ҒТАМР 10.81.45 https://doi.org/10.26577/JAPJ2024.112.i4.a12

Н.Б. Кубанова[1]*, Л.С. Серикова[2]

[1]Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы, Алматы қ., Қазақстан
[2]І. Жансүгіов атындағы Жетісу университеті, Талдықорған қ., Қазақстан
*e-mail: nurgul_kubanova@mail.ru

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ КИБЕРШАБУЫЛДАРДЫ ЖІКТЕУ ЖӘНЕ ҚҰҚЫҚТЫҚ РЕТТЕУ ҚАҒИДАТТАРЫ

Цифрлық технологиялардың дамуы киберқауіптердің өсуіне әкеледі, бұл кибершабуылдарды жіктеуге жүйелі көзқарасты және тиісті құқықтық реттеуді талап етеді. Цифрлық ортаны кеңінен қолдану нәтижесінде дәстүрлі қылмыстар да цифрлық кеңістікке көшті. Кибершабуыл – бүкіл әлемде өсіп келе жатқан қауіп. Кибершабуылдар мен деректердің бұзылу қаупі үкіметтер, кәсіпорындар және жеке тұлғалар үшін маңызды мәселе болып табылады.

Мақаланың мақсаты кибершабуылдарды жіктеу принциптерін зерттеу және Қазақстан Республикасындағы құқықтық реттеуді бағалау. Негізгі назар кибершабуылдардың негізгі түрлерін, олардың сипаттамалары мен жіктеу әдістерін анықтауға, сондай-ақ осы саладағы құқықтық реттеуді жақсарту бойынша ұсыныстар беру мақсатында киберқауіпсіздік саласындағы қолданыстағы заңнаманы талдауға аударылады.

Бұл тақырыптың өзектілігі киберкеңістіктегі қауіптердің өсуіне және кибершабуылдарға тиімді қарсы тұру қажеттілігіне байланысты. Интернет қолданушылар санының артуымен және ақпараттық технологиялардың дамуымен киберқылмыс жасау ықтималдығы артады. Осы саладағы құқықтық реттеу киберқауіпсіздікті қамтамасыз етуде және азаматтар мен ұйымдардың құқықтарын қорғауда шешуші рөл атқарады.

Кибершабуылдарды жіктеу қағидаттарын бағалау және Қазақстан Республикасында құқықтық реттеуді талдау, киберқауіптердің алдын алу және жолын кесу жөніндегі тиімді шараларды әзірлеу үшін үлкен практикалық маңызға ие.

Талдау әдебиеттерді шолуды, қарсы тұру әдістерін зерттеуді қамтитын кешенді тәсіл негізінде жүргізілді. Әр түрлі техникалар мен қауіп деңгейлерін ескере отырып, шабуылдарды ресми жіктеу әдістері де қолданылды.

Түйін сөздер: кибершабуыл, кибертерроризм, ақпараттық қауіпсіздік, киберқауіпсіздік, киберқалқан.

N.B. Kubanova[1]*, L.S. Serikova[2]

[1]Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Almaty, Kazakhstan
[2]Zhetysu University named after I. Zhansugurov, Taldy-Kurgan, Kazakhstan
*e-mail: nurgul_kubanova@mail.ru

Principles of classification of cyber attacks and legal regulation in the Republic of Kazakhstan

The development of digital technologies leads to an increase in cyber threats, which requires a systematic approach to the classification of cyber attacks and appropriate legal regulation. As a result of the widespread use of the digital environment, traditional crimes have also moved into the digital space. Cyberattack is a growing threat worldwide. The threat of cyber attacks and data leaks is a major concern for governments, businesses and individuals.

The purpose of the article is to study the principles of classification of cyber attacks and assessment of legal regulation in the Republic of Kazakhstan. The main focus is on identifying the main types of cyber attacks, their characteristics and classification methods, as well as analyzing current legislation in the field of cybersecurity in order to develop proposals for improving legal regulation in this area.

The relevance of this topic is due to the growing threats in cyberspace and the need to effectively counter cyber attacks. With the increase in the number of Internet users and the development of information technology, the likelihood of committing cybercrimes increases. Legal regulation in this area plays a key role in ensuring cybersecurity and protecting the rights of citizens and organizations.

Assessment of the principles of classification of cyber attacks and analysis of legal regulation in the Republic of Kazakhstan are of great practical importance for the development of effective measures to prevent and suppress cyber attacks.

The analysis was carried out on the basis of an integrated approach, including a review of the literature, the study of methods of counteraction. Methods of formal classification of attacks were also used, taking into account various methods and levels of danger.

Key words: cyberattack, cyberterrorism, information security, cybersecurity, cyber shield.

Н.Б. Кубанова[1]*, Л.С. Серикова[2]

[1]Алматинская академия МВД Республики Казахстан им. М. Есбулатова, г. Алматы, Казахстан
[2]Жетысуский университет имени И. Жансугурова, г. Талдыкорган, Казакстан
*e-mail: nurgul_kubanova@mail.ru

Принципы классификации кибератак и правовое регулирование в Республике Казахстан

Развитие цифровых технологий приводит к росту киберугроз, что требует системного подхода к классификации кибератак и соответствующего правового регулирования. В результате широкого использования цифровой среды традиционные преступления также переместились в цифровое пространство. Кибератака – растущая угроза во всем мире. Угроза кибератак и утечки данных является серьезной проблемой для правительств, предприятий и частных лиц.

Цель статьи изучение принципов классификации кибератак и оценка правового регулирования в Республике Казахстан. Основное внимание уделяется выявлению основных видов кибератак, их характеристик и методов классификации, а также анализу действующего законодательства в области кибербезопасности с целью выработки предложений по улучшению правового регулирования в данной сфере.

Актуальность данной темы обусловлена ростом угроз в киберпространстве и необходимостью эффективного противодействия кибератакам. С увеличением числа пользователей интернета и развитием информационных технологий возрастает вероятность совершения киберпреступлений. Правовое регулирование в этой области играет ключевую роль в обеспечении кибербезопасности и защите прав граждан и организаций.

Оценка принципов классификации кибератак и анализ правового регулирования в Республике Казахстан имеют большое практическое значение для разработки эффективных мер по предупреждению и пресечению кибератак.

Анализ проводился на основе комплексного подхода, включающего обзор литературы, изучение методов противодействия. Также использовались методы формальной классификации атак с учетом различных методов и уровней опасности.

Ключевые слова: кибератака, кибертерроризм, информационная безопасность, кибербезопасность, киберщит.

