

**А. Т. ЖАРКИМБЕКОВА, А. Б. ОСПАНОВА, К. М. САГИНДЫКОВ**

*Еуразиялық ұлттық университеті, Нұр-Сұлтан, Қазақстан*

## **КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДІҢ ҚАУІПСІЗДІГІН ЗЕРТТЕУ БАРЫСЫНДА ҚОЛДАНЫЛАТЫН АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ НОРМАТИВТІК ҚҰЖАТТАРДЫҢ РӨЛІ**

*Берілген жұмыста компьютерлік желі қауіпсіздігін зерттеу барысында қолданылған халықаралық және отандық стандарттар қарастырылған. Ақпараттық қауіпсіздік аймағындағы стандарттардың қысқаша тарихы берілген. Ақпаратты қорғау саласындағы стандарттардың қажеттілігі айқындалған. Стандарттардың ерекшелігі мен талаптары зерттелген. Сондай-ақ, автордың ғылыми зерттеу жұмысында қолданылған ақпараттық қауіпсіздік аймағындағы анықтамалар мен нормативтік құжаттар келтірілген.*

**Түйін сөздер:** *ақпараттық технология, ақпаратты қорғау, компьютерлік желі, ақпараттық қауіпсіздік, қауіпсіздікті қамтамасыз ету құралдары мен әдістері, тестілеу.*

Ақпараттық технологиялардың қауіпсіздігін қамтамасыз ету мәселелері компьютерде ақпараттарды өңдеу мезетінен бастау алып, қарқынды түрде дамыған қоғамды ақпараттандырумен бірге артып, компьютерлік жүйелер мен желілерді жетілдіруде маңызды орын алады. Ақпараттық технологияның қауіпсіздігін қамтамасыз ету кешенді үрдіс, ол көптеген факторлардан тәуелді болады. Соның ішінде, ақпараттық технология қауіпсіздігінің аймағындағы жұмыстарды жүргізу барысында заңды негіз болып саналатын нормативтік құжаттардың талаптары маңызды фактор болып саналады. Ақпараттық технологияның қауіпсіздік мәселесін шешудің басты қыры - ақпараттық технология қауіпсіздігінің деңгейін бағалау үшін талаптардың, критерийлердің және көрсеткіштердің жүйесін әзірлеу болып табылады.

Компьютер желісінің қауіпсіздігін талдау есептерінде қолданылатын және компьютер желісінің қауіпсіздігін талдау орны мен рөлін анықтау мүмкіндігін беретін негізгі анықтамалар және нормативтік құжаттарды қарастырайық. Алдымен ақпаратты қорғау аймағындағы әйгілі халықаралық стандарттарға тоқталып, олардың отандық жағдайда қолданылу мүмкіндіктерін зерттейміз.

Ақпараттық қауіпсіздік аймағындағы стандарттардың қажеттілігі компьютерлік желінің даму мезетінен бастап белгілі болды, осы бағытта 1990 жылдары бекітілген құжаттар айтарлықтай өзгерістерге қол жеткізді. Осы саладағы алғашқы құжат 1985 жылы жаңартылып басылып шыққан, АҚШ Қорғаныс Министрлігінің стандарты - «Қызғылт сары кітап» деп аталып кеткен «Компьютерлік желілердің қауіпсіздігін анықтау критерийлері» болатын. Бұл кітапта компьютерлік жүйелердегі қауіпсіздік құралдарының тиімділігін бағалау үшін қажетті негізгі шарттар анықталған. Осы кітаптың аналогы 2005 жылы жетілдіріліп басылып шыққан және көп елдерге жақсы таралған «Ақпараттық технологиялар қауіпсіздігін бағалаудың жалпы критерийлері» деп аталатын ISO/IEC 15408 халықаралық стандарты. Мұнда ақпараттық технология қауіпсіздігі талаптарының жиынтығы жіктеледі, оларды топтау құрылымы және пайдалану қағидалары анықталады. Жалпы критерийлердің басты артықшылықтары

- қауіпсіздік талаптарының және оларды жүйелеудің толықтығы, қолдану икемділігі және әрі қарай дамыту үшін ашықтық болып табылады [1].

