ҒТАМР 10.77.21 **DOI 10.47649/vau.26.v80.i1.54**
ОӘЖ 343.33

З.З.Нұрыш[1*] , Е.И. Исибаева[2] , Ж.Б.Шаяхметова[3] , Д.С.Серік[4]

[1] Қазақстан Республикасы ІІМ М.Бөкенбаев атындағы Ақтөбе заң институты
Ақтөбе қ., Қазақстан Республикасы
[2] Қ.Жұбанов атындағы Ақтөбе өңірлік университеті
Ақтөбе қ., Қазақстан Республикасы
[3]Х.Досмұхамедов атындағы Атырау университеті
Атырау қ., Қазақстан Республикасы
[4] Astana IT University,
010000, Астана қ., Қазақстан Республикасы
*e-mail: zina.nurush@mail.ru

КИБЕРҚАУІПСІЗДІК САЛАСЫНДАҒЫ ХАЛЫҚАРАЛЫҚ ТӘЖІРИБЕ ЖӘНЕ КИБЕРҚАУІПСІЗДІКТІҢ ҚАМТАМАСЫЗ ЕТІЛУ МОДЕЛЬДЕРІ

Аңдатпа

Мақалада авторлар киберқауіпсіздік мәселелеріндегі мемлекеттің ұлттық қауіпсіздіктің шетел тәжірибесімен тікелей байланысты мүмкіндіктерін зерттейді. Киберқауіпсіздікті қамтамасыз етудегі халықаралық тәжірибенің ғылыми - теориялық негіздерін зерделеу, заңнаманы жетілдіру, киберқауіпсіздікті қамтамасыз ету саласындағы мамандарды даярлау және олардың біліктілігін арттыру арқылы пайдаланушылардың дербес деректерін, мемлекеттік органдар сайттарын киберқауіпсіздіктен қорғауды жетілдіру арқылы Қазақстан Республикасында киберқауіпсіздікті қамтамасыз етуді арттыру мақсатында мемлекеттік басқару тетіктері қаралатын болады. Мақаланың мақсаты – киберқауіпсіздік саласындағы халықаралық тәжірибені зерделеу негізінде Қазақстан Республикасында киберқауіпсіздікті қамтамасыз етудің тиімді мемлекеттік басқару тетіктерін айқындау және жетілдіру. Негізгі бағыттары - осы саладағы халықаралық зерттеулерді ескере отырып, көптеген міндеттерді жедел шешуге мүмкіндік береді. Ғылыми зерттеу идеясы арнайы құзыреттіліктерін дамыту үшін жағдай жасау мақсатында киберқауіпсіздік негіздерін зерделеу, ақпараттық қауіптердің түрлері, киберқауіптермен күресудің құралдары мен әдістері, дербес ақпараттарды қорғау, киберқауіптердің нақты қауіп екеніне сендіру. Жұмыстың ғылыми тұрғысында, тәжірибелік маңыздылығын сипаттау. Жүргізіліп жатқан жұмысты бағалау, талдау және жүйелеу. Киберқауіпсіздіктің қауіпті соқтығыстарға кездесуіне құпия ақпараттың сақталуын, инфрақұрылымнан тұрақты жұмысты қамтамасыз ете отырып, қауіптердің алдын алу, анықтау және оларға ден қою әдістерін қамтиды. Киберқауіпсіздік жеке тұлғалардан бастап ірі корпорацияларға дейін барлығы үшін маңызды және үнемі жетілдіруді және жаңа қауіптерге бейімделуді көздейтін зерттеу. Ккибершабуылдарға тиімді қарсы тұру және тәуекелдерді азайту үшін киберқауіпсіздіктің негізгі принциптері мен технологияларын түсіну. Жыл сайын хакерлік шабуылдар мен олардан келтірілген залал тез өсуде. Кибершабуылдар әрдайым дерлік өзімшілдік мақсатта деректерге қол жеткізумен байланысты. Жүргізілген зерттеудің мәні – Қазақстан Республикасында киберқауіптердің ықтималдығын төмендету үшін ұйымдастырушылық, құқықтық, техникалық құрамдас бөліктерді қамтитын кешенді шаралар қабылдау.

Негізгі сөздер: Жаһандық киберқауіпсіздік, инновация, киберкеңістік, киберқылмыс, медиа және ақпараттық сауаттылық, инфрақұрылым.

Кіріспе

Президент Қасым - Жомарт Тоқаевтың 2024 жылғы 2 қыркүйектегі Қазақстан халқына Жолдауында әділ және тұрақты қоғам құру үшін негіз ретінде заң мен тәртіптің маңыздылығын атап өтті [1]. Осыған байланысты Үкімет «Заң және тәртіп» тұжырымдамасын әзірледі, оның шеңберінде инновациялық технология мен цифрлық сервистің дамуы аясында интернет алаяқтық секілді құқық бұзушылықтарға жедел ден қоюға ғана емес, сонымен қатар азаматтардың құқықтық сауаттылығының алдын алуға және арттыруға да баса назар аударылды [2].

Киберқауіпсіздік стратегияларын құрастыру тәсілдері де ерекшеленеді. Қазақстанда киберқауіпсіздік саласын дамыту мәселелеріне ерекше көңіл бөлінеді. Елдегі киберқауіпсіздік саласын дамытудың негізгі тұжырымдамалары ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуді, сондай-ақ бірыңғай ақпараттық кеңістікті қалыптастыруды

және цифрлық экономикаға деген сенімді арттыруды қамтиды. Киберқауіпсіздікті дамыту аясында кибершабуылдардың ақпараттық қауіпсіздігі үнемі бақылау да маңызды.

