ҒТАХР 81.93.29 DOI: https://doi.org/10.62687/STJ.7.1.2025.8

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ЭЛЕКТРОНДЫҚ МЕМЛЕКЕТТІК ҚЫЗМЕТТЕРДЕГІ ДЕРЕКТЕРДІҢ ҚҰПИЯЛЫЛЫҒЫН БАСҚАРУ ТЕТІКТЕРІ

[1]Ә.Ж. Алимгазиева*, **[2]Д.С. Байгожанова**
[1,2]Астана халықаралық университеті, Астана, Қазақстан
*e-mail: aliya_alimgazieva@aiu.edu.kz

Ә.Ж. Алимгазиева – техника ғылымдарының магистрі, ақпараттық технологиялар және инженерия жоғары мектебінің оқытушысы, Астана халықаралық университеті, Астана, Қазақстан, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

Д.С. Байгожанова – педагогика ғылымдарының кандидаты, ақпараттық технологиялар және инженерия жоғары мектебінің қауымдастырылған профессоры, Астана халықаралық университеті, Астана, Қазақстан, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Аңдатпа. Зерттеу жұмысы Қазақстан Республикасындағы цифрлық қызметтерді ұсыну барысында деректерді қорғауды қамтамасыз ету механизмдеріне талдауға арналған. Цифрландыру үдерісінің қарқынды дамуы мемлекеттік қызметтердің қолжетімділігін арттыру, дербес деректердің қауіпсіздігі мен құпиялылығын қорғау мәселесін өзекті ете түсуде. Зерттеу аясында электрондық үкімет жүйесінде қолданылатын құқықтық, ұйымдастырушылық және технологиялық механизмдер қарастырылып, олардың тиімділігіне талдау жасалады. Зерттеу барысында сапалы талдау, салыстырмалы әдістер және жеке деректерді қорғауды реттейтін нормативтік-құқықтық базаларға шолу жасалады. Деректерді өңдеуге, сақтауға және ведомствоаралық ақпарат алмасуға байланысты негізгі тәуекелдер мен осалдықтарды анықтауға ерекше назар аударылады. Сонымен қатар, деректердің құпиялылығын қамтамасыз етудегі негізгі тәуекелдер мен проблемалар айқындалып, халықаралық тәжірибемен салыстыру жүргізіледі. Зерттеу нәтижелері Қазақстанның цифрлық мемлекеттік жүйелерде ақпараттық қауіпсіздік деңгейін арттыруға бағытталған практикалық ұсыныстарды қалыптастыруға мүмкіндік береді.

Түйін сөздер: цифрлық мемлекеттік қызметтер, ақпараттық жүйелер, электрондық үкімет, дербес деректер, ақпараттық қауіпсіздік, деректердің құпиялылығы.

МЕХАНИЗМЫ УПРАВЛЕНИЯ КОНФИДЕНЦИАЛЬНОСТЬЮ ДАННЫХ В ЭЛЕКТРОННЫХ ГОСУДАРСТВЕННЫХ УСЛУГАХ РЕСПУБЛИКИ КАЗАХСТАН

[1]Ә.Ж. Алимгазиева*, [2]Д.С. Байгожанова
[1,2]Международный университет Астана, Астана, Казахстан
*e-mail: aliya_alimgazieva@aiu.edu.kz

Ә.Ж. Алимгазиева – магистр технических наук, преподаватель высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

Д.С. Байгожанова – кандидат педагогических наук, ассоциированный профессор высшей школы информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Аннотация. Исследовательская работа посвящена анализу механизмов обеспечения защиты данных при предоставлении цифровых услуг в Республике Казахстан. Динамичное развитие процесса цифровизации делает актуальным вопрос повышения доступности

государственных услуг, защиты безопасности и конфиденциальности персональных данных. В рамках исследования рассматриваются правовые, организационные и технологические механизмы, используемые в системе электронного правительства, проводится анализ их эффективности. В ходе исследования дается обзор нормативно-правовых баз, регулирующих качественный анализ, сравнительные методы и защиту персональных данных. Особое внимание уделяется выявлению основных рисков и уязвимостей, связанных с обработкой, хранением данных и межведомственным обменом информацией. Кроме того, будут выявлены основные риски и проблемы в обеспечении конфиденциальности данных, проведено сравнение с международным опытом. Результаты исследования позволят сформировать практические рекомендации, направленные на повышение уровня информационной безопасности Казахстана в цифровых государственных системах.

Ключевые слова: цифровые государственные услуги, информационные системы, электронное правительство, персональные данные, информационная безопасность, конфиденциальность данных.

