіпсіздік, ақпараттық жүйе

1.1 Ақпаратты қорғау-ақпараттық қауіпсіздік пәнінің объектісі

Жалпылама компьютерлендіру және жаңа ақпараттық технологиялардың дамуы міндетті түрде бүкіл ақпаратты қорғау ғана емес сонымен бірге ақпараттық жүйенің мінездемелерінің бірі болуда. Бірінші дәрежелі роль атқаратын қорғаныс факторын жинақтауда ақпараттарды өңдеу жүйесінің барынша кеңейтілген класын көруге болады (мысалы, банкілік ақпараттық жүйе).

Ақпараттық жүйені қорғау- деп жүйенің қалыпты процессіне, оның функциялануына абайсызда немесе әдейі кедергі келтіруден, ақпаратты ұрлауға әрекет жасаудан (жасырылған ақпаратты алу) және компоненттерін физикалық бүлдіруден қорғауды айтады. Басқаша айтқанда ақпараттық жүйеге жасалған қарсы әрекетке қарсы тұра алу мүмкіндігі.

Ақпараттық қорғаудың қауіп-қатері деп кедергі әсерінен бүлінуге соқтыру, бекітілмеген қолданулар және де тіпті басқарушы жүйенің, бағдарламалық және аппараттық амалдардың ақпараттық ресурстарының бұзылуын түсінуге болады. Егер де кез-келген басқарушы жүйенің кибернетикалық моделін классикалық жағынан қарағанда шығатын оған қарсы әрекеттер кездейсоқ мінездеме алады. Сондықтанда, ақпаратты қорғаудың қатерлері арасында *кездейсоқ* немесе *<u>арнайы емес</u> (непреднамеренные)* қауіп түрін бөліп алу керек. Оның негізіне аппараттық құралдардың жұмыс істемей қалуы, ақпараттық жүйемен жұмыс істейтін жұмысшылардың немесе оны пайдаланушылардың дұрыс қолданбауы, бағдарламалық қамтамасыз етуде арнайы емес қателер болуы және т.с.с жатады. Мұндай қатерлерді де шығын еленбейтіндей болғандықтан назарда ұстауға болады. Дегенмен берілген тарауда кездейсоқ қауіпке қарағанда басқару жүйесі немесе қолданушыға шығын келтіру мақсатында ұйымдастырылған қауіптерге назарды көбірек аударамыз. Бұл жеке табысқа жету үшін жиі қолданылады. Ақпараттық жүйенің жұмысын бұзуға тырысатын немесе ақпаратқа бекітілменген рұқсат алатын адамдарды әдетте бұзушылар, кейде *“компьютерлік қарақшылар”*(хакерлер) деп атайды. Бөгде құпияларды басқаруға бағытталған өздерінің заңға қайшы әрекеттерінде бұзушылар анығырақ және ең үлкен көлемде жасырын ақпараттар көзін ең аз шығынмен табуға ұмтылады. Әр түрлі

айлалар және көптеген тәсілдер, түрлі жолдарды таңдаудың көмегімен күрделі ақпарат көздеріне қол жеткізе алады. Берілген жағдайда ақпарат көзі айла ойлаушы немесе бәсекелестердің нақты қызығушылығын тудыратын мағұлматтарды анықтауды басқаратын материалды объект.

1.2 Ақпаратты және ақпараттық жүйені қорғау мәселелері

Бүгінгі таңда компьютерлік ақпараттық жүйелерде және мәліметті жіберу желілерінде ақпаратты қорғау технологиясы - жаңа қазіргі заманғы технология тууда деп бекітуге болады. Бұл технологияның іске асырылуы өсуші шығындарды және күш салуды талап етеді. Дегенмен бұл ақпараттық жүйе және ақпараттық технология нақты қауіп төну кезінде көзге түсерліктей аса басым түсетін шығындар мен залалдардан құтылуға мүмкіндік береді.

Ғылыми-техникалық революция соңғы кездерде қоғамды ақпарат-тандыру аумағында есептеу техникасының қазіргі заманғы амалдар базасында, байланыстарда, сонымен қатар ақпаратты өңдеуді автоматтан-дырудың қазіргі заманғы тәсілдерінде көрнекті масштабтарды қабылдады. Бұл әдістер және тәсілдер негізінде құрылған ауқымдық яғни аумақтарға бөлінетін бірдей технологиялық процестерді жинақтауда, жіберуде, сақтауда, іздеуде, ақпараттарды өңдеуде және оларды қолдану үшін жіберуде ақпараттық – есептеуіш жүйелер мен желілерге айналу жалпылама мінездемеге ие болды.

Қазіргі замандағы ақпарат – оған рұқсаты жоқ бекітілмеген адамнан қорғауды қажет ететін өмірдегі өте қымбат заттардың бірі.

Жиырмасыншы жылдардың ортасында бірінші электронды-есептеуіш машиналардың шығуы шифрлеу аумағында жағдайды түбегейлі өзгертті. Компьютердің өмірімізге енуі, олардың әр түрлі сфераларға кіруі жаңа бір саланың – ақпараттық индустрияның пайда болуына әкелді.

Ақпаратты қорғау құралдарымен керекті дәрежеге дейін қамтамасыз ету өте қиын болып табылды (бұл теориялық зерттеулермен бекітілгендей, тәжірибелі іс-тәжірибе шешімі арқылы бекітілді). Ол ғылыми, ғылыми-техникалық жиынтықтарды, ұйымдастырылған амалдар қолдануды және амалдар мен тәсілдерді жүзеге асыруды талап етті.

Қоғамда айналып жүруші ақпараттар көлемі тұрақты өсуде. Бүкіл әлемдік желі интернеттің атақтылығы соңғы жылдарда, жыл сайын ақпараттың екі есе көбеюіне апарды. Шынайы тұрғыдан қарағанда жаңа мыңжылдық табалдырығында адамзат ақпаратты өңдеудің табыстылығынан тыныштық және тіпті адамзат өмірінің әрі қарай жалғасуына қатысы бар ақпараттық өркениетті құрды. Осы уақыт мерзімінде болған өзгерістерді келесі жолдармен суреттеуге болады:

- өңделуші ақпараттардың көлемі жарты ғасырда бірнеше ретке өсті;
- анықталған мәліметтерге рұқсат алу материалдық және қаржылық құндылықтарға көрнекті бақылау жасауға мүмкіндік береді; ақпарат санауға болатындай бағаға ие болды;
- өңделуші мәліметтер қалыптан тыс, әр алуан, әсіресе текстік мәлімет болып келді;

Жоғарыдағы өзгерістерден кейін іскер ортада компьютерлердің жылдам таралуы криптографияның бірден бірнеше бағытта өсуіне әкелді:

- Біріншіден, мықты кілттік бағана құрылды. Ол криптографиялық ортада жіберілетін және сақталынатын ақпараттардың құпиялылығын және толықтығын қамтамассыз етеді. Бұл кілттік бағана криптографиялық қорғаныстар тәсілдері ретінде қазірге дейін қолданылады;
- Екіншіден, ақпаратты қорғау ортасында жаңа тапсырмалардың шешімдеріне жету тәсілдері шығарылды. Ол сандық құжаттардың қолтаңба-сының және кілттердің ашық түрде жіберілуінің ең танымал түрі болып табылады.

Қазіргі әлемде ақпараттық ресурс экономиканың өсуіне қарай мықты рычагтардың бірі болды. Керекті дәрежеде, керекті уақытта ақпаратты иемдену кез-келген шаруашылықтың тыбысына кепілдік береді. Бәсекелестік күресте көп көлемде ақпаратты иемдену маңызды роль ойнайды, сондықтан “ақпараттық фактор” жоғары бағаланады.

Бақылау сұрақтары:

1. Ақпарат қауіпсіздігі дегеніміз не?
2. Ақпараттық қауіпсіздік негіздері пәнінің мақсаты?
3. Ақпарат және ақпараттық жүйеге деген қауіптер?
4. Ақпарат қауібінен қорғану жолдары

Дәріс№2.

Тақырыбы:Ұлттық қауіпсіздік түсінігі және оның түрлері.

Мақсаты: Ұлттық қауіпсіздік түсінігімен жіне оның түрлерімен таныстыру

Жоспар:

2.1. Ұлттық қауіпсіздік және оның түрлері

2.2. Экономикалық қауіпсіздік

2.3. Әскери қауіпсіздік

2.4. Ақпараттық қауіпсіздік

Кілттік сөздер: ұлттық қауіпсіздік, ақпараттық қауіпсіздік, әскери қауіпсіздік, экономикалық қауіпсіздік.

2.1 Ұлттық қауіпсіздік және оның түрлері

Жаһандану үрдісі жағдайындағы жекелеген елдердің қауіпсіздігі көбіне әлемдік және аумақтық қауіпсіздікке, халықаралық қарым-қатынастардың түзілуіне, іргелес мемлекеттердегі саяси және экономикалық, әлеуметтік тағы да басқа мәселелерінің дамуына тығыз байланысты болып отыр. Қазақстан жағының бастамасымен сонау 1992 жылдың сәуір айында ТМД елдерінің барлау қызметтерінің ынтымақтастығы туралы келімге қол қойылды. Осыдан кейін барып тәуелсіз мемлекеттер достастығының, алыс және жақын шетелдердің (Ұлыбритания, Алмания, АҚШ, Қытай, Түркия, Корей Республикасы және т.б.) арнаулы қызметтері арасындағы ынтымақтастық туралы келісімдер мен протоколдарға қол жеткізілді. Қарсы барлау жұмысын оңтайландыру жұмысы тәуелсіз ел тарихында көптеген шетелдік арнаулы қызметтердің белсенділігін төмендетуге, қызметтерін кері бұруға, немесе оларды қауіпсіздік органдарының бақылауында ұстауға әсер етті.

Лаңкестікке шын мәнінде қарсы тұру мақсатында Қазақстан көптеген халықаралық санқырлы келісімдерге қосылды. Оның ішінде «лаңкестікпен, сепаратизммен және экстремизммен күрес туралы Шанхай конвенциясы», сондай-ақ лаңкестікті қаржыландырумен күрес, бомбалық лаңкестікпен күрес туралы конвенциялар бар.

2.2 Экономикалық қауіпсіздік

Экономикаға нұқсан келтіруі мүмкін үрдістер туралы алдын ала тиісті орындарды ақпараттандыру да қауіпсіздік органдарының маңызды міндеттерінің бірі болып табылады. Мемлекеттік экономикалық бағдарламаларға, жүргізіліп жатқан реформаларға қолдау көрсету, қаржылық-банктік жүйені сыртқы және ішкі қауіп-қатерлерден қорғау міндеті қауіпсіздік органдарына жүктелген. Есірткілік құралдар мен жүйкеге әсерлі заттардың халықаралық заңсыз айналымына қатысы бар ұйымдасқан қылмыстық топтар, қоғамдастықтармен күрес арнаулы қызметтің көптеген міндеттерінің бірі.

Ұлттық қауіпсіздік органдарының осы бағытта жүргізген жұмыстарына назар салсақ, мемлекеттік билік, сот, құқық қорғау, банк-қаржы, бизнес, тіпті әлеуметтік салаларға еніп кеткендігін айтып өту керек.

Әскери қауіпсіздік

Мемлекеттік шекараны орнықтыру және қорғау, Шекара Қызметін нығайту мен дамытуға байланысты мемлекеттік бағдарламаны әрдайым күн тәртібінде ұстап отыру стратегиялық маңызды міндеттердің бірі болып табылады. Айтарлықтай аз уақыт ішінде аталған қызметтің штаттық санын біртіндеп арттыру, шекара бойына құрамалар мен бөлімдер ұйымдастыру жұмыстары атқарылды. Инфрақұрылымдық, оның ішінде инженерлік-техникалық жүйе жасақталды. Материалдық-техникалық, қаржылық жағынан бұрындары бірнеше жылдарға созылатын жұмыстар қысқа мерзімде атқарылғандығын атап айту керек.

Аймақтық қауіпсіздікті нығайтудың бір саласы – арнаулы қызметтердің ынтымақтастық, өзара іс-қимыл мәселесіне тығыз байланысты, осы бағытта жүргізіліп жатқан түрлі іс-қимыл қадамдары, қабылданған келісімдердің орындалуы бірнеше жылдардан бері нәтижесін беруде.

2.3 Ақпараттық қауіпсіздік

Ақпарат қауіпсізідігін әртүрлі контексте әртүрлі ойдың мағыналарын ұйқастырады. Кең айтылған ой информациялық ортада ұлттық қызығушылықта қорғалғандай болады, жеке ортада немесе балансировты қызығушылық жиынтығын анықтайды.

Ақпаратты қорғау –бұл мәліметтердің қауіпсіздігін қамтамасыздандыру бағытындағы жиын.

Рұқсаттылық, бүтіндік, құпиялылық түсініктерін қарастырайық.

Рұқсаттылық-бұл аз уақыт аралығында қажет етілген ақпараттық қызметті алу болып табылады.Бүтіндік деп ақпараттың актуалдылығы мен қарсылық көрсетпеуін ж/е оның заңсыз бүлінуі мен өзгертілуінен қорғауды айтады. Ендеше,құпиялылық-бұл ақпаратты заңсыз қолданудан қорғау. Ақпараттық жүйелер белгілі бір ақпараттық қызметтерді алу үшін құрылады.Егер бұл қызметті кейбір себептермен қолданушыға тапсырсақ,ол барлық ақпараттық қарым-қатынасқа залалын тигізетіндігі белгілі.Сондықтан қалған аспектілерге рұқсаттылыққа қарсылық білдірмей,біз оны ақпараттық қорғаныстың маңызды элементі ретінде қарастырамыз.

Рұқсаттылықтың әсіресе маңызды ролі әр түрлі басқару жүйелерінде өндірістік, көліктік жүйелерінде көрінеді.Бүтіндікті статистикалық(ақпараттық объектілердің бір қалыптылығы ретінде түсіндіріледі)ж/е динамикалық(қиын жағдайларды дұрыс орындау)деп 2-ге бөлуге болады.Динамикалық бүтінділікті сақтау көбінесе ұрлықты

анықтайтын финанстық хабарламаларды тексергенде,қайта орналастырғанда және жеке хабарламаларды қайталау кезінде қолданылады.

