

DOI 10.54596/2958-0048-2025-4-205-210

ӨОЖ 004.056

FTAMA 28.21.00

КИБЕРҚАУІПСІЗДІК: ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ МӘСЕЛЕЛЕРІ

Нәби А.А.^{1*}

^{1*} «Манаш Қозыбаев атындағы Солтүстік Қазақстан университеті» КеАҚ
Петропавл, Қазақстан

*Хат-хабар үшін автор: akbayannabieva@gmail.com

Аңдатпа

Бұл мақалада цифрлық заманда жеке деректердің қорғалуының маңыздылығы мен киберқауіпсіздік саласындағы өзекті мәселелер қарастырылады. Жеке деректер дегеніміз - адамның аты-жөні, жеке сәйкестендіру нөмірі (ЖСН), мекенжайы, телефон нөмірі, банк шоттары сияқты ақпараттар. Мұндай деректердің қауіпсіздігіне нұқсан келсе, жеке тұлғаның құқықтары бұзылып, материалдық және моральдық зиян келуі мүмкін. Мақалада дербес деректердің не екені, оларды қорғаудың заманауи тәсілдері, сонымен қатар заңнамалық және техникалық шаралар талданады. Зерттеу барысында қазақстандық және шетелдік тәжірибелерге сүйене отырып, нақты ұсыныстар берілді.

Кілт сөздер: киберқауіпсіздік, жеке деректер, ақпараттық қауіпсіздік, қорғау, цифрлық орта, деректердің құпиялылығы, дербес ақпарат.

КИБЕРБЕЗОПАСНОСТЬ: ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Наби А.А.^{1*}

^{1*} НАО «Северо-Казахстанский университет имени Манаша Козыбаева»
Петропавловск, Казахстан

*Автор для корреспонденции: akbayannabieva@gmail.com

Аннотация

В данной статье рассматриваются важность защиты персональных данных в цифровую эпоху и актуальные проблемы в сфере кибербезопасности. Персональные данные - это информация, такая как имя и фамилия человека, индивидуальный идентификационный номер (ИИН), адрес, номер телефона, банковские счета. Нарушение безопасности таких данных может привести к нарушению прав личности, а также к материальному и моральному ущербу. В статье анализируются понятие персональных данных, современные методы их защиты, а также правовые и технические меры. На основе казахстанского и зарубежного опыта даны конкретные рекомендации.

Ключевые слова: кибербезопасность, персональные данные, информационная безопасность, защита, цифровая среда, конфиденциальность данных, персональная информация.

CYBERSECURITY: ISSUES OF PERSONAL DATA PROTECTION

Nabi A.A.^{1*}

^{1*} Manash Kozybayev North Kazakhstan University NPLC, Petropavlovsk, Kazakhstan

*Corresponding author: akbayannabieva@gmail.com

Abstract

This article examines the importance of personal data protection in the digital age and current issues in the field of cybersecurity. Personal data refers to information such as a person's full name, personal identification number, address, phone number, and bank accounts. Breaches of data security may result in violations of individual rights and cause material and moral damage. The article analyzes the concept of personal data, modern protection methods, as well as legal and technical measures. Based on Kazakhstani and foreign experience, specific recommendations are provided.

Keywords: cybersecurity, personal data, information security, protection, digital environment, data confidentiality, personal information.

Кіріспе

Қазіргі цифрлық дәуірде ақпараттық технологиялардың дамуы адам өмірінің барлық саласына терең еніп отыр. Әсіресе, интернет пен мобильді құрылғылардың жаппай таралуы жеке деректердің онлайн кеңістікте жиналуына, сақталуына және өңделуіне әкелді. Бұл жағдай азаматтардың құпиялылығы мен жеке бас қауіпсіздігіне жаңа қауіптер төндіріп отыр. Жеке деректерді қорғау мәселесі тек жеке тұлғалар үшін ғана емес, мемлекеттік органдар мен коммерциялық ұйымдар үшін де маңызды болып отыр.

