

FTAMP 06.56.31

DOI: <https://doi.org/10.55871/2072-9847-2025-68-3-125-138>**Жұбаназаров С. А.***

PhD докторант

Қазтұтынуодағы Қарағанды университеті

Қарағанды қ., Қазақстан

e-mail: szhubanazar@gmail.com

ORCID: 0000-0002-0782-7719

Жаров Е. Қ.

Э.Ф.К

Қазақстан Республикасы Президентінің

жанындағы Мемлекеттік басқару академиясының

Ақмола облысы бойынша филиалының

директоры

Көкшетау қ., Қазақстан

e-mail: yerzhan.zharov@apa.kz

ORCID: 0000-0003-3567-4673

Кемелбек Р. Қ

сарапшы

«Жастар» ғылыми-зерттеу орталығы

Астана қ., Қазақстан

e-mail: kemelbek_rk@mail.ru

ORCID: 0009-0009-5485-5542

Турдиева З. М.

PhD

Alikhan Bokeikhan University

Семей қ., Қазақстан

e-mail: kalibaeva.z@mail.ru

ORCID: 0000-0002-6255-0599

МЕМЛЕКЕТТІК БАСҚАРУ ЖҮЙЕСІНДЕ АҚЫЛДЫ ҚАЛАЛАРҒА ТӘН КИБЕРҚАУІПСІЗДІКТІҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ

Аңдатпа. Бұл мақала ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздік мәселелерін қарастырады. Зерттеудің мақсаты – ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті дамытудың шешімдерін зерттеп және талдап, олардың заманауи киберқауіптерге қарсы тұрудағы ең тиімді жолын анықтау. Зерттеу барысында киберқауіпсіздікті қамтамасыз етудегі заманауи тәсілдер, соның ішінде ақпараттық қауіпсіздік стратегиялары, мемлекеттік және жеке сектор арасындағы ақпарат алмасу платформалары, жасанды интеллект технологияларын қолдану, сондай-ақ білікті кадрларды даярлау маңыздылығы жан-жақты талданды. Зерттеу әдістемесіне ғылыми деректерді талдау мен синтездеу, салыстырмалы талдауы, сондай-ақ киберқауіпсіздік және мемлекеттік басқару саласындағы сараптамалық, эмпирикалық сауалнама жүргізу әдістерін қамтиды. Сауалнама нәтижелері көрсеткендей, респонденттердің басым бөлігі киберқауіптерге қарсы тұрақтылықты арттыруда мемлекеттік органдар мен жеке сектор арасындағы тиімді ақпарат алмасуды негізгі фактор деп есептейді. Кибершабуылдарды ерте анықтау, тұрғындарды ақпараттандыру және үзіліссіз мониторинг жүргізу арқылы қауіпсіздікті қамтамасыз етудің негізгі элементтері ретінде қарастырылады. Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті қалыптастырудағы негізгі қиындықтар, сондай-ақ қауіпсіздікті қамтамасыз етудегі адам факторының рөлі екінші реттік мәліметтер базасының көмегімен қарастырылады. Зерттеу нәтижесі киберқауіпсіздік саласындағы саясатты жетілдіруге, тиімді басқару шешімдерін қабылдауға және қауіпсіз, сенімді «ақылды қала» экожүйесін қалыптастыруға үлес қосады. Сонымен қатар, экономикалық тиімділік көзқарасынан мемлекеттік жүйелердің кибершабуылдарға төзімділігін арттыра алатын болашақ трендтерге ерекше назар аударылады. Оған қоса зерттеудің соңында нәтижелер мен талдауларға сүйене отырып, Қазақстан Республикасының мемлекеттік басқаруына киберқауіпсіздікті дамыту бойынша ең тиімді шешімдер ұсынылды.

Түйін сөздер: ақылды қала, киберқауіпсіздік, мемлекеттік басқару, жасанды интеллект, цифрлық технология.

КІРІСПЕ

Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті дамытудың өзектілігі энергетика, көлік және қаржы сияқты маңызды жүйелерге кибершабуылдар санының өсуіне байланысты артып келеді. Оған қоса құпия деректер мен стратегиялық ақпаратты сақтауға байланысты мемлекеттік органдар шабуылдаушылар үшін негізгі нысанаға айналуда. Осы қауіптерге қарсы тұру үшін заманауи технологиялар мен киберқорғаныстың кешенді шешімдері қажет. Себебі деректерді қорғау заңнамасын сақтау және киберқауіпсіздіктің

озық технологияларын қолдану қазіргі сын-қатерлер жағдайында мемлекеттік органдардың тұрақты және қауіпсіз жұмыс істеуі үшін маңызды.

A. Asllani, C.S. White, L. Ettkin ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті арттыру үшін тиісті құқықтық, әлеуметтік және этикалық негізді құрудағы үкіметтің рөлін зерттейді [1]. Бұрынғы киберқауіпсіздік доктриналары қысқаша талданып, киберқауіпсіздіктің қоғамдық игілік ретінде қоғамдық игіліктермен салыстырады. Зерттеу үкіметтің киберқауіпсіздікті арттыру және киберқауіпсіздікті азайтудағы рөлін көрсететін мысалдар жиынтығымен аяқталады.

E. A. Kaijankoski мемлекеттік және жеке секторлардың ынтымақтастығына ақылды қалаларды дамытуға кедергі келтіретін мәселелерді анықтау және киберқауіпсіздік алмасуды ілгерілету үшін мемлекеттік-жекеменшік әріптестіктің (МЖӘ) тиімділігін бағалау үшін АҚШ-тың маңызды инфрақұрылымы саналатын банк және қаржы секторларын зерттейді. Олар мемлекеттік органдар мен жеке секторлар арасында ақпарат алмасуда неліктен проблемалар бар екенін анықтап, МЖӘ механизмінің ұлттық киберқауіпсіздік қажеттіліктерін қалай шешуге болатынын және өз кезегінде ашық диалогты ынталандыратын саясатты әзірлеу кезінде саясаткерлер ескеруі тиіс мәселелерді анықтайды [2].

A. Pollini және т.б. киберқауіпсіздік адами факторлардың маңыздылығын дәстүрлі түрде технологияға баса назар аударып, адам элементі әлсіз буын ретінде сипаттайды [3]. Жеке, ұйымдық және технологиялық факторлардың қалалардағы денсаулық сақтау ұйымдарының деректерін сапалық және сандық әдістерді пайдалана отырып, жетілген киберқауіпсіздік мәдениеті әрқашан жақсы нәтижеге әкелмейтінін және процедуралар арасындағы қайшылықтар осалдықтарды күшейтетінін анықтайды. Сонымен қатар, техникалық шешімдердің үйлесімі мен пайдаланушының хабардар болуының жоғарылауы киберқауіпсіздікті жақсы басқаруға көмектесетінін атап өтеді.