Бақылау сұрақтары:

1. Ұлттық қауіпсіздік дегеніміз не?
2. Экономикалық қауіпсіздік шаралары?
3. Әскери қауіпсіздік мақсаттары?
4. Ақпарат қауіпсіздігін қорғау?

Дәріс№3

Тақырыбы:Ақпараттық қауіп

Мақсаты: Ақпараттық қауіп түрлерімен және оған қарсы шаралармен таныстыру.

Жоспар:

3.1. Ақпараттық қауіп түрлері.

3.2. Құпия ақпараттардың ағып кетуі

Кілттік сөздер: енжар, белсенді қауіп, ішкі жіне сыртқы қауіп, трояндық ат, вирус, құрт.

3.1. Ақпараттық қауіп түрлері.

Ақпараттық жүйенің ақпараттық ресурстарын бекітілмеген қолдану негізінде бағытталған *енжар* (пассивные) қауіп, ол сонымен қатар ақпараттық жүйенің функциялынуына әсерін тигізбейді. Мысалға, деректер қорына енуге бекітілмеген рұқсат алу, байланыс каналдарын тыңдау және т.б.

Белсенді (активные) қауіп, оның мақсаты арнайыланған әрекеттер арқылы ақпараттық жүйенің қарапайым функциялануын бұзу. Белсенді қауіптерге мысалға келесілер жатады: компьютерді немесе оның операциялық жүйесін істен шығару, деректер банкінің сипаттамасын бұрмалау, компьютердің бағдарламалық қамтамасыз етуін бұзу, сызықтық байланыс жұмысын бұзу және т.б. Белсенді қауіптер көзі бұзушылардың әрекеттері және зиян бағдарламалар және т.б. болып табылады.

Сонымен қатар алдын ала ойластырылған қауіптер *сыртқы* және *ішкі* (басқарушы ұйымның ішінде туындайтын) болып бөлінеді.

Ішкі қауіп көбіне арнайы қиындықтармен және ауыр моральдық климатпен анықталады.

Сыртқы қауіп бәсекелестердің залал келтіру үшін жасаған әрекетінен, экономикалық шарттан немесе басқада себептермен анықталады.(мысалға, апаттық жағдай).

Ақпарат қорғанысының негізгі қауіптеріне және ақпараттық жүйенің қарапайым функциялануына келесілер жатады;

- құпия ақпараттың ағып кетуі;
- ақпаратты компрометациялау;

- ақпараттық ресурстарды бекітілмеген жолмен қолдану;
- ақпараттық ресурстарды қателесіп қолдану;
- абоненттердің арасында бекітілмеген ақпарат алмасу;
- ақпараттан бас тарту;

Трояндық ат – негізгілерге қосымша әрекеттер орындайтын бағдарлама, яғни қайта жобаланған және құжатталған әрекеттерге олардың құжаттарында жазылмаған қосымша әрекеттерді орындайды. Трояндық аттар қатерлі әрекетті қолданушының жеңілдіктерінің кеңейтілген жиынына ие болса ғана орындай алады.

Вирус – басқа бағдарламаларды олардың түрлендірілген көшірмесін жасау жолымен зақымдайтын, алдағы уақытта көбейіп кету мүмкіндігі бар бағдарлама.

Вирус екі негізгі мінездememен ерекшеленеді деп есептелінеді:

1. өздігінен көбею мүмкіндігімен;
2. есептеу процесіне кедергі келтіру мүмкіндігімен (яғни басқару мүмкіндігіне ие болу).

Соңғы жылдары вируспен күресу проблемесы актуальды проблема болғандықтан көбі сонымен жұмыс жасауда. Бұған әртүрлі ұйымдастырылған құралдар қолданылады, жаңа антивирустық бағдарлама осы құралдардың барлығын енгізуге насихаттайды. Соңғы уақыттары зақымдалған және бұзылғандарды шектеу азды-көпті іске асырылуда. Бірақта тірі табиғаттағыдай, ол күресте толық жетістікке жеткен жоқ.

Құрт – желі арқылы таралатын бағдарлама, ол магниттік жинақтау-шыларда өзінің көшірмесін қалдырмайды. Құрт зақымдалатын желінің механизмінің анықталған бөлігінде қолданылады. Бұл вирустың ең танымал түріне - Internet желісін 1988 жылы зақымдаған Морриса вирусын (Морриса құртын) жатқызуға болады. Құрттан қорғанудың жақсы тәсілдерінің бірі - желіге бекітілмеген енуге қарсы алдын ала шаралар қолдану.

Құпия сөздерге шабуыл жасаушы – бұл бағдарлама арнайы құпия сөз-дерді ұрлауға арналған. Шабуыл жасаушы - бағдарламаның иесі компьютерге бағдарламасын енгізіп қояды. Содан соң қолданушы өз бағдарламасын ашу үшін өзінің есімін және құпия сөзін енгізгенде, оның компьютеріне шабуыл жасаушы бағдарламаны қайта жүктеңіз деген мәлімет шығарады.

3.2. Құпия ақпараттардың ағып кетуі

Құпия ақпарттардың ағып кетуі – ақпараттық жүйе аумағындағы арнайы жасалған ақпараттан бақылаусыз шығу. Бұл ағып кету келесі мәселелердің нәтижесінде туындауы мүмкін:

- арнайы жасалған ақпаратты жарыққа шығару;
- ақпаратты әр түрлі тәсілмен қарау, негізгі тәсіл техникалық, каналдық;

- арнайы жасалған ақпаратқа әр түрлі тәсілмен бекітілмеген енуге рұқсат алу;

Ақпаратты жарыққа шығару оны иемденуші немесе иесі ойлаған немесе байқаусыз әрекет арқылы арнайы жасалған ақпараттың визуальды-оптикалық, акустикалық, электромагниттік және басқада каналдармен бақылаусыз шығуы мумкін.

Ақпаратқа бекітілмеген ену рұқсаты- бұл қорғалған ортаға енуге құқығы жоқ тұлғалардың әдейі заңға қайшы жасалған ақпаратты иемденуі.

Ақпаратқа бекітілмеген енуге рұқсат алудың көп таралған жолдары келесідей:

- электронды сәуле шашуды ұстау;
- әкелінген паразитті модуляцияны алу мақсатында байланыс сызығына қиындықтармен электромагнитті сәуле түсіру;
- ОЖ және бағдарламалау тілдерінің жеткіліксіздігін қолдану;
- аппаратқа және байланыс желісіне ақпаратқа енуді қамтамасыз ететін арнайы өңделген аппараттық құралды заңсыз қосу;
- қорғау механизмін қасақана істен шығару;
- ақпараттық инфекциялар;

Бекітілмеген енуге рұқсат алудың алдын алу жолдары бар:

- құжаттық қалдықтарды және ақпараттық жинақтаушыларды тығып қою;
- жігерлі бірігіп жұмыс жасау;
- бұзушы жағынан бірігіп жұмыс істеуді ұйымдастыру;
- қиындықпен шынын айттыру;
- тыңдау;

Бақылау сұрақтары:

1. Ішкі және сыртқы қауіп дегеніміз не?
2. Трояндық ат дегеніміз не?
3. Вирус дегеніміз не?
4. Жеңілдіктерді заңсыз пайдалануды түсіндіріңіз?

Дәріс№4.

Тақырыбы:Ақпаратты қорғау амалдары мен тәсілдері.

Мақсаты: Ақпаратты қорғау амалдарымен және оның тәсілдерімен таныстыру.

Жоспар:

4.1. Ақпаратты қорғау амалдары мен тәсілдері

4.2. Қорғау амалдарының мақсаты

Кілттік сөздер: ақпараттық қорғаныс жүйесі, бөгет, шифрлеу механизмі.

4.1. Ақпаратты қорғау амалдары мен тәсілдері

Ақпараттық жүйе және ақпараттық технологияларға *ақпараттық қорғаныс жүйесін* (АҚЖ) құру келесі принциптерге негізделеді:

Ақпараттық өңдеудің технологикалық циклінің барлық этаптарын қолданудағы отандық және шетелдік қорғаныс жүйесін тәжірибе жүзінде құруды ұстанатын арақатынасы ұйымдастырылған бағдарламалық, аппараттық, физикалық және басқа да құрлығылардың оптимальді қиылысуын білдіретін қорғаныс жүйесін құрудағы *жүйелік жарасу.*

Жүйенің өсуінің үзіліссіз принципі. Бұл принцип компьютерлік ақпараттық жүйе үшін негізге алатын принциптердің бірі, және де ол АҚЖ үшін актуальді.

Өңдеу процедураларына және өңделуші ақпаратқа енуге рұқсат беру бойынша *өкілдікті азайту және бөлу*, яғни қолданушылармен қатар ақпараттық жүйе қызметкерлеріне де өздерінің қызметін атқаруға жеткілікті миминум анықталған өкілеттілік беру.

Бекітілмеген енуге рұқсат беру әрекетін тіркеу және толықтай бақылау, яғни әрбір қолданушының бірегейлігін толығымен қондыру қажет-тілігі және оның әрекетін хаттамалау.

Функцияланған қорғаныс жүйесіне бақылауды қамтамасыз ету, яғни қорғау механизмінің жұмыс жасау қаблеттілігіне бақылау жасау құралдарын не тәсілдерін құру.

Зиянды бағдарламалармен күресудің мүмкін болатын барлық құралдарымен қамтамасыз ету.

Қорғаныс жүйесін экономикалық мақсатқа лайықты қамтамасыз ету.

Қазіргі кездегі ақпараттық жүйе және ақпараттық технология ақпаратын қорғау қиыншылығын шешу нәтижесінде келесідей негізгі принциптер болуы керек:

- әртүрлі дәрежеде арнайыланып жасалған ақпараттардың бар болуы;
- ақпараттарды жіберу кезіндегі құпия ақпараттарды әртүрлі дәрежеде криптографиялық қорғаумен қамтамасыз ету;
- жергілікті желіде ақпаратты жіберу сияқты алшақ қашықтықтағы байланыс каналдарында ақпаратты жіберу міндетті түрде басқарылады;
- баспаға шығарылатын ақпараттық жүйедегі оқиғада және құжаттарда бекітілмеген енуге рұқсат алу амалын тіркеу механизмінің бар болуы;

Ішкі жүйелерді қамтамасыз етуді ерекшелеуші - АҚЖ құрлымын қарастыру кезінде дәстүрлі әрекет жасау мүмкін.

Ақпараттық қорғаныс жүйесінде кез-келген ақпараттық жүйе сияқты, өзінің мақсатты функциясын орындай алатын, өзіндік бағдарламалық қамтамасыз етудің анықталған түрі болуы керек.

1. *Құқықтық қамтамасыз ету* – құқықтық актілер, нормативті-құқықтық құжаттар, ауыр жағдайлар, басшылықтар ақпараттық қорғаныс жүйесіндегі әрекеттер жиынтығы.
2. *Ұйымдастыруды қамтамасыз ету.* Ақпараттық қорғанысты іске асыру анықталған құрлымдық бірліктер арқылы іске асады, мысалға, фирманың қауіпсіздік қызметі және оның құрлымы: ереже, күзетші және т.б.
3. *АҚЖ функциялдануын қамтамасыз ететін* тапсырманы шешу негізіндегі параметрлер, көрсетікштер, деректер және сипаттамаларды қоса алғандағы ақпараттық қамтамасыз ету.

Бөгет – қаскүнемнің қорғалатын ақпаратқа енуіне физикалық тәсілмен кедергі келтіруі (аппаратқа, ақпаратты жинақтаушыларға және т.б).

Енуге рұқсат алуды басқару – ақпараттық жүйе және ақпараттық технологияның барлық ресурстарын үнемі қолданудың ақпараттық қорғаныс тәсілдері. Бұл тәсілдер ақпаратқа енудің барлық мүмкін болатын жолдарына қарсы тұруы қажет. Енуге рұқсат алуды басқару келесі қорғаныс функцияларынан тұрады:

Шифрлеу механизмі – ақпаратты криптографиялық жабу. Бұл тәсілдер өңдеу тәсілінде сонымен қатар ақпаратты магниттік жинақтаушыда сақтау кезінде барынша кең көлемде қолданылады. Ақпаратты үлкен байланыс каналы арқылы жіберген кезде бұл тәсіл жалғыз сенімді тәсіл болып табылады.

4.2. Қорғау амалдарының мақсаты

Қорғау амалдарының мақсаты – бұл ақпараттық жүйе администраторын (АИС) тексеру ықтималдылығын ойластыру, залалданған жүйенің фактілерін анықтау; ақпараттық инфекцияның нәтижесінің әсерін азайту, вирустардың жайылып кетпеуін қадағалау немесе жою; Ақпараттық жүйенің ақпараттарын қалпына келтіру.

Тәртіп белгілеу – қорғалатын ақпаратты сақтау және жіберу кезінде қорғау стандарттары мен нормаларын үлкен дәрежеде орындауды автоматтандыру.

Еріксіз көндіру – ақпараттық жүйе қызметкерін немесе қолданушысын қорғалатын ақпаратты сақтау немесе жіберу кезінде еріксіз өңдеу ережелерін сақтауға көндіру арқылы орындалатын қорғаныс тәсілі;

Барлық техникалық амалдар жиынтығы аппараттық және физикалық болып бөлінеді.

Аппараттық амалдар – есептеуіш техникаға қондырылатын құрылғы немесе онымен стандартты интерфейс арқылы байланысатын құрылғы.

Физикалық амалдар – қаскүнемнің физикалық енуіне қарсы тұратын әр түрлі инженерлік құралдар және құрлығылар, ол персоналға материалдық, қаржылық және ақпараттық құралдарын заңға қарсы әрекеттен сақтайды. Физикалық амалдардың

мысалдары: есіктегі кілттер, терезелердегі тор, электронды қорғаныс сигналдар қою амалдары және т.б.

Бақылау сұрақтары:

1. Ақпаратты қорғаудың амалдары мен тәсілдерін атаңыз?
2. Шифрлеу механизмі дегеніміз не?
3. Қорғау амалдарының мақсаты?
4. Бағдарламалық амалдар дегеніміз не?

Дәріс№5.

Тақырыбы:Қорғаныс саясаты және стандарттары.