DATA PRIVACY MANAGEMENT MECHANISMS IN ELECTRONIC PUBLIC SERVICES OF THE REPUBLIC OF KAZAKHSTAN

[1]A.Zh. Alimgaziyeva*, [2]D.S.Baigozhanova
[1,2]Astana International University, Astana, Kazakhstan
*e-mail: aliya_alimgazieva@aiu.edu.kz

A.Zh. Alimgaziyeva – master of technical sciences, Lecturer at the Higher School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: aliya_alimgazieva@aiu.edu.kz, https://orcid.org/0009-0005-4488-3305

D.S. Baigozhanova – PhD, Associate Professor, School of Information Technology and Engineering, Astana International University, Astana, Kazakhstan, e-mail: dametken_baigozanova@aiu.edu.kz, https://orcid.org/0009-0001-9310-3118

Abstract. The research paper is devoted to the analysis of data protection mechanisms in the provision of digital services in the Republic of Kazakhstan. The dynamic development of the digitalization process makes the issue of increasing the availability of public services, protecting the security and confidentiality of personal data relevant. The study examines the legal, organizational and technological mechanisms used in the e-government system, and analyzes their effectiveness. The study provides an overview of the regulatory frameworks governing qualitative analysis, comparative methods, and personal data protection. Special attention is paid to identifying the main risks and vulnerabilities related to data processing, storage and interagency information exchange. In addition, the main risks and problems in ensuring data confidentiality will be identified and compared with international experience. The results of the study will make it possible to form practical recommendations aimed at improving the level of information security of Kazakhstan in digital government systems.

Keywords: Digital Public Services, Information Systems, e-Government, personal data, information security, data privacy.

Кіріспе. Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктері қоғамды цифрландыру және электрондық үкіметті белсенді енгізу жағдайында дербес деректерді қорғау мәселелері өзекті бола түсуде. Қазақстан Республикасы цифрлық сервистерді белсенді дамыта отырып және өз азаматтарына мемлекеттік қызметтерге онлайн-форматта қол жеткізуді қамтамасыз етуге ұмтыла отырып, ерекшелік болып табылмайды. Алайда, ыңғайлылық пен тиімділікпен қатар, рұқсатсыз кіруге, ақпараттың ағып кетуіне және құпиялылықтың бұзылуына байланысты тәуекелдер де артады.

Электрондық мемлекеттік қызметтердегі деректердің құпиялылығын басқару техникалық және нормативтік аспектілерді қамтитын көп қырлы міндет болып табылады. Халықаралық стандарттарға сәйкес келетін және қазақстандық заңнаманың ерекшелігін

ескеретін тиімді қорғау тетіктерін әзірлеу және енгізу қажет. Азаматтардың ақпаратты бақылау және оларға қол жеткізу құқығына кепілдік бере отырып, деректерді өңдеу процестерінің ашықтығын қамтамасыз ету маңызды.

Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктерін зерттеу маңызды ғылыми міндет болып табылады. Қолданыстағы құқықтық нормалар мен техникалық шешімдерге талдау жүргізу, олқылықтар мен кемшіліктерді анықтау, дербес деректерді қорғау жүйесін жетілдіру жолдарын ұсыну қажет. Осы зерттеудің нәтижелері азаматтардың электрондық мемлекеттік қызметтерге деген сенім деңгейін арттыруға ықпал ететін нормативтік-құқықтық базаны жақсарту және тиімді техникалық шешімдерді енгізу жөніндегі ұсынымдарды әзірлеу үшін пайдаланылуы мүмкін.

Қазақстан Республикасының электрондық үкімет қызметтері жүйесіндегі деректердің құпиялылығын басқарудың қолданыстағы тетіктерін талдау елімізде жеке ақпаратты қорғаудың көп деңгейлі моделі жасалғанын көрсетеді, оған құқықтық, ұйымдастырушылық және технологиялық компоненттер кіреді. Дегенмен, бұл модельдің тиімділігі көбінесе оларды іс жүзінде енгізудің тұрақтылығына және цифрлық үкіметтің институционалдық жетілу деңгейіне байланысты. Құқықтық тұрғыдан алғанда, Қазақстанда электрондық үкімет жүйелерінде деректерді жинауды, өңдеуді, сақтауды және беруді реттейтін жеке деректерді қорғаудың негізгі нормативтік базасы бар. Дегенмен, реттеуші талаптар мен орындау тетіктері арасында алшақтық анықталды. Атап айтқанда, заңнамалық ережелер көбінесе декларативтік сипатта болады және әрқашан толыққанды бақылау, аудит және есеп беру рәсімдерімен бірге жүре бермейді, бұл деректердің құпиялылығын нақты қорғау деңгейін төмендетеді.

Ұйымдық құпиялылықты басқару тетіктері мемлекеттік органдар арасында рөлдер мен өкілеттіктерді бөлу, сондай-ақ лауазымды тұлғалардың ақпараттық ресурстарға қол жеткізуін реттеу арқылы жүзеге асырылады.

Талдау көрсеткендей, ведомствоаралық деректер алмасу цифрлық мемлекеттің негізгі элементі болғанымен, жүйенің ең осал буындарының бірі болып табылады. Қолжетімділікті басқару тәсілдерінің жеткіліксіз біріздендіруі және бірыңғай есеп беру моделінің болмауы жеке деректерді рұқсатсыз пайдалану қаупін арттырады.