M. N. O. Sadiku, O. I. Fagbohunbe, S. M. Musa қазіргі әлемде маңызды болып саналатын компьютерлік желілерді кибершабуылдардан қорғау шарасына желі мен деректер қауіпсіздігін арттырудың шешімі ретінде кибершабуылдармен тиімді күресуге көмектесетін құрал негізінде жасанды интеллекттің маңыздылығына тоқталады [4]. Жасанды интеллекті (ЖИ) киберқауіпсіздікті арттыру құралы ретінде қосарланған рөліне назар аудара отырып, үздіксіз білім беру және бейімделу қажеттілігінің маңыздылығы атап көрсетіледі. Осылайша, жасанды интеллект киберқауіпсіздіктің болашағын түсінуге мүдделі кез келген адам үшін құнды ресурсқа айналып отыр.

R. Ramakrishnan, M. Leethial, S. Monisha зерттеулерінде жеке адамдар мен ұйымдардың алдағы жылдарда кездесуі мүмкін ықтимал қауіптерге шолу жасалады [5]. Бұл заттар интернетінің (IoT) осалдықтарын, жасанды интеллект (AI) және машиналық оқытуды (ML) пайдалануды, кванттық есептеулермен байланысты тәуекелдерді, бұлттық қауіпсіздік мәселелерін, әлеуметтік инженерия мен фишингтік шабуылдарды қамтиды. Осы қауіптерді түсіну арқылы жеке адамдар мен ұйымдар киберқауіпсіздік шараларын күшейту және цифрлық активтерін қорғау үшін белсенді стратегияларды әзірлей алады. Ынтымақтастық, технологиялық инновациялар және пайдаланушылардың хабардар болуы киберқауіпсіздік болашағын сәтті басқарудың және цифрлық инфрақұрылымымыздың тұтастығын қамтамасыз етудің маңызды шаралардың бірі болып отыр.

МАТЕРИАЛДАР МЕН ӘДІСТЕР

Зерттеуде ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті зерттеуде талдау және синтез әдістері, контент талдау, сызба деректер, биометрикалық негізде салыстырмалы логикалық әдіс және жүйелік тәсіл, сонымен бірге ақылды қалаларды басқарудағы киберқауіпсіздік мәселелерін зерделеу үшін сапалық және сандық әдістер қолданылды. Мемлекеттік басқару жүйесінде киберқауіпсіздікке қатысты проблемаларды тәжірибелік деңгейде анықтау мақсатында эмпирикалық сауалнама жүргізілді. Сауалнама Қазақстанның бес ірі қаласында (Астана, Алматы, Шымкент, Ақтөбе және Қарағанды) жүргізілді. Жи-

налған жауаптар «Google Forms» және «Microsoft Excel» бағдарламалары арқылы жүйеленіп, пайыздық көрсеткішпен есептелді. Нәтижелерді визуализациялау үшін диаграмма және жиілік кестелері пайдаланылды. Бұл әдіс зерттеліп отырған проблеманың практикалық маңыздылығын нақтылауға және мемлекеттік басқару құрылымындағы түйткілді тұстарды анықтауға мүмкіндік береді. Негізгі назар қазіргі заманғы киберқауіптерге қарсы тұру үшін мемлекеттік органдар қолданатын қолданыстағы стратегиялар мен құралдарды талдауға, сондай-ақ оларды дамытудың перспективалық бағыттарын анықтауға аударылады.

Сонымен қатар, сауалнама нәтижелері тек пайыздық көрсеткіштермен шектелмей, зерттеу нәтижелерінің нақтылығын арттыру мақсатында қарапайым статистикалық әдістерді қолдану да қарастырылды. Бұл әдістер киберқауіпсіздікке әсер ететін факторлар арасындағы байланыстарды тереңірек бағалауға мүмкіндік береді.

Сандық деректер Microsoft Excel бағдарламасында кодталды және диаграммалар арқылы визуализацияланды. Сапалық деректер контент-талдау әдісімен сарапталды. Респонденттердің түсіндірмелі жауаптары жиілікпен және тақырыптық жіктеу арқылы өңделді.

Сауалнама құралдарының сенімділігі мен валидтілігін қамтамасыз ету мақсатында алдын ала сараптамалық бағалау жүргізілді. Зерттеу қатысушылары зерттеу мақсаты мен шарттары туралы толық ақпарат алғаннан кейін саналы келісім (informed consent) берді. Барлық мәліметтер құпия және анонимді түрде өңделді. Тест нәтижесінде сұрақтардың түсініктілігі мен ішкі үйлесімділігі нақтыланып, негізгі сауалнама құрылымы бекітілді. Зерттеу қосымша деректерге, соның ішінде ғылыми жарияланымдарға, киберқауіпсіздік тақырыбына арналған аналитикалық материалдарға сүйенді. Деректер зерттеу тақырыбына сәйкестігі, негізділігі және дәлдігі негізінде таңдалды.

Қойылған зерттеу сұрақтарын шешу үшін Қазақстан Республикасы Үкіметінің қаулысымен бекітілген Киберқауіпсіздік тұжырымдамасының мазмұндық талдауы, сондай-ақ ақылды қалаларда киберқауіпсіздікті қамтамасыз ету тәжірибесіне салыстырмалы талдау жүргізілді. Маңызды инфрақұрылымды қорғау тәсілдерін, киберқауіпсіздікті қамтамасыз етуде жасанды интеллекті пайдалануды және киберқауіптердің алдын алудағы адам факторының рөлін зерделеуге ерекше назар аударылады.

Алынған нәтижелер негізінде экономикалық тиімділікке және технологиялық өзгерістерге бейімделуге бағытталған мемлекеттік жүйелердің кибершабуылдарға төзімділігін арттыру бойынша практикалық ұсыныстар тұжырымдалды.

НӘТИЖЕЛЕР ЖӘНЕ ТАЛҚЫЛАУ

Ақылды қалаларды мемлекеттік басқаруда киберқауіпсіздікті дамытудың маңызды мәселелерінің бірі – оның дамуындағы негізгі қиындықтарды жеңу. Бұл мәселелер бірнеше аспектілерге байланысты, соның ішінде технологиялық өзгерістер, халықаралық құқықтық талаптар және ресурстардың шектеулілігі бар.

Біріншіден, технологиялық өзгерістердің жылдамдығы цифрлық технологиялардың тез қарқынмен дамуы заңнамалық базаны үнемі жаңартуды талап етеді. Алайда, технологиялық прогресс соншалықты жылдам, заң шығарушылар әрдайым оның соңынан ере алмайды. Сондықтан мемлекет технологиялық инновациялармен бірге құқықтық жүйені де жетілдіру қажет.

Екіншіден, киберқұқықтың трансұлттық сипаты көбіне мемлекеттердің шекараларынан тыс жерде орын алады және халықаралық ынтымақтастықты қажет етеді. Мемлекеттер арасындағы ақпарат алмасу мен бірлескен операцияларды ұйымдастыру қиындықтары халықаралық юрисдикция мәселелерін туғызады. Осы қиындықтарды жеңу үшін мемлекеттер халықаралық құқықтық жүйелер мен келісімдер негізінде тығыз ынтымақтастық орнатуы тиіс.

