ӘОЖ 343.34
ҒТАМР 81.93.29

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ МЕН ШЕТ МЕМЛЕКЕТТЕРДІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚЫЛМЫСТЫҚ-ҚҰҚЫҚТЫҚ ҚОРҒАУ САЛАСЫНДАҒЫ ЗАҢНАМАЛЫҚ ТӘЖІРИБЕСІН САЛЫСТЫРМАЛЫ ТАЛДАУ

Багдат Тлектесовна Ауешова[1]
Заң ғылымдарының кандидаты, ҚР БҒМ қауымдастырылған профессоры, Ш.Есенов атындағы Каспий технологиялар және инжиниринг университетінің құқықтану кафедрасының меңгерушісі; Ақтау қ., Қазақстан Республикасы; e-mail: baueshova@mail.ru; ORCID iD: https://orcid.org/0000-0003-1449-9941; Researcher ID WOS:C-8118-2018; SCOPUS ID: 57205601320

Айгуль Айдарбаевна Утенова
Құқық магистрі, Ш.Есенов атындағы Каспий технологиялар және инжиниринг университетінің профессор ассистенті; Ақтау қ., Қазақстан Республикасы; e-mail: aygul.utenova@mail.ru; ORCID iD: https://orcid.org/0009-0005-2673-9000

Гулнар Қосшықызы Ізтұрғанова
Құқық магистрі, Ш.Есенов атындағы Каспий технологиялар және инжиниринг университетінің профессор ассистенті; Ақтау қ., Қазақстан Республикасы; e-mail: izturganova_gulnar@mail.ru; ORCID iD: https://orcid.org/0009-0007-0170-5079

Аннотация. *Ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғау тақырыбын зерделеу жаңа технологиялардың пайда болуы, қоғамдық өмірдің әртүрлі салаларында, оның ішінде мемлекеттік қызметтер көрсету саласында цифрландыру жетістіктерін енгізу тұрғысынан ұлттық қылмыстық заңнаманы дамыту мен жетілдірудің кейбір аспектілерін қарауға бағытталған. Елдің ұлттық қауіпсіздігінің құрамдас бөлігі ретінде ақпараттық қауіпсіздікті қамтамасыз ету тек заңнамалық қана емес, сонымен қатар мемлекет органдары тарапынан құқық қолдану қызметін де қамтиды. Жұмыста зерттелетін зерттеу тақырыбы бойынша нормативтік-құқықтық актілер, сондай-ақ оларды жүзеге асыру тетіктері сипатталған. Ақпараттық қауіпсіздікті қамтамасыз ету объектісі ретіндегі «ақпарат» ұғымы мазмұнының мәні осы саладағы отандық, сондай-ақ шетелдік зерттеушілердің идеяларына сүйене отырып қарастырылады. Мақала авторлары қоғамдық қатынастардың зерттелетін саласында қабылданатын заңнамалық актілердің Қазақстан Конституциясында белгіленген азаматтардың құқықтары мен заңды мүдделеріне сәйкестігі қажеттілігін қолдайды. Осыған байланысты халықаралық құжаттарды олардың ақпараттық қауіпсіздікті қорғаудың негізгі терминологиясы мен тетіктерін белгілеу бөлігінде қарау өзекті болып табылады. ТМД-ға кіретін немесе Қазақстанмен заңнаманы дамытудың ортақ тарихи тәжірибесі бар мемлекеттердің тәжірибесі ерекше көрсетілген. Осыған байланысты заңнаманың тиісті ережелерін жеке тарауға немесе бөлімге бөлу немесе зерттелетін мәселені құқық бұзушылық құрамының саралауына байланысты әр түрлі тараулардың ережелері негізінде реттеу бөлігінде ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғау жөніндегі елдердің тәсілдерін бөліп көрсетуге болады. Әр түрлі мемлекеттердің заңнамалары терминологияны («Киберқылмыс», «Ақпараттық қауіпсіздікке қарсы қылмыстар» және т.б.) зерттелетін жұмыс тақырыбына қатысты ережелерді бұзғаны үшін жауапкершілікті анықтауда қолданады. Жұмыста ақпараттық қауіпсіздікті қорғаудың қолданыстағы тетігінің оны бұзуға мүмкіндік беретін технологияларға сәйкестігі жөніндегі қызметті жүзеге асыру қажеттігін куәландыратын статистикалық материал келтірілген.*

Түйінді сөздер: *ақпараттық қауіпсіздік, қылмыстық заңнама, ақпарат, ақпараттық технологияларды дамыту, қылмыс, цифрландыру.*

[1] *Хат-хабарларға арналған автор*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬНОГО ОПЫТА РЕСПУБЛИКИ КАЗАХСТАН И ИНОСТРАННЫХ ГОСУДАРСТВ В ОБЛАСТИ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ауешова Багдат Тлектесовна
Кандидат юридических наук, ассоциированный профессор (доцент) МОН РК, заведующая кафедрой Каспийского университета технологий и инжиниринга имени Ш. Есенова; г. Актау, Республика Казахстан; e-mail: baueshova@mail.ru; ORCID iD: https://orcid.org/0000-0003-1449-9941; Researcher ID WOS:C-8118-2018; SCOPUS ID: 57205601320

Утенова Айгуль Айдарбаевна
Магистр права, ассистент профессора Каспийского университета технологий и инжиниринга имени Ш. Есенова; г. Актау, Республика Казахстан; e-mail: aygul.utenova@mail.ru; ORCID iD: https://orcid.org/0009-0005-2673-9000

Ізтұрғанова Гулнар Қосшықызы
Магистр права, ассистент профессора Каспийского университета технологий и инжиниринга имени Ш. Есенова; г. Актау, Республика Казахстан; e-mail: izturganova_gulnar@mail.ru; ORCID iD: https://orcid.org/0009-0007-0170-5079

Аннотация. *Изучение темы уголовно-правовой охраны информационной безопасности направлено на рассмотрение некоторых аспектов развития и совершенствования национального уголовного законодательства в свете появления новых технологий, внедрения достижений цифровизации в различных сферах общественной жизни, в том числе в области предоставления государственных услуг. Обеспечение информационной безопасности как составляющего компонента национальной безопасности страны включает в себя не только законодательную, но и правоприменительную деятельность со стороны органов государства. В работе описаны нормативно-правовые акты по изучаемой теме исследования, а также механизмы для их реализации. Сущность содержания понятия «информация» как объекта обеспечения информационной безопасности рассмотрена, опираясь на идеи отечественных, а также зарубежных исследователей в данной области. Авторы статьи поддерживают необходимость соответствия принимаемых законодательных актов в изучаемой сфере общественных отношений с правами и законными интересами граждан, установленных в Конституции Казахстана. В этой связи актуально рассмотрение международных документов в части установления ими основной терминологии и механизмов защиты информационной безопасности. Особо показателен опыт государств, входящих в СНГ или имеющих общий исторический опыт развития законодательства с Казахстаном. В этой связи можно выделить подходы стран по уголовно-правовой охране информационной безопасности в части выделения соответствующих положений законодательства в отдельную главу или раздел либо регулирования изучаемого вопроса на основе положений различных глав в зависимости от квалификации состава правонарушения. Законодательства различных государств используют терминологию («Киберпреступность», «Преступления против информационной безопасности» и т.д.) в определении ответственности за нарушение положений относительно исследуемой темы работы. В работе приведен статистический материал, свидетельствующий о необходимости осуществления деятельности по соответствию действующего механизма защиты информационной безопасности технологиям, позволяющим ее нарушать.*