Қазіргі уақытта цифрлық технологияларды толық көлемде қолдану азаматтардың күнделікті қажеттіліктерін қанағаттандырудың ажырамас бөліктерінің бірі. Көптеген елдер мемлекеттік басқарудағы киберқауіпсіздік мәселелеріне, кибершабуылдар әскери немесе экономикалық жүйелерге зиян келтіріп қана қоймай, сонымен қатар елдегі сыртқы және ішкі қауіпсіздікті тұрақсыздандыру арқылы саяси процестерге теріс әсер етуі мүмкін. Осылайша, ерекше маңызды цифрлық және ақпараттық жүйелер мен технологияларды қорғауға көп көңіл бөле бастады.

Зерттеу материалдары мен әдістері

Халықаралық құқықтық актілерді талдау тиісті қатынастар шеңберін халықаралық құқықтық реттеудің бағдарламалық, стратегиялық актілері негізінде БҰҰ қамқорлығымен киберқылмысқа қарсы күресте мемлекеттердің ынтымақтастығын кеңейту қажеттілігі туралы қорытынды жасауға мүмкіндік берді. Киберқылмысқа қарсы іс-қимылдың ұйымдастырушылық және заңнамалық шараларын құру мен әзірлеудің, әртүрлі мемлекеттердің құзыретті органдары арасындағы өзара іс-қимылды жетілдірудің маңызы зор.

2016 жылы Дүниежүзілік экономикалық форумда киберқауіпсіздік үкіметтің ең жоғары деңгейінде қатысуды талап ететін мәселе екенін атап өтті. Қазақстан, үкіметтік деңгейде киберқауіпсіздік мәселелерін цифрландырумен қамтамасыз ету [3] және «Қазақстанның кибер қалқаны» киберқауіпсіздік тұжырымдамасын [4] қабылдады.

Аталған құжаттар ақпаратты жинауға, беруге, сақтауға, алуға немесе таратуға байланысты киберкеңістіктің нақты субъектісінің (азаматтың, ұйымның, мемлекеттік билік органының, сондай-ақ қарулы қақтығыстар субъектілерінің, сондай-ақ қылмыстық, оның ішінде террористік ұйымдардың) қажеттіліктерін қанағаттандыру үшін электрондық ортаны пайдалану әдістері мен тәсілдерін айқындайды. Осылайша, цифрлық деректерді қорғау саласындағы озық халықаралық тәжірибенің киберқауіпсіздігін қамтамасыз етудің ғылыми - теориялық негіздерін зерделеу, заңнаманы жетілдіру, киберқауіпсіздікті қамтамасыз ету саласындағы мамандарды даярлау және олардың біліктілігін арттыру арқылы пайдаланушылардың дербес деректерін, мемлекеттік органдар сайттарын киберқауіпсіздіктен қорғауды жетілдіру арқылы Қазақстан Республикасында киберқауіпсіздікті қамтамасыз етуді арттыру мақсатында мемлекеттік басқару тетіктері қаралатын болады [5].

Мемлекеттердің сындарлы инфрақұрылымына деструктивті кибершабуыл мемлекеттердің өңірлік ынтымақтастығы, сондай-ақ екіжақты қарым-қатынастары шеңберінде мақұлданған барлық құжаттарда басты қатерлерінің бірі ретінде танылады. Осылайша, цифрлық кеңістікте киберқауіпсіздікті қамтамасыз ету Қазақстанда ғана емес, басқа елдерде де өзекті болып табылады, өйткені халықаралық деңгейде кибер соғыстардың туындау қаупі бар. Олар ұлттық қауіпсіздікке қатысты ықтимал қауіптер мен олардың жағымсыз әсерлері цифрландыруды кеңінен қолдану ақпараттың қолжетімділігіне алып келді. Соңғы жылдары кибершабуылдар жиі және күрделі бола бастады. Киберқылмыскерлер несие картасының нөмірлері мен жеке сәйкестендіру ақпараты сияқты құпия ақпаратты ұрлап, оны алаяқтық әрекеттер үшін пайдалана алады. Киберқауіптер әртүрлі формада болады. Бұзу-кибершабуылдардың ең көп таралған түрлерінің бірі. Хакерлер компьютерлік жүйелер мен желілерге рұқсатсыз қол жеткізу үшін өздерінің техникалық дағдыларын пайдаланады. Олар құпия ақпаратты ұрлауы немесе ауыр шабуылдарды бастау үшін құрылғыларды басқаруы мүмкін.

Шанхай Ынтымақтастық Ұйымының халықаралық келісімдерінде және кейбір екіжақты келісімдерінде «киберкеңістік» ұғымы ақпаратты қалыптастыруға, құруға, өзгертуге, беруге, пайдалануға, сақтауға байланысты және әсер ететін қызмет саласы ретінде қолданылады. Бұл ұғым инновациялық қызмет саласына қатысты Тәуелсіз Мемлекеттер Достастығының үкіметаралық келісімінде ашылады [6]. Жоғарыда айтылғандарға сүйене отырып, киберкеңістікте мемлекет үстемдігінің негізгі саласы ерекшеленеді: - ұлттық аумақта орналасқан есептеу техникасы құралдары желілерінің, байланыс және коммуникация

құралдары желілерінің және ақпаратты сақтау құралдары желілерінің жиынтығымен жасалатын ақпаратты жинаудың, берудің, сақтаудың және өңдеудің электрондық ортасы.