Мақсаты: Ұйымға ақпаратты қорғауға қорғаныс саясатын құру негіздерін анықтау .

Жоспар:

5.1 Қорғаныс саясаты

5.2 Қорғаныс стандарттары

Кілттік сөздер: қорғаныс саясаты, қорғаныс стандарттары, жүйелік протоколдар.

5.1. Қорғаныс саясаты

Ұйымның қорғаныс саясаты-ұйым өз жұмысында пайдаланатын қорғаныс аймағындағы басқару принциптерінің, ережелерді, процедура мен практикалық амалдардың жиынтығы.

Қорғаныс саясатының негізгі бағыттары:

Анықталуы қажет:

-қандай мәліметтерді және қаншалықты маңыздысы қорғалуы қажет

- фирмаға анықтамалық аспектіде кім және қандай шығын келтіруі мүмкін

-қауіпті анықтау және оны мүмкін болатын деңгейге дейін азайту мүмкіндігі

Ұйымның ақпараттық қорғанысы аймағында болып жатқан жағдайды бағалаудың екі жүйесі бар. Олар: «төменнен жоғарыға зерттеу», «жоғарыдан төменге қарай зерттеу»

Бірінші әдіс қарапайым болып табылады, аз қаржылық салымды қажет етеді, алайда сонымен қатар аз мүмкіншілікке ие. Ол белгілі схемаға негізделген:<Сіз-қарақшысыз, Сіздің әрекетіңіз?>. Яғни, ақпараттық қорғаныс қызметі барлық белгілі қауіптерге негізделіп, оларды тәжірибеде тексеру үшін істеп қарапшын мәніндегі қарақшыдан мұндай қауіптің болуы мүмкін бе соны тексереді.

Жоғарыдан төмен қарай әдісі ақпаратты қорғау мен өңдеудің бар схемаларына егжей-тегжейлі анализ жасауды білдіреді. Бұл әдістің бірінші этапы: қандай ақпараттық объектімен оның ағымын қорғау керек. Содан соң ақпаратты қорғаудың классикалық әдістерінің қайсысы және қай деңгейде орындататынын анықтау үшін ақпараттық қорғау

жүйесінің ағымдық жағдайын зерттеу. Үшінші этапта, барлық ақпараттық объектілірдің классификациясы кластарға оның конфиденциалдығына, бүтіндігінің талаптарына қарай бөлінеді. Ары қарай әр нақты ақпараттық объектіге келетін қауіп немесе қауіптің ашылуы фирмаға қаншалықты қатты шығын келтіретінін анықтау. Бұл этаптың аты қауіп-қатерді анықтау. Қауіп-қатерді анықтаудың көптеген схемалары бар, ең қарапайымына тоқталайық:

Қауіптің шығыны теріс емес санмен берілуі мүмкін. Оны келесі кестемен теңестіріп қарайық:

Шығын деңгейі	Сипаттама
0	Ақпараттың ашылуы фирмаға ең аз моральды және қаржылық шығын әкеледі.
1	Қауіптен шығын бар, бірақ ол көп емес, нарықтағы фирманың жағдайы мен қаржылық операциясына кедергісі жоқ
2	Біраз уақыт бойы қаржылық операциялар жүргізілмейді, осы уақытта фирма шығынғы ұшырайды, бірақ оның нарықтағы жағдайы және клиенттердің саны аз өзгереді
3	Нарықтық және қаржылық жағдайда да комақты шығын бар. Фирмадан біраз клиенттер кетеді.
4	Шығын өте көлемді, бір жыл ішінде фирма нарықтағы жағдайынан айырылады, жағдайды қайтару үшін үлкен қаржылық несие қажет.
5	Фирма толықтай өз жұмысын тоқтатады.

Қауіптің мүмкін болу жағдайы теріс емес санмен келесі кестемен сәйкестендіріліп беріледі:

Қауіптің мүмкін болу жағдайы	Қауіптің болуының орташа жиілігі
0	Қауіптің бұл түрі жоқ
1	Жылына бір реттен аз
2	Жылына бір рет
3	Айына бір рет
4	Аптасына бір рет
5	күнде

Келесі этапта ұйымның қауіп-қатерінің кестесі жасалады. Оны түрі:

Қауіп-қатерді сипаттау	Шығын	мүмкіндік	қауіп
Спам(пошта жәшігінің толып кетуі)	1	4	4
Басты офистегі қатты дискіні көшіріп алу	3	1	3

Барлығы:9

Қауіп-қатер кестесін анализдеу этабында ең көп мүмкін болатын қауіптің мәні беріледі, мысалы 7. Алдымен, кестенің әрбір қатары берілген саннан аспайтындығына тексеріледі. Егер мұндай жағдай байқалса, онда бұл қатар-қорғаныс саясатын құрудың басты мақсаты. Содан соң екі еселенген мәнді интегралды қауіппен салыстыру жүргізіледі(біздің жағдайымызда ол 7*2=14)

Егер интегралды қауіпмүмкін болатын мәннен асса, онда қорғаныс жүйесінде көптеген ұсақ қателіктер жіберілген, олар ұйымға тиімді жұмыс жасауға кедергі келтіреді. Мұндай жағдайда интегралды қауіптің мәніне үлкен әсер беретін қатар алынып, оны азайтуға немесе толығымен жоюға жағдай жасалады.

Ең маңызды этапта ұйымның қорғаныс саясаты жасалады, ол жеке және интегралды кауіпке қажетті деңгейді қамтамасыз етеді. Оны жасау кезінде қорғаныс саясатын жүргізуге кедергі келтіретін объективті проблемаларды ескеру қажет. Мұндай проблемаларға мыналар жатады: ел және халықаралық ұйым заңдары,корпарацияның ішкі талаптары, қоғамның этикалық нормалары.

Орындалуға қажетті барлық техникалық және әкімшілік әрекеттер сипатталған соң берілген бағдарламаның экономикалық бағасы есептеледі. Егер бағдарлама қауіптен қорғануды ақтамайтын болса, яғни қаржылық жағдайынан фирманы шығынға ұшыратын болса, онда бұрынғы деңгейге қайтадан оралып оны бір немесе екі пунктке еселейді.

Қорғаныс саясаты фирманың басқрушыларының бекітуімен және құжаттардың дайындалуымен аяқталады.

5.2. Қорғаныс стандарттары

Ақпараттың қорғаныс стандарттары екі топқа бөлінеді: нормативті және қызметтік.

Қорғаудың нормативтік стандарты қорғалған ақпараттық жүйелерге берілетін талаптардың жиынтығымен сипатталады. Олар қорғалған жүйелермен қорғаныс әдістерінің сипаттамасының формализациясына мүмкіндік береді. Оған «Ақпараттық технология қорғанысын бағалаудың критерийі» стандарты жатады. Нормативтік стандарттар бұрын құрылған жүйенің талаптарының жиынтығы болғандықтан, тәжірибеде олар қызметтік стандарттармен толықтырылады.

Қызметтік стандарттар ақпараттық қорғаныс режимінің орындалуын қамтамасыз ететін қорғалған ақпараттық жүйедегі шаралар жиынтығын сипаттайды. Бұл стандарттарға халықаралық стандарттар BSI, BS7799 немесе қорғалған жүйе процессін сипаттайтын отандық нормативтер.

Бақылау сұрақтары:

1. Қорғаныс саясаты не үшін қажет?
2. Қорғаныс саясатын құрудың этаптарын атаңыз?
3. Қауіп-қатерді анықтаудың схемасын түсіндіріңіз?
4. Қорғаныс стандарттары дегеніміз не?
5. Қандай қорғалған жүйелік протоколдарды білесіз?

Дәріс№6.

Тақырыбы:Қауіпсіздік жүйесін практикалық іске асыру.

Мақсаты: Ақпараттық қауіпсіздікті практикалық түрде жүзеге асырудың жолдарын, криптографияның негізгі тапсырмаларымен таныстыру.

Жоспар:

6.1 Криптографияның негізгі тапсырмалары. 6.2 Қорғаудың криптографиялық амалдары

6.3. Криптожүйенің жұмыс жасау принципі 6.4. Криптографиялық кілттерді басқару.

Кілттік сөздер: криптография, криптожүйе,криптографиялық кілт.

6.1. Криптографияның негізгі тапсырмалары.

Криптографияның тапсырмасы т.б. жасырын түрде жіберілетін қорғанысқа мұқтаж ақпарат үшін ғана туындайды. Бұндай жағдайда ақпарат арнайы, құпия, жасырылған немесе қорғалған делінеді. Мұндай көп кездесетін жағдайлар үшін арнайы түсініктер енгізілген:

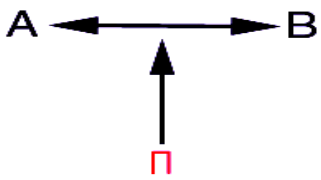
- мемлекеттік құпия;
- әскери құпия;
- коммерциялық құпия;
- заңгерлер құпиясы;
- дәрігерлер құпиясы және т. б.

6.2. Қорғаудың криптографиялық амалдары.

Қорғаудың криптографиялық амалдары - деп қорытындысында оның мазмұны жаттығатындай арнайы тәсілдерді және ақпаратты қайта өндеу тәсілдерін айтады. Криптографиялық жабудың негізгі түрлері сақталатын мәліметтерді шифрлау және кодтау болып табылады. Сонымен қатар бұл жағдайда шифрлеу жүйесінің әр түрі: ауыстыру, орналастыру, гаммирлеу, аналитикалық түрмен мәліметті алмастыру қолданылады.

Жалпы кең таралғандардың ішіне аралас шифрлеулер жатады, яғни әуелгі текст тізбектеле келіп, екі немесе үш түрлі шифрді пайдалана отырып ауысады.

6.3. Криптожүйенің жұмыс жасау принципі.



1-сурет

1-суретте криптография тәсілі пайда болатын жағдайдың негізгі мысалы көрсетілген. Мұндағы А және В – сақталған ақпараттың заңды пайдаланушылары, олар ақпаратты орта берілетін байланыс каналдарынан алмастырғысы келеді. Ал П–заңсыз пайдаланушылар (қарсылаушы, хакер), олар байланыс каналдарынан берілетін хаттамаларды ұстап алғысы келетіндер және олар солардың ішінен өзіне қажетті ақпаратты пайдаланады. Бұл қарапайым схеманы *жалпы жағдайдың моделі* деп санауға болады, яғни ақпаратты қорғаудың криптографиялық тәсілдері немес тек шифрлеу.

Шифрді ашу (бұзу) – бұл шифрді қолдану білімі болмаса да шифрленген хаттамадан қорғалған ақпаратты алу процессі. Қарсылас сақталған ақпаратты жіберген кездегі процесте алу үшін емес, оны жойып немесе түрлендіру үшін жасайды. Бұл ақпарат үшін тіпті басқа қорқыту түрі болып табылады, яғни шифрді ұстап алу мен жасырудан айырмашылығы бар. Мұндай қорқытуларды қорғау үшін өзінің арнайы тәсілдері өндіріледі. Тізбектеле, бір заңды пайдаланушыдан екінші пайдаланушыға ақпарат әр түрлі күдіктерге қарсы тұратындай, әр түрлі тәсілдермен қорғалу керек. Көп түрлі байланыстырудан ақпаратты қорғайтын әрекеттер тізбегі пайда болады. Егерде шифрде ауыспалы кілт болса, онда қарсыластың жасаған қиянаттардың барлығы қорғалған ақпаратқа әсер етпейді.

6.4. Криптографиялық кілттерді басқару.

Криптографияның кілтінен шифрдің жүйелік элементі түсіндіріледі, яғни дәл хаттаманы шифрлеу үшін пайдаланылады. Енді хабарламаны заңды пайдаланушылар бір-бірінен шифрленген хаттамаларды алмастырмас бұрын, қарсыластан жасырын түрде кілттерін алмастырып алулары керек немесе байланыс каналдарының екі жағына да бірдей кілтті қою керек. Ал қарсыласқа жаңа тапсырма пайда болады, яғни бірінші кілтті анықтап содан соң осы кілттегі шифрленген хаттаманы оқу оңай болады.

Криптографияның негізгі объектісінің формальді жазбасына келейік (№1 сурет). Енді оған жаңадан пайда болған өзгерістерді енгізейік –кілттерді алмастыру үшін қарсыласқа белгісіз жасырын байланыс каналын қосу керек (№2 сурет).

2-сурет

Қазіргі кездегі криптографиялық жүйе криптографиялық кілт негізінде құрылған. Ол анықталған амалдар шифрлеудің бір немесе бірнеше алгоритмінен (математикалық формулалардан), осы шифрлеу алгоритмдерінде қолданылатын кілттерден, кілттерді басқару жүйесінен, шифрленбеген мәтін және шифрленген мәтін (шифрмәтін) бойынша жұмыс жасайды.

Ақпаратты қайта өңдеу және қорғау жолдарымен жұмыс жасайтын тәсіл *криптоло-гия* (*kryp*tos-құпия, lo*gos*-ғылым) деп аталады. Криптоло-гияның өзі екі бағытқа бөлінеді – *криптография* және *криптоанализ*. Осы екі бағыттың мақсаттары бір-біріне қарама-қарсы болған.

Криптография ақпараттың қайта өнделуін іздеумен және математикалық әдістерді зерттеумен жұмыс жасайды.

Ал *криптоанализ* болса - жалпы кілтті ашу білімінсіз ақпаратты ашу мүмкіндіктері бар.

Қазіргі криптография өзіне төрт үлкен бөлімдерді қамтиды.

1. Симметриялық криптожүйелер.
2. Ашық кілтті криптожүйелер.
3. Электронды қол қою жүйелері.
4. Кілттермен басқару.

Алфавит – ақпараттың белгішелерін кодтау үшін пайдаланылатын жиын болып табылады.

Мәтін – алфавит элементтерінен реттелген жиын.

Қазіргі ақпараттық жүйелерде қолданатын алфавит ретінде келесіні мысал ете аламыз:

* алфавит Z_{33} - 32 орыс әріптері және бос орын;
* алфавит Z_{256} - ASCII және КОИ-8 стандартты кодтарына кіретін символдар;
* бинарлы алфавит - $Z_2 = \{0,1\}$;
* сегіздік немесе оналтылық алфавит;

Шифрлеу – алмастыру процесі: ашық мәтіннің атынан тұратын *негізгі мәтін*, ол шифрленген мәтінмен алмасады.

