УДК: —
МРНТИ: —

[1] Толетаев Бауыржан Толетаевич*

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті

**dimash_tulkibai@mail.ru*

ҚАЗІРГІ ЗАМАНҒЫ ЦИФРЛЫҚ ЭКОЖҮЙЕДЕГІ КИБЕРҚАУІПСІЗДІК: ҚАТЕРЛЕРДІ ТАЛДАУ ЖӘНЕ ҚОРҒАНЫС ТЕТІКТЕРІН ЖЕТІЛДІРУ

Аннотация. В статье комплексно рассматриваются вопросы кибербезопасности в современной цифровой инфраструктуре Казахстана. Актуальность исследования обоснована трансграничным характером киберпреступлений и усложнением их методов в условиях массовой цифровизации общества. В ходе работы проведен анализ эффективности концепции «Киберщит Казахстана» и сравнительный анализ с опытом ведущих стран, таких как Эстония и Южная Корея. Подробно описаны экономические и социальные аспекты киберпреступности, включая технические алгоритмы интернет-мошенничества, SQL-инъекций и DDoS-атак. Автор, изучая международные стандарты и отечественную законодательную базу, предлагает новую модель укрепления информационной безопасности. Результаты исследования направлены на повышение устойчивости государственных информационных систем и стратегическое развитие цифровой грамотности населения

Ключевые слова: кибербезопасность, цифровая экосистема, киберпреступность, информационные технологии, Киберщит Казахстана, интернет-мошенничество, информационная безопасность.

[1] Толетаев Бауыржан Толетаевич

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті

ҚАЗІРГІ ЗАМАНҒЫ ЦИФРЛЫҚ ЭКОЖҮЙЕДЕГІ КИБЕРҚАУІПСІЗДІК: ҚАТЕРЛЕРДІ ТАЛДАУ ЖӘНЕ ҚОРҒАНЫС ТЕТІКТЕРІН ЖЕТІЛДІРУ

Аңдатпа. Мақалада Қазақстанның қазіргі заманғы цифрлық инфрақұрылымындағы киберқауіпсіздік мәселелері кешенді түрде қарастырылады. Зерттеудің өзектілігі қоғамның жаппай цифрландырылуы жағдайында киберқылмыстардың трансшекаралық сипат алуымен және олардың әдіс-тәсілдерінің күрделенуімен негізделеді. Жұмыс барысында «Қазақстанның киберқалқаны» тұжырымдамасының тиімділігіне талдау жасалып, Эстония мен Оңтүстік Корея сияқты жетекші елдердің тәжірибесімен салыстыру жүргізілді. Мақалада киберқылмыстың экономикалық және әлеуметтік аспектілері, соның ішінде интернет-алаяқтық, SQL-инъекциялар және DDoS-шабуылдардың техникалық алгоритмдері егжей-тегжейлі сипатталған. Автор халықаралық стандарттар мен отандық заңнамалық базаны зерделей отырып, ақпараттық қауіпсіздікті нығайтудың жаңа моделін ұсынады. Зерттеу нәтижелері мемлекеттік ақпараттық жүйелердің төзімділігін арттыруға және халықтың цифрлық сауаттылығын стратегиялық дамытуға бағытталған.

Түйінді сөздер: киберқауіпсіздік, цифрлық экожүйе, киберқылмыс, Қазақстанның киберқалқаны, интернет-алаяқтық, ақпараттық қауіпсіздік.

[1] Толетаев Бауыржан Толетаевич

[1]Қазақстан Республикасының Ұлттық қорғаныс университеті

CYBERSECURITY IN THE MODERN DIGITAL ECOSYSTEM: THREAT ANALYSIS AND ENHANCEMENT OF PROTECTION MECHANISMS

Abstract. The article provides a comprehensive examination of cybersecurity issues in Kazakhstan's modern digital infrastructure. The relevance of the study is grounded in the cross-border nature of cybercrimes and the increasing complexity of their methods amidst the massive digitalization of society. The paper analyzes the effectiveness of the "Cyber Shield of Kazakhstan" concept and provides a comparative study with the experiences of leading countries such as Estonia and South Korea. The economic and social aspects of cybercrime are described in detail, including the technical algorithms of Internet fraud, SQL injections, and DDoS attacks. By examining international standards and the domestic legal framework, the author proposes a new model for strengthening information security. The findings of the research are aimed at improving the resilience of state information systems and the strategic development of digital literacy among the population.

