УДК 004.056.5

Токпанова Камиля Еркиновна – т.ғ.д., профессор (Алматы қ., М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясы)

Қабылда Али – магистрант (Алматы қ., Еуразия технологиялық университеті)

ВЕБ-ТОРАПТАРҒА АРНАЛҒАН АҚПАРАТТЫ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ ӘДІСТЕМЕСІН ЖАСАУ ТУРАЛЫ

Хабарлар тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа біраз шабуылдар жасау мүмкіндігі бар.

Бұзушы - тиым салынған операцияларды қателескендіктен, білместіктен орындауға әрекет жасаған немесе ол үшін саналы түрде әртүрлі мүмкіншіліктерді, әдістерді және құралдарды қолданатын тұлға.

Бұзушының үлгісін зерттеген кезде мыналар анықталды:

- Қорғаныс жүйесін құру;
- Ақпаратты қорғау әдістері;
- Ақпаратты қорғаудың криптографиялық әдісі.

Ақпаратты қорғау құралдары - мемлекеттік құпия болып табылатын мәліметтерді қорғауға арналған техникалық, криптографиялық, программалық және басқа да құралдар, олар жүзеге асырылған құралдар, сондай-ақ, ақпарат қорғаудың тиімділігін бақылау құралдары.

Ақпараттық қорғау жүйесі жобалау әр түрлі жағдайда жүргізілуі мүмкін және бұл жағдайларға негізгі екі праметр әсер етеді: ақпарат қорғау жүйесіне арнап әзірленіп жатқан деректерді өңдеудің автоматтандырылған жүйесінің қазіргі күй-жағдайы және ақпаратты қорғау жүйесін жасауға кететін қаржы мөлшері [1].

Ақпаратты қорғау жүйесі.Қолдануға қажетті кез-келген басқа программаның тұжырымдамасы сияқты қорғаныс жүйесін құру тұжырымдамасы да мынадай сұрақтарды қарастырады: ақпаратты қорғау аймағындағы практикалық зерттемелердің өзектілігі, қорғаныс жүйесін құрудың негізгі кезеңдері және қорғаныс мәселесін шешудің әр түрлі әдістемелерінің салыстырмалы талдауы.

Қорғаныс жүйесін құрудың негізгі кезеңдері төмендегідей болып жіктеледі (сурет 1):

Сурет 1- Қорғаныс жүйесін құру кезеңдері

1. Мүмкін болатын қауіп-қатердің талдауы келесі қауіп-қатерден қорғанудың негізгі түрлерін зерттеумен айналысады:

- Ақпараттың конфиденциалдығының бұзылуының қауіп-қатері;
- Ақпараттың бүтінділігінің бұзылуының қауіп-қатері.

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

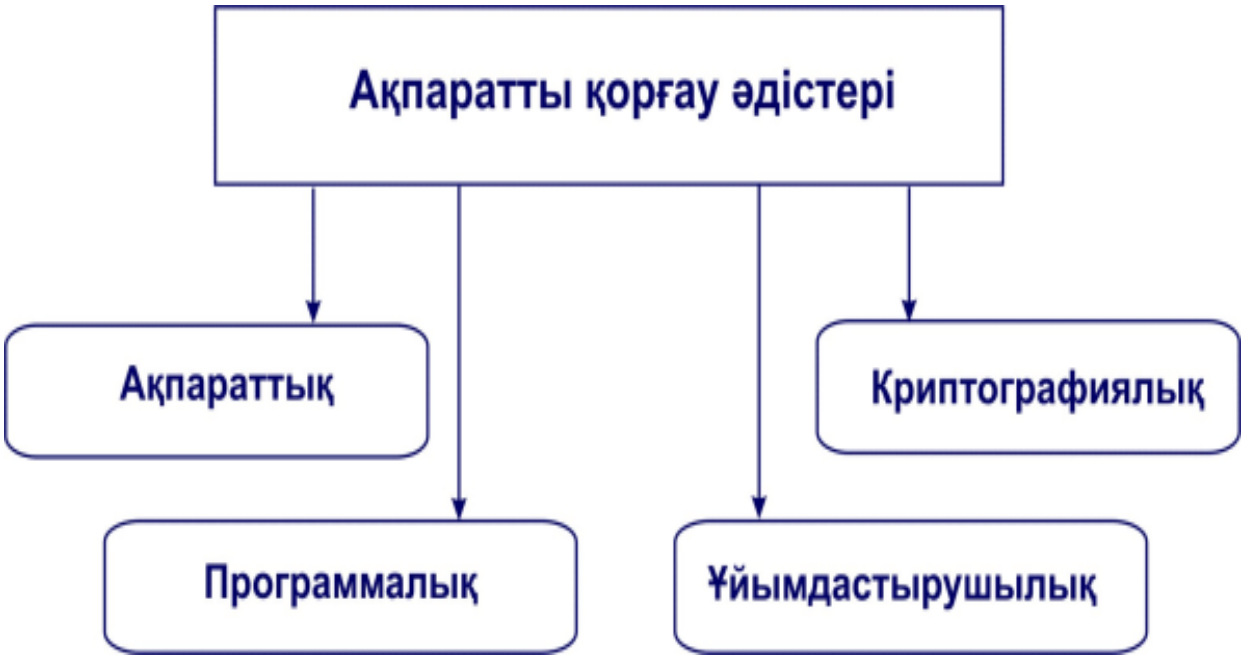
2. Қорғаныс жүйесін жоспарлау кезеңі қорғалатын құрылымдар тізімінен және оларға мүмкін болатын қауіп-қатерден тұрады. Бұл кезде қорғанысты қамтамасыз етудің келесі бағыттарын назарға алу қажет:

- құқықтық-этикалық;
- моральды-этикалық;
- қорғанысты қамтамасыз етудің әкімшіліктік шаралары;
- қорғанысты қамтамасыз етудің аппараттық-программалық шаралары.

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

4. Қорғаныс жүйесін сүйемелдеу кезеңі жүйенің жұмысын бақылау, ондағы болып жатқан оқиғаларды тіркеу, қорғанысты бұзуды айқындау мақсатымен оларды талдау және қажетінше қорғаныс жүйесін түзетумен сипатталады [2-4].

Ақпаратты қорғау әдістері төмендегідей болып жіктелінеді (сурет 2).



Сурет 2 - Ақпаратты қорғау әдістерінің жіктелуі

Қорғаныстың аппараттық әдістерін қолдану мынадай техникалық құралдарды пайдалануды ұсынады:

1.Тыңдалатын және жазылатын құрылғылардан қорғайтын TRD-800 категориялы радиохабарлағыштар мен магнитофондар детекторы;

2. Жасырын бейне бақылау құратын модульдік нөмірлер;

3. Ақпаратты жеткізудің дұрыстылығын қамтамасыз ететін ақпаратты анықтылыққа тексеру сызбалары;

4. Құпиялы құжаттарды жіберуге арналған SAFE-400 категориялы факстік хабардың скремблері.

Қорғаныстың аппараттық әдістері ресурстардың үлкен шығынын талап етеді.

Программалық әдістер есептеуіш алгоритмдер мен қатынауды шектеуді қамтамасыз ететін программаларды және ақпаратты рұқсатсыз пайдаланудан шығаруды ұсынады. Программалық әдістер келесі функцияларды іске асырады:

1. Идентификация, аутентификация, авторизация (Pin кодтар, парольдер жүйелері арқылы);

2. Резервті көшіру және қалпына келтіру процедуралары;

3. Антивирустық программаларды белсенді қолдану және антивирустық қорларды жиі жаңартып отыру;

4. Транзакцияны өңдеу.

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

Мұндай қорғау әдісі стандартты операциялар немесе программалар дестесі түрінде жүзеге асырылады. Операциялық жүйенің негізіндегі қорғау көбінесе қатынас құруды басқарудың процедураларын жүзеге асыруға мүмкіндік беретін мәліметтер қорын басқару жүйелері деңгейіндегі қорғау құралдарымен толықтырылуы керек [5].

Қазіргі кезде ақпарат қорғаудың криптографиялық әдісінің көпшілік қаблдаған жіктеуі жоқ. Дегенмен, жіберілетін хабарламаның әрбір символы шифрлауға түскенде шартты түрде 4 негізгі топқа бөлуге болады:

- ауыстыру шифрланушы мәтіннің символдары сол немесе басқа алфавит символдарымен алдын ала белгіленген ережеге сәйкес ауыстырылады;
- аналитикалық түрлендіруде шифрланушы мәтін қандай да бір аналитикалық ереже бойынша түрлендіріледі;
- орын ауыстыру шифрланушы мәтіннің символдарының орны жіберілетін мәтіннің берілген блогының шегінде қандай да бір ереже бойынша шифрланады.

Ақпаратты шифрлаудың сенімділік дәрежесі бойынша көптеген программалық өнімдер бар. Кең таралған программалардың бірі болып Циммерменн құрған Pretty Good Privacy (PGP) болып табылады. Оның криптографиялық қорғау құралы өте күшті. Танымдылығы мен ақысыз таратылуы іс жүзінде PGP-ны дүние жүзінде электрондық хат алысу стандартына айналдырды. PGP программасына желіде көпшіліктің шығуына мүмкіндігі бар.