Қазақстан Республикасында да жеке деректерді қорғауға байланысты заңнамалық негіздер қалыптасып келеді. Алайда киберқауіпсіздік саласындағы қатерлер күн санап түрленіп, күрделене түсуде. Сондықтан бұл тақырып ғылыми тұрғыда терең зерттеуді талап етеді. Осы мақалада киберқауіпсіздік түсінігі, жеке деректердің мәні және оларды қорғаудың маңыздылығы талданады. Сонымен қатар, Қазақстанда және халықаралық деңгейде қабылданған заңнамалық және техникалық шаралар қарастырылады. Зерттеудің мақсаты - жеке деректерді қорғау саласындағы қазіргі жағдайды бағалап, тиімді киберқауіпсіздік стратегияларын ұсыну.

Зерттеу әдістері

Бұл зерттеу жұмысы Қазақстан Республикасының нормативтік-құқықтық актілері мен халықаралық стандарттар негізінде жүргізілді. Негізгі құқықтық база ретінде Қазақстан Республикасының 2013 жылғы 21 мамырдағы №94-V «Жеке деректер және оларды қорғау туралы» Заңы қолданылды. Аталған заңда жеке деректерді жинау, сақтау, өңдеу және қорғау тәртібі, сондай-ақ субъектілердің құқықтары мен операторлардың міндеттері анық көрсетілген.

Сонымен қатар, зерттеу барысында Еуропалық Одақтың Жалпы деректерді қорғау регламенті (General Data Protection Regulation, GDPR) қарастырылды. Бұл құжатта деректер субъектісінің құқықтары, соның ішінде деректерге қол жеткізу, оларды түзету немесе өшіру құқығы кеңінен қарастырылып, деректерді өңдеуге келісім негіздері мен операторлардың жауапкершілігі нақты жазылған.

Зерттеу барысында ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің және Мемлекеттік техникалық қызметтің ашық дереккөздері пайдаланылды. Бұл ресурстардан кибершабуылдарға қатысты статистикалық мәліметтер, ақпараттық қауіпсіздік саласындағы оқиғалар және ұлттық қауіпсіздік стандарттарының жай-күйі туралы деректер алынды.

Сонымен бірге халықаралық тәжірибені зерттеу үшін Cybersecurity Ventures және Group-IB сияқты ұйымдардың жыл сайынғы есептері талданды. Бұл есептерде киберқауіптердің әлемдік тенденциялары, шабуыл түрлері, шабуылдаушылардың мотивациясы және қорғану әдістері көрсетілген.

Осы дереккөздерге сүйене отырып, салыстырмалы талдау, құқықтық сараптама, контент-талдау және логикалық жүйелеу әдістері қолданылды.

Зерттеу нәтижелері

Зерттеу барысында Қазақстандағы жеке деректерді қорғауға байланысты заңнамалық база мен тәжірибелік жағдайлар талданып, бірнеше маңызды тұжырымдар жасалды.

• Біріншіден, нормативтік-құқықтық негіз қалыптасқанымен, оны тәжірибеде қолдану деңгейі төмен. Мемлекеттік техникалық қызметтің дерегіне сәйкес, 2023 жылы республика бойынша 18 миллионнан астам жеке дерек хакерлік шабуылдарға ұшыраған. Бұл - деректерді сақтау жүйелеріндегі осалдықтың айғағы.

• Екіншіден, жеке деректерді жинау, сақтау және өңдеу үдерістері көптеген мекемелерде жүйесіз, ашық түрде жүзеге асырылады. Көптеген азаматтар қандай деректері жиналатынын және олармен кімнің жұмыс істейтінін нақты білмейді. Бұл құқықтық сауаттылықтың төмендігі мен заңнаманың олқылықтарын көрсетеді.

• Үшіншіден, мемлекеттік ұйымдарда ақпараттық қауіпсіздік ережелері салыстырмалы түрде жақсы сақталғанымен, жекеменшік секторда бұл талаптар жиі ескерілмейді. Көп жағдайда арнайы IT-мамандардың болмауы және қызметкерлердің жеткілікті білімінің жоқтығы деректердің таралуына себеп болады.