Ключевые слова: *информационная безопасность, уголовное законодательство, информация, развитие информационных технологий, преступление, цифровизация.*

COMPARATIVE ANALYSIS OF THE LEGISLATIVE EXPERIENCE OF THE REPUBLIC OF KAZAKHSTAN AND FOREIGN COUNTRIES IN THE FIELD OF CRIMINAL LAW PROTECTION OF INFORMATION SECURITY

Aueshova Bagdat Tlektesovna
Candidate of Legal Sciences, Associate Professor of Ministry of Education and Science of the Republic of Kazakhstan, Head of the Department at Caspian University of Technology and Engineering named after Sh. Yessenov; Aktau c., Republic of Kazakhstan; e-mail: baueshova@mail.ru; ORCID iD: https://orcid.org/0000-0003-1449-9941; Researcher ID WOS:C-8118-2018; SCOPUS ID: 57205601320

Utenova Aigul Aidarbaevna
Master of Law, Assistant Professor at Caspian University of Technology and Engineering named after Sh. Yessenov; Aktau c., Republic of Kazakhstan; e-mail: aygul.utenova@mail.ru; ORCID iD: https://orcid.org/0009-0005-2673-9000

Izturganova Gulnar Kosshykyzy
Master of Law, Assistant Professor at Caspian University of Technology and Engineering named after Sh. Yessenov; Aktau c., Republic of Kazakhstan; e-mail: izturganova_gulnar@mail.ru; ORCID iD: https://orcid.org/0009-0007-0170-5079

Abstract. *The study of the topic of criminal law protection of information security is aimed at considering some aspects of the development and improvement of national criminal legislation in the light of the emergence of new technologies, the introduction of digitalization achievements in various spheres of public life, including in the field of public services. Ensuring information security as an integral component of the national security of the country includes not only legislative, but also law enforcement activities on the part of state bodies. The paper describes the normative legal acts on the studied research topic, as well as the mechanisms for their implementation. The essence of the content of the concept of "information" as an object of information security is considered, based on the ideas of domestic as well as foreign researchers in this field. The authors of the article support the need for compliance of the adopted legislative acts in the studied sphere of public relations with the rights and legitimate interests of citizens established in the Constitution of Kazakhstan. In this regard, it is important to consider international documents in terms of establishing their basic terminology and mechanisms for protecting information security. The experience of the CIS member states or those with common historical experience in the development of legislation with Kazakhstan is particularly indicative. In this regard, it is possible to distinguish the approaches of countries on the criminal law protection of information security in terms of allocating the relevant provisions of legislation into a separate chapter or section or regulating the issue under study based on the provisions of various chapters, depending on the qualification of the offense. The legislation of various states uses terminology ("Cybercrime", "Crimes against information security", etc.) in determining responsibility for violating the provisions regarding the topic of study. The paper provides statistical material indicating the need to carry out activities to ensure that the current information security protection mechanism complies with technologies that allow it to be violated.*

Keywords: *information security, criminal law, information, information technology development, crime, digitalization.*

DOI: 10.52026/2788-5291_2025_80_1_135

Кіріспе

Ақпараттық технологияларды, желілерді тарату және оларды жедел жетілдіру ақпараттық қауіпсіздікті қамтамасыз етуге ерекше өзектілік береді. Бұл ретте осы құқықтық қатынастардың мәні - ақпарат және ақпараттық технологияларда заңсыз әрекеттерді жүзеге асыру құралына айналды[1]. Сондықтан Қазақстан Республикасының Қылмыстық кодексінде ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтарға қатысты құқықтық қатынастарды реттеу жеке 7-тарауды бөлу арқылы іске асырылады. Дегенмен, интернет ақпарат

алудың негізгі көзі және құралы болып табылатын жаңа техникалық шешімдердің пайда болуы заңнаманы іске асыру мәселелерінің артуына әкеледі. Бұл заң шығарушы тарапынан белгілі бір шешімдерді талап етеді. Осыған байланысты ақпараттық қауіпсіздікті қылмыстық-құқықтық қамтамасыз ету ақпараттық саланың дамуын білдіруге және азаматтар, қоғам үшін мүмкін болатын жағымсыз салдарға уақтылы жауап беруге тиіс. Ақпараттық қауіпсіздікті қорғауға қатысты тиімді қызмет заңнаманың өзгермелі қоғамдық қатынастарға тұрақты өзгеруі, қолданыстағы құқық нормаларының тиімділігін арттыру және өзге елдермен өзара іс-қимыл негізінде жүзеге асырылады. Атап айтқанда, жеке өмірге қол сұғылмаушылық және жеке деректер туралы ақпарат құқығын қылмыстық-құқықтық қорғаудың тиімділігі, бұл шектеулі жария ету туралы ақпаратқа қатысты, 20 ғасырдың ортасынан бастап пайда болды. Бұл дербес деректерді қорғау қажеттілігін түсінумен және соның салдарынан жеке өмірге қол сұғылмаушылық құқығын белгілейтін халықаралық құжаттарды қабылдаумен байланысты болды. Сонымен қатар, бұл өзгерістер ақпараттық технологиялардың дамуына байланысты болды. Бұл ретте заңнама кибершабуылдар үшін жауапкершілікке қатысты мәселелер күтілетін режимде тұр[2], бірақ мұндай термин заңнамада қолданылмаса да, қылмыстық кодексте компьютерге, ұялы телефонға және басқа да байланыс құралдарына арналған вирустық бағдарламалардың таралуы анықталған, ал кодтық вариациялардың, жеке парольдердің заңсыз айналымына қатысты құқықтық қатынастар, жеке ақпаратты заңсыз өңдеу әлі заңнамалық тұрғыдан бекітілмеген. Ақпараттық қауіпсіздік пен заңнамамен қорғалатын ақпаратты қорғауға қарсы емес, ақпараттандыру және байланыс саласындағы қылмыстар ретінде бір-бірімен біріккен заңнамалық ережелердің болуы, Л.В. Головконың пікірінше, зерттелетін салада заңнамалық нормаларды үнемі жетілдіруді талап ететін табиғи процесс болып табылатын «қылмыстық заң нормаларының инфляциясының» көрінуіне себеп болады [2].

Материалдар мен әдістер

Жұмыста отандық және шетелдік ғалымдардың ақпараттық қауіпсіздік институтының мазмұнын қарау саласындағы еңбектері пайдаланылды. Сонымен қатар, қарастырылып отырған елдердің заңнамаларынан, халықаралық құжаттардан, сондай-ақ зерттеліп жатқан салада Қазақстан Республикасының аумағында тіркелген құқық бұзушылықтар бойынша статистикалық материалдардан ережелер келтірілген.

Мақаланың тақырыбын қарастыруда зерттеудің негізгі әдістері жалпы ғылыми, ресми-құқықтық, талдау және синтез, сондай-ақ салыстырмалы-құқықтық әдіс орын алды. Материалдарды зерделеу нәтижесінде ақпараттық қауіпсіздіктің бұзылуына жол бермеу және мемлекет азаматтарының жеке өміріне қол сұғылмаушылықты қорғау үшін ТМД мен шет елдердің заңнамалық тәжірибесін пайдалану қажет екендігі анықталды.

Бұл жұмыстың мақсаты ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғауды заңнамалық реттеу мәселесінде шет мемлекеттердің әртүрлі тәсілдерін зерделеу, тиісті ережелерді талдау және оны жетілдіру бойынша қылмыстық заңнамаға ұсыныстар енгізу мүмкіндігін қарастыру болып табылады.