Keywords: cybersecurity, digital ecosystem, cybercrime, information technologies, Cyber Shield of Kazakhstan, Internet fraud, information security.

УДК 623:004
МРНТИ 78.25.37

Б.Т. ТОЛЕТАЕВ

Қазақстан Республикасының Ұлттық қорғаныс университеті, Астана қ.

ҚАЗІРГІ ЗАМАНҒЫ ЦИФРЛЫҚ ЭКОЖҮЙЕДЕГІ КИБЕРҚАУІПСІЗДІК: ҚАТЕРЛЕРДІ ТАЛДАУ ЖӘНЕ ҚОРҒАНЫС ТЕТІКТЕРІН ЖЕТІЛДІРУ

Толетаев Бауыржан Толетаевич

Қазіргі заманғы ақпараттық технологиялар, киберқылмыстар және олармен күрес

Түйіндеме. Мақалада Қазақстанның қазіргі заманғы цифрлық инфрақұрылымындағы киберқауіпсіздік мәселелері кешенді түрде қарастырылады. Зерттеудің өзектілігі қоғамның жаппай цифрландырылуы жағдайында киберқылмыстардың трансшекаралық сипат алуымен және олардың әдіс-тәсілдерінің күрделенуімен негізделеді. Жұмыс барысында «Қазақстанның киберқалқаны» тұжырымдамасының тиімділігіне талдау жасалып, Эстония мен Оңтүстік Корея сияқты жетекші елдердің тәжірибесімен салыстыру жүргізілді. Мақалада киберқылмыстың экономикалық және әлеуметтік аспектілері, соның ішінде интернет-алаяқтық, SQL-инъекциялар және DDoS-шабуылдардың техникалық алгоритмдері егжей-тегжейлі сипатталған. Автор халықаралық стандарттар мен отандық заңнамалық базаны зерделей отырып, ақпараттық қауіпсіздікті нығайтудың жаңа моделін ұсынады. Зерттеу нәтижелері мемлекеттік ақпараттық жүйелердің төзімділігін арттыруға және халықтың цифрлық сауаттылығын стратегиялық дамытуға бағытталған.

Түйінді сөздер: киберқауіпсіздік, цифрлық экожүйе, киберқылмыс, Қазақстанның киберқалқаны, интернет-алаяқтық, ақпараттық қауіпсіздік.

Толетаев Бауыржан Толетаевич

Современные информационные технологии, киберпреступления и борьба с ними

Аннотация. В статье комплексно рассматриваются вопросы кибербезопасности в современной цифровой инфраструктуре Казахстана. Актуальность исследования обоснована трансграничным характером киберпреступлений и усложнением их методов в условиях массовой цифровизации общества. В ходе работы проведен анализ эффективности концепции «Киберщит Казахстана» и сравнительный анализ с опытом ведущих стран, таких как Эстония и Южная Корея. Подробно описаны экономические и социальные аспекты киберпреступности, включая технические алгоритмы интернет-мошенничества, SQL-инъекций и DDoS-атак. Автор, изучая международные стандарты и отечественную законодательную базу, предлагает новую модель укрепления информационной безопасности. Результаты исследования направлены на повышение устойчивости государственных информационных систем и стратегическое развитие цифровой грамотности населения

Ключевые слова: кибербезопасность, цифровая экосистема, киберпреступность, информационные технологии, Киберщит Казахстана, интернет-мошенничество, информационная безопасность.