Кіріспе

Цифрландыру дәуірінде кибершабуылдар қазіргі заманның ажырамас бөлігіне айналуда. Бұл киберқауіпсіздіктің техникалық аспектілері үшін ғана емес, сонымен қатар киберкеңістіктегі қызметті реттейтін құқықтық механизмдер үшін де қиындық тудырады. Қазіргі цифрлық орта, ақпараттық жүйелерге киберқауіпсіздік саласында үнемі қиындықтар туғызады. Шабуылдарды қауіп деңгейіне қарай тиімді жіктеу, алдын алу шараларын әзірлеу мен инциденттерге жауап берудің негізгі элементі болып табылады.

Қасым-Жомарт Тоқаев шетелде Қазақстанға іріткі салуды көздейтін күштер барын айтты: – «Біз кибершабуылдардан сақ болуымыз керек. Кейбір күштер шетелден шабуылдар ұйымдастыруға және ел ішінде ақаулық тудырып, Қазақстандағы оң өзгерістерге кедергі жасағысы келеді. Бірақ біз таңдалған бағыттан бас тартпаймыз», – деді Президент (https://egemen.kz/article/324493-sayasi-nauqanda-kibershabuyldargha-saq-boluymyz-qadget toqaev).

Қазіргі заманғы ақпараттық-коммуникациялық виртуалды ортада барлық кибершабуылдар дәстүрлі түрде үш негізгі түрге бөлінеді: хакерлік, кибер соғыс және кибертерроризм. Ресми статистика 2020 жылы пандемия жағдайында компьютерлік шабуылдар оқиғаларының көбеюін көрсетеді (Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence, 2021).

Қазіргі таңда хакерлік жалғыз қылмыскердің жеке шабуылдары ғана емес, сонымен қатар ірі компаниялар мен үкіметтер қолдайтын және жиі қаржыландыратын ірі бизнес. Іс жүзінде әрбір кибершабуылды, ұйымда сауатты қауіпсіздік саясаты болған жағдайда ғана алдын алуға болады (Denning, 1982).

Зерттеу материалдары мен әдістері

Ғылыми мақаланы жазу кезінде жалпы ғылыми әдістер (логикалық, құрылымдық және жүйелік талдау, синтез, салыстыру, абстракциялау, индукция және дедукция, модельдеу) қолданылды. Киберқауіпсіздікке қатысты Қазақстан Республикасының заңнамалық актілерін талдауды қамтиды. Кибершабуылдарды жіктеу қағидаттарын және олардың құқықтық реттеуге сәйкестігін бағалау үшін жүйелі талдау, салыстырмалы талдау және сараптамалық бағалау әдістері қолданылады. Талдау әдебиеттерді шолуды, қарсы тұру әдістерін зерттеуді қамтитын кешенді тәсіл негізінде жүргізілді. Әр түрлі техникалар мен қауіп деңгейлерін ескере отырып, шабуылдарды ресми жіктеу әдістері де қолданылды.

Нәтижелер мен талқылаулар

В.П. Харченко кибершабуылдарға қарсы тиімді әдістер мен құралдарды әзірлеу және таңдау үшін олардың негізгі принциптерін ескере отырып, кибершабуылдардың жалпыланған классификациясын ұсынады (Харченко, 2009:134). Осы жіктеудің көмегімен оларды таңдау тиімділігін арттыру және оларды әзірлеу кезінде талаптарды қалыптастыру үшін, іс-қимылға қарсы жүйелері мүмкіндіктерін ресімдеуге болады.

А.В. Яковлеваның пікірінше, киберкеңістіктің, оның ішінде халықаралық деңгейде басқарылмауы мен реттелмеуі әлемнің барлық үкіметтері үшін маңызды мәселе болып табылады, сондықтан киберкеңістіктік ортада нормативтік-құқықтық құжаттармен реттелуі тиіс киберқауіпсіздікті қамтамасыз ету мәселесі бірінші орынға шығады (Яковлева, 2021: 70).

М. А. Желудковтың, А. М. Поповтың, М. М. Дубровинаның пікірінше, киберкеңістіктің қорғалуын халықаралық құқық түрғысынан емес, әр мемлекеттің құқықтық өкілеттіктері бар және өзінің ақпараттық кеңістігін ұлттық заңнама нормаларымен реттелетін өз бетінше басқаруы керек екенін ескере отырып жүзеге асыруға болады, мұнда өзінің тиімділігін көрсеткен киберқауіпсіздікті қамтамасыз етудің халықаралық нормалары лайықты орын табады (Желудков және басқалар, 2018).

М. Е. Бегларян, Х.В. Мамакаев ақпараттық-құқықтық кеңістікті құру жолында жаңа заңдарды қабылдау, сондай-ақ қолданыстағы заңдарды өзгерту перспективаға және жұмыс істеуге мүмкіндік беру үшін техникалық қызметкерлердің білімін пайдалану қажет деп жазады. Заң және кибернетикалық ғылымдар одағы ғана біздің заңнамамызға дұрыс түжырымдамалық аппарат пен нақты баптар береді (Бегларян, Мамакаев 2017:50).

Әдетте, сіз қандай инфрақұрылымды: жергілікті немесе бұлтты қолданғаныңыз маңызды емес, егер сіз жіберген деректер құнды болса, біреу оны алғысы келеді. Шабуылдаушылардың әрекеттерін екі негізгі түрге бөлуге болады – таратылған және мақсатты шабуылдар (Палаева және басқалар, 2017).

Таратылған кибершабуылдар бот желісін пайдалануды білдіреді және бір уақытта көптеген пайдаланушылар мен компания ресурстарына бағытталған. Әдетте, мұндай шабуылдар ұйымдар мен пайдаланушылардың тарап кеткен дерекқорларын пайдаланады.