Мұндай аймақтандыру процестері шеңберіндегі ең маңызды оқиғалар:

- 2001 жылы Европа Кеңесінің киберқылмыс туралы Будапещт Конвенциясы ұсынылды [7];
- 2007 жылы ШЫҰ-ның «халықаралық ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі бірлескен іс-қимыл жоспарына» қол қойылды [8];
- 2010 жылы АҚШ киберкеңістікте шабуылдарды өткізуді шектейтін келісім бойынша бірлескен жұмысты бастау туралы ұсыныс жасады;
- 2011 жылы Ресей Федерациясы, Қытай, Тәжікстан және Өзбекстан БҰҰ Бас Ассамблеясының сессиясында «Халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы тәртіп ережелері» жобасын ұсынды;
- 2011 жылы БҰҰ-да ақпараттық қауіпсіздікті қамтамасыз ету туралы конвенция жобасын ұсынды;
- 2011 жылы 10 АҚШ-тың «киберкеңістіктегі іс-қимыл жөніндегі халықаралық стратегиясы» қабылданды;
- 2012-2013 жылдары ЕҚЫҰ 2016 жылы қайта қаралған және толықтырылған киберкеңістікте сенімді нығайту жөніндегі шаралар жобасын және басқаларын ұсынды [9].

Нәтижелер және оларды талқылау

Құпия деректерді ұрлауға және желілерді бұзуға байланысты бірқатар атышулы оқиғалар цифрлық ақпараттың бизнестің, мемлекеттік инфрақұрылымның жұмыс істеуіне негіз болғанын, сондай-ақ пайдаланушылардың жеке өміріне берік енгенін дәлелдейді.

Киберқауіпсіздікті дамытудың маңыздылығы қосылған ғаламтор заттары құрылғыларының үлкен өсу қарқынына байланысты артуда. Әлемдік бағалау көрсеткіштерінің мәліметтері бойынша, 2028 жылға қарай жасанды интеллект нарығының көлемі жыл сайын шамамен 38% өсіммен 224,9 млрд жетеді деп күтілуде. Жоғарыда аталған барлық аспектілерден басқа, киберқауіпсіздік адам факторымен де байланысты. Статистикаға сәйкес, оқиғалардың көпшілігі пайдаланушылардың қарапайым қателіктеріне байланысты: әлсіз парольдер, зиянды сілтемелерді басу немесе күмәнді файлдарды жүктеу. Киберқауіпсіздік деректерді, жүйелер мен желілерді хакерлер мен вирустардың цифрлық шабуылдарынан, ақпараттық қауіпсіздік кез-келген түрдегі ақпаратты (сандық, қағаз түрінде) кез-келген қауіптен қорғауға негізделген. Бұған деректердің бұзылуы немесе физикалық жою кіреді. Киберқауіпсіздік-бұл ақпараттық қауіпсіздіктің бір бөлігі, бірақ цифрлық ортаға баса назар аударылады.

Киберқауіпсіздік стратегиясы-бұл киберкеңістікте мемлекеттің қауіпсіздігін қамтамасыз етуге бағытталған мемлекеттік саясатты белгілейтін және анықтайтын құжат. Зерттеу үшін Еуропалық одақтың бірнеше мемлекеттерінің киберқауіпсіздік стратегиялары таңдалды, Германия, Испания, Франция, Эстония жаһандық киберқауіпсіздік индексінің бірінші орнын алады. Қазақстанда киберқылмысқа қарсы іс-қимыл бойынша мамандандырылған бөлімшелер мен орталықтар құруды қоса алғанда, белсенді күрес жүргізілуде. ҚР ІІМ киберқылмыстарды анықтау және ашу, сондай-ақ күрес стратегияларын әзірлеу үшін киберқылмысқа қарсы іс-қимыл департаментін құрды. Қаржы саласында күдікті операцияларды бұғаттау үшін антифрод орталығы құрылды.

Қабылданған шараларға қарамастан, киберқылмыс мәселесі өзекті болып қала береді және әртүрлі мемлекеттік органдар арасындағы өзара іс-қимылды жақсартуды, қылмыстарды ашу деңгейін арттыруды және халықаралық ынтымақтастықты нығайтуды қоса алғанда, күрес әдістерін одан әрі жетілдіру талап етіледі. Киберқылмыстың дүниежүзілік проблема екенін түсіну маңызды. Кибершабуылдар жеке ұйымдарды да, мемлекеттік құрылымдарды да параличке айналдыруы мүмкін. Сарапшылар киберқылмыстардың кідірісін өте жоғары бағалайды: 80 % - АҚШ - та, 75% - Германияда, Ұлыбританияда - 85 %, ал Ресейде-90% - дан астам.

Киберқылмыс құбылысына қарсы іс-қимылдың тиімділігі мемлекеттік және жеке секторлардың бірлескен іс-әрекеттерінде, халықаралық және ұлттық заңнаманы жетілдіруде,

киберқылмысқа қарсы күресте халықаралық бөлімшелер мен құрылымдарды ұйымдастыруда көрінеді.

Қазақстанға келетін болсақ, бүгінгі таңда интернетте жасалып жатқан қылмыстардың барлық спектрін қамтитын құбылыстар ретінде кибертерроризм мен киберқылмысқа қарсы күрес бойынша кешенді зерттеулер әлі жоқ.

Киберқылмысқа қарсы зерттеулер, әсіресе халықаралық өлшем контекстінде және киберқылмысты жаһандық құбылыс ретінде қарастыруды қазіргі уақытта тек шетелдік ғалымдар жүргізеді. Сонымен қатар, олар, әрине, қазақстандық заңнаманың аспектілерін қамтымайды [10].