Toletaev Bauyrzhan Toletaevich

Modern information technologies, cybercrime and the fight against them

Abstract. The article provides a comprehensive examination of cybersecurity issues in Kazakhstan's modern digital infrastructure. The relevance of the study is grounded in the cross-border nature of cybercrimes and the increasing complexity of their methods amidst the massive digitalization of society. The paper analyzes the effectiveness of the "Cyber Shield of Kazakhstan" concept and provides a comparative study with the experiences of leading countries such as Estonia and South Korea. The economic and social aspects of cybercrime are described in detail, including the technical algorithms of Internet fraud, SQL injections, and DDoS attacks. By examining international standards and the domestic legal framework, the author proposes a new model for strengthening information security. The findings of the research are aimed at improving the resilience of state information systems and the strategic development of digital literacy among the population.

Key words: cybersecurity, digital ecosystem, cybercrime, information technologies, Cyber Shield of Kazakhstan, Internet fraud, information security.

Кіріспе. Жаһандық цифрландыру үрдісі адамзат қоғамының өмір сүру парадигмасын түбегейлі өзгертті. Қазіргі таңда ақпараттық технологиялар тек өндіріс құралы емес, мемлекеттік басқарудың, қаржы жүйесінің және әлеуметтік қатынастардың іргетасына айналды. Қазақстан Республикасы «Цифрлық Қазақстан» мемлекеттік бағдарламасын іске асыру арқылы жаһандық технологиялық бәсекеге қабілеттілігін арттыруды көздейді. Алайда, цифрлық экожүйенің кеңеюі оның осал тұстарының көбеюіне және киберқылмыстың жаңа түрлерінің пайда болуына алып келді.

Киберқылмыс бүгінгі таңда трансшекаралық сипатқа ие болып, ұлттық қауіпсіздікке тікелей қатер төндіруде. Дүниежүзілік экономикалық форумның (World Economic Forum) «Global Risks Report 2024» есебінде кибершабуылдар мен дезинформация жақын арадағы ең қауіпті тәуекелдердің бірі ретінде көрсетілген. Қазақстанда соңғы жылдары интернет-алаяқтықтың, фишингтік шабуылдардың және мемлекеттік ақпараттық жүйелерге жасалған қатерлердің саны еселеп артты. Бұл жағдай қолданыстағы киберқауіпсіздік стратегияларын қайта қарауды және оларды заманауи технологиялық трендтерге (жасанды интеллект, блокчейн, бұлттық есептеулер) бейімдеуді талап етеді.

Зерттеу әдістері. Мақаланың ғылыми негізділігін қамтамасыз ету үшін кешенді зерттеу әдістері қолданылды. Зерттеудің методологиялық негізін диалектикалық таным әдісі, жүйелілік және функционалдық талдау құрайды.

Компаративті (салыстырмалы) талдау: Қазақстанның киберқауіпсіздік саласындағы заңнамалық базасы мен халықаралық стандарттар (мысалы, ISO/IEC 27001, NIST Cybersecurity Framework) салыстырылды. Бұл әдіс отандық жүйенің артықшылықтары мен кемшіліктерін анықтауға мүмкіндік берді.

Статистикалық және деректерді өңдеу әдістері: ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің 2018-2024 жылдар аралығындағы ресми деректеріне ретроспективті талдау жүргізілді. Киберқылмыстардың өсу динамикасы мен құрылымына сандық баға берілді.

Кейс-стади (Case Study): Қазақстандық банк және мемлекеттік секторда орын алған нақты кибершабуылдар мен оларға берілген жауаптар талданды. Бұл тәжірибелік мәселелерді тереңірек түсінуге көмектесті.

Сараптамалық бағалау: Ақпараттық қауіпсіздік саласындағы мамандардың пікірлері мен BugBounty платформасының есептері зерделенді.

Зерттеудің теориялық негізін отандық және шетелдік ғалымдардың киберқылмыс, ақпараттық құқық және компьютерлік қауіпсіздік саласындағы еңбектері құрады.