E-gov порталы және мобильді қосымша ("Ұлттық Ақпараттық Технологиялар" АҚ операторы) арқылы биометриялық аутентификация (бет, саусақ іздері). Электрондық үкіметтің мемлекеттік қызметі арқылы келісім бойынша автоматтандырылған құралдар; электрондық үкіметтің инфрақұрылым операторы жүзеге асыратын иесіздендіру. Шифрлау, резервтік көшірмелер және мемлекеттік техникалық қызмет аудиттері; академиялық әдебиеттерде тұтастық үшін ұсынылған блокчейн (әлі кеңінен енгізілмеген). Қол жеткізу және аутентификация: биометрия мен сеансты басқару; рұқсатсыз кірудің алдын алу бойынша жалпы ұсыныстар (СІМ және ПҚИ іс жүзінде қолданылады, бірақ барлық көздерде нақты көрсетілмеген). Әрі интерфейстері және электрондық үкімет арқылы бақыланатын алмасу; мемлекеттік қызмет арқылы расталған келісім. Жою және инциденттерге ден қою: мақсатты орындау немесе келісімді қайтарып алу кезінде Міндетті түрде жою; 1 күн ішінде бұзушылық туралы хабарлама; оқиғалар туралы хабарлау және оның салдарын барынша азайту.

Зерттеу материалдары мен әдістері. Зерттеу әдістері ретінде: нормативтік құжаттарды талдау, жарияланымдарды контент-талдау, мемлекеттік органдар мен IT-компаниялардың өкілдерімен сараптамалық сұхбаттар, сондай-ақ халықаралық тәжірибені салыстырмалы талдау пайдаланылды.

Зерттеу сұрақтары: Қазақстан Республикасының электрондық мемлекеттік қызметтеріндегі деректердің құпиялылығын басқару тетіктерін қандай нормативтік-құқықтық актілер реттейді? Мемлекеттік ақпараттық жүйелерде дербес деректерді қорғау үшін қандай техникалық және ұйымдастырушылық шаралар қолданылады? Қазақстан Республикасының электрондық мемлекеттік қызметтерінде деректердің құпиялылығын қамтамасыз етуде қандай проблемалар мен кемшіліктер бар?

Ұсынылған гипотеза: Қазақстан Республикасының электрондық мемлекеттік қызметтерінде деректердің құпиялылығын басқару тетіктерін жетілдіру тиімді Нормативтік-құқықтық, техникалық және ұйымдастыру шараларын әзірлеу мен енгізуді, сондай-ақ азаматтар мен мемлекеттік қызметшілердің дербес деректерді қорғау мәселелері туралы хабардарлығын арттыруды қамтитын кешенді тәсілді талап етеді.

Зерттеу кезеңдері:

1. Нормативтік-құқықтық базаны талдау.
2. Техникалық және ұйымдастырушылық шараларды бағалау.
3. Проблемалар мен кемшіліктерді анықтау.
4. Ұсынымдар әзірлеу.

Зерттеу әдістері: нормативтік құжаттарды талдау, жарияланымдарды мазмұнды талдау, сараптамалық сұхбаттар, салыстырмалы талдау.

Технологиялық қорғау механизмдері, соның ішінде аутентификация, шифрлау және қол жеткізуді тіркеу жүйелері, жалпы алғанда, қазіргі заманғы ақпараттық қауіпсіздік талаптарына сәйкес келеді. Дегенмен, оларды енгізу фрагменттелген және кейбір жағдайларда деректердің өмірлік циклін басқаруға емес, негізінен инфрақұрылымды қорғауға бағытталған. Бұл деректерді басқару тұжырымдамасына қарағанда техникалық тәсілдің басым екенін көрсетеді, мұнда құпиялылық ақпаратты өңдеудің барлық кезеңдерінде басқарылатын процесс ретінде қарастырылады.

Электрондық үкімет қызметтерінде қолданылатын интеллектуалды жүйелер мен аналитикалық платформалардың әсері 2026 жылы ерекше маңызды болады. Жасанды интеллект пен үлкен деректер технологияларын пайдалану, тіпті анонимдеу талаптары ресми түрде орындалған кезде де деректер субъектілерін қайта сәйкестендіру қаупін арттырады. Осыған байланысты қолданыстағы құпиялылықты басқару механизмдері жаңа технологиялық қиындықтарға шектеулі бейімделуді көрсетеді.

Негізгі заң - "Дербес Деректер және Оларды Қорғау туралы" Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы (ХДП Заңы, 2020-2025 жж.өзгертілген). Ол келісім принциптерін, мақсаттарды шектеуді, деректерді азайтуды, иесіздендіруді және жоюды анықтайды. Негізгі қолдау заңдарына мыналар жатады: "Ақпараттандыру туралы" заң (электрондық ресурстардың ерекшеліктері және электрондық үкіметтің интеграциясы). "Жасанды интеллект туралы" № 230-VIII заң (2025/2026 жылғы 18 қаңтардан бастап күшіне енеді), ол жеке деректер ережелерін сақтауды және жасанды интеллект жүйелері үшін тәуекелдерді басқаруды міндеттейді. Алдағы цифрлық кодекс (2026 жылдың 11 шілдесінен бастап күшіне енеді), ол жою, өңдеуді тоқтата тұру және 15 күндік әрекет ету міндеттемелерін жүйелейді. Қосымша талаптар (2024 жылғы түзетулерден бастап): бір жұмыс күні ішінде министрлікке бұзушылықтар туралы міндетті түрде хабарлау; 2025 жылғы 8 қаңтардан бастап Қазақстанда деректерді локализациялау; келісімді басқару үшін барлық жүйелерді "мемлекеттік қызмет" электрондық үкіметімен біріктіру.