Шифрлеуді қалпына келтіру - шифрлеуге кері процесс болып табылады. Кілттің негізінде шифрленген мәтін негізгі мәтінге ауысады.

Кілт - мәтіндерді кедергісіз шифрлеу мен шифрлеуді қалпына келтіруге арналған ақпарат.

Криптографиялық жүйе - ашық мәтіннің T бөлімін көрсетеді. Осы бөлімше-нің әрбіреуі индекстеледі немесе *k* белгісімен белгіленеді; *k* параметрі кілт болып табылады. K кілттердің кеңістігі – бұл кілттің мүмкін мәндерінің жинағы. Негізінен кілт алфавит әріптерінің тізбегінен тұрады.

Криптожүйелер симметриялық және ашық кілттерге бөлінеді.

Симметриялық криптожүйелерде шифрлеу үшін де, қалпына келтіру үшін де бір код қолданылады. Ал ашық кілтті жүйелерде екі, ашық және жабық кілттер қолданылады, яғни олар бір-бірімен математикалық түрде байланысады. Ақпарат ашық кілттің көмегімен шифрленеді, ол барлық пайдаланушыларға шексіз ашық болады, ал шифрін жабу үшін жабық кілт пайдаланылады, ол тек хаттаманы алушыға ғана белгілі болады.

Кілттерді бөлу және кілттерді басқару термині ақпаратты өндеу жүйелерінің процесіне жатады. Мазмұны пайдаланушылар арасында кілттерді құру және анықтап бөлу болып табылады.

Электронды (цифрлік) қол қою – хаттаманы және оның түп нұсқасы мен авторлығын басқа пайдаланушы алған кезде оны криптографиялық алмастыру үшін кілтке қосылуын айтамыз.

Криптотұрақтылық деп шифрдің тұрақтылығын кілттің құпиясын білмей қайта қалпына келтіруді анықтайтын сипаттамасын айтамыз.

Криптотұрақтылықтың бірнеше көрсеткіштері бар, олар:

- Барлық мүмкін кілттердің саны;
- Криптоанализ үшін маңызды ортақ уақыт.

T_k –ның ауысуы сәйкесінше алгоритммен және *k* параметрінің мәнімен анықталады.

Бақылау сұрақтары:

1. Криптография дегеніміз не?
2. Криптоанализ дегеніміз не?
3. Криптография қандай бөлімдерден тұрады?
4. Электрондық қол қою дегеніміз не?
5. Кілт дегеніміз не?

Дәріс№7.

Тақырыбы:Симметриялық криптожүйелер.

Мақсаты: Криптографиялық әдістердің классификациясымен таныстыру.

Жоспар:

7.1 Криптографиялық әдістердің классификациясы

7.2 Ауыстыруларды тексеру жүйесі.

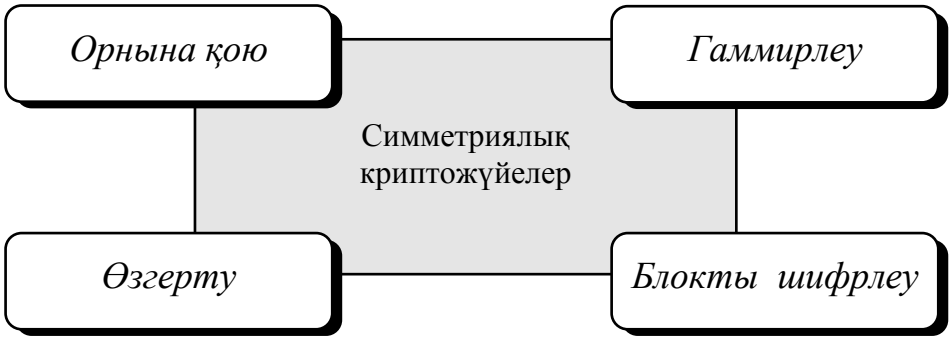
7.3. Цезардің өзгертулерін тексеру.

7.4. Көпалфавитті жүйелер. Бір рет пайдаланудың жүйесі.

Кілттік сөздер: көпалфавитті қою, орын ауыстырулар, гаммирлеу, Цезарь жүйесі.

7.1. Криптографиялық әдістердің классификациясы.

Барлық көптүрлі криптографиялық әдістерді келесі түрлендіру класстарына бөлуге болады:



1 сурет .Симметриялық криптожүйелердің алмасу класстары

Көпалфовитті қою - түрлендірудің өте қарапайым түрі болып табылады. Алдыңғы мәтіннің күрделі немесе қарапайым (сол алфавит бойынша) ережелері бойынша символдарды ауыстырумен қорытынды-лайды. Жоғарғы криптотұрақтылықты жабдықтау үшін үлкен кілттерді қолдану қажет болады.

Орын ауыстырулар (перестановки) – криптографиялық алмасудың қарапайым тәсілі болып табылады. Оны басқа да әдістермен сәйкестігі үшін қолданады.

Гаммирлеу (гаммирование) – бұл тәсіл кілт негізінде басқарылатын кейбір кездейсоқ, бірізділікпен жіберілетін мәтінге енгізуде қорытындыланады.

Блокты шифрлер – түрлендірудің негізгі тәсілдерінің тізбектелуін (қайталау және кезекпен келу мүмкіндіктерін) көрсетеді, яғни шифрленетін мәтіннің бөлікке қолданылуын айтамыз.

Бүтін сандар жинағының *орын ауыстыруын* σ (0,1,...,N-1) оны қайта ретке келтіру деп атайды. Бүтін i, осы позициядан σ(i), мұндағы $0 \le (i) < n$, позициясына өткізілуін көрсету үшін келесі жазбаны қолданамыз:

σ=(σ(0), σ(1),..., σ(N-1)).

(0,1,...,N-1) осылардан шыққан ауыстыру сандары *n*!=1*2*...*(N-1)*N – ге тең болады. Бір мағыналық өзара сәйкестік жинағын $S=\{s_0, s_1, ..., s_{N-1}\}$ көрсету үшін σ мәнін еңгіземіз (гомоморфизм), яғни *n* элементтерінен тұратындар.

$\sigma: S \to S$

$\sigma: s_i \to s_{\sigma(i)}, 0 \le i < n$

Бұл жағдайда σ-ның негізгі ролі S элементін ауыстыру болып табылады және керісінше S автоморфизмі бүтін сандардың ауыстыруына сай келеді (0,1,2,.., *n*-1).

Криптографиялық ауыстырудағы T–ны Z_m алфавиті үшін автоморфизм-нің тізбектелуі деп аталады: $T=\{T^{(n)}: 1 \le n < \infty\}$

$T^{(n)}: Z_{m,n} \to Z_{m,n}, 1 \le n < \infty$

Әрбір $T^{(n)}$ бұл жағдайда *n*-граммның $Z_{m,n}$ –нен ауыстыруы болады.

Қаншалықты $T^{(i)}$ мен $T^{(j)}$ бір-бірінен $i \ne j$ жағдайда тәуелсіз бола алады, ал криптографиялық ауыстырудың саны негізгі мәтіннің *n* өлшемімен $(m^n)!$[1]- ға тең болады. Ол *m* және *n* өскен кезде пропорционалды емес болып өседі: сонымен, *m*=33 және *n*=2 әртүрлі криптографиялық аысулардың саны 1089!.

Кпирптографиялық жүйелерді іске асыруының тәжірибелік бөлімі $\{T_k: k \in K\}$ өзгертулер біркелкі аз көлемдегі параметрлерге (кілттерге) байланысты алгоритмдермен анықталуын талап етеді.

7.2. Ауыстыруларды тексеру жүйесі.

Анықтамасы: π ауыстыруларды тексеруде Z_m алфавитте автоморфизм деп аталады, яғни мұндағы негізгі мәтіннің әріптері t шифрленген мәтіннің әріптерімен орындарын ауыстарған π(t):

$Z_m \to Z_m; \pi: t \to \pi(t)$.

Барлық ауыстыруларды тексерудің жинағын Z_m -нің симметриялық тобы деп атаймыз және келешекте $SYM(Z_m)$ болып белгіленетін болады.

Дәлелдеу $SYM(Z_m)$ өзгерту операцияларымен топ болып табылады, яғни келесі қасиеттерімен белгілі операция:

Тұйықтық: $\pi_1\pi_2$ өзгертулерін туындау орынауыстыруды тексеру болып табылады:

$\pi: t \to \pi_1(\pi_2(t))$.

Біріктірушілігі: $\pi_1\pi_2\pi_3$ туындысының нәтижесі жақшалардың дұрыс қойылғанына қарамайды:

$(\pi_1\pi_2)\pi_3=\pi_1(\pi_2\pi_3)$

Анықтама. *k* ауысуын тексеру кілті Z_m үшін Z_m симметриялық топтың элементтерінің тізбегі деп аталады:

$k=(p_0,p_1,...,p_{n-1},...)$, $p_n \in SYM(Z_m)$, $0 \le n < \infty$

k кілтімен анықталатын ауысуды тексеру T_k криптографиялық өзгерту болып табылады, ол *n*-граммның негізгі мәтіннің көмегімен орындалатын $(x_0, x_1, .., x_{n-1})$, *n*-граммның шифрленген мәтіні $(y_0, y_1, ..., y_{n-1})$:

$y_i=p(x_i)$, $0 \le i < n$

мұндағы *n* – туындама (n=1,2,..). T_k көпалфавитті ауыстыруды тексеру деп аталады, егер *p* қандай да бір і-де өзгермесе, і=0,1,..., керісінше T_k көпалфавитті ауыстыруды тексеру деп аталады.

Ескерту. T_k ауыстыруларды тексерулерге келесілер жатады:

1.Негізгі мәтін символ бойынша шифрленеді. *n*-граммның шифрленуі $(x_0, x_1, .., x_{n-1})$ және префиксі $(x_0, x_1, .., x_{s-1})$ арақатынаспен байланысты

$T_k(x_0, x_1, .., x_{n-1})=(y_0, y_1, ..., y_{n-1})$

$T_k(x_0, x_1, .., x_{s-1})=(y_0, y_1, ..., y_{s-1})$

2. y_i шифрленген мәтіннің әріпі, тек і компоненттінің функциясы болып табылады және x_i негізгі мәтіннің і әрпінің p_i кілтімен анықталады.

7.3. Цезардің өзгертулерін тексеру.

Цезардің өзгертулерін тексеру өзгертуді тексерудің ең қарапайым нұсқасы болып табылады. Ол моноалфавитті өзгертулерді тексерулерге жатады.

Анықтама. Көбіне $C_m=\{C_k: 0 \le k < m\}$-де $SYM(Z_m)$ симметриялық тобының, *m* өзгертуді тексеруден тұратын

$C_k: j \to (j+k) \pmod m$, $0 \le k < m$,

Цезардің өзгертулерді тексеруі деп аталады.

Өзгерту орын басу таблицасы арқылы анықталады, яғни сай келетін қос әріптердің «негізгі мәтіні – шифрленген мәтін» болады. C_3 үшін ауыстыруды тексеру 1.1. кестеде берілген. (→) беғдарлау белгісі негізгі мәтіннің әріпі (солдан), шифрленген мәтіннің (оңнан) C_3 -тің көмегімен шифрленеді.

Анықтама. *Цезардің жүйесі деп* моноалфавитті ауыстыруды тексеру болып табылады, негізгі мәтіннің *n*-граммасын қайта келтіретін $(x_0, x_1, .., x_{n-1})$ шифрленген мәтіннің *n*-граммасы $(y_0, y_1, ..., y_{n-1})$ ережелеріне сәйкес

$y_i=C_k(x_i)$, $0 \le i < n$ болады.

Мысалы, ЖАҢА_НҰСҚАУДЫ_ЖІБЕРІҢІЗ C_3 орын ауыстыруды тексерумен пайдаланатын болсақ, онда бұл мәтін йгюгврвфюгцзювйюдиуюююк түріне түрленетін болады.

А→г	Й→м	Т→х	Ы→ю
Б→д	К→н	У→ц	Ь→я
В→е	Л→о	Ф→ч	Э→_
Г→ж	М→п	Х→ш	Ю→а
Д→з	Н→р	Ц→щ	Я→б
Е→и	О→с	Ч→ъ	_→в
Ж→й	П→т	Ш→ы	
З→к	Р→у	Щ→ь	
И→л	С→ф	Ъ→э	

1 кесте: Цезардің ауыстыруды тексерулерін қолдану.

Цезардің орын ауыстыруларды тексерулерінде бәрінен де тиімді болып – *Хилла шифрі мен Плэйфер шифрі саналады*. Олар ауыстыруларды тексеруде бөлек белгі болып негізделмеген, 2-грамм (Плэйфер шифрі) немесе *n*-грамм[2] (Хилл шифрі) болады. Бұдан да жоғары криптотұрақтылықта олар іске асу үшін анағұрлым қиынырақ және үлкен көлемдегі кілттік ақпаратты талап етеді.

7.4. Көпалфавитті жүйелер. Бір рет пайдаланудың жүйесі.

Моноалфавитті ауыстыруларды тексеру шамалы криптотұрақтылығы көпалфавитті ауыстыруларды тексерумен жеңеді.

Көпалфавитті ауыстыруларды тексеру $\pi = (\pi_1, \pi_2,)$ кілтімен анықталады, яғни олар кем дегенде екі түрлі ауыстыруды тексеруден тұрады. Басынды көпалфавитті жүйелердің нолден бастап солға жалжыту тексерулерін қарастырайық. $\{K_i: 0 \le i < n\}$ – тәуелсіз кездейсоқ айнымалылар шындықты бірдей таратын болсын, олар Z_m көптігінде мәндерін қабылдайды

$P\text{кл}\{(K_0, K_1, ..., K_{n-1})=(k_0, k_1, ..., k_{n-1})\}=(1/m)^n$

Бір рет пайдалану жүйесі негізгі мәтінді

$X=(X_0, x_1, ..., x_{n-1})$

Цезардің ауыстыруларды тексеруі көмегімен

$Y_i=C_{Ki}(x_i)=(K_i+X_i) \pmod m$ i=0...n-1 (1)

шифрленген мәтінге $Y=(Y_0, y_1, ..., y_{n-1})$ өзгертеді.