Халықаралық тәжірибе елдегі киберқауіпсіздікті қамтамасыз етудің өзектілігі мен маңыздылығын көрсетті. Осыған байланысты, бүгінгі таңда әлемде киберқауіпсіздікті қамтамасыз ету деңгейін бағалаумен тікелей айналысатын екі ғылыми-зерттеу институты бар:

1. Жаһандық киберқауіпсіздік индексі (GCI) - бұл мемлекеттердің киберқауіпсіздік мүмкіндіктерін бағалауға арналған itu-ABI research бірлескен жобасы.

2. Ұлттық киберқауіпсіздік рейтингі (NCSI) - бұл елдердің киберқауіптердің алдын алуға және киберқылмыстарды басқаруға дайындығын өлшейтін жаһандық индекс [11].

Қазақстан басқа елдермен ынтымақтастықта дамуы және жұмыс істеуі қажет. Үкімет деңгейінде киберқауіпсіздік мәселесі, жоғарыдағыдай, 2017 жылы Қазақстанның киберқауіпсіздік тұжырымдамасы қабылданған сәттен бастап қарастырыла бастағанын атап өтуге болады. Ақпараттық-коммуникациялық технологияларды қылмыстық пайдаланумен күресте мемлекеттер ынтымақтастығының маңызды мәселелері Халықаралық электрбайланыс одағына жүктелді. Кейіннен жоспарланған іс-шараларды орындау үшін ХЭО-ның компьютерлік қылмыстармен күресуге бағытталған бірқатар қарарлары қабылданды. Іс жүзінде ТМД қатысушылары болып табылатын барлық мемлекеттер тиісті міндеттерді жүзеге асырған жоқ, бұл кешенді трансұлттық ынтымақтастықты талап ететін ақпараттық қылмысқа қарсы іс-қимылды айтарлықтай төмендетеді. Соңғы жылдары киберқылмыспен күресте құқықтық реттеуді күшейтуге және халықаралық ынтымақтастықты жақсартуға бағытталған бірнеше маңызды құжаттар әзірленіп, қабылданды. Осылайша, киберқылмысқа тиімді қарсы тұру үшін тек технологиялық аспектілерді ғана емес, сонымен қатар әлеуметтік салдарды, сондай-ақ осы саладағы халықаралық ынтымақтастық пен бірлескен күш-жігердің қажеттілігін ескеру қажет.

Қорытынды

Мемлекеттегі «Ақпараттандыру туралы» заң қабылданған сәттен бастап 15 реттен астам, «ҚР Ұлттық қауіпсіздігі туралы» заңға 30-дан астам, «Дербес деректер және оларды қорғау туралы» заңға 5 реттен астам өзгерістер мен толықтырулар енгізілгенін атап өткен жөн [12]. Осылайша, Қазақстанның киберқауіпсіздік заң жобасында мынадай негізгі 4 бағытты қамтуды ұсынамыз:

1. Маңызды ақпараттық инфрақұрылымды кибершабуылдардан қорғауды күшейту. Маңызды ақпараттық инфрақұрылым - бұл негізгі қызметтерді ұсынуға тікелей қатысатын компьютерлік жүйелер.

2. Заңға сәйкес киберқауіпсіздік жөніндегі уәкілетті орган киберқауіпсіздік саласындағы қауіптер мен инциденттерді зерттейді, олардың әсерін анықтайды және киберқауіпсіздікке байланысты одан әрі инциденттердің пайда болуына жол бермейді. Үкімет Қазақстан азаматтарына киберқауіптерге тиімді әрекет ете алатынына және Қазақстан мен олардың азаматтарының қауіпсіздігін қамтамасыз ете алатынына кепілдік береді.

3. Кибершабуылдар туралы ақпарат алмасу үшін негіз жасау. Заң ақпарат алмасуды жеңілдетеді, бұл өте маңызды, өйткені уақтылы ақпарат Үкімет пен акт жүйелерінің иелеріне осалдықтарды анықтауға және киберқауіптердің алдын алуға тиімдірек көмектеседі. Киберқауіпсіздік жөніндегі уәкілетті органның ақпарат сұрауына негіз болады.

4. Отандық бизнесті ынталандыру және қолдау мақсатында киберқауіпсіздік қызметтерін жеткізушілер үшін клиентке бағдарланған лицензиялау жүйесін құру. Сондай-ақ, басқарылатын қауіпсіздік операциялары орталығының енуіне тестілеу және мониторинг

саласында қызмет көрсетушілерді лицензиялауға жеңіл тәсілді енгізу.

Цифрландыру дәуірінде мемлекет пен оның қоғамына қандай сын-қатерлер туындайды. Қазақстан, басқа елдер сияқты, киберқауіпсіздік саласында бірқатар сын-қатерлерге тап болды. Олардың арасында кибершабуылдар, кибер тыңшылық және кибертерроризм түріндегі қауіптер олар үнемі дамып, жетілдіріліп отырады. Экономиканы цифрландырудың өсуі, киберқауіпсіздіктің ең әлсіз буындарының бірі-адами фактор.

Бүгінгі таңда АҚШ пен Еуропа одақтарының агенттіктері өздерінің киберқауіпсіздігін қамтамасыз ету шеңберінде тәуекелдерді белсенді түрде қадағалап, ең ірі мемлекеттік мекемеден бастап жеке пайдаланушыға дейін барлығына назар аударады. Интернетті пайдаланатын кез-келген адам оны қалай қауіпсіз және ыңғайлы ету керектігін түсінуі керек. Күн сайын мыңдаған адамдар өз желілері мен қауіпсіздік ұрлығына ұшырайды, өйткені олар веб-құрылғыларын қалай дұрыс қорғау керектігін білмейді, сондықтан хабардар болу үшін шаралар қабылдау өте маңызды.

