Т. Рысқұлов атындағы ҚазЭУ-дің
осы заманғы оқу басылымдары

Қ.С. АЛДАЖАРОВ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК НЕГІЗДЕРІ

Оқу құралы

ЭКОНОМИКА БАСПАСЫ

Алматы
2011

УДК 002. 56(075.8)
ББК 73 я 73
А 40

ҚР жоғары оқу орындарының экономикалық мамандықтары бойынша ЖОО және ЖОО-дан кейін, Т. Рысқұлов атындағы ҚазЭУ-дің Ғылыми кеңесі және ОӘК ұсынған

Пікір жазғандар: **О.Н. Нұржұмаев** – ф-м.ғ.д., профессор, Т. Рысқұлов атындағы ҚазЭУ-дің «Қолданбалы информатика» кафедрасы; **Д.Н. Шоқаев** – т.ғ.д., профессор, Қ. Сәтбаев атындағы ҚазҰТУ-дің «Техникалық кибернетика» кафедрасының меңгерушісі; **Н.Т. Сайлаубеков** – ф-м.ғ.к., ҚБТУ «Экономика және менеджмент» кафедрасының сеньор-лекторы.

А 40 **Алдажаров Қ.С.**
Ақпараттық қауіпсіздік негіздері: Оқу құралы. – Алматы: Экономика, 2011. – 120 бет.

ISBN 978–601–225–254–5

Ұсынылып отырған оқу құралы күндізгі және сырттай оқу бөліміндегі студенттер үшін «Ақпараттық қауіпсіздік негіздері» пәні бойынша жазылды.

Бұл оқу құралында ақпараттық қауіпсіздікке байланысты теориялық мәліметтер, негізгі түсініктер және әр түрлі қауіпсіздік модельдері мен әдістері, мәтіндерді шифрлау алгоритмдері, вирустарға қарсы программалар туралы мәліметтер берілген.

УДК 002. 56(075.8)
ББК 73 я 73

ISBN 978-601–225–254–5

КІРІСПЕ

Ақпараттық технологиялардың дамуы, оларды адам қызметтерінде кең пайдалануы жыл сайын ақпараттық қауіпсіздік проблемаларының өзектілігін және бірегей күрделілігін анықтайды.

Ақпаратты өңдеу технологиялары үздіксіз жетілдірілуде, ал сонымен бірге күнделікті ақпараттық қауіпсіздікті қамтамасыз ету әдістері де өзгеруде. Шынында, әмбебапты қорғау әдістері жоқ, нақты жүйеге қауіпсіздік механизмдерді жасау барысында жетістіктер жүйенің ерекшеліктеріне байланысты. Оларды есепке алу өте күрделі мәселелер, сондықтан ақпараттық қауіпсіздікті әр түрлі ақпаратты қорғау жүйелерді құрастыруға формалды емес ұсыныстар жыйынтығы ретінде қарастырады.

Дегенмен барлығы да күрделі болып келеді. Практикада қорғау жүйелерін жасауда оларды іске асыру кезінде техникалық ерекшеліктеріне тәуелді емес жалпы заңдылықтар есепке алынады. Осындай әмбебапты принциптер ақпараттық қауіпсіздікті жеке ғылыми пән ретінде ерекшелейді.

Оқу құралы «Ақпараттық қауіпсіздік негіздері» пәніне арналған және келесі мәселелер қарастырылған: пәннің қысқаша сипаттамасы, ұлттық қауіпсіздік негіздері жөнінде түсінік, ақпаратты қорғау проблемалары: ақпараттық қауіптер және оларға қауіптерге қарсы әрекеттер, қорғаныштың программалық әдістері, ақпараттық жүйелердің аппараттық және программалық платформасын талдау: қорғаудың техникалық әдістері, ақпараттық қауіпсіздік есептерін шешу әдістері. Осымен қатар оқу құралында келесі мәселелер: ақпараттық жүйелердің қауіпсіздік үлгілері, ақпаратты қорғаудың абстракты модельдері, ақпараттық қауіпсіздік саясаттары, симметриялық және асимметриялық криптожүйелер (кілті ашық криптожүйелер), ақпаратты қорғау дұрыстығының әдістемесі, ақпаратты рұқсатсыз алу әдістеріне және ақпараттың қорғанышына қойылатын талаптар, DoS шабуылдарының түрлері мен олардан қорғану әдістері, компьютерлік желілердегі ақпараттың қауіпсіздігі, вирустардан қорғану тыс қалмаған.

1. Пәннің қысқаша сипаттамасы. Ұлттық қауіпсіздік негіздері жөнінде түсінік

1.1. Ұлттық қауіпсіздендірудің түсініктері

Елдің дамуы үшін маңызды мәселенің бірі – ұлттық қауіпсіздікті қамтамасыз ету. Оның шешімдерін табу үшін сәйкес күш, құралдар, қорлар, арнайы құрылымдар, басқарушы кадрлар мен үздік мамандар, ғылыми, ұйымдастырушылық, құқықтық және басқа да қамсыздандыру әрекеттері қажет. Осыған орай мемлекетімізде келесі заңдар қолдануда: Қазақстан Республикасының Ұлттық қауіпсіздігі туралы Заңы (26.06.1998), Мемлекеттік құпиялар туралы Заңы (15.03.1999), Терроризмге қарсы күрес туралы Заңы (13.07.1999), Электрондық құжат және электрондық цифрлық қолтаңба туралы Заңы (07.01.2003), Ақпараттандыру туралы Заңы (08.05.2003), Экстремизиге қарсы іс-қимыл туралы Заңы (18.02.2005).

Ұлттық қауіпсіздік – саясат, экономика, әскер, ақпарат, экология, әлеумет және басқа да қауіпсіздік объектілерінің іс-әрекет ету орталарында тұлға, қоғам, мемлекеттің (ұлттық мүдде) өмірлік маңызды мүдделерінің қорғалу күйі. Сондай-ақ, бұл тек ұлттық мүдделердің қорғалу күйі ғана емес, соған сәйкес билік институттарының осы мүдделердің қорғалуына қатысты қорғанышты жүзеге асыру тетігін құру дайындығы мен мүмкіндігі.

Ұлттық қауіпсіздіктің анықтамасының мазмұны дәстүрлі түрде келесіге негізделінеді – ұлттың өз-өзін сақтандыру және дамыту керектігін сезіне отырып осыған орай ұлттық мүдделерін қалыптастыру.

Мүдде дегеніміз жеке адамның, топтардың, әлеуметтік қоғамның әлеуметтік тәртіптерін анықтайтын іс-әрекеттері. Ұлттық мүдде елдің басты мақсаттарын анықтап, ішкі және сыртқы саясаттың мақсатты және ағымдағы мәселелерін қалыптастырып, мемлекеттік басқару жүйесі арқылы жүзеге асырылады.

Мүдделер келесіге бөлінеді:

1. Жеке даралығына байланысты:
- жеке адам мүддесі;
- топ мүдделері;
- қоғам мүдделері.

2. Бағыттарына байланысты:
- экономикалық;
- саяси;
- отаншылдық, патриоттық.

3. Сезіну деңгейіне байланысты:
- берекесіз түрде іске асырылуы;
- бағдарлама арқылы іске асырылуы.

4. Орындау мүмкіншілігіне байланысты:
- нақты мүдделер;
- жалған мүдделер.

5. Қоғамның даму үрдісіне (тенденциясына) байланысты:
- үдемелі (прогресивті);
- ескішіл (сақтанымпазды, консервативті);
- кертартпалық.

6. Іске асыру мерзіміне қарай:
- ұзақ мерзімді;
- орта мерзімді;
- қысқа мерзімді.

7. Субъектінің сипатына (мінезіне) қарай:
- таптық (классовые);
- ұлттық;
- мамандық.

Ұлттық мүдделердің қалыптасу идеясы ең бірінші – тайпалардың, содан кейін мемлекеттердің пайда болуына байланысты. Сол кездерде адамның санасында *біз – олар*, *біздікі – біздікі емес* деген ұғымдар пайда болды. Бірақ, ұлттық мүдделердің қазіргі ұғымы XVIII және XIX ғасырлардың межелерінде жаңадан қалыптаса басталды. Бұған ықпал жасаушы – азаттық қоғамдардың қалыптасуы және демократиялық элементтердің пайда болуы.

Қазақстанның ұлттық қауіпсіздік туралы заңында (4-тармағы) ұлттық мүдделер туралы былай айтылған:

Қазақстан Республикасының ұлттық мүдделері төмендегідей:

1. Адамның және азаматтың бостандығы мен құқықтарын қамтамасыз ету.
2. Мемлекетте саяси тұрақтылық пен қоғамдық келісімдерді сақтау.
3. Бүкіл Қазақстан елі үшін экономикалық даму.
4. Қазақстандық патриотизмді тәрбиелеу және Қазақстан елінің бірлігін бекіту.
5. Қазақстандық қоғамның патриоттық және материалдық байлығын сақтау және өсіру.
6. Қазақстан Республикасының конституциялық құрылысының өзгермелілігі: мемлекеттік тәуелсіздігінің, мемлекеттік шекараның, президенттік басқару формасының.
7. Мемлекеттік институттардың тұрақты жұмыс істеу және олардың қызметтерінің тиімділігінің өсуі.
8. Қазақстан Республикасының әскери жасақтары мен Қарулы күштерінің дайындығы.
9. Заңдардың мұқият орындалуы және тәртіптің сақталуы.
10. Серіктестік негізде халықаралық қатынастардың дамуы.

Қоғамдық қауіпсіздік – Қазақстан азаматтары өмірінің, денсаулығының және игілігінің, сондай-ақ Қазақстан қоғамы құндылықтарының оларға залал келтіре алатын ықтимал қауіптер мен қатерлерден саяси-құқықтық, рухани-адамгершілік, әлеуметтік қорғалуы:

- ұлттық қауіпсіздік объектілері – жеке адам, оның құқықтары мен бостандықтары, қоғам, оның материалдық және рухани құндылықтары, мемлекет, оның конституциялық құрылысы, тәуелсіздігі және аумақтық тұтастығы;
- ұлттық қауіпсіздік субъектілері – өз өкілеттігін биліктің заң шығарушы, атқарушы және сот билігі тармақтарының органдары арқылы жүзеге асыратын мемлекет, азаматтар мен ұйымдар;
- ұлттық қауіпсіздікке төнетін қауіп-қатер – ұлттық мүдделерді іске асыруға кедергі жасайтын немесе оларға қауіп төндіретін жағдайлардың, процестер мен факторлардың жиынтығы;

– экологиялық қауіпсіздік – жеке адамның, қоғам мен мемлекеттің өмірлік маңызды мүдделері мен құқықтарының қоршаған ортаға антропогендік және табиғи әсері салдарынан туындайтын қауіп-қатерден қорғалуының жай-күйі;
– экономикалық қауіпсіздік – Қазақстан Республикасы ұлттық экономикасының оның тұрақты дамуы мен экономикалық тәуелсіздігіне қатер төндіретін ішкі және сыртқы жағдайлардан, процестер мен факторлардан қорғалуының жай-күйі.

Қауіпсіздікке қатер төну дегеніміз – өмірлік маңызды мүдделерге қауіп тудыратын жағдайлар мен шарттар жиынының бар болуы. Қатерлер ішкі, сыртқы көздерден туындауы мүмкін, оларға адамзаттың іс-әрекет ететін түрлі ортасындағы елдегі қоғамдық дамуды және халықаралық аренаны айтуға болады. Қатер – қарама-қайшылықты көрсету формасы. Жоғарыдағы қатерлерді тауып айқындап, залалсыздандыру ұлттық қауіпсіздікті қамтамасыз ету негізіне жатады.

1.2. *Қауіпсіздіктің түрлері мен санаттары*

«Ұлттық қауіпсіздік» түсінігі ішкі, сыртқы болып бөлінетін қатерлердің, қорғаныш объектінің өмірлік маңызды мүдделерінің, олардың арасындағы тепе-теңдіктің бар болуын бейнелейді. Ұлттық қауіпсіздікті қамтамасыз ету мәселесін тиімді шешу үшін түрлі қауіпсіздік факторларын (саяси, экономикалық, әскери, ақпараттық, әлеуметтік, экологиялық және т.б.) жүйелі түрде қарастыру, мемлекеттің барлық негізгі құрылымдарының өзара әрекет ету тетігін қалыптастыру керек. Жоғарыда келтірілген заңдарда келесі қауіпсіздіктің түрлері мен санаттары (категориялары) берілген:

Қоғамдық қауіпсіздік – Қазақстан азаматтары өмірінің, денсаулығының және игілігінің, сондай-ақ Қазақстан қоғамы құндылықтарының оларға залал келтіре алатын ықтимал қауіптер мен қатерлерден саяси-құқықтық, рухани-адамгершілік, әлеуметтік қорғалуы.

Ұлттық қауіпсіздік объектілері – жеке адам, оның құқықтары мен бостандықтары, қоғам, оның материалдық және рухани құндылықтары, мемлекет, оның конституциялық құрылысы, тәуелсіздігі және аумақтық тұтастығы.

Ұлттық қауіпсіздік субъектілері – өз өкілеттігін биліктің заң шығарушы, атқарушы және сот билігі тармақтарының органдары арқылы жүзеге асыратын мемлекет, азаматтар мен ұйымдар.

Ұлттық қауіпсіздікке төнетін қауіп-қатер – ұлттық мүдделерді іске асыруға кедергі жасайтын немесе оларға қауіп төндіретін жағдайлардың, процестер мен факторлардың жиынтығы.

Экологиялық қауіпсіздік – жеке адамның, қоғам мен мемлекеттің өмірлік маңызды мүдделері мен құқықтарының қоршаған ортаға антропогендік және табиғи әсерлер салдарынан туындайтын қауіп-қатерден қорғалуының жай-күйі.

Экономикалық қауіпсіздік – Қазақстан Республикасы ұлттық экономикасының оның тұрақты дамуы мен экономикалық тәуелсіздігіне қатер төндіретін ішкі және сыртқы жағдайлардан, процестер мен факторлардан қорғалуының жай-күйі.

1.3. *ҚР ұлттық қауіпсіздендірудің жүйесіндегі ақпараттық қауіпсіздендірудің рөлі мен орны*

Ел Президентінің 1997 жылғы 10 қазандағы «Қазақстан – 2030. Барлық қазақстандықтардың өсіп-өркендеуі, қауіпсіздігі және әл-ауқатының артуы» атты Қазақстан халқына Жолдауында ұзақ мерзімді басымдық ретінде ұлттық қауіпсіздік айқындалды, оның құрамының бірі ақпараттық қауіпсіздік болып табылады. Қоғам мен мемлекеттің әлеуметтік-экономикалық және мәдени өміріндегі ақпараттық технологиялардың даму серпіні ақпараттық қауіпсіздік мәселелерін шешуге жоғары талаптар қояды.

Мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету ақпарат алу саласында адамның және азаматтың конституциялық құқықтары мен бостандықтарын іске асыруға қабілетті ұйымдастырушылық, техникалық, бағдарламалық, әлеуметтік

тетіктерді қамтитын кешенді көзқарасты пайдалануды, оны конституциялық құрылыстың мызғымастығын, Қазақстан Республикасының егемендігі мен аумақтық тұтастығын, саяси, экономикалық және әлеуметтік тұрақтылықты, заңдылық пен құқықтық тәртіпті қорғау мақсатында пайдалануды, ақпараттық қауіпсіздік саласында өзара тиімді халықаралық ынтымақтастықты дамытуды талап етеді.

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі мақсаттары:

1. Ақпарат қорғаудың ұлттық жүйесін, оның ішінде мемлекеттік ақпараттық ресурстарды құру және нығайту;
2. Мемлекеттік ақпараттық ресурстарды, сондай-ақ ақпарат саласында адам құқықтары мен қоғам мүдделерін қорғау;
3. Қазақстанның ақпараттық тәуелділігін, басқа мемлекеттер тарапынан ақпараттық өктемдікті немесе тосқауылды, Президенттің, Парламенттің, Үкіметтің және басқа да мемлекеттік органдар мен ұйымдардың ақпараттық оқшауланuын төмендету немесе оған жол бермеу болып табылады.

Қазақстан Республикасының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі негізгі міндеттер:

- ақпараттық қауіпсіздік саласында ұлттық заңнаманы жетілдіру;
- ақпараттық қауіпсіздік қатерлерінің көздерін анықтау, бағалау, болжау, қорғалатын объектілердің барлауға қолжетімділік өлшемдерін айқындау;
- ақпараттық қауіпсіздіктің мемлекеттік саясатын қамтамасыз етудің, іс-шаралар кешенін және оларды іске асыру әдістерін әзірлеу;
- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мемлекеттік органдар мен ұйымдардың қызметін құқықтық реттеу және үйлестіру;
- ақпараттық қауіпсіздікті қамтамасыз ету жүйесін дамыту, оны ұйымдастыруды, нысандарын, әдістерін және ақпараттық қауіпсіздік қатерлерін бейтараптау құралдарын, оны бұзу зардаптарын жоюды жетілдіру;
- Қазақстанның жаһандық ақпараттық желілер мен жүйелерді құру және пайдалану процестеріне белсенді қатысуын қамтамасыз ету;

- техникалық барлауларға қарсы іс-әрекет ету жөніндегі нормативтік құқықтық және әдістемелік базаны әзірлеу және жетілдіру жолымен техникалық барлауларға қарсы іс-қимыл жасау жүйесін құру болып табылады.

Сонымен қатар, мемлекеттің, жеке және заңды тұлғалардың қызметтері саласының әрқайсысында ақпараттық қауіпсіздікті қамтамасыз етудің өз ерекшеліктері бар, бұл ең алдымен, қойылған міндеттерді шешу ерекшелігіне, ақпараттық қауіпсіздіктің әрбір саласына тән әлсіз элементтер мен осал буындардың болуына байланысты.

Сондықтан, әрбір сала үшін арнайы жұмыстарды ұйымдастыру, оның жай-күйіне әсер ететін ерекше факторларды ескере отырып, ақпараттық қауіпсіздікті қамтамасыз ету нысандары мен тәсілдерін пайдалану талап етіледі.

Баяндалған мәліметтер негізінде мемлекет қызметінің саяси, әскери, экономикалық және басқа да салаларындағы ақпараттық қауіпсіздік саясатын қалыптастыру мен іске асырудың басым бағыттары айқындалады.

Ақпараттық қауіпсіздік саласындағы мемлекеттік саясат ақпараттық қатынастар субъектілері мүдделерінің келісілуін, қоғамдық және үкіметтік емес ұйымдардың кеңінен өкілдік етуімен мемлекеттік органдар және ұйымдардың тиімді жұмысын ұйымдастыруды көздейді.

Қазіргі уақытта Қазақстанның саяси өміріндегі және экономикасындағы болып жатқан процестері оның ақпараттық қауіпсіздігінің жай-күйіне тікелей әсерін тигізеді. Бұл ретте ақпараттық қауіпсіздіктің нақты жай-күйін бағалау және осы саладағы негізгі проблемалар мен бағыттарды айқындау кезінде ескеруді қажет ететін жаңа факторлар туындайды.

Көрсетілген факторларды саяси, экономикалық және ұйымдастырушылық-техникалық деп бөлуге болады.

Саяси факторлар:

– әлемнің түрлі өңірлерінде геосаяси жағдайдың өзгеруі;

– әлемдік саяси, экономикалық, әскери, экологиялық және басқа да процестердің жаһандық мониторингін жүзеге асыратын,

ақпаратты біртарапты артықшылықтар алу мақсатында тарататын әлемнің дамыған елдерінің ақпараттық өктемдігі;

– демократия, заңдылық, ақпараттық ашықтық, елдің қауіпсіздігін қамтамасыз ету жүйесін жетілдіру принциптері негізінде жаңа Қазақстан мемлекеттілігінің қалыптасуы;

– ішкі саяси дағдарыстардың туындауы: билік тармақтары арасындағы, аумақтық мемлекеттік құрылым субъектілері арасындағы жанжалдар, қорғалатын тұлғаларға қастандық жасалуы;

– ішкі саяси блоктардың, одақтардың, альянстардың қызметі, әлемде күштердің геосаяси орналасуына әсер ететін жаңа әскери-саяси бірлестіктердің құрылуы;

– реформалар жүргізу процесінде Қазақстанның шетелдермен неғұрлым тығыз ынтымақтастық жасауға ұмтылуы;

– терроризм және экстремизм, қылмысты жағдайдың ушығуы, әсіресе кредит-қаржы саласында компьютерлік қылмыстар санының өсуі болып табылады.

Экономикалық факторлар арасында:

Қазақстанның дүниежүзілік экономикалық кеңістікке белсенді кіруі, көптеген отандық және шетелдік мемлекеттік емес құрылымдардың – ақпаратты өндірушілер мен тұтынушылардың, ақпараттандыру және ақпаратты қорғау құралдарының пайда болуы, ақпараттық өнімнің тауарлық қатынастар жүйесіне қосылуы;

– Қазақстанның ақпараттық инфрақұрылымын дамыту мүддесінде шетелдермен кеңейіп келе жатқан кооперация;

– бүкіл әлемдегі экономикалық процестердің дамуына өспелі әсерін тигізетін коммуникациялық жаһандану;

– қазіргі әлемде экономикалық-технологиялық даму деңгейін барынша жоғары дәрежеде айқындайтын жаңа ақпараттық технологияларды дамыту мен енгізуде Қазақстанның артта қалуы неғұрлым елеулі болып табылады.

Ұйымдастырушылық-техникалық факторлар:

Ұйымдастырушылық-техникалық факторлардың ішінен мыналар айқындаушы болып табылады:

– ақпараттық қатынастар саласында, оның ішінде ақпараттық қауіпсіздікті қамтамасыз ету саласында, нормативтік құқықтық базаның жеткіліксіздігі;

– мемлекеттің Қазақстандағы ақпараттандыру құралдары, ақпараттық өнімдер мен қызмет көрсетулер нарығының жұмыс істеу және даму процестерін нашар реттеуі;

– ақпаратты сақтау, өңдеу, беру және қорғау үшін мемлекеттік басқару саласында, кредит-қаржы және басқа салаларда ақпараттың сыртқа шығып кетуінен және сыртқы әсерден қорғалмаған импорттық техникалық және бағдарламалық құралдардың кеңінен пайдаланылуы;

– ашық байланыс арналары және деректер беру жүйелері бойынша берілетін ақпараттар көлемінің өсуі.

Қазақстандағы ақпараттық қауіпсіздіктің қазіргі жай-күйін талдау оның қазіргі заманғы деңгейінің адам, қоғам және мемлекет қажеттіліктеріне сәйкес келмейтінін көрсетті.

Елдің саяси және әлеуметтік-экономикалық дамуының бүгінгі жағдайы ақпаратпен еркін алмасуды кеңейтудегі қоғам қажеттілігі мен оны таратуға жекелеген шектеулерді сақтау қажеттілігі арасында қайшылықтардың шиеленісуін тудырады.

Мемлекеттік органдарды толық, сенімді және қазіргі заманғы ақпаратпен қамтамасыз ету үшін негізделген, оның ішінде мемлекеттік ақпараттық ресурстарды қорғауға арналған шешімдер қабылдау, сондай-ақ отандық ақпаратты қорғау құралдарын және импортталатын техникалық құралдардың белгіленген талаптарға сәйкестігін растау жүйелерін әзірлеу талап етіледі.

Ақпаратты қорғау саласында кәсіби мамандар санының жеткіліксіздігі республикада ақпараттық қауіпсіздікті ұйымдастыруға кері әсерін тигізеді.

Техникалық барлауларға қарсы іс-әрекеттер, ақпараттық қарудан қорғау мен осы саладағы нормативтік құқықтық базаны жетілдіру мәселелерін одан әрі пысықтау талап етіледі.

Осы мақсаттарда ақпараттың тұтастығы мен құпиялылығын қамтамасыз ету үшін ақпаратты жалпымемлекеттік ауқымда және ведомстволық деңгейде қорғау жөніндегі іс-шараларды кешенді үйлестіру қажет.

Ақпараттық кеңістікте интернеттің рөлінің өсуімен адамның және қоғамның құқықтары мен бостандықтарын зорлық жасау мен қатыгездікті насихаттайтын ақпараттан, оларға өтірік және жалған

ақпаратты таңудан, болашақ ұрпақтың мақсатты бағытталған теріс дүниетанымын қалыптастырудан қорғау қажеттілігі туындайды. Бұл ретте, сыртқы қатер көздері Қазақстан Республикасының заңнамалық құзырынан тыс болуы мүмкін, бұл құқық шаралары жүйесін қолдануды елеулі қиындатады.

Отандық ақпараттық технологиялардың болмауы өзекті проблема болып табылады, бұл жаппай пайдаланушыларды ақпараттық қауіпсіздік талаптары бойынша сәйкес емес импорттық техниканы сатып алуға мәжбүр етеді. Бұл деректер базалары мен банктерінің ақпараттық қауіпсіздігіне қатер, сондай-ақ елдің шетелдік компьютер мен телекоммуникация техникасын және ақпарат өнімдерін өндірушілерге ықтимал тәуелділігін тудырады.

Ақпарат саласындағы құқық қатынастарының субъектілері меншік нысанына қарамастан жеке және заңды тұлғалар болып табылады.

Ақпараттың меншік иелері: мемлекет (мемлекеттік органдар мен ұйымдар, лауазымды тұлғалар тұрғысында), жеке және заңды тұлғалар болып табылады.

Ақпараттық қатынастар субъектілері ақпаратты жасау және пайдалану тұрғысынан авторлар, меншік иелері, иеленушілер немесе пайдаланушылар ретінде болуы мүмкін.

Ақпарат және ақпараттық ресурстар заттай меншік немесе зияткерлік меншік бола алады. Сондықтан ақпараттық жүйелерде ақпаратты өңдеу кезінде ақпараттың құпиялылығын қамтамасыз ету ғана емес, оның тұтастығы мен қолжетімділігін, ал электрондық құжаттар үшін әрбір электрондық құжаттың авторлығын электрондық цифрлы қолтаңбамен растау талап етіледі.

Мемлекеттік құпияларды құрайтын мәліметтерді қамтитын ақпаратқа қатысты барлық қатынас субъектілері үшін белгіленген құпиялық режимі жұмыс істейді. Осы ақпараттың меншік иесі мемлекет болып табылады.

Мемлекет меншік иесі болып табылатын қол жеткізу шектелген ақпаратты қорғауды қамтамасыз ету үшін мемлекеттік ақпаратты қорғау жүйесі жұмыс істейді.

Қазіргі заманғы қоғамының табысты жұмыс істеуі онда болып жатқан ақпараттық процестердің қаншалықты тиімді ұйымдастырылғанына және жолға қойылғанына тұтастай байланысты. Осыған байланысты Қазақстан Республикасы үшін аталған процестердің мемлекет шеңберінде ақпараттық кеңістікке бірлесуі барған сайын маңызды бола түсуде.

Бірыңғай ақпараттық кеңістік жеке және заңды тұлғалардың ақпараттық қажеттіліктерін қанағаттандыруды қамтамасыз етуге мүмкіндік береді, ақпаратты өндірушілер мен тұтынушылар қызметін ынталандыруға, елдің әлемдік ақпараттық кеңістікке кіруіне жәрдем ететін болады.

Бірыңғай ақпараттық кеңістікті қалыптастыру барысында құрылуы Қазақстан Республикасы Президентінің 2004 жылғы 10 қарашадағы N 1471 Жарлығымен бекітілген Қазақстан Республикасында «Электронды үкімет» қалыптастырудың 2005-2007 жылдарға арналған мемлекеттік бағдарламасымен көзделген «Электронды үкіметтің» рөлі өсе түсуде. «Электронды үкімет» барлық билік тармақтарының қызметін ақпараттық қолдау мен олардың арасындағы, сондай-ақ экономика субъектілерімен және халықпен арадағы ақпараттық өзара іс-қимылды серпінді ұйымдастыру есебінен олардың жұмыс істеу тиімділігін елеулі түрде көтеруге мүмкіндік береді.

Қазақстан Республикасында «Электронды үкімет» қалыптастырудың 2005-2007 жылдарға арналған мемлекеттік бағдарламасы шеңберінде «Жеке тұлғалар», «Заңды тұлғалар», «Жылжымайтын мүлік тіркелімі», «Мекенжай тіркелімі» мемлекеттік деректер базасы құрылуда, олардың қауіпсіздігі ақпараттық қатынастар субъектілері арасындағы қорғалған ақпараттық өзара іс-қимыл нәтижесінде қамтамасыз етілетін болады.