Шексіз кілтті шифрлеудің мысалын қарастырайық және кілт түрінде мәтінді мысал етіп алайық “ШЕКСІЗ КІЛТ ....”.

“ШИФРДІ_АШПАЙМЫЗ” мәтіні көмегімен шифрлейік. Шифрлеуді кестеге енгізейік:

ШИФРЛЕНЕТІН_МӘТІН	24	8	20	16	19	5	12	27	9	32	18	5	10	17	18
ШЕКСІЗ_КІЛТ	1	5	17	10	14	13	5	23	13	27	9	32	10	11	30
ЩРДЪАТТССЦЪЫДФЫП	25	13	4	26	0	18	17	7	22	26	27	4	20	28	15

Бақылау сұрақтары:

1. Криптографиялық әдістерді қандай кластарға бөледі?
2. Блокты шифрлеу дегеніміз не?
3. Шексіз кілтті шифрлеу дегеніміз не?
4. Цезарь жүйесі дегеніміз не?

Дәріс№8.

Тақырыбы:Симметриялық және симметриялық емес әдістеме.

Мақсаты: Симметриялық және симметриялық емес әдістемені пайдалану негіздерін үйрену.

Жоспар:

8.1 Симметриялық (құпиялы) әдістеме.

8.2 Симметриялы емес (ашық) әдістеме.

Кілттік сөздер: Симметриялық және симметриялы емес әдістеме, симметриялы кілтті жүйелер.

8.1. Симметриялық (құпиялы) әдістеме.

Осы әдістемеде жіберуші және қабылдап алушының арасында шифрлеу және шифрді ашу үшін, байланысудан бұрын олар алдын-ала келісілген сол бір кілтті қолданады. Егер кілт ашылмаса, онда шифрді ашу кезінде автоматты түрде жіберушінің аутентификациясы болады, жіберушіде ақпаратты ашуға болатын кілт бар болғаннан кейін ғана, яғни ақпаратты шифрлеуге болатын кезде, қабылдап алушыда ақпаратты ашуға болатын кілт болады. Жіберуші мен қабылдап алушылар ғана бір симметриялық

кілтті береді, сондықтан кілттің беделі түскен жағдайда тек қана осы екі пайдаланушылар жауап береді. Басқа да криптожүйелерге актуалды болатын проблемалар симметриялық кілттердің қауіпсіз таралуындағы сұрақтар болады.

Симметриялық шифрлеудің алгоритмдері қатты үлкен емес ұзындықтағы кілттерді пайдаланады және үлкен көлемдегі мәліметтерді тез шифрлейді.

Симметриялық кілтті жүйелерді пайдалану ережесі:

1. Симметриялық құпия кілт қауіпсіз құрылады, таралады және сақталады.
2. Жіберуші мәтін үшін хэш-функция есебінің көмегімен және мәтінге қосылған жаңа жолдарға электронды қол қоюды шығарады.
3. Жіберуші шифрленген мәтінді алу үшін шифрлеу-шифрді ашу тез симметриялық алгоритмін алынған пакетке (мәтінге электронды қолымен бірге) құпиялы симметриялық кілтпен пайдаланады. Тек қана жіберуші симметриялық құпия кілтін білгендіктен осы пакетті шифрлей алады, осындай ашық емес түрде аудентификация болады. Ал бұл симметриялық құпия кілтін тек қабылдап алушы ғана біледі және оның шифрін ашады.
4. Жіберуші шифрленген мәтінді беріп жібереді. Симметриялық құпия кілт ешқашанда қорғалмаған байланыс каналдарынан берілмейді.
5. Қабылдап алушы сол шифрлеу-шифрді ашу симметриялық алгоритмді шифрленген мәтінге негізгі мәтінді қалпына келтіру және электронды қол қою үшін сол симметриялық кілтпен бірге пайдаланады. Оның сәтті қалпына келтіруі біреуді аутентифицирлейді, яғни құпия кілтін білетінге.
6. Қабылдап алушы мәтіннен электронды қол қоюды бөліп тастайды.
7. Қабылдап алушы хаттаманың бүтіндігі үшін осы екі электронды қол қоюды салыстырады.

Бұл әдістемеде шифрлейтін және шифрді ашатын кілттер бірге шығарылғанмен екі түрлі болады. Бір кілт барлығына белгілі етіп жасалады, ал екіншісі құпияда болады. Мәліметтер, бір кілтпен шифрленсе тек қана екінші кілтпен ашылады.

Барлық симметриялық емес криптожүйелер кілттің тікелей шегіну жолының шабуыл объектісі болып табылады, сондықтан оларда қорғаудың эквивалентті көрсеткішін қамтамасыз ету үшін симметриялық крипто жүйелерде пайдаланатындарға қарағанда ұзын кілт қолдану қажет. Брюс Шнейер "Прикладная криптография: протоколы, алгоритмы и исходный текст на С" атты кітабында № 1-ші кестедегідей келесі кілттің эквивалентті ұзындығы жайында мәліметтерді көрсеткен.

№ 1 кесте.

Симметриялық кілттің ұзындығы	Симетриялық емес кілттің ұзындығы
56 бит	384 бит
64 бит	512 бит
80 бит	768 бит
112 бит	1792 бит
128 бит	2304 бит

Симметриялық емес шифрлеу алгоритмдерінің төменгі жылдамдығы-нан қашу үшін, уақытша симметриялық кілт әрбір хаттама үшін қуат береді және ол тек симметриялық емес алгоритммен шифрленеді. Хаттаманың өзі әуелде жазылған шифрлеу/шифрді ашу алгоритмдері және осы уақытша сеансты кілті пайдаланумен шифрленеді. Сосын осы қабылдап алушының сеансты кілт ашық симметриялық емес кілттің көмегімен шифрленеді. Осыдан соң мына шифрленген сеансты кілт шифрленген хаттамамен қабылдап алушыға беріледі. Қабылдап алушы сол симметриялы емес алгоритм шифрлеуін пайдаланады және өзінің құпия кілтін сеансты кілтті ашу үшін, ал қабылданған сеансты кілт хабарламаның шифрін ашу үшін қолданылады.

Симетриялы емес криптожүйелерде өздері жабдықтайтын сеансты және симметриялық емес кілттер қауіпсіз көрсеткіштер қатынасына сәйкес келеді. Симметриялы емес ашық кілттер оларды ауыстыру қиын болғандықтан тікелей шабуылға осал болады. Егер шабуыл жасаушы құпия симметриялық емес кілтті біліп қалса, онда тек қана кезектегі емес сонымен қатар жіберуші мен қабылдап алушының арасындағы байланыстарының беделі түседі.

Симметриялы емес кілттерді пайдалану реті:

1. Симметриялы емес ашық және құпия кілттер қауіпсіз құрылып, таралады. Құпия симметриялы емес кілт оның иесіне беріледі. Ашық симметриялы емес кілт мәліметтер қорында сақталады және сертификат беретін орталықпен басқарылады. Пайдаланушылардың осындай жүйеде қауіпсіз құрылу жүретіндігінде сену қажет. Бұдан басқа, егер кілтті өндіруші және оларды басқаратын тұлға немесе жүйе ғана емес болса, онда соңғы пайдаланушы кілтті өндіруші шың мәнінде көшірмелерін жойып тастағанына сену қажет.
2. Мәтіннің электронды қол қоюы хэш-функцияның есептеу көмегімен жасалады. Алынған мәндер жіберушінің симметриялық емес құпия кілтінің пайдалануымен шифрленеді, ал содан соң алынған символдардан тұратын жол берілетін мәтінге қосылады (тек жіберуші ғана электронды қол қоюды шығара алады).

3. Симметриялық құпия кілті шығарылады, ол тек осы хаттама үшін шифрленуге пайдаланатын немесе өзара байланысу сеансында пайдаланады, сосын шифрлеу/шифрлемеу симметриялық алгоритмінің көмегімен және осы кілтті негізгі мәтін шифрленеді, осыған қосылып электронды қол қою қосылғанда шифрленген мәтін шығады.
4. Енді хаттаманы алатынға сеансты кілтті беру проблемасын шешу қажет.
5. Жіберуші симметриялы емес ашық кілтті сертификат беретін орталықтан алу қажет. Осы ашық кілтті алу үшін шифрленбеген сұраныстарды ұстап алу шабуылдың кең таралған формаларының бірі болады. Ашық кілттің нақты дәлелденген бүкіл сертификат жүйелері болуы мүмкін.

Бақылау сұрақтары:

1. Ақпараттық қорғаныстың құрылу жүйесінің мақсаттары?
2. Құқықтық қамсыздандыру дегеніміз не?
3. Симметриялы емес (ашық) әдістеменің жұмыс негізін түсіндіріңіз**?**
4. Симметриялы емес кілттерді пайдалану ретін атаңыз?.
5. Қорғау объектісінің анализінің этаптарын атаңыз

Дәріс№9.

Тақырыбы:Компьютерлік жүйені бұзу тәсілдері.

Мақсаты: Компьютерлік жүйені бұзу тәсілдерімен таныстыру.

Жоспар:

9.1 Компьютерлік жүйені бұзу тәсілдері.

9.2 Мәліметтер қорын басқару жүйесі дәрежесінде шабуыл жасау.

9.3. Операциялық жүйе дәрежесінде шабуыл жасау.

9.4. Желілік бағдарламалық қамтамасыз ету дәрежесінде

шабуыл жасау.

Кілттік сөздер: Мәліметтер қорын басқару жүйесі, операциялық жүйе дәрежесінде және желілік бағдарламалық қамтамасыз ету дәрежесінде шабуыл жасау.

9.1. Компьютерлік жүйені бұзу тәсілдері.

Жалпы жағдайда әмбебап компьютерлік жүйені бағдарламалық қамтамасыз ету негізгі үш компоненттен тұрады: операциялық жүйе, желілік бағдарламалық қаматамасыз ету (ЖБҚ) және мәліметтер қорын басқару жүйесі (МҚБЖ). Сондықтанда компьютерлік жүйе қорғанысын бұзу әрекетін үш топқа бөлуге болады:

- Операциялық жүйе дәрежесінде шабуыл жасау;

- Желілік бағдарламалық қаматамасыз ету дәрежесінде шабуыл жасау;
- Мәліметтер қорын басқару жүйесі дәрежесінде шабуыл жасау;

9.2. Мәліметтер қорын басқару жүйесі дәрежесінде шабуыл жасау.

МҚБЖ-ны қорғау ең қарапайым тапсырмалардың бірі. Бұл МҚБЖ-де қатаң ішкі құрлымның болуы және МҚБЖ элементтерімен әрекеттер жеткілікті анық берілгендігімен байланысты. Төрт негізгі әрекеттер бар – элементті іздеу, қою, жою және алмастыру. Қалған әрекеттер қосымша болып табылады және өте сирек кездеседі. МҚБЖ-нің қатаң құрлымы мен нақты анықталған әрекеттердің бар болуы мәліметтер қорын басқару жүйесін қорғау тапсырмасын жеңілдетеді. Көптеген жағдайда хакерлер компьютер жүйесінің қорғанысын операциялық жүйе дәрежесінде бұзуды және операциялық жүйенің көмегімен мәліметтер қорын басқару жүйесінің файлдарына енуге рұқсат алуды таңдайды. Ондай жағдайда МҚБЖ жеткілікті сенімді қорғау механизмі жоқ болса, немесе МҚБЖ-нің жаман тестіленген түрі болса, немесе қатесі бар, немесе МҚБЖ қауіпсіздігі администраторынан қате кеткен болса хакерге мәліметтер қорын басқару жүйесін бұзуға көмектеседі.

Сонымен қатар қоғану үшін арнай тәсілдер қолдану керек. МҚБЖ-не шабуылдың арнайыланған екі сценариі бар. Бірінші жағдайда МҚБЖ-нің сандық алаңдарымен арифметикалық операциялардың нәтижесі аз жағына қарай дөңгеленіп, ал айырмашылық МҚБЖ-дегі басқа мәліметпен қосылып кетеді. Екінші жағдайда хакер МҚБЖ-нің алаңдарындағы мәліметке енуге рұқсат алады. Хакерлердің МҚБЖ-не шабуыл жасауының мақсаты – статистикада жиналатын көптеген жазбалардың тек қана бір жазбадан құралуы үшін сұраныс формуласын құрастыру.

9.3. Операциялық жүйе дәрежесінде шабуыл жасау.

Операциялық жүйені қорғау МҚБЖ-не қарағанда анағұрлым қиынырақ. Қазіргі кездегі операциялық жүйелердің ішкі құрлымдары қиын болағндықтан қорғанудың адекватты саясаты көрнекті түрде қиындау тапсырмасы болып табылады. Бұндайдан бейхабар адамдардың ойынша операциялық жүйеге ең тиімді шабуыл жасау бұл тек қиын амалдардың көмегімен жүзеге асады және хакер ең жоғарғы квалификациялы программист болуы керек. Осы немесе басқа хакерлердің шабуыл жасау алгоритмдері тәжірибе жүзінде, осы шабуылдың объектісі болып табылатын,операциялық жүйенің нақты конфигурациясына және архитектурасына байланысты. Сонымен қатар іс-тәжірибе жүзінде кез-келген операциялық жүйені азаптайтын шабуылдар бар:

- Құпия сөзді (парольді) ұрлау:

- Операциялық жүйе жұмысына рұқсат беретін құпия сөзді қолданушы енгізген кезде қарап отыру (тіпті құпия сөзді енгізу кезінде экран дисплейінде құпия сөз шықпасада, хакер қолданушы саусақтарының пернетақтадағы қозғалысына қарап оңай шеше алады);
- Құпия сөздер туралы ақпараттар бар сыртқы жинақтаушыны ұрлау (дискеттер немесе операциялық жүйеге кіруге арналған қолданушының құпия сөздері сақталған электронды кілттер);
- Құпия сөздің барлық нұсқауларын толық қарап шығу;

9.4.Желілік бағдарламалық қамтамасыз ету дәрежесінде шабуыл жасау.