Үшіншіден, қалалық маңызды инфрақұрылымға жасалатын шабуылдарға қарсы тұру үшін бірнеше кешенді стратегия мен шараларды қолданады. Бірақ, құқықтық негіздің жеткіліксіздігі көптеген елдерде, соның ішінде дамыған мемлекеттерде де киберқауіпсіздікке қа-

тысты заңнамалық база толық қалыптаспаған. Мысалы, Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген «Киберқауіпсіздік тұжырымдамасы» тек белгілі бір әрекеттерді ғана қамтиды [6], ал киберқылмыстардың кең ауқымын реттейтін қосымша заңнамалар қажет етеді. Бұл мәселені шешу үшін құқықтық жүйелердің кеңеюі мен бейімделуі қажет.

Сонымен қатар, қалалардағы қаржылық ресурстардың шектеулілігі киберқауіпсіздік шараларын жүзеге асыруда үлкен қаржылық шығындарды талап етеді. Қаржылық ресурстардың жетіспеушілігі қалалық киберқауіпсіздікке жеткілікті деңгейде инвестиция салуына кедергі келтіреді. Осы аталған қиындықтарды жеңу үшін кешенді қауіпсіздік негіздерін қалыптастыру қажет.

Біздің зерттеуіміздегі жүргізілген сауалнамamız мемлекеттік басқару, цифрландыру және IT қауіпсіздік саласында жұмыс істейтін мамандардың көзқарасы негізінде талданды. Зерттеу кезеңі 2025 жылдың наурыз-мамыр айлары аралығын қамтиды. Зерттеу мақсаты – Қазақстан қалаларындағы киберқауіпсіздік жүйесін дамытудағы негізгі кедергілерді анықтау. Зерттеуге 813 респондент (Астана қаласы – 196, Алматы қаласы – 184, Шымкент қаласы – 143, Ақтөбе қаласы – 140, Қарағанды қаласы – 150) қатысты. Мақсатты іріктеу (purposeful sampling) әдісі қолданылып, зерттеу нысаны ретінде мемлекеттік цифрландыру және IT саласында жұмыс тәжірибесі бар мамандар таңдалды. Оның ішінде: I) мемлекеттік басқару органдарының өкілдері – 63%, II) ақпараттық технологиялар және ақпараттық қауіпсіздік мамандары – 24%, III) цифрландыру жобаларының сарапшылары мен менеджерлері – 13% болды.

Сауалнама түрі көп жауапты жабық сұрақ (multiple-choice) түрінде респонденттерге бірнеше жауап нұсқасын таңдай алу мүмкіндігі берілді. Бұл әдіс зерттеліп отырған проблеманың практикалық маңыздылығын нақтылауға және мемлекеттік басқару құрылымындағы түйткілді тұстарды анықтауға мүмкіндік берді (1-кесте).

1-кесте. Ақылды қалалардағы киберқауіпсіздік мәселелері мен мемлекеттік басқаруға қатысты сауалнама сұрақтары

№	Санаттары	Сауалнама сұрақтары
1	Ақылды қалалардағы киберқауіпсіздікті жетілдіруде кедергілер	Сіздің ойыңызша, ақылды қалаларда киберқауіпсіздік жүйесін жетілдіруге кедергі келтіріп отырған басты қиындық не?
2	Мемлекеттік секторда киберқауіпсіздікті дамытудағы басым бағыттар	Сіздің ойыңызша, мемлекеттік органдарда киберқауіпсіздікті арттыру үшін қай бағыт ең басым?
3	Қалалық деңгейде киберқауіпсіздікті қамтамасыз ету шаралары	Сіз қалалық қауіпсіздікті қамтамасыз ету үшін қандай шараларды маңызды деп санайсыз?
4	Киберқауіпсіздікте мемлекеттік және жеке сектор арасындағы ақпарат алмасу платформаларының тиімділігі	Сіздің ойыңызша, мемлекеттік органдар мен жеке сектор арасындағы ақпарат алмасу платформалары киберқауіпсіздікті қамтамасыз етуде қаншалықты тиімді?

Ескерту: авторлар құрастырған

Зерттеу нәтижесінде алынған сауалнама деректері негізінде бірқатар маңызды тұжырымдар жасауға болады.

Біріншіден, ақылды қалалардағы киберқауіпсіздікті жетілдіруге кедергі келтіретін негізгі факторлар ретінде респонденттер көбіне нормативтік-құқықтық базаның жетілмегендігін, кадрлық ресурстардың тапшылығын және техникалық инфрақұрылымның жеткіліксіздігін атады. Аталған негізгі факторлар мемлекеттік басқару құрылымдарының киберқауіптерге шұғыл және үйлесімді жауап беруіне кедергі келтіреді.

Екіншіден, мемлекеттік сектордағы киберқауіпсіздікті дамытуда басым бағыттар ретінде сарапшылар деректерді қорғау жүйелерін автоматтандыру, қызметкерлердің кибергиги-

ена бойынша тұрақты даярлығын ұйымдастыру және азаматтардың жеке деректерін қорғау шараларын күшейтуді атады. Яғни, мемлекеттік басқарудың цифрлық трансформациясындағы маңызды қадам ретінде бағаланады.

Үшіншіден, қалалық деңгейде киберқауіпсіздікті қамтамасыз ету шаралары бойынша сарапшылар заманауи технологияларды енгізу (мысалы, көп факторлы аутентификация, адами фактор мен киберқауіпсіздік мәдениетін жетілдіру, жасанды интеллект, жеке оқыту бағдарламаларын енгізу және биометриялық аутентификация) қажеттілігін алға тартты.

Төртіншіден, мемлекеттік және жеке сектор арасындағы ақпарат алмасу платформалары киберқауіпсіздікті қамтамасыз етуде әлеуетті құрал ретінде танылды. Дегенмен, сарапшылар бұл бағытта ақпарат алмасу және мәліметтердің қорғалуына қатысты күмәндердің бар екенін атап өтті.

Жүргізілген сауалнама нәтижелері Қазақстанда ақылды қалалардағы киберқауіпсіздікті қамтамасыз ету үшін кешенді және жүйелі тәсілдің қажет екенін көрсетеді. Мемлекеттік басқару жүйесінде бұл бағытта нормативтік, техникалық және адами факторларды тең дәрежеде ескеру қажет. Сондай-ақ мемлекеттік-жекеменшік әріптестікті нығайту және деректермен қауіпсіз жұмыс істеу мәдениетін қалыптастыру арқылы болашақ қалаларды мемлекеттік басқарудағы табысты трансформацияның кепілі.

Сауалнамаға қатысқан респонденттердің ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті қалыптастырудағы «Сіздің ойыңызша, ақылды қалаларда киберқауіпсіздік жүйесін жетілдіруге кедергі келтіріп отырған басты қиындық не?» деген сауалнама сұрағының нәтижесі 2-кестеде берілген. Респонденттер бірнеше нұсқаны таңдай алды, сондықтан пайыздардың жалпы қосындысы 100%-дан асады. Бұл біздің зерттеуіміздің нақты түсіну қажеттілігін көрсетеді.