Бақылау және тест сұрақтары

1. Ұлттық қауіпсіздіктің міндеттері қандай?
2. Ұлттық қауіпсіздіктің түрлері қандай?
3. Ақпараттық қауіпсіздіктің маңызы қандай?
4. ҚР қауіпсіздігінің жай-күйіне тікелей әсерін тигізетін саяси факторлар қандай?
5. ҚР қауіпсіздігінің жай-күйіне тікелей әсерін тигізетін экономикалық факторлар қандай?
6. ҚР қауіпсіздігінің жай-күйіне тікелей әсерін тигізетін ұйымдастырушылық-техникалық факторлар қандай?
7. **Мүдделер қоғамдық дәрежесіне байланысты келесілерден тұрады:**

а) жеке, топтық, қоғамдық;
ә) табиғи немесе бағдарлама;
б) нақты және жалған;
в) үдемелі, кері тартпалы, ескішіл;
г) ұзақ мерзімді, қысқа мерзімді.

8. **Субъектінің сипатына байланысты мүдделер келесілерге бөлінеді:**

а) жеке, топтық, қоғамдық;
ә) табиғи немесе бағдарлама;
б) таптық, ұлттық, мамандық ;
в) үдемелі, кері тартпалы, ескішіл;
г) ұзақ мерзімді, қысқа мерзімді.

9. **Мемлекетпен қорғалатын оның әскери, сыртқы саяси, экономикалық т.б. жағдайлары, олардың таралуы мемлекеттің қауіпіне зиян келтірсе – бұл:**

а) коммерциялық құпия;
ә) қызметтік құпия;
б) жеке құпия;
в) мемлекеттік құпия;
г) саяси құпия.

10. **Коммерциялық құпия кімнің көмегімен қорғалып келеді?**

а) мемлекеттің;
ә) жұмыс берушінің;
б) азаматтардың;
в) жұмысшылардың;
г) саясаттың.

2. Ақпаратты қорғау

2.1. Ақпараттық қауіптер

Ақпараттық жүйелердің қауіпсіздігін қарастыру барысында авторлар қауіптерді 3 түрге бөледі:

1. Ақпараттың құпиялылығының қауіптері.
2. Ақпараттың бүтіндігінің қауіптері.
3. Қызмет көрсетуіндегі бас қауіптер.

Ақпараттық қауіпсіздік қатерлерін олардың шығу тегіне байланысты сыртқы және ішкі деп бөлуге болады. Ақпараттық қауіпсіздік қатерлерінің көздері:

1. Жекелеген шетелдік саяси, экономикалық, әскери және ақпараттық құрылымдар.
2. Шетел мемлекеттерінің барлау және арнайы қызметтері.
3. Халықаралық террористік және экстремистік ұйымдар.
4. Құрылымға қарсы бағыттағы заңсыз саяси, діни және экономикалық құрылымдар.
5. Ұйымдасқан қылмыстық қоғамдастықтар мен топтар.
6. Жекелеген жеке және заңды тұлғалар.
7. Дүлей зілзалалар және апаттар болып табылады.

Сыртқы қатерлерге:

1. Шетел мемлекеттерінің жаһандық ақпараттық мониторинг, ақпарат тарату және жаңа ақпараттық технологиялар саласындағы сындарлы емес саясаты.
2. Шетелдік барлау және арнайы қызметтердің іс-әрекеттері.
3. Халықаралық топтардың, құралымдар мен жеке тұлғалардың қылмыстық іс-әрекеттері, өнеркәсіптік және банктік шпионаж.
4. Дүлей зілзалалар және апаттар.
5. Халықаралық террористік және экстремистік ұйымдардың қызметі.

6. Шетелдік саяси және экономикалық құрылымдардың Қазақстан Республикасының мүдделеріне қарсы бағытталған қызметі жатады.

Мыналар ішкі қатерлер болып табылады:

1. Ақпарат түзу, тарату және пайдалану саласындағы саяси және экономикалық құрылымдардың заңға қарсы қызметі.

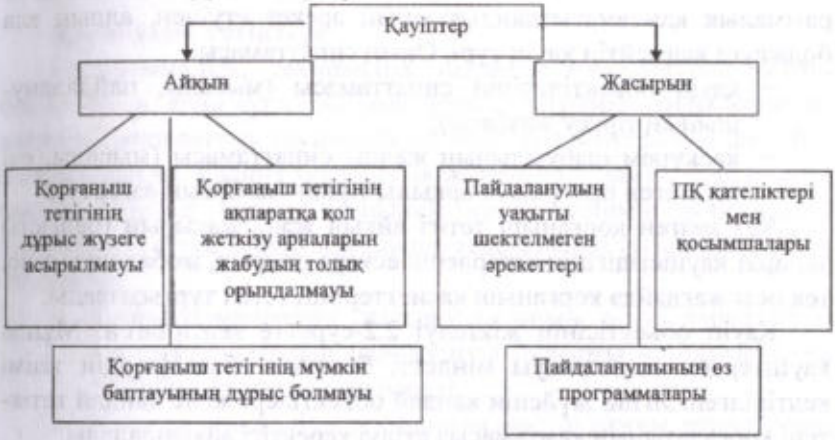
2. Жеке және заңды тұлғалардың, мемлекеттің ақпарат саласындағы заңдық құқықтары мен мүдделерін бұзуға әкелетін мемлекеттік құрылымдардың заңға қайшы іс-әрекеттері.

3. Ақпарат жинаудың, өңдеудің, сақтаудың және берудің белгіленген регламенттерін бұзу.

4. Ақпараттық жүйелер персоналының әдейі жасаған заңсыз іс-әрекеттері және әдейі жасамаған қателері.

5. Ақпараттық және телекоммуникациялық жүйелердегі техникалық құралдардың істен шығуы және бағдарламалық қамтамасыз етудің іркілістері.

Қауіптердің жүзеге асырылу әдістері бойынша жіктелуі төмендегі 2.1-суретте келтірілген.



2.1-сурет. Қауіптердің жүзеге асырылу әдістері бойынша жіктелуі

Айқын қауіптер дегеніміз қорғаныш тетігінің дұрыс жүзеге асырылмауынан болатын, баптаулардан кеткен қателерден туын-

дайтын, алдын ала болжауға келетін қауіп түрі. Қорғаныш тетігінің дұрыс жүзеге асырылмауына себептері :

- жүйелік дискіге «жазу» және жүйемен қолданбалы ортақ каталогтарға қатынас құруды басқарудың болмауы (корзина, Temp, Мои документы);
- енгізу құрылғысына «орындау» құқығына шек болмауы. Осы себепті пайдаланушылар сырткы тасымалдауыштардан кез келген программаларды жүктей алады.

Қорғаныш тетігінің мүмкін баптауларының дұрыс болмауы келесі себептерден болады: баптаудың дұрыс болмауы және баптауды орындау әдісінің дұрыс болмауы. Иерархиялық жүйеде баптауды қауіпсіздік әкімшісі, дерекқорды басқару жүйесі және қолданбалар әкімшісі, пайдаланушы және т.б. жүзеге асырады. Мысалы, әркайсысы өзіне рұқсаты бар ортада әрекет етіп баптаулар жасай алады. Ал қауіпсіздікті сақтау үшін мұның бәрі қауіпсіздік әкімшісі арқылы орындалуы керек.

Жасырын қауіптер. Жасырын қауіптер – пайдаланушының мақсатты жасалған әрекеттерінен, бұзуға бағытталған программалық қамтамасыздандыруының әрекет етуінен, алдын ала болжауға келмейтін қауіп түрі. Оның сипаттамасы:

- қауіп объектілерінің сипаттамасы (мысалы, пайдаланушының тіркеу жазбасы);
- қаскүнем шабуылының жалпы сипаттамасы (мысалы, өзі жүктеген программа арқылы тіркеу жазбасын өзгерту).

Кез келген қорғаныш тетігі айқын және жасырын (белгісіз) ақпарат қауіпсіздігінің қатерлерін ескере отырып, жобалануы тиіс, тек осы жағдайда қорғаныш қасиеттерінің тетігі тұрғызылады.

Қауіп объектісінің жіктелуі 2.2-суретте келтірілген. Мұнда қауіптерден сақталынуы міндетті болатын объектілердің тізімі келтірілген. Яғни, жүйенің қандай объектілері және қандай тетіктері қорғалатынын қамтамасыз етілуі керектігі айқындалады.

2.2-сурет. Қауіп объектілерінің жіктелуі

2.2. *Ақпараттық қауіптерге қарсы әрекет*

Қауіпсіздік тетіктері

Программалық, техникалық шаралар компьютерлік мәнін бақылайтын, яғни құрал-жабдықтарды, программаларды және деректерді, ақпараттық қауіпсіздіктің маңызды және соңғы шебі болып табылады. Қазіргі ақпараттық жүйелердің дамуы қорғанысқа көп мүмкіндік береді. Сонымен қатар, сенімді қорғанысты қамтамасыз етуге кейбір жағдайлар кедергілерді туғызады. Бұның себептері:

1. Микросхемалардың жылдамдығының өсуі, параллельді архитектуралардың пайдалануы бұрынғы қорғаныстарды онай бұзуға мүмкіндік береді.
2. Желілер мен желілік технологиялардың дамуы, арналардың тасымалдау қабілеттілігінің өсуі және ақпараттық жүйелердің арасындағы байланыстардың өсуі, қаскүнемдер санын ұлғайтады.
3. Жаңа ақпараттық сервистердің пайда болуы.

4. Программалық қамтамасыздандыруларды жасаушылар арасындағы бәсекелестік сол өнімге жұмсайтын уақытын азайту, сапасыз өнімді шығаруға мүмкіндік береді.
5. Пайдаланушыларға аппараттық және программалық құралдардың қуаттылығының өсуі сенімді тексерілген конфигурацияны ауыстыру кезінде бюджеттің тапшылығынан қауіпсіздікті төмендетеді.

Программалық техникалық деңгейде қауіпсіздік сервисі деген ұғым пайдаланады. Қазіргі ақпараттық жүйелерді жасау кезінде, объектілі бағытталған программалау технологиясы пайдаланылған қауіпсіздік сервисі 2 түрден тұрады:

1. Негізгі.
2. Қосымша.

Қауіпсіздік сервистер келесілерге бөлінеді:

1. Идентификация және аутентификация.
2. Қатынас құруды басқару.
3. Хаттамалау және аудит.
4. Шифрлау.
5. Бүтіндікті тексеру.
6. Экрандау.
7. Қорғалғанды таңдау.
8. Бас тарту тұрақтылығын қамтамасыз ету.
9. Қауіпсіз қалпына келтіруді қамтамасыз ету.
10. Туннельдеу.
11. Басқару.

Қауіпсіздік сервистерді талдау барысында олардың қандай шараларды орындауға бағытталғанын ажыратуға болады. Жалпы қауіпсіздік шаралар келесіге бөлінеді:

1. Алдын алу шаралары.
2. Бұрмалаушылық.
3. Бұзушылықтың аумағын кішірейту шаралары.
4. Бұзушыны табу шаралары.
5. Қауіпсіздік режимді қалпына келтіру шаралары.

Қауіпсіздік жағынан қарағанда қазіргі ақпараттық жүйелердің ерекшеліктері келесідей:

1. Корпоративтік желілердің бөліктерінің әр жерде әр аймақта орналасуы.
2. Корпоративтік желінің Intranetke қосылу нүктесінің бар болуы.
3. Қолданушылардың компьютерлік сервиске қол жеткізуіне компьютерлермен қатар басқа да тұтынушы құрал жабдықтардың пайдалануы.

Компьютерлік жүйеде элементтер объектілер мен субъктілерге бөлінеді. Субъект белсенді элемент болып табылады және әр субъект бір компьютердің ішіндегі объектілермен қарым-қатынас жасай алады. Осы әр компонентке қатынас жасау монитор деп аталады. Осы монитор арқылы барлық жергілікті қатынас құру бақыланады. Компоненттерді байланыстыратын коммуникациялық арналар тасымалданған ақпараттың бүтіндігін және құпиялылығын сақтайды. Сонда барлық мониторлардың жиыны желілік конфигурацияның бірегей мониторын қалыптастырады. Бұл компьютерлік жүйелерде негізгі тұжырымдама болып саналады. Осы тұжырымдама арқылы келесі үш принципті ажыратуға болады.

1. Өмірге, бірегей қауіпсіздік саясатты қалыптастыру және оны іске асыру қажеттілігі.
2. Желі арқылы әрекеттестік жағдайға деректердің құпиялылығы мен бүтіндігін қамтамасыз етудің қажеттілігі.
3. Маңыздылығына қарай құрамдас сервистердің қалыптастыру қажеттілігі.

Осы принциптерді іске асыру барысында қорғаныстың толық қамтамасыздандыруын пайдалануға болады. Егерде қорғаныс шаралар жеткіліксіз болатын болса, онда қосымша сервистерді пайдалану қажет. Осы қосымша сервистер экрандау сервистері деп аталады. Практикалық жағынан қауіпсіздік архитектурасының келесі принциптері маңызды болып саналады:

1. Кеңістік пен уақыт ішінде қорғаныстың үздіксіздігі.
2. Белгілі сенімді тексерілген стандарттарға жүгіну.
3. Ақпараттық жүйенің иерархиялық түрде ұйымдастырылуы.
4. Осал буынды күшейту.
5. Қауіпті жағдайға өтуге мүмкіндік бермеу.
6. Басымшылықтарды төмендету.

7. Міндеттерді бөліп беру.
8. Қорғанысты көп деңгей түрінде ұйымдастыру.
9. Әр түрлі қорғаныс құралдарды пайдалану.
10. Ақпараттық жүйенің қарапайымдылығы және басқарылуы.

Ақпараттық жүйеге қол жеткізуді ұйымдастыру барысында қауіпсіздік архитектураның келесі принциптерін ұстау қажет:

1. Конфигурацияға артықшылықты енгізу.
2. Төтенше жағдайларды табуға және болдырмауға қолданылатын құралдардың болуы.
3. Шабуылға тап болған компоненттерді ауыстыруға, шоғырландыруға, оқшаулауға және қалпына келтіруге құралдардың болуы.
4. Желілік басқарудың бөлінуі.
5. Желіде ішкі жүйелердің топтастырылуы және қолданушылар топтарды өзара бөлу.

Әкімшілік ету – жүйе қорларына қатынас құруды басқару процесі. Бұл процесс келесілерді қамтиды:

1. Субъектінің идентификаторын құрастыру.
2. Субъектінің аутентификациясына пайдаланатын деректерді басқару.
3. Субъектінің жүйе қорларына қатынас құру құықтарын басқару.

Идентификация – пайдалануышының атын енгізу арқылы жүйедегі қорларға рұқсат алу тәртібі (процедурасы). Егер енгізілген пайдаланушының аты жүйеде бар болса, онда оның жүйедегі қорларға қатынас құру құқықтары анықталады.

Идентификация технологияларының келесі түрлерін ажыратуға болады:

1. Штрих кодтық идентификациялау.
2. Радиожиілік идентификациялау.
3. Биометриялық идентификациялау.
4. Магнитті жолақы бар карталар арқылы идентификациялау.

Аутентификация – идентификация рәсімін (процедурасын) бақылауға арналған, яғни өзін идентификациялаушы пайдаланушының шынайылығы тексеріледі. Егер жүйеге кірмекші болған пайдаланушының нағыз өзі болса, онда аутентификация

процедурасы орындалды деп түсіну керек, ал қарсы жағдайда аутентификация кері қайтарылып, жүйенің қауіпсіздік саясаты іске қосылады. Мысалы, пайдаланушы құпия сөзі бірнеше рет қате терілсе, жүйеге бұғалық салынады. Идентификация және аутентификация процедураларының қатар орындалуын авторизация деп айтады.

Аутентификация технологияларының келесі түрлерін ажыратуға болады:

1. Көп парольдік аутентификация.
2. Сервер.
3. Сервермен клиент екеуінің арасындағы байланыс.

Алыс қашықтықта аутентификацияны жүргізу үшін арнайы хаттамалар пайдаланылады.

Соның ішінде радиус хаттамасын қарастырайық. Радиус хаттамада келесі модульдерді ажыратуға болады:

1. «Клиент-радиус» – қолданушылардың аутентификацияға сұраныстарды қабылдайды. Барлық қабылданған сұраныстарды сервер радиусқа аутентификацияға және авторизацияға жібереді.

2. «Сервер-радиус» – бұл жерде бірнеше клиенттердің аутентификациясы мен авторизациясы орындалады. Әр серверде әр түрлі базалар пайдаланылады.

3. «Делдал-радиус» – сервермен клиенттер арасындағы әрекеттестік арнайы хабарлар арқылы жүргізіледі. Бұл жерде делдал ретінде арнайы желілік құрылғы пайдаланады. Бұл құрылғының міндеті хабарды серверге беру.

Қауіпсіздік саясаты – ақпаратты қалай өңдейтінін, қорғайтынын, тарататынын анықтайтын заңдар, ережелер, тәртіп нормалар жиынтығы, ол мүмкін болатын қауіптерге алдын ала тосқауыл қояды. Қалыптасқан қауіпсіздік саясатына байланысты жүйенің қауіпсіздігін қамтамасыз ететін нақты тетіктерді таңдауға болады. Қауіпсіздік саясаты арқылы мүмкін болатын қатерлер мен қарсы тұру шараларын талдаудан тұратын қорғаныштың белсенді сыңары.

Аудит – жүйеде болып жатқан барлық оқиғаларды тіркеу тәртібі (процедурасы). Оның параметрлері келесідей болуы мүмкін: объектіге қатынас құру күні, уақыты, қатынас құрушы субъектінің идентификаторы, құпиясөзі және т.б.

Бақылау сұрақтары

1. Қауіптердің жүзеге асырылу әдістері бойынша қалай жіктеледі?
2. Қауіп объектілері қалай жіктеледі?
3. Идентификация деген не?
4. Аутентификация деген не ?
5. Қауіпсіздік саясаты деген не?
6. Аудит деген не?
7. Биометриялық деректерге не жатады?
8. Құпиясөздер саясатын баптау жайлы не білесіз?

3. Қорғаныштың программалық әдістері

3.1. Автоматтандырылған жүйе қауіпсіздігі

Автоматтандырылған жүйе компоненттері: аппараттық құралдар, программалық қамтамасыздандырулар, өңделетін ақпарат, байланыс арнасы, персонал мен құжатнама болғандықтан автоматтандырылған жүйеге келтірілетін қауіп-қатер өте ауқымды ұғым. Әлемдік практика бойынша: ақпарат құны оның жоғалуынан, сондай-ақ оны қалпына келтіргендегі шығындардың шамасына тең.

Автоматтандырылған жүйе қауіпсіздігін келесі 3 топқа бөліп қарастырады:

1. Автоматтандырылған жүйе сыңарларының физикалық қауіпсіздігін қамтамасыз ету. Мұнда табиғи апаттардан, ұрлықтан, нұқсан келтіруден сақтау.

2. Автоматтандырылған жүйе сыңарларының логикалық қауіпсіздігін қамтамасыз ету. Мұнда рұқсатсыз қатынас құрудан қорғау, пайдаланушылар мен программаның мақсатты/мақсатсыз қателерінен қорғау.

3. Автоматтандырылған жүйенің әлеуметтік қауіпсіздігінің мәселесі. Мұнда автоматтандырылған жүйе пайдалануды реттейтін және қауіпсіздікті бұзуды зерттеу мен жазаға тартуды анықтайтын заң шығару тетігін құру қаралады.

Барлық қатерлерді мыналардың біріне жатқызуға болады:

Үзу – жүйе компонентінің жоғалуы, қол жеткізерліксіз (бұғат) немесе жұмыс істеу мүмкіндіктерін жоғалту.

Ұстап қалу – қаскүнем автоматтандырылған жүйеге қол жеткізеді, соның нәтижесінде деректер мен программааларды заңсыз көшіру, компьютер торабының байланыс желісінен деректерді рұқсатсыз оқу.

Өзгерту – қаскүнем жүйеге қол жеткізіп қана қоймай, оны басқарады.

Жасандылық – қасқүнем жүйемен қарастырылмаған өзіне керекті әрекеттерді орындау үшін жасанды процесті жүйеге ендіреді немесе жүйеге файлдар және пайдаланушылар файлына жазбалар жасайды.

Автоматтандырылған жүйедегі ақпаратты қорғауға келесі негізгі мәселелерді шешуді қамтамасыз ететін әдістер мен құралдардың, шаралардың жиынын жатқызады:

1. Ақпараттың тұтастығын тексеру;
2. Автоматтандырылған жүйе қорларына және онда сақталатын деректер мен программаларға рұқсатсыз қатынас құруды болдырмау.
3. Автоматтандырылған жүйеде сақталған программалардың рұқсатсыз пайдаланылуын болдырмау (яғни, көшірмелеуден қорғану).

3.2. *Көшірмелеуден қорғаныш әдістері*

Кодтаудан қорғаныш жүйесі немесе авторлық құқықтарды қорғау жүйесі деп программалық өнімді заңсыз анықтау, пайдалану немесе өзгертуді қиындататын, не тыйым салуды қамтамасыз ететін программалық немесе программа-аппараттық шешімдердің кешенін айтады.

Көшірмелеу арқылы қорғаныш жүйесінің сенімділігін арттыру үшін қойылатын талаптар:

1. Дискілердің автоматты көшіргіштермен көшірмеленбеуі (көшіруді орындау үшін дискінің құрылымын физикалық меңгеру керек).
2. Түзеткіш көмегімен программа жұмысының логикасын меңгерудің мүмкін болмауы. Ол үшін программаға код салу немесе аппараттың түзеткішінің панелін қажет ету;
3. Қорғалған программаның немесе оның ең маңызды үзінділерін дизассемблерлеудің мүмкін болмауы. Кері ассемблерлеу үшін арнайы программаны жазу керек болады;

4. Стандарт құралдар көмегімен маңызды үзулерді орындаудың мүмкін болмауы. Ондайда программа «сыртқы әлеммен» байланыста болмайды, (яғни дискімен, DOS-пен және сыртқы программалармен). Жүйе жұмыс істеу кезінде программаны рұқсатсыз пайдалануға тыйым салады.
5. Программалардың дұрыс жұмыс істеуін тексеру үшін әр түрлі тәсілдер пайдаланылады, соның ішінде «бақылау қосындысын» мерзім аралығында тексеру. Сенімділікті арттыру үшін жалпы бақылау қосындысы жеке блок, жеке қатар, берілген программаға жүргізіледі. Сондай-ақ, бақылау қосындысын алу жолын құпия ұстау қажет.
6. Жүйедегі маңызды программаларды мерзім аралығында жаңарту. Сондай-ақ, программаны жаңарту командасы ерекше қорғанылған басқарушы программалар арқылы жүзеге асырылуы тиіс.
7. Программаға және оның жеке блоктарына қатынас жасаудың бірнеше бейстандарт (ложные точки входа) кіріс нүктелерін ұйымдастыру. Ол жасырын болады және жиі өзгертілуі тиіс.
8. Программалардың көшірмелерін сақтау. Пайдалану алдында программаның қорғалған көшірмесімен салыстыру.
9. Программаға криптографиялық әдістерін қолдану.

Ең тиімді әдіс – модульдік диалог әдісі. Қандай да бір жасырын процедуралар қарастырылады. Мысалы, берілген кодтың қайбір жұп разрядтарын екілік модуль бойынша қосу. Мұндай процедуралардың командалары шифрланып, жасырын күйінде модульдің белгілі бір қатарында сақталады. Сонда модуль мазмұнның функциясы болып табылатын қандай да бір код анықталады. Мысалы, модуль процедураларынан белгілі ретпен тандалынған разрядтар жиынтығы. Ақпараттық жүйелердің жеке параметрлерін танып білу құрылымын меңгеру мүмкіндігін қиындату. Мысалы, апппараттық кілттерді пайдаланғанда – оларды ашу кезінде өздерінің жұмысы жайлы маңызды ақпарат бермеуі тиіс.

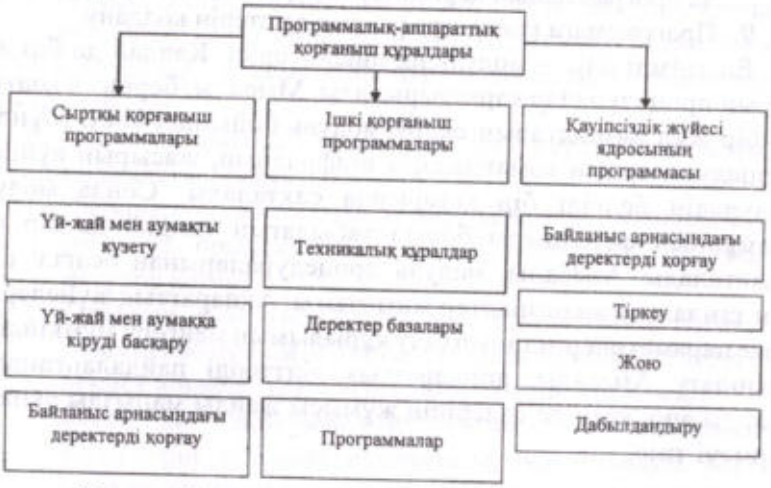
3.3. *Ақпарат қорғанышының программалық құралдары*

Программалық-аппараттық қорғаныш құралдары қазіргі кездегі автоматтандырылған жүйенің маңызды бөлігі болып саналады. Ол келесі артықшылықтармен ерекшеленеді: әмбебаптылығы, икемділігі, қарапайым түрде жүзеге асырылуы, сенімділігі, өзгерту мен дамыту мүмкіндігі. Кемшіліктері: санауыш жұмыс уақытын және оперативті жады көлемін қажет етеді. Программалық-аппараттық қорғаныш құралдары ішкі және сыртқы құралдар болып бөлінеді (3.1-сурет).

Программалық-аппараттық қорғаныш құралдарын жасауға қойылатын талаптар:

1. Функционалдық толықтық.
2. Икемділік.
3. Пайдалануды үйлестіру (унификация).

Программаларды қорғау программалары. Программистердің білімінің жеткіліксіздігінен, программалау, тестілеу, түзету құралдары мен технологияларына байланысты программалар да мүлтіксіз бола бермейді. Ол ақпаратқа рұқсатсыз қатынас құрудың көзі болады.



3.1-сурет. Программалық-аппараттық қорғаныш құралдары

Программаларды қорғау шаралары:

1. Әрбір құрылған программа үшін рұқсат етілген функциялар тізімін анықтау.
2. Программалау тілін таңдағанда рұқсатсыз әрекеттерді мейлінше аз орындалатын орташа таңдау.
3. Программаны құру және пайдалану кезінде рұқсатсыз өзгертулерді болдырмау.

Бұл код жадының қорғалған өрісінде сақталады. Сонда модульге қатынас жасағанда қосымша (приложение) қатынастың рұқсатын, программалық айырбасталмауын, рұқсатсыз өзгертілмегендігін тексереді. Қорғанышты арттыру үшін бақылау процедуралары мен бақылау кодтары бір мерзім ішінде өзгертіледі.

Бақылау және тест сұрақтары

1. Автоматтандырылған жүйе қауіпсіздігінің топтары.
2. Ақпаратқа төнетін қатерлерді қалай жіктеуге болады?
3. Ақпараттық қорғаныштың программалық құралдары қандай?
4. Программалық-ақпараттық қорғаныш құралдарына қойылатын талаптарды атаңыз?
5. Программаларды қорғаудың қандай шаралары бар?
6. Программаны көшірмелеуден қандай қорғаныш бар?
7. Көшірмелеуден қорғаныш жүйесінің сенімділігін арттыру үшін қандай талаптар қойылады?
8. **Жүйеде жұмыс істегенде ұйымдық шегерімдерді елемеу қандай қатерге жатады?**

а) жоспарланбаған жасанды; в) жасанды;
ә) жоспарланған жасанды; г) аралас.
б) табиғи;

9. **Тыңдау құрылғылары, дистанционды фото және бейнетаспаға (видеоға) түсіру т.б. қатердің қандай түріне жатады?**

а) жоспарланбаған жасанды; в) жасанды;
ә) жоспарланған жасанды; г) аралас.
б) табиғи;

10. **Ақпаратты тасымалдаушыларды санкциясыз көшіру қатердің қай түріне жатады?**

а) жоспарланбаған жасанды; в) жасанды;
ә) жоспарланған жасанды; г) аралас.
б) табиғи;

4. Ақпараттық жүйелердің аппаратық және программалық платформасын талдау

4.1. Жалпы сипаттамалар

Ақпаратты қорғаудың барлық әдістерін мамандар үш топқа бөледі:

1. *Заң шығарушылық.*
2. *Әкімшілікті.*
3. *Техникалық.*

Заң шығарушылық әдістер қорғауға алынған мәліметке кімнің және қай формада рұқсат алуын және белгіленген тәртіпті бұзғанына байланысты жауапкершілікті анықтайды. Мысалы, ерте заманның көп ұлттарында мистерий деп аталатын сенетін құпия діндері болған. Мистерийге ерекше істер жасап, мойындалған адамдарды ғана кіргізген болатын. Мистерийдің бар мазмұны міндетті түрде құпияда сақталуы қажет болды. Ал мистерийдің құпияларын ашқанды қуғынға, тіпті кейбір жағдайда өлімге де жазалаған. Сонымен қатар мистерийге рұқсатсыз қатысқаны үшін де өлімге кесілген болатын. Қазіргі таңда мемлекеттік құпияларды сақтау және авторлық құқық заңдары, жеке хат алмасуды құпиялы жүргізуге құқықтар белгіленген құжаттар сияқтылар бар. Бұл заңдар құпиялы ақпаратқа кімнің және қандай жағдайларда рұқсат ала алатынын ашып көрсетеді. Алайда заң шығарушы әдістер белгіленген ережелердің орындалуына кепілдік бере алмайды, олар тек ережелерді және оларды бұзған жағдайдағы жауапкершіліктерді жариялайды.