Ақпаратты қорғаудың ұйымдастырушылық әдісі келесі іс-шаралардың ұйымдастырылуы мен іске асырылуын қарастырады:

1. өртке қарсы қорғаныс;
2. жанбайтын сейфтерде аса қажетті құжаттарды сақтау;
3. өту жүйесі арқылы қатынау регламенті;
4. бақылау жүйесін ұйымдастыру;
5. қолданушылардың әр түрлі категорияларының қорғаныс объектілері мен олардың орындалу талаптарына қатынауды регламентациялайтын көмекші нұсқамаларды даярлау.
6. мамандарды таңдау мен даярлау;
7. қауіпсіздік мәселесі бойынша семинарларға, конференцияларға қаты- суды қамтасыз ету мен ұйымдастыру.

Дербес компьютердің программалық өнімі мен жіберілетін ақпаратқа рұқсатсыз шығудан ең сенімді қорғау - әр түрлі шифрлау әдісін (ақпарат қорғаудың криптографиялы әдістері) қолдану болып табылады.

Қорғаудың криптографиялық әдістері деп ақпаратты түрлендірудің арнайы құралдарының жиынтығын айтамыз, нәтижесінде оның мазмұны жасырылады.

Криптографиялық әдістердің маңызды аймақтарда қолданылуына қарамастан криптографияны эпизодтық қолдану оның бүгінгі қоғамда атқаратын ролі мен маңызына тіптен жақын көрсеткен жоқ. Криптография өзінің ғылыми пәнге айналуын көрсеткен жоқ. Криптография өзінің ғылыми пәнге айналуын электрондық ақпараттық технологиямен туындаған практиканың қажеттілігіне парыз [6].

Криптографиялық әдістердің теориялық негізі болып математика мен техниканың төмендегідей бөлімдерінде қолданылатын математикалық идеялар табылады:

- қалдықтар кластарының жүйесіндегі модульдік арифметика;
- сандардың жай көбейткіштерге жіктелуі;
- ақырлы өрістердің математикалық ақпараттары;
- алгебралық көпмүшеліктер қасиеттері;
- дискреттік логарифм мәселесі;
- кодтау теориясы.

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

Симметриялық әдісте жіберуші мен қабылдаушыда тек бір ғана кілт қолданылады (құпия кілт).

Ал ассиметриялық әдісте 2 кілт қолданылады: құпия және ашық кілт.

Симметриялық әдістер: DES, IDEA, ГОСТ

Ассиметриялық әдістер: RSA, Diffi-Hellman

Шифрлауға және шифрланған ақпаратты ашуда қолданылатын ақпарат ретінде – белгілі бір алфавитте құрылған мәтіндер қарастырылады.

- алфавит-ақпарат белгілерін кодтауда пайдаланатын соңғы көбейтінді;
- мәтін – алфавит элементтерінің реттелген жиыны.

Қазіргі ақпараттық жүйелерде қолданылатын алфавитке мысал ретінде келесілерді келтіруге болады:

- алфавит Z_{33} – орыс алфавитінің 32 әрпі және бос орын;
- алфавит Z_{256} – ASCII және КОИ-8 стандартты кодына кіретін символдар;
- бинарлы алфавит - Z_2=(0, 1);
- сегіздік немесе он алтылық алфавит [7].

Қорытынды. Қорғаныштың мақсаты - қатынас құруға рұқсат етілмеген арналарды ақпараттың түрін өзгертуге, ақпаратты жоғалтуға және сыртқа келтіруге бағытталған әсерлерден сенімді түрде сақтауды қамтамасыз ететін өзара байланысты бөгеттердің біріңғай жүйесін құру. Жүйе жұмысын қалыпты режимде көзделмеген осындай оқиғалардың біреуінің пайда болуы рұқсат етілмеген қатынас құру деп саналады.

ӘДЕБИЕТ

1 Андрончик А. Н., Богданов В. В., Домуховский Н. А., Коллеров А.С., Синадский Н. И., Хорьков Д. А., Щербаков М. Ю. Защита информации в компьютерных сетях. Екатеринбург : УГТУ-УПИ, 2008 - 248 с.

2 Биячуев Т.А. Безопасность корпоративных сетей. /Под ред. Л.Г.Осовецкого. - СПб: СПб ГУ ИТМО, 2009. – 420 с. - ISBN:5-279- 02549-6

3 Безбогов А.А. Методы и средства компьютерной информации: учебное пособие / А.А.Безбогов, А.В.Яковлев, В.Н. Шамкин. – Тамбов : Изд-во Тамб. Гос. Техн. Ун-та, 2006.-196 с. – ISBN 5-8265- 0504-4

4 Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации:Книжный дом“Либроком”,2012.- 376 с.

5 Исаев А.Б. Современные технические методы и средства защиты информации: Учеб. пособие. – М.: РУДН, 2008. – 253 с.

6 Аяжанов С.С.,Емелин П.В.Компютерлік желілерде ақпаратты қорғау.- Қарағанды: ҚЭУ, 2008.- 325 б.

7 Аяжанов Қ.С., Есенова А.С. Ақпараттық қауіпсіздік және ақпаратты қорғау. Алматы:ЖШС РПБК «Дәуір», 2011.-376 б.