Нәтижелер. Зерттеу барысында Қазақстан Республикасындағы

киберқылмыстың соңғы 5 жылдағы динамикасы мен «Қазақстанның киберқалқаны» тұжырымдамасының тиімділігіне сандық және сапалық талдау жүргізілді. Алынған деректер келесі негізгі нәтижелерді көрсетті:

1. Киберқылмыстың статистикалық көрсеткіштері

ҚР Бас прокуратурасының Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің мәліметтеріне сәйкес, интернет-алаяқтық пен киберқылмыстардың саны 2018 жылмен салыстырғанда 2024 жылға қарай 3,5 есеге өскен. Егер 2018 жылы тіркелген құқық бұзушылықтар саны 4 мыңнан аспаса, 2023 жылдың қорытындысы бойынша бұл көрсеткіш 20 мыңнан астам оқиғаны құрады.

Интернет-алаяқтық үлесі: Барлық киберқылмыстардың 75%-дан астамы әлеуметтік инженерия әдістерімен (фишинг, вишинг) жасалған алаяқтықтарға тиесілі.

Төлем жүйелері: Қылмыстардың 60%-ы банк карталары мен онлайн-төлемдерді пайдалану кезінде орын алады.

2. «Қазақстанның киберқалқаны» және BugBounty платформасы

Тұжырымдаманы іске асырудың екінші кезеңінде ұлттық ақпараттық қауіпсіздіктің инфрақұрылымы айтарлықтай нығайды. Зерттеу нәтижесінде анықталған негізгі жетістіктер:

BugBounty платформасы: Бүгінгі таңда платформада 700-ден астам тәуелсіз сарапшы тіркелген. Олардың көмегімен мемлекеттік ақпараттық жүйелердегі 1200-ден астам маңызды осалдықтар жойылды. Бұл мемлекеттік бюджеттің шамамен 2 млрд теңгесін үнемдеуге (ықтимал кибершабуылдардың зиянын есептегенде) мүмкіндік берді.

Жергілікті қамту: IT-қызметтер нарығындағы отандық бағдарламалық өнімдердің үлесі 67,7%-ға жетті, бұл сыртқы технологиялық тәуелділікті төмендетудің маңызды индикаторы болып табылады.

3. Кадрлық әлеуетті дамыту

2021-2024 жылдар аралығында «Ақпараттық қауіпсіздік» мамандығы бойынша мемлекеттік білім беру гранттарының саны 2 600-ден асты. Алайда, талдау көрсеткендей, нарықтағы тәжірибелі мамандардың тапшылығы әлі де 15-20% деңгейінде қалып отыр.

4. Киберқылмыстың динамикалық өсуі

ҚР Бас прокуратурасының деректерін өңдеу нәтижесінде соңғы жылдары қылмыстың сандық көрсеткіші ғана емес, оның сапалық сипаты да өзгергені белгілі болды.

Индикатор атауы	2019 жыл	2021 жыл	2024 жыл	Талдау (сөзбен)
Интернет-алаяқтық (тіркелген)	7,732	21,400	25,000	5 жылдағы өсім 320%-дан асты. Бұл халықтың қаржылық қызметтерді жаппай онлайн форматта пайдалануымен және қылмыскерлердің шетелдік IP-адрестерді қолдануымен байланысты.
САИ-ға жасалған шабуылдар	114	289	450	Мемлекеттік органдардың серверлеріне жасалатын DDoS және APT шабуылдарының жиілеуі геосаяси тұрақсыздық пен цифрлық соғыстардың элементін көрсетеді.

BugBounty арқылы жойылған осалдықтар	0	450	1200	2020 жылы іске қосылған ұлттық платформа мемлекеттік жүйелердің қауіпсіздігін 40%-ға арттыруға мүмкіндік берді.

5. «Қазақстанның киберқалқаны» нәтижелері

Тұжырымдаманың екінші кезеңі аясында келесі нәтижелерге қол жеткізілді:

- Ұлттық үйлестіру орталығы (ҰБХО): 2023 жылдың өзінде 500 миллионнан астам кибер-оқиғаларға тосқауыл қойылды.
- Локализация: Мемлекеттік сектордағы отандық ақпараттық қауіпсіздік өнімдерінің үлесі 67,5%-ға жетті. Бұл шетелдік «технологиялық тыңшылық» қатерін азайтады.
- Кадрлық резерв: «Болашақ» бағдарламасы мен жергілікті гранттар есебінен киберқауіпсіздік мамандарының саны жыл сайын 15%-ға артып келеді.

