С.Сейфуллин атындағы Қазақ агротехникалық университетінің 60 жылдығына арналған **«Сейфуллин оқулары– 13: дәстүрлерді сақтай отырып, болашақты құру»** атты Республикалық ғылыми-теориялық конференциясының **материалдары** = **Материалы** Республиканской научно-теоретической конференции **«Сейфуллинские чтения – 13: сохраняя традиции, создавая будущее»**, посвященная 60-летию Казахского агротехнического университета имени С.Сейфуллина. - **2017. - Т.I, Ч.5.** - Б.281-284

АҚПАРАТТЫ ШИФРЛАУДЫ ТАЛАП ЕТІЛГЕН ДЕҢГЕЙДЕ ҚОРҒАУДЫҢ КРИТЕРИЙЛЕРІН САРАПТАП ТАҢДАУДЫҢ МӘСЕЛЕЛЕРІ

Алымова Б.

Кіріспе. Ақпараттық технологиялардың қарқынды дамуы ақпаратты қорғаудың жаңа жүйелерінің пайда болуынаалып келді. Ақпаратты қорғаудың қағидалары және жүйелік құрылымы түбегейлі өзгерді. Ақпараттың қорғаудың ауқымды дамуы және оларды қолдану саласының көлемінің ұлғаюы сондай, ақпаратты өңдеу құралдарының жұмыс істеуінің сенімділігі мен орнықтылығы мәселелері мен қатар сол өңделіп отырған ақпаратты қорғау есептері маңызды орын алып, кететін уақытқа және орасан шығатын қаражаттық шығынға қарамай күн тәртібінің алдына шықты. Маңыздылығына орай, осы проблеманы шешу күрделене түседі, өйткені осы уақытқа дейін Қазақстан Республикасында және шетелде бірыңғай және жалпы қабылданған теориялық бірлік және ортақ ымыраға келген концепция жоқ. Сондықтан, ақпараттың қорғаудың толық теориясын жасауда, ақпарат қауіпсіздігін сақтаудың бірыңғай, бірдей концепциясын және ақпараттың қорғаудың жүйелігін жасау өте маңызды болып табылады.

Аталған мәселелерге сәйкес жазылып отырған мақаланың мақсаты талап етілген деңгейдегі ақпарат қауіпсіздігін қамтамасыз етудің критерийлерінің таңдау әдістемесін дайындау барысындағы шолулар мен ұсыныстар [1-6].

Іске асырылған ақпаратты қорғаудың механизмдерінің негізінде ақпаратты шифрлауда оған қойылатын сенім деңгейін анықтау әдістемесін әзірлеу мейлінше маңызды мақсат болып табылады, себебі, ол ақпаратты қорғаудың деңгейін оны құру кезеңінде де, сонымен бірге ақпаратты шифрлау барысында да нәтижесін бағалауға мүмкіндік береді [2].

Шешілетін есептер. Қойылған мақсатқа қол жеткізу үшін мынадай міндеттерді шешу қажет:

1. Ақпаратты шифрлауда қазіргі қолданыстағы шифрлау стандарттарын және онда сипатталған ақпаратты қорғау механизмдеріне шолу жасау;
2. Талап етілетін деңгейде ақпарат қауіпсіздігін сақтауды қамтамасыз ететін ақпаратты шифрлау моделін жасау;
3. Ақпаратты қорғауды бағалау критерийлерін таңдау жүйесін ақпаратты шифрлау стандарттарының топтамасының тетіктеріне сәйкес және оларды құру ерекшеліктерін ескере отырып оны қорғау механизмдерін іске асу барысын бағалай құру;

4. Ақпаратты шифрлаудың сенімділік деңгейін бағалау жүйесіне негізделген, ақпаратты шифрлауда жаңа сенімділік деңгейдегі жүйені әзірлеу;

5. Ақпаратты қорғау үшін талап етілетін қорғалу деңгейіндегі ақпаратты шифрлау моделі негізінде ақпаратты шифрлау үшін қорғау профилінің топтамалық жүйесінің әдістемелігін құру;

6. Ақпаратты шифрлау жүйесінде қорғаудың тиімділігі мен беріктігін кешенді бағалайтын әдістемемен қамтамасыз ету;

7. Критерийлерді және шифрлау жүйесінің элементтерінің сипаттамаларын таңдау
талаптарының жүйесін жасау, сонымен қатар, қорғау жүйесін құрамы және құрылымына қойылатын талаптарды негіздеу.