Медиа және ақпараттық сауаттылықты оқыту пайдаланушыларға жауапкершілік сезімін ояту үшін өте маңызды. Медиа және ақпараттық сауаттылықты оқыту киберқауіпсіздік стратегиясының бір бөлігі ғана болмауы керек, ол ұлттық коммуникациялық саясаттың нәтижесі болуы керек. Осының арқасында коммуникациялық жүйелер мен технологияларды қоғамның игілігі үшін үйлестірілген, дәйекті және жүйелі түрде әзірлеуге және пайдалануға болатын қолайлы шеңберлер қалыптасады. Нәтижесінде қоғамның ұлттық деңгейде ақпараттық-коммуникациялық технологиялардың дамуынан туындаған күрделі мәселелерді тиімді және жүйелі түрде шешуге дайын болуына әкеледі.

Қазақстан Республикасында киберқауіптердің ықтималдығын төмендету үшін ұйымдастырушылық, құқықтық, техникалық құрамдас бөліктерді қамтитын кешенді шаралар қабылдау қажет, атап айтқанда:

1. Электрондық ақпараттық ресурстарды, ақпараттық жүйелерді және ақпараттық-коммуникациялық инфрақұрылымды пайдаланушылардың хабардарлығын арттыру;
2. Киберқауіпсіздікті қамтамасыз етуге байланысты қызметті жүзеге асыратын отандық компанияларды ынталандыру және олардың қызметінің ауқымдылығын мемлекет деңгейіне дейін көтеру;
3. Киберқауіптерден (кибершабуылдардан) отандық қорғау құралдарының үлесін ұлғайту;
4. Киберқауіпсіздікті қамтамасыз етудің нормативтік құқықтық базасын жетілдіру, атап айтқанда;
5. Ақпараттық қауіпсіздік тақырыбына арналған халықаралық және өңірлік полигондарды, конференцияларды ұйымдастыру;
6. Киберқауіпсіздік мамандарының біліктілігін арттыру курстарын ұйымдастыру.
7. Киберқауіпсіздік саласында сенімді және тиімді құқықтық базаны құру қиын міндеттердің бірі болып табылады. Ұлттық киберқауіпсіздік стратегиясын және құқықтық негізді әзірлеу, білім беру жүйесіндегі деңгей мен талаптарды арттыру.

Қазақстандағы ақпараттық қауіпсіздік пен киберқауіпсіздік тұрақтылықты қамтамасыз етуде, экономиканы дамытуда және мемлекет пен оның азаматтарының мүдделерін қорғауда шешуші рөл атқарады. Қарқынды цифрлық даму жағдайында киберқауіпсіздік мәселелері Үкіметтің де, жеке сектордың да жүйелі көзқарасы мен келісілген күш-жігерін талап ете отырып, ерекше өзектілікке ие болуда. Цифрлық әлемде киберқауіпсіздік технологияның маңызды аспектісіне айналды. Интернетке тәуелділіктің және электронды құрылғыларды пайдаланудың артуына байланысты киберқауіпсіздікке деген қажеттілік бұрынғыдан да жоғары. Киберқауіпсіздік электрондық құрылғыларды, желілерді және құпия ақпаратты рұқсатсыз кіруден, ұрлықтан және зақымданудан қорғау тәжірибесін білдіреді. Киберқауіпсіздіктің маңыздылығы, киберқауіпсіздік түрлері және кибершабуылдардан қорғану үшін қолданылатын шаралар қарастырылады.

ӘДЕБИЕТТЕР ТІЗІМІ

1 Қасым-Жомарт Тоқаевтың «Әділетті Қазақстан: заң мен тәртіп, экономикалық өсім, қоғамдық оптимизм» атты Қазақстан халқына Жолдауы 2024 жылғы 2 қыркүйек. [Электронды ресурс] – URL: https://egov.kz/cms/kk/articles/stateplan (қаралу уақыты: 04.03.2025 ж.).

2 Қазақстан Республикасы Президентінің «Қоғаммен әріптестікте қоғамдық қауіпсіздікті қамтамасыз етудің 2024-2028 жылдарға арналған Тұжырымдамасы» туралы 22 ақпан 2023 жылғы Жарлығы. [Электронды ресурс] – URL: https://adilet.zan.kz/kaz/docs/P2300001233 (қаралу уақыты: 04.03.2025 ж.).

3 Қазақстан Республикасы Үкіметінің 2023 - 2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы 2023 жылғы 28 наурыздағы №269 қаулысы. [Электронды ресурс] - URL: https://adilet.zan.kz/kaz/docs/P2300000269 (қаралу уақыты: 17.04.2025 ж.).

4 Қазақстан Республикасы Үкіметінің «Киберқауіпсіздік тұжырымдамасын бекіту туралы» ("Қазақстанның кибер қалқаны") қаулысы: 2017 жылғы 30 маусым № 407. [Электронды ресурс] - URL: https://adilet.zan.kz/kaz/docs/P1700000407. 04.07.2025. (қаралу уақыты: 17.04.2025 ж.).

5 Исабаева С., Кармыс Г., Бексултанов А., Жусупова Г. Сравнительный анализ рейтинга стран по цифровизации и кибербезопасности: проблемы и возможности // Казахстан – Спектр. – 2018. - №3(85). – С. 23-36.