2-кесте. Киберқауіпсіздік саласындағы негізгі кедергілер респонденттердің пікірі бойынша %-дық көрсеткішпен

№	Қиындықтар	Нәтижесі	Пайыздық үлесі
1	Қаржы ресурстарының шектеулігі	612	75,3 %
2	Заңнамалық базаның жеткіліксіздігі	481	59,2 %
3	Білікті кадрлардың жетіспеушілігі	426	52,4 %
4	Халықаралық ынтымақтастықтың әлсіздігі	347	42,7 %
5	Цифрлық инфрақұрылымның төмен деңгейі	309	38 %
6	Басқару құрылымдарының үйлеспеушілігі	267	32,8 %
7	Қауіпсіздік мәдениетінің төмендігі	213	26,2 %
8	Стратегиялық жобаларды жүзеге асырудағы кедергілер	179	22 %

Ескерту: сауалнама нәтижесі бойынша авторлар құрастырған

Респонденттердің басым бөлігі ақылды қалалардағы киберқауіпсіздікке жеткілікті қаржы бөлінбейтінін атап өтті. Яғни, техникалық жабдықтар, жаңа платформалар мен жүйелер сатып алуға кедергі келтіреді. Сонымен бірге, респонденттердің пікірінше, «қолданыстағы заңдар мен нормативтік актілер киберқауіпсіздік саласындағы нақты механизмдерді, жауапкершілікті және техникалық талаптарды қамтымайды. «Ақпараттандыру туралы» заңда ақылды қалаларға қатысты тармақтар нақты көрсетілмеген. Мемлекеттік басқару органдарында IT-мамандардың тапшылығы жиі айтылатын мәселелердің бірі. Олардың пікірінше, «әкімдіктер мен басқармаларда цифрлық қауіпсіздікпен айналысатын арнайы бөлім немесе маман жоқ».

3-кестеде көрсетілгендей, «Сіздің ойыңызша, мемлекеттік органдарда киберқауіпсіздікті арттыру үшін қай бағыт ең басым болып табылады?» сұрағының нәтижесі берілген. Бұл нәтиже кибершабуылдарға тек қана техникалық жолмен емес, адами капиталды дамыту арқылы да қарсы тұру қажет екенін көрсетеді.

3-кесте. Мемлекеттік органдардағы киберқауіпсіздік басымдықтары туралы респонденттердің пікірі

%-дық көрсеткішпен

№	Бағыттар	Нәтижесі	Үлесі
1	Көп факторлы аутентификация мен серіктес верификация	176	21,6 %
2	Адами фактор мен киберқауіпсіздік мәдениетін жетілдіру	234	28,8 %
3	Жасанды интеллект арқылы аномалияны анықтау және ескерту	143	17,6 %
4	Жеке оқыту бағдарламаларын енгізу және мінез-құлықты өзгерту	112	13,8 %
5	Биометриялық аутентификация және чат-бот қолдану	148	18,2 %
	Барлығы	813	100 %

Ескерту: сауалнама нәтижесі бойынша авторлар құрастырған

Нәтижесінде респонденттердің ең көп бөлігі (28,8%) қауіпсіздік шараларын күшейту, киберқауіпсіздік мәдениетін арттыру және адами факторды жетілдіруді маңызды деп таныды. Екінші орында, көпфакторлы аутентификация мен серіктес верификация 21,6%-ды құрады. Бұл цифрлық инфрақұрылымды нақты қорғаудың өзектілігін көрсетеді. Ал жасанды интеллект негізіндегі аномалияларды ерте анықтау (17,6%) мен биометриялық жүйелерді қолдану (18,2%) респонденттердің айтарлықтай бөлігін қызықтырған. Жеке оқыту бағдарламаларын енгізу қажеттілігін 13,8% құрады.

Бұл нәтижелер мемлекеттік құрылымдардың техникалық құралдармен қатар адами капиталды дамытуға назар аударуы қажеттігін көрсетеді. Атап айтқанда, киберқауіпсіздік мәдениетін қалыптастыру тек техникалық шешімдер арқылы емес, ұзақ мерзімді білім беру стратегиялары мен мінез-құлықты өзгертетін бағдарламалар арқылы жүзеге асуы тиіс. Бұл адами фактордың рөлін қайта бағалауға және оны қорғаныстың мықты тұсына айналдыруға мүмкіндік береді.

4-кестеде жауаптардың үлестік бөлінісі негізінде респонденттердің киберқауіпсіздікке қатысты негізгі проблемалар туралы пікірін анықтауда «Сіздің ойыңызша, ақылды қалаларда киберқауіпсіздік жүйесін жетілдіруге кедергі келтіріп отырған басты қиындық не?» деген сұрақ қойылды. Респонденттер бірнеше жауап нұсқасын таңдауға мүмкіндік алғандықтан, пайыздық үлестердің жалпы қосындысы 100%-дан артық болуы мүмкін. Нәтижесі киберқауіпсіздік саласындағы күрделі әрі көпқырлы мәселелердің бар екенін және оларды нақты түсіну қажеттігін көрсетеді.

4-кесте. Қалалық қауіпсіздікті қамтамасыз ету үшін маңызды деп саналатын шаралар

%-дық көрсеткішпен

№	Шаралар	Нәтижесі	Үлесі
1	Бейнебақылау жүйелерін көбейту	612	75,3 %
2	Құқық қорғау органдарының жұмысын жақсарту	583	71,7 %
3	Smart-қала технологияларын енгізу (ЖИ талдау, деректермен болжау)	509	62,6 %
4	Көше жарығын жақсарту	462	56,8 %
5	Қоғамдық тәртіпті сақтау бойынша тұрғындармен ынтымақтастық орнату	438	53,9 %

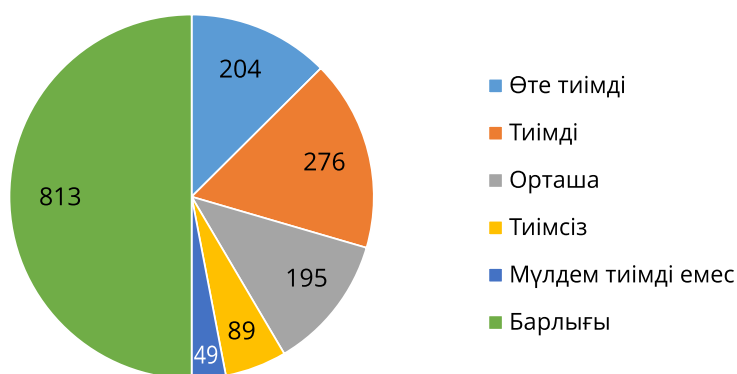
Ескерту: сауалнама нәтижесі бойынша авторлар құрастырған

Респонденттердің жауабы негізінде қалалық қауіпсіздікке қатысты басты шара ретінде бейнебақылау жүйелерін көбейту (75,3%) таңдалғаны анықталды. Бұл тұрғындардың визуалды қадағалауды қауіпсіздік кепілі ретінде қабылдайтынын көрсетеді. Сонымен қатар, құқық қорғау органдарының жұмысын жақсарту (71,7%) және «Ақылды қала» технологияларын енгізу (62,6%) де маңызды бағыт ретінде қарастырылып отыр. Бұл цифрлық құралдар мен адам факторына тең дәрежеде сенім артылатынын білдіреді.