• Төртіншіден, бағдарламалық қамтамасыз ету және деректерді шифрлау құралдарының басым бөлігі шетелдік өнімдерге тәуелді. Бұл - ұлттық ақпараттың өзге елдердің юрисдикциясына түсу қаупін күшейтеді. ENISA сараптамасына сәйкес, Еуропада отандық шифрлау жүйелерін дамытуға ерекше көңіл бөлінеді, ал Қазақстанда бұл бағыт әлі де жеткілікті деңгейде емес.

• Бесіншіден, киберқауіпсіздік мәдениеті кең таралмаған. Респонденттердің басым бөлігі фишингтік шабуылдарға жиі алданады, құпиясөздерін сирек ауыстырады және антивирус бағдарламаларын орнатпайды. Бұл жағдай кибершабуылдардың жиілеуіне ықпал етеді.

• Алтыншыдан, кейбір жеке дерекқорлар интернетте ашық түрде қолжетімді. Telegram желісіндегі боттар арқылы адамның ЖСН немесе мекенжайы жайлы ақпаратты табу мүмкіндігі заңнамалық талаптардың бұзылуы ғана емес, сонымен қатар ақпараттық қауіпсіздік құрылымдарының әлсіздігін көрсетеді.

Сондай-ақ, GDPR жүйесімен салыстыру барысында «деректер субъектісінің құқықтары» -мысалы, ұмытылу құқығы, өңдеуге келісім беру және қол жеткізу құқығы -Қазақстанда әлі толық енгізілмегені анықталды. Бұл тетік енгізілсе, азаматтардың деректеріне иелік ету деңгейі артар еді.

Ақпараттық жүйелерге аудит жүргізу, есеп беру мен ішкі бақылау тетіктерінің әлсіздігі де - қазіргі жүйенің тағы бір осал тұсы. Көптеген мекемелер деректер қауіпсіздігін қамтамасыз етуді шығын ретінде қабылдайды.

Соңында, жасанды интеллектті жеке деректерді қорғау саласында қолдану - келешекте тиімді шешімдердің бірі бола алады. Автоматты түрде қауіп-қатерлерді болжау және кибершабуылдарды ерте анықтау жүйелері деректердің қорғалуын арттыра түсер еді.

Бұл жағдайлар жеке деректерді қорғау саласында әлі де шешілмеген мәселелер бар екенін көрсетеді. Қазіргі таңда Қазақстанда азаматтардың өз деректерін бақылау мүмкіндіктерін кеңейту, ұйымдардың ақпараттық қауіпсіздікке деген жауапкершілігін арттыру маңызды болып отыр. Сонымен қатар деректердің қорғалуын тек заңнама арқылы ғана емес, практикалық тетіктер мен заманауи технологиялар арқылы қамтамасыз ету қажет. Автоматты қауіп-қатерді анықтау, алдын алу жүйелерін енгізу жеке деректердің қауіпсіздігін күшейтуге және цифрлық ортаға деген сенімді арттыруға мүмкіндік береді. Азаматтардың көпшілігі өз деректерінің қалай жиналып, қай жерде сақталатынын нақты біле бермейді. Осыған байланысты халық арасында ақпараттық қауіпсіздік бойынша түсіндіру жұмыстарын күшейту маңызды. Сонымен қатар ұйымдар

деректермен жұмыс істеу барысында қауіпсіздік талаптарын формалды емес, күнделікті тәжірибеде нақты іске асыруы тиіс.



Сурет 1. Жеке деректерге бағытталған кибершабуыл түрлерінің үлесі (%)

Талқылау

Жүргізілген зерттеу жеке деректерді қорғаудың маңызын және бұл салада қалыптасқан жағдайдың күрделілігін айқын көрсетті. Алынған нәтижелер киберқауіпсіздік тек техникалық мәселе емес, сонымен қатар құқықтық, әлеуметтік және мәдени аспектілермен де тығыз байланысты екенін дәлелдейді.