Желілік бағдарламалық қамтамасыз ету әлсіз болса, хабарлама жіберген кезде осы каналға енуге рұқсаты бар барлық қолданушы оны жолдан ұстап алып өз нұсқасын жібере алады. Сондықтанда, желілік бағдарламалық қамтамасыз ету дәрежесінде шабуылға келесідей мінездеме беруге болады:

- Жергілікті желі сегментін тыңдау (бір жергілікті желінің сегменттері арасында құрылған компьютерлер сол жергілікті желідегі басқа компьютерден хабарлама ала алады немесе осы сегменттегі компьютерлер арасындағы барлық ақпараттарға өзгерту енгізуге не олардың ішіне енуге болады);
- Жалған маршрутизатор құру (хакер желіге өзінің арнайы хабарламасын қосып, өз компьютерін желінің маршрутизаторы ете алады, содан соң ол арқылы өтетін барлық хабарламаға енуге рұқсат алады);
- Хаттамамен мазалау (хаттама желісіне жалған желілік адреспен хаттама жіберіп, хакер өз компьютеріне желілік байланысты жүктейді, нәтижесінде қолданушы құқығын алады);

Бақылау сұрақтары:

1. Компьютерлік жүйе қорғанысын бұзу неше топқа бөлінеді?
2. Мәліметтер қорын басқару жүйесі дәрежесінде шабуылдың екі сценарийін атаңыз?
3. Операциялық жүйеге жасалатын шабуылдарды атаңыз?
4. Желілік бағдарламалық қамтамасыз ету дәрежесінде шабуылға мінездеме беріңіз?

Дәріс№10.

Тақырыбы:Ақпаратты қорғау дұрыстығының әдістемесі.

Мақсаты: Қорғау жүйелерінің дұрыстығын зерттеуді қарастыру.

Жоспар:

10.1 Қорғау жүйелерінің дұрыстығын зерттеу

10.2 Ақпараттық қауіпсіздіктің қамсыздандырулары

Кілттік сөздер: Ақпараттық қорғаныстың құрылу жүйесі, құқықтық қамтамасыздандыру, қорғау объектісінің анализі.

10.1 Қорғау жүйелерінің дұрыстығын зерттеу

Қорғаныс саясаты – бүкіл белгілер өз жұмысында пайдаланатын қорғаныс аймағындағы басқару ережелері мен практикалық амалдар жиыны.

Ақпараттық қорғаныстыңәдістері мен құрылу тәсілдері. Және оның құрылысы. Ақпараттық қорғаныстың құрылу жүйесі (АҚҚЖ) Аж және АТ келесідей мақсаттан тұрады;

1. Өзара байланысқан жүйелік құрылуға жақын келетін ұйымдық, бағдарламалық, ақпараттық, физикалық және басқа қасиеттерді білдіретінүйлесімді үйлестіруді және барлық технологиялық қолданылатындардың цикл кезеңі.
2. Жүйенің толассыз дамуының принципі. Бұл принцип компьютерлік ақпараттықжүйелермен негіз болатын, жәнеде АҚҚЖ үшін көбірек өзекті.
3. Үнделетін хабардың бүлінуі және минимализация жасауы рұқсатпен және өңдеу процедураларына, т.б. пайдаланушыларға ьеру сияқты және сол қызметкерлердің өздерімен АЖ-ң қатал өкілеттердің минимумы, олардың орындалуға арналған жеткіліктердің өз қызмет міндеттері.
4. Толықтық бақылаудың және бекітілмеген рұқсат әрекеттерінің тіркеулері, т.б. әрбір падаланушының құру қажеттілігі және протоколданатын оның әрекеттерін өткізуге арналған ИТ-та іске асыру мүмкіншілігінің кез келгені оның алдын ала тіркеусіз өңдеу операциясы.

10.2 Ақпараттық қауіпсіздіктің қамсыздандырулары

Құқықтық қамтамасыздандыру.

Заң шығарушылардың жиыны нормативті-заңды құжаттардың, міндетті ортасында жайлардың, нұсқаулардың, басшылықтың талаптары ақпарат жүйесінде қорғанысы.

Ұйымдық қамтамасыздандыру.

Бұл ақпараттың қауіпсіздік орындалуы айқын құрылысты бірліктер жүйесінде асады солармен, мысалы, қауіпсіз қызмет сияқты фирмалар және оның құрама құрылымының: тәртібі, күзет және т.б.

Ақпараттық қамтамасыздандыру.

Өзіне қосылғанмәліметтердің, көрсеткіштері, параметрлері, осы мақсаттар шешімі негізіне жататын, СИБ жұмысын қамтамасыздандыру.

Техникалық (аппараттық) қамтамасыздандыру.

Техникалық құралдардың кең қолдануы ақпаратты қорғауға арналған, сол сияқты СИБ да қорғауға арналған.

Бағдарламалық қамтамасыздандыру.

Әр түрлі ақпараттық, еспетік, статистикалық және есеп айыратын бағдарлама торында болуға бағалауды қамтамасыздандыру және әртүрлі каналдардың қауіп қатерлері және ақпараттың бекітілген рұқсат тәсілдері.

Математикалық қамтамасыздандыру.

Бұл – математикалық әдіс, әртүрлі есеп-қисаптармен жұмыс жасайтын, техникалық құралдар қауіп-қатерімен баланысқан, қасконемедерді жалғастырады, аймақ және қажетті қорғаныш нормалары.

Лингвистикалық қамтамасыздандыру.

Мамандардың арнайы тілдік қатынасы және пайдалунышылардың ақпараттық қауіпсіздік ортасынад қамтамасыз ету.

Нормативті-әдістемелік қамтамасыздандыру.

Мұнда нормалар және органдардың қызмет тәртіптері, қызметтердің, құралдардың, іске асушы функцияның ақпарат қорғаныштары, әртүрлі әдістемелер түрлері, пайдаланушыларды қамтамасыз етуші өз жұмысын орындауы жөнінде жасырын талаптарды сақтаулар.

Қорғау объектісінің анализі бірнеше этаптардан тұрады:

Бірінші кезең

Анықтамадан тұратын, не керек қорғау:

- ақпарат анықтамалары, қорғанышқа мұқтаж;
- ең маңызда элементтер /сындар/ ақпаратпен қорғалған;
- сын ақпарат мерзімі анықталады /уақыт, кажетті табылған ақпарат орындауына арналған бәсекеліге/;
- ақпарат маңызды элементтермен анықталады /индикаторлар/ мәлімдеулердің қайтарушы мінез-құлқымен қорғалады;

Екінші кезең.

Қорқытулардың алдын ала ескерту табуы:

- кімді қорғайтын анықтаманы қызықтыратының анықтайды;

- әдістерді бағалайды, бәсекешілермен қолданылатындар мына анықтаманы алуына арналған;
- хабар келулері болуы мүмкін каналдарды бағаланады;
- бәсекеші әрекеттерінің қиылысымен шаралардың жүйесі өңделеді.

Үшінші кезең.

Өткізілудің қауіпсіздік қамтамасыз етуі қабылданған және тұрақты жұмыс істейтін ішкі жүйелерінің нәтіжелік талдауы /физикалық қауіпсіздік, құжатнамалар, қызметші сенімділік, қауіпсіздік қолданылатындарының байланыс ақпарат тапсыруына арналған/.

Төртінші кезең.

Қорғаныш қажетті өлшемді табады. Негізінде өткізілгендердің аналитикалық зерттеулердің бірінші үш кезеңі кіріскен іс қауіпсіздігі қамтамасыз етуімен қажетті қосымша өлшемдер және құралдарды дағдылайды.

Бақылау сұрақтары:

1. Ақпараттық қорғаныстың құрылу жүйесінің мақсаттары?
2. Құқықтық қамсыздандыру дегеніміз не?
3. Техникалық қамсыздандыру дегеніміз не?
4. Нормативті-әдістемелік қамтамасыздандыру.
5. Қорғау объектісінің анализінің этаптарын атаңыз

Дәріс№11.

Тақырыбы:Ақпаратты қорғау жүйесіне баға беру.

Мақсаты: Желідегі ақпаратқа қауіп жергілікті желідегі ақпаратты қорғау негіздерімен таныстыру.

Жоспар:

11.1 Жүйелілік ұғымы

11.2 Жүйелендіру әдістемесі және комплексті ақпаратты қорғау жүйесіндегі АҚКЖ

Кілттік сөздер: ақпаратты қорғауды бағалау деңгейі, ақпаратты қорғауды компьютерлік жүйесі(АҚКЖ).

11.1 Жүйелілік ұғымы.

Жүйелілік ұғымы қорғаныс механизмдері сияқтыларда ғана емес , сонымен қатар ол АЖ барлық өмірлік кезеңдеріндегі этаптарын жүзеге астатын жүйелі процес ұсынады. Сонымен қатар барлық ақпаратты қорғау құралдары, әдістер мен шаралар бір тұтас қорғау

механизмі – қорғау жүйесіне бірігеді. Өкінішке орай ақпараттық технологияның қауіпсіздігін комплексті қамтамасыз ету қажеттілігі қазіргі АЖ пайдаланушыларынан тиісті түрде түсінік ала алмай жатыр. Сонымен қатар ақпаратты қорғау жүйесінің құрылысы жәй қорғаныс құралдарын таңдаумен шектелмейді. Мұндай жүйелерді құруда айқын арналған теориялық білімдер қажет болады, атап айтқанда:

- Қорғалған ақпараттық жүйе өзімен не ұсынада;
- Ақпаратты қорғау жүйесі дегеніміз не және оған қандай талаптар қойылады;
- Ақпараттық технологияның қауіпсіздігін бұзатын қандай себептер түрлері бар;
- Қандай қорғаныс функциялары бар және олар қандай түрде болуы керек, олар қалай қауіпсіздікті бұзу себептерін жояды;
- Комплексті ақпаратты қорғау жүйесін қалай құрады;

11.2. Жүйелендіру әдістемесі және комплексті ақпаратты қорғау жүйесінде (АҚКЖ) қаралатын экспертті білім талаптарының ұсынулары.

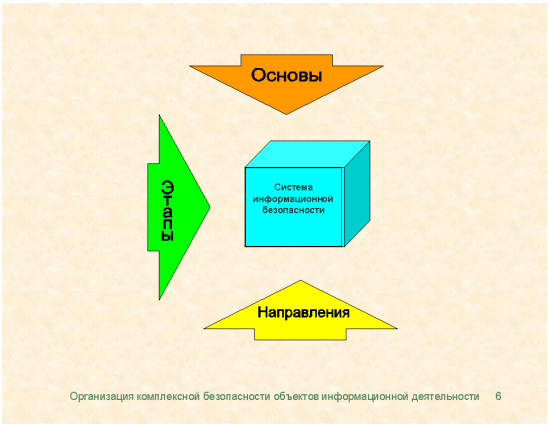
Белгілі жолдар мен әдстемелер қорғауды бағалау деңгейі АҚКЖ -ң жеке элементтерінің көрсеткіштерінен байқалады, бірақта осы уақытқа дейін АҚКЖ ң есепке алынған логикалық және функционалдық талаптарының жеткілікті толық бағалаулары өткізілген жоқ. Әдеби талдау негізінде, нормативті құжаттарды, мақалаларды және де басқа материалдарды, сонымен қатар практикалық істелінген жұмыстарды есепке ала отырып келесі жүйелендіру әдістемесі мен АҚКЖ – де қаралған экспертті білім талаптары ұсынылады.

АҚКЖ үлгісі көрсеткіштің негізгі блок түрінде берілген:

«негіздер» көрсеткіш блогы;

«бағыттар» көрсеткіш блогы;

«кезеңдер» көрсеткіш блогы.



НЕГІЗДЕР көрсеткіштер блогы (Оі)

АҚКЖ ИССН құруындағы өткізілген талдау қорытындысы көрсеткендей, жүйенің НЕГІЗІ немесе құрама бөлімі (1 сурет), соның ішінде ақпаратты қорғау жүйесі болып табылатындар:

- Заң шығарушы, нормативті-заңға сүйенген және ғылыми база;
- АЖ қауіпсіздігін қамтамасыз ету құрылымы және органдардың (бөлімшелердің) мақсаттары;
- Ұйымдық-техникалық және тәртіп шаралары (ақпараттық қауіпсіздік саясаты);
- Бағдарламалық – техникалық тәсілдер мен құралдар.

Көрсетілген АҚКЖ көрсеткіштерін келесідегідей түрде белгілейміз:

01 – нормативті құқықтық және ғылыми база сапалығы;

02 – құрылым толықтығы және қорғаныс қамтамасыз ететін органдар мақсаты;

03 – ұйымдық шаралар мен ақпарат қорғау әдістерінің (қауіпсіздік саясаты) сапалығы;

04 – бағдарламалық-техникалық тәсілдердің және қорғау құралдарының сапалығы.

БАҒЫТ көрсеткіштерінің блогы (Hj)

Белгілі әдістермен жүргізілген тәжірибеде және КСЗИ бағалауындағы БАҒЫТ тәжірибесінде көрсетілгендей ақпаратты қорғау әдістерін ерекшелеуге рұқсат етіледі. Бұл бағыттар 3.3. суретінде графикалық түрде бейнеленген.

Көрсеткіштерін белгілейік:

H1- ИССН объектілерін қорғау деңгейі;

H2 – қорғау процестерінің, процедуралардың және ақпаратты өңдеу бағдарламаларының деңгейі;

H3 – байланыс каналдарын қорғау деңгейі;

H4 – қосымша электр-магниттік сәулелердің басу деңгйі;

сапалығы.

КЕЗЕҢДЕР көрсеткіштерінің блогы (Mk)

Көрсетілген кезеңдерді көрсеткіштер түрінде көрсетейік:

M1 – қорғауға жататын ақпараттар анықтамасының толықтығы;

M2 – потенциалды мүмкін қиындықтар мен ақпараттық кемулер каналдарының табылу толықтығы;

M3 – осалдылыққа өткізілген бағалаулар және ақпаратқа қиындық тудырушы каналдардың тәуекелділігің сапалығы;

M4 – қорғаныс жүйесіне қойылатын талаптар анықтамасының сапалығы;

M5 – ақпаратты қорғау құралдарының сипаттамасының және таңдалу сапалығы;

Кезеңдер небір көбірек пунктілерге (қадамдарға) бөліне алады. «КЕЗЕҢДЕР» көрсеткіштерінің жалпы санын Mk деп белгілейміз (мұнда, k – 1 ден n - дейін).