Салыстырмалы түрде көше жарығын жақсарту (56,8%) және қоғаммен ынтымақтастық (53,9%) көрсеткіштері төмен болғанымен, олардың жартысынан астамы тарапынан қолдау тапқаны бұл факторлардың да елеулі екенін көрсетеді. Аталған нәтижелер болашақта ақылды қала жүйелерінде адам мен технология арасындағы тепе-теңдікті сақтау қажеттігін көрсетеді.

1-суретте киберқауіпсіздікті қамтамасыз етуге қатысты, «Сіздің ойыңызша, мемлекеттік органдар мен жеке сектор арасындағы ақпарат алмасу платформалары киберқауіпсіздікті қамтамасыз етуде қаншалықты тиімді?» сауалнама сұрағы мен соған сәйкес талданған нәтижесі ұсынылған. Бұл нәтижелер мемлекеттік құрылымдардың цифрлық қауіпсіздік саласында қабылдап жатқан шаралары қоғам тарапынан оң қабылданатынын көрсетеді.

1-сурет. Мемлекеттік органдар мен жеке сектор арасындағы ақпарат алмасу платформаларының киберқауіпсіздікті қамтамасыз етудегі тиімділігі



Ескерту: сауалнама нәтижесі бойынша авторлармен құрастырылған

Нәтижелер көрсеткендей, респонденттердің басым бөлігі мемлекеттік органдар мен жеке сектор арасындағы ақпарат алмасу платформалары киберқауіпсіздікті қамтамасыз етуде тиімді немесе өте тиімді (59%) деп есептейді. Сонымен қатар, 24%-ы бұл платформалардың тиімділігін «орташа» деп бағаласа, тек 16,9%-ы олардың тиімсіз екенін білдірген. Бұл негізгі көрсеткіштері аталған платформалар бойынша халықтың сенім деңгейін айқындайды және болашақта осы бағыттағы шараларды жетілдіру қажеттігін көздейді.

Бұл нәтиже мемлекеттік және жеке сектор арасындағы өзара әрекеттестіктің әлеуетін көрсететін маңызды индикатор. Ақпарат алмасу механизмдерінің тиімді жұмыс істеуі кибершабуылдарға жедел әрекет ету мен алдын алу жүйесінің негізі болып саналады. Сондықтан да бұл платформаларды дамыту тек техникалық интеграциямен шектелмей, сенімділік пен ашықтық қағидаларына негізделуі тиіс.

Ақылды қалаларды мемлекеттік басқару жүйесіне қойылатын талаптар үнемі дамып отыратын технологиялық және құқықтық ортаға бейімделуді қажет етеді. Сонымен қатар, халықаралық ынтымақтастық, және қаржылық ресурстарды оңтайлы пайдалануда маңызды рөл атқарады.

Жоғарыдағы аталған мәселелерге байланысты ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті қалыптастырудың негізгі қиындықтары мен күрделілігі қалалардағы маңызды инфрақұрылымға әсер ету қабілетімен сипатталады.

Жасанды интеллект қалалық мемлекеттік органдардың киберқауіптерге қарсы тұруын айтарлықтай күшейту үшін әртүрлі қосымшалар мен стратегияларды пайдалана алады [7]. Жасанды интеллект қала дамуын басқарудағы қауіпсіздік қатерлерін анықтау, зерттеу және оларға жауап беру қабілетін арттыру арқылы киберқорғаныста шешуші рөл атқарады. Қалалық мемлекеттік органдар мен тұрғындар арасында өзара әрекеттесе алады, сұрақтарға жауап бере алады. Осылайша киберқауіпсіздікті тергеуде виртуалды көмекші ретінде әрекет етеді. Сонымен қатар киберқауіпсіздік мамандарының қазіргі тапшылығы жағдайында

жасанды интеллекттің күш мультипликаторы ретінде қызмет етеді. Яғни жасанды интеллект бар қызметкерлерге автоматтандыру арқылы тиімдірек және кеңейтілген аналитикалық мүмкіндіктер арқылы ақылды жұмыс істеуге мүмкіндік береді. Бұл ақылды қалаларда өсіп келе жатқан талаптарды қанағаттандыруға көмектеседі.

Жалпы жасанды интеллект қалаларды мемлекеттік басқарудағы қауіптерді анықтау, тергеулерді қолдау және жұмыс күшінің тиімділігін оңтайландыру арқылы киберқорғанысты жақсартады [8]. Бұл оны заманауи киберқауіпсіздік стратегияларында таптырмас құралы. Мемлекеттік органдар өздерінің киберқауіпсіздік шараларын жақсарту үшін аномалиялар мен ықтимал шабуыл сценарийлерін анықтау, тергеуді жеңілдету алу және күш мультипликаторы ретінде қызмет көрсету сияқты жасанды интеллект құралдарын қолдана алады. Бұл құралдар заңдылықтарды талдау және әлеуетті қауіптерді жүзеге аспай тұрып анықтауға көмектеседі.

Жалпы жасанды интеллект шешімдерін енгізу бастапқы инвестицияны қажет етуі мүмкін, бірақ олар киберинциденттердің жиілігі мен әсерін азайту арқылы ұзақ мерзімді перспективада шығындарды үнемдеуге әкеледі [9]. Автоматтандырылған жүйелер деректер мен қауіптерді дәстүрлі әдістерге қарағанда тиімдірек өңдей алады. Мемлекеттік органдардың киберқауіптерге дайындық деңгейін арттыруға және олардың тұрақтылығын қамтамасыз етуге болашақ трендтердің маңызы өте көп.

Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздік шараларын жетілдіру үшін болашақтағы негізгі трендтер қатарына адамдардың біліктілігін арттыруда оқыту мен жалдауға көңіл бөлуді, көп факторлы аутентификацияны енгізуді және заттар интернеті (IoT) мен бұлттық технологияларды қолдануды жатқызуға болады [10].

Осыған орай жасанды интеллекттің қалаларды мемлекеттік басқарудың артықшылықтары мен кемшіліктері және де оларға мысал келтірілді (5-кесте).

5-кесте. Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздік шараларын жетілдірудегі болашақ негізгі трендтерінің сипаттамасы

№	Тренд	Артықшылықтар	Кемшіліктер	Мысалдар
1.	Заттар интернеті (IoT) [11].	- Ақпаратты автоматты түрде жинау. - Қалалық инфрақұрылымды тиімді басқару.	- Көп құрылғыға байланысты қауіптің артуы. - Қауіпсіздік стандарттарының жетіспеуі.	- Күшті шифрлау хаттамаларын және бағдарламалық жасақтаманың тұрақты жаңартуларын енгізу.
2.	Бұлттық технологиялар [12].	- Масштабталу мүмкіндігі. - Деректерді оңай сақтау.	- Бұлттағы деректердің ұрлану қауіпі. - Бұлт қызметтерінің бұзылуы.	- Amazon Web Services. - Google Cloud және Microsoft Azure қызметтері.
3.	Жасанды интеллект (AI) [13].	Киберқауіпсіздікке қатысты мінез-құлықты өзгерту.	- Аномалияларды анықтау және алдын ала ескерту. - Жеке киберқауіпсіздік оқыту бағдарламалары.	- Құрылғыны және деректерді шифрлау құралдары.
4.	Адамдардың біліктілігін арттыру [14].	- Қала тұрғындарының цифрлық сауаттылығын арттыру. - Киберқауіпсіздік мәдениетін қалыптастыру.	- Қаржылық шығындар. - Уақыт шығыны. - Тұрақсыздық.	IT мамандары.
5.	Көп факторлы аутентификация [15].	- Жүйеге кірудің күрделілігі азайту. - Қосымша қауіпсіздік шараларын ұсыну. - Қауіп-қатер моделін құру.	- Ыңғайсыздық. - Құрылғыларға тәуелділік.	Биометрия немесе SMS-код. AI чат-боттарын қолдану.