Талдау және нәтижелер. Халықаралық тәжірибелермен салыстырмалы талдау Қазақстанда цифрлық қызметтердің жобалау кезеңінде кіріктірілген құпиялылықты қорғауды білдіретін жобалау бойынша құпиялылық принципі жеткіліксіз дамығанын көрсетеді.

Құпиялылықты басқару көбінесе реактивті, жүйелік тәуекелдерді басқаруға емес, оқиғалардың алдын алуға бағытталған. Осылайша, жүргізілген талдау Қазақстан Республикасының электрондық үкімет қызметтері жүйесіндегі деректердің құпиялылығын басқарудың қолданыстағы тетіктері институционалдық даму сатысында деген қорытынды жасауға мүмкіндік береді. Оларды одан әрі жетілдіру үшін фрагменттелген қауіпсіздік шараларынан халықаралық стандарттарға негізделген кешенді деректерді басқару моделіне көшу, ведомствоаралық үйлестіру және жеке ақпаратты өңдеудегі ашықтықты арттыру қажет.

Жеке бас деректерін қорғау кезеңдері. Бұл бөлім кестеде анықталған тізбекті кезеңдерді синтездейді және оларды азаматтардың деректерін жинаудан қолжетімділікке

дейін қорғау мәселесімен байланыстырады. Дереккөздер деректерді өңдеудің өмірлік циклінің элементтеріне баса назар аударады және қорғауды қалыптастыратын құжатталған оқиғалар мен басқарудағы олқылықтарды атап өтеді. Кезеңдер тізімі Деректерді жинау және сәйкестендіру, өңдеу және агрегациялау, сақтау және тұтастықты сақтау, қолжетімділік және аутентификация, ведомствоаралық бөлісу және өзара әрекеттесу, сақтау және жою, сондай-ақ оқиғаларға жауап беру және есеп беру әдебиетте баса назар аударылатын өмірлік цикл кезеңдері болып табылады (Әміров, 2023: 143–151).

Ауқымды ағып кетулер: 2018-2025 жылдар аралығында 16,3 миллион азаматқа (аты-жөні, Жсн, мекен-жайы, телефондары) әсер еткен Қазақстан тарихындағы ең ірі бұзушылықпен (2025 жылдың маусымы) аяқталған көптеген оқиғалар болды. Бұрынғы жағдайларға мыналар жатады zaimer.kz (2 миллион жазба, 2024) және GitHub экспозициялары. Мемлекеттік жүйелер көбінесе тікелей ақпарат көзі болған жоқ, бірақ ескірген немесе жеке толықтырылған мәліметтер кеңінен таралды. Бөлшектелген енгізу және дизайн бойынша құпиялылықтың болмауы (gdpr-ге қарағанда). Ведомствоаралық ақпарат алмасу жеткіліксіз бірігуге байланысты осалдық болып қала береді. Жасанды интеллект, үлкен деректер тәуекелдері (ресми анонимизациядан кейін де қайта сәйкестендіру) жеткіліксіз шешіледі, дегенмен 2025 жылғы жасанды интеллект Туралы Заң мен 2026 жылғы цифрлық кодекс бұл олқылықты азайта бастады. Құқық қолдану әлсіз: заңдар ішінара декларативті болып қала береді, тексерулер шектеулі және тәуекелдерді алдын-ала басқарудан гөрі реактивті. Халықаралық алшақтық: Қазақстандық режим GDPR сәйкестік стандарттарына сәйкес келмейді (әлсіз келісім, міндетті DPIA болмауы, қатаң санкциялар). (Әміров, 2025: 151-157)

Тәуекелдің дәлелдері 2018-2025 жылдар аралығында Қазақстанда ірі көлемдегі жеке бас деректерінің таралуы мен бұзушылықтар туралы хабарланған, бұл қорғаудың әрбір кезеңіне назар аударуға итермелейді (Досжанова, Бұғыбай, 2024: 339–350).

Идентификацияға баса назар аудару жеке бас деректерін өңдеу және жүйеге кіру кезінде биометриялық сәйкестендіруді (бет-әлпет, саусақ іздері) пайдалану электрондық үкіметті енгізудің бөлігі ретінде айқын сипатталған (Әмірова, 2025), (Умитчинова, 2025) Мақала АИ және цифрлық басқару контекстінде дербес деректерді қорғауды реттеудің құқықтық аспектілерін қарастырады, халықаралық тәжірибені және оның Қазақстанда қолданылуын талдайды-цифрлық басқару мен деректерді қорғауды талқылау үшін өзекті.