Мысалы, ҚР Ұлттық қауіпсіздік туралы заңының 7-бабында ұлттық қауіпсіздікті қамтамасыз ету жүйесінің негізгі міндеттері келтіріледі:

1) ұлттық қауіпсіздікке төнетін қауіп-қатерді болжау және анықтау;

2) ұлттық қауіпсіздікке төнетін қауіп-қатердің алдын алу мен оны зарарсыздандыру жөніндегі жедел және ұзақ мерзімді шаралар кешенін әзірлеп, жүзеге асыру;
3) ұлттық қауіпсіздікті қамтамасыз етуші күштерді құрып, әзірлікте ұстау;
4) Қазақстан Республикасының халықаралық шарттарына сәйкес жалпыға бірдей және аймақтық қауіпсіздікті қамтамасыз етуге қатысу болып табылады.

Әкімшілік әдістер қорғалатын ақпаратқа рұқсат алу процедураларын анықтамауға және оның қатал орындалуына негізделген. Бекітілген тәртіптің орындалуын қадағалау арнайы дайындалған персоналға жүктеледі. Әкімшілік әдістер көптеген ғасырлар бойы қолданылып, әрқашан дұрыс оймен басқарылып келді. Кездейсоқ адамның қолына маңызды құжат түспеу үшін оларды күзететін орында сақтау қажет. Құпиялы құжаттың орнын ауыстыру кезінде оны сеніммен берілген құпия үшін өз өмірін қиюға әзір адамнан беріп жіберіп отырған. Кітапханадан белгісіз жағдайда кітаптар жоғалмау үшін кітапхана қорына рұқсат етілу бойынша жүргізілетін есепті жүргізіп отыруы тиіс. Қазіргі кездегі ақпаратты қорғаудың әкімшілік әдістері алуан түрлі. Мысалы, мемлекеттік құпиясы бар құжаттармен жұмыс істеу үшін алдымен осы құпия құжаттарға рұқсат жасау қажет. Құжатты алған жағдайда және оларды қоймаға қайтарғанда тіркеу журналына сәйкес жазбалар жазады. Құжаттармен жұмыс арнаулы жабдықталған және сертификатталған орында жүргізіледі. Кез келген сатыда сақталудағы құжаттың құпиялылығы мен бүтінділігіне жауапты адам белгілі болады. Ақпаратқа рұқсат берудегі ұқсас процедуралар әр түрлі ұйымдарда бар. Мысалы, қауіпсіздік саясатының элементі ретінде ұйым аумағынан ақпарат тасымалдаудың (қағаз, магнитті, оптикалық түрінде) кіріп шығуын бақылауды алуға болады. Қорғаудың әкімшілік әдістерін көбінесе заң шығарушымен қосып, рұқсат беру процедураларын бұзу әрекетін жасағаны үшін жауапкершілікті бекітеді.

4.2. *Қорғаудың техникалық әдістері*

Қорғаудың техникалық әдістері заң шығарушы және әкімшілікке қарағанда адам факторынан ең жоғары шамада (максималды) арылуға бағытталған. Шынына келгенде, заңды сақтау адамның жеке мінезі мен жаза алдындағы қорқынышынан болады. Әкімшілік шаралардың сақталуын адамдар бақылайды, ал оларды алдау, сатып алу немесе қорқыту әбден мүмкін. Осыдан нақты белгіленген ережелерді орындамауға болады. Ал қорғаудың техникалық әдісін қолданған жағдайда әлеуетті (потенциалды) қарсылас алдына кейбір техникалық есеп қойылады, ақпаратқа рұқсат алу үшін оған осы есепті шығару керек. Оның үстіне заңды қолданушы үшін оңайлана түскен, яғни күрделі есептерді шығармай-ақ ақпарат берудің жолы жасалуы тиіс. Қорғаудың техникалық әдістерін кітап сақталған сандықтағы құлыпты және заңсыз қолдануға әрекет жасағанда өзін жоюшы ақпарат тасымалдаушысын да айтуға болады. Алайда шындап айтқанда мұндай тасымалдаушылар шынайы өмірге қарағанда шытырман фильмдерде жиі кездеседі.

Техникалық әдіс қорғаудың барлық түрлерінің арасында алуан түрлілікке ие. Сондықтан бұл дәрісте ақпаратты қорғаудың сандық формада берілген техникалық әдістерді қарастыруға арналған.

Ақпаратты қорғаудың техникалық әдісі ежелден өңделіп келеді. Мысалы, б.з.д. V-IV ғ. Грецияда шифрлайтын құрылғылар қолданылған. Ежелгі грек тарихшысы Плутархтың айтуы бойынша, шифрлайтын құрылғы «сцитал» деп аталатын жуандығы бірдей екі таяқтан тұрған. Олар құпия ақпаратпен алмасқысы келген екі абоненттің қолында болған. Сциталға спираль бойынша орын тастамай папирустың жіңішке жолағы айналдырылып, осы қалыпта жазбалар жазылды. Одан кейін папирустың жолағын шешіп алып екінші абонентке жөнелтті. Ал ол өз кезегінде оны өзінің сциталына айналдырып, мәліметті оқуға мүмкіндік алады. Бұл шифрлайтын құрылғыда құпиялылықты қамтамасыз ететін элемент ретінде сциталдың диаметрін алған.

Қорғаудың техникалық әдістерімен бірге оларды бұзу әдістері жасалып отырды. Мысалы, ежелгі грек философы Аристотель шифрланған мәліметі бар лентаны ұзын конусқа орауды қолдануды ұсынды. Оның бір жерінде мәліметтің бөліктері көріне бастайды, ал бұл сциталдың диаметрін анықтап, содан барлық мәліметті толық түсінуге мүмкіндік береді.

Ақпараттық қауіпсіздікке сәйкес қорғаудың техникалық әдістері осы проблеманың барлық міндеттерді шешуді қамтамасыз етуге арналған. Бұл міндеттерді шешу әдістерін шартты түрде бұзуға төзімділігінің математикалық негіздеуі бар және онысы жоқ деп екіге бөлуге болады.

Беріктілігінің математикалық негіздеуі жоқ әдістерді «қара жәшік», яғни кіруіне берілімдер түсетін, ал шығуында нәтиже алынатын кейбір құрылғы ретінде қарастырған жөн. «Қара жәшіктің» ішінде жүіп жатқан барлық процестер қоданушыға да, әлеуетті (потенциалды) қарсыласқа да түсініксіз және белгісіз болып қала береді.Негізінде мұндай әдістердің беріктілігі «жәшік» ешуақытта ашылмайды және ішкі құрылғысы талдауға түспейді деген болжамға негізделген. Алайда шынайы өмірде әр түрлі жағдай болып тұрады. Сондықтан кейде «қара жәшіктің» ашылып қалуы немесе тайынбайтын зерттеуші жәшікті ашпай-ақ оның жұмыс жасау алгоритмін шешуі мүмкін. Осы жағдайда қорғау жүйесінің беріктілігі нөлге тең. «Қара жәшік» принципімен жұмыс жасайтын қорғау әдісін Security Through Obscurity (белгісіздік көмегімен қауіпсіздік) деп атайды.

Беріктіліктің математикалық негіздеуі бар қорғаудың әдісінің ерекшелігі – ішкі құрылымы ашық деген болжам арқылы олардың сенімділігі бағалануында. Яғни, қорғауды қамтамасыздандыру үшін қолданылатын барлық алгоритмдер мен хаттама әлеуетті қарсыласқа белгілі деп есептелінеді. Оған қарамастан қарсылас қорғау құралдарын өте алмайды, өйткені қорғауды жасау кезінде тиімді шешімі болмаған математикалық мәселені шешу керек. Алайда біраз уақыт өткеннен кейін математикалық мәселені шешуге бағытталған алгоритм жасалуы мүмкін, ол оның беріктілігінің төмендеуіне әкеліп соғады. Беріктіліктің математикалық негіздеуі бар әдістердің көбісі криптографияның (шартты белгілермен жазылған құпия жазу) әдістеріне жатады.

Енді ақпараттық қауіпсіздіктің негізгі міндеттерін шешуде қолданылатын қорғаудың әдістерін қарастырамыз.

4.3. *Ақпараттық қауіпсіздік есептерін шешу әдістері*

Құпиялылықты қамтамасыз ету үшін көп жағдайда криптография әдістері қолданылады. Кілттің құпиялылығын қамтамасыз ету шартымен шифрлаудың қазіргі алгоритмдері үкіметтік агенттіктер сияқты қарсыластардан да қорғауға мүмкіндік береді.Алайда белгілі бір берілімдер құпиялылығы тек тыйым салынған әрекеттер жасағанда ғана қамтамасыз етіледі, ал қалған жағдайда берілімдерге рұқсат ашық болуы тиіс болатын жағдайлар кездеседі.

DVD дискілердегі ақпараттарды қорғау.

Кинофильмдері бар DVD дискілер белгілі аймақтар (региондар) (Солтүстік Америка, Еуропа т.б) үшін жазылуы мүмкін және олар ешбір қиыншылықсыз осы аймақтың аудио-бейне мәліметтерді өңдеуге арналған құралдар арқылы ойналуы керек. Бірақ АҚШ-та сатып алынған диск Еуропада сатып алынған DVD бейне мәліметтерді өңдеуге арналған құралдар арқылы орындалмауы тиіс. Дегенмен, DVD дискідегі деректер шифрланған болып, белгілі бір DVD пластинка ойнатқыш (проигрыватель) оны ойнай алатын болса, диск мәліметінің мәнін түсіну үшін дискі мен проигрывательде қажетті ақпарат бар екені ішкі түйсік (интуитивті) арқылы түсінікті болады. Бұдан шифрлау кілті жүйеде бар екендігі және DVD пластинка ойнатқыш (проигрыватель) жасайтын істі қайталайтын болсақ дискінің шифрын ашуға болады деген шешімге келеміз. DVD дискілер үшін әзір қорғау есебі тиімді шешілмегендігін айтып өткен жөн.

Деректерді байланыс арналар арқылы бергенде пайда болатын қателер немесе ақпарат тасымалдаушыларды оқу кезінде өзгерістер салдарынан шығатын тұтастықтың бұзылуынан қорғалатын ақпаратқа артықшылықтарды қосу жолы арқылы күресуге болады. Ол үшін код арқылы кедергіге төтеп беру теориясы бар. Қазіргі архиваторлардың көбісінде ашылған файлдың тұтастығын бақылау үшін CRC-32 (Cyclic Redundant Code) алгоритмі қолданылады.

Файлды архивтеу алдында CRC-32 мәні анықталады да, ол архивте тығыздалған деректермен бірге сақталады. Ашылғаннан кейін CRC-32 мәні қайтадан есептелінеді, егер есептелінген мән архивте сақталғаннан басқа болса, файл ақауланған деп есептелінеді.

Көбінесе идентификация кезінде онша қиыншылық болмайды, өйткені қолданушы өз идентификаторын көрсетеді, ал жүйе оны қабылдайды. Идентификатор ретінде пернетақтадан енгізілген қолданушы аты, пластикалық картаның магниттік жолағындағы немесе смарт-картаның жадысындағы ақпарат немесе белгілі бір биометриялық көрсеткіш, яғни қолдың формасы, саусақ ізі (отпечатогы), дауыс т.б бола алады. Бірақ әрқашан идентификациядан кейін аутентификация жүреді, өйткені биометриялықтан басқа идентификаторлар тек иесі беретініне кепілдік бере алмайды.

Аутентификацияның мәні келесіде: идентификаторын көрсеткен қолданушы тек оған белгілі құпия ақпаратты енгізеді, ол өз кезегінде кейбір түрлендіруден өтіп тексеруші жаққа беріледі. Ол пароль, немесе PIN – код (Personal Identification Number, персоналды идентификация нөмірі) тексеруші жақ өзінде бар ақпарат негізінде қолданушының шынайылығын, яғни дұрыс екені туралы шешім қабылдайды.

Идентификацияның есептерін дұрыс шығару және одан кейінгі аутентификация бірнеше ішкі есептерді шығаруды қосады.

Идентификация мен аутентификацияның дәл қайталануының мүмкін еместігін қамтамасыз ету желілік трафикті ұстап алу және дұрыс жауапты қайта жіберу арқылы жүзеге асады. Ол үшін сауал/жауап (challenge/response) жүйесі қолданылады.

Өзін жоятын DVD - дискілер

Walt Disney компаниясы 2003 жылдың тамызында нарыққа өзін жоятын DVD - дискілер партиясының шыққанын жариялады. Мұндай дискілерді қорабын ашқаннан 48 сағат бойы ғана қолдануға болады. Одан кейін дискінің беті DVD проигрыватель арқылы лазерлік сәулелер өтпейтіндей қарайып кетуі керек.

Windows 95/98-дегі желілік қосылуының аутентификациясы

1999 жылдың 5 қаңтарында LOpht компаниясы Windows 95/98-дің желілік қорын қосу кезінде сауал жауап жүйесін таратуда кемшіліктер табылғаны туралы мақала жариялады. Windows 95/98-

ді қосуға әрекет жасағанда 15 минут бойы бір сұрауды шақыра береді, ал бұл қарсыластың осы уақыттың ішінде аутентификациясын ұстап алуға үлгерген желілік қорға сол қолданушы атынан қосылуы мүмкін.

LAN (жергілікті есептеуіш желі) MAN (ауқымды есептеуіш желі) – аутентификациясы үшін парольдердің хэштері

Windows NT/2000 сияқты операциялық жүйелерде пароль хэштерінің екі нұсқасы сақталуы мүмкін. Бір нұсқасы Windows NT-нің өз қауіпсіздік құралдарымен қолданылса, Екінші түрі Windows 95/98-де қолданылатын LAN MAN аутентификациясының протоколымен сәйкес келуін қамтамасыз ету үшін керек.

Ұзындығы 14 символдан аспайтын LAN MAN паролінің хэшін есептеу үшін 7 символы бар 2 бөлікке бөледі және әр бөлікке хэш бөлек есептелінеді. Бұдан пароль таңдау кезінде тексеретін сөздердің ең жоғары шамадағы ұзындығы 7 символ болады, бұл парольдің барлық нұсқасын қарап шығуға мүмкіндік береді.

Егер пароль 7 символдан ұзын емес болса, онда екінші бөлік бос қалып, әрқашан хэштің бір мәнін туғызады. Бұл хэштің екінші жартысы бойынша 8 символдан қысқа парольдарды тез анықтауға мүмкіндік береді.

Хэшті есептеу алдында парольдің барлық әріптері бас әріпке ауыстырылады, бұл мүмкін болатын комбинациялар шамамен 4 немесе 9 есе қысқарады.

LAN MAN хэші бойынша пароль таңдалғаннан кейін, егер NT паролінің ұзындығы 14 символдан аспаса, ол парольді қысқа мерзімде табуға болады. Ол үшін 2^{14} вариация (түрлендірме) әріптер қажет, яғни ол 16384 комбинациялы болады.

Бірінші жақ (заңды қолданушыға рұқсат бермеу) және екінші жақ (құқылы емес қолданушыға рұқсат беру) қателер ықтималдығын азайту керек. Идентификация мен аутентификация үшін биометриканы қолдану кезінде бірінші және екінші жақтың қателері айтарлықтай рөл атқарады, өйткені биометрика өлшенген биофизикалық сипаттаманы алдын ала сақталған мәнімен сәйкестік дәрежесін бағалағанда статистикалық әдіске сүйенеді. Верификаторды (тексеру) орындау кезінде сәйкестік дәлдігіне деген талаптарды жеңілдетсе, жасырын түрде қолданушыға жүйеге

кіру оңай болады. Ал егер сәйкестік дәлдігіне деген талаптарды жоғарылататын болсақ, ресми қолданушылар жиі рұқсат алмай қалулары мүмкін. Жақсы орнатылған идентификация жүйесі саусақ ізі бойынша 50 жағдайдың бірінде кіруге рұқсат бермейді де миллиард ішінен бір жасырын қолданушыны қателесіп, өткізіп алады.

Идентификацияның биометрикалық жүйесінің плюстары мен минустары.

Ең алдымен биометрикалық жүйенің артықшылығы ретінде биометриканың пароль немесе смат-карта сияқты құрылғыларды емес, адамды аутентификация етуін айтуға болады. Оның үстіне биометрикалық идентификаторды қолданушы ұмытып қалуы, жоғалтуы немесе басқа адамға беруі мүмкін емес.

Шындап келгенде биометрикалық жүйелер әзірге айтарлықтай қымбат болып келеді және олардың дәлдігі адамның психофизикалық қалпына тәуелді болады. Биометрикалық жүйенің тағы бір кемшілігі – егер біреу қолданушының дауысын, саусақ ізін жасап үйренсе бұл идентификатор иесі оны өзгертуге ешқандай мүмкіндік болмайды.

Рұқсат етуге шек қоюдың екі негізгі моделі бар: *мандатты* және *дискрецонды*. *Мандатты рұқсат алу* деп компьютерлік қорлар құпия (конфиденциалдық) деңгейге сәйкес топтарға бөлінуін айтамыз. Әр қорға оған бекітілген деңгейді көрсететін жіктеуші таңба беріледі. Осыған сәйкес қолданушы құқығынан жоғары емес деңгейдегі берілімдерге ғана рұқсат беріледі.

Рұқсат берудің *дискрецондық басқаруы* дегеніміз – қолданушының немесе қолданушы кіретін топтың құқылық есебіне негізделген компьютерлік қорға рұқсат беруге шек қою әдісі. Бұл модельді қолдану әр қолданушыға рұқсат берілетін қорлар тізімін жасауға мүмкіндік береді.

Қазіргі кезде кез келген салада сертификация міндеттері кездеседі, ал бұл есептерді шешу үшін ашық кілтті криптография қолданылады. Нақтылайтын жақ сертификация берген кезде сертификат құрамы дәл екеніне кепілдік береді. Көбінесе сертификаттар ашық кілттерге және орындалатын файлдарға беріледі.

Ашық кілттік криптографияны қолданғанда адресаттың ашық кілт дұрыстылығына сену мәселесі туындайды. Ашық кілт кез келген адаммен жасалынуы мүмкін. Егер ол қауіпсіз жерден алынбаса жасанды болып шығуы мүмкін. Бұл мәселені ашық кілттер сертификатын қолдану арқылы шешуге болады. Ол үшін растайтын базалық орталықтардың түбірлік сертификаттар деп аталатын бір немесе бірнеше данасының болуы жеткілікті.

Орындалатын файлдар сертификациясы сертификатталған кілтке ие дайындаушы жасағанын растайды. Бұл қауіпсіздіктің өзіндік бір кепілдігі болады, өйткені алдыда қиыншылықтар кездескен жағдайда сұрақтарды шешуде кімге бару керегін білуге болады.

Сертификация сияқты қол қою ашық кілтті криптография құралымен таралады. Әдетте қол қоюға құжаттар түседі, бірақ кез келген затқа, мысалы, орындалатын файлдарға қол қояды. Мұнда сертицикациядан айырмашылығы қолының дұрыстығын автордың өзі растайды, ал сертификация кезінде кепілдік пен жауапкершілік одан да үлкен инстанциялар (бір-біріне бағынышты мекемелер жүйесінің сатылары) құзырында болады.

Adobe Acrobat программалар үшін кеңейту модульдеріне қол қою.

Adobe Acrobat программасы функционалдылықты ұлғайтуға арналған кеңейту модульдерін қосуға мүмкіндігі бар. Adobe Acrobat Reader бағдарламасына кеңейту модулін жүктеу үшін дайындаушы қол қою керек. DRM (Digital Rights Management, сандық құқықтарды басқару) көмекшісіне түйіскен кейбір режимдерде Adobe компаниясымен сертификатталған және қол қойылған модульдерді ғана жүктеуге рұқсат етіледі,

Бірақ EfcomSoft компаниясының зерттеушілерінің айтуынша кеңейту модулін тексеру кезінде тек орындалатын файлдың кейбір бөліктері қатысады. Бұл файлға сертификаттың тұтастығын бұзбай өзгерістер енгізуге мүмкіндік береді. Бұл кеңейту модулін коррекциялау арқылы кез келген, оның ішінде қауіпті әрекеттерді жасауға соқтыруы мүмкін.

Қолхат алудағы куәландыру және даталау сияқты есептерді шығару сертификация мен қол қою есептерін шығарумен тығыз

байланысты және ол асимметриялық криптография әдістерімен қамтамасыз етіледі.

Microsoft Corporation сертификаттарының компрометациясы (басқалардың немесе жұртшылықтың алдында біреудің беделін түсіру, абыройын төгу).

2001 жылдың 30 және 31 қаңтарында VeriSign компаниясының куәландыру орталығы өзін алдап арбау арқылы Microsoft компаниясының жұмысшысы деп аталған адамға екі сандық сертификат берді. Бұл сертификаттар ActivX компоненттерін, Microsoft Office макростарын және басқа орындайтын модульдерге қол қою үшін қолданылуы мүмкін. Алдауды білгеннен соң VeriSign компаниясы бұл сертификаторды қайтарып алынған сертификаттар тізіміне қосты.

Құпия атын қамтамасыз ету үшін арнайы криптографиялық хаттамалар дайындалған. Олар құпия компьютерлік дауыс беру және құпия атын интернет арқылы тауар мен қызмет ақысын төлеу сияқты операцияларды оындауға мүмкіндік береді.

Бақылау сұрақтары

1. Заң шығарарушылық әдістерге сипаттама беріңіз.
2. Әкімшілікті әдістерге сипаттама беріңіз.
3. Техникалық әдістерге сипаттама беріңіз.
4. CRC-32 (Cyclic Redundant Code) алгоритмі не үшін қолданылады?
5. DVD - дискілер қалай қорғайды?
6. Идентификацияның түрлері.
7. Идентификацияның биометрикалық жүйесінің плюстары мен минустары.
8. LAN және MAN аутентификациясы үшін парольдердің хэштері.
9. Мандатты рұқсат алу деген не?
10. Adobe Acrobat Reader программасының сипаттамалары.

5. Ақпараттық жүйелердің қауіпсіздік үлгілері

5.1. *Ақпаратты қорғаудың абстракты модельдері*

Қауіпсіздік саясаты моделі – бұл ақпаратты өңдеу, тарату және қорғау әдістерін анықтайтын белгілі жүйе немесе жүйелердің жіктелуіне бағытталған қауіпсіздік саясаттың формалды түрде берілуі.

Модельдердің көбісінде формалды ережелер маңыздылығына сәйкес келесі талаптарды анықтайды:

1. Қол жететіндік.
2. Бүтінділік.
3. Құпиялылық.
4. Есеп берушілік.

Қауіпсіздік саясаты моделінде әр талап өз аймағына жауап береді.

Қол жететіндік – бұл ақпаратқа қатынас жасауына мүмкіндік беретін талап, яғни:

- жария қолданушыларға рұқсат берілген шеңберінде қатынас жасауды ұйымдастыру;
- рұқсатсыз қатынас жасауға тыйым салу.

Бүтінділік келесі екі салаға жауапты:

- ақпарат бүтінділігі – сақтау, өңдеу және тасымалдау процесінде рұқсатсыз әрекеттерден ақпаратты қорғауды қамтамасыз ету;
- жүйе бүтінділігі – жүйе жұмысында екі жақтылығының (двойственность) жоқтығы.

Құпиялылық – меншік және құпия ақпаратқа қойылатын талап, сақтау, өңдеу және тасымалдау процесінде қолданылады. Кейбір деректерге мысалы, құпия кілтке, аутентификация серверіне маңызды талап болып саналады.

Есеп берушілік – кез келген іс-әрекетті басынан соңына дейін бақылауға мүмкіндік беретін талап. Рұқсатсыз жүйені

пайдаланғанын табуға, жүйені қателерден қорғауға және бұл жағдай болған кезде жүйені бастапқы қалпына келтіруге қолданылады.

Талаптардан басқа модельді іске асыруына әсер ететін модельдің ең маңызды атрибуты ретінде *жүйеге қатынас жасауды бақылау әдісі* болып табылады. Қорғалған *жүйеге қатынас жасауда бақылау әдістерінің* көбісі екі класқа бөлінеді:

- Жүйеге қатынас жасаудағы еркін (өзіндік) бақылау (Discretionary Access Control). Бұның мағынасы: ақпарат иесі өз еркімен ақпаратқа қатынас жасауды өзі таңдай алады. Мұндай әдіс коммерциялық және ғылыми мақсаттарға жетуге бағытталған модельдерге тән болады.
- Жүйеге қатынас жасаудағы мандаттық бақылау (Mandatore Access Control). Ереже ретінде, бұл жағдайда жүйеге қатынас жасаудың бақылауы ақпараттың қасиеттері мен осы ақпаратқа қатынас жасаушының қасиеттеріне қарай және оларға тәуелсіз ережелерімен іске асырылады. Мұндай әдіс әскері және мемлекеттік қорғаныс жүйелерді іске асыруға бағытталған модельдерге тән болады.

80-жылдары АҚШ әскері министрлігінің (Department of Defense) басқаруымен компьютерлік қауіпсіздік саласында стандарттар жүйесін анықтайтын «Компьютерлік жүйелердің қауіпсіздігін бағалау өлшемі (критерийі)» (The Trusted Computer System Evaluatin Criteria) атты бірінші құжат жасалынды. Бұл құжат түсіне байланысты «Қызыл сары кітап» деп аталып кетті. Қазіргі кезде компьютерлік қауіпсіздігі стандарттарын анықтайтын оннан астам құжаттар бар.

5.2. *Қауіпсіздік модельдің сипаттамалары*

Модель қауіпсіздік жүйенің қасиеттерін математикалық терминдер көмегімен қалыптастыруы болып табылады. Екінші жағынан қарағанда модельде белгісіз қасиеттері де болуы мүмкін. Ал модельді құрастыру кезінде математикалық белгісіздер төмен

болуына керек, сондықтан модельге қосымша (бұрын болмаған) қасиеттерді немесе шектеулерді енгізу қажет.

Автомат теориясы жүйесінде рұқсат алуды басқаруды көрсететін модельді сипаттау.

Осы модель компьютерлік жүйе ретінде көрсетіледі. Ол операциялық жүйе және аппаратура жұмысын ұқсастырады (имитациялайды). Қалыпты күй айнымалы жүйедегі әрбір bit және әрбір байт үшін абстракция болып табылады. Бір күйден екінші күйге өту функциясы – бұл операциялық жүйеге қатынас жасау абстракциясы болып саналады және қалып күй өзгеруін (немесе өзгермеуін) нақты бейнелейді.

Қатынас жасауды басқару моделі барлық айнымалылар және жүйе функцияларымен жұмыс жасамайды. Осы айнымалылар мен функцияларды таңдау модельді жасаушының қолында.

Қатынас жасауды басқару моделін құрастыруы модельдің элементтерін (айнымалыларды, функцияларды, ережелерді және т.б.) және қауіпсіздіктің бастапқы қалыпты күйін анықтау болып табылады. Математикалық түрде дәлелденеді: бастапқы қалыпты күй қауіпсіз болған жағдайда барлық функциялар да қауіпсіз болады. Кейін математикалық индукция жолымен келесі нәтиже шығарылады: егер жүйе бастапқы кезде қауіпсіздік қалыпты күйінде болса, онда қандай функциялар және қандай ретпен орындалған кезінде жүйе бастапқы қауіпсіздік қалыпты күйінде қалады.

Сондықтан, бұл модельде құрастыру барысында келесі қадамдарды ерекшелеуге болады:

1. *Қауіпсіздікке қатынасы бар қалыпты күй айнымалыларын анықтау.* Әдетте қалыпты күй айнымалылары жүйенің субъектілер мен объектілері, олардың қауіпсіздік атрибуттары және субъектілер мен объектілер арасындағы қатынас құру құқықтары болып табылады.