Ескерту: деректер негізінде авторлар құрастырған

Айтылған трендтер мемлекеттік басқарудың киберқауіпсіздік жүйелерін дамыта отырып, олардың қорғаныс деңгейін арттыруға және кибершабуылдарға қарсы тұрақтылығын нығайтуға мүмкіндік береді.

Бұл трендтердің әрқайсысы жеке бағыт ретінде ғана емес, кешенді түрде өзара байланысқан стратегия ретінде қарастырылуы қажет. Мысалы, жасанды интеллекті қолдану IoT құрылғыларымен біріктіріліп, аномалияны автоматты түрде тануға мүмкіндік береді. Сонымен қатар, адами капитал мен көп факторлы аутентификация бір-бірін толықтырып, техникалық және поведенциялық қауіпсіздікті қатар қамтиды. Сондықтан болашақта трендтерді оқшау емес, интеграцияланған тәсіл арқылы енгізу тиімдірек болады деген қорытынды жасауға болады.

Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті дамытуда кездесетін негізгі шешімдері киберқауіпсіздік саясатын қайта құруда негіз бола алады. Мұнда адами факторды күшейту, институционалдық үйлестіру, технологиялық интеграция және құқықтық қамтамасыз ету арқылы бір-бірін толықтыратын элементтер ретінде қарастырылады. 2-суретте жиі кездесетін жауаптардың бірізділігі мен қайталануы аталған проблемалардың шын мәнінде жүйелік сипат алатынын дәлелдейді. Осыған байланысты, бұл қиындықтарды шешу үшін формалды тәсілдерден тыс, стратегияны кешенді түрде бейімдеу қажет.

2-сурет. Ақылды қалаларды мемлекеттік басқарудағы киберқауіпсіздікті дамытуда ең жиі және бірегей кездесетін жауаптар



Ескерту: авторлар дереккөз негізінде құрастырған

Көрсетілген шаралар мемлекеттік органдардың киберқауіптерге қарсы тұру қабілетін едәуір арттырады және маңызды инфрақұрылымды тиімді қорғауға көмектеседі. Киберқауіпсіздікке арналған кешенді стратегиялардың арқасында қалалық инфрақұрылымдардың қауіпсіздігі нығайып, кибершабуылдарға төзімділік артады.

Мемлекеттік органдар киберқауіпсіздікті қамтамасыз етуде цифрлық технологияларды кеңінен қолданады. Бұл қалалық инфрақұрылымдарды қорғауға және кибершабуылдардың алдын алуға бағытталған ақпарат алмасу платформалары киберқауіптер туралы ақпаратты

мемлекеттік және жеке сектор арасында жедел бөлісуге мүмкіндік береді [16]. Мұндай платформалар кибершабуылдарды ерте анықтап, оларға қарсы бірлескен шаралар қабылдауға мүмкіндік береді. Сондай-ақ, мемлекеттік органдардың киберқауіпсіздігін нығайтып, кибершабуылдарға қарсы тұрақтылықты қамтамасыз етеді. Жалпы цифрлық технологиялар қалалық инфрақұрылымдарды қорғауда маңызды рөл атқарады және қауіпсіздікті қамтамасыз етудің сенімді негізін құрайды.

Киберқауіпсіздікті қамтамасыз етуде адам факторы шешуші рөл атқарады. Себебі адамдар киберқауіпсіздіктің бірінші желісі. Олар көбінесе киберқауіпсіздіктің ең әлсіз буыны ретінде қарастырылады, алайда олар киберқауіптерден қорғаныстың алғашқы деңгейіне жатады.

Сәтті киберқауіпсіздік стратегиясы технологияларды, ұйымдық саясаттарды және адам факторларын интеграциялауды талап етеді. Бұл кешенді тәсіл барлық компоненттердің киберқауіптермен тиімді күресуіне мүмкіндік береді.

ҚОРЫТЫНДЫ

Қорытындылай келе, мемлекеттік органдар мен жеке сектор арасындағы ақпарат алмасу процесі киберқауіптер туралы хабардарлықты арттырудың негізгі құралдарының бірі. Кибершабуылдарды болдырмау және олардан қорғау үшін мемлекеттік және жеке сектор өкілдері өзара ынтымақтастық орнатып, қауіпсіздік шараларын нығайтады. Киберқауіпсіздік саласында білікті мамандарды даярлау – киберқауіптерге қарсы тұрудың маңызды аспектілерінің бірі. Мемлекеттік органдар қала тұрғындарының білімін арттыру үшін тұрақты оқыту бағдарламаларын ұйымдастырады. Бұл шара киберқауіптерге дайындықты жақсартып, ақпараттық жүйелердің қауіпсіздігін нығайтады.

Зерттеу нәтижелері көрсеткендей, ақылды қалаларды басқарудағы киберқауіпсіздік мәселелері Қазақстанда өзекті болып қала береді. Сауалнамаға қатысқан 813 респонденттің көпшілігі киберқауіпсіздікті қамтамасыз етудегі негізгі кедергілер ретінде тиісті қаржы ресурстарының шектеулілігі (75,3%), заңнамалық базаның жеткіліксіздігі (59,2%), сонымен бірге кадрлық ресурстардың жетіспеушілігін (52,4%) атап өтті.

Бұл көрсеткіштер қазіргі таңда мемлекеттік басқару жүйесінде киберқауіпсіздікті жүйелі басқару және цифрлық платформалармен ықпалдастыру саласында институционалдық және ұйымдастырушылық проблемалар бар екенін дәлелдейді. Сонымен қатар, респонденттердің 38%-ы дербес мәліметтердің қорғалмауы тұрғындардың сенімін төмендететінін алға тартты. Бұл қала дамуын мемлекеттік басқарудағы сервистік және адамға бағытталған мемлекеттік басқару моделін дамытуда аса маңызды фактор.

Нәтижелер мен талдауларға сүйене отырып, біз ақылды қалаларды мемлекеттік басқаруыда киберқауіпсіздікті дамыту бойынша ең тиімді шешімдерді ұсынамыз:

1. Киберқауіпсіздік саласына арналған кадрлық әлеуетті арттыру арқылы ақылды қалаларды басқарумен айналысатын мемлекеттік құрылымдар мен жергілікті атқарушы органдар үшін ақпараттық қауіпсіздік саласында арнайы мамандандырылған оқу бағдарламаларын енгізу қажет.

2. Қаржыландыру тетіктерін жетілдіру негізінде қалалық цифрлық инфрақұрылым мен киберқауіпсіздікті қорғауға бағытталған бюджеттік бағдарламалар аясында тұрақты әрі мақсатты қаржыландыру көздерін қарастыру керек.