Техникалық механизмдердің кезеңдері бойынша талдау сипаттамасы. Бұл бөлімде әдебиеттермен бірге әрбір өмірлік цикл кезеңі үшін нақты талқыланған немесе ұсынылған негізгі техникалық механизмдер көрсетілген. Алғашқы абзацта механизмдерді кезеңдерге сәйкестендіру және дәлелдердің әлсіз немесе осал тұстарын белгілеу мақсаты түсіндіріледі. Төменде кезеңдердің, типтік әрекеттердің, әдебиетте талқыланған механизмдердің және дәлелдемелердің күші туралы ескертпелердің қысқаша салыстырмалы кестесі берілген (Кесте-1).

Кесте 1. Техникалық механизмдерді зерттеу және дәлелдеу кезеңдері бойынша салыстырмалы талдау сипаттамасы

Кезең	**Зерттеулер**	**Әдебиетте талқыланған техникалық механизмдер**	**Дәлелдер**
Жинау және сәйкестендіру	Жеке басты куәландыру атрибуттарын алу, биометриялық деректерді тіркеу	Жеке басты куәландыру және порталға кіру үшін биометриялық аутентификация (түр-әлпет, саусақ іздері)	Қазақстанның электрондық үкімет жүйелері үшін жақсы құжатталған
Өңдеу және агрегациялау	Индекстеу, байланыстыру, аналитика	Қауіпсіз өңдеуге қойылатын жалпы талаптар және автоматтандырылған өңдеуге қойылатын шектеулер	Жоғары деңгейде сипатталған; нақты әдістер толыққанды сипатталмаған

Кезең	Зерттеулер	Әдебиетте талқыланған техникалық механизмдер	Дәлелдер
Сақтау және тұтастық	Хостинг, сақтық көшірме жасау, құқық бұзудан қорғау	Тұтастық пен қауіпсіздікті қамтамасыз ету үшін блокчейн ұсыныстары (болашақ шешім ретінде талқыланады) (Ильясова және т.б., 2025)	Әдебиетте ұсынылған; іске асыру мысалдары расталмаған
Қолжетімділік және аутентификация	Пайдаланушы/агент кіруі, авторизациялау, сеансты басқару	Қолжетімділікке арналған биометрия; рұқсатсыз кірудің алдын алу бойынша жалпы ұсыныстар (Кассен, 2015).	Биометрия құжатталған; берілген дереккөздерде нақты көрсетілмеген басқа аутентификация механизмдері (мысалы, MFA, PKI) (Кассен, 2015).
Бөлісу және өзара әрекеттесу	Ведомствоаралық деректер алмасу, API интерфейстері	Деректерді бөлісуге арналған басқару және саясат негіздері; техникалық механизмдер көрсетілмеген (Қожанұлы және т.б., 2023: 68–76).	Әдебиеттерде басқарудағы олқылықтар және бақыланатын бөлісу қажеттілігі атап өтілген (Қожанұлы және т.б., 2023: 68–76).
Сақтау, жою, аудит	Жазбаларды сақтау кестелері, қауіпсіз жою, аудит журналдары	Бұзушылықтардан кейін құқықтық/техникалық қорғаныс шаралары мен қалпына келтіру механизмдеріне шақырулар (Қоғабаев, Банерджи, 2024)	Заңды/нормативтік күтулер атап өтілді; техникалық енгізулер (қауіпсіз жою) егжей-тегжейлі сипатталмаған (Қоғабаев, Банерджи, 2024)
Оқиғаға жауап беру және есеп беру	Бұзушылықтарды анықтау, хабарлау, санкциялар	Бұзушылықтардан кейін сілтеме жасалған заңды жауапкершілік және құқықтарды қалпына келтіру ережелері[9]	Заңды шаралар талқыланды; техникалық анықтау/ криминалистикалық мәліметтер шектеулі (Қоғабаев, Банерджи, 2025: 183-207)