Күтілетін ғылыми жаңалықтар. Зерттеліп және жасалатын ғылыми еңбекте күтілетін ғылыми жаңалықтар:

1. Ақпараттың қорғалуын бағалау критерийінің тетіктеріне сәйкес, ондағы іске асырылған қорғау механизімі негізінде ақпаратты шифрлаудың қорғалуын бағалайтын критерийлерін таңдаудың жаңа жүйесін жасау;

2. Бағалаудың сенімділік деңгейі негізінде ақпаратты шифрлаудың жаңа сенімділік жүйесін жасау;

3. Ақпараттың қауіпсіздігін қорғаудың деңгейін бағалау критерийлерінің топтамасын құру және оларды негіздеу.

4. Ақпаратты шифрлау деңгейін бағалау критерийлерін іске асыру әдістемелігін жасау.

Тәжірибелік бағалығы. Жасалатын еңбектің бағалылығы онда жасалған ақпаратты шифрлаудың беріктігін және сенімділігінің деңгейін бағалайтын критерийлер мен көрсеткіштер талап етілген дәрежеде ақпарат қауіпсіздігін сақтап, кәсіпорындар мен мемлекеттік санатта құпиялықты іске асырады.

Ақпаратты шифрлауда талап етілген дәрежеде ақпарат қауіпсіздігін сақтау деңгейін бағалайтын критерийлер негізінен екі топқа бөлінеді [3]:

1. Криптографиялық критерийлері;
2. Аутентификация критерийлері.

Әр топ бірнеше компоненттерді қамтиды.

Криптографиялық критерийлері:

1. Криптографиялық алгоритмдер;
2. Қолданылатын кілт ұзындығы;
3. Динамикалық немесе статикалық кілтті қолдану;
4. Хабарламаның бүтіндігін тексеретін технология (MIC, CCMP).

Аутентификация критерийлері:

1. Протокол;
2. Серверде аутентификацияның болуы;
3. Өзара аутентификацияның болуы;
4. Цифрлық сертификатты қолдану.

Зерттеу объектісі.Ақпаратты шифрлаудыңталап етілген деңгейде қорғалуының ақпараттық қорғау жүйесі.

*Зерттеу предметі.*Ақпаратты шифрлауды талап етілген деңгейде қорғаудың және критерийлерді таңдаудың әдістемелігімен қамтамасыз ету.

*Зерттеу әдістемелігі.*Жұмыста жүйелік талдау, математикалық бағдарламалау, математикалық статистика және ақпараттар қауіпсіздігі теориясы.

Еңбекте қарастырылған ғылыми тұжырымдардың қорытындысы мен ұсынысы, келтірілген ғылыми қағидалардың негізделуінің дәрежесі, төмендегі әдістемеліктермен қамтамасыз етіледі: жүйелік талдауды; математикалық бағдарламаны; математикалық статистиканы; белгілі жекелей ғылыми нәтижелерді салыстыру; ұсынылып отырған әдстемеге экстремальды шамаларды ендіру арқылы зерттеу; жұмыста сәйкес ҚР Мемлекеттік стандарттарын қолдану.

Критерийлері талап етілетін деңгейде ақпарат қауіпсіздігін сақтауды қамтамасыз ететін ақпаратты шифрлау моделін жасау және сол критерийлердің сандық бағалауын анықтау басты мақсат. Сонымен қатар, анықталған критерийлердің сандық көрсеткіштері ақпаратты шифрлаудың нақты сапалық сипатын айқындауы тиіс. Модельдеудің нәтижесі қауіпсіздігін сақтау үшін ақпаратты шифрлағанда онда қолданылған және қажетті бірнеше критерйлердің нақты сандық мөлшерін есептеу. Мәселен, щифрлауға кететін уақыт, шығын, кері шифрлаудың дәл болуынан басқада бірнеше көрсеткіштерді қарастырамыз және ақпаратты шифрлаудың күрделігі, оны кері шифрлауға өзгелердің қол жетімсіздігін мейлінше қиындату, яғни, оның сандық көрсеткіштері [4].