6 Қазақстан Республикасының Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы Төтенше жағдайларды жоюда көмек көрсету кезінде өзара іс-қимыл жасау туралы келісімді ратификациялау туралы 2007 жылғы 29 мамырдағы N257 Заңы. [Электронды ресурс] - URL: https://www.google.com/search. (қаралу уақыты: 17.04.2025 ж.).

7 Компьютерлік қылмыстар туралы Конвенция (Еуропа Кеңесінің киберқылмыс туралы Конвенциясы, Cybercrime CETS Конвенциясы № 185) (Будапешт, 23 қараша 2001 ж.). [Электронды ресурс] - URL: https://online.zakon.kz/Document/?doc_id=30170556&show_d. (қаралу уақыты: 17.04.2025 ж.).

8 Ұжымдық қауіпсіздік туралы шарт ұйымына мүше мемлекеттердің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастығы туралы келісімді ратификациялау туралы Қазақстан Республикасының Заңы 2019 жылғы 5 наурыздағы №234-VI ҚРЗ. [Электронды ресурс] - URL: https://adilet.zan.kz/kaz/docs/Z1900000234 (қаралу уақыты: 17.04.2025 ж.).

9 «Шанхай ынтымақтастық ұйымына мүше мемлекеттердің үкіметтері арасындағы халықаралық ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ынтымақтастық туралы келісімді ратификациялау туралы" Қазақстан Республикасы Заңының жобасы туралы Қазақстан Республикасы Үкіметінің 2010 жылғы 28 қаңтардағы №26 Қаулысы». [Электронды ресурс] - URL: https://prg.kz/Document/?doc_id=30574651 (қаралу уақыты: 16.02.2025 ж.).

10 Зейнелгабдин А., Исабаева С., Кибербезопасность Казахстана в период цифровой трансформации// Государственный аудит. - 2019. - №4 (45). – С. 46-55.

11 Губайдуллина М. Внешнеполитическая деятельность и дипломатия в современных условиях транспарентного информационного пространства // International Relations and International Law Journal. – 2018. – Т. 79, №3. – С. 14-22.

12 Қазақстан Республикасының Ақпаратқа қол жеткізу туралы 2015 жылғы 16 қарашадағы №401-V ҚР Заңы. [Электронды ресурс] – URL: https://adilet.zan.kz/kaz/docs/Z1500000401 (қаралу уақыты: 16.02.2025 ж.).

МЕЖДУНАРОДНЫЙ ОПЫТ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ И МОДЕЛИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Аннотация

В статье авторы исследуют возможности государства в вопросах кибербезопасности, непосредственно связанные с зарубежным опытом национальной безопасности. Будут рассмотрены механизмы государственного управления в целях повышения обеспечения кибербезопасности в Республике Казахстан путем изучения научно - теоретических основ международного опыта в обеспечении кибербезопасности, совершенствования законодательства, подготовки и повышения квалификации специалистов в области обеспечения кибербезопасности путем совершенствования защиты персональных данных пользователей, сайтов государственных органов от кибербезопасности. Цель статьи-определение и совершенствование эффективных механизмов государственного управления обеспечением кибербезопасности в Республике Казахстан на основе изучения международного опыта в области кибербезопасности. Основные направления-позволяют оперативно решать многие задачи с учетом международных исследований в данной области. Идея научного исследования заключается в изучении основ кибербезопасности с целью создания условий для развития специальных компетенций, типов информационных угроз, средств и методов борьбы с киберугрозами, защиты персональной информации, убеждения в том, что киберугрозы являются реальной угрозой. Описание практической значимости работы в научном контексте. Оценка, анализ и систематизация проводимой работы. Кибербезопасность включает в себя методы предупреждения, выявления и реагирования на угрозы, обеспечивая сохранность

конфиденциальной информации при столкновении с опасными столкновениями, стабильную работу с инфраструктуры. Кибербезопасность важна для всех, от отдельных лиц до крупных корпораций, и представляет собой исследование, направленное на постоянное улучшение и адаптацию к новым угрозам. Понимание основных принципов и технологий кибербезопасности для эффективного противодействия атакам и снижения рисков. С каждым годом хакерские атаки и ущерб от них стремительно растут. Кибератаки почти всегда связаны с доступом к данным в корыстных целях. Суть проведенного исследования заключается в принятии комплексных мер, включающих организационную, правовую, техническую составляющие для снижения вероятности киберугроз в Республике Казахстан.

Ключевые слова: глобальная кибербезопасность, инновации, киберпространство, киберпреступность, медиа и информационная грамотность, инфраструктура.

INTERNATIONAL CYBERSECURITY EXPERIENCE AND CYBERSECURITY MODELS

Abstract

In the article, the authors explore the state's capabilities in cybersecurity issues directly related to foreign national security experience. The mechanisms of public administration will be considered in order to improve cybersecurity in the Republic of Kazakhstan by studying the scientific and theoretical foundations of international experience in cybersecurity, improving legislation, training and advanced training of cybersecurity specialists by improving the protection of personal data of users, websites of government agencies from cybersecurity. The purpose of the article is to identify and improve effective public administration mechanisms for ensuring cybersecurity in the Republic of Kazakhstan based on the study of international experience in the field of cybersecurity. The main directions allow us to quickly solve many tasks, taking into account international research in this field. The idea of scientific research is to study the basics of cybersecurity in order to create conditions for the development of special competencies, types of information threats, means and methods of combating cyber threats, protection of personal information, and the belief that cyber threats are a real threat. Description of the practical significance of the work in a scientific context. Assessment, analysis and systematization of the work carried out. Cybersecurity includes methods for preventing, detecting and responding to threats, ensuring the safety of confidential information in the event of dangerous collisions, and stable operation of the infrastructure. Cybersecurity is important for everyone, from individuals to large corporations, and is a study aimed at continuous improvement and adaptation to new threats. Understanding the basic principles and technologies of cybersecurity to effectively counter attacks and reduce risks. Hacker attacks and damage from them are growing rapidly every year. Cyber attacks are almost always associated with access to data for personal gain. The essence of the study is to take comprehensive measures, including organizational, legal, and technical components to reduce the likelihood of cyber threats in the Republic of Kazakhstan.