Талқылау

«Ақпараттық қауіпсіздік» ұғымына қатысты оның анықтамасы «Ұлттық қауіпсіздік туралы» Қазақстан Республикасының Заңында белгіленген[3]. Ол бүкіл ақпараттық саланың және азаматтық, қоғамдық, мемлекеттік құқықтар мен мүдделердің қоршаған әлемнің белгілі бір қауіптерінен ажыратуға және тұрақты даму мен жетілдіруді қамтамасыз етуге мүмкіндік беретін ерекше жағдайын білдіреді. Технологияны дамытудың азаматтық қоғам мен әлемдік қоғамдастық үшін жағымсыз жақтары болуы мүмкін [3, с. 27]. Бұл киберқауіпсіздікті ұлттық қауіпсіздік саласына енгізуді негізді етеді. Қазіргі уақытта киберқылмыс өткен жылдармен салыстырғанда ең ауқымды қауіптердің біріне айналуда. Осыған байланысты ақпараттық қақтығыстардың пайда болу мүмкіндігі әлемде бұрыннан бар қарулы қақтығыстар аясында нақты болады.

Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету мақсатында мемлекетте киберқауіпсіздік тұжырымдамасы немесе «Қазақстанның киберқауіпсіздігі» немесе

---

[2] *210 бап. Қазақстан Республикасының Қылмыстық кодексі. Қазақстан Республикасының кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ // https://adilet.zan.kz/kaz/docs/K1400000226 (жүгінген күні 25.12.2023).*

[3] *Қазақстан Республикасының ұлттық қауіпсіздік туралы. Қазақстан Республикасының 2012 жылғы 6 қаңтардағы Заңы № 527-IV Заңы // https://adilet.zan.kz/kaz/docs/Z1200000527 (жүгінген күні 12.12.2023).*

«Қазақстанның киберқалқаны» әзірленді[4]. Бұл құжат электрондық нысаны бар немесе электрондық ақпараттық ресурстар мен жүйелерде қамтылған ақпаратты қорғауды қамтамасыз етуге бағытталған. Мазмұны бойынша киберқауіпсіздік ақпараттандыру саласында іске асырылатын ақпараттық қауіпсіздік түрі ретінде айқындалады. Бұл ретте ақпараттық қауіпсіздік үшін тұтастай алғанда іргелі компоненттер белгіленді: оның объектісінің, ақпараттың тұтастығы, қолжетімділігі, сондай-ақ құпиялылығы. Соңғы компонентті сақтамау ақпаратқа заңсыз қол жеткізу ретінде анықталады. Ақпараттың тұтастығы тұрғысынан маңызды ақпараттық объектілерге, механизмдерге қатысты ерекше сипатқа ие болатын бастапқы, нақты нысанды сақтау қажет. Оларға қызметі өңір, мемлекет азаматтарына қызмет көрсететін ақпараттық жүйелер, құралдар, ресурстар болып табылатын стратегиялық маңызы бар объектілер жатады және олардың жұмысын тоқтату не жұмыстағы өзге де іркілістер халықтың мемлекеттік қызметтерді алу мүмкіндігін жоғалтуына әкеп соғады. Бұл жүйелер қазіргі уақытта банктер мен өзге де қаржы ұйымдарының, авиацияның, денсаулық сақтау объектілерінің, коммуналдық ұйымдардың және т. б. қызметтер саласында қызметтер көрсету саласын жетілдіруге бағытталған.

Компьютерлік жүйелер саласындағы ақпараттық қауіпсіздікті қорғауды қамтамасыз ету бөлігінде шешімдердің бірі ақпарат қауіпсіздігін қорғау жөніндегі ережелерді сақтамаудың алдын алу үшін зерттелетін саладағы қауіптерге мониторинг жүргізетін, сондай-ақ жылдам шешімдер қабылдауда және жасалған заңсыз әрекеттің теріс нәтижелерін жою жөніндегі іс-қимылдарды іске асыруда құзыретті жедел орталықтарды қалыптастыру болып айқындалды [4]. Компьютерлік инциденттерге әрекет ету ұлттық қызметінің (KZ-CERT) жұмысына назар аудару қажет: ол ақпараттық қауіпсіздіктің жай-күйі және оны бұзудың ықтимал қауіптері туралы ақпаратты талдауға, оның негізінде мемлекеттік органдарға талдау беріледі, сондай-ақ зерттелетін саладағы қызметті жетілдіру жөнінде ұсыныстар дайындауға бағытталған. Бұл ретте аталған қызмет мемлекеттік басқару органдарының барлық ақпараттық жүйесіне мониторингті жүзеге асырады. Бұл функция «Ақпараттандыру туралы» Заңда[5] бекітілген және әртүрлі мемлекеттік серверлердің жұмысына заңсыз қол сұғушылықтардың көбеюіне қатысты.

Ақпараттық қауіпсіздік институтын құқықтық реттеуді қарастыра отырып, іске асыру және қорғау тетігі туралы түсінік беретін бірыңғай әмбебап заңнамалық актінің болуы туралы айтуға болмайды. Қайнар көздер ретінде Қылмыстық кодекстің ережелері, Әкімшілік құқық бұзушылық туралы Кодекс, «Дербес деректер және оларды қорғау туралы»[6], «Ақпаратқа қол жеткізу туралы» Заң[7] және т. б. Бұл нормативтік актілер зерттелетін институттың жекелеген аспектілерін қарастырады. Бұл ретте ақпараттық қауіпсіздік нысанасын құрайтын объектілердің белгілі бір техникалық ерекшеліктерінің болуына байланысты мамандардың, атап айтқанда ақпараттық-коммуникациялық техникалық құралдарды қолдануға қатысты түсіндірмелері қажет. Бұл ерекшелік ақпараттық қауіпсіздік пен ақпараттық-коммуникациялық технологияларды қорғау саласындағы бірыңғай талаптарды бекіткен Қазақстан Республикасы Үкіметінің қаулысын қабылдау тұрғысынан өзекті болып табылады[8]. Бұл компьютерлік технологиядағы қауіпсіздікке қатысты негізгі стандарттар.

Ақпараттық жүйе, ресурстар, технологиялар сияқты ақпараттық қауіпсіздікті қамтамасыз етуге байланысты ұғымдарды қарастыра отырып ақпараттық-коммуникациялық желі, электрондық тасымалдаушылар және басқалар, олардың мазмұны «Ақпараттандыру

---

[4] *Киберқауіпсіздік тұжырымдамасын («Қазақстанның киберқалқаны») бекіту туралы. Қазақстан Республикасының Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы // https://adilet.zan.kz/kaz/docs/P1700000407 (жүгінген күні 22.12.2023).*

[5] *Ақпараттандыру туралы. Қазақстан Республикасының Заңы 2015 жылғы 24 қарашадағы № 418-V ҚРЗ // https://adilet.zan.kz/kaz/docs/Z1500000418 (жүгінген күні 18.01.2024).*

[6] *Дербес деректер және оларды қорғау туралы. Қазақстан Республикасының Заңы 2013 жылғы 21 мамырдағы № 94-V Заңы // https://adilet.zan.kz/kaz/docs/Z1500000418 (жүгінген күні 18.01.2024).*