2. *Қауіпсіздік қалыпты күйін көрсететін шарттарды анықтау.* Бұл жерде қалыпты күй айнымалылары арасындағы қатынастарды анықтау болып табылады. Қатынастың ақиқаттығы қалыпты күйлерден өтуінде қамтамасыз етілуі қажет.

3. *Бір қалыпты күйден басқа қалыпты күйге өту функцияларын анықтау.* Бұл функциялар қалыпты күйлер айнымалылардың

өзгеру тәсілдерін бейнелейді. Олар қатынас құрудың өзгеру ережелері деп те аталады, өйткені олардың мақсаты барлық өзгерулерді анықтау емес, тек қана жүйенің жасай алатын өзгертулерді көрсету болып табылады.

Ауысу функцияларына тән бірнеше сипаттамаларын ерекшелеуге болады:

- *функцияның тағайындалуы* – алдыңғы және жаңа қалыпты күйлер айнымалыларының арасындағы өзара байланыстарды анықтау;
- *функция операция алгоритмінің орындалуына қандай да болмасын нақтылы реттілікті бермейді.* Басқаша айтқанда, функция операцияны аяқталғаннан кейін қалыпты күйдің жағдайы қандай болатынын анықтайды;
- *ең қарапайым функция*. Бұл функцияның тиімділігі ұсақ іс-әрекеттерге бөлінбейді және үздіксіз деген мағынаны білдіреді. Көрсетілген қалыпты күй өзгерісі дереу орындалады, яғни өзгеру уақытын анықтау мүмкін емес.

4. *Функциялар қауіпсіздік қалыпты күйін сақтауын қамсыздандыратыны дәлелденеді.* Модель қауіпсіздік жағдайда екенін білу үшін келесі тармақ орындалу қажет: егер әр ауысу функциясында бастапқы кезде жүйе қауіпсіздік қалыпты күйінде екені дәлелденсе, онда жүйе функция орындалғаннан кейін қауіпсіздік қалыпты күйінде екені дәлелденеді.

5. *Бастапқы қалыпты күйді анықтау.* Жүйенің бастапқы қалыпты күйі математикалық түрде жүйенің барлық қалыпты күй айнымалылар жиынымен бейнеленеді. Жүйенің қарапайым қалыпты күйі субъектілер мен объектілер жоқтығымен анықталады. Сондықтан айнымалылардың бастапқы мәндерін анықтау қажет емес, өйткені жүйенің қалыпты күйі әрдайым қауіпсіздік жағдайында болады. Нақты жағдайда бастапқы қауіпсіздік қалыпты күйі субъектілер мен объектілер жиынымен анықталады.

6. *Бастапқы қалыпты күйі анықтама бойынша қауіпсіз екені дәлелденеді.*

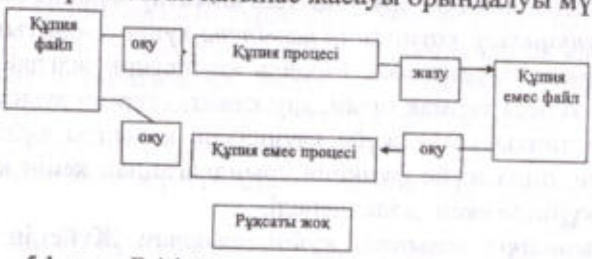
Қауіпсіздіктің негізгі теоремасы: егер жүйенің бастапқы қалыпты күйі қауіпсіз болса және барлық келесі қалыпты күйлерге өтулер қауіпсіз болса, онда жүйе толық қауіпсіз болады.

5.3. *Белл – Ла Падул қауіпсіздік моделі*

Модельдер ішінде бірінші болып және компьютер жұмыстарын үлгілеуге Дэвид Белл мен Леонардо Ла Падул жасаған ең жиі қолданылатын модель болып табылады.

Екі файлдан және екі процестен тұратын жүйені қарастырайық (5.1-сурет). Бір файл және бір процес-құпиясыз, басқа файл және процесс-құпиялы болсын.

Қауіпсіздікдіктің жалпы ережесі бойынша құпиясыз процеспен құпия файлды оқуға болмайды. Құпиясыз файлға осы екі процесс деректерді оқи және жаза алады. Бірақ, егер құпия процесс құпиясыз файлдан хабарды оқыса және құпиясыз файлға оны жазып қойса, онда қатынас құруды басқару ережесі бұзылуы мүмкін. Бұл жерде файлдардың қатынас құру кластары өзгермегеннің өзінде ақпаратқа авторланбаған қатынас жасауы орындалуы мүмкін.



5.1-сурет. Екі файл мен екі процестен тұратын жүйе

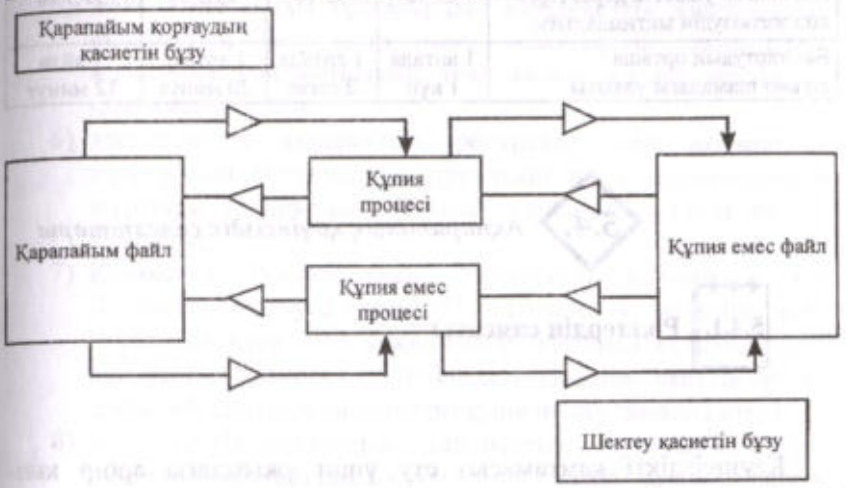
Егер процестің қатынас құру класы файлдың қатынас құру класынан жоғары болса және ақпаратты файлға жазса, онда «төмен жазу» процесі орындалады. Осы шектеу Белл – Ла Падул моделінде «*-қасиет» немесе шектеу қасиеті деп аталады.

Сонымен көп деңгейлі қауіпсіздік моделінде екі негізгі қасиеттері болады:

- **қарапайым қауіпсіздік**: егер субъектінің қатынас құру класы объектінің қатынас құру класынан басымды болса, онда субъект объектіні тек қана оқи алады. Басқаша айтқанда, субъект «төмен» оқи алады, ал «жоғары» оқи алмайды;

- **шек қою қасиеті**: субъект объектіге тек қана жазып қоя алады, егер субъектің қатынас құру класы объектің қатынас құру класынан басым болса. Субъект «жоғары» жаза алады, бірақ «төмен» жаза алмайды.

Процесс қатынас құрудың жоғары класындағы объектіні оқи алмайды (қауіпсіздіктің қарапайым қасиеті), қатынас құрудың төменгі класындағы объектісіне жаза алмайды (*- қасиет немесе шек қою қасиеті). Осы жағдай 5.2-суретте көрсетілген.



5.2-сурет. Шек қою қасиеті

Белл – Ла Падул моделінде қатынас құруды басқару матрицасы арқылы жүргізілген. Бұл модельде матрицаны өзгерту кезінде жиырмаға жуық функциялар анықталады.

Есептеу техникасы және автоматтандырылған ақпараттық құралдардың қорғану кластарын әр түрлі сипаттамаларына қарай жіктеуге болады. Бұзылу тұрақтығына қарай төрт класқа бөлуге болады:

5.1-кесте. Қорғану кластарын жіктеу

Параметр	0 класс	1 класс	2 класс	3 класс
Мах жұмыс істеу қабілеттілігі	1 апта	1 тәулік	1 сағат	1 сағат
Қандай уақытта жұмыс істеу қабілеттілігі	Жұмыс кезінде	Жұмыс кезінде	Жұмыс кезінде	Тәулікте 24 сағаттан жоғары болмауы керек
Кез келген уақытта деректерге қол жеткізудің ықтималдығы	80 %	95 %	99,5 %	99,9 %
Бас тартудың орташа ең көп шамадағы уақыты	1 аптада 1 күн	1 аптада 2 сағат	1 аптада 20 минут	1 айда 12 минут

5.4. *Ақпараттық қауіпсіздік саясаттары*

5.4.1. Рөлдердің саясаты

Қауіпсіздікті қамтамасыз ету үшін ұжымдағы әрбір қызметкерлердің функцияларын, қандай ақпаратпен қалай жұмыс істеу керектігін анықтаған жөн.

Қазақстан Республикасының 2007 жылғы 11 қаңтардағы N 217 Ақпараттандыру туралы Заңында ұлттық оператор деген ұғым енгізілген және оған (9-бап) келесі міндеттері мен құқықтары белгіленген:

1) ақпараттандыру саласындағы біртұтас техникалық саясатты іске асыру мақсатында мемлекеттік органдардың инвестициялық жобалары мен бағдарламаларын жоспарлауға, қалыптастыруға және талдауға қатысады, сондай-ақ оларды дамытуға қатысуға құқылы;
2) мемлекеттік ақпараттық жүйелердің өзара іс-қимылын, олардың әлемдік ақпараттық жүйелерге интеграциялануын қамтамасыз етеді;

3) Қазақстан Республикасының «Электронды үкіметі» инфрақұрылымының жобалық интеграторы қызметін жүзеге асырады;
4) бағдарламалық-аппараттық құралдарға жүйелік-техникалық қызмет көрсетуді, ұлттық электрондық ақпараттық ресурстар мен ұлттық ақпараттық жүйелер енгізуді және оларды сүйемелдеуді жүзеге асырады, сондай-ақ осы мақсаттар үшін персоналды оқытуға құқылы;
5) жеке және заңды тұлғалардың мемлекеттік электрондық ақпараттық ресурстар мен мемлекеттік ақпараттық жүйелерге қол жеткізуіне техникалық жағдай жасалуын қамтамасыз етеді;
6) электрондық ақпараттық ресурстар мен ақпараттық жүйелердің мемлекеттік тіркелімін және депозитарийін жүргізуді техникалық жағынан қамтамасыз етуді жүзеге асырады;
7) Қазақстан Республикасы Үкіметінің веб-сайты мен Қазақстан Республикасы «Электронды үкіметінің» веб-порталын құру мен техникалық жағынан сүйемелдеуді, сондай-ақ Қазақстан Республикасының мемлекеттік органдары веб-сайттарының мониторингін қамтамасыз етеді;
8) мемлекеттік электрондық ақпараттық ресурстар мен мемлекеттік ақпараттық жүйелердің өзара іс-қимылының бірыңғай коммуникациялық ортасын құруға және оған техникалық қызмет көрсетілуін қамтамасыз етуге қатысады;
9) «Электронды үкіметті» қалыптастыру кезінде мемлекеттік органдарға консультациялық және практикалық көмек көрсетеді;
10) «Электронды үкіметтің» ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жұмыстарды жүргізу кезінде ұлттық электрондық ақпараттық ресурстар мен ұлттық ақпараттық жүйелердің қорғалуын ұйымдастыруды жүзеге асырады;
11) Қазақстан Республикасының «Электронды үкіметін» қалыптастыру кезінде жобаларды басқару және техникалық жағынан сүйемелдеу функцияларын жүзеге асырады.

Оператор – қорғаныс жүйесін пайдалану арқылы хабарламаларды қабылдау, жинау, өңдеу, беру және қабылдауды тікелей жүзеге асыратын деректер базасын пайдаланушы қызметкер. Бұның функциялары әр процесте нақты анықталып, осыған сәйкес нұсқаулықта (инструкцияда) көрсетіледі.

5.4.2. *Ақпараттық қауіпсіздік саясатты жасау*

Ақпараттық қауіпсіздік саясаты – шектеулі таратылатын ақпаратты басқаруды, қорғауды және бөлуді реттейтін нормалар және практикалық тәсілдер.

Ұйымның және деректер базасын пайдаланушылардың кешенді қауіпсіздік жүйесі аясында корпоративті қауіпсіздікті басқару – ақпараттық қауіпсіздік саясатының жалпы талаптарын орындауды тұрақты бақылаумен, оған жедел түрде түзету енгізу және оның деңгейін көтеру арқылы қамтамасыз етіледі.

Ақпараттық қауіпсіздік саясатында қолданылып отырған ақпараттық жүйе құрамының сипаты, ұйымның ақпараттық жүйені пайдаланушыларының тізімі, олардың ақпараттарға, программаларға және техникалық құралдарға кіру құқықтары (олардың қызметтік жағдайы мен орындап отырған жұмысының сипатына байланысты) және ол мыналарды белгілейді:

1) ақпараттық қауіпсіздік аясындағы жұмыстың жалпы бағыттары;
2) ақпараттық жүйені қорғаудың мақсаты мен міндеттері;
3) қажетті қауіпсіздік деңгейіне жетудің негізгі принциптері мен тәсілдері;
4) ақпараттық қауіпсіздік саясатын белгілеуге қажетті талаптарды әзірлеуге жауапты тұлғаларды анықтау;
5) ақпараттық жүйенің және оны қорғау жүйесінің жұмыс қабілетін құруға және қолдау көрсетуге жауапты ұйымдар бөлімшелерін анықтау;
6) табиғи апаттар, апаттар, өрт, электр қуатының ажырауы, байланыс желілерінің бүлінуі, жаппай тәртіпсіздіктер, ереуілдер, әскери қимылдар сияқты дүлей күш пайда болған

жағдайдағы ақпараттық жүйенің қауіпсіздік режимінің бұзылуын болдырмау жөніндегі шаралар.

Кәсіпорында ақпараттық қауіпсіздік аймақта ағымдағы жағдайды бағалауға екі жүйе пайдаланылады. Олар: «зерттеу төменнен жоғары» («снизу вверх») және «зерттеу жоғарыдан төмен» («сверху вниз»). Бірінші әдісте: басында жүйенің жеке есептері қойылады; содан кейін кейбір ең қарапайым функциялардың жиыны жасалынады; ең қарапайым функциялардың негізінде жүйенің ірілеу компоненттері құрастырылады. Кейін барлық ірі компоненттер бірегей жүйеге біріктіріледі.

Екінші әдісі: басында жүйенің жалпы сипаттамасы жасалынады; жүйенің компоненттері ерекшеленеді; кезекпен осы компоненттерден ішкі компоненттер ерекшелінеді. Бұл процесс жүйені толық құрастырғанша жүргізіледі.

Жазып жіберу немесе әрбір нақтылы ақпараттық объектісіне басқа шабуыл фирмаға зиян әкеле алады. Ол қаншалықты зиянды екені айқындалуы керек. Сол кезеңді «тәуекелдердің есептеуі» деп атайды. Бірінші жақындауда тәуекелмен «шабуыл сондай ықтимал» деп аталады. Тәуекелдердің есептеу схемаларының жиыны болады.

Шабуылдың зиянын шамалау үшін сандар пайдаланады, оларды келесі кестеде көруге болады :

5.2-кесте. Шабуылды шамалау

Залал өлшемі	Сипаттама
0	Ақпаратты ашу мәнсіз шығынға әкеледі
1	Шабуыл нәтижесінде, шығын шамалы болып келеді. Нарықта фирма жағдайы өз қалпында болады.
2	Қаржы операциялары тоқтатылады, сол уақыт аралығында фирма шығынға ұшырайды. Нарықтағы жағдайы және клиент саны ең аз шамада өзгереді.
3	Нарықта шығынға ұшырайды.
4	Көп шығын шығады. Сол кезеңде фирма нарыққа шыға алмайды. Жағдайды жақсарту үшін көптеген қаржыландыру қажет.
5	Фирма өз өмірін аяқтайды

Бақылау сұрақтары

1. Модельдерге қойылатын талаптар қандай?
2. Автомат теориясы жүйесінде рұқсат алуды басқару барысында қандай қадамдарды ерекшелеуге болады?
3. Белл – Ла Падул қауіпсіздік моделі қай жылдары ұсынылды және негізгі сипаттамалар қандай?
4. Есептеу техникасы және автоматтандырылған ақпараттық құралдардың қорғану кластарын қандай сипаттамаларына қарай жіктеуге болады?
5. Ұлттық оператор ұғымы қандай?
6. Рөлдердің саясаты қандай?
7. «Зерттеу төменнен жоғары» («снизу вверх») алгоритмі қандай?
8. «Зерттеу жоғарыдан төмен» («сверху вниз») алгоритмі қандай?
9. Шабуылдың зиянын қалай шамалауға болады?

6. Қорғау және қауіпсіздендіру жүйелерін практикалық іске асырудың мысалдары

6.1. Негізгі түсініктер

Түрлендіру арқылы ақпаратты қорғау мәселесімен криптология (Грекше – құпия ғылым (сөз) деген мағынаны білдіреді) айналысады.

Криптология екі бағытқа жіктеледі:

1. Криптография.
2. Криптоталдау.

Бұл екі бағыттың мақсаты – бір-біріне қарама-қарсы. Криптография – құпия жазу – ақпаратты заңсыз пайдаланушылардан қорғау мақсатымен оны түрлендіру әдістері жайындағы ғылым, ақпаратты, оның мазмұнын жасыру мақсатында түрлендіру тәсілдерін іздеп, зерттеумен айналысады. Өзге адамдардан ақпараттың құпиясын сақтап қалу криптографияның негізгі мақсаты болып табылады. Ақпаратпен заңсыз таныспақшы болған осындай адамдарды қаскөйлер (қаскүнемдер), жолдан ұстап қалушылар деп атайды.

Криптологиядағы негізгі терминдер:

Алфавит – ақпараттарды шифрлауға пайдаланылатын символдар жиыны.

Мәтін – алфавит элементтерінен тұратын реттелген жиын.

Шифрлау – түрлендіру процесі, бастапқы мәтінді шифрлаған мәтінге түрлендіру, ауыстыру.

Кері шифрлау – шифрланған мәтінді бастапқы мәтінге келтіру.

Кілт – мәтінді шифрлауға және кері шифрлауға пайдаланылатын ақпарат.

Криптографиялық жүйе – бұл берілген мәтінді шифрлауға қолданатын әдістер мен алгоритмдер жиыны. Бұл жерде негізгі параметр кілт болып табылады. Криптожүйелер 2 түрге бөлінеді:

Симметриялық криптографиялық жүйелерде шифрлауға және кері шифрлауға бір ғана кілт пайдаланылады.

Асимметриялық криптографиялық жүйелерде (ашық кілт) екі кілт пайдаланылады. Шифрлауға – бір кілт, кері шифрлауға – екінші кілт.

Кілттерді тарату және кілттерді басқару термині: бұл пайдаланушылар арасындағы ақпаратты түрлендіруге қолданылатын кілттерді керекті жерге керекті уақытта жеткізу процесі.

Электронды қолтаңба – басқа да пайдаланушыға мәтіннің авторының шынайылығын және хабардың дұрыстығын тексеруге арналған мәтінге қосымша криптографиялық түрлендіру.

Криптоталдау – кілтті білмей-ақ, ақпарат шифрын ашу мүмкіндіктерін зерттейді. Криптографиялық жүйеге сәтті жүргізілген криптоталдау (аналитикалық) зерттеулер негізінде хабардың бастапқы ашық мәтінімен қатар оның кілтін де ашуға мүмкін болады. Криптоталдау шифрланған хабарды, немесе кілтті және екеуін де оқуға мүмкіндік беретін криптографиялық жүйенің осал жерлерін іздеумен шұғылданады.

Криптоберіктілік шифрдың негізгі сипаттамасы болып табылады. Ол кілтті белгісіз жағдайда шифрдың кері шифрлауға (яғни криптоталдауға) беріктігін анықтайды. Әдетте бұл сипаттама шифрды ашу үшін керекті уақыт мөлшерін анықтайды.

Криптографиялық жүйе (криптожүйе) – шифрлау алгоритмі, сондай-ақ алуан түрлі кілттердің, ашық және шифрланған мәтіндердің жиынтығы.

Криптографиялық алгоритм (*шифр* немесе *шифрлау алгоритмі*) деп шифрлау және кері шифрлау үшін қолданылатын математикалық функцияны атайды. Егер дәлірек айтсақ мұндай функция екеу: біреуі – шифрлау үшін, ал екіншісі кері шифрлау үшін қолданылады.

Криптография ақпаратты түрлендірудің математикалық әдістерін іздеумен және зерттеумен шұғылданады. Криптография ақпаратты оқу (бұрынғы қалпына келтіру) тек оның кілтін білген кезде ғана мүмкін болатындай етіп түрлендіреді.

Қазіргі кезде криптографияны 4 ірі класқа жіктейді:

1. Симметриялық криптожүйелер.
2. Ашық кілтті криптожүйелер немесе асимметриялық криптожүйелер.

3. Электронды-цифрлық қолтаңбалар жүйелері.
4. Кілттерді басқару жүйелері.

Криптографиялық әдістерді қолданудың негізгі бағыттары мыналар: жасырын ақпаратты байланыс арналары (мысалы, электрондық пошта) арқылы тасымалдау, жіберілген хабарлардың шынайылығын анықтау, ақпаратты (құжаттарды, деректер базасын) шифрланған түрде тасымалдағыштарда сақтау.

Криптографиялық жүйелерге келесі талаптар қойылады:

1. Шифрланған мәтін қолға түскенде тек қана кілт арқылы оқылуы керек.
2. Шифрлауда қолданатын кілттің операциялық саны шифрланған хабарламаның көрінісі мен оған сәйкес ашық мәтінге қажетті кілттердің жалпы санынан кем болмауы керек.
3. Қайта шифрлауға қажетті ақпараттың операция саны барлық кілттерді іріктеуде қатал түрде төменгі бағаға ие болуы керек және қазіргі заманғы компьютерлер мүмкіндігінен асып түсуі керек.
4. Шифрлау алгоритмін білу қорғау тиімділігіне әсер етпеу керек.
5. Кілтті азғантай өзгертуі шифрланған хабарлама түрін бірдей кілт пайдаланғанда да маңызды өзгертуге әкелмеуі керек.
6. Шифрлау алгоритмінің құрама элементтері өзгермейтіндей болуы керек.
7. Кілттер арасында шифрлау кезінде жүйелі түрде пайдаланатын қарапайым және оңай тәуелділік болмауы керек.
8. Шифрланған мәтін ұзындығы берілген мәтін ұзындығынан аспау керек.
9. Алгоритм программада, сонымен қатар ақпараттық жүйеде де өзгеруге мүмкіндік беруі қажет және ұзындығының өзгеруі шифрлау алгоритмнің сапасына әсерін тигізбеу керек.

Криптографияда К әріпімен белгіленетін кілт қолданылады. ***Кілт*** (key) – ақпаратты шифрлау және кері шифрлау, сондай-ақ, оған қол қою үшін арналған цифрлық код. Ол барлық мүмкін нұсқаулардан (варианттардан) криптографиялық түрлендіру алго-

ритмі үшін тек бір нұсқаны таңдауды қамтамасыз етеді. Кілттің ортақ, жеке меншік және құпия деп аталатын түрлері болады.

Шифрлау E функциясы да, кері шифрлау D функциясы осы кілтке тәуелді болады: $E_K(P) = C$, $D_K(C) = P$.

Сонда мына тепе-тендік ақиқатты болады: $D_K(E_K(P)) = P$.

Бұл жерде, P (plaintext) – ашық мәтін, ал C (ciplertext) – E функциясы мен K кілті арқылы шифрланған мәтін (шифромәтін). Осы айтылғанды келесі суретпен бейнелеуге болады.

6.1-сурет. Шифрлау әдісі

Мәліметтерді криптографиялық жабу процесі программалық түрде де, ақпараттық түрде де іске асырылады. Ақпаратты өткізу ақша жағынан көп қаржыны талап етеді, бірақ оның да артықшылықтары бар. Жоғары өнімділік, қарапайымдылық, қорғаныстылық және т.б.

Тізбектің қауіпсіздігі ең әлсіз буыннан құралады, ол тұрақты болған сайын сенімді болады.

Жақсы тұрғызылған криптожүйеде алгоритм де, хаттама да кілт және қалған барлығы өте күрделі тексерістерден өтуі қажет.

Егер криптографиялық алгоритм тұрақты болмаса, онда кез келген криптоталдаушы бұл қателікті біліп қояды. Егер Генераторды күшейткенде компьютер жадының ұяшықтары қорғалмаған болса, онда мұндай қауіпсіздік ешкімге керек болмайды. Сонымен қатар, тәжірбие жүзінде ақпараттық қауіпсіздікті қамтамасыз ету тек қана криптоталдаушыға байланысты болмайды.

Симметриялық криптографиялық жүйелер

Қазіргі кезде дербес компьютерлерді қолданушыларда әр түрлі программалық өнімдерде қойылған шифрлау алгоритмдерді қолдануға мүмкіндік бар, мысалы, Word мәтіндік редакторында, Excel электронды кестелер редакторында немесе Windows NT операциялық жүйесінде. Осы программалық өнімдердің ортақ құралдардан басқа, іштей орнатылған шифрлау алгоритмдері бар.

Қандай алгоритм жақсы – симметриялық па немесе асимметриялық па? Дегенмен, криптожүйелердің артықшылықтары мен кемшіліктері жөнінде пікір-таластар ашық кілтті ашық алгоритм ойлап табылғалы бері жүргізілуде. Симметриялық криптографиялық алгоритмнің кілт ұзындығы үлкен емес және ассиметриялыққа қарағанда тез жұмыс істейді.

Бірақ ашық кілтті криптожүйелердің ойлап тапқандардың бірі американдық криптолог У. Деффидің айтуына қарағанда, оларды универсалды криптодүниенің жаңа түрі ретінде қарастыруы керек.

Ашық кілтті криптография және симметриялық криптография арасында үлкен айырмашылық бар, олар әр түрлі проблемаларды шешуге арналған алгоритмдер.

Бірақ симметриялық криптографияда құпиялы кілтті алгоритм жұмыс істей алмайтын аймақтарда ашық кілтті криптография істей алады.

Файлдарды шифрлау

Бір қарағанда файлдарды шифрлау хабарламаларды шифрлауға ұқсас секілді. Мұнда жіберуші де қабылдап алушы да бір адам, ал жіберу ортасы мәліметтерді сақтаудың компьютерлік құрылғысы болып табылады. Бірақ мұның бәрі өте күрделі жүйе.

Криптография үлкен құпияны кішкентай құпияға айналдыруға көмектеседі. Күрделі құрылымда файлды жаттап жүрудің орнына, оны шифрлап, кілт жадысына сақтауға болады. Хабарламаларға қарағанда шифрланған файлдар көптеген жылдар бойы сақталып жата алады. Ол үшін кілтті ұмытпай құпияда ұстау керек.

Ең тиімді әрбір файлға жеке кілттер шифрлап, содан кейін барлық кілттерді кілттер шебері көмегімен бірге орналастыруға болады. Мұндай криптожүйенің тұрақтылығы, басқа барлық файлдарға бір кілт пайдалануға қарағанда жоғары. Барлық криптографиялық әдістерді мынадай түрлендіру кластарына бөлуге болады.

Көп алфавитті ауыстыру – бастапқы мәтіннің символдарын басқа күрделі ережеге сай түрлендірудің қарапайым түрі, жоғарғы криптографиялық тұрақтылыққа ие болу үшін күрделі кілттерді пайдалану керек. Симметриялық криптожүйелердің түрлендіру кластары 6.2-суретте көрсетілген.

6.2-сурет. Симметриялық криптожүйелердің түрлендіру кластары

Орын ауыстыру – криптографиялық түрлендірудің аса күрделі емес әдісі. Әдетте, басқа әдістермен бірігіп пайдаланылады.

Гаммерлеу – бұл әдіс кілт негізіне генерацияланған алғашқы мәтінге бірқатар жалған кездейсоқ тізбек қоюмен пайдаланылады.

Шифрлар блогы – шифрланатын мәтіннің блогына пайдаланатын түрлендірудің негізгі әдістерінің жүйелілігін көрсетеді. Шифрлар блогы таза блогының түрлендіруге немесе жоғары криптографиялық тұрақтылыққа сәйкес басқа да кластарға қарағанда, тәжірбиеде жиі кездеседі. Ресейлік және американдық шифрлау стандарты тек осы кластарға негізделген.