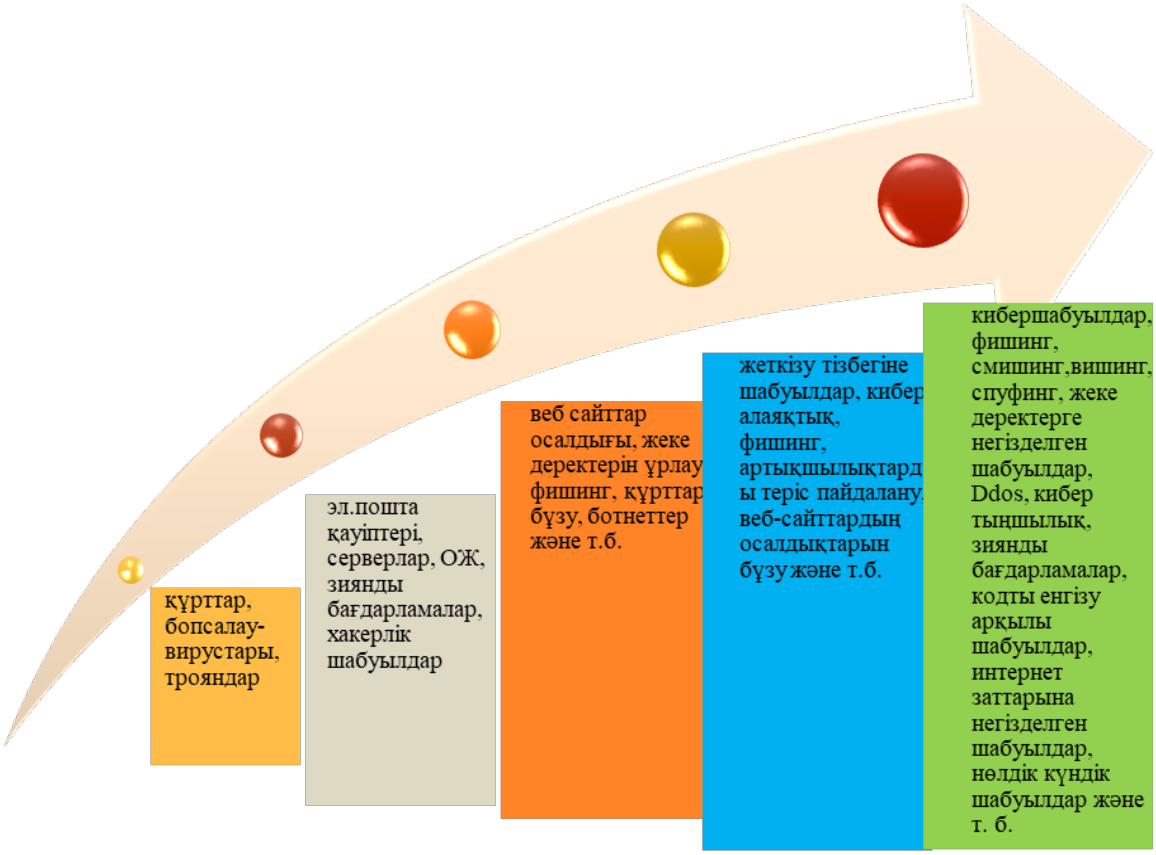
Мақсатты шабуылдардар (APT) деп, белгілі бір компанияға немесе инфрақұрылымға алдын-ала жоспарланған «шабуылды» айтады. Бұл оқиғаларда шабуылдаушы ішкі ресурстарға қол жеткізіп қана қоймайды, сонымен қатар ол анықталғанға дейін компанияның желісінде қалады – бұл күндер, айлар және тіпті жылдар болуы мүмкін. Мақсатты шабуылдарды жоғары техникалық құзыретті хакерлер жүзеге асырады. Олар автоматтандырылған құралдарды пайдаланады, шабуыл векторларын өз бетінше анықтайды, өз тәжірибелеріне сүйене отырып, 0-day осалдығын және жүйенің кейбір ерекшеліктерін пайдаланады.

Кибершабуылдардың дамуы, жыл сайын киберқауіптердің әртүрлілігі жаңа формаларға ие болатынын көрсетеді (1-сурет).

Жыл сайын әлемде шабуылдардың түрлері, саны, қуаты, ұзақтығы және шығындары артып келеді. Бұл шабуылдар әлемдік экономикаға жыл сайын миллиардтаған доллар шығын әкеледі. Сонымен қатар, смартфондар мен IoT құрылғылары сияқты жаңа құрылғылар кибершабуылға кіру нүктелерінің санын көбейтті. Хакерлер әртүрлі нұсқаларды жасау және смартфондар мен IoT құрылғыларына қол жеткізу арқылы шабуылдардың жаңа нұсқаларын пайдалану арқылы өздерінің қылмыстары үшін бар құралдарды үнемі жетілдіріп отырады.

Шабуылдаушылардың іс-әрекеттерін жақсы түсіну үшін инфрақұрылымға шабуылдың қандай түрлері бар екенін және олардың негізгі ерекшеліктерін, сондай-ақ Қазақстан Республикасының заңнамалық актілеріне сәйкес қылмыс-

тың осы түрін реттеу жөніндегі нормативтік-құқықтық құжаттаманы білу қажет. Қазақстан Республикасында заңнамалық реттеу саласында мерзімді жаңарту жүріп жатыр, оның ішінде Қазақстан Республикасының Қылмыстық кодексінің 7-тарауы (1-кесте).



1-сурет – Кибершабуылдардың дамуы

1-кесте – Кибершабуыл түрлері және ҚР ҚК тиісті баптары

Шабуыл әдістері	*Шабуыл түрі*	*ҚР ҚК бойынша тиісті бап*
Зиянды бағдарлама	Ransomware	210
	Файлсыз зиянды бағдарлама	
	Шпиондық бағдарлама	
	Жарнамалық бағдарлама	
	Троян (HookDump, Back Orifice, Pinch, TDL-4, Trojan.Winlock)	
	Құрттар	
	Руткиттер	
	Мобильді зиянды бағдарлама	
	Эксплойттар	
	Кейлоггер	
	Ботнет (Reus botnet, mirai botnet, gameover botnet)	

Кестенің жалғасы

Шабуыл әдістері	*Шабуыл түрі*	*ҚР ҚК бойынша тиісті бап*
DOS	TCP Syn fload	205, 207
	Ботнеттер	
	Smurf	
	ping-of-dealth	
	Blue whale attack	
Фишинг	Мақсатты фишинг	210
	Смишинг	
	Вишинг	
	Spear фишинг	
	Whaling	
	Search engine phishing	
	E – mail phishing	
Спуфинг	Доменды ауыстыру	207
	Эл. поштаны ауыстыру	
	ARP ауыстыру	
Жеке деректерге негізделген шабуылдар	Kerberjasting	205
	(MITM) ортадағы адам шабуылы (Wi fi MITM, SSL strip, сеансқа шабуыл, ARP спуфинг, IP спуфинг)	
	Pass the hash	
	Қатты күш шабуылдары	
	Брутфорс (SSH brute force, RDP brute force)	
Кодты енгізу арқылы шабуылдар	Sql инекция	210
	XSS сайтаралық скриптинг (Stored Xss, reflected XSS, DOM based XSS)	
Жеткізу тізбегіне шабуылдар		207, 210
Инсайдерлік қауіптер	Зиянды ішкі қауіп, абайсыз инсайдерлік қауіп	208
DNS туннельдеу		205, 207
Интернет заттарына негізделген шабуылдар		205, 210
Нөлдік күндік шабуылдар		207