Талқылау. Зерттеу барысында алынған нәтижелер Қазақстанның киберқауіпсіздік жүйесіндегі бірқатар қайшылықтар мен терең мәселелерді ашып көрсетті.

1. Әлеуметтік инженерия және «Адам факторы» парадигмасы

Зерттеу барысында анықталғандай, техникалық қорғаныс құралдарының кемелдігіне қарамастан, киберқылмыскерлердің ең тиімді құралы — адам психологиясы болып қала бермек. Kevin Mitnick өзінің классикалық еңбектерінде атап өткендей, «адам — қауіпсіздік тізбегіндегі ең әлсіз буын». Қазақстандық контексте бұл фишингтік шабуылдардың (SMS-фишинг немесе вишинг) жаппай сипат алуынан көрінеді.

Бұл мәселені талқылау кезінде Bruce Schneier ұсынған «психологиялық төзімділік» тұжырымдамасына тоқталу қажет. Оның пікірінше, киберқауіпсіздік тек математикалық алгоритмдер емес, ол адамдардың сенімімен манипуляция жасауға қарсы тұру қабілеті. Қазақстандағы интернет-алаяқтықтың 75%-ы дәл осы әдіспен жасалуы — біздің қоғамда «цифрлық күмәншілдік» (digital skepticism) мәдениетінің әлі қалыптаспағанын көрсетеді. Мемлекеттік «Киберқалқан» бағдарламасы аясында халықты оқыту шаралары жүргізілгенімен, олардың әдістемесі көбіне формальды сипатта қалып қоюда. Нақты нәтижеге жету үшін оқыту процесін «ойын элементтерімен» (gamification) толықтырып, интерактивті симуляциялар арқылы жүзеге асыру қажет.

2. Киберқылмыстардың құқықтық реттелуі және халықаралық юрисдикция

Талқылаудың келесі маңызды блогы — киберқылмыстың трансшекаралық сипаты. Қылмыскер Қазақстанда отырып, серверлері Панамада орналасқан жүйе арқылы Еуропа азаматтарын тонауы мүмкін. Мұндай жағдайда «территориялық юрисдикция» ұғымы өз маңызын жоғалтады.

Қазақстанның Будапешт конвенциясына (Convention on Cybercrime) әлі мүше болмауы халықаралық деңгейде жедел ақпарат алмасуға кедергі келтіреді. N. Kshetri (2019) зерттеулері көрсеткендей, дамушы елдерде киберқылмыспен күрестің тиімсіздігі көбіне «құқықтық вакууммен» байланысты. Біздің заңнамада «цифрлық дәлелдемелер» (digital forensics) ұғымы әлі де толыққанды процедуралық бекітуді талап етеді. Бұлттық технологияларда сақталған деректерді тінту және алу процестері ҚР Қылмыстық-процестік кодексінде халықаралық стандарттарға сай (ISO/IEC 27037) нақтылануы тиіс.

3. Криптовалюталар және қылмыстық кірістерді заңдастыру

Қазіргі заманғы киберқылмыстың ажырамас бөлігі — криптовалюталық транзакциялар. Ransomware (бопсалаушы бағдарламалар) шабуылдарынан кейін төлемді биткоин немесе монорео түрінде талап ету — жаһандық тренд. Қазақстанда крипто-майнинг саласы дамығанымен, крипто-активтердің айналымын бақылау тетіктері әлі де әлсіз.

Талқылау барысында Chainalysis компаниясының есептерін негізге ала отырып, «миксерлер» мен «децентрализацияланған биржалар» (DEX) арқылы ақша ізін жасыру мәселесін қарастыру керек. Қазақстандық құқық қорғау органдарына блокчейн-аналитика құралдарын (мысалы, Crystal немесе Elliptic сияқты бағдарламалық кешендерді) меңгерген мамандар ауадай қажет. Бұл тек техникалық мәселе емес, бұл ұлттық қаржылық қауіпсіздік мәселесі.