Цезарьдың орын ауыстыру әдісі

Цезарьдың орын ауыстыру әдісі орын ауыстырудың ең қарапайым тәсілі болып табылады. Ол көпалфавитті орын ауыстыру тобына жатады. Бұл әдіс Рим императоры Гай Юлий Цезарь

атымен аталған Ол Марк Тулий Цецеронға 50 әріпті алфавит пен С=3 орын ауыстыруды пайдаланып хаттамаларды құрастыруды бұйырған. Орын ауыстыру *Бастапқы мәтін* – шифрланған мәтінге сәйкес әріптер жұбынан тұратын кесте арқылы анықталады.

С-3 орын ауыстыруда 1-кестеде берілген бағыт (→) бастапқы мәтін әріптері (сол жақтағы) С=3 шифрлауы арқылы оң жақтағы шифрланған мәтін әріптеріне ауыстырылады.

Мысалы «Мен жұмыс жасадым» сөйлемі С-3 орын ауыстыруы арқылы **пзрйцпюфйгфгжюп** ауысады.

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

6.3-сурет. Цезарь орын ауыстыруын қолдану

Өзінің қарапайымдылығына байланысты жүйе әлсіз келеді. Егер қаскүнемдегі жағдай төмендегідей болса:

1) шифрланған немесе сәйкес келетін бастапқы мәтін;

2) қаскүнеммен таңдап алынған бастапқы мәтіннің шифрланған мәтіні болса, онда ешқандай қиындықсыз кілтті анықтап, шифрды аша алады.

Хилл және Плэйфер шифрлары Цезарь орын ауыстыруына қарағанда тиімдірек. Олар жеке символдардың орын ауыстыруына емес, 2 граммды (Плэйфер шифры) және н-граммды (Хилл шифры) ауыстыруға негізделген. Жоғарғы криптографиялық тұрақтыларға қарамастан бұл әдіс өте күрделі және таратуда көп ақпаратты талап етеді.

6.3. Асимметриялық криптографиялық жүйелер (кілті ашық криптожүйелер)

6.3.1. Кілті ашық криптожүйелерді құру принциптері

Асимметриялық (кілті ашық) криптожүйелердің ерекше сипаттамалары:

1. Ашық кілт және криптограмма қорғалмаған арна арқылы берілмеуі мүмкін, яғни ашық кілт және криптограмма қарсыласқа белгілі болуы мүмкін.
2. Шифрлау және кері шифрлау алгоритмі ашық болады

Асимметриялық криптожүйелерде ақпаратты қорғау процесі құпия кілтке негізделген. Осы ашық кілтті жүйенің алгоритмін ұсынған Деффи мен Хелман асимметриялық криптожүйенің қауіпсіздігін қамтамасыз ететін талаптарды ұсынады:

1. Ашық кілт және құпия кілттерді есептеу процесінің байланыс шарттары қарапайым болуы қажет.
2. Ақпаратты беруші ашық кілтті және мәтінді пайдалана отырып, криптограмманы оңай есептей алады.
3. Қабылдаушы құпия кілтпен криптограмманы пайдалана отырып, бастапқы мәтінді бастапқы түрге келтіре алады.
4. Жау ашық кілтті біле отырып, жабық кілтті есептеу кезінде шешілмейтін есептеу проблемасына тап болуы қажет.
5. Ашық кілтті және криптограмманы мәтінді есептеу кезінде шешілмейтін есептеу процесіне тап болуы керек.

Кілті ашық криптожүйенің негізінде бір жаққа бағытталған функция f түсінігі жатыр, ол келесі қасиеттерді қамтиды:

- $y = f(x)$ функциясының мәндерін қарапайым есептеу (үлкен ресурстарды қажет етпейді);
- f^{-1} кері функциясының бар болуы;
- $x = f^{-1}(y)$ кері функциясының мәндерін күрделі есептеу (қазіргі компьютерлердің мүмкіндігі аумағында ресурстарды қажет етеді);

Асимметриялық криптографияда бір жаққа бағытталған класс тармағы бар – ол айналма жолды бір жаққа бағытталған функция, ол үшін айналма жол туралы арнайы ақпарат болса, кері функция негізгі функция секілді оңай табылады. Бұл арнайы ақпарат құпиялы кілт рөлін атқарады.

pk – E шифрлаудың ашық кілті болсын, ал sk – D кері шифрлаудың құпия кілті болсын. E және D асимметриялық криптожүйені құру үшін келесі шарттарды қанағаттандыру қажет:

1. $D_{sk}(E_{pk}(P)) = P$ (кері шифрлау P мәтінін қалыптастыру керек).
2. E_{pk} және D_{sk} функциялары қолдануда қарапайым болу керек.
3. E_{pk} көмегі арқылы орындалатын өзгертуді ашқан кезде D_{sk} көмегі арқылы орындалатын өзгерту ашылмау керек (ашық кілттен құпия кілтті алуға болмайды).
4. $D_{sk}(E_{pk}(P)) = P$ (құпия кілтті шифрлауға, ал ашық кілтті кері шифрлауға қолдануға болады).

Төрт шарт міндетті емес және барлық асимметриялық криптожүйелер оларды қамтымайды.

Асимметриялық криптожүйелердің негізгі қолдануларына келесілер жатады:

- ашық жүйе арқылы симметриялық шифрлаудың кілтін беру (жіберуші алған ақпаратты тек өзінің құпия кілті арқылы аша алатын қабылдаушының ашық кілті көмегімен бұл кілтті шифрлайды);
- электрондық құжаттарды қорғау үшін электрондық цифрлы қол қою жүйесі (құжатты жасаушы оның шынайылығын өзінің құпия кілті арқылы растайды, одан соң ашық кілттің сәйкес кез келген иеленушісі құжаттың түпнұсқалылығын тексере алады);

Асимметриялық криптожүйелерді электрондық цифрлы қол қоюды тексеру және алу үшін ол жоғарыда аталып кеткен төрт шарттың соңғысын қанағаттандыру қажет.

Ашық кілтті криптографиялық жүйе классикалық криптографиялық жүйеге қарағанда салыстырмалы түрде жақын арада, яғни XX ғасырдың екінші жартысында пайда болды.

Қазіргі асимметриялық криптожүйелердің симметриялық криптожүйелердің орнын баспайтындай негізгі ерекшеліктеріне келесілер жатады:

- шифрлау және кері шифрлау процедураларының ұзақтылығы (жобамен 1000 есе көп);
- шифрдың криптотұрақтылығын қамтамасыз ету үшін шифрлау үшін ұзын кілт қолдану қажеттілігі (мысалға, 56 bit ұзындықты симметриялық кілтке 384 bit ұзындықты асимметриялық кілт, ал 112 bit ұзындықты симметриялық кілтке 1792 bit ұзындықты асимметриялық кілт сәйкес келеді).

Ашық кілтті криптографияларды қолдану идеясы дәстүрлі шифрлау кезіндегі пайда болатын қиын мәселелердің шешімін табу әрекетінен пайда болды. Дәстүрлі шифрлауда кілттерді тарату деректер алмасушы екі жақ та не (1) қандай да бір әдіспен оларға жеткізілген ортақ кілттері бар, не (2) қандай да бір кілт таратушы орталығы қызметін пайдаланғанын қамтамасыз етеді. Уитфилд Диффи ашық кілтті шифрлау тәсілін ашушылардың бірі (Мартин Феллманмен бірге Станфорд университетінде жұмыс жасады) өз құжатыңыздың толық қауіпсіздігін қамтамасыз етуіне екінші талап мүлдем қарсы деп санады.

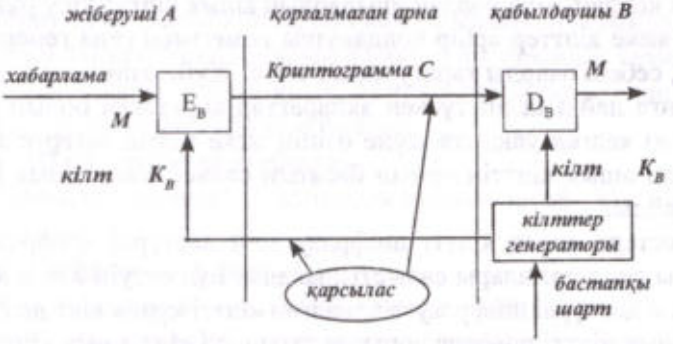
Диффи бірінші мәселеге мүлдем ұқсамайтын екінші мәселені қозғады, ол – «цирфлық қол қою» мәселесі. Егер криптография тек әскери қызметте ғана емес, коммерция және коммуникациядағы электрондық ақпараттар және құжаттар қағаздық құжатта қолданылатын эквивалентті қол қоюды мұқтаждық етеді. Басқа сөзбен айтқанда, екі жақ та цифрлық ақпарат нақты адамнан келгеніне сенімді болатындай тәсіл құрастырып шығуға бола ма?

Диффи және Хеллман жоғарыда аталған мәселелер шешілетіндей тәсілді 1976 жылы жасап шығарды.

Көп таралған асимметриялық криптожүйелерге RSA (Rivest, Shamir, Adleman), Диффи-Хеллман, Эль-Гамаль және эллиптикалық қисықтар негізіндегі криптожүйелер жатады.

6.3.2. Ашық кілтті криптожүйелер

Ашық кілтпен шифрлау шифрлауға арналған бір кілт пен онымен байланысты кері шифрлауға арналған келесі кілтке байланысты.



6.4-сурет. Ашық кілтті шифрлау процесінің жалпы схемасы

Бұл алгоритмдер келесі маңызды ерекшеліктерден тұрады:

- Есептеу тұрғысынан қарағанда қолданылған криптографиялық алгоритм мен шифрлау кілтін біле тұра кері шифрлау кілтін білу мүмкін емес.

Одан басқа, кейбір алгоритмдер (мысалға, RSA) келесі қасиеттерді қамтиды.

- Бұл екі байланысқан кілттің кез келгені шифрлауға қолданыла алады, сол кезде келесісі кері шифрлауға қолданыла алады.

Ашық кілтті шифрлау процесінің жалпы схемасы 6.3-суретте көрсетілген, ол келесідей:

1. Желідегі әрбір түпкі жүйе алынған ақпаратты шифрлау және кері шифрлауға арналған екі кілтті генерациялайды.
2. Әрбір жүйе өз шифрлау кілтін шығарады, оған қоса оны барлығына ашық реестрде (тізілімде) немесе файлда орналастырады. Бұл дегенміз ашық кілттің өзі. Екінші кілт, ашыққа сәйкес келеді, бірақ жеке иелігінде қалады.

3. Егер А қолданушы В қолданушыға ақпарат жібермекші болса, ол В қолданушының ашық кілтін қолданып ақпаратты шифрлайды.
4. В қолданушы ақпаратты алған кезде ол өзінің жеке кілті арқылы кері шифрлайды. Басқа қолданушы ақпаратты кері шифрлай алмайды, себебі В қолданушының жеке кілтін тек В қолданушы өзі ғана біледі.

Бұл қолданымда қолданушылардың ашық кілтке кіру рұқсаты бар, ал жеке кілттер әрбір қолданушы көмегімен ғана генерацияланады, себебі оларды тарату қажет емес. Жүйе өзінің жеке кілтін сақтағанға дейін келіп түскен ақпараттар қорғалған болып саналады. Кез келген уақытта жүйе өзінің жеке кілтін өзгерте алады және ескі ашық кілттің орнын басатын сәйкес жаңа ашық кілтті жариялайды.

1-кестеде ашық кілтті шифрлау мен дәстүрлі шифрлаудың маңызды сипаттамалары салыстырылады. Бұл екеуін өзара айыра білу үшін дәстүрлі шифрлауға арналған кілтті құпия кілт деп атаймыз. Ашық кілтті шифрлау орындалатын екі кілт ашық кілт және жеке кілт деп аталатын болады.

6.1-кесте. Дәстүрлі шифрлау және ашық кілтті шифрлау

Дәстүрлі шифрлау	Ашық кілтті шифрлау
Жұмыс үшін мыналар қажет: 1. Екеуіне де ортақ кілтті алгоритм шифрлауға да және кері шифрлауға да қолданылады. 2. Жіберуші және қабылдаушы бірдей алгоритм және кілт қолдану керек. Қорғау үшін мыналар қажет: 1. Кілт құпия болу керек. 2. Қосымша ақпарат жоқ кезінде ақпаратты кері шифрлау мүмкін болмау керек. 3. Алгоритмді білу және шифрланған мәтін түрлерін білумен кілтті қалпына келтіру мүмкін болмау керек.	Жұмыс үшін мыналар керек: 1. Шифрлауға де және кері шифрлауға де бір алгоритм, бірақ екі кілт қолданылады: бір кілт шифрлауға, ал екіншісі кері шифрлауға. 2. Жіберуші және қабылдаушы сәйкес келетін кілттің бірін қолдану керек (бірақ бірдей емес). Қорғау үшін мыналар қажет: 1. Екі кілттің бірі құпия болу керек. 2. Қосымша ақпарат жоқ кезінде ақпаратты кері шифрлау мүмкін болмау керек. 3. Алгоритмді білу, кілттің бірін және шифрланған мәтін түрлерін білгені мен екінші кілтті қалпына келтіру мүмкін болмау керек.

6.3.3. *Ашық кілтті криптографиялық жүйелерді қолдану*

Ашық кілтті криптографиялық жүйе екі кілтті криптографиялық алгоритмді қолданады, оның бірі жеке қолдануда, ал екіншісі бәріне ортақ ашық болып келеді. Қосымшаға байланысты жіберуші не өзінің кілтін, не қабылдаушының ашық кілтін, не тіпті арнайы криптографиялық функцияны орындау кезінде екеуін де қолданады. Ашық кілтті криптографияны қолдануды үш санатқа (категорияға) бөлуге болады:

- **Шифрлау/кері шифрлау.**

Жіберуші ақпаратты қабылдаушының ашық кілті арқылы шифрлайды.

- **Цифрлық қол қою.**

Жіберуші өзінің жеке кілті арқылы ақпаратқа «қол қояды». Қол қою ақпаратқа немесе ақпарат функциясы болып табылатын кішкене деректер блогына криптографиялық алгоритм қолдану нәтижесінде пайда болады.

- **Кілттермен алмасу.**

Екі жақ сеанстық кілттермен алмасу үшін өзара үлес қосады. Бұндайда бір немесе екі жақтың да кілттерін қолданылуы болады.

Кейбір алгоритмдер осы қолданудың үш типіне де сәйкес келеді, ал қалғандары категорияның бір немесе екеуіне сәйкес келеді. Келесі кестеде қазіргі кезде кең пайдаланатын кейбір алгоритмдердің қолданылу мүмкіндіктері 6.2-кестеде көрсетілген:

6.2-кесте. Алгоритмдердің қолданылу мүмкіндіктері

Алгоритм	Шифрлау/кері шифрлау	Цифрлық қол қою	Кілттермен алмасу
RSA	+	+	+
Диффи – Хеллман	-	-	+
DSS	-	+	-

6.4. *Стеганографиялық жүйелерді іске асыру түрлері*

6.4.1. *Жалпы мәліметтер*

Стеганография – ақпаратты қорғаудағы жаңа бағыт. Ақпараттық қауіпсіздік мәселесінің өзектілігінің үнемі өсіп отыруы себептері ақпарат қорғаудың жаңа әдістерін шығаруға талап етеді. Осы себепке байланысты компьютерлік стеганография әдістерінің дамуына ақпарттық технологиялардың қарқынды дамуы әсер етіп отыр. Ауқымды желілердің кең таралуы, электрондық сауданы ұйымдастыруы және де басқа қызметтердің желі арқылы іске асырылуы хакерлердің санын көбейтуде және олардың жасайтын әрекеттері осы компьютерлік стеганографияның дамуына жол салып отыр.

Қазіргі кезде ақпаратты қорғауға көбінесе криптологиялық әдістер қолданылады. Дегенмен, компьютерлік вирустар, логикалық бомбалар сияқты шабуылдар түрлері кең таралуын жалғастыруда. Мұндай жағдайларда компьютерлік стеганография мен криптографияны қатар пайдалану әдісі өте тиімді.

Криптографияның мақсаты – құпия хабардың мазмұнын жасыру (шифрлау). Ал стеганографияның мақсаты – сырт көздерден құпия хабардың бар болуын жасыру. Мұндайда құпия хабарлар басқа деректерге қыстырылып, солармен бірге сақталады және тасымалданады. «Стеганография» грек тілінен аударғанда «құпия жазба» (Steganos – құпия, graphy – жазба) дегенді білдіреді. Құпия жазба үшін кроссвордтар; музыкалық ноталар, шахмат партиясы «ауыз екі тілдің шифрлары» қолданылады, яғни қарапайым сөздер тіптен басқа мағынаны білдіреді.

Стеганографияға көптеген құпия байланыс құралдары мен ақпаратты тасымалдау құралдары: көрінбейтін сиялар, микрофотосуреттер (микронүктелер), белгілердің шартты орналасуы, қолжазба символдарындағы байқалмайтын айырмашылықтары

жатады. Сонымен қатар, өлең жолдарындғы қатарлардың арасына қыстырып жазу: сүтті қолдану мен күрделі химиялық реакцияларға дейін пайдаланылады. Оларды оқу кезінде өңдеуден өткізеді.

Геродот баяндауларында қанішер Гистийдің (474 ж. б.э.д.) стеганографиялық әдістерді қалай пайдаланғаны айтылады. Ол құпия хабарды сырт көздерден жасыру үшін хабарды байқаусыз жеткізуді көзделі. Осылай бір құлдың шашын қырып тастап, оның басының терісіне хабарды «татуировка» арқылы жазып, шашы қайта өскенше күтіп, құлды хабарды апаратын жерге жібереді. Сондай-ақ Демарт та стеганография әдісін пайдаланды. Ол воск тақшаларын қырып, тақшаның өзіне хабарды тырналап жазып, кейіннен тақшаға қайтадан воск жаққан. Әрине бұл алдыңғы әдіске қарағанда жылдам процесс.

Ежелгі Римдіктер жазу жолдары арасына көрінбейтін сиямен жазған. Көрінбейтін сия ретінде жемістердің шырыны, сүт және т.б. қолданылған.

Екінші дүниежүзілік соғыс кезінде «микронүктелер» кеңінен пайдаланған. Онда хабар кәдімгі типографиялық (баспаханалық) нүкте өлшемімен микрофото түрінде беріліп, қабылдау жағында үлкейтіліп, стандартты өлшемдегі баспа парағында өлшемдегі анық хабарды беретін.

Мұндай нүктелер кәдімгі хаттарға жапсырылып, үлкен өлшемдегі суреттер мен сызбалар сияқты ақпаратты тасымалдау мүмкіндігін берді.

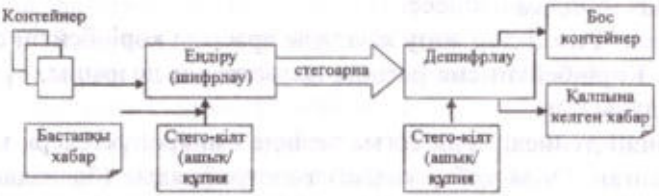
6.4.2. Компьютерлік стеганографияны құру негіздері

Стеганография криптографияны толықтырады. Стеганография арқылы хабарды тасымалдау фактісін жасырып, хабардың өзін криптографиялық әдіспен шифрлауға болады.

Стеганографиялық жүйе немесе стегожүйе – ақпаратты тасымалдаудың жасырын арнасын құруда қолданылатын құралдар мен әдістер жиыны. Стеганографиялық жүйенің жалпы үлгісі 6.5-суретте келтірілген.

Қабылданушы жаққа жіберілетін хабар арнайы программалық қамтаманың көмегімен контейнерлерге салынады. Контейнер – құпия хабарды жасыруға арналған кез келген ақпарат. Контейнер деректері аса ретсіз болуы керек. Себебі оған сәл өзгерістер жасалғанда контейнер деректерінің қасиеті аса байқалмауы қажет. Контейнерлердің келесі түрлері болуы мүмкін:

1) стегожүйе генерациялаған контейнерлер;
2) контейнерлер кандай да бір контейнерлер жиынынан таңдалады;
3) контейнер сырттан алынады;
4) ретсіздік сипаттамаларын модуляциялау арқылы алынған контейнерлер.



6.5-сурет. Жалпылама стегожүйе схемасы

Криптография сияқты барлық стегожүйелердегі стегокілттер типтері бойынша 2 түрге бөлінеді:

– құпия кілттермен;
– ашық кілттермен.

Құпия кілтті стегожүйелерде бір ғана кілт қолданылады. Ол құпия хабарлармен алмасу алдында анықталады, не болмаса қорғалған арна бойымен беріледі. Ашық кілтті стегожүйелерде хабарды салу және шығарып алу үшін екі кілт қолданылады. Екеуі бір-бірінен тәуелсіз болу керек. Сол себепті бір кілт (ашық кілт) қорғалмаған байланыс арнасымен беріледі. Сонымен қатар, бұл жүйе жіберуші мен қабылдаушы арасындағы шынайылықты дәлелдеуде тиімді.

Ақпаратты қорғау деңгейінің санына байланысты стегожүйеде бір немесе бірнеше стеганографиялық кілттер болуы мүмкін.

Стеганография қолданбаларының негізгі үш бағыты:

– деректерді жасыру;

– цифрлық су таңбалары.

Үлкен көлемдегі деректерді жасыру үлкен көлемді контейнердің болуын талап етеді. Контейнер көлемі хабар көлеміне қарағанда бірнеше есе болуы керек.

Цифрлық су таңбалары цифрлық бейнелерге фотосуреттер немесе басқа цифрлық түрге түрлендірілген өнер туындыларына авторлық немесе мүліктік қорғау құқықтарын қолдану мүмкіндігін береді.

Тақырыптар цифрлық бейнелер, аудио және бейне файлдарды үлкен электрондық қоймаларда (кітапханалар) бейнелерді таңбалау үшін пайдаланылады.

Стеганографиялық жүйелердің міндеттері. Ақпараттық қауіпсіздікті талдау нәтижелерінің көрсетулері бойынша стеганографиялық жүйелер келесі негізгі мәселелерді шешу үшін пайдаланылады:

– жасырын ақпаратты рұқсатсыз қатынас құрудан қорғау;
– тораптық қорғауды басқару және бақылау жүйелерін жеңу;
– программалық қамтамасыз етуді қалқалау;
– кейбір интеллектуалдық меншік түрін өзгерту түрлерінің авторлық құқықтарын қорғау.

6.4.3. Компьютерлік стеганография әдістерінің жүзеге асырылуы

Хабарларды қыстырудың бірнеше әдістері бар (6.6-сурет).

6.6-сурет. Компьютерлік стеганография әдістері

Бүгінгі күні компьютерлік стеганография әдістері негізгі екі бағыт бойынша дамуда:

- компьютерлік форматтың арнайы қасиеттерін пайдалануға негізделген әдіс.
- дио және бейне ақпараттың артықтығына негізделген әдіс.

Стеганографиялық мақсатта пайдаланатын түрлі программалық өнімдер бар. Олар графикалық, аудио және бейне файлдарға хабарларды салуды жүзеге асырады. Олар өте ыңғайлы түрде ұйымдастырылған. Мысал келтірсек StedoDos, WNS, S-Tools for Windows v. 3. 00, Covert_TCP 1.0, HidSeek v 5.0

Бақылау сұрақтары

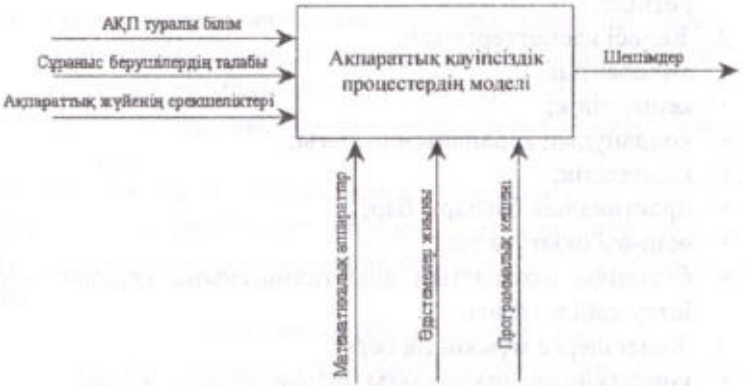
1. Криптология қандай мәселемен айналысады?
2. Криптография дегеніміз не?
3. Криптоталдау дегеніміз не?
4. Криптографиялық жүйе дегеніміз не?
5. Криптоберіктілік деп нені түсінеміз?
6. Имитотұрақтылық деген не?
7. Стеганография деген не?
8. Стеганография мен криптографияның айырмашылықтары қандай?
9. Стеганографияның тарихынан не білесіз?
10. Стеганографиялық жүйе деген не?
11. Стегоконтейнердің қандай түрлерін ажыратады?

7 Ақпаратты қорғау дұрыстығының әдістемесі

7.1. *Қорғау жүйелерінің дұрыстығын зерттеу және қорғауды зерттеу мен жобалаудың әдістемесі*

Қазіргі кезде ақпаратты, оның маңыздылығына немесе құпиялылығына байланысты қорғауға көп көңіл аударуда. Соған қарамастан ақпаратқа көптеген шабуылдар жасалынады және ол көп жағдайларда жүзеге асады. Осындай шабуылдарға қарсы тұру үшін ақпаратты қорғау модельдері жасалынады. Модель қорғаудың неғұрлым көп жақтарын қарастырса, солғұрлым қорғаныс төзімді болады.

Осы оқу құралында В. Доморев құрастырған модельді қарастырамыз. Жалпы модельдің схемасын төмендегі суретпен бейнелеуге болады. Ақпаратты қорғауды жүйе түрінде қарастырған.



7.1-сурет. Ақпаратты қорғау жүйесінің моделі

Модельдің негізгі есебі ретінде ақпараттық қорғау жүйесін жасау процесін ғылыми қамтамасыз ету болып табылады. Бұл процесті қамтамасыз ету үшін қатынас шешімдердің тиімді бағалауын

пайдалану және техникалық жабдықтарды дұрыс іске асыруына байланысты. Осындай жүйені құру ерекшеліктері төмендегідей:

1. Ақпараттық жүйе туралы бастапқы мәліметтердің белгісіздігі және толық еместігі, осымен қатар қауіп-қатерлер туралы сипаттамалардың белгісіздігі және ақпараттардың толықтығы. Есептің көп шарттылығы, яғни жүйені құрастыру барысында көп көрсеткіштерді есепке алу.
2. Ақпаратты қорғау жүйесін жасау мен іске асыру кезінде сапалы және сандық көрсеткіштерді есепке алу.
3. Классикалық ұтымды әдістерді қолдануға болмауы.

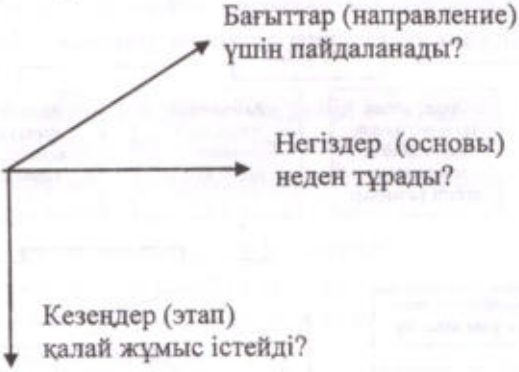
Модельге қойылатын талаптар:

Жоғары көрсетілген модель келесі талаптарды қанағаттандыру қажет:

1. Келесілерге пайдалану:
   - ақпараттық қорғау жүйесін құруға нұсқау;
   - ақпаратты қорғау жүйесіндегі көрсеткіштер мен талаптарды қалыптастыру әдістемелері;
   - ақпаратты қорғау жүйесін бағалау құралы;
   - зерттеулерді жүргізуге ақпаратты қорғау жүйесінің моделі ретінде.
2. Келесі қасиеттерге тән:
   - әмбебаптық;
   - кешенділік;
   - қолданудың қарапайымдылығы;
   - көрнекілік;
   - практикалық бағдары бар;
   - өзін-өзі оқытуға тән;
   - бастапқы ақпараттың анықталмағанына қарамай жұмыс істеу қабілеттілігі.
3. Келесілерге мүмкіндік беру:
   - көрсеткіштер арасындағы байланыстарды жасау;
   - әр түрлі қорғау деңгейлерін беру;
   - сандық бағаларды беру;
   - ақпаратты қорғау жүйесінің қауіпті күйін бақылау;
   - әр түрлі баға беру әдістемелерді қолдануға мүмкіндік беру;

- жұмыс істеу ортаның өзгеруіне жедел әрекет жасау;
- әр түрлі мамандарды проблеманы шешуге біріктіру.

Модельдің кеңістіктегі координаталары төменгі 7.2-суреттегідей анықталады.