Қазақстан Республикасының қылмыстық кодексінде «киберқылмыстарға» қатысты баптар, атап айтқанда 205-213 – баптар бар (Қазақстан Республикасының Қылмыстық кодексі, 2014). Бұл баптар Қазақстан Республикасының Қылмыстық кодексінің «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» деп аталатын 7-ші тарауында орналасқан, алайда бұл жерде «кибершабуыл» және «киберқылмыс» ұғымдары жазылмаған. Қазақстан Республикасының Қылмыстық кодексінде 1-кестеде келтірілген шабуылдарға толық арналған жеке бап жоқ, бірақ мұндай шабуылдарға байланысты әрекеттер зардап шеккендердің мақсаттары мен салдарына, әрекеттердің сипатына, жәбірленушіге келтірілген залалға және істің басқа да мән-жайларына байланысты Қазақстан Республикасының Қылмыстық кодексінің басқа да тиісті баптары шеңберінде сарапануы мүмкін, айыппұлды қоса алғанда, қылмыстық жауаптылықтың әртүрлі деңгейлері және/немесе бас бостандығынан айыру қолданылуы мүмкін.

Кибершабуылдар, сөзсіз, қылмыстық кодекстің құзырына жатады. Қылмыстық кодексе сәйкес, қылмыскерлер жауапқа тартылған баптардың тізімі бар. Заң шығарушыларға қыл-

мыстық жазамен жазаланатын киберқылмысқа байланысты кейбір қылмыстық әрекеттер үшін санкцияларды күшейту шараларын қолдану тиімдірек болар еді. Мысалы, DDoS шабуылы жағдайында қылмыскерлер зиянды компьютерлік бағдарламаларды таратқаны үшін ғана жазаланады, дегенмен шабуылдаушының түпкі мақсаты DDoS шабуылынан асып түседі – бұл желілік ресурстарды уақытша тоқтату немесе беделге нұқсан келтіру болуы мүмкін. Осыған байланысты, Қазақстан Республикасының қылмыстық кодексіне өзгерістер енгізу ұсынылады: Қазақстан Республикасының Қылмыстық кодексінің «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» деп аталатын 7-ші тарауын жаңа біліктілік белгілерімен толықтыру ұсынылады, оның ішінде фишинг пен спам, DDoS-шабуылдарды ұйымдастыру және жасау.

Қазақстан Республикасының Үкіметі қауіпсіздікті қамтамасыз ету қағидатын негізге ала отырып, кең ауқымды кибершабуылдардың барлық қауіптілігін, жойқын ықпалын және қорқынышты салдарын сезіне отырып, «Қазақстанның киберқалқан» бағдарламасын құруды тапсырды, оған мыналар: ағымдағы ахуалды талдау, әлемдік тәжірибе, мақсаттар, міндеттер, іске асыру нәтижелері мен кезеңі, сондай-ақ кибершабуылдарға қарсы іс-қимылдың негізгі қағидаттары мен тәсілдері кіреді.

2017 жылдың маусым айында Қазақстан Республикасының «Киберқалқан» киберқауіпсіздік мемлекеттік тұжырымдамасы бекітілді (Киберқауіпсіздік тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы). Құжат мемлекеттік органдарды ақпараттандыру, көрсетілетін мемлекеттік қызметтерді автоматтандыру саласындағы ағымдағы жағдайға, цифрлық экономиканы дамыту әлеуетіне және өнеркәсіптегі өндірістік процестерді технологиялық жаңғыртуға, ақпараттық-коммуникациялық қызметтер көрсету саласын кеңейтуге негізделген. Тұжырымдама электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникациялық желілерді қорғау, ақпараттық-коммуникациялық технологиялардың қауіпсіздігін қамтамасыз ету саласындағы мемлекеттік саясаттың негізгі бағыттарын айқындады. «Киберқалқан» негізінде Қазақстанның киберқауіпсіздік жүйесі жетістікке жетіп, дұрыс бағытпен дамуы тиіс.

«Қазақстанның киберқалқан» тұжырымдамасының мақсаты электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның жаһандық бәсекелестік жағдайында Қазақстан Республикасының орнықты дамуын қамтамасыз ететін сыртқы және ішкі қатерлерден қорғалу деңгейіне қол жеткізу және қолдау болып табылады.

«Киберқалқан» – бұл пайдаланушыларды, олардың ақпараттық жүйелерін, желілерін, бағдарламаларын цифрлық шабуылдардан қорғауды қамтамасыз етуге бағытталған қызмет. Мұндай кибершабуылдардың негізгі мақсаты хакердің өз мақсаттары үшін осы ақпаратты одан әрі теріс пайдалану үшін, пайдаланушының құпия ақпаратын алу және бүкіл бизнес-процестің жұмысын бұзу болуы мүмкін. Сондықтан, әсіресе, мемлекеттік бөлімшелер мен ірі жеке ұйымдардың контекстінде, Қазақстан үшін, әлемнің басқа елдері үшін интернетте тиімді және қауіпсіз болу үшін негізгі міндеттердің бірі дәл осы киберқауіпсіздік саласын дамыту болып табылады.

Ақпараттық қауіпсіздік мәселесі әсіресе коронавирустық пандемия кезінде өзекті болды. Пандемия кезінде киберқылмыстардың түрлері мен ауқымы айтарлықтай өсті. Жұқтыру қаупінен аулақ болу үшін адамдар күнделікті өмірінің көптеген аспектілерін, азық-түлік сатып алудан бастап жұмыс міндеттеріне дейін, деректердің бұзылу қаупі жоғары онлайн кеңістікке ауыстырды. Мұндай жағдайда ақпараттық қауіпсіздікті қамтамасыз ету, өсіп келе жатқан киберқауіптермен күресу және азаматтардың дербес деректерін, ақпараттық инфрақұрылымды, сондай-ақ стратегиялық маңызды объектілерді қорғау, соның салдарынан ұлттық ақпараттық кеңістіктің қорғалуын арттыру өте маңызды болды. Осы міндеттерді шешу үшін осы тұжырымдама бекітілді.

Тұжырымдама мемлекеттік мекемелерді ақпараттандыру, мемлекеттік қызметтерді автоматтандыру, цифрлық экономиканы дамыту перспективалары және өнеркәсіптегі өндірістік процестерді технологиялық жаңғырту саласындағы ағымдағы ахуалды талдауға, сондай-ақ ақпараттық-коммуникациялық қызметтер көрсету саласын кеңейтуге негізделеді. Құжат электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен телекоммуникациялық желілерді қорғау, ақпараттық-коммуникациялық технологияларды қауіпсіз пайдалануды қамтамасыз ету саласындағы мемлекеттік саясатты іске асырудың негізгі бағыттарын айқындайды.