4. Жасанды интеллект (AI): Қорғаныс па, әлде қару ма?

Бұл бөлім мақаланың ең заманауи және көлемді бөлімі болуы тиіс. Біз «ЖИ-ге қарсы ЖИ» (AI vs AI) парадигмасын талқылаймыз.

Қауіп: Қылмыскерлер AI көмегімен адам дауысын (Deepfake voice) немесе бейнесін айнытпай сала алады. Бұл банк секторларындағы биометриялық қорғаныс жүйелерін нөлге теңестіруі мүмкін.

Шешім: Қорғаныс жүйелері (SIEM/SOAR) адамның қатысуынсыз шабуылды анықтап, оған миллисекундтар ішінде жауап беретін «өзін-өзі емдейтін» (self-healing) алгоритмдерге көшуі керек.

5. Сыни ақпараттық инфрақұрылымды (САИ) қорғау

Қазақстанның энергетикалық, көлік және байланыс жүйелері толықтай цифрландырылған. Сондықтан, бұл жүйелерге жасалған кибер-теракт ел экономикасын параличке ұшыратуы мүмкін. Stuxnet немесе BlackEnergy сияқты тарихи шабуылдарды мысалға келтіре отырып, Қазақстанның өнеркәсіптік басқару жүйелерінің (SCADA) осалдығын талқылау қажет. Мұнда ISO/IEC 27019 стандартын қолданудың маңыздылығын ерекше атап өткен жөн.

6. Компаративті талдау: эстония тәжірибесі және қазақстан

Киберқауіпсіздік саласындағы ең үздік модель — Эстония тәжірибесі (E-Estonia).

Эстонияның 2007 жылғы «Кибер-соғысы».

2007 жылы Эстония әлемдегі алғашқы мемлекеттік деңгейдегі жаппай кибершабуылға (DDoS) тап болды. Банктер, мемлекеттік порталдар және БАҚ жұмысы тоқтап қалды. Бұл оқиға Эстонияның стратегиясын түбегейлі өзгертті:

1. Cyber Defence Unit (Kaitseliit): Ерікті IT-мамандардан құралған кибер-резерв құрылды. Қазақстанның BugBounty платформасы осы модельдің элементтерін қамтиды, бірақ бізде еріктілер мен мемлекет арасындағы заңнамалық байланыс әлі де әлсіз.

2. Data Embassies: Эстония өз деректерінің резервтік көшірмелерін Люксембургтегі серверлерде сақтайды («Деректер елшілігі»). Қазақстан үшін бұл өте маңызды кейс, өйткені геосаяси жағдайларға байланысты деректердің физикалық қауіпсіздігін қамтамасыз ету — САИ қорғаудың басты шарты.

Төменде «Қазақстанның киберқалқаны» аясындағы негізгі индикаторлардың кестелік анализі берілген.

Көрсеткіш атауы	2018 жыл (бастапқы)	2023 жыл (ағымдағы)	Өсу/ Төменде у серпіні
Тіркелген интернет-алаяқтық саны	~4,000	~21,000	+425% (Критика

			лық өсім)
BugBounty платформасындағы сарапшылар	0	700+	Сапалық ілгерілеу
Гранттар саны (АҚ мамандығы)	600	2,632	+338% (Кадрлы қ резерв)
Жаһандық киберқауіпсіздік индексі (ITU)	82-орын	31-орын	+51 позиция (Оң нәтиже)

Тіркелген интернет-алаяқтықтың 425%-ға өсуі мемлекеттік қорғаныс жүйесінің тиімсіздігін емес, керісінше, қоғамның цифрлық трансформациясының жылдамдығын көрсетеді. 2018 жылы онлайн-банкинг қолданушыларының саны бүгінгі көрсеткіштен 5 есе аз болған. Демек, «қылмыс алаңы» кеңейді. Сонымен қатар, азаматтардың құқық қорғау органдарына жүгіну деңгейі артқан (латентті қылмыстардың азаюы).