Соңғы уақытта әртүрлі елдерде ақпараттық қауіпсіздікті басқару сұрақтарын қарастыратын халықаралық және отандық стандарттар қатары пайда болды. Солардың бірі ақпаратты қорғау саласындағы аса әйгілі стандарт «Ақпараттық технологиялар – Ақпараттық қауіпсіздікті басқару» («Information technology – Information security management») ISO/IEC 17799:2000 (BS 7799-1:2000) халықаралық стандарты болып табылады. ISO/IEC 17799:2000 (BS 7799-1:2000) стандартының қазіргі қолданыстағы нұсқасы ақпараттық қауіпсіздікті қамтамасыз ету қажеттіліктері, ақпараттық қауіпсіздіктің негізгі ұғымдары мен анықтамалары, қауіпсіздік саясаты, ресурстарды басқару, физикалық қауіпсіздік сияқты өзекті сұрақтарды қарастырады [2].

1998 жылы шыққан «Қорғанудың базалық деңгейі үшін ақпараттық технологияларды қорғау жөніндегі нұсқаулық» деп аталатын BSI неміс стандартында ақпараттық қауіпсіздікті басқарудың жалпы әдісі, замануи ақпараттық технологиялардың компоненттерін сипаттау, ақпараттық қауіпсіздік режимін ұйымдастырудың негізгі компоненттерін сипаттау, әр түрлі желілік технологиялар негізіндегі компьютерлік желілердің сипаттамалары, қауіпсіздік қатерлері мен бақылау шараларының толық каталогтары беріледі [3].

Ақпараттық қауіпсіздікті басқарудың алғашқы халықаралық стандарттарының бірі – BS 7799 британдық стандарты. Оның бірінші бөлімі BS 7799-1 «Ақпараттық қауіпсіздікті басқарудың практикалық ережелері» - Shell, National Westminster Bank, Midland Bank, Unilever, British Telecommunications, Marks & Spencer, Logica және т.б. сияқты коммерциялық ұйымдардың қатысуымен Британдық стандарттау институтымен (British Standards Institution) 1995 жылы әзірленген. Бұл стандарттың екінші бөлімі BS7799-2 «Ақпараттық қауіпсіздікті басқару жүйесі. Қолдану бойынша ерекшеліктер және нұсқаулық» 1998 жылы шықты, онда ақпараттық қауіпсіздікті басқару жүйесін құрудың жалпы моделі және де сертификаттау жүргізілуіне тиіс міндетті талаптардың жиынтығы анықталды [4].

Бағалаушы стандарттардың ішіндегі ең толығы ISO/IEC 15408 «Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері» стандарты, бұл стандарт «Жалпы критерийлер (Common Criteria)» атымен әйгілі. Онда ақпараттық технология қауіпсіздік талаптарының кең жиынтығына жіктеулер келтірілген, оларды топтастыру құрылымы мен пайдалану қағидалары анықталған. Жалпы критерийлердің (ЖК) басты ерекшелігі – қауіпсіздік талаптарының және оларды жүйелеудің толықтығы, қолдану икемділігі және одан әрі дамыту үшін ашықтық. Жалпы критерийлердің талаптары іс жүзінде ақпараттық қауіпсіздіктің энциклопедиясы болып табылады, сондықтан оны ақпараттық технологияның қауіпсіздігі бойынша анықтамалық ретінде пайдалануға болады.

Компьютер желісінің қауіпсіздігін зерттеу және ғылыми зерттеу жұмысын жазу барысында негізгі анықтамалар мен терминдер келесі отандық стандарттар аясында анықталды [5-6]:

1. ҚР СТ 34.007-2002 Ақпараттық технология. Телекоммуникациялық желілер. Негізгі терминдер мен анықтамалар.

2. ҚР СТ 34.005-2002 Ақпараттық технология. Ақпараттық технология.

3. ҚР СТ 34.026-2006 Ақпаратты қорғау. Терминдер мен анықтамалар.

1-кестеде зерттеу барысында қолданылған, ISO/IEC 27002 стандартына негізделген қауіпсіздік саласындағы стандарттар берілген.