2017 жылы киберқауіпсіздік тұжырымдамасын іске асыру жөніндегі іс-шаралар жоспары бекітілді, бұл ақпараттық қауіпсіздік саласындағы заңнамалық нормаларды жетілдіру және бекіту үшін негіз болды. Маңызды қадамдардың бірі компьютерлік инциденттер мен деректердің бұзылуына байланысты мүліктік және моральдық зиянды өтеуге мүмкіндік беретін салалық заңнамаға «кибер сақтандыру» ұғымын енгізу болды. Елімізде тұңғыш рет дербес деректерді қорғау жөніндегі уәкілетті орган Қазақстан Республикасының ЦДИАӨМ-не қарасты ақпараттық қауіпсіздік комитеті анықталды, ол осы бағытта белсенді жұмыс істейді. 2020 жылы дербес деректерді жинау және өңдеу ережелері бекітілді, олар жиналған сәттен бастап жойылғанға дейін деректермен жұмыс істеу рәсімдерін реттейді. Сондай-ақ, 2020 жылы электрондық ақпараттық ресурстарда дербес деректерді қорғау жөніндегі талаптарды бұзғаны үшін жауапкершілікке тарту бойынша құқық қолдану қызметі басталды. 2018 жылдан бастап ақпараттық қауіпсіздік инциденттеріне ден қоюдың ұлттық дағдарысқа қарсы жоспары шеңберінде киберқауіптерге ден қою тетіктерін сынақтан өткізу үшін әртүрлі мемлекеттік органдар өкілдерінің қатысуымен командалық-штабтық оқу-жаттығулар өткізілуде.

2018 жылы ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы, мемлекеттік мекемелердің ақпараттық ресурстарын және елдің аса маңызды ақпараттық инфрақұрылымын кибершабуылдардан қорғау мақсатында Қазақстан Республикасының Ұлттық қауіпсіздік комитетімен құрылды. Бұл 2020 жылы – ақпараттық қауіпсіздіктің 70 мыңнан астам бірегей оқиғаларын, 2021 жылы – 120 мың оқиғаларды тіркеуге мүмкіндік берді, сондай-ақ тек 2022 жылы шамамен 28 млн. шабуылды тойтаруға мүмкіндік берді.

2020 жылға қарай 17 орталық мемлекеттік орган вирусқа қарсы қорғау, компьютерлік шабуылдар мен ақпараттың тарап кетуін болдырмау құралдарымен, сондай-ақ ақпараттық қауіпсіздік оқиғаларын бақылау жүйелерімен жабдықталды. Осы бағдарламалық-техникалық құралдарды енгізу нәтижесінде ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы мемлекеттік органдарда 4 мың ақпараттық қауіпсіздік инцидентіне алып келген оқиғалардың 55 мыңнан астам бірегей түрін тіркеді. Ақпараттық қауіпсіздіктің сыни оқиғалары Мемлекет басшысына міндетті түрде хабарлануға тиіс. 2022 жылы қазақстандық ақпараттық желілер хакерлік шабуылдардың едәуір санына ұшырады, алайда «Киберқалқан» тұжырымдамасын қолданудың арқасында мемлекеттік органдар мен интернеттің басқа да пайдаланушыларының тұрақты жұмысын қамтамасыз етуге мүмкіндік туды. Атқарылған жұмыс нәтижесінде Қазақстан киберқауіпсіздік жүйесінің жетілдірілген және тиімді жұмыс істейтін тетігін алды (// http://astanazan.kz/?p=4689).

Осы стратегияға сәйкес, 2019 жылы Қазақстан Республикасы ІІМ Мақан Есболатов атындағы Алматы академиясының базасында киберқылмысқа қарсы іс-қимыл бойынша кадрлар даярлау орталығы ашылды. Сонымен қатар, академия құрамында киберлаборатория мен киберполигон құрылды, бұл киберқылмысқа қарсы іс-қимылдың тиімділігін арттыруға ықпал етеді.

Тұжырымдаманы іске асыру шеңберінде 2022 жылға дейін атқарылған жұмыстарға талдау жасайық (2-кесте).

2021 жылы киберқауіпсіздік мәселелері бойынша халықтың хабардарлық деңгейі 75% құрағанын атап өту маңызды. Ақпараттық шабуылдармен күресу үшін «Ақпараттық қауіпсіздік» мамандығы бойынша білім беру гранттарының санын 2021-2022 жылдарға 2632-ге дейін арттыруды қоса алғанда, халықтың ақпараттық сауаттылығын арттыруға бағытталған бірқатар шаралар қабылданды. Киберқауіпсіздік тұжырымдамасын әзірлеуден басқа, кибертерроризмге қарсы іс-қимыл мақсатында 2014 жылы ақпараттандыру және байланыс саласындағы қылмыстық жауапкершілік туралы бірқатар баптарды қамтитын қылмыстық кодекс қабылданды. Жергілікті және шетелдік БАҚ-пен жұмыс істеуге ерекше назар аударылады, ресми заңнамалық сайттарға мониторинг, сондай-ақ елдің арнайы қызметтеріне бақылау жүргізіледі. Қазақстанның киберкеңістігінде оқу платформалары мен білім беру сайттарына көп көңіл бөлінеді. Киберқауіпсіздікке жауапты барлау агенттіктері оқушылардың деректерін қорғауды қадағалайды және кибершабуылдардың алдын алады.

Қазақстан Республикасы Президентінің нұсқауы бойынша «Киберқалқан – 2» деп аталатын цифрлық экожүйені дамытудың 2023-2027 жылдарға арналған жаңа тұжырымдамасы әзірленді. Осы тұжырымдама шеңберінде жеке деректерді таратқаны үшін әкімшілік жауапкершілікті күшейтуді, ел аумағында отандық және шетелдік медиа-платформаларды пайдалануды реттеуді қоса алғанда, негізгі бағыттар айқындалатын болады. Жаңа құжат сонымен

қатар кибертерроризмге қарсы халықаралық тәжірибеге сүйене отырып, киберқауіпсіздікке қатысты қиындықтар мен қауіптерді ескере-ді (//https://kz.kursiv.media/2022-03-31/v-2022-godu-budetprinyata-novaya-redakciya-koncepcii-kibershhitkazahstana/).