[7] *Ақпаратқа қол жеткізу туралы. Қазақстан Республикасының Заңы 2015 жылғы 16 қарашадағы № 401-V ҚРЗ // https://adilet.zan.kz/rus/docs/Z1500000401 (жүгінген күні 18.01.2024).*

[8] *Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы. Қазақстан республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы //https://adilet.zan.kz/kaz/docs/P1600000832 (жүгінген күні 24.01.2024).*

туралы» Заңда айқындалады. Қылмыстық кодекс ақпараттық технологияларға қатысты заңсыз әрекеттерді қарау кезінде осы институттарды пайдаланады. Бұл ретте осы институттардың қарастырылып отырған құқықтық қатынастарды реттеудегі орны толық анық емес: заңсыз қол сұғушылықтарды іске асырудың мәні немесе құралы, атап айтқанда, ақпаратқа заңсыз қол жеткізу, оны жою, иемдену, мәжбүрлеу электрондық өнімді беру, тарату және т. б.[9] Заңсыз әрекеттерді жүзеге асыру кезінде қолданылатын ақпараттық технологиялар қол сұғу құралы ретінде олар бұзушылыққа ұшырайды, яғни олар әрекет объектісінің қасиеттерін алады. Осыған байланысты бұл технологияларды қорғаудың әртүрлі тәсілдері бұзылуы мүмкін, желінің өзі немесе оларды қолданатындарға зиян тигізеді. Сондықтан Қылмыстық кодекстің 205, 208, 209, 211, 212, 213 баптарын қарастыру барысында, белгілі бір адамдардың ақпарат алу құқығы қылмыстық әрекеттің объектісіне айналады.

Ақпараттың өзі ұлттық заңнамада азаматтық құқықтарының дербес объектісі ретінде белгіленбейтіні атап өткен жөн[10]. Бұл ретте ақпарат иесі оның құндылығына қарай оған қол жеткізуді шектейтін қызметтік, коммерциялық ақпарат азаматтық заңнама нормаларымен қорғалуға тиіс[11]. Осыған байланысты заң шығарушы ерекше режим мен құқықтық қорғау шаралары қолданылатын ақпарат түрін анықтады. Кодексте анықтама берілмеген, «ақпарат иесі» термині қолданылады. Сондай-ақ, иесінің ережесін, оның құқықтарының мазмұнын белгілейтін құжат жоқ. Ресей Федерациясының заңнамасында ақпарат иесі-белгілі бір ақпаратқа қол жеткізуді шектеу, рұқсат беру мүмкіндігі бар заңды түрде жасаушы немесе сатып алушы [5, с. 105]. Сонымен бірге, осы тұжырымдаманы еңгізе отырып, оған меншік құқығын тану қажет, бұл тек бір меншік иесіне тиесілі болуды талап етеді. Ақпарат белгіленбеген адамдар санына таралуымен сипатталады. Сондықтан, оған қатысты меншік мәселелерін анықтай отырып, заңнама оларды ақпарат тасымалдаушыларына жүгінеді. Сондықтан қылмыстық заңнаманың баптарында құқықтарды бұзу бөлігінде олардың кімге қатысты бұзылғаны, сондай-ақ ақпараттық-коммуникациялық желі арқылы өтетін ақпараттың тиесілігі белгісіз болады.

Осыған байланысты шетелдік зерттеушілер тарапынан ақпарат ұғымына көзқарасы қызығушылық тудырады. Атап айтқанда, О. Керр ақпарат алу оны бақылау екенін айтады [6]. Бұл жағдайда ол жеке немесе басқа түрге қарамастан қорғалуы керек, өйткені оған қол жеткізу үшін электрондық поштаны ашу, сілтеме арқылы өту, сайтқа кіру және т.б. жеткілікті. Қол жеткізу құралы компьютер немесе ноутбук болуы міндетті емес. Америка Құрама Штаттарында ақпараттық қауіпсіздік бойынша қылмыстық жауапкершілікті белгілейтін заң 1977 жылы қабылданды. Осыған сүйене отырып, компьютерлік технологияның дамуымен оларды қолдану туралы алаяқтық туралы заң шығарылды.

М. Нилесқа сәйкес ақпараттық қауіпсіздік ақпарат пен жүйелерді құпиялылықты, тұтастықты және қолжетімділікті қамтамасыз ету мақсатында рұқсатсыз қол жеткізуден, пайдаланудан, ашудан, бұзудан, өзгертуден немесе жоюдан қорғау ретінде анықталады[7]. Ақпараттық қауіпсіздікті бақылау шараларын мұқият енгізу ұйымның ақпараттық активтерін, сондай-ақ оның беделін, құқықтық жағдайын, қызметкерлерін және басқа да материалдық немесе материалдық емес активтерін қорғау үшін өте маңызды. Бұл ретте Д.Каннаттачи ақпараттық қауіпсіздікті қорғау жөніндегі заңнаманың шамадан тыс дамуы азаматтардың жеке өміріне, дербес деректеріне қол сұғылмаушылық бөлігінде құқықтарының бұзылуына әкелуі мүмкін деп санайды [8]. Жоғарыда аталған тәсілдердің әрқайсысы орын алады және біз соңғысын ең маңызды деп санаймыз, себебі осы саладағы заңнаманы дамыту адамның конституциялық құқықтарын бұзбауы керек. Осыған байланысты жақын маңдағы мемлекеттер мен өзге де шет елдердің ақпараттық қауіпсіздікті қылмыстық-құқықтық қорғауға қатысты заңнамалық тәжірибесіне назар аудару қажет.

ТМД елдеріне қатысты 2001 жылы олардың арасында зерттелетін саладағы құжат-

---

[9] 7 тарау. Қазақстан Республикасының Қылмыстық кодексі. Қазақстан Республикасының кодексі 2014 жылғы 3 шілдедегі № 226-V ҚРЗ // https://adilet.zan.kz/kaz/docs/K1400000226 (жүгінген күні 25.12.2023).

[10] 115 бап. Қазақстан Республикасының Азаматтық кодексі. Қазақстан Республикасының кодексі 1994 жылғы 27 желтоқсандағы № 268-XIII ҚРЗ // https://adilet.zan.kz/kaz/docs/K940001000_ (жүгінген күні 25.12.2023).

[11] 126 бап. Қазақстан Республикасының Азаматтық кодексі. Қазақстан Республикасының кодексі 1994 жылғы 27 желтоқсандағы № 268-XIII ҚРЗ // https://adilet.zan.kz/kaz/docs/K940001000_ (жүгінген күні 25.12.2023).

тарға қол қойылды: «Киберқылмыс туралы» Конвенция[12], қылмыстарға қатысты компьютерлік ақпаратпен өзара іс-қимыл туралы келісім[13]. Бұл құжаттардың ерекшелігі - негізгі институттардың мазмұнын анықтау. Компьютерлік деректер ұғымы Конвенцияда беру және қабылдау мүмкіндігімен байланыс құралы болып табылатын ақпарат ретінде қамтылған. Конвенция оларды компьютерлік жүйемен өңдеуге болатын ақпарат, фактілер, берудің басқа түрлері ретінде анықтайды. Осылайша, Конвенциядағы анықтама адам анықтай алмайтын бағдарламалық жасақтаманы қамтымайды, бірақ ол компьютер жүйесінің қызметі үшін қажет. Оған кез-келген қол сұғушылық азаматтар үшін ауыр зардаптарға әкеледі, сондықтан Конвенцияда белгіленген анықтама толық болып табылады. Сонымен қатар, Келісім компьютерлік ақпаратқа қатысты қылмыстың мазмұнын компьютердегі ақпарат объектісі болып табылатын заңсыз қол сұғушылық ретінде анықтайды. Айта кету керек, бұл ақпарат қол сұғудың құралы бола алады.