Бақылау сұрақтары:

1. Ақпараттық қауіпсіздік жүйесіне не жатады?
2. Ақпараттық қауіпсіздіктің бағыттары?
3. Ақпараттық қауіпсіздіктің бағалауға жататын кезеңдерін атаңыз?

Дәріс№12.

Тақырыбы:Ақпаратты қорғаудың компоненттері.

Мақсаты: Қандай қорғаныс жүйелерін таңдау, құпия сөзді қолдануды қарастыру.

Жоспар:

12.1 Қорғаныс жүйесін таңдау.

12.2 Құпия сөздерді қолдану.

12.3. Қарапайым қорғаныс шаралары.

Кілттік сөздер: құпия сөз, DES мемлекеттік шифрлеу стандарты.

12.1. Қорғаныс жүйесін таңдау.

Кез-келген компьютерлік жүйе идеальды бола алмайды, яғни сіздің дербес компьютеріңізді толықтай қорғаныспен қамтамасыз ете алмайды. Деректерді өзгелердің қолына түсуден 100% сақтау тек жойып жіберу арқылы іске асады. Қорғаныс дәрежісі жоғарылаған сайын оны айналып өту тәсіліде талап етіледі. Қорғаныс амалын таңдау

жеткілікті дәрежеде қорғаныспен қамтамасыз ету керек, сонымен қатар келеңсіздіктер тудырмауы керек. Әрбір қолданушы өзіндік тәуекел анализін жүргізіу және де қандай қорғаныс амалын таңдау керек екенін білуі керек. Дербес компьютерлер үшін тәуекел анализінің үш түрі бар: автономдық жүйенің анализі, яғни бір компьютердің, жергілікті жүйе анализі және ауқымды желімен (мысалға Internet) байланысқан жойылған рұқсаты бар жүйе анализі.

12.2. Құпия сөздерді қолдану.

Құпия сөздерді қолданудың мақсаты келесілермен анықталады: егерде біреу сіздің деректеріңізбен немесе аппараттық амалдарыңызбен байланысқысы келсе, құпия сөздер оған көптеп кедергі кедтіру керек. “Маңдай кедергісі” құпия сөзіне шабуыл жасау кезінде біреуі сәйкес келгенше барлық мүмкін болатын құпия сөздер комбинациясы тексеріледі. Құпия сөз ұзындығы өскен сайын, көп уақыт кететін болғандықтан шабуылда қиындайды. Әрине көптеген банктер тек төрт разряздты (PIN) кодтарды қолданып қана қоймайды, сонымен қатар қорғанысты күшейтудің басқада амалдары қолданылады, мысалға, видеокамералар және карточкаларды жауып тастайтын АТМ-дер.

12.3. Қарапайым қорғаныс шаралары.

Көп жылдан бері қолданып келе жатқан бағалы ақпаратты қорғау үшін қиын емес амалдар бар. DOS және оның алдындағы операциялық жүйеде файлдарды толығымен жоймай жойылған файлдарды сақтайды. Жою кезінде қарапайым FAT іске қосылады: файлдың аты шынайысыз болады және файл жазылған сектор бос болып тұрады. Бұл жойылған файлдарды кейбір кең таралған утилиттердің көмегімен қалпына кетіруге болатынын дәлелдейді (мысалға, undelete).

Бақылау сұрақтары:

1. Қорғаныс жүйесін таңдау дегеніміз не?
2. Құпия сөзді қолданудың мақсаты?
3. Қандай қорғаныс шараларын білесіз?

Дәріс№13.

Тақырыбы:Компьютерлік желілердің қауіпсіздік ерекшеліктері.

Мақсаты: Компьютерлік желідегі қауіпсіздік ерекшеліктерімен және желі арқылы таралатын шабуылдармен таныстыру.

Жоспар: 13.1 Компьютерлік желілердің қауіпсіздік ерекшеліктері

Кілттік сөздер: желідегі қауіпсіздік, каналдарға рұқсатсыз ену, каналдан ақпараттың ағып кетуі.

13.1 Компьютерлік желілердің қауіпсіздік ерекшеліктері

Кез-келген желілік жүйенің ерекшелігі, оның компоненттері кеңістікте орналасады, ал олардың арасындағы байланыс физикалық түрде болады(коаксикальды кабель, витая пара,оптоволокно және т.б.) және бағдарламалық түрде хабарландыру механизмі көмегімен. Есептеуіш жүйенің объектілерінің арасындағы байланыс желілік байланыс бойынша ауыстыру пакеті ретінде жіберіледі.

Желілік жүйелерге жергілікті шабуылдан басқа желілік шабуылдар да жасалады. Оладың ерекшелігі біріншіден, қарақшы шабуыл жасалатын объектіден мыңдаған километр жерде орналасуы мүмкін, екіншіден шабуыл жеке компьютерге емес, желімен берілетін ақпаратқа жасала алады. Жергілікті және ауқымды желілердің дамуына байланысты алыстан шабуыл жасау қолданылуына қарай ең жоғарғы көрсеткіштер көрсетуде.

Алыстан шабуыл деп есептеуіш жүйеге байланыс каналы бойынша бағдарламалық түрде жүзеге асатын ақпараттық зақым келтіретін әсерді айтады.

Ақпаратты қорғау – ақпаратты ағып кетуден, ұрлаудан, өзгертуден, рұқсатсыз көшіру мен жоюдан қорғау мақсатында жасалатын әрекеттер жиыны. Ақпаратқа қауіп техникалық жағынан да келетін болғандықтан, келесі жағдайларды ескеру қажет: сервер сенімділігі, винчестер жұмысының кемшіліктері, қолданылған бағдарламалық жабдықтың кемшіліктері және т.б.

Дербес компьютермен жұмыстан желідегі жұмысқа өту ақпараттық қорғаныстың келесі себептер бойынша қиындатады:

1. желідегі қолданушылардың саны және олардың ауысуы. Құпия сөз және атау қою желіні бөгде адамның кіруінен қорғай алмайды;
2. желінің сөзылымы және желіге енудің потенциалды каналдарының көп болуы;
3. ақпараттық және бағдарламалық жабдықтардың кемшліктері, олар қолдану кезінде анықталады. Соның ішінде қуатты желілік ОЖ Windows NT немесе NetWare ақпарат қорғанысың дұрыс қондырылмауы.

Үлкен қашықтықты қамтитын желінің коаксикальды қабельді бір сегментінде проблеманың тереңдігін байқау үшін сур. 13.1 назар аударыңыз. Желіде ақпаратқа еніге мүмкіндік беретін каналдардың көптігі көрінеді. Желідегі барлық құрылғы электромагниттік сәулеленудің көз болып табылады, себебі сәйкес алаңдар нашар экрандалған.. Кабельдік желінің жерде болуы желідегі ақпаратқа енуге рұқсат береді. Коаксикальды немесе витая пара кабельдерін пайдалану, кабельдік жүйеге физикалық түрде қосылуға мүмкіндік береді. Желіге енетін құпия сөз белгілі болып немесе табылған болса, желіге ену файл-серверден немесе жұмыс станциясынан мүмкін болады. Сонымен қатар, желіден тыс каналдардан ақпарат ағып кетуі мүмкін:

- ақпарат тасымалдаушылардың қоймасы,

- құрылыс конструкциялары және терезелер, микрофондық эффект көмегімен құнды ақпаратттың ағып кетуіне себеп болады.,
- телефондық, радио-, және басқа да проводты және проводсыз каналдар (соның ішінде ұялы байланыс каналдары).

Компьютерлік желідегі ақпаратқа рұқсатсық енудің каналдары мен орындары Интернет арқылы таралатын желілік шабуылдардың классификациясы:

- Сниффер пакеттері – promiscuous режимінде жұмыс жасайтын желілік картаны пайдаланатын қолданбалы бағдарлама.
- IP-спуфинг– корпорацияда немесе одан тыс жерде бола тұрып хакер өзін рұқсатты қолданушы ретінде ақпаратқа қол жеткізуі.
- Парольді шабуылдар – Рұқсаты бар қолданушының паролімен желіге ену мүмкіндігі.
- Қосымшалар деңгейіндегі шабуылдар .
- Вирустар және "трояндық ат".

Бақылау сұрақтары:

1. Компьютерлік желілердің қауіпсіздік ерекшеліктері қандай?
2. Қандай себептер компьютермен жұмыстан желідегі жұмысқа өтуде ақпараттық қорғанысты қиындатады?
3. Интернет арқылы таралатын желілік шабуылдардың классификацияларын атаңыз?

Дәріс№14.

Тақырыбы:Ауқымды желідегі ақпаратты қорғау.

Мақсаты: Интернет желісіндегі және электрондық поштадағы ақпаратты қорғау негіздерімен таныстыру.

Жоспар:

14.1 Internet желісінде ақпаратты қорғау

14.2 Электрондық поштаны қорғау

Кілттік сөздер: Internet желісі, Левин ісі, электрондық поштаны қорғау.

14.1 Internet желісінде ақпаратты қорғау

Internet желісінің бірегейлігі қандайда бір физикалық тұлғаның немесе жекеменшік компанияның, мемлекеттің немесе жеке елдің меншігінде еместігі. Сондықтанда іс-тәжірибе жүзінде оның барлық сегменттерінде орталықтан басқару және де басқа ақпараттарға бақылау жасау тәсілдері жоқ. Осының нәтижесінде тәжірибе жүзінде қылмыскерлер қолданатын кез-келген ақпаратқа кіру мүмкіндігі шектелмейді. Internet

желісін тек компьютерлік қылмыстың орындалу құралы ретінде қарамай, сонымен қатар әр түрлі қылмыстық іс-әрекеттің енгізілу ортасы деп те айтуға болады.

Internet желісін қолдану кылмыстық іс-әрекетте заң бұзушылар үшін қылмыстық ақпаратты алмасуға шақырады. Бұрын бүкіл әлеммен байланысу барлық державаның тек қана арнайы қызметкерлерінің мүмкіндіктері болды, олар қажетті ғарыштық технология болды. Internet желісінің қылмыскерлер үшін тағыда бір ерекшелігі ауқымды масштабта адамдарға ақпаратты-психологиялық әсер ету. Қылмыстық қоғам өзінің доктриндерінің және білімдерінің таралуына көңіл бөледі және қоғамдық ойларды тыңдайды, қылмыстық әлем өкілінің позициясының бекуіне және құқық қорғау органдарының беделін түсіруге жұмыс жасайды.

Бірақ та Internet желісі қылмыстың орындалу құралы ретінде айтарлықтай қызығушылық көрсетті (көбіне экономика және қаржы сферасында). Ең қарапайым нұсқауы бұл авторлық құқықты бұзумен байланысты қылмыс. Осындай қылмыс түрлеріне бірінші кезекте иемденуші компанияның серверінде орналасқан бағдарламаны заңсыз көшіру және сату жатады. Қылмыстың екінші тобына тауарды және қызметті ресми емес түрде алу, яғни әртүрлі телефон компаниялары төлейтін қызметті ақысыз пайдалану. Қызметтерді заңсыз пайдаланудың басқа тәсілдерінің негізіне, осы қызметті көрсететін компаниялардың мәліметтер қорынан осы қызмет туралы мәліметтерді модификациялау жатады. Мұндай қылмыстар түріне несиеге алынған зат туралы ақпаратты заңсыз пайдалану немесе оны жойып жіберу, не басқа төленген қызметтің орнына жіберу болып табылады.

Internet желісінде қылмыскерлердің көптеп пайда болуының алғы шарты компьютерлік желінің өсуімен ақпараттың бағалы тауарға айналуы. Әсіресе бұл банк сферасында ақша салу мен ақша салушы мәліметінде, банк пен клиенттің қаржылық жағдайы, банк саясаты аумақтарында кездеседі. Несиелік-қаржылық субъекттің қазіргі кездегі шарттарына байланысты ақпарат алмасудың болуы, және сонымен қатар банктік алшақталған филиалдарымен байланысып отыру үшін Internet желісі қолданылады. Бұл қылмыскерлерге құпия ақпараттарға енуге нақты шанс беріп отыр. Қылмыскерлердің бұндай ақпараттарды жойып жіберуі мекememен бәсекелестіктен туындайды. Internet ағымы арқылы орындалатын компьютерлік қылмыстардың қосымша сферасында электронды банктік есептердің шығуымен қылмыста күшейді. Электронды түрдегі ақпаратты алудың әр түрлі тәсілдері бар. Банктегі клиенттермен есеп айырбастайтын ақпаратты қылмыскерлердің басқаруы, электронды банктік есептегі алгоритмнің өзіне өзгеріс енгізу және т.б. Мысалы, валютаның курсын өзгерту, банк валютасын клиенттерге қымбат бағамен, ал банкке төмен бағамен жасап арасындағы ақшаны

қылмыскерлердің өзіне қалып отыруы. Қаскүнемдердің корпоративтік компьютерлік желілеріне заңсыз кіруімен байланысты Интерполдың қарастырған Левин ісі деп аталатын өте маңызды трансұлттық компьютерлік желілік қылмысы нәтижесінде американдық Сити-банк 400 мың долларынан айырылды, сондықтан бұндай қылмыстар тек компьютерлік мәліметтерді өңдеу аумағындаға мамандарды ғана емес сонымен қатар компанияның бастықтарының да назарын аударды. Соңғы кездерде кеш болса да барлық мекемелер өз компьютерлерінің бүкіл әлемдік Internet желісіне шығуға мүмкіндік алғанда қандай тәуекелге баратынын түсінді. Олар қаскүнемдердің барлық ұсталары (мамандандырылған бұзушылар және ұрылар, кекті бағынушылар немесе бәсекелестер) алдында тәуекелге барады және де оларды төмендегідей метериалдық шығынға ұшыратады. Нәтижесіде компьютерлік желілердегі ақпаратты қорғауда, нақты құралдарды таңдау негізгі роль ойнайды.

- Компьютерлік жүйеде сақталған ақпараттың бағалылығын анықтау;
- Қаскүнем компьютерлік жүйенің қорғанысын жеңу үшін қолданылатын уақыттық және қаржылық шығын бағасы;
- Компьютерлік жүйеге шабуылдаған кездегі қаскүнем қылығының ықтималдық моделі;
- Ұйым үшін компьютерлік жүйені адекватты қорғауға қажетті уақыттық және қаржылық шығын бағасы.