Шифрлау және RBAC туралы ескерту Берілген әдебиетте блокчейн және рұқсатсыз кіруден кеңірек қорғаныс сияқты тұтастықты сақтайтын технологиялар талқыланады, бірақ Қазақстанның электрондық үкімет жүйелеріндегі шифрлау/тасымалдау немесе рөлдік кіруді бақылауды орналастырудың нақты, егжей-тегжейлі сипаттамалары берілмеген; сондықтан берілген корпуста олардың нақты қолданылуын растау үшін жеткілікті дәлелдер жоқ Қазақстандық модель институционалдық-даму сатысында. Ол қауіпсіздіктің негізгі заманауи талаптарына (аутентификация, шифрлау) сәйкес келеді, бірақ өмірлік циклге емес, фрагменттелген және инфрақұрылымға бағытталған. 2025-2026 жылдарға арналған заңнамалық толқын (жасанды интеллект Туралы Заң, Цифрлық Кодекс, деректерді оқшаулау, бұзушылықтар туралы хабарлау) прогресті көрсетеді, дегенмен дизайн бойынша құпиялылық және жасанды интеллект тәуекелдерін белсенді басқару GDPR-мен салыстырғанда әлі де дамымаған. Ведомствоаралық алмасу ең әлсіз буын болып табылады және ауқымды ағып кетулер (2018-2025) құқық қорғау органдарындағы олқылықтарды көрсетеді. Жақсарту бойынша ұсыныстар (Түзетілген Және Кеңейтілген) Анықталған олқылықты жою және ғылыми / практикалық маңыздылығын арттыру: Барлық жаңа электрондық мемлекеттік қызметтер үшін дизайн бойынша құпиялылыққа және деректерді қорғауға әсерді міндетті бағалауды заңнамалық түрде бекіту (GDPR 25-Бабына сәйкес). Бірыңғай ведомствоаралық стандарттарды және деректермен алмасудың бірыңғай есеп беру моделін енгізу. Мемлекеттік ақпараттық жүйелерде жасанды интеллектті қайта анықтау тәуекелдерін жүйелі түрде тексеруді міндеттеңіз (2025 жылғы жасанды интеллект туралы Заңды қолдана отырып). Құқық қолдану практикасын күшейту: жаппай ағып кетулер үшін қылмыстық жауапкершілік (2026 жылға дейін ұсынылған) және әкімшілік айыппұлдарды көбейту. Азаматтар мен мемлекеттік қызметшілерді келісімнің күшін жою және деректерді беру құқықтары туралы хабардар

етудің жалпыұлттық бағдарламаларын іске қосыңыз (e-gov арқылы). Деректердің тұтастығы үшін блокчейн ұшқыштарын енгізіңіз (соңғы әдебиеттерде ұсынылғандай). Халықаралық эталондарды пайдалана отырып, жыл сайынғы тәуелсіз аудиттер жүргізіңіз және ашықтық туралы есептерді жариялаңыз. Бұл ұсыныстар дәлелді болып табылады, зерттеу сұрақтарына тікелей жауап береді және реактивтіден жүйелік тәуекелдерді басқаруға көшудің нақты жол картасын ұсынады. Іске асыру азаматтардың электрондық мемлекеттік қызметтерге деген сенімін едәуір арттырады. (Калашникова, 2021:73-79).

Қорытынды. Зерттеу нәтижелері дербес деректерді өңдеу, сақтау және беру мәселелерін реттейтін нормативтік-құқықтық базаны одан әрі жетілдіру қажеттігін көрсетеді. Ұлттық заңнаманы халықаралық стандарттармен және деректерді қорғау саласындағы озық тәжірибелермен үйлестіруге ерекше назар аудару қажет. Сондай-ақ, цифрлық қызметтерді ұсынатын мемлекеттік органдар мен ұйымдарда ақпараттың қауіпсіздігін қамтамасыз етуге бағытталған ұйымдастырушылық шаралардың тиімділігін арттыру маңызды аспект болып табылады. Бұған заманауи қауіпсіздік саясатын әзірлеу және енгізу, тұрақты аудиттер жүргізу және ақпаратты қорғау саласындағы қызметкерлердің біліктілігін арттыру кіреді.

Деректерді қорғаудың технологиялық шаралары үнемі жаңартылып, жаңа қауіптер мен сын-қатерлерге бейімделуді қажет етеді.

Шифрлаудың, аутентификацияның және деректерге қол жеткізуді бақылаудың заманауи технологияларын белсенді енгізу, сондай-ақ ақпараттық қауіпсіздік инциденттеріне мониторинг және ден қою жүйелерін дамыту қажет. Зерттеу нәтижелеріне негізделген ұсынылған ұсынымдар азаматтардың электрондық үкіметке және цифрлық сервистерге сенімін қамтамасыз етуге, сондай-ақ елдің цифрлық экономикасын одан әрі дамытуға ықпал етуге қабілетті Қазақстанның цифрлық ортасында деректерді қорғаудың кешенді жүйесін қалыптастыруға бағытталған.

Азаматтарға тікелей қатысты элементтерге - келісім, құқықтар, ашықтыққа - назар аударады және әдебиетте бар және егжей-тегжейлі ақпараттың жоқтығын түсіндіреді. Құпиялылық және жеке құқықтар әдебиеттерде жеке деректерді қорғау конституциялық құпиялылық құқықтары шеңберінде нақты көрсетілген және рұқсатсыз жариялау мен бақылауға қарсы заңды кепілдіктер талқыланады.

Ашық деректерді келісім және пайдалану Талдаулар келісімге қатысты юрисдикциялар арасындағы айырмашылықтарды, соның ішінде ашық көздерден (әлеуметтік желілерден) алынған деректерді келісімсіз пайдалануға рұқсат етілуі туралы пікірталастарды көрсетеді, бұл аймақтық контексте сәйкес келмейтін тәжірибелерді немесе түсіндірмелерді көрсетеді. Ашықтық және құқықтық қорғау құралдарына қол жеткізу.