Ақпараттық қауіпсіздік саласындағы қылмыстардың құрамына қатысты бұл құжаттар бір атауды көрсетсе де, оған әртүрлі мазмұнын белгілейді. Атап айтқанда, Келісім ақпаратқа заңсыз қол жеткізуді компьютерге, ақпараттық жүйелерге, желілерге немесе ақпараттың өзіне қатысты жою, бұзу, бұғаттау және т.б. түрінде тиісті салдары бар қылмыстық жазаланатын әрекет ретінде анықтайды. Конвенция оларға заңсыз қол жеткізуді өзге біліктілік белгілерін белгілемей, заңсыз қол сұғушылық ретінде айқындайды[9]. Осы құжаттарда ақпараттық қауіпсіздікке қол сұғатын іс-әрекеттердің мазмұнына қатысты осындай сәйкессіздіктер байқалады; қолданылатын терминологияның мазмұнына көзқарастар және бұл ТМД-ға қатысушы мемлекеттерге ұлттық заңнаманы қолдану мен енгізуде қиындықтар туғызады. Сондықтан мұндай мәселелерді халықаралық-құқықтық әдістермен, атап айтқанда, елдер арасында консультациялық іс-шаралар өткізу арқылы шешу қажет.

ТМД-ға кіретін елдер үшін Модельдік Қылмыстық кодексте[14] зерттелетін тақырыпқа қатысты «Ақпараттық қауіпсіздікке қарсы қылмыстар» атты жеке тарау бар, ол аттас бөлімге кіреді. Онда ақпаратқа заңсыз қол жеткізуге, оны модификациялауға, иемденуге, вирустық қамтамасыз етуді өндіруге, қолдануға және таратуға, ақпаратқа заңсыз қол жеткізуге арналған құралдарға, сондай-ақ ақпараттық желіні пайдалану жөніндегі ережелерді сақтамауға қатысты жеті бап айқындалған. Ақпараттық қауіпсіздік саласындағы қылмыстық жауапкершілікті реттеудің осындай құрылымын Беларусь Республикасы[15] мен Тәжікстан[16] қабылдады, олардың қылмыстық заңнамасында сол атаумен тарау мен бөлім бар. Зерттелетін тақырып бойынша мәселелерді реттеу бойынша Өзбекстан Республикасының Қылмыстық кодексінде[17] жеке тарауда қарастырылған, онда қол сұғушылық ақпараттық технологиялар саласындағы қылмыс деп аталады. Қылмыстың нақты атауын компьютерлік ақпарат саласындағы заңсыз әрекеттерге қатысты жеке тарау бар Ресей Федерациясының[18], Түрікменстанның[19], Қырғыз Республикасының[20], Армения Республикасының[21]

---

[12] *«Киберқылмыс туралы» Конвенция – Convemtion on Cybercrime. 2001 жылдың 23 қарашада Будапештте қабылданды // https://kk.mgwiki.top/wiki/Convention_on_Cybercrime (жүгінген күні 02.01.2024).*

[13] *ТМД қатысушы мемлекеттердің ақпараттық технрологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы. Қазақстан Республикасының Заңы 2019 жылғы 9 желтоқсандағы № 277-VI ҚРЗ // https://adilet.zan.kz/rus/docs/Z1900000277 (жүгінген күні 18.01.2024).*

[14] *Модельный Уголовный кодекс для государств Содружества Независимых Государств. Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств. Санкт-Петербург, 17 февраля 1996 года*

[15] *12-бөлім, 31-тарау. Уголовный кодекс Республики Беларусь от 9 июля 1999 года № 275-З //https://online.zakon.kz/Document/?doc_id=30414984 (дата обращения: 20.01.2024).*

[16] *11-бөлім, 28-тарау. Уголовный кодекс Республики Таджикистан от 21 мая 1998 года № 574// https://online.zakon.kz/Document/?doc_id=30397325 (дата обращения: 20.01.2024).*

[17] *20-1--тарау. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII// https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 20.01.2024).*

[18] *9-бөлім, 28-тарау. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ // https://online.zakon.kz/Document/?doc_id=30397073 (дата обращения: 20.01.2024).*

[19] *23-бөлім, 33-тарау. Уголовный кодекс Туркменистана от 12 июня 1997 года № 222-I// https://online.zakon.kz/Document/?doc_id=31295286 (дата обращения: 20.01.2024).*

[20] *29-бөлім, 227-228-1 баптар. Уголовный кодекс Кыргызской Республики от 28 октября 2021 года № 127// https://online.zakon.kz/Document/?doc_id=36675065 (дата обращения: 20.01.2024).*

[21] *9-бөлім, 24-тарау. Уголовный кодекс Республики Армения от 18 апреля 2003 года// https://wipolex-res.wipo.int/*

қылмыстық заңнамасы анықтайды. Грузияның Қылмыстық кодексі[22] компьютерлік қылмыстар үшін жауапкершілікті анықтауда ақпарат түрін нақтылайды. Бұл Әзірбайжан Республикасы Қылмыстық кодексінің[23] «Киберқылмыс» тарауының атауына ұқсас.

Эстония, Латвия сияқты елдердің қылмыстық заңнамасы ақпараттық қауіпсіздікке қарсы қылмыстарды жеке тарауға бөлмейді, бірақ басқа тараулар мен бөлімдер аясында қарастырылады. Атап айтқанда, Латвия Республикасының Қылмыстық кодексі[24] ақпаратты меншік құқығының объектісі ретінде анықтайды, сондықтан «Меншік саласындағы қылмыстар» тарауында, және «Қоғамдық қауіпсіздікке қарсы қылмыстар» тарауында қарастырады [10, с. 52]. Эстония заңнамасы осындай көзқарасты ұстанады, қарастырылып отырған құқықтық қатынастарды мүліктік сипатқа ие деп анықтайды[25].

Сонымен қатар, интернет пен компьютерлік қылмысқа қарсы бағытталған алғашқы халықаралық құжат компьютерлік қылмыстар туралы Конвенция болды[26]. Бұл құжаттың мақсаты іс жүргізу іс-шараларын жүргізу арқылы мемлекеттер арасындағы тиімді өзара іс-қимылды қалыптастыру, деректерді қорғауды құқықтық қамтамасыз етуге, жедел іс-шараларды жүзеге асыруға қатысты, сондай-ақ ақпараттық технологияларды қолдана отырып, заңсыз қол сұғушылықтан, оның ішінде шабуылдардан, алаяқтықтан, порнографияны таратудан, зияткерлік меншік және зияткерлік меншік саласындағы заңнаманы сақтамаудан қорғауға қатысты ережелерді елдердің ұлттық заңнамаларына енгізу болып табылады.

Нәтижелер

Жоғарыда айтылғандарға сүйене отырып, елдердің заңнамалық тәжірибесі қолданылатын терминологиясының қазіргі жағдайға сәйкессіздігін, демек, заңнаманың ережелерін іске асырудың төмен тиімділігін көрсететінін атап өткен жөн. «Компьютерлік қылмыс» институты ақпараттық жүйенің техникасына, құрамдас бөлігіне қатынасын айқындайды. Бұл ақпарат айналымы саласында, оның ішінде ұялы телефон, спутниктік және деректерді берудің өзге де жүйелері және т. б. қолданылатын түрлі технологиялар түрлерімен орынсыз болып табылады.