7.2-сурет. Модельдің координаталары

Кез келген күрделі жүйенің соның ішінде ақпаратты қорғау жүйенің *негіздері* ретінде келесілер болып табылады:

1. Ғылыми нормативтік құқықтық және заңдылық базасы.
2. Ақпараттық технологиялардың қауіпсіздік қамтамасыз ететін ұжымдардың есептерімен құрылымы.
3. Ұйымдастырушылық-техникалық және режимді шаралар әдістері.
4. Программалық-техникалық тәсілдер мен құралдары.

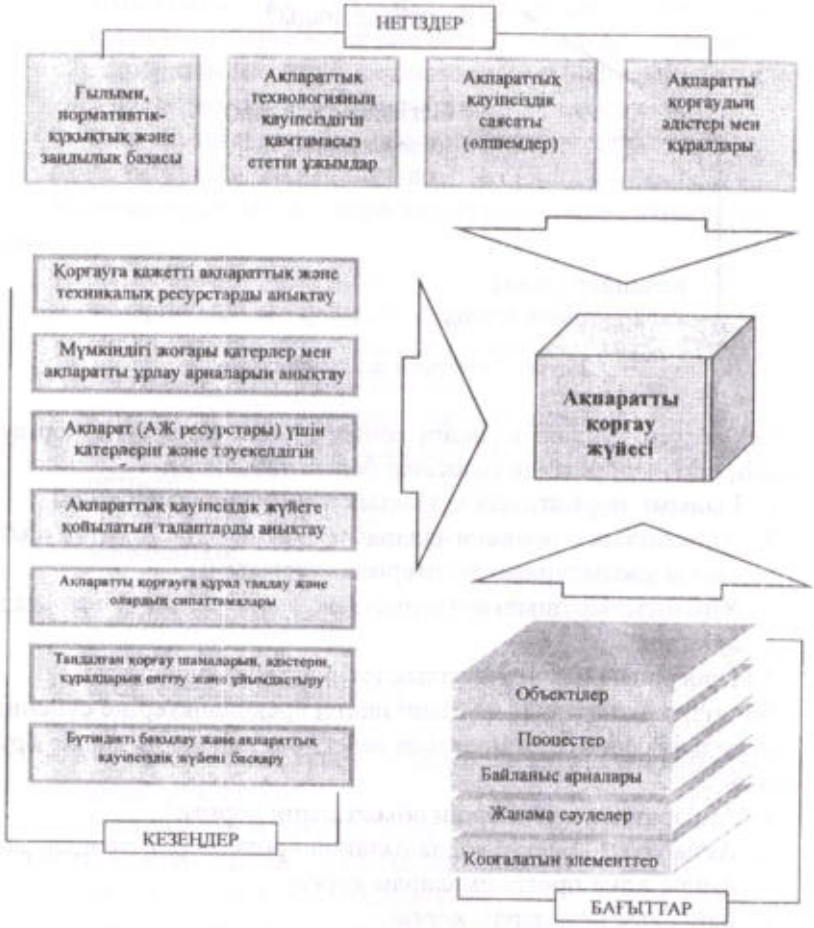
Бағыттар ақпараттық жүйенің нақты ерекшеліктеріне сүйеніп қалыптастырылады. Бұл модельде келесі *бағыттарды* қарастыру ұсынады:

1. Ақпараттық жүйелердің объектілерін қорғау.
2. Ақпаратты өңдеуге қолданылатын процестерді, процедураларды және программаларды қорғау.
3. Байланыс арналарды қорғау.
4. Жанама электромагниттік сәулелерді басу.

Келесі *кезеңдер* ұсынады:

1. Қорғауға жататын ақпараттық жүйенің объектілерін ақпараттық және техникалық қорларды анықтау.

2. Ақпараттық негізгі бағытынан тыс кету арналарды және толық мүмкіндік қауіп-қатерді табу.
3. Ақпараттық қауіп төнетініне баға беру.
4. Ақпаратты қорғау жүйесіне қойылатын талаптарды анықтау.



7.3-сурет. Ақпараттық қорғау моделі қолданылатын объект

5. Ақпаратты және олардың сипаттамаларын қорғауға құралдарды таңдап алу.

6. Таңдалған шараларды, тәсілдер мен қорғау құралдарын ұйымдастыру және енгізу.
7. Қорғау жүйесінің басқаруын және бүтіндігін бақылауын іске асыру.

Бұл модельде жүйені сипаттайтын көрсеткіштер үш өлшемді матрицамен берілген, мұнда әр координата кеңістіктің әр бағытын білдіреді:

X00 – кезең, X – 1-ден 7-ге дейін өзгереді.

0X0 – негіз, X – 1-ден 4-ке дейін өзгереді.

00X – бағыт, X – 1-ден 5-ке дейін өзгереді.

Мысалы:

300 – бұл ақпараттық қауіп төнетініне баға беру,

020 – ақпаратты өңдеуге қолданылатын процестерді, процедураларды және программаларды қорғау.

001 – нормативтік базасы.

Ал, матрицаның 321 деген координатасы – Ақпараттық жүйелер мен процестердегі ақпаратқа төнетін қатерлер мен тәуекелділіктерді бағалауға қолданыладын мәселелерді заңдылық, әдістемелік және нормативті құжаттарда жазу.

7.2. *Ақпараттың бүтіндігін сақтау*

Жүйенің компонентінің бүтіндігі дегеніміз тек қана осы компонентке байланысты құқығы бар субъект оны өзгерте алады. Бүтіндік компоненттің кез келген уақытта жұмыс істей алатынына кепілдік бере алады.

Ақпаратты қорғау барысында көп сервистер (қызметтер) қолданылады.

1. Хаттамалау дегеніміз – ақпараттық жүйеде болған және болып жатқан оқиғалар туралы ақпараттарды жинау және теріп жинақтау. Кез келген сервистер әр түрлі оқиғалар жиынын кездестіруге болады. Олар келесіге бөлінеді:

- *Сыртқы* – басқа сервистің әсерінен пайда болған оқиға.
- *Ішкі* – сервистің өзінің іс-әрекетінен пайда болған оқиға.

• *Клиенттік* – администраторлармен қолданушылардың іс әрекетінен пайда болған оқиға.

2. *Аудит* – жиналған ақпаратқа жедел немесе мерзімді талдау жүргізу. Аудит екі түрге бөлінеді:

• активті аудит;
• пассивті аудит.

Сервиске тыс пайда болған оқиғаға жедел аудит жүргізілсе, онда ол аудит түрі белсенді аудит деп аталады.

Хаттамалау мен аудит келесі мәселелерді шешеді:

• қолданушылар мен администратордың есеп беруін қамтамасыз етеді;
• оқиғалардың тізбектелуін қайтадан құруына мүмкіндік береді;
• ақпараттық қауіпсіздіктің бұзуына әсерлерін табуға мүмкіндік береді;
• проблемаларды табу және талдауға ақпараттарды береді.

Сенімді компьютерлік жүйелердің бағалау шарттарын 1983 жылы Пентагон ұсынған. Бұл кітапта келесі оқиғалар ерекшелінген:

• жүйеге кіру;
• жүйеден шығу;
• алыс қашықтықтағы жүйеге қатынас жасау;
• файлдарға қолданатын операциялар;
• қауіпсіздіктің атрибуттарын немесе артықшылықтарын ауыстыру.

Оқиғаларды хаттамалау барысында келесі ақпараттарды жазу керек:

• оқиғаның күні мен уақыты;
• қолданушының өзіне сай идентификаторын;
• оқиғаның түрін;
• іс-әрекеттің нәтижесін;
• сұраныстың қайнар көзін;
• іс-әрекеттің жасалынған объектілердің атауы;
• қорғаныстың деректер базасына негізделген өзгерістерді сипаттау.

Шабуыл сигнатурасы дегеніміз – бұл шабуыл жасалатын және нақты орындалатын шарттар жиыны.

Активті аудитте келесі функционалдық компьютерді ажыратуға болады:

1. Тіркеу ақпараттарын генерациялайтын компьютер. Бұл компьютер белсенді аудит пен бақылау объектілер қиылысында жатады.
2. Генерацияланған тіркеу ақпараттарын сақтау компьютері.
3. Тіркелген ақпараттарды алу компьютері немесе оларды сенсор деп атайды. Әдетте желілік және хостық сенсорларды ажыратады. Желілік сенсорлар дегеніміз – желі карталарды тыңдау режиміне қойылған ерекшелінген компьютерді атайды. Хостық сенсорлар – операциялық жүйедегі тіркеу журналдарын оқуға арналған программалар.
4. Тіркелген ақпаратты қарап шығу компьютері.
5. Сенсорлардан келген ақпаратты талдау компьютері. Бұл жерде қауіп саясатын бұзатын оқиғаларды зерттеу анализаторы. Шабуыл сигнатураларды табатын сараптамалық жүйе және статикалық талдағыш (анализатор).
6. Талдауға пайдаланылған ақпараттарды сақтау компьютері.
7. Шешімдерді қабылдау және оны іске асыру компьютері.
8. Бақылауға алынған объектілері туралы ақпараттарды сақтау.
9. Интерфейстік компьютер.
10. Қауіпсіздік администратордың жүйемен байланыс жасайтын интерфейс компьютері.

Белсенді аудиттің құралдары менеджер архитектурасында пайдалана отырып құрылады. Негізгі агенттік компоненттер сенсорлар болып табылады. Ал, шешімдерді қабылдауын талдау бұл менеджерлер функциялары. Менеджерлер мен агенттер арасында сенімді арналар қалыптастырылуы қажет.

Криптографиялық әдістер деректердің кейбір бөліктерінің бүтіндігін және сол бөліктер жиынының бүтіндігін бақылауға мүмкіндік береді. Осымен қатар бұл әдістер деректердің қайнар көзінің шынайылығын анықтайды және іс-әрекеттерін нақты

орындауға бас тартпауына кепілдік береді. Бүтіндікті тексеру криптографиялық бақылау арқылы жүргізгенде екі ұғым пайдаланылады:

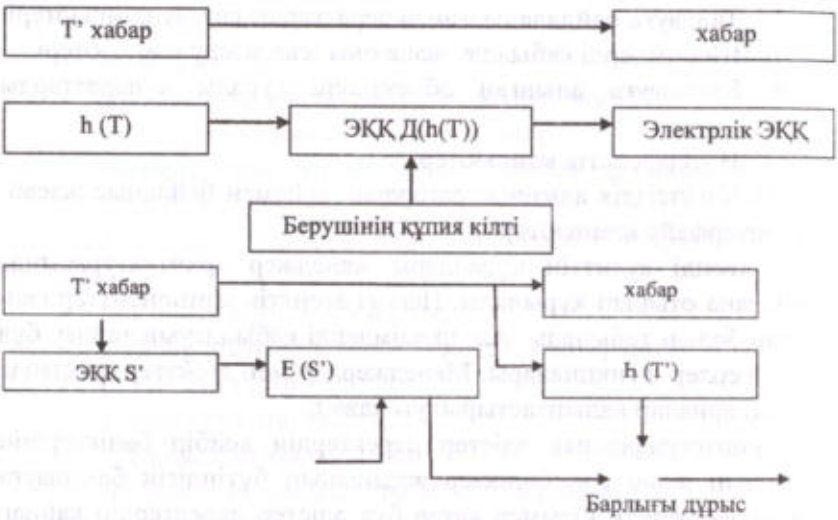
1. ХЭШ – бір бағытты функция.
2. Электрондық цифрлы қолтаңба.

ХЭШ функция блоктарды өзара байланыстыруда симметриялық шифрлау құралдары арқылы іске асырылады. Соңғы блоктың шифрлау нәтижесі ХЭШ функцияның нәтижесі болып саналады. Айталық, бүтіндігін тексеруге керек деректер бар деп. ХЭШ функция және оның алдын ала берілген деректерге қолдану нәтижелері бар. ХЭШ функцияны n деп белгілейміз, бастапқы мәліметтерді – Т, тексерілген мәліметтер –Т1.

$$h(T) = h(T1) => T = T1$$

Көп жағдайда дайджестердің бір-біріне сәйкес келуі коллизия деп аталады. Айталық, Е(Т) ашық кілт көмегімен Т хабарды шифрлау нәтижесі, ал Д(Т) жабық кілт көмегімен Д(Е) кері шифрлау нәтижесі. Асимметриялық әдіс электрондық қол қою іске асыруға пайдаланады дегеніміз – ол келесі тепе-теңдіктің орындалуы.

$$Е (Д (Т)) = Д (Е(Т)) = Т$$



7.4-сурет. Электрондық қолтаңбаның қалыптасуы

Цифрлық сертификаттар

Асимметриялық шифрлау әдісін пайдалану барысында екі параметрдің (қолданушының атауы және қолданушының ашық кілті) растығына кепілдік болуы қажет. Бұл мәселені шешуге x.509 спецификациясында келесі ұғымдар енгізіледі:

1. Цифрлық сертификат.
2. Растайтын орталық.

Растайтын орталық дегеніміз – бұл ауқымды каталогтар қызметінің компоненті. Ол қолданушылардың криптографиялық кілттерін басқаруға жауап береді. Ашық кілттер және қолданушылардың басқа ақпараттары растайтын орталықтарда цифрлық сертификаттар түрінде сақталады. Сертификат құрылымы келесідей.

1. Сертификаттың реттік нөмірі.
2. Электрондық қолтаңба алгоритмінің идентификаторы.
3. Растайтын орталықтың атауы.
4. Жарамды мерзім.
5. Сертификаттың иесінің аты.
6. Сертификаттың иесінің ашық кілттері.
7. Сертификаттың иесінің ашық кілттерге сәйкес алгоритмдердің идентификаторы.
8. Растайтын орталыққа құпия кілтпен жасалған электрондық қолтаңба.

Цифрлық сертификаттарға келесі қасиеттер тән:

1. Кез келген қолданушы растайтын орталықтың ашық кілтін біле отырып, басқа қолданушылардың ашық кілттерін біле алады және сертификат бүтіндігін тексере алады.
2. Растайтын орталықтан басқа бірде біреу сертификаттың бүтіндігін бұзбай қолданушы туралы ақпаратты өзгерте алмайды.
3. X.509 спецификацияларында криптографиялық кілттердің жасалу процедурасында және кілттерді басқару туралы нақты операциялар бейнеленбеген. Бірақ та кейбір жалпы ұсыныстар берілген.

Мысалы: екінші кілт келесі әдістермен жасалады деп көрсетілген:

1. Кілтті қолданушы өзі жасай алады.
2. Кілттерді сенімді адам жасай алады.
3. Кілттерді сенімді орталық жасай алады.

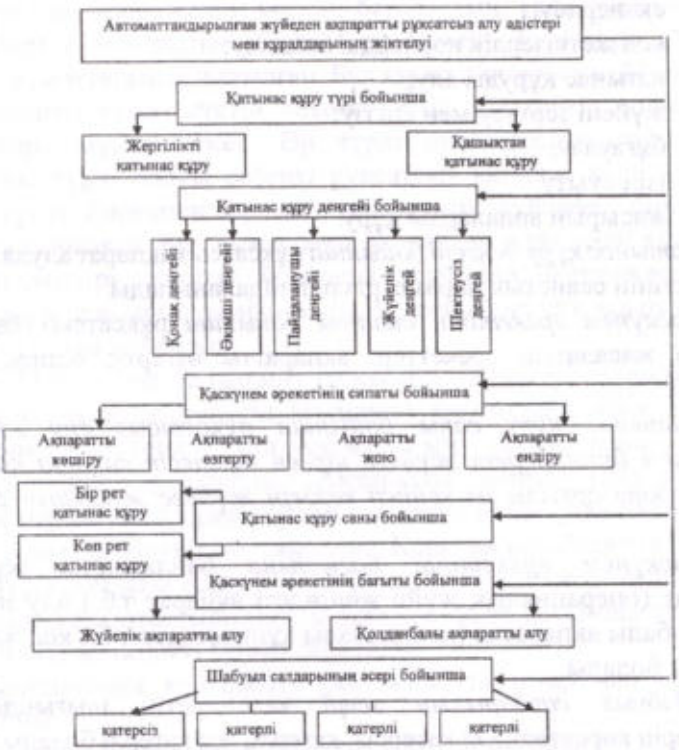
Бақылау сұрақтары

1. Модельдің негізгі элементтері қандай?
2. Модельдегі бағыттар не анықтайды?
3. Модельдегі кезеңдер не анықтайды?
4. Модельдегі негіздер не анықтайды?
5. Модельге қойылатын талаптар қандай?
6. Ақпараттың бүтіндігін сақтауға қандай сервистер пайдаланылады?
7. Аудит сипаттамасы.
8. Шабуыл сигнатурасы деген не?
9. Растайтын орталық дегенді қалай түсіндіресіз?
10. Хэш функция деген не?

8. Ақпаратты рұқсатсыз алу әдістеріне және ақпараттың қорғанышына қойылатын талаптар

8.1. Ақпаратты рұқсатсыз алу әдістеріне шолу

Ақпараттық қауіпсіздік мәселесінің ең осал жері ақпаратқа рұқсатсыз қатынас құру болып табылады. 8.1-суретте автоматтандырылған жүйеден ақпаратты рұқсатсыз алу әдістері келтірлген.



8.1-сурет. Автоматтандырылған жүйеден ақпаратты рұқсатсыз алу әдістері мен құралдарының жіктелуі

Мұндағы бөлімдерге түсіндірме беріп өтейік.

Жергілікті қатынас құру арқылы жасалатын әрекеттер:

- ұрлау арқылы ақпарат алу;
- заңды пайдаланушының ашық сеансын пайдалану;
- заңды пайдаланушының құпиясөзін тауып пайдалану;
- өкілеттігін кеңейту үшін заңды пайдаланушының тіркеу жазбасын пайдалану;
- таңдаған операциялық жүйені тасымалдаушыдан жүктеу арқылы жүйеге кіру.

Қашықтан қатынас құру. Бұл әдіс келесі процедуралар тізбегі бойынша орындалады:

- ақпарат жинау;
- сканерлеу;
- қол жеткізерлік қорларды анықтау;
- қатынас құруды алу;
- жүйені зерттеу мен енгізу;
- бұғаулау;
- ізін суыту.
- жасырын арналарды құру.

Қатынас құру деңгейі бойынша рұқсатсыз ақпарат алуда заңды субъектінің сеанстық параметрлері пайдаланылады.

Қаскүнем әрекетінің сипаты бойынша рұқсатсыз қатынас құруда жасалатын әрекеттер: ақпаратты өзгерту, өшіру, жою, көшіру.

Қатынас құру саны бойынша рұқсатсыз ену әдісінде қаскүнем бірінші рет жүйеге кірген нүктесін сақтап қалады. Осы нүкте арқылы ол кейінгі кездері жүйеге жасырын енетін болады.

Қаскүнем әрекетінің бағытына байланысты жүйелік ақпарат (операциялық жүйе жөніндегі ақпарат т.б.) алу немесе қолданбалы ақпаратқа (қолданбалы құпиясөздер т.б.) қол жеткізу мүмкін болады.

Шабуыл салдарының әсері келтірілетін шығындардың мөлшерін көрсетеді. Ол қатерсіз, қатерлі, аса қатерлі болады. Яғни салдары ауыр болған сайын келтірілген шығындар жоғары және жүйені істен шығару әрекеті аса сәтті болады.

Компьютерлік ақпараттың қорғанышына қойылатын талаптар

Жалпы қорғаныш жүйесіне қойылатын екі түрлі талап бар:

1. Бірінші топтың талаптары (қажетті талаптар) – қауіпсіздіктің формалды шаралары. Ақпараттық жүйенің қорғанышының қажетті тетіктеріне қойылатын формалды талаптар Ресей мемлекеттік техкомиссияның басқарушы құжаттарында жазылған. «Қызғылт сары кітап» – сенімді компьютерлік жүйелерді бағалау критерийлері жайында болады (АҚШ қорғаныс министрлігі). Ақпараттық жүйелердің қаупін бағалаудың сәйкестелген критерийлері – Information Technology Sewrity Evaluation Criteria, ITSEC құжаттарында жазылған. Бұл құжаттың мақсаты бір. Мұнда қорғанышты қажет ететін объектілердің жіктелімін толығымен қарастыру мүмкін емес. Әр түрлі операциялық жүйелердің құрылуы түрлі болуы себепті рұқсатсыз қатынас құру әдістері де әр түрлі. Дегенмен барлық операциялық жүйелерге бірдей талаптар қойылған. Бұл құжаттарда қорғалған жүйелерді құру мен әкімшілдендіру әдістері бойынша ұсынулар берілмеген, яғни ненің жүзеге асырылуы айтылады, ал «қалай жүзеге асыру керек» деген сұраққа жауап жоқ.

2. Екінші топ талаптары (қосымша талаптар) – нақты қорғалатын объектіге төнетін ағымдағы қауіптердің және мүмкін болатын қауіптердің статистикасының есептеулерін ескеру қажеттілігінен туындайды. Ақпаратты қорғау облысындағы сәйкес нормативтік құжаттармен анықталатын формалды талаптар жиынтығы қажетті болып саналады. Қорғалатын объектіге төнетін қауіптер ағымдағы есебі және мүмкін болатын қауіптерді талдау негізінде қалыптастырылған формалды және қосымша талаптар жиынтығы жеткілікті болып саналады.

Қорғанышқа қойылатын формалды талаптар мен олардың жіктелімі:

Есептеу техникалық құралдарына қойылатын талаптар – операциялық жүйе, дерекқорларды басқару жүйесі (ДҚБЖ) және қолданба сияқты жеке құралдардың қорғалу жағдайын құрайды.

Автоматтандырылған жүйенің қорғанышына қойылатын талаптар төмендегіні ескере отырып, объектінің қорғанылу жағдайын береді:

- қорғалған объектіде орнатылған құралдардың операциялық жүйе (ОЖ), дерекқорларды басқару жүйесі (ДҚБЖ), қолданба, үстемеленген қорғаныш тетіктерін қоса алғанда, қорғаныш тетіктерінің жиынтығы;
- автоматтандырылған жүйенің қауіпсіз қызмет етуі үшін жасалатын қосымша ұйымдастырылған шаралар.

Қолданбалар операциялық жүйенің қорғаныш тетіктерін пайдаланады. Ал деректер базаларын басқару жүйесінің қорғаныш тетіктері операциялық жүйенің қорғаныш тетіктерін толықтырады, өйткені деректер базаларын басқару жүйесінде қатынас құрудың қосымша объектісі – кестелер бар. Операциялық жүйе үшін қорғалатын файлдық объектілер: логикалық дискілер (томдар), хаттамалар, файлдар. Ал кестелер (бірнеше парақтан болсын) бір файлда орналасуы мүмкін. Мұндайда операциялық жүйе қорғаныш тетіктері арқылы деректер базаларына қатынас құруды басқару мүмкін емес. Дегенмен бұл тек деректер базаларын басқару жүйесіне қатысты. Басқа қолданбалар операциялық жүйе қорғаныш тетіктерін пайдаланады. Яғни, автоматтандырылған жүйенің барлық тетіктері келісім бойынша операциялық жүйе арқылы жүзеге асырылады.

Автоматтандырылған жүйеге қойылатын талаптар есептеу техникалық құралдарға қойылатын талаптарға қарағанда қатаңдау. Талаптардан келесідей қорғаныш тетіктері туындайды:

- қатынас құруды басқару тетіктері (ҚҚБТ);
- тіркеу және есепке алу тетіктері;
- криптографиялық қорғаныш тетіктері;
- тұтастықты бақылау тетіктері.

Қатынас құруды басқару компьютерлік ақпаратты рұқсатсыз қатынас құруға қарсы тұрудың амалы. Қалған үш топ мыналарға қарсы тұрады:

- пайдаланушы әрекеттерін бақылау үшін;
- ұрланған ақпараттар жасырылуы;

- объектінің өзгерілуін айқындау, қосар көшірмелерден қорғалатын ақпараттық қосымша келтіру тұтас бақылау типі.

Жасырын ақпаратқа қойылатын талаптар

Қатынас құруды басқарудың ішкі жүйесі келесі талаптарды қанағаттандыруы тиіс:

1. Жүйеге кірерде пайдаланушылардың шынайылығын анықтау және тексеру.
2. Терминал, ЭЕМ, компьютерлік торап түйіндерін, байланыс арналарын, логикалық мекені бойынша ЭЕМ-нің сыртқы құрылғыларын анықтау.
3. Программаларды, томдарды, каталогтарды, файлдарды, жазбаларды және жазба өрістерін атаулары бойынша іздеу.
4. Хаттамаларды құру матрицасына сәйкес қорғалған ресурстарға субъектілердің қатынас құруын бақылауды жүзеге асыру.

Тіркеу мен есепке алудың ішкі жүйесі мыналарды қамтамасыз етуі тиіс:

1. Субъектілердің жүйеге кіріс, шығысын тіркеу, операциялық жүйе жүктелуі мен инициализациясын және программаның тоқтауын тіркеу. Сонымен қатар параметрлерде төмендегілер көрсетіледі:

- субъектілік жүйеге кіріс, шығыс уақыты мен жүктелу мен тоқтау уақыты;
- кіру пиғылының нәтижесі – сәтті және сәтсіз (НСД) болуы;
- қатынас құру берілгенде көрсетілген идентификатор;
- сәтсіз пиғыл болғанда көрсетілген коды немесе құпиясөз.

Автоматтандырылған жүйе өшірілгенде жүйеден шығу және тоқтау оқиғалары тіркелмейді.

2. Құжаттарды баспаға шығаруды тіркеу. Тіркеу параметрлерінде төмендегілер көрсетіледі :

- шығу уақыты (шығару ішкі жүйесіне қатынау);
- құжаттың қысқаша мазмұны;
- баспа құрылғысының айқындамасы;
- құжатты сұраған қатынас құру субъектісінің идентификациясы.

3. Қорғалған файлдарды өңдеуге арналған программалық және процестердің жүктелуін тіркеу.

Тіркеу параметрлері :

- жүктеу уақыты;
- программа, аты;
- программаны сұраған қатынас құру субъектісінің идентификациялары;
- жүктеу нәтижесі (сәтті, сәтсіз, рұқсатсыз).

4. Қорғалған файлдарға программалық құралдардың қатынас құру пиғылын тіркеу. Параметрлері:

- қорғалған файлға қатынас құру пиғылының уақыты;
- қорғалған файлдың айқындамасы.

5. Қосымша қатынас құру объектісіне қатынас құру пиғылын тіркеу.

Қорғалған қосымша қатынас құру объектісі: терминал, ЭЕМ, ЭЕМ торабы түйіндері байланыс арналары. ЭЕМ сыртқы құрылғылар, программалар, том, каталог, файл, жазба, жазба өрістері. Параметрлері:

- қорғалған файлға қатынас құру пиғылы;
- сәтті, сәтсіз, рұқсатсыз нәтижесін көрсету;
- қатынас құру субъектісінің идентификаторы;
- қорғалған объектінің айқындамасы.

6. Барлық қорғалған тасымалдаушыларды маркерлеу, журналға тіркеу деректерін түсіру арқылы есепке алуды жүзеге асыру.

7. Қорғалған тасымалдаушыларды беру, алуды тіркеу.

8. ЭЕМ-нің босаған оперативтік жадысы және сыртқы жинақтағыштарды тазалауды орындау.

Құпия ақпараттарды қорғауға қойылатын талаптар

Қатынас құруды басқару ішкі жүйесі мыналарды қамтамасыз етуі тиіс:

- жүйеге енер алдында субъектінің шынайылығын тексеру;
- терминал егер компьютерлік торап түйіндерін, байланыс арналарын, логикалық мекені бойынша ЭЕМ сыртқы құрылғыларын анықтау;
- программаларды, томдарды, каталогтарды, файлдарды, жазбаларды және жазба өрістерін атаулары бойынша іздеу;

- хаттамаларды құру матрицасына сәйкес қорғалған ресурстарға субъектілердің хаттамаларын құруды бақылау жүзеге асырылады;
- құпиялылық таңбалары көмегімен ақпарат ағынын басқару. Мұнда жинақтаушының құпиялылық таңбасы оған жазылатын ақпараттың құпиялылық таңбасынан төмен болмауы тиіс.

Тіркеу және есепке алу ішкі жүйесі мынаны қамтамасыз етуі тиіс:

1. Субъектілердің жүйеге кіріс, шығысын тіркеу, операциялық жүйе жүктелуі мен инициализациясын тіркеу. Сонымен қатар параметрлерде көрсетіледі:

- субъектілік жүйеге кіріс, шығыс уақыты мен жүктеуді тоқтату уақыты;
- кіру пиғылының нәтижесі – сәтті және сәтсіз;
- қатынас құру берілгенде көрсетілген идентификатор;
- сәтсіз пиғыл болғанда көрсетілген коды және құпия сөздер ақпараттық жүйе өшірілгенде жүйеден шығу және тоқтату болмайды;

2. Құжаттарды баспаға шығаруды тіркеу. Тіркеу параметрлерінде көрсетіледі :

- шығу уақыты (шығару ішкі жүйесіне қатынау);
- құжаттың қысқаша мазмұны;
- баспа құрылғысының айқындамасы;
- құжатты сұраған хаттамалық құру субъектісінің идентификациясы;
- шығарылған құжаттың көлемі.