**1-кесте** – ISO/IEC 27002 стандартына негізделген қауіпсіздік саласындағы стандарттар

№	Стандарт	Атауы
1	ҚР СТ ISO/IEC 27011-2018	Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. ISO/IEC 27002 стандартына негізделген телекоммуникациялық қызметтерді ұсынатын ұйымдардың ақпараттық қауіпсіздігіне бақылау жүргізу бойынша тәжірибелік нұсқаулық.
2	ҚР СТ ISO/IEC 27011-2013	Ақпараттық технологиялар. Қауіпсіздік әдістері. Телекоммуникациялық қызметтерді ұсынатын ұйымдар үшін ISO/IEC 27002 негізделген, ақпараттық қауіпсіздікті басқару жөніндегі жалпы нұсқаулар
3	ҚР СТ ISO/IEC 27011-2015	Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпаратты қорғауды басқару құралдары жөніндегі ережелер жинағы

Халықаралық ISO/IEC 17799-2005 стандартына балама болып, Қазақстан Республикасының мемлекеттік стандарты ҚР СТ ИСО/МЭК 17799-2006 құрылды [7].

Біздің еліміздегі ақпараттық қауіпсіздік саласында қолданылып жүрген және автордың ғылыми зерттеу жұмысында қолданылған, ақпараттық қауіпсіздікті реттейтін ҚР мемлекеттік стандарттарының бірқатар тізімі 2 - кестеде берілген.

**2-кесте** – Ақпараттық қауіпсіздік саласындағы ҚР мемлекеттік стандарттары

№	Стандарт	Атауы
1	2	3
1	ҚР СТ ГОСТ Р 51188-2007	Ақпаратты қорғау. Бағдарламалық құралдарды компьютерлік вирустардың болуына сынаулар. Жалпы талаптар
2	ҚР СТ 34.022-2006	Ақпаратты қорғау. Ақпараттық жүйелерді жобалауға, орнатуға, ретке келтіруге, пайдалануға және олардың қауіпсіздігін қамтамасыз етуге қойылатын талаптар
3	СТ РК 34.023-2006	Ақпараттық технология. Қауіпсіздік талаптарына ақпараттық жүйелердің сәйкестігін бағалау әдістемесі
4	СТ РК 34.024-2006	Ақпаратты қорғау. Қорғалған орындалудағы автоматтандырылған жүйелер. Жалпы техникалық талаптар

Кестенің-2 соңы

1	2	3
5	СТ РК 34.025-2006	Ақпаратты қорғау. Қорғалған орындалудағы автоматтандырылған жүйелер құру тәртібі. Жалпы ережелер
6	СТ РК 1699-2007	Қол жеткізуді бақылау және басқару жүйелері. Жалпы техникалық талаптар
7	ҚР СТ ISO/IEC 27002-2015	Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпаратты қорғауды басқару құралдары жөніндегі ережелер жинағы.
8	ҚР СТ ИСО/МЭК 15408-2-2017	«Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау өлшемшарттары. 2-бөлім. Қауіпсіздікке қойылатын функционалдық талаптар»
9	ҚР СТ ИСО/МЭК 13335-5-2008	«Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық және коммуникациялық технологияларды қорғауды басқару. 5-бөлім. Желіні қорғауды басқару жөніндегі басшылық»
10	ҚР СТ ISO/IEC 27001-2015	«Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздік менеджменті жүйелері»

Қорыта айтсақ, осы мақалада «Компьютер желілерінің қауіпсіздігін зерттеу үшін Raspberry Pi микрокомпьютер негізінде істелген мобильді программалық-аппараттық құрылғыларды жасау әдістері» тақырыбындағы ғылыми зерттеу жұмысы бойынша желі қауіпсіздігін зерттеу барысында қолданылған стандарттар қарастырылған. Осы зерттеу жұмысында компьютерлік желілердің қауіпсіздігін тестілеуге арналған практикалық мақсатта қолданылатын бағдарлама әзірленген болатын. Осы бағдарлама аясында жүргізілген тестілер ақпараттық қауіпсіздік саласындағы қандай да бір талаптарды бұзбайды. Себебі, компьютерлік желі қауіпсіздігіне жүргізілетін сынақтарды орындаудан бұрын, осы мақалада қарастырып кеткен стандарттардың талаптары зерттеліп, компьютер желісінің қауіпсіздігін талдау орны мен рөлін анықтау мүмкіндігін беретін негізгі анықтамалар және нормативтік құжаттардың рөлі қарастырылды.