Әлеуметтік қатынастардың зерттелетін саласындағы технологиялардың күрделілігі әртүрлі құқық бұзушылықтардың пайда болуының алғышарттарын жасайды[11]. Бұл ретте оларды ұлттық заңнаманың ережелерімен қамтымау мүмкіндігі қалады.

Кесте 1. Ақпараттық қауіпсіздік саласындағы құқық бұзушылықтар саны

№	Позиция атауы	2022 жыл	2023 жыл	% ұлғаю (+) кему (-)
1	Барлық құқық бұзушылықтар	8,9 мың	12,9 мың	+ 46,3 %
2	Вирустық бағдарламаларды жасау және тарату	5,9 мың	8,5 мың	+ 41,8 %
3	Кибершабуылдарды жүзеге асыру (ботнеттер)	1,6 мың	2,4 мың	+ 53,8 %
4	Әлеуметтік медиа сілтемелерін тарату арқылы алаяқтық (фишинг)	461	379	- 18 %
5	Деректерге заңсыз қол жеткізу және өзгерту	41	245	+ 6 есе

edocs/lexdocs/laws/ru/am/am012ru.pdf (дата обращения: 20.01.2024).

[22] *35-тарау Уголовный кодекс Грузии от 22 июля 1999 года// https://www.matsne.gov.ge/ru/document/view/16426 (дата обращения: 20.01.2024).*

[23] *30-тарау. Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 года № 787-IQ// https://online.zakon.kz/Document/?doc_id=30420353 (дата обращения: 21.01.2024).*

[24] *20-тарау. Уголовный кодекс Латвийской Республики от 30 декабря 1999 года № 787-IQ// http://www.alex-lawyer.lv/ugolovnijzakonlatviirus.pdf (дата обращения: 21.01.2024).*

[25] *14-тарау. Уголовный кодекс Эстонской Республики от 1 сентября 2002 года// https://constitutions.ru/?p=24972&ysclid=ls308s51pz906093362 (дата обращения: 20.01.2024).*

[26] *Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on cybercrime CETS № 185). Будапешт,23 ноября 2001 года// https://rm.coe.int/1680081580(дата обращения: 21.01.2024).*

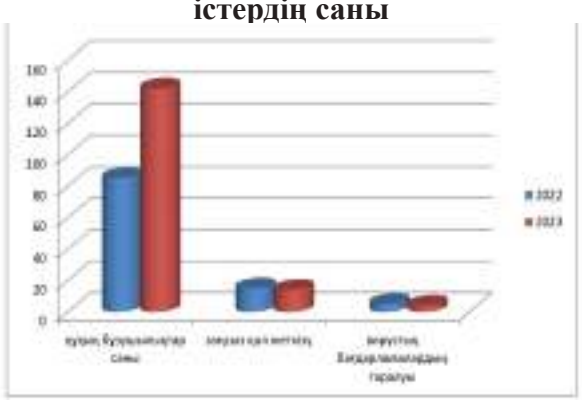
Ақпараттық қауіпсіздік саласындағы құқық бұзушылықтарды қарастыра отырып, жоғарыда аталған KZ-CERT қызметінің жұмысына назар аудару қажет. Ол жүргізген мониторингке сәйкес, Қазақстанда құқық бұзушылықтар саны артып келеді[27].

Кестеде зерттелетін қоғамдық қатынастар саласындағы бұзушылықтар жағдайларының көбеюі расталады, атап айтқанда вирустық бағдарламалардың таралу санының артуымен көрінеді. Қолданылған кибершабуылдар немесе ботнеттер саны 53,8 пайызға өсті. Әлеуметтік желілерде сілтемелерді 18 пайызға жіберу арқылы мүліктік сипаттағы заңсыз іс-әрекеттер санының азаюы аясында, деректерге заңсыз қол жеткізу бөлігінде ақпараттық қауіпсіздікті бұзу жағдайлары алты есе өсті.

Цифрлардың азаюына не ұлғаюына мемлекеттің ақпараттық кеңістігін қорғау тетігі сияқты цифрландырудың ықпалы мен дамуы да әсер етеді. «Қазақстанның киберқалқаны» сияқты техникалық және ұлттық қорғаныс жүйелері бар. Бұл мән-жайлар қорғау тетігінің тиімділігін немесе осы саладағы құқық бұзушылықтар санының азаюын белгілей алмайды.

Зерттелетін тақырып бойынша қылмыстық істерді сотқа дейінгі тергеп-тексерулердің бірыңғай тізілімінде тіркеу бөлігінде құқық бұзушылықтардың 15 пайызға артқаны байқалады. Бұл ретте негізгі саны заңсыз қол жеткізуге, деректерді өзгертуге келеді, олардың саны 7 пайызға азайды. Вирустық бағдарламалардың таралуы бөлігінде 2022 жылмен салыстырғанда құқық бұзушылықтар саны сақталуда.

Диаграмма 1. Тіркелген қылмыстық істердің саны

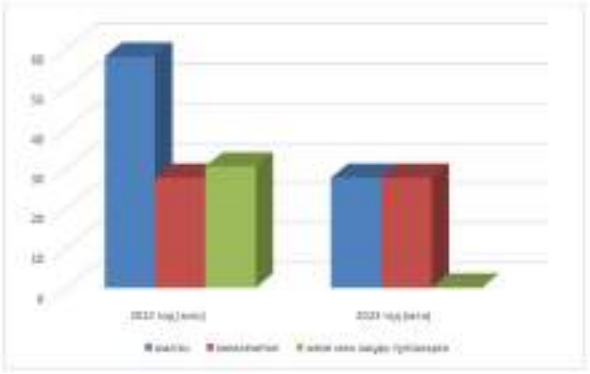


Осы санатың қылмыстық істерді сот органына жеткізу қиындығы - ол кінәлі адамды анықтау, дәлелдемелер базасын жинау қиындығы. Бұл ретте күдікті адам немесе «хакер» ақпараттық жүйеге ену, вирустық бағдарламаларды құру және тарату, деректерге заңсыз қол жеткізу және т.б. үшін білім мен дағдыларға ие. Бұл ретте қылмыстық жауапкершілікке тартылғандардың көпшілігі отыз-отыз тоғыз жастағы ер адамдар. Әйелдер мен кәмелетке толмағандар сирек кездеседі.

Ақпараттық қауіпсіздікке қарсы қылмыстар жасауға байланысты келтірілген материалдық залалға қатысты 2-диаграмма жәбірленуші қатысушыларды бөле отырып, соңғы екі жылдағы жалпы залалдың динамикасын көрсетеді. 2022 жылы мемлекетке материалдық залал осы құқықтық қатынастардың басқа қатысушыларына қарағанда жабылды.

Бұл ретте, осы статистикалық ақпарат Қазақстан Республикасының Қылмыстық кодексіне сәйкес ақпараттық қауіпсіздік саласындағы қылмыстардың жай-күйін көрсетеді. Бұл ретте ақпараттық кеңістікпен заңсыз әрекеттерге бағытталған, бірақ істердің басқа санаттары бойынша, көбіне меншікке қатысты сараланатын қылмыстар жасалады. Атап айтқанда, төлем карточкаларын қолдана отырып, банктік және қаржы мекемелерінің ақпараттық желілерін бұза отырып, интернеттегі алаяқтық әрекеттер және т. б.