3. Қорғалған файлдарды өңдеуге арналған программалық және процестердің жүктелуін тіркеу. Тіркеу параметрі:

- жүктеу уақыты;
- программа, аты;
- программаны қамтамасыз ету субъектісінің идентификациялары;
- жүктеу нәтижесі (сәтті, сәтсіз, рұқсатсыз).

4. Қорғалған файлдарға программа құралының хаттаманы құру пиғылын тіркеу. Параметрлері:

- қорғалған файлға қатынас құру пиғылының уақыты;
- қорғалған файлдың айқындамасы;
- файлдарға қатынас құратуды жүзеге асыратын программаның аты немесе процесі, тапсырманың аты;
- сұралып отырған операцияның түрі (оқу, жазу, өшіру, кеңейту, орындау және т.б.).

5. Қосымша қатынас құру объектісіне қатынас құру пиғылын тіркеу қорғалған қосымша қатынас құру объектісі: терминал, ЭЕМ желісі, қосылатын сыртқы құралдар, программалар, томдар, каталогтар, файлдар, жазба өрістері. Параметрлері:

- қорғалған файлға қатынас құру пиғылы;
- сәтті, сәтсіз, рұқсатсыз нәтижесін көрсету;
- қатынас құру субъектісінің идентификаторы;
- қорғалған объектіні анықтау;
- файлдарға қатынас құратуды мүмкіндік беретін программаның аты немесе процесс, тапсырманың аты;
- сұралып отырған операцияның түрі (оқу, жазу, өшіру, кеңейту, орындау және т.б.)

6. Қатынас құру субъектісінің өкілеттілігінің, сонымен қатар қатынас құру объектісінің өзгеруін тіркеу. Тіркеу параметрлерінде мыналар көрсетіледі:

- өкілеттігін өзгерту күні мен уақыты;
- қатынас құру субъектісінің идентификаторы, өзгеріс жасаған әкімші жөніндегі ақпарат.

7. Әрбір құрылған қорғалған файлдарды автоматты түрде есепке алу. Оны қатынас құруды басқару ішкі жүйесінде қолданылатын қосымша таңбалау көмегімен жасайды. Таңбалау объектісінің құпиялылық деңгейі бейнеленуі тиіс.

8. Барлық қорғалған тасымалдаушыларды маркерлеу, журналға тіркеу деректерін түсіру арқылы есепке алуды жүзеге асыру.

9. Қорғалған тасымалдаушылардың алынған/берілген уақытын арнайы журнал (картотека) тіркеуіне есепке алуды жүргізу.

10. Қорғалған ақпараттық тасымалдауыштарды есепке алудың бірнеше түрін жүргізу.

11. ЭЕМ оперативті жады мен сыртқы жинақтауыштардың босаған аймақтарын тазартуды орындау. Ол үстінен екі рет қайталап жазу арқылы жүзеге асады.

12. Қорғанышты бұзу пиғылдары жөнінде әкімшіге дабыл беру.

Тұтастықты қамтамасыз ету ішкі жүйесі мыналарды орындауы тиіс:

1. Өңделіп жатқан ақпараттың және рұқсатсыз қатынас құруға қарсы ақпаратты қорғау құралдарының программалық құралдарының тұтастығын, программалық ортаның орнықтылығын қамтамасыз ету. Мұнда және рұқсатсыз қатынас құруға қарсы ақпаратты қорғау құралдарының тұтастығы жүйе жүктелгенде ақпаратты қорғау құралдары сынарының бақылау қосындысын тексеру арқылы жүргізіледі.

2. Есептеу техникалық құралын физикалық қорғауды қамтамасыз ету керек. Автоматтандырылған жүйе орналасқан үй-жай арнайы жабдықтар мен қатаң өткізу режимі мен арнайы персоналмен қамдалуы тиіс.

3. Рұқсатсыз қатынас құруға қарсы ақпаратты қорғау құралдары жұмысын тексеретін және дұрыс қызмет етуіне жауапты әкімшілер мен ақпарат қорғау қызметінің бар болуы тиіс. Әкімші терминалмен және жылдам бақылау мен автоматтандырылған жүйе қауіпсіздігіне қатысты құралдармен қамтамасыз етілуі қажет.

4. Рұқсатсыз қатынас құруға қарсы ақпаратты қорғау құралдары функцияларын арнайы құралдармен кезең-кезеңмен тексеру керек, программалық орта немесе автоматтандырылған жүйе персоналы өзгерсе тексеру жиілігі жылына бір реттен төмен болмауы тиіс.

5. Рұқсатсыз қатынас құруға қарсы ақпаратты қорғау жүйесі қалпына келтіру үшін оның екі көшірмесін сақтау және оны кезең-кезеңмен жаңартып, жұмыс істеу мүмкіндігін бақылау.

6. Қорғаныш құралдарының тек сертификатталған нұсқаларын пайдалану. Сертификаттау арнайы сертификаттау орталықтарында (СО) немесе сертификаттауға құқығы бар арнайы мекемеде өткізіледі.

Бақылау сұрақтары

1. Қорғаныш жүйесіне қойылатын талаптар қандай?
2. Қатынас құруды басқару дегенді қалай түсінесіз?
3. Жасырын ақпаратқа қойылатын талаптар қандай?
4. Мұндағы тіркеу мен есепке алу ішкі жүйесі нені қамтамасыз етуі керек?
5. Құпия ақпараттарды қорғауға қойылатын талаптар?
6. Тұтастықты қамтамасыз ету ішкі жүйесі нені қамтамасыз етуі керек?

9 DoS шабуылдарының түрлері мен олардан қорғану әдістері

DoS-шабуыл (ағылш. denial of service, қызмет көрсетуден бас тарту) – және DDoS-шабуыл (ағылш. distributed denial of service, үлестірілген қызмет көрсетуден бас тарту) – бұл компьютерлік жүйеге шабуылдардың түрлері. Бұл шабуылдардың мақсаты – жүйені жұмыс істей алмайтындай жағдайға жеткізу, яғни жүйені заңды қолданушылар жүйе ұсынатын ресурстарға кіре алмайтындай немесе кіру мүмкіндігін қиындататын жағдайлар жасау.

DoS шабуылдарының түрлері

DoS шабуылдарының түрлері: Ping of Death, SSPing, Land, Smurf, Syn Flood, CPU Hog, Win Nuke, RPC Locator, Jolt2. Төменде осы DoS шабуылдарының әрқайсысының қалай жүзеге асырылатынын қарастырайық (1-кесте).

Ping of Death. Ұзындығы шамадан тыс дестелерді жіберу арқылы шабуылдау. Мұндай шабуылға ұрынған құрбан машина жұмысын жалғастыра алмайды. Ұзындығы шамадан тыс дестелерді қабылдаған құрбан машинаның операциялық жүйесі ол дестелерді өңдей алмауы себепті тоқтап қалады (зависнет) немесе операциялық жүйе жауап бермей қалады. Осылайша «өлімнің көк қалқасы» пайда болады.

Қорғану тәсілдері. Кейінгі кезде көптеген операциялық жүйелер ұзындығы шамадан тыс ping дестелерін қабылдамайды. Осындай жаңартылған нұсқадағы операциялық жүйелерді пайдалану. Сонымен қатар, ping дестелерін программалары немесе желіаралық экрандар арқылы бұғаулауға болады.

SSPING. Қатты үзінділенген өлшемі үлкен ICMP-дестелерінің тізбегін жіберу арқылы жүзеге асатын DoS шабуылының бір түрі. Ол Windows 95/NT, MAC OS басқаруындағы торапта жұмыс істеп отырған кез келген машинаның жұмысына қатты кедергі келтіреді.

Қорғану тәсілдері. Операциялық жүйелердің жаңартылған нұсқаларын пайдалану. Мұндай шабуылдарды болдырмау үшін Microsoft компаниясы TCP\IP хаттамалар стегін жаңартқан болатын.

LAND. Қабылдаушы мен жіберушінің мекендері мен порттарының нөмірлері бірдей TCP SYN дестелерін жіберу арқылы жүзеге асатын DoS шабуылының бір түрі.

Қорғану тәсілдері:

- операциялық жүйелердің жаңартылған нұсқаларын пайдалану;
- программа сүзгісін IP-адресінің ауыстырылмауына сай баптау.

SMURF. Кеңтаралымды мекенге жіберілетін жалған ICMP дестелерін пайдалану арқылы жасалатын DoS шабуылының бірі.

Мұнда қаскүнем жіберушінің мекенін құрбан болатын машинаның адресіне ауыстырып, кеңтаралымды IP-адресіне ICMP-сұратымдарын (ping) жібереді. Осы сұратымды алған белсенді адресаттардың барлығы жауап дестелерін қайтарады. Осылайша ағын көлемді болып, құрбан-машина қызметтерінің жұмысы нашарлайды немесе осы торап сегменті қызмет көрсетуден бас тартады.

Қорғану тәсілдері. Көріп отырғандай бұл шабуыл үш жақ арқылы жүзеге асады. Олар құрбан-компьютер, ортадағы машина (кеңтаралымды IP-адрестегі адресаттар) және қаскүнем. Практикада мұндай шабуылдарды болдырмау мүмкіндігіне ортадағы машина ие болады. Ортадағы машина үшін шешім: кеңтаралымды мекендерге арналған дестелерді программаларда бұғаулау және операциялық жүйені кеңтаралымды IP-мекендерге арналған ICMP дестелерін қабылдамайтындай етіп баптау.

SYN FLOOD – SYN ДЕСТЕЛЕРІМЕН ТОЛТЫРУ. Қаскүнем байласуды орнату үрдісін үзіп, көптеген жартылай ашық TCP/IP-байласуларын тудырады.

Қорғану тәсілдері. Жартылай ашық байласулардың санын шектеу арқылы желіаралық экрандар немесе программаларды бұғаулау. Шабуылды анықтау үшін netstat программасын пайдалануға болады. Ол барлық жартылай ашық байласуларды көрсетеді.

CPU HOG. Барлық қорларды жұмсай отырып, қызмет көрсетуден бас тартуды жүзеге асыратын DoS шабуылының бір түрі.

Қорғану тәсілдері. CPU Hog программасының жүктелгендігін білу үшін қауіпсіздік аудитін қосу керек. Мұнда қауіпсіздік саясаты мен процестердің өзгеруін қадағалау қажет. Сонымен қатар, CPU Hog файлының жүктелгендігі арқылы шабуылды оңай табуға болады. Машина мұндай шабуылдарға қарсы тұру үшін Microsoft компаниясының жаңартуларын қолдану керек. Сондай-ақ тапсырмалар қадағалауышына ең жоғары (16-дәреже) артықшылық дәрежесін тағайындау арқылы қызмет көрсетуден бас тартуды болдырмауға болады.

WIN NUKE. Операциялық жүйе үшін еш мағынасы жоқ дестелерді жіберу арқылы шабуылдау. Қаскүнем WinNuke программасын пайдаланып, құрбан-машинаның 139-портына арнайы TCP/IP командасын жібереді. Ол команда (Out of Band – OOB) өткізу жолағын толтыру ретінде белгілі. OOB деректері операциялық жүйе күтпеген деректерге жатады. Бұл программада қаскүнем құрбан-машинаның IP-мекенін енгізіп, «nuke» батырмасына басса болғаны құрбан-машина авариялық хабар шығарып, қызмет көрсетуден бас тартады.

Қорғану тәсілдері. Microsoft компаниясының жаңартуларын үстемелеу.

RPC Locator. 135-портқа деректерді жіберу арқылы орталық санашықты 100 пайызға жүктемелеу жолымен жасалатын шабуыл түрі.

Қорғану тәсілдері. Мұндай шабуылдан қорғану үшін Windows NT ОЖ жаңартуларын орнату керек. Оны келесі мекеннен жүктеуге болады:

Jolt2. Бірегей үзінділенген IP-дестелерді құрбан-машинаға көптеп жіберу арқылы жүзеге асырылатын DoS шабуылының бір түрі. Jolt2 шабуылы арқылы үзінділенген IP-дестелерді көптеп жіберу жолымен орталық санауышты 100 пайызға жүктеп, көптеген операциялық жүйелерді шабуылдауға болады.

Қорғану тәсілдері. Байласу күйін тексеретін, дестелерді сүзгілейтін желіаралық экрандарда дестелер тұтастығына

қойылатын тест шабуылды таба алады. Дегенмен дұрыс күйге келтірілмеген брандмауердің өзі DoS-шабуылына ұрынуы мүмкін. Сол себептен өндірушінің жаңа толықтырғыштарын алып, брандмауерді дұрыс күйге келтіре білу керек. Сонымен қатар, пайдаланылмайтын порттарды жабу. Операциялық жүйелерді үнемі жаңартулармен қамтып отыру керек.

9.1-кесте. DoS шабуылдарының түрлері

Шабуыл атауы	Шабуылданатын операциялық жүйе	Қолданылатын хаттама/ қызмет түрі
Ping of death	Көптеген ОЖ	ICMP Ping
SSPing	Windows 95/NT	ICMP Ping
Land	Көптеген ОЖ мен брандмауерлер	IP
Smurf	Көптеген ОЖ мен брандмауерлер	ICMP Ping
SYN Flood	Көптеген ОЖ мен брандмауерлер	TCP/IP
CPU Hog	Windows NT	Қолданбалар артықшылық деңгейлері
Win Nuke	Windows көптеген ОЖ	Net Bios 139-порт
RPC Locator	Windows NT	RPCSS.EXE, 135-порт
Jolt2	Windows 95/98/NT4/2000, Be/OS 5.0, Cisco 26xx, Cisco 25xx, Cisco 4500, Cisco 36xx, Network Associates Gauntlet, Webshield, Solaris, NT жүйесіндегі Checkpoint фирмасынан Firewall-1, Nokia, Bay Router, Fore желіаралық экрандары	

DoS шабуылдарын болдырмау жолдары:

- тиімді және сенімді жобалау;
- өткізу мүмкіндігін шектеу;
- жүйелерді уақтылы жаңарту;
- қызметтерді неғұрлым аз жүктеу;
- қажетті ағынды ғана өткізуге рұқсат беру;
- IP-мекендерді бұғаулау.

Бақылау сұрақтары

1. DoS шабуылдарының түрлерін атаңыз?
2. Ping of Death шабуылы қалай жасалады, одан қорғану әдістері?
3. SSPing шабуылы қалай жасалады, одан қорғану әдістері?
4. Land шабуылы қалай жасалады, одан қорғану әдістері?
5. Smurf шабуылы қалай жасалады, одан қорғану әдістері?
6. CPU Hog шабуылы қалай жасалады, одан қорғану әдістері?
7. RPC Locator шабуылы қалай жасалады, одан қорғану әдістері?

10. Компьютерлік желілердегі ақпараттың қауіпсіздік мәселелері

10.1. *Желілік қауіпсіздік. Шабуылдың желілік компоненттері*

2004 жылы жылы дүние жүзінде 450 желіге арнайы мониторинг жасалған болатын, сол дайындалған мониторингтің негізінде 40% рұқсатсыз шабуылдар, рұқсатсыз қатынас жасау 26% , 21% әр түрлі қорларды сканерлейтін шабуылдар, 9% қызмет көрсетуден бас тарту – DoS шабуылдар, 3% программаның дұрыс істемеуіне арналған болды. Жалпы желілерді қорғау проблемасын қарастыру үшін оның құрамына назар аудару керек. Олар әр түрлі серверлер, жұмыс станциялар, ақпаратты тасымалдау ортасы, коммутациялау түйіндері.

Серверлер. Серверлер ақпаратты сақтау үшін немесе қызметтердің белгілі бір түрін ұсыну үшін арналған. Осыған байланысты, серверлерге қарсы шабуылдардың негізгі түрлеріне «сервисте қабыл алмау» және құпия ақпаратты ашу әрекеттері жатады.

Жұмыс станциялары. Қаскүнемнің жұмыс станцияларына қатысты негізгі мақсатына олардың қатты дискілерінде локальді сақталған ақпаратты алу, немесе пернетақта буферін көшіріп алу жолымен опертордың көмегімен енгізілетін парольдерді алу жатады.

Ақпаратты тарату ортасы. Ақпаратты таратудың әр түрлі орталары (эфирлік, кабельдік) қаскүнемнен оларды естіп отыру үшін әр түрлі шығындарды талап етеді.

Желілердің коммутация түйіндері. Желілердің коммутация түйіндеріне шабуылдар әдетте екі мақсатта жүреді: не желінің тұтастығын бұзу («сервисте қабыл алмаушылық»), не трафикті қаскүнемге тиімді дұрыс емес жолмен қайта бағыттау.

Кез келген ақпараттық желілердің негізгі компоненттеріне серверлер және жұмыс станциялары жатады. Серверлер ақпараттық

немесе есептеуіш қорларын ұсынады, жұмыс станцияларында персонал жұмыс істейді. Шындығында желідегі кез келген ЭЕМ бір уақытта сервер де, жұмыс станциясы да бола алады – бұл жағдайда серверлерге де, жұмыс станцияларына да арналған шабуылдар қолданылады.

Серверлердің негізгі міндеттеріне ақпаратқа рұқсатты ұсыну мен сақтау және сервистердің кейбір түрлері жатады. Сондықтан қаскүнемдердің барлық мүмкін мақсаттарын былайша таптастыруға болады:

- ақпаратқа рұқсатты алу;
- қызметтерге рұқсат етілмеген енуді алу;
- қызметтердің анықталған класын жұмыс тәртібінен шығару әрекеті;
- қандай да бір аса ірі шабуылдың көмекші кезеңі ретінде ақпаратты немесе қызметтерді өзгерту әрекеті.

Ал сервистерді істен шығару мәселесі (қалыпты функциялауды бұзу) қазіргі компьютерлік әлемде аса өзекті. Мұндай шабуылдардың класы «сервисте қабыл алмаушылық» (ағыл. deny of service – DoS) шабуылы деген атқа ие болды. «Сервисте қабыл алмаушылық» шабуылы OSI моделінің деңгейлерінің бүтін диапазонында жүзеге асырылуы мүмкін: физикалық, арналық, желілік, сеанстық.

Ақпараттың немесе қызметтердің аса ірі масштабты (ауқымды) шабуылдың бөлігі ретінде өзгеруі серверлерді қорғауда өте маңызды мәселе болып табылады. Егер серверде пайдаланушылардың парольдері немесе қаскүнемдерге оларды өзгерте отырып жүйеге (мысалы, кілттердің сертификаты) кіруге рұқсат ететін қандай да бір мәліметтер сақталса, онда әрине жүйеге шабуылдың өзі осы сияқты серверге шабуылдан басталады. Модификацияға (түрленуге) аса жиі ұшырайтын қызметтер сервері ретінде DNS-серверін атаған жөн.

DNS-қызметі (ағыл. Domain Name System – домендік аттардың қызметі) Intra- және Inter- Net желілерінде «айтылатын» және жеңіл есте сақталатын домендік аттарды (мысалы, www.intel.com немесе mail.metacom.ru) олардың IP-адрестеріне салыстыруға жауап береді.

Жұмыс станциясы. Жұмыс станциясының шабуылының негізгі мақсаты болып, әрине, не өзінде локальді сақталатын,

не өңделетін мәліметтерді алу болып табылады. Ал осындай шабуылдардың негізгі тәсіліне қазіргі уақытқа дейін «трояндық» бағдарламалар жатады. Бұл бағдарламалар өз құрылымы бойынша компьютерлік вирустардан ешқандай ерекшелігі жоқ, бірақ ЭЕМ-ға түскенде өздерін көзге түсірмеуге тырысады. Сонымен бірге олар берілген трояндық бағдарламамен жұмыс істеу протоколын білетін кез келген бөтен адамға ЭЕМ-да жоюлы түрде кез келген әрекеттерді орындауға рұқсат етеді. Яғни, берілген бағдарламалардың жұмыстарының негізгі мақсаты болып станцияның желілік қорғанысының жүйесін ішінен бұзу болып табылады.

Трояндық бағдарламалармен күресу үшін әдеттегі вирусқа қарсы БҚ сияқты тек соларға ғана бағытталған бірнеше ерекше әдістер де қолданылады. Бірінші әдіске қатысты компьютерлік вирустардағыдай вирусқа қарсы БҚ ел бойынша кең таралған және зақымдаудың көптеген жағдайлары болған вирустардың үлкен санын табатынын білу қажет. Вирус немесе трояндық бағдарлама тек Сіздің ЭЕМ-ға немесе корпоративті желіге енуге рұқсатты алу мақсатымен жазылатын жағдайларда ол 90% ықтималдықпен стандартты вирусқа қарсы БҚ-мен анықталмайды.

Сондықтан компьютерлік вирустардан сияқты трояндық бағдарламалардан да сенімді қорғайтын аса қарапайым жол – бұл әрбір жұмыс станциясында жүйелік файлдарда және мәліметтердің қызметтік облыстарында (реестрде, дискілердің жүктемелі облыстарында және т.б.) өзгерістерді бақылау бағдарламаларын орнату – адвизор деп аталатын (ағыл. adviser – хабарлаушы).

Ақпаратты тасымалдау ортасы. Әрине, ақпаратты тарату ортасына шабуылдың негізгі түріне оның тыңдалуы жатады. Тыңдалу мүмкіндіктеріне байланысты барлық байланыс сызықтар мынаған бөлінеді:

- кең тарататын шектеусіз рұқсатпен;
- кең тарататын шектеулі рұқсатпен;
- «нүкте-нүкте» арналары.

Бірінші категорияға ақпараттың оқылу мүмкіндігі ештеңемен басқарылмайтын ақпаратты тарату схемалары жатады. Мұндай схемаларға, мысалы, инфрақызыл және радиотолқынды желілер жатады. Екінші және үшінші категорияларға тек қана сымды сызықтар жатады: олардан ақпараттың оқылуы не берілген сымға

қосылған (кең тарататын категория) барлық станциялардан, не тек пакет жіберілу пунктінен берілу пунктіне дейін («нүкте-нүкте» категориясы) жүретін станциялар мен коммутация түйіндерінен мүмкін.

Желілердің кең таралымды категориясына коаксиальды кабель және қайталауыштардағы (хабах – ағыл. hub) TokenRing желісі, EtherNet желісі жатады.

Желілердің коммутациялау түйіндері. Желілердің коммутация түйіндері қаскүнемдер үшін 1) желілік трафиктің маршрутизациясының аспабын және 2) желінің жұмысқа икемділігінің қажетті компонентін білдіреді.

Бірінші мақсатқа байланысты маршрутизация кестесіне рұқсатты алу жасырын ақпараттың ағын жолын қаскүнемнің назарына ілігетін жаққа өзгерте алады. Оның одан арғы әрекеттері тікелей басқарумен, егер қаскүнем қандай да бір жолмен администратор құқығына ие болса (бәрінен жиірек администратордың паролін біліп алды немесе үнсіз ауыстырылмаған паролін пайдаланып қалды) DNS-сервердегі шабуылға ұқсауы мүмкін.

«Сервисте қабыл алмау» класының шабуылында қаскүнем әдетте коммутация түйінін не хабарламаларды дұрыс емес «тұйық» жолмен таратуға, не мүлдем хабарламаны таратуды тоқтатуға мәжбүрлейді.

10.2. *Желілік шабуылдар түрлері*

Желі арқылы шабуылдар жасау себептері:

1. Хаттамалардың ақауларына негізделінген осал тұстарын пайдалану.
2. Операциялық жүйенің осал тұстарын пайдалану.
3. Программалардың, сонымен бірге деректер базаларының осал тұстарын пайдалану.
4. Адам мінезіндегі осал тұстарды пайдалану.
5. Т.б. топтар (вирустар, желілік құрттар және т.б. программалар).

Компьютерлік желіде және желілерде байқалған қауіп-қатерлерді келесі екі класқа бөлуге болады:

- құрал-жабдықтарға – қауіп-қатер: қоректендіруден бас тарту, істен шығу, шулар, қызып кету, электромагниттік әсерлер;
- деректерге – қауіп-қатер: деректерді жоғалту, бұрмалау, қатынас жасауға жол бермеу, қызмет көрсетуден бас тарту, құпиялылықты бұзу, деректерді ұрлау, жалған идентификациялау, шабуылдар.

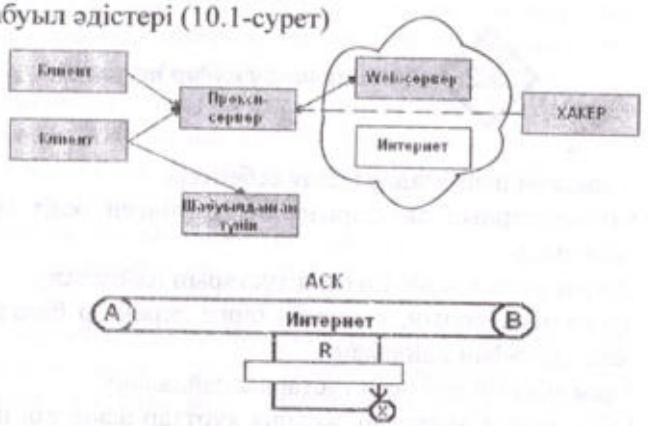
Шабуылдар келесі түрге бөлінеді:

– адам мінезіндегі осал жерлер;
– DoS шабуыл;
– рұқсатсыз қатынас жасау.

Шабуылдар вирустар арқылы іске асады. Шабуыл жасалатын порттар:

- 21 – TCP, FTP;
- 22 – TCP, SSH;
- 23 – TCP, DNS;
- 80 – TCP, HTTP;
- 111 – TCP, Surrbc;
- 137, 138, 139 – UDP, NetBios;
- 443 – TCP, HTTPS;
- 1433 – MS SQL, Server.

Шабуыл әдістері (10.1-сурет)



10.1-сурет. Маршрутизаторларды және пакеттерді айналы әдіспен бұрмалау

Интернетте порольді ұрлауға немесе бұзуға көп әдістер пайдаланады. Олардың ішінде екі әдіс кең таралған:

1. Шифрланған порольды бұзу;
2. Порольдер сақталған пакеттерді ұрлауға деректер тасымалданатын арналарды бақылау.

UNIX операциялық жүйесінде порольдерді шифрлап файлға сақтайды. Ол файлды кез келген қолданушы оқи алады. Сондықтан шабуылшы бұл файлды оңай аша алады.

Аутентификацияға байланысты басқа проблема кейбір TCP және UDP қызметтері тек қана жеке хост компьютердің аутентификациясын тексереді, ал қолданушылардың өзін тексермейді. Сервер администраторы жеке қолданушыға қатынас құруға рұқсат беруі мүмкін, бірақ осы хоста жұмыс істейтін басқа қолданушыларға қатынас құруға бөгет жасай алмайды. Осымен қатар келесі проблемаларды ерекшелеуге болады:

№1 проблема – әлсіз және осал идентификация.

№2 проблема – тасымалданатын деректерге оңай бақылау жүргізу.

№3 проблема – басқаларға оңай бүркемелену (маскировка).

№4 проблема – жергілікті желідегі қызметтердің аздығы және хостар арасындағы өзара сенімділігі.

№5 проблема – қорғау шаралары мен конфигурацияның күрделілігі.

Хостарға қатынас жасау, жүйелерді басқару және оларды баптау, олардың жұмыс істеу дұрыстығын тексеру өте қиын. Егер де қорғау конфигурациясы дұрыс жасалынбаса, онда хакерге осы желіге кіру оңай болады.

Интернеттегі тәуелділік деңгейлеріне келесі факторлар әсер етуі мүмкін:

1. Жүйедегі желілер саны.
2. Желіде қандай қызметтер пайдаланылатыны.
3. Интернетке ұғым қалай қосылғандығына байланысты.
4. Желі конфигурациясына байланысты немесе сол конфигурация туралы мәліметтер.

Компьютерді желілер арқылы төнетін шабуылдардан қорғау үшін желілік экран немесе бранд мауер деген жүйе көмегімен іске

асырылады. Бранд Мауэр дегеніміз – қауіпсіздікке көзқарас, оның оның көмегімен қауіпсіздік саясаты жүзеге асырылады. Бранд Мауэр жүйесі маршруттар, дербес компьютер, хост, арнайы желіні немесе ішкі желіні дұрыс емес хаттамаларды пайдаланудан және дұрыс емес хостар қызметіне пайдаланудан қорғауға арналған маршруттар, хост, дербес компьютер немесе хостар тобы болуы мүмкін.