3. Қалалық ведомствоаралық үйлестіруді күшейту арқылы киберқауіпсіздік мәселелерімен айналысатын мемлекеттік және жергілікті құрылымдар арасында өзара әрекеттестікті күшейту үшін бірыңғай цифрлық қауіпсіздік стратегиясын қабылдау қажет.

4. Қоғамдық сенімді арттыру үшін ақылды қалаларда пайдаланылатын жүйелердің ашықтығы мен тұрғындардың жеке деректерінің қауіпсіздігін қамтамасыз ету арқылы азаматтардың цифрлық қызметтерге деген сенімін нығайту.

Жалпы алғанда, адами фактор киберқауіпсіздіктің маңызды аспектісі болып табылады, және оны жетілдіру оқыту, психологиялық әсерлерді түсіну, ыңғайлы жүйелерді жоба-

лау және киберқауіпсіздікті басқарудың әртүрлі элементтерін біріктіруді қамтиды. Осы салаларға назар аудара отырып, мемлекеттік органдар киберқауіптерге қорғанысын күшейте алады.

Стратегиялық басқарушылық көзқарас тұрғысынан алғанда, бұл зерттеу мемлекеттік басқару жүйесіне келесі нақты бағыттар бойынша практикалық бейімделуді ұсынады:

Біріншіден, киберқауіпсіздікті тек IT саласына қатысты мәселе ретінде емес, ұлттық стратегиялық актив ретінде қабылдайтын басқарушылық парадигма қажет. Мемлекеттік органдардың стратегиялық жоспарлау құжаттарында (мысалы, өңірлік даму жоспарлары немесе цифрлық трансформация стратегиялары) киберқауіпсіздік жеке тармақ ретінде енуі тиіс.

Екіншіден, стратегиялық бақылау мен мониторинг құралдары (KPI, risk management framework, scenario-based planning) кибершабуылдарға дайындық деңгейін өлшейтін индикаторлармен толықтырылуы керек.

Үшіншіден, бұл зерттеуде ұсынылған шаралар (мәселен, адами капиталды дамыту, ақпарат алмасу платформаларын жетілдіру, ЖИ технологияларын қолдану) Smart Governance қағидаттарына сәйкес келеді. Демек, олар Data-driven decision making, Citizen-centric services және Resilience planning сияқты қазіргі мемлекеттік басқару трендтерімен интеграциялануы қажет.

Төртіншіден, ұсынылып отырған шешімдер Қазақстанның «Цифрлық Қазақстан» бағдарламасы мен «Киберқауіпсіздік тұжырымдамасына» сәйкестендіріліп, ведомствоаралық стратегия деңгейінде жүйеленуі тиіс. Бұл нақты құзырет пен ресурстар бөлінісін қамтамасыз етеді.

Осылайша, зерттеу нәтижелері стратегиялық басқарушылық модельдерді цифрлық қауіпсіздік талаптарымен бейімдеу үшін практикалық негіз қалайды.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Asllani, A., White, C. S., Ettkin, L. Viewing cybersecurity as a public good: The role of governments, businesses, and individuals // J. Legal Ethical&Regul. Isses. – 2013. – V. 16. – p. 7.
2. Kaijankoski, E. A. Cybersecurity information sharing between public-private sector agencies: dis. – Monterey, California: Naval Postgraduate School, 2015.
3. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. Leveraging human factors in cybersecurity: an integrated methodological approach // Cognition, Technology&Work. – 2022. – V. 24. – №. 2. – p. 371-390.
4. Sadiku, M. N. O., Fagbohunbe, O. I., Musa, S. M. Artificial intelligence in cyber security // International Journal of Engineering Research and Advanced Technology. – 2020. – V. 6. – №. 05. – p. 01-07.
5. Ramakrishnan, R., Leethial, M., Monisha, S. The future of cybersecurity and its potential threats // International Journal for Research in Applied Science&Engineering Technology. – 2023. – V. 11. – №. 7.
6. Киберқауіпсіздік тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы [Электрондық ресурс]. – URL: <https://adilet.zan.kz/kaz/docs/P1700000407> (қол жеткізу күні: 08.06.2025).
7. Carroll, J. The US National Cybersecurity Strategy: A Vehicle with an International Journey // European Conference on Cyber Warfare and Security. – 2024. – V. 23. – №. 1. – p. 107-115.
8. Srebalová, M., Peráček, T. Effective public administration as a tool for building smart cities: The experience of the Slovak Republic // Laws. – 2022. – V. 11. – №. 5. – p. 67.
9. Kaiser, Z. R. M. A. Smart governance for smart cities and nations // Journal of Economy and Technology. – 2024. – V. 2. – p. 216-234.
10. Vitunskaitė, M., He, Y., Brandstetter, T., Janicke, H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership // Computers&Security. – 2019. – V. 83. – p. 313-331.
11. Bokhari, S. A. A., Myeong S. The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective // IEEE Access. – 2023.
12. Kalinin, M., Krundyshev, V., Zegzhda, P. Cybersecurity risk assessment in smart city infrastructures // Machines. – 2021. – V. 9. – №. 4. – p. 78.

13. Florido-Benítez, L. The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities // *Smart Cities*. – 2024. – V. 7. – №. 1. – p. 475-495.
14. Sengan, S., Subramaniaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., Ravi, L. Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network // *Future generation computer systems*. – 2020. – V. 112. – p. 724-737.
15. Hossain, S. T., Yigitcanlar, T., Nguyen, K., Xu, Y. Local government cybersecurity landscape: A systematic review and conceptual framework // *Applied Sciences*. – 2024. – V. 14. – №. 13. – p. 5501.
16. Oliha, J. S., Biu, P.W., Obi, O. C. Securing the smart city: a review of cybersecurity challenges and strategies // *Engineering Science&Technology Journal*. – 2024. – V. 5. – №. 2. – p. 496-506.