- Бірінші кезекте, кибершабуылдардың саны артып келе жатқанын ескерсек, жеке деректердің қорғалуына деген қажеттілік бұрынғыдан да өзекті бола түсті. Бұл мәселе тек мемлекеттік бақылаумен шектелмей, әрбір ұйым өз ішкі ақпараттық қауіпсіздік жүйесін жүйелі түрде жетілдіруі тиіс. Себебі техникалық қорғаныс шаралары жеткіліксіз болған жағдайда, деректердің тарап кету қаупі жоғарылайды.

- Екіншіден, деректер қауіпсіздігіне әсер ететін негізгі факторлардың бірі - адам. Зерттеу барысында көпшілік өз жеке мәліметтерінің қауіпсіздігіне салғырт қарайтыны байқалды. Бұл - ақпараттық сауаттылықтың төмен екенін көрсетеді. Осыған байланысты киберқауіпсіздік мәдениетін қалыптастыру - білім беру жүйесінің маңызды бір бағыты болуы керек. Әсіресе мектептер мен жоғары оқу орындарында ақпараттық қауіпсіздік негіздерін оқыту - алдағы онжылдықтағы басымдықтардың бірі болуы қажет.

- Үшіншіден, халықаралық тәжірибені негізге ала отырып, Қазақстанда GDPR секілді деректерді қорғау ережелерін кезең-кезеңмен енгізу тиімді қадам болар еді. Мұндай жүйелер азаматтардың құқықтарын нақты белгілеп, деректермен жұмыс істейтін ұйымдардың жауапкершілігін арттырады. Сонымен қатар, бұл шаралар электронды үкімет пен цифрлық қызметтердің қауіпсіздігі мен сенімділігін күшейтеді.

- Төртіншіден, зерттеу барысында отандық бағдарламалық шешімдердің тапшылығы анықталды. Көптеген мекемелер шетелдік технологияларға тәуелді. Бұл жағдай ұлттық ақпараттық тәуелсіздікке қауіп төндіреді. Сондықтан қазақстандық IT-

саланың дамуына ерекше көңіл бөлініп, отандық өнімдер мен шешімдерді қолдауға бағытталған мемлекеттік бағдарламалар әзірленуі тиіс.

•Бесіншіден, жеке деректерді қорғау тек заңнамамен шектеліп қалмауы керек. Қоғамда ақпараттық мәдениетті қалыптастыру - осы саладағы ұзақмерзімді шешімдердің бірі. Азаматтар өздері туралы қандай ақпаратты ашық жариялауға болады, ал қандай мәліметтер құпия болып қалуы керек екенін түсінуге тиіс. Бұл үшін мемлекет пен бұқаралық ақпарат құралдары бірлесе отырып, ақпараттық-ағартушылық шараларды жүргізуі қажет.

Жалпы алғанда, зерттеу нәтижелері қазіргі жүйеде көптеген осал тұстардың бар екенін көрсетті. Бұл бағытта өзгерістер кешенді түрде жүргізілуі қажет - тек құқықтық шеңберде ғана емес, институционалдық және технологиялық деңгейлерде де реформа жасау маңызды. Сонда ғана жеке деректерді тиімді қорғауға мүмкіндік туады.

Өзгеріс түрі	2024 жылғы мән	2025 жылғы мән	Өзгеріс (%)
Жалпы кибершабуылдар саны	15 000 оқиға	30 000 оқиға	+100 %
Botnet шабуылдар	1 700 оқиға	17 600 оқиға	+935 %
Phishing шабуылдары	-	2 000 оқиға	+37 %
Вирустар, трояндар, worm-тар	9 600 оқиға	7 900 оқиға	-17.9 %

Кесте 1. Қазақстандағы қаңтар-мамыр 2025 кезеңіндегі кибершабуылдар статистикасы

Қорытынды

Жүргізілген зерттеу қазіргі қоғамдағы киберқауіпсіздіктің стратегиялық маңызын айқын көрсетті. Жеке деректерді қорғау - тек техникалық мәселе емес, ол әлеуметтік, құқықтық және мәдени факторлармен өзара байланыста қарастырылатын күрделі сала екені дәлелденді.