14.2 Электрондық поштаны қорғау

Көптеген электронды пошталар оқуға болатын мәтіндік түрде Интернет хаттамалары немесе басқада ауқымды желілер арқылы жіберіледі. Электронды коммуникацияның конфеденциалды түрі туралы заң сіздің электронды поштаңызды қарапайым телефон қоңырауына теңейді.

Хакерлер сіздің электронды поштаыңзға енуге әртүрлі тәсілдерді қолданады, ал сіздің деректеріңіз шифрленген болса, ол электронды поштаға кіргенмен оны оқи алмайды. Егер сізге құпия ақпаратты қорғау керек болса, онда жіберу алдында шифрлеу үшін PGP-ны қолданыңыз.Compaq компаниясы қол жетерлік бағадағы саусақтардың ізі бойынша қолданушылар идентификациясына негізделген бағдарламалық-аппараттық шешім шығарды. Биометрикалық ақпараттық анализ технологиясын қолдана-тын бұл құрылғы соңғы технологияның жетістіктерімен сәйкестендрілген және ол diskpro дербес компьютері, Armada қол компьютері және Compaq фирмасынан шыққан жұмыс станцияларымен бірлесіп жұмыс жасайды. Бұл шешім желідегі ақпаратты қорғау жүйесінің сенімділігін арттырады, жүйеге кіру кезіндегі қолданушының тіркелу

процедурасын жеңілдетеді және ірі корпоративтік желіні басқарумен байланысты шығындарды қысқартады

Бақылау сұрақтары:

1. Интернет желісіндегі қылмыстың қандай түрлерін білесін? Мысал келтіріңіз?
2. Интернет желісіндегі қылмыскерліктің көбеюін қалай түсіндіре аласыз?
3. Электрондық поштаны қалай қорғауға болады?

Дәріс№15.

Тақырыбы:Компьютерлік жүйелер қауіпсіздігі.

Мақсаты: Желідегі ақпаратқа қауіп жергілікті желідегі ақпаратты қорғау негіздерімен таныстыру.

Жоспар:

15.1 Желі қауіпсіздігінің моделі

15.2 Жергілікті желідегі ақпаратты қорғау

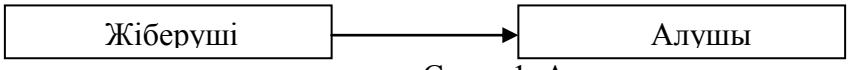
15.3 Рұқсатсыз кіруден қорғауды тану

Кілттік сөздер: желілік шабуыл, актив және пассив шабуыл, желілік қауіпсіздік моделі.

15.1 Желі қауіпсіздігінің моделі

Желілік шабуылдың классификациясы

Жалпы алғанда, жіберушіден (файл, қолданушы,компьютер) алушыға (файл, қолданушы,компьютер) жіберілетін ақпараттық лек болады.



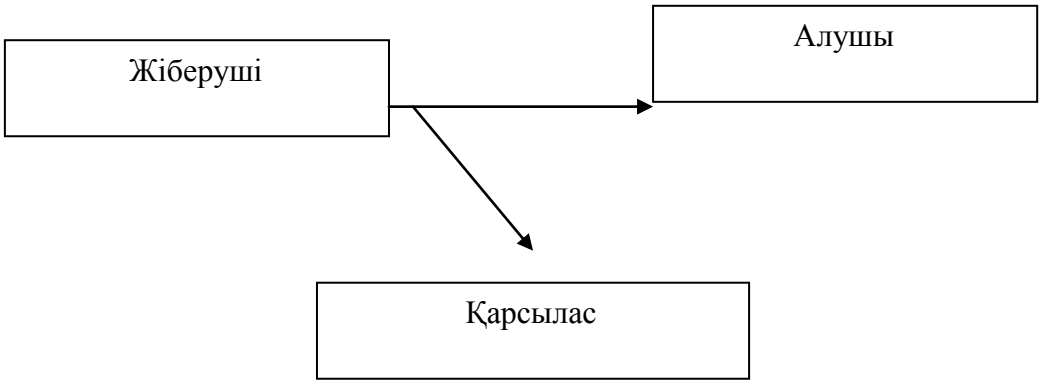
Сурет.1. Ақпараттық лек

Барлық шабуылдарды екі топқа бөлуге болады: пассив және актив

I.Пассив шабуыл

Берілген хабарламаны қарсыласы модификациялай алмайтын және ақпараттық каналға жөнелтуші мен алушының арасына өз хабарларын қоя алмайтын шабуылды пассив шабуыл деп атайды.

Пассивтік шабуылдың мақсаты-берілген хабарлар мен трафика анализдерін тыңдау.



Сурет.2. Пассивтік шабуыл

II. Актив шабуыл

Қарсыластың жіберілген хабарларды модификациялай алатын және өз хабарларын қоя алатын шабуылды актив шабуыл деп атайды.

Активтік шабуылдың мынадай түрлері бар:

1. Қызмет етуден бас тарту-DOS- шабуыл (Denial of Service)

Қызметтен бас тартужелілік сервистің дұрыс қызметін бұзады. Қарсылас белгілі бір адреске бағытталған барлық хабарламаларды ұстай алады. Мұндай шабуылдың мысалы трафиканың жасалуы болып табылады, сол себепті желілік сервис заңды тұтынушының сұранысын өңдей алмайды.

TCP/IP желісіндегі мұндай шабуылдың классикалық мысалы ретінде SYN шабуылын айтуға болады.

Бұзушы TCP-біріктіруші қондырғысына ұқсайтын пакетті жібереді, бірақ бұл бірігудің қондырғысын аяқтайтын пакетті жібермейді. Нәтижесінде серверде жадының шамадан тыс толығуы жүзеге асады да, сервер заңды тұтынушымен жалғастыруды жүзеге асыра алмайды.

2. Берілген лектің модификация шабуылы «man in the middle »

Берілген лектің модификациясы дегеніміз-берілген хабарламаның мазмұнының өзгеруі немесе хабарлау тәртібінің өзгеруі.

3. Жалған лектің пайда болуы(фальсификация)

Фальсификация дегеніміз-бір субъектінің өзін басқа адам ретінде беруі.

4. Қайталама қолдану.

Берілген мәліметті рұқсат етілмеген жолмен алатын пассивтік ұстау-қайталама қолдану деп аталады.

Replay-шабуылы.Шынында, replay-шабуыл фальсификация нұсқасының бір түрі,оны рұқсат етілмеген мәліметті алудың кең таралған түрі деп есептейді де,шабуылдың ерекше түрі ретінде көп қарайды.

15.2 Жергілікті желідегі ақпаратты қорғау

Қаіпсіздік сервисының негізі келесілер:

Құпиялылық – жіберілетін немесе сақтауға арналған енжар шабуылды тоқтату.

Аудентификация – ақпаратты заңды бастамадан алудың кепілдігі.

Байланысты орнатқан жағдайда екі аспект пайда болады.Біріншіден байланыс кезінде сервис кепілдік беру керек, бұл жағдайда екі қатысушыда міндетті. Екінщіден, сервис кепілдік беру керек, бұл жағдайда байланыс әсер етпейді, үшіншіден байланыс орнатылғаннан кейін заңсыз жақпен жасырынуы мүмкін.

Бүтінділік – сервис, ақпаратты сақтаған немесе жіберген кезде өзгермейтініне кепілдік береді. Лек хабарламаларға, жалғыз хабарламаларға немесе хабарламалардың ішіндегі жеке өрістерге сонымен қатар сақталған файлдармен жеке жазьа файлдарға қолданылуы мүмкін.

Мүмкін еместілік – қабылдаушыға сол сияқты жіберушігеде, жіберілген фактыдан бас тарту. Сонымен хабарлама жіберілген кезде қабылдаушы заңсыз жіберушінің хабарлама жібергенінесенімді бола алады.

Рұқсат бақылауы – коммуникациалдық линиялар арқылы жүйеге және приложения рұқсатты шектеу және бақылау мүмкіндігі.

Рұқсаттылық – шабуылдың нәтижесі сол немесе басқа сервистің жоғалуы немесе томендеу рұқсаттылығы.

15.3 Рұқсатсыз кіруден қорғауды тану

Мысалы, үшінші жақ екі қатысушының арасындағы құпия ақпаратты қарсыласқа ыңғайлы болмас үшін бөлуге жауапты болуы мүмкін. Немесе үшінші жақ екі қатысушының расындағы жіберілетін хабарламаның дұрыстығына қатысты таластарды шешуге қатысады.

Жағымсыз кіру мүмкіндігінің басқа типі редакторлар, компиляторлар және т.с.с. қолданбалы бағдарламалар мен бағдарламалық утилиттерге әсер ететін нәрселерді есептеуіш жүйеге енгізу. Осылайша, шабуылдың екі типі болады:

1. Жүйеде сақталған мәліметтерді модификациялау немесе алу мақсатында ақпаратқа қол жеткізу мүмкіндігі.
2. Серверлерді қолдануға әсер ету мақсатындағы серверлерге шабуылдар.

Вирустар мен құрттар – осындай шабуылдың мысалы. Мұндай шабуылдар дискета арқылы да, желі арқылы да жүзеге асуы мүмкін.

Жағымсыз кіру мүмкіндігінің алдын алатын қауіпсіздік серверлерін екі категорияға бөлуге болады:

1. Бірінші категория күзету функциялары термині арқылы анықталады. Бұл механизмдер авторленген қолданушыларға ғана кіру мүмкіндігін беретін, парольді қолдану негізінде құрылған кіру процедурасын қосады. Бұл механизмдер сонымен қоса TCP/IP протоколының түрлі деңгейдегі стектерінде болатын шабуылдардың алдын алады, және де вирустар мен құрттардың енуі туралы хабарлайды да, осындай типтегі барлық шауылдарға қарсы тұрады.

2. Екінші қорғау шебі қолданушылардың іс – әрекетін бақылайтын және кіру мүмкіндігін қадағалайтын түрлі ішкі мониторлардан тұрады.

Ақпараттық жүйе қауіпсіздігін қамтамасыз ету кезіндегі негізгі ұғымдардың бірі – авторизация. Авторизация – белгілі бір ресурстар мен объектілерді қолдану мүмкіндігі ережелерін анықтайтын ұғым.

Ақпараттық жүйе қауіпсіздігін қамтамасыз ету кезінде мынадай негізгі принциптер бар:

1. Ақпараттық жүйе қауіпсіздігі бұл жүйені қолданылып отырған мекеменің ролі мен мақсатына сай болуы тиіс.

2. Ақпараттық жүйе қауіпсіздігін қамтамасыз ету комплекстік және біртұтастықты талап етеді.

3. Ақпараттық жүйе қауіпсіздігі мекемедегі басқарушы жүйенің ажырамас бөлігі болуы керек.

4. Ақпараттық жүйе қауіпсіздігі экономикалық жағынан расталған болуы керек.

5. Қауіпсіздікті қамтамасыз ету жауапкершілігі нақты анықталған болуы керек.

Бақылау сұрақтары:

1. Желідегі ақпаратты қорғау дегеніміз не?
2. Жергілікті желідегі ақпаратты қорғау?
3. Рұсатсыз кіруден қорғану және оның жолдары?

Пайдаланған әдебиеттер тізімі.

Негізгі әдебиеттер:

1. Воробьев, "Защита информации в персональных ЭВМ", изд. Мир, 1993 г
2. Ковалевский В., "Криптографические методы", Компьютер Пресс 05.93
3. Ақпаратты қорғау және қауіпсіздік аймағындағы Қазақстан Мемлекетінің Заң актілері.
4. Ақпаратты қорғау және қауіпсіздік аймағындағы Қазақстан Мемлекетінің нормативті құжаттар.
5. Лавров Д.Н. Элементы теории чисел и криптографии. Омск, 2003. Ковалевский В., "Криптографические методы", Компьютер Пресс 05.93
6. Зегжда Д.П. Ивашко А.М. Основы безопасности информационных систем. М., 2000.
7. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. М.: ДМК Пресс, 2002
8. Романец Ю.В., Тимофеев П.А. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: Радио и Связь, 1999 .
9. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М: Кудиц – ОБРАЗ, 2001.
10. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. – М.: “Яхтсмен”, 1993.
11. Специвцев А.В. и др. Защита информации в персональных ЭВМ. –М.:Радио и связь, 1993.
12. Герасименко В.А. Защита информации в автоматизированных системах. ч.1,2. – М.:”Высшая школа”, 1995.
13. Ященко В.В. Введение в криптографию. Новые математические дисциплины. – М.: МЦНМО Питер,2001.

Қосымша әдебиеттер:

14. Мафтик С., "Механизмы защиты в сетях ЭВМ", изд. Мир, 1993 г.
15. Я люблю компьютерную самооборону. “Только для взрослых” Москва 2002 г.
16. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. –М.: Горячая линия – Телеком, 2000.
17. Алексеев В.Е. Вычислительная техника и программирование. Практикум по программированию. Москва. Высшая школа. 1991.
18. Фаронов В.В. Турбо Паскаль 7.0 Начальный курс. Учебное пособие.-М.:Нолидж,2001г.
19. Исаев С.Ә. Компьютерлік технология негіздері курысына арналған практикум.: Әдістемелік оқу құралы. – Алматы. 2000ж.
20. Microsoft Office 2000: шаг за шагом: прак. пособ. /пер с англ...-М.: Эком, 2000.
21. Бэндл Д. Защита и безопастность в сетях Liпих: для профессионалов /+СД/.- СПб.: Питер, 2002.
22. Богатоф Д. Ф., Богатоф Ф. Г. Основы информатики и математики для юристов: учеб пособ. Т. 1. .- М.: Приор, 2001.
23. Беркінбаев К. М. /Педагогика ғылымдарының кандидаты/ Информатика: оқулық.- Алматы, Заң әдебиеті, 2007
24. Симонович С. В. и др. Информатика: Базовый курс.- СПб.: Питер, 1994
25. Каймин В. А. Информатика.- М.: Инфра-М, 2003.
26. Гаврилов О. А. Курс правовой Информатики.- М.: Норма.
27. Гордеев А. В. Операционные системы: Учеб.для вузов.- СПб.: Питер, 2007.