2-кесте – «Киберқалқанның» іске асырылуы

Күтілетін нәтиже	*Орындалды*
Қазақстанның жаһандық киберқауіпсіздік индексі 2022 жылға қарай – 0,600 құрайды;	2019 жылы Қазақстанның жаһандық киберқауіпсіздік индексі 40-шы орынға, 2021 жылы 31-орынға көтерілді.
2022 жылғы кезеңге ақпараттық қауіпсіздікке төнетін қатерлер туралы хабардарлықты 20%-ға арттыру;	Әлеуметтік зерттеу нәтижелері бойынша халықтың хабардарлық деңгейі 2021 жылы – 78%, 2022 жылы -77,4% құрайды
2022 жылы ақпараттық қауіпсіздік саласында қайта даярланған мамандар саны-800;	2021-2022 жылдарға «Ақпараттық қауіпсіздік» мамандығы бойынша білім беру гранттарының саны 2 632-ге дейін үлғайтылды.
2022 жылы мемлекеттік және квазимемлекеттік секторларда пайдаланылатын ақпараттандыру және байланыс саласындағы отандық бағдарламалық өнімдер үлесін үлғайту – 50%;	150-ге жуық ақпараттық жүйе сынау рәсімінен өтіп, «ақпараттық қауіпсіздік талаптарына сәйкестігін сынау нәтижелері бойынша акт беру» мемлекеттік қызметі бойынша актілер алды. 2022 жылғы 25 ақпандағы жағдай бойынша тізілімге 56 отандық өндірушілерден акт өнімдерінің 173 атауы енгізілген. Қазақстанда 3 бейінді қоғамдық ұйым, киберқауіпсіздік талаптарына сәйкестігін бағалау бойынша аспаптық аудитпен айналысатын және киберқауіпсіздік оқиғаларының мән-жайларын, себептері мен жағдайларын зерттеуге, сондай-ақ зиянды бағдарламалық қамтамасыз етуді техникалық зерттеуге маманданған 8 отандық компания (сынақ зертханалары) құрылды және жұмыс істейді. Алғашқы отандық антивирустық қорғаныс құралдары жасалды.
2022 жылы деректерді .kz және .kaz доменімен интернет-ресурстармен шифрланған мәліметтерді беру кезінде отандық қауіпсіздік сертификаттарын пайдалану үлесі – 100%;	Интернеттің қазақстандық сегментінің кеңістігінде 160 мыңнан астам .kz және .kaz домендік атаулар тіркелген, домендік атауларды тіркеумен айналыса алатын 12 компания аккредиттелген.Маңызды инфрақұрылымы бар 495 стратегиялық нысан анықталды. Мемлекеттік қызметтер көрсету саласын оңтайландыру мақсатында ақпараттық қауіпсіздік талаптарына сәйкестігін сынау актісін алуға электрондық лицензиялау веб-порталы арқылы өтінім беру рәсімі енгізілді.
2022 жылы мемлекеттік органдардың ақпараттық жүйелерінің, мемлекеттік органдармен интеграцияланатын мемлекеттік емес ақпараттық жүйелердің, ақпараттық қауіпсіздік мониторингі орталықтарына қосылған ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілерінің ақпараттық жүйелерінің үлесі – 100%.	Мемлекет басшысының тапсырмасын орындау мақсатында сапалы көсіби қызметтер нарығын дамыту мақсатында ақпараттық қауіпсіздіктің 26 жеке жедел орталығы құрылды. Сонымен қатар, bugbounty осалдықты анықтайтын жеке платформа – ақпараттандыру объектілеріндегі ақпараттық қауіпсіздікті қоғамдық және кәсіби бақылау тетігі құрылды. Қазақстанда қаржы нарығы мен қаржы ұйымдарының ақпараттық қауіпсіздігіне төнетін қатерлерді талдау, бағалау, болжау және алдын алу жөніндегі қызметті жүзеге асыру мақсатында ақпараттық қауіпсіздіктің салалық жедел орталығы да құрылды.

Киберқауіпсіздік – кез келген бизнестің немесе ұйымның инфрақұрылымы үшін маңызды мәселе. Еліміздің өркендеп үлкен жетістіктерге жетуі үшін, ең алдымен киберқауіпсіздікті қамтамасыз ету керек (Muhammad Kashif and others, 2018: 201).

Киберқауіпсіздік ақпаратты, желілерді және деректерді ішкі және сыртқы қауіптерден қорғау үшін белсенді жұмыс істейді. Киберқауіпсіздік мамандары желілерді, серверлерді, интернетті және компьютерлік жүйелерді қорғаумен айналысады, оларға тек уәкілетті адамдар қол жеткізе алады. Киберқауіпсіздіктің әртүрлі аспектілерін түсіну, тиімді қорғауды қамтамасыз етуде маңызды рөл атқарады. Киберқауіпсіздіктің формаларын қарастырайық: желілік қауіпсіздік – негізгі желілік инфрақұрылымды рұқсатсыз кіруден және дұрыс пайдаланбаудан, сондай-ақ ақпаратты үрлаудан қорғау. Технология құрылғыларға, қолданбаларға және пайдаланушыларға қауіпсіз инфрақұрылым құруды қамтиды; ақпараттық қауіпсіздік – сандық деректерді заңсыз пайдаланудан, ашудан, рұқсатсыз кіруден, заңсыз өзгертуден және жоюдан қорғауды қамтиды; операциялық қауіпсіздік – құпия ақпараттың бөтен қолға түсуіне жол бермейтін қауіпсіздік пен тәуекелдерді басқару процесі; бағдарлама қауіпсіздігі: антивирустық қосымшалар, шифрлау және брандмауэрлер тәрізді бағдарламалық жасақтаманы пайдалану немесе жүйелерді қауіптен қорғау үшін аппараттық құралдарды пайдалану; бұлттық қауіпсіздік – бұлтты есептеу жүйелерін киберқауіптерден қорғау саясаттарының, басқару элементтерінің және құралдарының өзара байланысты жиынтығы. Бұлттық қауіпсіздік шаралары деректердің, онлайн инфрақұрылымның, сондай-ақ қолданбалар мен платформалардың қауіпсіздігін қамтамасыз етуге бағытталған (Malik, 2022:11).

Шабуылдырдың болуын ынталандыратын негізгі себептерді атауға болады: қолданыстағы жүйелік қателіктерден туындайтын себептер; жаңа технологиялардан туындайтын себептер; білім көлемінің үлғаюына байланысты себептер; күнделікті өмірді цифрлық ортаға көшіру себебінен; шабуылдардың географиялық шекаралары жоқ, бұл шабуылдарды анықтауды қиындатады (Aslan and others, 2023:10).