Keywords: global cybersecurity, innovation, cyberspace, cybercrime, media and information literacy, infrastructure.

REFERENCES

1 Memleket basşysy Qasym-Jomart Toqaevtyñ Qazaqstan halqyna «Ädılettı Qazaqstan: zañ men tärtıp, ekonomikalyq ösım, qoğamdyq optimizm» atty Joldauy 2024 jylğy 2 qyrküiek. *[Address of Kassym-Jomart Tokayev to the People of Kazakhstan "A Fair Kazakhstan: Law and Order, Economic Growth, Public Optimism" September 2, 2024]*. Available at: - URL: https://egov.kz/cms/kk/articles/state_plan [in Kazakh]. (accessed: 04.03.2025).

2 Qazaqstan Respublikasy Prezidentınıñ 22 aqpan 2023 jylğy «Qoğammen ärıptestıkte qoğamdyq qauıpsızdıktı qamtamasyz etudıñ 2024-2028 jyldarğa arnalğan Tūjyrymdamasy» turaly Jarlyğy. *[Decree of the President of the Republic of Kazakhstan dated February 22, 2023 on the "Concept of Ensuring Public Safety in Partnership with Society for 2024-2028"]*. Available at: - URL: https://adilet.zan.kz/kaz/docs/P2300001233 [in Kazakh]. (accessed: 04.03.2025).

3 2023 - 2029 jyldarğa arnalğan sifrlyq transformasia, aqparattyq-komunikasialyq tehnologialar salasyn jäne kiberqauıpsızdıktı damytu tūjyrymdamasyn bekıtu turaly Qazaqstan Respublikasy Ükımetınıñ 2023 jylğy 28 nauryzdağy №269 qaulysy. *[Resolution of the Government of the Republic of Kazakhstan No. 269 of March 28, 2023 on approval of the Concept for the Development of Digital Transformation, Information and Communication Technologies and Cybersecurity for 2023-2029]*. Available at: - URL: https://adilet.zan.kz/kaz/docs/P2300000269 [in Kazakh]. (accessed: 17.04.2025).

4 Qazaqstan Respublikasy Ükımetınıñ Kiberqauıpsızdık tūjyrymdamasyn bekıtu turaly ("Qazaqstannyñ kiber qalqany") qaulysy.: 2017 jylğy 30 mausym №407. *[Resolution of the Government of the Republic of Kazakhstan "On Approval of the Concept of Cybersecurity" ("Cyber Shield of Kazakhstan"): June 30, 2017 No. 407]*. Available at: - URL: https://adilet.zan.kz/kaz/docs/P1700000407 [in Kazakh]. (accessed: 17.04.2025).

5 İsabaeva S., Karmys G., Beksultanov A., Jusupova G. Sravnitelnyi analiz reitiña stran po sifrovizasii i kiberbezopasnosti: problemy i vozmojnosti [Comparative Analysis of Country Rankings on Digitalization and Cybersecurity: Challenges and Opportunities]. // Kazahstan – Spektr. – 2018. - №3(85). – P. 23-36. [in Russian].

6 Qazaqstan Respublikasynyñ Şanhai yntymaqtastyq ūiymyna müşe memleketterdiñ ükımetterı arasyndağy Tötenşe jağdailardy joiuda kömek körsetu kezınde özara ıs-qimyl jasau turaly kelısımdı ratifikasialau turaly 2007 jylğy 29 mamyrdağy N257 Zañy. *[Law of the Republic of Kazakhstan No. 257 of May 29, 2007 on ratification of the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in ProvidingAssistance in Eliminating Emergency Situations]*. Available at: - URL: https://www.google.com/search [in Kazakh]. (accessed: 17.04.2025).

7 Kömpüterlık qylmystar turaly Konvensia (Europa Keñesınıñ kiberqylmys turaly Konvensiasy,Cybercrime CETS Konvensiasy № 185) (Budapeşt, 23 qaraşa 2001 j). *[Convention on Computer Crime (Council of Europe Convention on Cybercrime, Cybercrime CETS Convention No. 185)]*. Available at: - URL: https://online.zakon.kz/Document/?doc_id=30170556&show_d [in Kazakh]. (accessed: 17.04.2025).

8 Ūjymdyq qauıpsızdık turaly şart ūiymyna müşe memleketterdiñ aqparattyq qauıpsızdıktı qamtamasyz etu salasyndağy yntymaqtastyğy turaly kelısımdı ratifikasialau turaly Qazaqstan Respublikasynyñ Zañy 2019 jylğy 5 nauryzdağy №234-VI QRZ. *[Law of the Republic of Kazakhstan on ratification of the Agreement on cooperation in the field of ensuring information security of the member states of the Collective Security Treaty Organization]*. Available at: - URL: https://adilet.zan.kz/kaz/docs/Z1900000234 [in Kazakh]. (accessed: 17.04.2025).