Диаграмма 2. Материалдық залалдың мөлшері туралы ақпарат



Осылайша, ақпараттық технологиялардың ерекшелігі мен күрделі техникалық сипаттамаларының болуы, қылмыстық істердің осы санаты бойынша дәлелдемелер жинаудағы қиындықтар тіркеудің төмен көлеміне, сотқа жеткізудің негіздемесі болып табылады. Бұл ретте осы технологияларды жетілдіру қылмыстық заңнамада белгіленбеген қылмыстардың жаңа құрамдарының пайда болуына әкеп соғуы мүмкін, ол ақпараттық

[27] *В Казахстане растет число киберпреступлений// https://wfin.kz/publikatsii/kazakhstan-v-tsifrakh/91787-v-kazakhstane-rastjot-chislo-kiber-prestuplenij.html?ysclid=lupjetzha36877422 (дата обращения: 26.01.2024).*

қауіпсіздікке заңсыз қол сұғудың неғұрлым күрделі жаңа нысандарын қалыптастыруға алып келеді. Сондықтан ақпаратты өңдеу құралдарының техникалық ерекшеліктері мен мазмұнын егжей-тегжейлі түсіндіретін ұғымдардың нақты анықтамаларын қалыптастыру қажет. Бұл өзгеріп отырған қоғамдық қатынастарға уақтылы ден қоюға мүмкіндік береді. Бұдан басқа, бұл құқық қорғау және өзге де мемлекеттік органдардың құқық қолдану тәжірибесін, атап айтқанда, жасалған іс-әрекеттердің біліктілігіне қатысты айтарлықтай жеңілдетеді; қателіктер, дәлсіздіктер жіберу мүмкіндігін азайтады.

Цифрландырудың өсуі, қоғамдық өмірдің әртүрлі маңызды салаларына цифрлық технологияларды енгізу құқықтық қатынастарға қатысушылардың өмір сүру жағдайларын жеңілдетіп қана қоймай, ақпаратты қорғау жөніндегі іс-шараларды жүзеге асыруды талап етеді. Ақпараттық қауіпсіздікті қорғау жүйесі тұрақты бақылауда және жетілдіруде болуға тиіс. Осы саладағы заңсыз қол сұғушылықтардың санын азайту үшін ақпараттық қауіпсіздікті қамтамасыз етудің құқықтық, техникалық, ұйымдастырушылық әдістерін кешенде пайдалану қажет. Технологиялық инновацияларды бір мезгілде енгізу, дамыту арқылы оларды қолдана отырып, заңсыз әрекеттер санының артуы байқалады. Бұл ретте зерттелетін салада білімі мен дағдылары бар қызметкерлердің кадрлық қамтамасыз етуі аз санды құрайды. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі шараларды жетілдіру мәселелері қазіргі уақытта өзекті болып табылады және болашақта күшейтілетін болады. Осы шараларды әзірлеу мен қабылдаудың мақсаты зерттелетін саладағы заңсыз әрекеттердің теріс нәтижелерін азайтуға, олардың пайда болуының алдын алуға жәрдемдесу болып табылады.

Қорытынды

Ақпараттық қауіпсіздікті қамтамасыз ету үшін үш міндет бойынша іс қимылдарды жүзеге асыру қажет деп санаймыз:

- зерттелетін салада мемлекеттік, өңірлік және халықаралық деңгейде заңнамалық негіз қалаушы ережелерді қалыптастыру;
- ақпараттық қауіпсіздік саласындағы қылмыстардың алдын алу тетігін жетілдіру;
- ақпараттық қауіпсіздік саласындағы құқық бұзушылықтарға қарсы іс-қимыл бойынша елдер арасындағы өзара іс-қимылды жүзеге асыру.

2023 жылы ТМД Парламентаралық Ассамблеясы «Киберқылмысқа қарсы іс-қимыл туралы» модельдік заң қабылдады. Ол осы саладағы негізгі ұғымдарды, соның ішінде киберқылмыс терминінің мазмұнын, осы тұжырымдамаға кіретін құқық бұзушылықтардың тізімін анықтады, сондай-ақ мемлекеттік биліктің барлық тармақтары органдарының өкілеттіктерін қарастырды. Бұдан басқа, онда аталған құқық бұзушылықтардың алдын алу, сондай-ақ мемлекет азаматтары, шетел азаматтары және азаматтығы жоқ адамдар болып табылатын адамдарды қылмыстық жауапкершілікке тарту жөніндегі шаралар қаралды. Осы субъектілердің ішінде кейбір белгіленген жағдайларда шетелдік заңды тұлғалар ерекшеленеді. Осы заңның негізінде ақпараттық қауіпсіздікті қамтамасыз етудің бірыңғай құқықтық тетігін әзірлеу қажет.

Зерттелетін проблеманың шешімдерінің бірі жұмыс істеп тұрған ақпарат алмасу, ақпараттық қауіпсіздікті қамтамасыз ету саласындағы құқық бұзушылықтарды оларды жасау тәсілдері бойынша, сәйкестендіру кодтары негізінде және т.б. есепке алатын мемлекетаралық ақпараттық банкті қалыптастыру болуы мүмкін. Осыған байланысты мемлекеттер жәрдемдесу туралы сұрау салулардың орындалу уақытына қатысты уағдаласуы қажет, өйткені мұндай әрекет ТМД-ға қатысушы мемлекеттердің 2018 жылғы Ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімнің ережелерінде көрсетілген[28]. Бұл процестің уақыт шеңбері белгіленбеген. Бұл ереже ақпараттық қауіпсіздікті бұзу фактісі пайда болған кезде бірден күдікті адам орналасқан мемлекетке ақпараттың барлық көлемін жіберуге мүмкіндік береді.

Ақпараттық қауіпсіздіктің бұзылуына қарсы іс-қимыл бөлігінде осы бұзушылықтарды тудыратын жағдайлар мен себептерді анықтау және жою зерттелетін мәселенің шешімі бола алады. Осыған байланысты келесі әрекеттерді анықтауға болады:

- мемлекеттің ақпараттық ресурстарына шабуылдар мониторингі;
- ақпараттық желілерде киберқылмыс

[28] *ТМД қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстармен күрестегі ынтымақтастығы туралы келісімді ратификациялау туралы. Қазақстан Республикасының Заңы 2019 жылғы 9 желтоқсандағы № 277-VI ҚРЗ // https://adilet.zan.kz/kaz/docs/Z1900000277 (жүгінген күні 28.09.2024).*

белгілері бар әртүрлі деректер мен материалдардың таралуын анықтау және жою;

- мемлекеттің ақпараттық ресурстарында дербес деректерді қорғау және оларды өңдеу тетігін құру;

- консультациялық және ақпараттық-түсіндіру іс-шараларын жүзеге асыру;

- цифрлық валюталардың айналысы жөніндегі қызметті бақылау;

- қоғамдық ұйымдармен, азаматтармен ақпараттық қауіпсіздікті бұзудың алдын алу бойынша бірлескен іс-қимылдар.

Мемлекеттегі ақпараттық қауіпсіздікті қамтамасыз ету міндеті ұлттық ауқымнан асып түседі, сондықтан халықаралық ынтымақтастықтың қажеттілігі айқын. Заңсыз әрекеттерді жасаған адам және жәбірленуші адам әртүрлі юрисдикцияларда болуы мүмкін. Бұл электрондық дәлелдемелерді алуға, кінәлі адамдарды ұстап беруге, сот үкімін орындауға, қылмыстық қудалауға және т. б. қатысты уақтылы ден қою тетігін талап етеді. Бұдан басқа, мемлекеттердің құқықтық көмегі активтерге тыйым салуды жүзеге асыруға, осы кірістерді заңдастыруға, сот билігі органдарының актілерін тануға және т.б. қатысты көрінеді.