## ӘДЕБИЕТ

1 Международный стандарт ISO/IEC 15408. [http://citforum.ru/security/articles/zahita\\_aktivov/](http://citforum.ru/security/articles/zahita_aktivov/) [Международный стандарт ISO/IEC 15408. [http://citforum.ru/security/articles/zahita\\_aktivov/](http://citforum.ru/security/articles/zahita_aktivov/)]

2 Стандарты ISO/IEC 17799:2002 (BS 7799:2000) <https://helpiks.org/2-38949.html> [Standarty ISO/IEC 17799:2002 (BS 7799:2000) <https://helpiks.org/2-38949.html>]

3 Германский стандарт BSI <https://helpiks.org/2-38950.html> [Германский стандарт BSI <https://helpiks.org/2-38950.html>]

4 BS 7799 британдық стандарты. <https://studfile.net/preview/6211050/page:2/> [VS 7799 britandyq standarty. <https://studfile.net/preview/6211050/page:2/>]

5 СТ РК 34.005-2002 Информационная технология. Основные термины и определения. <https://www.enbek.gov.kz/ru/node/595> [ST RK 34.005-2002 Informacionnaya tekhnologiya. Osnovnyye terminy i opredeleniya. <https://www.enbek.gov.kz/ru/node/595>]

6 СТ РК 34.007-2002 Ақпараттық технология. Телекоммуникациялық желілер. Негізгі терминдер мен анықтамалар. <https://www.egfntd.kz/rus/tv/80253.html> [ST RK 34.007-2002 Aqparattyq tekhnologiya. Telekommunikaciya lyq zheliler. Negizgi terminder men anyqtamalar. <https://www.egfntd.kz/rus/tv/80253.html>]

7 Қазақстан Республикасының мемлекеттік стандарты ҚР СТ ИСО/МЭК 17799-2006. <https://www.egfntd.kz/kaz/tv/339075.html> [Qazaqstan Respublikasynuñ memlekettik standarty KR ST ISO/MEK 17799-2006. <https://www.egfntd.kz/kaz/tv/339075.html>]

***А. Т. ЖАРКИМБЕКОВА, А. Б. ОСПАНОВА, К. М. САГИНДЫКОВ***

*Евразийский национальный университет, Нур-Султан, Казахстан*

## **РОЛЬ НОРМАТИВНЫХ ДОКУМЕНТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИСПОЛЬЗУЕМЫХ ПРИ ИССЛЕДОВАНИИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ**

*В данной работе рассмотрены международные и отечественные стандарты, используемые при изучении безопасности компьютерных сетей. Представлена краткая история стандартов в области информационной безопасности. Определена необходимость стандартов в области защиты информации. Изучены особенности и требования стандартов. Также приведены определения и нормативные документы в области информационной безопасности, используемые в научно-исследовательской работе автора.*

**Ключевые слова:** *информационные технологии, защита информации, компьютерная сеть, информационная безопасность, средства и методы обеспечения безопасности, тестирование.*

***А. Т. ZHARKIMBEKOV, А. В. OSPANOV, К. М. SAGINDYKOV***

*Eurasian National University, Nur-Sultan, Kazakhstan*

## **THE ROLE OF REGULATORY DOCUMENTS IN THE FIELD OF INFORMATION SECURITY USED IN THE STUDY OF THE SECURITY OF COMPUTER NETWORKS**

*This paper examines international and domestic standards used in the study of computer network security. A brief history of standards in the field of information security is presented. The necessity of standards in the field of information protection is determined. The features and requirements of the standards are studied. Definitions and normative documents in the field of information security used in the author's research work are also given.*

**Key words:** *information technologies, information security, computer network, information security, security tools and methods, testing.*