REFERENCES

1. Asllani, A., White, C. S., Ettkin, L. Viewing cybersecurity as a public good: The role of governments, businesses, and individuals // *J. Legal Ethical&Regul. Isses*. – 2013. – V. 16. – p. 7.
2. Kaijankoski, E. A. Cybersecurity information sharing between public-private sector agencies: dis. – Monterey, California: Naval Postgraduate School, 2015.
3. Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D. Leveraging human factors in cybersecurity: an integrated methodological approach // *Cognition, Technology&Work*. – 2022. – V. 24. – №. 2. – p. 371-390.
4. Sadiku, M. N. O., Fagbohunbe, O. I., Musa, S. M. Artificial intelligence in cyber security // *International Journal of Engineering Research and Advanced Technology*. – 2020. – V. 6. – №. 05. – p. 01-07.
5. Ramakrishnan, R., Leethial, M., Monisha, S. The future of cybersecurity and its potential threats // *International Journal for Research in Applied Science&Engineering Technology*. – 2023. – V. 11. – №. 7.
6. Kiberqayıpsızdik tujyrymdamasyn bekity týraly Qazaqstan Respýblıkasy Úkimetiniń 2017 jylǵy 30 maýsymbaǵy № 407 qaýlysy [Resolution of the Government of the Republic of Kazakhstan No. 407 dated June 30, 2017, on approval of the Concept of Cybersecurity] [Electronic resource]. – URL: <https://adilet.zan.kz/kaz/docs/P1700000407> (accessed: 08.06.2025).
7. Carroll, J. The US National Cybersecurity Strategy: A Vehicle with an International Journey // *European Conference on Cyber Warfare and Security*. – 2024. – V. 23. – №. 1. – p. 107-115.
8. Srebalová, M., Peráček, T. Effective public administration as a tool for building smart cities: The experience of the Slovak Republic // *Laws*. – 2022. – V. 11. – №. 5. – p. 67.
9. Kaiser, Z. R. M. A. Smart governance for smart cities and nations // *Journal of Economy and Technology*. – 2024. – V. 2. – p. 216-234.
10. Vitunskaitė, M., He, Y., Brandstetter, T., Janicke, H. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership // *Computers&Security*. – 2019. – V. 83. – p. 313-331.
11. Bokhari, S. A. A., Myeong S. The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective // *IEEE Access*. – 2023.
12. Kalinin, M., Krundyshev, V., Zegzhda, P. Cybersecurity risk assessment in smart city infrastructures // *Machines*. – 2021. – V. 9. – №. 4. – p. 78.
13. Florido-Benítez, L. The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities // *Smart Cities*. – 2024. – V. 7. – №. 1. – p. 475-495.
14. Sengan, S., Subramaniaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., Ravi, L. Enhancing cyber-physical systems with hybrid smart city cyber security architecture for secure public data-smart network // *Future generation computer systems*. – 2020. – V. 112. – p. 724-737.
15. Hossain, S. T., Yigitcanlar, T., Nguyen, K., Xu, Y. Local government cybersecurity landscape: A systematic review and conceptual framework // *Applied Sciences*. – 2024. – V. 14. – №. 13. – p. 5501.
16. Oliha, J. S., Biu, P. W., Obi, O. C. Securing the smart city: a review of cybersecurity challenges and strategies // *Engineering Science&Technology Journal*. – 2024. – V. 5. – №. 2. – p. 496-506.

АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ, ПРИСУЩЕЙ УМНЫМ ГОРОДАМ В СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Жубаназаров С.А.*

PhD докторант
Карагандинский университет Казпотребсоюза
г.Караганда, Казахстан
e-mail: szhubanazar@gmail.com
ORCID: 0000-0002-0782-7719

Жаров Е.К.

К.Э.Н
директор филиала Академии государственного
управления при
Президенте РК по Акмолинской области
г.Кокшетау, Казахстан
e-mail: yerzhan.zharov@apa.kz
ORCID: 0000-0003-3567-4673

Кемелбек Р.Қ.

эксперт
Научно-исследовательский центр
«Молодежь»
г.Астана, Казахстан
e-mail: kemelbek_rk@mail.ru
ORCID: 0009-0009-5485-5542

Турдиева З.М.

PhD
Alikhan Bokeikhan University
г.Семей, Казахстан
e-mail: kalibaeva.z@mail.ru
ORCID: 0000-0002-6255-0599

Аннотация. В данной статье рассматриваются вопросы кибербезопасности в государственном управлении умными городами. Цель исследования – изучить и проанализировать решения по развитию кибербезопасности в контексте государственного управления умными городами, а также определить наиболее эффективные пути противодействия современным киберугрозам. В рамках исследования подробно рассмотрены современные подходы к обеспечению кибербезопасности, включая стратегии информационной безопасности, платформы обмена информацией между государственным и частным секторами, использование технологий искусственного интеллекта и важность подготовки квалифицированных кадров. Методология исследования включает анализ и синтез научных данных, сравнительный анализ, а также проведение экспертного и эмпирического опроса в сфере кибербезопасности и государственного управления. Результаты опроса показали, что большинство респондентов считают эффективный обмен информацией между государственными органами и частным сектором ключевым фактором устойчивости к киберугрозам. Раннее выявление кибератак, информирование населения и непрерывный мониторинг определены как основные элементы обеспечения безопасности. Также с использованием вторичных данных рассмотрены ключевые вызовы формирования кибербезопасности в государственном управлении умными городами, включая роль человеческого фактора. Результаты исследования могут способствовать совершенствованию политики в сфере кибербезопасности, принятию эффективных управленческих решений и формированию безопасной и надежной экосистемы «умного города». Кроме того, особое внимание уделяется будущим трендам, способным повысить устойчивость государственных систем к кибератакам с точки зрения экономической эффективности. В заключение представлены наиболее эффективные решения по развитию кибербезопасности в государственном управлении Республики Казахстан, основанные на результатах и анализе исследования.

Ключевые слова: умный город, кибербезопасность, государственное управление, искусственный интеллект, цифровые технологии.

CURRENT ISSUES OF CYBERSECURITY INHERENT IN SMART CITIES WITHIN THE SYSTEM OF PUBLIC ADMINISTRATION

Zhubanazarov S.*

PhD student
Karaganda University of Kazpotrebsoyuz
Karaganda, Kazakhstan
e-mail: szhubanazar@gmail.com
ORCID: 0000-0002-0782-7719

Zharov Ye.

PhD
Director of the branch of the Academy of Public
Administration
under the President of the Republic of Kazakhstan
in Akmola region
Kokshetau, Kazakhstan
e-mail: yerzhan.zharov@apa.kz
ORCID: 0000-0003-3567-4673

Kemelbek R.

expert
Research Center «Youth»
e-mail: kemelbek_rk@mail.ru
ORCID: 0009-0009-5485-5542

Turdieva Z.

PhD
Alikhan Bokeikhan University
Semey, Kazakhstan
e-mail: kalibaeva.z@mail.ru
ORCID: 0000-0002-6255-0599

Annotation. This article explores the challenges of cybersecurity in the public administration of smart cities. The aim of the study is to investigate and analyze solutions for developing cybersecurity in the governance of smart cities and to identify the most effective approaches to countering modern cyber threats. The research examines current approaches to ensuring cybersecurity, including information security strategies, platforms for information exchange between public and private sectors, the use of artificial intelligence technologies, and the importance of training qualified personnel. The methodology includes analysis and synthesis of scientific data, comparative analysis, as well as expert and empirical surveys in the field of cybersecurity and public administration. Survey results indicate that the majority of respondents consider effective information exchange between government agencies and the private sector as a key factor in resilience to cyber threats. Early detection of cyberattacks, public awareness, and continuous monitoring are seen as essential elements of ensuring security. Using secondary data, the study also explores the main challenges of forming cybersecurity in the public governance of smart cities, including the role of the human factor. The results contribute to improving cybersecurity policy, supporting effective decision-making, and fostering a safe and reliable “smart city” ecosystem. Furthermore, special attention is given to future trends that can enhance the resilience of public systems to cyberattacks from an economic efficiency perspective. Finally, based on the findings and analysis, the most effective cybersecurity development solutions for Kazakhstan's public administration are proposed.

Keywords: smart city, cybersecurity, public administration, artificial intelligence, digital technology.