Қазақстанда ақпараттық қауіпсіздік саласында жеткілікті заңнамалық база құрылды, сондықтан қазіргі уақытта оны іске асыру және киберқылмысқа қарсы іс-қимыл тетігі қажет. Мұндай тетікті құруға ақпараттық қауіпсіздікті бұзуға қарсы іс-қимылдың бірыңғай халықаралық тетігін айқындайтын әмбебап халықаралық актіні қабылдау ықпал етуі мүмкін.

Авторлардың қосқан үлесі

Ауешова Б.Т. зерттеу әдістемесіне жауапты. Кіріспе мен қорытынды жазды. Статистикалық деректерге талдау жүргізді.

Утенова А.А. нәтижелер мен талқылауға жауапты. Библиографиялық дереккөздерді өңдеді және талдады. Әдебиет пен транслитерацияны ресімдеуге қатысты.

Ізтұрғанова Г.Қ. деректерді жинауға және өңдеуге жауапты. Зерттеу әдістері туралы бөлім жазды. Авторлар мен олардың үлестері туралы ақпарат дайындады.

ӘДЕБИЕТТЕР

1. *Marco G. Understanding cybercrime: phenomena, challenges and legal response - [Electronic resource] // URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf (date of reference:15.01.2024)7*

2. *Головко Л.В. Анализ Концепции проекта Уголовного кодекса Республики Казахстан - [Электронный ресурс] // URL: https://online.zakon.kz/Document/?doc_id=31141571 (дата обращения: 25.12.2023).*

3. *Михайлов Б.П., Хазов Е.Н., Богданов А.В. и др. Особенности противодействия киберпреступности подразделениями уголовного розыска: учебное пособие // Москва: Юнити-Дана, 2016. - 151 с.*

4. *Багий Э. Информационная безопасность в Казахстане - [Электронный ресурс] // URL: https://mg-partner.com/novosti/informacionnaya-bezopasnost-v-kazahstane?ysclid=lshjer4ml0554042142 (дата обращения: 29.12.2023).*

5. *Ханов Т.А., Нуркеев А.Ж. Современные подходы к определению компьютерной преступности и особенности компьютерных преступлений // Известия Алтайского государственного университета. - 2017. - № 6 (98). - С. 105–111.*

6. *Kerr O.S. Cyber Security: Protecting America's New Frontier: Hearing Before the H. Subcomm on the Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong., November 15, 2011 (Statement of Orin S. Kerr, Prof. of Law, GW Law School) - [Electronic resource] // URL: https://scholarship.law.gwu.edu/faculty_testimony/3/ (date of reference: 29.12.2023).*

7. *Nieles M., Dempsey K., Pillitteri V.Y. An Introduction to Information Security - [Electronic resource] // URL: https://www.academia.edu/57270668/ An_introduction_to_information_security (date of reference: 12.01.2024).*

8. *Cannataci J.A. Privacy, Technology Law and religions across cultures // Journal of Information, Law & Technology. – 2009. - №(1). – P. 1-22.*

9. *Лоскутов И.Ю. Преступления в сфере информационных технологий в проекте новой редакции Уголовного кодекса Республики Казахстан - [Электронный ресурс] // URL: https://online.zakon.kz/Document/?doc_id=31254918 (дата обращения: 18.01.2024).*

10. *Киютин В.Г., Новиков А.П. Правовое регулирование борьбы с киберпреступностью,*

кибертерроризмом и трафиком людей: опыт Европейского Союза // Бишкек; Москва: Кыргызско-Российский Славянский университет, 2010. - 240 с.

11. Мухамеджанова А. Д. Особенности динамики киберпреступности в Республике Казахстан и ее влияние на вопросы её предупреждения // Российско-Азиатский правовой журнал. – 2022. – С.49-55 - [Электронный ресурс] // https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya?ysclid=lupipc khby711682946 (дата обращения: 12.01.2024).

REFERENCES

1. Marco G. Understanding cybercrime: phenomena, challenges and legal response - [Electronic resource] // URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf (date of reference:15.01.2024)7

2. Golovko L.V. Analiz Koncepcii proekta Ugolovnogo kodeksa Respubliki Kazahstan - [Jelektronnyj resurs] // URL: https://online.zakon.kz/Document/?doc_id=31141571 (data obrashhenija: 25.12.2023).

3. Mihajlov B.P., Hazov E.N., Bogdanov A.V. i dr. Osobennosti protivodejstvija kiberprestupnosti podrazdelenijami ugolovnogo rozyska: uchebnoe posobie // Moskva: Juniti-Dana, 2016. - 151 s.

4. Bagij Je. Informacionnaja bezopasnost' v Kazahstane - [Jelektronnyj resurs] // URL: https://mg-partner.com/novosti/informacionnaya-bezopasnost-v-kazahstane?ysclid=lshjer4ml0554042142 (data obrashhenija: 29.12.2023).

5. Hanov T.A., Nurkeev A.Zh. Sovremennye podhody k opredeleniju komp'juternoj prestupnosti i osobennosti komp'juternyh prestuplenij // Izvestija Altajskogo gosudarstvennogo universiteta. - 2017. - № 6 (98). - S. 105–111.

6. Kerr O.S. Cyber Security: Protecting America's New Frontier: Hearing Before the H. Subcomm on the Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong., November 15, 2011 (Statement of Orin S. Kerr, Prof. of Law, GW Law School) - [Electronic resource] // URL: https://scholarship.law.gwu.edu/faculty_testimony/3/ (date of reference: 29.12.2023).

7. Nieles M., Dempsey K., Pillitteri V.Y. An Introduction to Information Security - [Electronic resource] // URL: https://www.academia.edu/57270668/ An_introduction_to_information_security (date of reference: 12.01.2024).

8. Cannataci J.A. Privacy, Technology Law and religions across cultures // Journal of Information, Law & Technology. – 2009. - №(1). – R. 1-22.

9. Loskutov I.Ju. Prestuplenija v sfere informacionnyh tehnologij v proekte novoj redakcii Ugolovnogo kodeksa Respubliki Kazahstan - [Jelektronnyj resurs] // URL: https://online.zakon.kz/Document/?doc_id=31254918 (data obrashhenija: 18.01.2024).

10. Kijutin V.G., Novikov A.P. Pravovoe regulirovanie bor'by s kiberprestupnost'ju, kiberterrorizmom i trafikom ljudej: opyt Evropejskogo Sojuza // Bishkek; Moskva: Kyrgyzsko-Rossijskij Slavjanskij universitet, 2010. - 240 s.

11. Muhamedzhanova A. D. Osobennosti dinamiki kiberprestupnosti v Respublike Kazahstan i ee vlijanie na voprosy ejo preduprezhdenija // Rossijsko-Aziatskij pravovoj zhurnal. – 2022. – S.49-55 - [Jelektronnyj resurs] // https://cyberleninka.ru/article/n/osobennosti-dinamiki-kiberprestupnosti-v-respublike-kazahstan-i-ee-vliyanie-na-voprosy-eyo-preduprezhdeniya?ysclid=lupipc khby711682946 (data obrashhenija: 12.01.2024).