Аталған киберқауіпсіздік тұжырымдамасына талдау жүргізе отырып, құжаттағы «компьютерлік шабуыл» сөзін «кибершабуыл» деп өзгерту ұсынылады. «Компьютерлік шабуыл» ұғымы киберкеңістікте болатын шабуылдардың барлық түрлерін қамтымайды, өйткені шабуылдар тек компьютерлерге ғана бағытталмауы мүмкін. Қазіргі уақытта жалпы киберкеңістіктегі шабуылдар әртүрлі сандық құрылғылар арқылы жасалады. Келесі ұсыныс ретінде, киберқауіптерге қарсы тұру үшін Қазақстанның «Киберқалқан» дамып келе жатқан цифрлық инфрақұрылымын жетілдіруді және қолдауды жалғастыру маңызды екенін айта кеткен жөн.

Қазақстан Республикасының ұлттық стратегияларына сәйкес 2023 жылғы 28 наурызда 2023-2029 жылдарға арналған Цифрлық трансформация, ақпараттық-коммуникациялық технологиялар мен киберқауіпсіздік саласын дамыту тұжырымдамасы қабылданды (https ://adilet.zan.kz/kaz/docs/P2300000269). Бұл құжат жаңа мақсаттар мен міндеттерді алға тартады және киберқауіпсіздікті нығайтуға бағытталған маңызды бағытты көрсетеді.

Тұжырымдама ұлттық деңгейде киберқауіпсіздікті күшейту үшін арнайы шараларды қамтиды, мысалы, саясаттың жоғарылауын ескере отырып, нормативтік реттеуді қайта қарау және отандық ақпараттық технологиялар нарығын қолдау. Киберқауіпсіздікке арналған бөлім елдегі киберқауіпсіздіктің жоғары деңгейіне жетуге бағытталған төрт негізгі көрсеткішті анықтады (https://www.gov.kz/memleket/entities/infsecurity/press/article/details/95401?lang=ru).

Кибершабуылдардың әртүрлі түрлері мен мысалдарын қарастыра отырып, шабуылдарды қауіп деңгейіне қарай жіктеудің негізгі принциптерін бөліп көрсетуге болады (2 сурет). Бұл принциптерді түсіну ақпараттық жүйелерді әртүрлі қауіптерден сенімді қорғауды қамтамасыз ете алатын тиімді киберқауіпсіздік стратегияларын әзірлеудің маңызды элементі болып табылады. Жаңа шабуыл әдістеріне және үнемі өзгеріп отыратын киберқауіпсіздікке бейімделу үшін осы салада жалғасын табатын зерттеулер қажет.

2-сурет – Шабуылдардың жіктелуі

Қорытынды

Кибершабуылдарға қарсы түру әдістері мен шараларын едәуір қиындататын мәселелер бар. Атап айтқанда, бұл мәселені реттеуге қабілетті заңнамалық актілердің болмауы. Айта кету керек, Қазақстанда негізінен киберкеңістіктегі қатынастарды реттейтін заң саласы жеткіліксіз дамыған.

Жүргізілген ғылыми зерттеулердің нәтижелері бойынша келесі ұсыныстар жасалады:

1. Қазақстан Республикасының қылмыстық кодексінің «Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар» деп аталатын 7-ші тарауын жаңа біліктілік белгілерімен толықтыру ұсынылады, оның ішінде фишинг пен спам, DDoS-шабуылдарды ұйымдастыру және жасау.

2. Қазақстан Республикасының «Киберқалқан» киберқауіпсіздік мемлекеттік тұжырымдамасындағы «компьютерлік шабуыл» сөзін «кибершабуыл» деп өзгерту ұсынылады;

3. Киберқауіптерге қарсы түру үшін Қазақстанның «Киберқалқан» дамып келе жатқан цифрлық инфрақұрылымын жетілдіруді және қолдауды жалғастыру маңызды: күрделі мақсатты кибершабуылдарды анықтау және бейтараптандыру мақсатында кибершабуылдарға қарсы іс қимыл орталығын құру ұсынылады;

4. Кибершабуылдармен күресуге бағытталған заңнаманы әзірлеу, соның ішінде қаржылық ақпаратты ұрлағаны, БАҚ қорғау, банк карталарымен алаяқтық және т. б. үшін жазаларды қарастыру.

Ақпараттық қауіпсіздікке жауапты көзқарас әр адамның жеке үлесінен басталады. Полицияның күнделікті қызметінде заманауи технологиялық мүмкіндіктерді кеңінен пайдалану, цифрландыру әлеуетін барынша пайдалану – ішкі істер органдарының алдында тұрған басты міндеттердің бірі.

Әдебиеттер

2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасын бекіту туралы Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысы. [Электрондық ресурс] URL: https ://adilet.zan.kz/kaz/docs/P2300000269 (қаралған күні 05.03.2024).

Aslan, Ö.; Aktu ˘g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. – P. 1- 42.

Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence, 2021. – P. 15. [Электрондық ресурс] URL: https: //www.fsb.org/2021/10/cyber-incident-reporting-existing-approaches-and-next-steps-for-broader-convergence/ (қаралған күні 10.02.2024).

Denning D.E.R. Cryptography and Data Security / D.E.R. Denning. – Boston: Addison-Wesley, 1982. – P. 112.

Бегларян М.Е., Мамакаев Х.В. Кибератаки и законодательство РФ. // Право и практика. 2017. №2. – С. 46-50. [Электрондық ресурс] URL: https://cyberleninka.ru/article/n/kiberataki-i-zakonodatelstvo-rf (қаралған күні 06.02.2024).

В 2022 году будет принята новая редакция концепции «Киберщит Казахстана». [Электрондық ресурс] URL: // https://kz.kursiv.media/2022-03-31/v-2022-godu-budet-prinyata-novaya-redakciya-koncepcii-kibershhit-kazahstana/ (қаралған күні 15.02.2024г).

Желудков М.А., А. М. Попов, М. М. Дубровина. Особенности противодействия киберпреступности в России и зарубежных странах. // Вестник Волгоградской академии МВД России. 2018. №3 (46). – С. 97-101. [Электрондық ресурс] URL: https://cyberleninka.ru/article/n/osobennosti-protivodeystviya-kiberprestupnosti-v-rossii-i-zarubezhnyh-stranah (қаралған күні: 07.02.2024).

Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы.

Қазақстан Республикасының Қылмыстық кодексі. 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. // [Электрондық ресурс] URL: https://adilet.zan.kz/rus/docs/K1400000226 (қаралған күні: 01.02.2024).