Жұмыстар азаматтардың құқықтарын қалпына келтіру және бұзушылықтардан кейін құқықтық қорғау құралдарын алу үшін ашықтықты, есеп берушілікті және тетіктерді күшейтуге шақырады және олар жауапкершілік пен құқықтарды қалпына келтіруді көздейтін қолданыстағы заңнаманы атап өтеді.

Тәжірибелік олқылықтар әдебиеттерде құқықтық қорғау мен операциялық ашықтық немесе азаматтарға бағытталған механизмдер арасындағы алшақтықтар (мысалы, айқын келісім ағындары, биометриялық пайдаланудың түсіндірмелері) бірнеше рет құжатталады, бұл Қазақстанның цифрлық қызметтеріндегі азаматтыққа бағытталған кешенді енгізулер туралы жарияланған дәлелдердің жеткіліксіз екенін көрсетеді.

Ұсыныстың баса назары бірнеше дереккөздер биометриялық деректерге арналған құқықтық қорғауды күшейтуді, хабарландыру және қалпына келтіру процедураларын жақсартуды және деректерді бөлісу мен автоматтандырылған өңдеуге қатысты саясаттың ашықтығын арттыруды ұсынады.

Әдебиеттер

Әміров, 2023 - Әміров А. «Жеке деректерді қорғау саласындағы заңнаманың қазіргі жағдайы туралы (ҚР материалдары негізінде)», Расследование преступлений: проблемы и пути их решений, № 1(39), 143–151 беттер, 2023, doi: 10.54217/2411-1627.2023.39.1.018.[In Rus]
Әмірова, 2025 - Әмірова А., «Қазақстандағы азаматтарға бағытталған мемлекеттік қызметтерді ілгерілету: құқықтық, институционалдық және цифрлық басқару перспективалары». Қолжетімді: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1679601/full [In Eng]
Досжанова, Бұғыбай, 2024 - Досжанова А., Бұғыбай Д. «Ақпараттық-коммуникациялық технологиялар арқылы тұлғаның жеке басын анықтаудың қазіргі жай-күйі мен перспективалары», H. Dosmùhamedov atyndaġy Atyrau memlekettìk университетінің habaršysy, № 4(75), 2024, pp. 339–350, doi. 10.47649/vau.24.v75.i4.29.[In Kaz]
Ильясова және т.б., 2025 - Ильясова Г., Әйтімов Б., Жұмағұлов М. «Блокчейн технологиясын қолдана отырып, жеке деректердің қауіпсіздігін қамтамасыз ету: заңнаманы жетілдіру мәселелері мен перспективалары», №18, 2025. [Онлайн]. Қолжетімді: https://ascelibrary.org/doi/abs/10.1061/JLADAH.LADR-1248 [In Eng]
Кассен, 2015 – Кассен М. «Электрондық үкімет жүйелерін түсіну: Америка Құрама Штаттары мен Қазақстандағы электрондық федерализм және электрондық орталықтандыру», 2015 жылдың қарашасы, [Онлайн] Қолжетімді: https : //books.google.com/books?hl = en&lr = &id = zLK6CgAAQBAJ&oi = fnd&pg = PR5&dq = Kazakhstan + AND + (e − government + OR + %22digital + government%22 + OR + %22digital + services%22) + AND + (%22data + privacy%22 + OR + %22data+protection%22+OR+%22personal+data%22)+AND+(%22digital+archives%22+OR+%22electronic+records%22+OR + %22citizen + data%22)&ots = uVuINIvZO8&sig = zDcdzVEjfycMGh3aNxMsNHjuozw [In Eng]
Калашникова, 2021 - Калашникова Э. Б. «Жеке деректерді қорғау цифрландырудың негізі ретінде», 73–79 беттер, 2021 жылғы сәуір, doi: https : //doi.org/10.1007/978 − 3 − 030 − 83175 − 2_11.
Қожанұлы және т.б., 2023 - Қожанұлы С., Айтчанқызы А.Г., Борисовна Д.О. «Цифрландыру дәуіріндегі дербес деректерді қорғау: конституциялық-құқықтық аспект», Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының жаршысы, т. 3, жоқ. 74, 68–76 беттер, қыркүйек 2023, doi: https : //doi.org/10.52026/2788 − 5291_2023_74_3_68.
Қоғабаев&Банерджи, 2024 - Қоғабаев Т., Банерджи С. «Қазақстандағы ақылды басқару: дамудың, қиындықтардың және болашақ бағыттардың жүйелі шолуы мен талдауы», Vol. 1 No. 1 (2024) [Онлайн]. Қолжетімді: https://scrd.eu/index.php/scrd-pp/article/view/575 [In Eng]
Қоғабаев&Банерджи, 2025 - Қоғабаев Т., Банерджи С. «Қазақстандағы ақылды басқаруды дамыту: сандық бастамалар мен саясаттың салдарын сыни талдау», 2025, pp. 183-207. [Онлайн]. Қолжетімді: https : //link.springer.com/chapter/10.1007/978 − 3 − 032 − 07370 − 9_15 [In Eng]
Умитчинова, және т.б., 2025 – Умитчинова Б.А., Гаврилова Ю.А., Мензюк Г.А. "Жасанды интеллектті дамыту жағдайындағы дербес деректерді құқықтық реттеу: шетелдік тәжірибе және Қазақстан үшін сын-қатерлер", 2025.DOI: https : //doi.org/10.52026/2788 − 5291_2025_80_3_37 [In Rus]