9 «Şanhai yntymaqtastyq ūiymyna müşe memleketterdiñ ükımetterı arasyndağy halyqaralyq aqparattyq qauıpsızdıktı qamtamasyz etu salasyndağy yntymaqtastyq turaly kelısımdı ratifikasialau turaly" Qazaqstan Respublikasy Zañynyñ jobasy turaly Qazaqstan Respublikasy Ükımetınıñ 2010 jylğy 28 qañtardağy №26 Qaulysy». *[On the draft Law of the Republic of Kazakhstan "On ratification of the Agreement on cooperation in the field of ensuring international information security between the governments of the member states of the Shanghai Cooperation Organization"]*. Available at: - URL: https://prg.kz/Document/?doc_id=30574651 [in Kazakh]. (accessed: 16.02.2025).

10 Zeinelgabdin A., İsabaeva S., Kiberbezopasnöst Kazahstana v period sifrovoi transformasii *[Cybersecurity of Kazakhstan in the period of digital transformation]*. //Gosudarstvennyi audit. - 2019.- №4 (45). – P. 46-55. [in Russian].

11 Gubaidullina M. Vneşnepoliticheskaia deiatelnöst i diplomatia v sovremennyh usloviah transparentnogo informasionnogo prostranstva [Foreign political activity and diplomacy in modern conditions of transparent information space].// International Relations and International Law Journal. – 2018. – T. 79, №3. – P. 14-22. [in Russian].

12 Qazaqstan Respublikasynyñ Aqparatqa qol jetkızu turaly 2015 jylğy 16 qaraşadağy №401-V QR Zañy. *[Law of the Republic of Kazakhstan No. 401-V of November 16, 2015 on Access to Information]*. Available at: - URL: https://adilet.zan.kz/kaz/docs/Z1500000401 [in Kazakh]. (accessed: 16.02.2025).

Information about authors:

Zina Nurysh **– corresponding author**, Master of Law, Police Colonel, Associate of the Aktobe Law Institute of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Bukenbayev, 030011, Aktobe, Republic of Kazakhstan

E-mail: nurush.zina@mail.ru

ORCID: https://orcid.org/0009-0004-7659-3321

Elizaveta Isibayeva - Candidate of Historical Sciences, Associate Professor of the Department of Jurisprudence, Aktobe Regional University named after K. Zhubanov, Aktobe, Republic of Kazakhstan

E-mail: isibaevaliza@mail.ru

ORCID: https://orcid.org/0000-0001-6727-2201

Zhanna Shayakhmetova - Associate Professor of the Department of Criminal Law Disciplines of Kh. Dosmukhamedov Atyrau University, Candidate of Law, Associate Professor of Law, Atyrau, Kazakhstan

E-mail: jan68@inbox.ru

ORCID: https://orcid.org/0000-0001-6965-9813

Darkan Serik Serikuly - master of science in cybersecurity, teacher at Astana IT University, 010000, Astana, Republic of Kazakhstan

E-mail: serik.darkan004@gmail.com

ORCID: https://orcid.org/0009-0009-0139-4113

Информация об авторах:

Зина Нурыш – **основной автор,** магистр юридических наук, полковник полиции, доцент кафедры организации безопасности на объектах транспорта Актюбинского юридического института МВД Республики Казахстан им. М. Букенбаева, 030011, г.Актобе, Республика Казахстан

E-mail: nurush.zina@mail.ru

ORCID: https://orcid.org/0009-0004-7659-3321

Елизавета Исибаева - кандидат исторических наук, доцент кафедры юриспруденции, Актюбинского регионального университета им. К. Жубанова, г. Актобе, Республики Казахстан

E-mail: isibaevaliza@mail.ru

ORCID: https://orcid.org/0000-0001-6727-2201
Жанна Шаяхметова – ассоциированный профессор кафедры уголовно-правовых дисциплин Атырауского университета им. Х. Досмухамедова, кандидат юридических наук, доцент права, г.Атырау, Республики Казахстан
E-mail: jan68@inbox.ru
ORCID: https://orcid.org/0000-0001-6965-9813
Даркан Серик – магистр наук в области кибербезопасности, преподаватель Astana IT University, 010000, г.Астана, Республика Казахстан
E-mail: serik.darkan004@gmail.com
ORCID: https://orcid.org/0009-0009-0139-4113

Авторлар туралы мәлімет:
Зина Нұрыш **– негізгі автор,** заң ғылымдарының магистрі, Қазақстан Республикасы ІІМ М.Бөкенбаев атындағы Ақтөбе заң институты көлік объектілерінде қауіпсіздікті ұйымдастыру кафедрасының доценті, полиция полковнигі, Ақтөбе қ., Қазақстан Республикасы
E-mail: zina.nurush@mail.ru
ORCID: https://orcid.org/0009-0004-7659-3321
Елизавета Исибаева – тарих ғылымдарының кандидаты, Қ.Жұбанов атындағы Ақтөбе өңірлік университеті құқықтану кафедрасының доценті, 030011, Ақтөбе қ., Қазақстан Республикасы
E-mail: isibaevaliza@mail.ru
ORCID: https://orcid.org/0000-0001-6727-2201
Жанна Шаяхметова - Х. Досмұхамедов атындағы Атырау университетінің қылмыстық-құқықтық пәндер кафедрасының қауымдастырылған профессоры, заң ғылымдарының кандидаты, құқық доценті, Атырау қ., Қазақстан Республикасы
E-mail: jan68@inbox.ru
ORCID: https://orcid.org/0000-0001-6965-9813
Даркан Серік - киберқауіпсіздік саласындағы ғылым магистрі, Astana IT University оқытушысы, 010000, Астана қ., Қазақстан Республикасы
E-mail: serik.darkan004@gmail.com
ORCID: https://orcid.org/0009-0009-0139-4113