Қазақстан Республикасының ЦДИАӨМ ақпараттық қауіпсіздік комитетінің сайты. [Электрондық ресурс] URL:https://www.gov.kz/memleket/entities/infsecurity/press/article/details/95401?lang=ru (қаралған күні 15.02.2024).

Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р. Основные виды кирбератак на автоматизированные системы управления технологическим процессом и средства защиты от них. Фундаментальные исследования. – 2017. – № 10-3. – С.507-511.

Саяси науқанда кибершабуылдарға сақ болуымыз қажет – Токаев. Егемен Қазақстан. 30 қыркүйек, 2022. [Электрондық ресурс] URL: https://egemen.kz/article/324493-sayasi-nauqanda-kibershabuyldargha-saq-boluymyz-qadget-toqaev (қаралған күні 10.02.2024).

Страну защитит концепция «Киберщит Казахстана». [Электрондық ресурс] URL: // http://astanazan.kz/?p=4689 (қаралған күні 15.02.2024).

Харченко В.П. Кибертерроризм на авиационном транспорте. Проблеми інформатизації та управління, 4(28), 2009. – С. 131-139.

Яковлева А.В. Кибербезопасность и ее правовое регулирование (зарубежный и российский опыт) // Социально-политические науки. 2021. Т. 11. № 4. – С. 70–81.

References

2023-2029 zhyldarga arnalgan digital transformation, akparattyk-communication technology salasyn zhane cyberkauipsizdikti damytu tuzhyrymdamasyn bekitu turaly Kazakhstan Republics Ukimetin 2023 zhylgy 28 nauryzdagi No. 269 kaulysy. [Electronic resource] URL: https ://adilet.zan.kz/kaz/docs/P2300000269 (accessed 05.03.2024).

Aslan, Ö.; Aktu g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A.; Akin, E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. – p. 1- 42.

Beglaryan M.E., Mamakaev H.V. Cyberattacks and legislation of the Russian Federation. // Law and practice. 2017. No.2. – pp. 46-50. [Electronic resource] URL: https://cyberleninka.ru/article/n/kiberataki-i-zakonodatelstvo-rf (accessed 06.02.2024).

Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence, 2021. – p. 15. [Electronic resource] URL: https: //www.fsb.org/2021/10/cyber-incident-reporting-existing-approaches-and-next-steps-for-broader-convergence / (accessed 10.02.2024).

Cyberkauipsizdik tuzhyrymdamasyn («Kazakhstan cyberkalkany») bekitu turaly Kazakhstan Republics Ukimetin 2017 zhylgy 30 mausymdagi No. 407 kaulysy.

Denning D.E.R. Cryptography and Data Security / D.E.R. Denning. – Boston: Addison-Wesley, 1982. – p. 112.

In 2022, a new version of the concept of «Cyber Shield of Kazakhstan» will be adopted. [Electronic resource] URL: // https://kz.kursiv.media/2022-03-31/v-2022-godu-budet-prinyata-novaya-redakciya-koncepcii-kibershhit-kazahstana / (accessed 15.02.2024).

Kazakhstan Republikasyn Kylmystyk codex. 2014 zhylgy 3 shildedegi No. 226-V KRZ. // [Electronic resource] URL: https://adilet.zan.kz/rus/docs/K1400000226 (accessed 01.02.2024).

Kazakhstan Republikasyn TSDIAOM akparattyk kauipsizdik komitetin sites. [Electronic resource] URL:https://www.gov.kz/memleket/entities/infsecurity/press/article/details/95401?lang=ru (accessed 02/15/2024).

Kharchenko V.P. Cyberterrorism in aviation transport. Problems of reformatization of the management, 4(28), 2009. – Pp. 131-139.

Palaeva L.V., Hafizov A.M., Gilyazetdinova A.M., Vakhitova A.R., Davydova K.N., Sirotina E.R. The main types of cyber attacks on automated process control systems and means of protection against them. Fundamental research. – 2017. – No. 10-3. – pp.507-511.

Sayasi naukanda kibershabuyldarga sak boluymyz kazhet – Tokayev. Egemen Kazakhstan. 30 kyrkuyek, 2022. [Electronic resource] URL: https://egemen.kz/article/324493-sayasi-nauqanda-kibershabuyldargha-saq-boluymyz-qadget-toqaev (accessed 10.02.2024).

The country will be protected by the concept of «Cyber Shield of Kazakhstan». [Electronic resource] URL: // http://astanazan.kz/?p=4689 (accessed 15.02.2024).

Yakovleva A.V. Cybersecurity and its legal regulation (foreign and Russian experience) // Socio-political sciences. 2021. Vol. 11. No. 4. – pp. 70-81.

Zheludkov M.A., A.M. Popov, M. M. Dubrovina. Features of countering cybercrime in Russia and foreign countries. // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2018. No.3 (46). – pp. 97-101. [Electronic resource] URL: https://cyberleninka.ru/article/n/osobennosti-protivodeystviya-kiberprestupnosti-v-rossii-i-zarubezhnyh-stranah (accessed 07.02.2024).

Автор туралы ақпарат:

*Кубанова Нургуль Байтоковна (корреспондент автор) – Қазақстан Республикасы ІІМ М. Есболатов атындағы Алматы академиясы PhD докторанты (Қазақстан, Алматы қ. *e-mail: nurgul_kubanova@mail.ru);*

Серикова Лаура Сериковна – І. Жансүгіров атындағы Жетісу университеті (Қазақстан, Талдықорған қ., e-mail: ss_laura@mail.ru).

Информация об авторе:

*Кубанова Нургуль Байтоковна (корреспондент автор) – PhD докторант Алматинской академии имени М. Есболатова МВД Республики Казахстан (Казахстан, г. Алматы, *e-mail: nurgul_kubanova@mail.ru);*

Серикова Лаура Сериковна – Жетысуский университет имени И.Жансугурова, Казакстан, г. Талдыкорган (Казахстан, г. Талдыкорган, e-mail: ss_laura@mail.ru).

Information about the author:

*Kubanova Nurgul Baytokovna (corresponding author) – PhD student at the Almaty Academy named after M. Esbolatova MIA RK (Kazakhstan, Almaty c., *e-mail: nurgul_kubanova@mail.ru)*

Serikova Laura Serikovna – Zhetysu University named after I. Zhansugurov (Kazakhstan, Taldy-Kurgan c., e-mail: nurgul_kubanova@mail.ru).

Тіркелген: 05.03.2024 ж.
Қабылданды: 10.12.2024 ж.