Зерттеу барысында кибершабуылдардың жиілеп, азаматтардың жеке деректерінің жиі заңсыз таралуы бұл салада жаңа әрі тиімді тәсілдерді енгізу қажеттігін көрсетті. Қазақстанда қабылданған заңнамалық актілер бар болғанымен, оларды іске асыру деңгейі төмен, ал азаматтардың киберсауаттылығы жеткіліксіз күйде қалып отыр (МТҚ, 2023). Бұл жағдай тек мемлекеттік құрылымдардың ғана емес, білім беру мекемелері мен бүкіл қоғамның бірлескен әрекетін талап етеді. Жалпы, зерттеу негізінде келесі тұжырымдар жасалды:

- Жеке деректерді қорғау үшін заңнамалық база жеткілікті түрде жетілдіріліп, оның тәжірибеде нақты жүзеге асуы қамтамасыз етілуі қажет;
- Ақпараттық қауіпсіздік мәдениетін қалыптастыру -елдің цифрлық даму жолындағы маңызды басымдықтардың бірі;
- Халықтың киберсауаттылығын жүйелі түрде арттыру -қауіпсіз әрі тұрақты цифрлық қоғам құрудың алғышарты;
- Ұлттық деңгейде отандық бағдарламалық шешімдер мен қорғау технологияларын дамыту қажет (Kaspersky Security Bulletin, 2023). Қорытындылай келе, киберқауіпсіздік пен жеке деректерді қорғау тек IT мамандарының емес, әрбір азаматтың саналы жауапкершілігіне айналуы тиіс. Бұл бағытта үйлесімді саясат пен жан-жақты қолдау көрсетілсе, мемлекет тұрақты цифрлық дамуға қол жеткізіп, азаматтардың құқықтарын толыққанды қорғай алады.

Әдебиет:

1. Қазақстан Республикасының «Жеке деректер және оларды қорғау туралы» Заңы. 2013 жылғы 21 мамырдағы №94-V. - <https://adilet.zan.kz/kaz/docs/Z1300000094>
2. European Parliament and Council. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. - <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
3. ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі. Ресми сайт. - <https://www.gov.kz/memleket/entities/cdiai?lang=kk>
4. Мемлекеттік техникалық қызмет (МТҚ). Киберқауіпсіздік бойынша 2023 жылғы есеп. - <https://www.nitec.kz/>
5. Kaspersky Security Bulletin. Threat Predictions for Industrial Cybersecurity. - <https://www.kaspersky.com/blog>
6. Group-IB. Hi-Tech Crime Trends 2023/2024. - <https://group-ib.com/resources/threat-research/>
7. Times of Central Asia. *Cyberattacks Double in Kazakhstan in Early 2025* - <https://timesca.com/cyberattacks-double-in-kazakhstan-in-early-2025>

References:

1. Law of the Republic of Kazakhstan On Personal Data and Their Protection. No. 94-V dated May 21, 2013. Available at: <https://adilet.zan.kz/kaz/docs/Z1300000094>
2. European Parliament and Council. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
3. Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan. Official website. Available at: <https://www.gov.kz/memleket/entities/cdiai?lang=kk>
4. State Technical Service. Cybersecurity Report for 2023. Available at: <https://www.nitec.kz/>
5. Kaspersky Security Bulletin. Threat Predictions for Industrial Cybersecurity. Available at: <https://www.kaspersky.com/blog>
6. Group-IB. Hi-Tech Crime Trends 2023/2024. Available at: <https://group-ib.com/resources/threat-research/>
7. Times of Central Asia. *Cyberattacks Double in Kazakhstan in Early 2025*. Available at: <https://timesca.com/cyberattacks-double-in-kazakhstan-in-early-2025>

Information about the authors:

Nabi A.A. – corresponding author, master's student, Department of Information and Communication Technologies, Manash Kozybayev North Kazakhstan University NPLC, Petropavlovsk, Kazakhstan; e-mail: akbayannabieva@gmail.com