Талап етілетін деңгейде ақпаратты шифрлау критерийлерінің жиыны, сол модельденіп отырған ақпаратты шифрлау элементтерінің сипаттарын және қасиеттерін анықтайды. Атап айтқанда, жиындағы критерийлеріне әртүрлі сандық мәндер беріп, ақпаратты шифрлауды талап етілген деңгейге жеткізіп, ақпараттың қауіпсіздігін сақтап, құпиялықты мейлінше берік етеді.

Ақпаратты шифрлау барысында қолданылған математикалық амалдар, арнайы жасалған әдістемелерді қолдану және белгілі нақты жағдайларда іске асыру шаралары шифрлау алгоритмінің нобайын анықтайды [5].

Сонымен бірге, шынайы қолданбалы есептерде талапқа сәйкес шифрлаудың өлшемдері, ақпаратты құпиялығын сақтау үшін жасалған түрлендірулер айрықша орын алады.

Ақпаратты шифрлау моделіне қарастырылып отырған критерийлер жиынының толықтырылған ұғымдарын ендіру, өз кезегінде, зерттеліп отырған объектінің элементтерінің өзара қатысы мен байланысын реттеп қойылған есепті шешу жолдарын анықтайды [6].

Есепті шешуде келесі мәселелерге назар аударуға тиістіміз:

- ақпаратты шифрлау моделі мен әдістемелігін құру құрылымы;
- ақпаратты шифрлау моделін жасаудағы бағдарлама тілінің ерекшелігі;
- ақпаратты шифрлау моделін жасаудағы алгоритм;
- ақпаратты шифрлау моделінің бағдарламасын арнайы аппараттық-платформада жасау;
- ақпаратты шифрлау моделін жасаудағы құрал-саймандар;

- талап етілген критерий деңгейіндегі ақпаратты шифрлау моделіндегі енетін параметрге әртүрлі сандық мәндер беріп нәтижені зерттеу;

- алынған нәтижелерді бағалау және интерпретациялау.

Есептің қойылуы формальды түрде және талап етілген критерий деңгейіндегі ақпаратты шифрлау моделі бірнеше шамалардың

$$\begin{cases} F(x) = G_x(a, b, g, d, ..., z) \\ F(y) = G_y(a, b, g, d, ..., z) \\ F(z) = G_z(a, b, g, d, ..., z) \end{cases} \quad (1)$$

мұндағы $a, b, g, d, ..., z$ жоғарыда айтылған ақпаратты шифрлау моделіне қарастырылып отырған критерийлер жиыны.

*Қорытынды.*Ақпаратты шифрлауды талап етілген деңгейде қорғаудың критерийлерін сараланып талданды. Ақпаратты шифрлаудың сапасын және беріктігін анықтайтын критерийлердің кейбір шамалары бірінші рет айтылды.

Талап етілетін деңгейде ақпаратты шифрлаудың критерийлерін анықтайтын модельді және әдістемені жасау мүмкіндіктері мен жолдарын көрсететін ұсыныстар айтылды

Ақпаратты шифрлауда талап етілген қорғалу деңгейін сақтау үшін жасалған әдістеме, өз кезегінде, кез-келген объектінің қауіпсіздігін білікті сапалы бағалауға мүмкіндік беретін критерийлерді таңдау және оны іске асыру үшін құрылған бағдарлама икемді аспаптық құралы болып табылады. Жасалатын әдістеме жалпы ақпараттың қауіпсіздігін сақтау жүйелерін құрудың бір бөлігі.

Әдебиеттер тізімі

1. Richard A. Mollin, «Codes: theguidetosecrecyfrom ancienttomoderntimes», Chapman&Hall/CRC, 2005, стр. 142.
2. Перейтик:1 2 WilliamStallings, «Cryptographyandnetworksecurity: principlesandpractice», PrenticeHall, 1999, стр. 80.
1. AmishKumar , Mrs. NamitaTiwari. Vol. 1 // Effectve implementation and a valanche Effect of AES. - Departmentof CSE manit-Bhopal: IJSPTM, August 2012. - С. 34.
2. Актуальные проблемы безопасности информационных технологий. Сборник материалов III Международной научно-практической конференции Красноярск 2009, стр. 214.
3. Hofheinz, Dennis; Jager, Tibor Designs codes and cryptography Том: 80 Выпуск: 1, Стр.: 29-61. Опубликовано: jul 2016