ӘОЖ 004.056.5

С.А. НҰГМАНОВА[1], А.М. АХМЕТОВА[2], Ш.У. МАКСУТОВА[3]

АҚПАРАТТЫ ҚОРҒАУ ЖҮЙЕСІ

[1,2]ҚАЗАҚСТАН, АЛМАТЫ,
АБАЙ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ ПЕДАГОГИКАЛЫҚ УНИВЕРСИТЕТ,
[3]ҚАЗАҚСТАН, АЛМАТЫ,
ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Ақпаратты қорғау мемлекеттік деңгейде қазіргі кезде өзекті мәселеге айналды және мемлекет алдындағы бірден-бір шешілуі қажет, ұлттық қауіпсіздіктің негізгі элементі ретінде қарастырылып отыр.Мақалада жалпыға ортақ құрал-саймандарын енгізу көмегімен мемлекеттік басқаруды жетілдіру, «ашық» және «мобильді үкіметті» құруды жетілдіру қарастырылады, сонымен бірге ақпараттық инфрақұрылымның қолжетімділігін дамыту мәселесі шешіледі. Ақпараттық қоғамның дамуы адам ресурстарының дамуымен бірге жүретіндігін ескеру қажет, электронды қалыптасу білім беру көмегімен ақпараттық технологиялармен жұмыс істеу және оларды меңгеру мүмкіндіктері қалыптасады.

*Кілттік сөздер:*криптография, ақпаратты қорғау, криптоанализ, желілік технологиялар, қорғаныс жүйесі, криптографиялық протокол

В настоящее время актуальной становится проблема защиты информации на государственном уровне, который необходимо решить, предусматривается в качестве основного элемента национальной безопасности. В статье с помощью всеобщего внедрения инструментов предполагается усовершенствование государственного управления, создание «открытого» и «мобильного правительства», а также будут решаться задачи разития доступности информационной инфраструктуры. Надо учесть, что развитие информационного общества должно сопровождаться развитием человеческих ресурсов, с помощью электронного образования формируются навыки работы с информационными технологиями и вожможности их освоения.

Ключевые слова: криптография, информационная безопасность, криптоанализ, сетевые технологии, система защиты, криптографический протокол

At present, the problem of protecting information at the state level, which needs to be solved, is envisaged as the main element of national security. In the circle of these directions, through the general introduction of tools, improvement of public administration, the creation of an "open" and "mobile government" are supposed, as will the tasks of developing the availability of information infrastructure. It should be taken into account that the development of the information society should be accompanied with the development of human resources, with the help of e-education, to develop skills in work with information technologies and the opportunities for their development.

Keywords: cryptography, information security, cryptanalysis, network technologies, protection system, cryptographic protocol

Қазіргі кезде ақпаратты қорғау жалпы ұлттық мәселеге айналып отыр. Ақпараттық технологияның қарқынды дамуы және Интернеттің тез таралуы конфиденциалды ақпаратты қорғаудың әдістерін дамытуға, әсіресе криптографияның дамуына көп әсер етті. Мемлекеттің барлық салаларына қатысты ақпарат нақты саяси, материалдық және бағалылығы жағынан да құнды болып саналады. Ақпаратты қорғау мемлекеттің көзқарасымен алғанда қазіргі кезде өзекті мәселеге айналды және мемлекет алдындағы бірден-бір шешілуі қажет, ұлттық қауіпсіздіктің негізгі элементі ретінде қарастырылып отыр. Жаңа қуатты компьютерлердің, желілік технологиялардың пайда болуы мен ақпараттың компьютерде шоғырлануы мүлдем ашылмайды деп саналған криптография жүйесін пайдалануға мүмкіндік береді. Криптография термині ежелгі гректердің cryptos – құпия және grapho – жазу сөздерінен құралған.

Күн сайын криптографиямен криптографиялық әдістер біздің күнделікті өмірімізбен тұрмысымызға кеңінен еніп келеді. Міне бірнеше мысал . E-mail-ді жібере отырып біз кей жағдайларда менюдің мына сұрағына жауап береміз: “Шифрлеу режимі қажет пе?”. Банк карточкасының иегері терминал арқылы банкке жүгіне отырып, алдымен карточканы аутентификациялаудың криптографиялық протоколын орындайды [1]. Криптографиялық әдістер (ақпаратты қорғау) мен криптоанализдің (қорғауды бұзу) көптеген түрлері шығып жатыр. Олардың криптотұрақтылық пен өнімділік сияқты талаптары әрдайым өсіп келеді. Соған байланысты соңғы жылдары сызықсыз, соның ішінде ақпаратты қорғауға хаостық динамиканы қолдану мәселелері қызығушылық туғызады.

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 қорғаныстың қамтамасыз етудің келесі бағыттарын назарға алу қажет:

- құқықтық-этикалық;
- моральды-этикалық;
- қорғаныстың қамтамасыз етудің әкімшіліктік шаралары;
- қорғаныстың 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, қорғаныстың бұзуды айқындау мақсатымен оларды талдау және қажетінше қорғаныс жүйесін түзетумен сипатталады.

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) [2]. .

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.

Қазіргі кезде ақпарат қорғаудың криптографиялық әдісінің көпшілік қабылдаған 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 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 қатысуды 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.

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 [4].

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

Соңғы жарты ғасырда компьютерлердің есептеу қуаты едәуір өскен, және бұл тенденция ары қарай жалғасатынына еш күмән жоқ.Көптеген криптографиялық бұзулар параллельді компьютерлер үшін жарамды: есептеу процессорлық қарым-қатынасты қажет етпейтін миллиардтаған шағын бөліктерге бөлінеді. Сондықтан сенімді криптографиялық жүйелер есептеу техникасының дамуын көптеген жылдарға дейін алдын ала ескеріп отырады.

Әдебиет тізімі

1.Баричев С. В. Криптография без секретов. – М.: Наука, 1998. – 120б.

2.Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке – С. 2-е изд . – М.: Вильямс, 2003. – 672б.

3.Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классическихшифров . – М.: Наука, 1995. – 208 б.

4. Криптология – наука о тайнописи //Компьютерное обозрение. –1999. – No3. – Б.10-17.