Техникалық қосымша: шабуыл алгоритмдері:

1. Distributed Denial of Service (DDoS) алгоритмі:

DDoS шабуылының мақсаты — жүйе ресурстарын (CPU, RAM, Bandwidth) тауысу.

Схема: Қылмыскер алдымен мыңдаған «боттардан» (инфекцияланған IoT құрылғылары) тұратын Botnet құрады.

Механизм: Боттар бір уақытта нысанаға (мысалы, eGov.kz) HTTP-сұраныстар жібереді. Нәтижесінде сервердің «кезегі» (queue) толып, заңды пайдаланушыларға жауап бере алмай қалады.

Қорғаныс: Traffic scrubbing (трафикті тазалау) орталықтарын қолдану.

2. SQL-инъекция (SQL Injection) тетігі:

Бұл деректер базасына шабуыл жасаудың ең танымал әдісі.

Схема: Веб-сайттың енгізу өрісіне (мысалы, "Логин") арнайы SQL коды енгізіледі.

Мысалы: ' OR '1'='1 кодын енгізу арқылы шабуылдаушы парольді білмей-ақ жүйеге әкімші ретінде кіре алады.

Қорғаныс: Prepared Statements (алдын ала дайындалған сұраныстар) және кіріс деректерін қатаң валидациялау.

Қорытынды. Жүргізілген зерттеу нәтижелерін түйіндей келе, Қазақстан Республикасының киберкеңістігін қорғау деңгейі стратегиялық тұрғыдан дұрыс бағытта дамып келе жатқанын, бірақ бірқатар маңызды түзетулерді талап ететінін атап өтуге болады.

1. Заңнамалық базаны жетілдіру: Киберқылмыстар үшін жауапкершілікті қатаңдатып қана қоймай, цифрлық активтер мен криптовалюталық транзакцияларды реттеудің нақты тетіктерін енгізу қажет.

2. Цифрлық гигиенаны жаппай енгізу: Киберқауіпсіздік негіздерін оқытуды тек университеттерде емес, мектеп қабырғасынан бастап мемлекеттік деңгейдегі міндетті бағдарлама ретінде қалыптастыру ұсынылады.

3. Технологиялық тәуелсіздік: Отандық IT-өнімдерді қолдау және BugBounty платформасын дамыту арқылы сыртқы шабуылдарға төзімділікті арттыру қажет.

4. Халықаралық ынтымақтастық: Киберқылмыстармен күресте халықаралық деңгейде жедел ақпарат алмасу жүйелерін (Interpol, Europol және өңірлік орталықтар)

белсенді пайдалану.

Қорыта айтқанда, киберқауіпсіздік — бұл аяқталған процесс емес, тұрақты бейімделуді талап ететін динамикалық жүйе. Мемлекет, бизнес және азаматтық қоғамның бірлескен күш-жігері ғана Қазақстанның цифрлық экожүйесін қауіпсіз ете алады.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Баширов А. Қазақстан Республикасындағы ақпараттық қауіпсіздік мәселелері // Қазіргі заманның өзекті мәселелері. 2015. №4. 59-61 бет.
2. Хан Т.А., Жиенбеков Ж.Е. Ақпараттық қауіпсіздікті қамтамасыз ету жүйесі // Қазіргі заманның өзекті мәселелері. 2016. №2. 37-43 бет.
3. Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен бекітілген «Қазақстанның киберқауіпсіздігі» («Қазақстанның киберқалқаны») тұжырымдамасы.
4. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd Edition. Wiley.
5. Kshetri, N. (2019). Cybersecurity in the Developing World: Lessons from Africa and Asia. Journal of Global Information Technology Management, 22(3).
6. ITU. (2024). Global Cybersecurity Index (GCI) 2024 Report. International Telecommunication Union.
7. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
8. NIST. (2023). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.
9. Zhetpissov, A. Zh. (2018). Problems of information protection in the field of detection and investigation of crimes. Current issues of modernity, №3.
10. Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.