References

Amirov, 2023-Amirov A. Zheke derekterdi qorġau salasyndagy zanamanyn qazirgi jaġdayy turaly (QR materialdary negizinde) [On the current state of legislation in the field of personal data protection (based on the materials of the Republic of Kazakhstan)]. Rassledovanie prestuplenii: problemy i puti ikh reshenii, No. 1(39), pp. 143–151, 2023. DOI: 10.54217/2411-1627.2023.39.1.018. [Rus]
Amirova, 2025- Amirova A. Qazaqstandaġy azamattarga baġyttalġan memlekettik qyzmetterdi ilgeriletu: quqyqtyq, institutsionaldyq zhane cifrlyq basqaru perspektivalary [Promoting citizen-oriented public services in Kazakhstan: legal, institutional and digital governance perspectives]. Available at: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025. 1679601/full, DOI: 10.3389/fpos.2025.1679601. [Eng]
Doszhanova & Bugybay, 2024- Doszhanova A., Bugybay D. Aqparattyq-kommunikaciyalyq tehnologiyalar arqyly tulġanyn zheke basyn anyqtawdyn qazirgi jaġdayy men perspektivalary [Current state and prospects of personal identification using information and communication technologies]. H. Dosmuhamedov atyndaġy Atyrau memlekettik universitetinin habarshysy, No. 4(75), pp. 339–350, 2024. DOI: 10.47649/vau.24.v75.i4.29. [Kaz]
Ilyasova et al., 2025 - Ilyasova G., Aitimov B., Zhumagulov M. Blokchein tehnologiyasyn qoldanu arqyly zheke derekterdin qauipsizdigin qamtamasyz etu: zanamany jetildiru maseleleri men perspektivalary [Ensuring personal data security using blockchain technology: issues and prospects for improving legislation]. Available at: https://ascelibrary.org/doi/abs/10.1061/JLADAH.LADR-1248, DOI: 10.1061/JLADAH.LADR-1248. [Eng]
Kalashnikova, 2021- Kalashnikova E. B. Zheke derekterdi qorġau cifrlanudyń negizi retinde [Personal data protection as the basis of digitalization]. 2021, pp. 73–79. DOI: https : //doi.org/10.1007/978 − 3 − 030 − 83175 − 2_11. [Rus]
Kassen, 2015- Kassen M. Understanding e-government systems: e-federalism and e-centralization in the USA and Kazakhstan [Understanding e-government systems: e-federalism and e-centralization in the USA and Kazakhstan]. November 2015. Available at: https://books.google.com/ [Eng]
Kogabayev & Banerjee, 2024- Kogabayev T., Banerjee S. Qazaqstandaġy aqyldy basqaru: damudyn, qiyndyqtardyn zhane bolashaq baġyttardyn zhuieli sholuy men taldauy [Smart governance in Kazakhstan: a systematic review and analysis of development, challenges and future directions]. Vol. 1, No. 1, 2024. Available at: https://scrd.eu/index.php/scrd-pp/article/view/575 [Eng]
Kogabayev & Banerjee, 2025 - Kogabayev T., Banerjee S. Qazaqstandaġy aqyldy basqarudy damytu: sandıq bastamalar men sayasattyn saldaryn syni taldau [Developing smart governance in Kazakhstan: a critical analysis of digital initiatives and policy implications]. 2025, pp. 183–207. DOI: https : //doi.org/10.1007/978 − 3 − 032 − 07370 − 9_15. [Eng]
Kozhanuly et al., 2023- Kozhanuly S., Aitchankyzy A. G., Borisovna D. O. Cifrlandyru dawirindegi derbes derekterdi qorġau: konstituciyalyq-quqyqtyq aspekt [Personal data protection in the era of digitalization: constitutional and legal aspects]. Qazaqstan Respublikasynyn Zanama zhane quqyqtyq aqparat instituty habarsysy, Vol. 3, No. 74, pp. 68–76, September 2023. DOI: https : //doi.org/10.52026/2788 − 5291_2023_74_3_68. [Kaz]
Umitchinova et al., 2025 - Umitchinova B. A., Gavrilova Yu. A., Menzyuk G. A. Razvitie iskusstvennogo intellekta usloviyakh pravovogo regulirovaniya personalnykh dannykh: zarubezhnyy opyt i vyzovy dlya Kazakhstana [Legal regulation of personal data in the context of artificial intelligence development: foreign experience and challenges for Kazakhstan]. 2025. DOI: https : //doi.org/10.52026/2788 − 5291_2025_80_3_37. [Rus]