Жалпы жағдайда Бранд Мауэр жүйесі жоғары деңгейлерді маршрутизаторлар негізінде жасалады:

- желі жүйесіне қатынас жасауды басқару;
- қауіпсіздікті шоғырландыру;
- жоғары құпиялылықты пайдалану;
- желіні пайдалану статистикасын жүргізу және хаттамалау;
- қауіпсіздік саясатты іске асыру.

Бранд Мауэрді пайдалануында да кейбір проблемалар кездеседі.

1. Керекті қызметтерге қол жеткізудің шеттелуі. Кейбір желі топологиялары Бранд Мауэрді пайдалануға мүмкіндік бермейді. Сондықтан, осындай желілерге Бранд Мауэрді орнату қажет болса, онда желіге күрделі өзгерістерді жасауға тура келеді.

2. Көп осал тұстардың болуы, оның ішінде люк-тесіктерден шабуыл жасау.

3. Өз қызметтердің шабуылына тосқауылды қоя алмау жағдайы және басқа проблемалар.

Бақылау сұрақтары

1. Желілердің қандай компоненттеріне шабуылдар жасалады?
2. Жергілікті желіге қатынас құру арқылы жасалатын шабуылдар?
3. Ауқымды желіге қатынас құру арқылы қандай шабуылдар жасалады?
4. Бранд Мауэрді пайдалану проблемалары қандай?
5. Интернеттің қызметтерінің қай порттарына шабуылдар жасалады?
6. Желіні қорғауға қойылатын талаптар қандай?

11. Вирустардан қорғану

Компьютерлік жүйелер мен программалық жабдықтарды қайта жаңғыртып дамытқан сайын оның көлемі өсіп, ондағы деректердің сақталуы жоғарылайды. Бұл сақтаудың жоғарылау себебінің бір факторы болып программалары қуатты және ЭЕМ-нің жаппай өндірісі болып табылады және де ол компьютерлік вирустардың жаңа түрлерінің пайда болуына себепкер саналады. Программаның қамтамасыз етуі компьютерлік вирустар мен жарақаттау арқылы келген ең үлкен қауіп өмірлік қажетті ақпараттарды жойып жіберуі мүмкін, яғни ол тек қаржылық және уақыттық шығындарға әкеліп қана қоймай адам шығындарына да душар етуі мүмкін.

11.1. *Вирустар және олардың әр түрлілігі*

Компьютерлік вирус – арнайы жазылған шағын көлемді (кішігірім) программа. Ол өздігінен басқа программалар соңына немесе алдына қосымша жазылады да, оларды «бүлдіруге» кіріседі, сондай-ақ компьютерде тағы басқа келеңсіз әрекеттерді істеуі мүмкін. Ішінен осындай вирус табылған программа «ауру жұққан» немесе «бүлінген» деп аталады. Мұндай программаны іске қосқанда алдымен вирус жұмысқа кірісіп, оның негізгі функциясы орындалмайды немесе қате орындалады. Вирус іске қосылған программаларға да кері әсер етіп, оларға да «жұғады» және басқа да зиянды іс-әрекеттер жасай бастайды (мысалы, файлдарды немесе дискідегі файлдардың орналасу кестесін бүлдіреді, жедел жадтағы бос орынды жайлап алады және т. с. с.).

Өзінің жабысқанын жасыру мақсатында вирустың басқа программаларды бүлдіруі және оларға зиян ету әрекеттері көбінесе сырт көзге біліне бермейді. Оның кері әсері белгілі бір шарттарды орындағанда ғана іске асады. Вирус өзіне қажетті

бүлдіру әрекеттерін орындаған соң, жұмысты басқаруды негізгі программаға береді, ал ол программа алғашында әдеттегідей жұмыс істей береді. Сөйтіп ол программа бұрынғы қалпынша жұмысын жалғастырып, сырт көзге «вирус жұққандығы» бастапқы кезде байқалмай қалады.

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

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

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

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

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

Вирустардың кейбір түрлерінің кері әсері тіпті одан да терең болады. Олар бастапқы кезде өзінің жұққанын ешбір әсерімен білдіртпей, көптеген программалар мен дискілерге үндемей таралып кетеді де, сонан соң бірден бел шешіп зиянкестік жасауға кіріседі, мысалға, компьютердегі қатты дискіні өздігінен қайта форматтап шығады. Ал зиянкестік әсерін программаларға өте аз тигізіп, бірақ қатты дискідегі мәліметтерді іштен «мүжіп», құртып жататын вирустарға не істеуге болады?!

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

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

Қазіргі кездегі вирустар негізгі екі топқа бөлінеді:

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

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

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

11.2. *Бүлінген және вирус жұққан файлдар*

Вирус дискідегі кез келген файлды бүлдіре алады, бірақ кейбір файлдарға ол бірден жабысады, яғни ол файлдың ішкі көлемінен орын алып, оның қызметін түрлендіріп, қолайлы жағдай туғанда, зиянды әрекетін бастап кетеді. Дегенмен, көптеген программалар

мәтіні мен құжаттарға, мәліметтер базасының информациялық файлдарына, электрондық кестелердегі мәліметтерге вирустар онша әсерін тигізе алмайды, тек оларды аздап қана зақымдауы мүмкін. Вирустардың мынадай файлдарға жұғуы мүмкін:

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

2. Операциялық жүйенің жүктеуіші мен қатты дискінің ең басты мәлімет жүктеу жазбасы. Бұл аумақтарды зақымдайтын вирустар «жүктегіш» (загрузочная) немесе Boot – вирустар деп аталады.

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

3. Құрылғылар драйверлері, яғни CONFIG.SYS файлының шеткері құрылғылар көрсетілетін Devise деген сөз тұрған жолында жазылған файлдар. Ондай файлдағы вирус сол құрылғыны іске қосқан сайын қызметке кіріседі. Бірақ драйверді бір компьютерден екінші компьютерге көшіру өте сирек болатындықтан, мұндай ви-

рустар көп тарала қоймаған. DOS жүйелік файлдарына (MS DOS. .SYS және IO.SYS) да вирус жұқтырылуы теория жүзінде мүмкін болғанымен, олардың таралуы іс жүзінде өте сирек кездеседі.

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

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

Барлық .COM және .EXE типті файлдар үшін – каталогтағы файлдың алғашқы мәліметі көрсетілген орынға вирус жазылған қате орын көрсетіліп, ал дұрыс көрсеткіш – таңбаланған (кодталған) түрде каталогтың пайдаланылмайтын бөлігіне жасырылады. Сол себепті кез келген программаны іске қосқанда дискіден бірінші вирус оқылады да, ол тұрақты ЭЕМ жедел жадында сақталып файлдарды өңдейтін DOS программаларына жабысады. Бірақ жалпы көрініс каталог дұрыс жұмыс атқарған сияқты болып сырт көзге мұның әсері білінбей тұрады. Тек вирусы бар дискеттерден программалық файл оқитын сәттерде оның нақты көлемі қысқарып небәрі 512 не 1024 байт қана болып қалады. Бірақ атқарылуға тиіс вирусы бар әрбір программа іске қосылғанда оның дұрыс емес екендігі байқалмайды. Міне осылай «ауырған» дискілерді дұрыс қалпына келтіру үшін тек арнайы вирусқа қарсы программалар қажет (мысалы, Aidstest программасының соңғы нұсқалары).

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

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

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

11.3. *Компьютерлік вирустардың қысқаша жіктелуі*

Қазіргі кезде 10 000 шамасында компьютерлік вирустар белгілі. Оларды әдетте мақсатына, жұмыс логикасына, көлеміне және жұмыс істеу аумағына қарай топтарға жіктейді.

Жұмыс логикасына және мақсатына қарай оларды шартты түрде төмендегідей жіктеуге болады:

1. **«Ұстауыш-вирустар»** программалық құралдар кешеніндегі қателіктер мен дәлсіздіктерді пайдаланады. Көлемді программаларды түзету кезінде белсенділік көрсетіп программаға жабысады. Әр түрлі зияндық әрекеттері бар вирус.

2. **«Логикалық бомбалар»** (баяу әсер ететін «бомбалар») қарапайым программаларға кіріп алып білінбей тұрады. Тек белгілі бір шарттар (көрсетілген күн-ай мерзімінде немесе уақытта, программа орындалуының белгілі кезеңінде) орындалғанда ғана әсер ете бастайды. Сол шарт орындалар мезетке дейін неғұрлым көп программаларға «жұғуға» тырысады.

3. «Құрттар» жүйелік программалаушылардың информациялық-есептеу желілерінің бос тұрған ресурстарын анықтау программаларына кіріп алып, сол бос құрылғыларды тектен тек жұмыс істеуге мәжбүр етеді. Мысалы, оларды шексіз циклге енгізіп, құрдан құр жүргізіп қояды немесе қажетсіз мәліметтерді баспаға шығартады және т.с.с.

4. «Троян аттары» қарапайым қолданбалы программаларға еніп алып, соларға рұқсат етілмеген әрекеттерді (жасырын информацияны оқып жария етеді, жедел жадтағы информацияларды «басқа жаққа» жіберуге дайындайды) орындатады. Жасалу құрылымы мен көбею жолы оңай болғандықтан, көбінесе компьютер желілерін жайлап алады.

Мақсаттарына қарай вирустар мынадай 4 бөлікке бөлінеді:

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

Бізде кең тараған Aids вирусқа қарсы программаларының авторы Д.Лозинскийдің ұсынысы бойынша вирустарды көлеміне қарай жеті топқа жіктеуге болатыны белгілі.

11.4. *Компьютерлік вирустардан сақтанудың негізгі тәсілдері*

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

Айта кететін жайт, вирустардың кейбір түрлері компьютерге келісімен зиянды ісіне кірісіп кетеді, ал олардың кейбірі файлдар құрамына енсе де іске кіріспей, біраз уақыт тым-тырыс жасырынып жатады, бұл уақытты «инкубациялық мезгіл» деп атайды.

Бұл мезгіл аралығында олар екпінді күйде файлдар арасына таратылып, зақым келтіруді белгілі бір уақыт мөлшері өткен соң немесе ол өзін-өзі белгіленген мөлшерде көбейтіп болған соң ғана бастайды.

Вирустардан сақтану үшін мынадай шаралар қолдануға болады:

- информацияны қорғаудың жалпы шаралары – дискіні физикалық зақымданудан сақтау, дұрыс жұмыс істемейтін программаларды қолданбауға және жұмыс істеп отырған адам қателіктер жібермеуге тырысуы;
- профилактикалық шараларды пайдалану, яғни вирусты жұқтыру мүмкіндігін азайту тәсілдерін қарастыру;
- вирустан сақтайтын арнайы программаларды пайдалану. Жалпы информация қорғау тәсілдері тек вирустан сақтануда ғана емес, басқа жағдайда да пайдалы болатынын есте сақтаған жөн. Ондай тәсілдің негізгі екі түрі белгілі.

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

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

Жалпы ақпаратты сақтаудың ортақ тәсілдерінің қажеттілігіне қарамастан, қазіргі кезде тіптен олардың өзі жеткіліксіз болып отыр. Вирустан сақтану үшін арнайы программалар қажет және оларды тұрақты түрде қолдана бастау керек. Мұндай программаларды бірнеше түрлерге бөлуге болады: детекторлар, докторлар (фаг-программалар), ревизорлар (файлдардағы және дискінің жүйелік аумақтарындағы өзгерістерді бақылайтын программалар), доктор-ревизорлар, сүзгі-программалар (вирустан сақтайтын резиденттік программалар) және вакциналар (иммунизаторлар).

Вирустардың әсерін жоятын вирусқа қарсы программаларды үш негізгі топқа бөлуге болады:

– файл мәліметтерінің бақылауға арналған олардың қосындыларын есте сақтауға негізделген программалар;
– программаға немесе операциялық жүйеге вирус жұққан сәтте оларды анықтайтын резиденттік программалар;
– вирустар жұқтырылғаннан кейін олардың бар екенін анықтайтын программалар.

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

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

Детектор-программалар тек бұрыннан белгілі вирус түрлерінен ғана қорғай алады, жаңа вирусқа олар дәрменсіз боп келеді.

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

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

Доктор-ревизорлар – доктор-программа мен ревизорлар арасынан шыққан гибрид. Бұлар тек файлдағы өзгерістерді анықтап қана қоймай, оларды автоматты түрде «емдеп» бастапқы қалыпты жағдайға түзеп келтіреді.

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

Вакцина-программалар (немесе **иммунизаторлар**) компьютердегі программалар жұмысына әсер етпей, оларды вирус «жұққан» сияқты етіп түрлендіреді де, вирустан сақтайды, бірақ бұл программаларды пайдалану онша тиімді емес.

Ең көп тараған антивирус – Д.Лозинскийдің Aidstest: программасы. Ол әрбір жаңадан шыққан вирустан хабардар болып, соларға қарсы шара қолдану жолдарын анықтап, үнемі өзгертіліп отырады. Бұл программаны пайдаланып компьютерді вирустардан сақтау үшін жиі-жиі дискілерді (мысалы, c:) мынадай командамен тексеріп отыру керек: aidstest c:.

Ал егер компьютерде вирус бар деген күмән болса, онда оны мына командамен емдеу қажет: aidstest c:/f.

Тек программалық файлдарды ғана емес, қалған мәліметтерді де түгел тексеру үшін мына команда орындалады: aidstest c:/f/g.

Бұдан басқа И.Даниловтың қуатты полифаг-вирусқа қарсы тобына жататын Doctor Web программасы да жиі қолданылып жүр, оның бұрынғы нұсқаларын іске қосу үшін web c: /f жолын пайдалану қажет немесе соңғы шыққан нұсқаларын drweb командалық жолы арқылы программалық ортаға кіріп, меню жүйесі бар терезеде қандай дискілерді, қалай тексеретінімізді енгізіп, оның бар мүмкіндігін (F1 пернесі – көмекші мәлімет ала отырып) толық қолдана аламыз.

Вирустардың жаңа түрлері күнбе-күн пайда болып жатыр, сондықтан вирусқа қарсы программалардың да тексеру-емдеу қабілеттері жоғары соңғы шыққандарын қолданған дұрыс болатыны түсінікті шығар.

Компьютерге вирус енгенін сезсеңіз, мына ережелерді мұқият орындаған абзал:

1. Алдымен аспай-саспай, ойланып іске кіріскен жөн екенін ұмытпаңыз.
2. Дегенмен, бір әрекет бірден орындалуы керек – вирустың зиянды әрекеттерін әрі жалғастырмас үшін компьютерді бірден өшіру қажет.
3. Егер компьютерге «жұққан» вирус түрін емдей алатын детектор-программаларыңыз болса, дискілерді тексеру мақсатында соларды дереу іске қосыңыз.
4. Біртіндеп вирус жұғуы мүмкін болған барлық дискілерді тексеріп шығу қажет.
5. Егер дискідегі барлық файлдарыңыздың архивтік көшірмелері болса, онда дискіні қайта форматтап, мәліметтеріңізді бұрынғы қалпына келтіруге тырысыңыз.

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

1. Информацияны әркімнің жиі пайдалануын шектеу және оның көшірмесін сақтау.
2. Сырттан келген мәліметтерді мұқият тексеруден өткізу.
3. Вирустан «емдеу аспаптарын» дайындап қою.

11.5. *Вирусқа қарсы программаларға қысқаша шолу*

Вирусқа қарсы программаны таңдауда вирустарды анықтау пайызы ғана емес, сол сияқты жаңа вирусты анықтау қабілеттілігі, вирусқа қарсы базадағы вирустар санын анықтау, Оны жаңарту жиілігі, қосымша функциялардың барлығы да есепке алынады.

Қазіргі уақытта байыпты вирусқа қарсы 2500-ден кем емес вирусты анықтай білу керек. Бұл яғни олардың барлығы «еркін-дікте» деген сөз емес. Шын мәнінде олардың көпшілігі өзінің тіршілігін тоқтатқан немесе лабораторияда жатыр, олар таралмайды.

Шынында 200-300 вирус кездестіруге болады, ал қауіп төндіретін олардың бірнеше ондаған түрі ғана. Бірнеше вирусқа қарсы программалар бар. Олардың біршама белгілерін қарастырамыз.

Norton AntiVirus 4.0 және 5.0 (өндіруші «Symantec») біршама белгілі және көбірек антивирусқа қарсы танымал. Вирустарды тану пайызы өте жоғары (100%-ға жуық). Бағдарламада жаңа белгісіз вирустарды танитын механизм қолданылады.

Norton AntiVirus программасының интерфейсында Live Update функциясы бар. Ол жалғыз бір кнопканың сыртымен Web арқылы бағдарламаны, вирустар сигнатуры жиынтығын жаңартады. Вирустармен күресуші мастер анықталған вирустар туралы тиянақты ақпарат берумен қатар сізге мүмкіндік береді. Вирусты автоматты режимінде жоюға, әлде неғұрлым қарайлап, біртіндеп емдеу арқылы, яғни әрбір орындалған жою процесінің әрекетін көруге мүмкіндік береді.

Вирусқа қарсы базалар өте жиі жаңартылады (кейде жаңарту аптасына бірнеше рет жүреді). Резиденттік мониторы бар.

Dr Solomon's Antivirus (өндіруші: Dr «Solomon's Software»). Жақсы антивирустың бірі болып есептеледі (Евгений Касперский бұл менің AVP бірден-бір бәсекелес деп айтқан екен.). Іс жүзінде 100% барлық белгілі және жаңа вирустарды анықтайды. Функциялардың көптігі, сканер, монитор, эвристика және вирустарға қарсы тұра алатын қажетті заттардың барлығы бар.

MsAfee Virus Scan (өндіруші «MsAfee Associates»). Бұл неғұрлым көбірек танымал вирусқа қарсы пакеттердің бірі. Вирусты өте жақсы жояды, бірақ та файлдық вирустардың жаңа түрлерін анықтауда басқа пакеттерге қарағанда елеулі кемшілігі бар. Ол жеңіл әрі жылдам келісімді түрде бастауды қолдану арқылы қойылады, оны өз ыңғайынша баптауға да болады. Сіз барлық файлды сканерлей аласыз немесе тек қана программаны сканерлейсіз, сығылған файлдарды сканерлеу процедурасын тарата аласыз немесе таратпайсыз. Интернет торымен жұмыс істеуге көп функциясы бар.

Dr.Web (өндіруші: «Диалог Наука») – танымал ресейлік вирусқа қарсы программа. Вирустарды жақсы таниды, бірақ оның базасында басқаларға қарағанда вирусқа қарсы программасы аз.

Antiviral Toolkit (өндіруші: «Лаборатория Касперского»). Бұл антивирус ең сенімді антивирус ретінде бүкіл әлемде танылған. Қолданылу қарапайымдылығына қарамастан ол вируспен күресуге қажетті барлық арсеналдарға ие. Эвристикалық механизм, сканерлеу көптігі.

Вирусқа қарсы екі модульден тұрады – сигнатуралық қорғау модулі және активті қорғау модулі. Осы модульдер базасында, ереже бойынша сканердің екі типі жұмыс жасайды. Жалпы сканер кесте бойынша немесе қолданушы талабы бойынша жүйені қарап шығуды орындайды, ал сканер-монитор жүйеде өзгерістерді іздейді және жаңа, өзгермелі файлдарды тексереді.

Сигнатуралық қорғаудың мақсаты – вирусқа қарсы күдікті файлдарды вирусқа қарсы базасында бар вирус үлгілерімен салыстырады. Мамандар жаңа вирустарды жіктейді және олардың үлгілерін вирусқа қарсы базасына енгізеді.

Активті қорғау модулі күдікті программаның активтілігін іздейді және ішкі критерийлерге сәйкес бағалайды.

Norton Antivirus 2008 вирусқа қарсы әмбебапты ерекшелігі лездік қорғанысты қамтамасыз ете отырып, әрбір 5-15 минут сайын тез импульсті жаңалауды орындауында. Ол қолайлы графикалық баптау менюіне ие. Бір кемшілігі – оның айтарлықтай жоғары жүйелік талаптары. Бағасы 1390 рубльді құрайды.

Dr.Web вирусқа қарсы активті вирустарды жоғары пайыздық тиімді емдеулерімен ерекшеленеді. Басқа да артықшылығы – файлдарды тексеру функцияларында. Программа ресурстарға талап қоймайды, жүйені жүктемей жұмыс жасайды. Жұмыс жасауда тек бір ғана шарт 32-bit-ті Windows XP немесе Vista ОЖ бар болуы. Dr.Web бағасы – бір жылға 1040 рубль немесе екі жылдық лицензиясымен 1835 рубль.

«Антивирус Касперского 2009» тек файлды, пошталық хабарларды, интернет-трафиктерді ғана емес, сонымен қатар, интернет-пейджерлерді (ICQ, MSN) сканерлейді. Microsoft Windows XP ортасында «Антивирус Касперского» ыңғайлы жұмыс жасауы үшін 256 Мбайт бос оперативті жады керек, Windows Vista ортасында екі есе көп. Вирусқа қарсы бір ғана күрделілік – сериялық нөмір

және лицензия нөмірін емес кілттік файлды қолдану, бұл жаңалау процедурасын қиындатады. Бағасы – 1000 рубль.

TopTenReviews, Inc – программалық жабдықтардың рейтингін анықтауда және сапасын бағалауда дүниежүзінде беделді, танымал американ компаниясы. Ең күшті вирусқа қарсы қорытынды рейтингі маңызды сипаттамаларды сараптамалық бағалау негізінде құрылады:

- вирусқа қарсы қолданудың қарапайымдылығы;
- вирустардан, құрттардан және де зиянды программалардан тиімді қорғау;
- вирусқа қарсы базаны жиі жаңалау;
- қорғау кешенінің сипаттамасы және мүмкіндігі;
- вирусқа қарсы программаны орнатудың қарапайымдылығы;
- техникалық қызмет деңгейі.

AV-Comparatives – негізгі қызметі вирусқа қарсы тестілеу болып табылатын беделді австрия лабораториясы. Тест әдістемесі үш бөлікті құрайды.

Бірінші – вирустардың пайда болуы кезінде вирусқа қарсы программалардың тиімділігі зерттеледі.

Екінші бөлік – жалған өңдеулер санын анықтауға бағытталған.

Үшінші бөлік – сканерлеу жылдамдығын өлшейді.

FS мәліметтерді қалпына келтіру лабораториясы – жоғалған мәліметтерді қалпына келтіруге бағытталған Ресей компаниясы. Сапаны баға ықтималдығы негізінде вирусқа қарсы салыстыру әдістемесін өңдеді. Сондағы нәтиже келесідей.

11.1-кесте. Вирусқа қарсы программаларды өзара салыстыру

Вируска қарсы рейтингі, қараша 2009 жыл								
	Вирусқа қарсы	VB100	AV-Comparative	PC World	PC Pro	FS	Кешенді сараптамалық баға	Рейтинг
Сараптамалық баға								
	Kaspersky	10	9	8	9	9	45	1

Кестенің соңы

	Kaspersky	10	9	8	9	9	45	1
	F-Secure	10	10	5	8		33	2
	Avira	10	8	4		8	30	3
	GDATA	10	8	10			28	4
	Symantec	0	10	9	9		28	4
	Microsoft	10	8		9		27	5
	McAfee	10	8	1		4	23	6
	Eset	10	9	2		1	22	7
	eScan	10	10				20	8
	Sophos	0	5		9	6	20	8
	...	...	...	...	...	...	...	...
	DrWeb					10	10	13

Компьютерлік вирустар кең таралып кетті және онымен күрес компьютерді пайдаланушыға көптеген келеңсіздіктер туғызады. Сондықтан онымен күресе білудің маңыздылығын түсінген жөн. Қазіргі таңда вирусқа қарсы программалар мен оларды қолдану әдістерін жасауда едәуір нәтижелер бар. Эвристикалық механизм, арқылы сканерлеу, файлдар мен архивтерді сканерлеу – бұлар оның мүмкіндіктерінің толық тізімі емес.

Вирустан қорғану көбінесе компьютерді пайдаланушының сауаттылығына да байланысты болады. Қорғаудың барлық түрін пайдалану компьютердің, яғни ондағы ақпараттық жоғары қауіпсіздігіне жетуге мүмкіндік беруі.

Бақылау сұрақтары

1. Компьютерлік вирус дегеніміз не?
2. Вирустың жұқтыру процесін сипаттаңыз?
3. Қандай тасушы-программалар вирус жұқтырып алады?
4. Программалық қосымша деген не?
5. Резидентті және резидентті емес қосымшаларға анықтама?
6. Қосымшалардың бұзушы әрекеттерін топтастырыңыз?

ӘДЕБИЕТТЕР

1. Қазақстан Республикасының 2007 жылғы 11 қаңтардағы N 217 Ақпараттандыру туралы Заңы.
2. Қазақстан Республикасының Ұлттық қауіпсіздігі туралы Заңы (26.06.1998). Мемлекеттік құпиялар туралы Заңы (15.03.1999).
3. Терроризмге қарсы күрес туралы Заңы (13.07.1999).
4. Электрондық құжат және электрондық цифрлық колтаңба туралы Заңы (07.01.2003).
5. Ақпараттандыру туралы Заңы (08.05.2003).
6. Экстремизиге қарсы іс-қимыл туралы Заңы (18.02.2005).
7. Тұрым А.Ш., Мұстафина Б.М. Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002 ж.
8. Щеглов А. Защита компьютерной информации от несанкционированного доступа: СПб:Наука и техника, 2004. – 384 с.
9. Ященко В.В. Введение в криптографию. Новые математические дисциплины. – М.: МЦНМО Питер, 2001.
10. Цвики. Э. Создание защиты в Интернете. СПб:Питер, 2002. – 600 с.
11. Эрик Коул. Руководство по защите от хакера. – М.: Наука и техника, 2004. – 350 с.
12. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001.
13. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
14. Хорошко А. Методы и средства защиты информации. М.: Радио и связь, 2003. – 440 с.
15. Романцев А.П. Стеганографическая защита цифровыми водяными знаками. – М: РИО МТУСИ, 2003. – 68 с.
16. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем.– М.: Горячая линия – Телеком, 2000. – 452 с.
17. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.– М.: Яхтсмен, 1996. – 71 с.
18. Уолкер Б. Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты: пер. с англ. – М.: Связь, 1980, – 112 с.

19. Касперский К. Фундаментальные основы хакерства (искусство дизассемблирования). – М.: Солон-Р, 2002.
20. Расторгуев С.П. Программные методы защиты информации в компьютерах и сетях. – М.:Яхтсмен,1993. – 187 с.
21. Спесивцев А.В. и др. Защита информации в персональных ЭВМ. – М.:Радио и связь,1993. – 190 с.
22. Романцев А.П. Криптография и стеганография. – М: РИО МТУСИ, 2002. – 80 с.
23. Оспанова Э.Е. Проектирование систем защиты и безопасности информации. Учебно-методический комплекс. – Алматы: КАЗНТУ, 2005.
24. Бузов Г.А. Защита от утечки информации по техническим каналам: – М:Горячая линия – телеком, 2005. – 416 с.
25. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. www.winblog.ru/2006/12/27/27120601.html.
26. http://www.citforum.ru/internet/infsecure/index.shtml – «Методы и средства защиты информации» (курс лекций). Авторские права: Беляев А.В.
27. www.cs.hut.fi/crypto/ – ағылшынша, криптография әдістеріне пайдаланатын мәліметтер.
28. www.subject.com/crypto/crypto.html – ағылшынша, криптография әдістеріне пайдаланатын мәліметтер (программалар, кітаптар және басқалар).
29. www..com/ – ағылшынша, RSA криптография әдісіне байланысты мәліметтер.
30. www.microsoft.com/workshop/prog/security/pkcb/crypt.htm – ағылшынша, шифрлау туралы мәліметтер.

МАЗМҰНЫ

АЛДАЖАРОВ Қанағат Смақұлы

Ақпараттық қауіпсіздік негіздері

Оқу құралы

Бас редактор	**Сәрсембаева А.Ж.**
Редакторы	**Өмірғалиева Қ.Ө.**
Компьютерде беттеген	**Нүсібәлиева М.С.**
Мұқаба дизайнері	**Мышбаев Қ.Т.**

Басуға 27.04.2011 ж. қол қойылды. Пішімі $60\times84^{1}/_{16}$.
Баспа табағы 7,5. Шартты баспа табағы 7,0.
Есептік баспа табағы 5,8. Көшірме басылым. Таралымы 200 дана.
Тапсырыс №3/114-10.

«Экономика» баспасы» ЖШС
050063, Алматы қаласы, Сайын көшесі, 81-үй

ISBN 978-601-225-254-5