ӘОЖ 343.00
ҒТАМР 10.85.45

КИБЕРШАБУЫЛДАРДЫҢ КРИМИНАЛИСТИКАЛЫҚ СИПАТТАМАСЫ

Нургуль Байтоковна Кубанова
Құқықтану магистрі, Қазақстан Республикасы Ішкі істер министрлігі М. Есболатов атындағы Алматы академиясының докторанты; Алматы қ., Қазақстан Республикасы; e-mail: nurgul_kubanova@mail.ru; ORCID: https://orcid.org/0009-0006-1141-1165

Аннотация. *Қазіргі әлемде ақпараттық технологиялар қоғамның қалыптасуында шешуші рөл атқарады. Интернет пен цифрлық коммуникацияның дамуы жаңа мүмкіндіктерді ашты, сонымен қатар кез келген ұйымға, оның көлемі мен саласына қарамастан, елеулі қауіп төндіретін кибершабуылдардың көбеюіне әкелді. Кибершабуылдар - бұл оларды ашу және алдын алу үшін ерекше назар аударуды және тәсілдерді қажет ететін қылмыстың ерекше түрі болып табылады. Қазіргі уақытта құқық қорғау органдары киберқылмыстарды тергеу кезінде бірқатар күрделі мәселелерге кездеседі, бұл мәселелер осы мақалада қарастырылды.*

Мақаланың негізгі мақсаты - кибершабуылдардың ерекшеліктерін зерттеу, олардың сипаттамаларын талдау, сондай-ақ киберқылмыстарды тиімді анықтау және тергеу бойынша ұсыныстарды әзірлеу.

Мақалада аналитикалық және салыстырмалы талдау әдістері, кибершабуылдар тақырыбы бойынша ғылыми әдебиеттерді, нормативтік құқықтық актілерді және практикалық материалдарды зерттеу және жалпылау қолданылды. Сонымен қатар, осы мақалада Қазақстан азаматтарына онлайн сауалнама жүргізу арқылы зерттеудің сапалы әдісі қолданылды. Сондай-ақ, Қазақстан Республикасындағы ақпараттандыру және байланыс саласындағы қылмыстың жай-күйін ашатын статистикалық деректерге талдау жүргізілді.

Алынған нәтижелерді құқық қорғау органдары, киберқауіпсіздік саласындағы сарапшылар, сондай-ақ заңнамалық және нормативтік актілерді әзірлеушілер кибершабуылдарға қарсы іс-қимылдың тиімділігін арттыру үшін пайдалана алады.

Кибершабуылдар - оларды анықтау мен тергеуге кешенді көзқарасты қажет ететін күрделі және көп қырлы қауіп болып табылады. Алынған деректерді талдау негізінде ақпараттандыру және байланыс саласындағы қылмысқа қарсы іс-қимыл мәселелерінде құқық қорғау органдары мен сот жүйесінің қызметін жетілдіру жөніндегі қызметтің тиімділігі туралы қорытынды жасалды. Бұл қылмыстарға тиімді қарсы тұру үшін құқық қорғау органдарының жұмыс әдістерін және халықаралық ынтымақтастықты үнемі жетілдіру қажет.

Түйінді сөздер: *киберқылмыс, кибершабуылдар, киберқауіпсіздік, киберкеңістік, ақпараттық технологиялар.*

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРАТАК

Кубанова Нургуль Байтоковна
Магистр юриспруденции, докторант Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова; г. Алматы, Республика Казахстан; e-mail: nurgul_kubanova@mail.ru; ORCID: https://orcid.org/0009-0006-1141-1165

Аннотация. *В современном мире информационные технологии играют ключевую роль в функционировании общества. Развитие интернета и цифровых коммуникаций открыло новые возможности, но также привело к росту числа кибератак, представляющих серьёз-*

ную угрозу для любой организации, независимо от ее размера и отрасли. Кибератаки являются специфическим видом преступлений, которые требуют особого внимания и подходов для их раскрытия и предотвращения. В настоящее время правоохранительные органы сталкиваются с рядом серьезных проблем при расследовании киберпреступлений, которые рассмотрены в данной статье.

Основной целью статьи является исследование особенностей кибератак, анализ их характеристик, а также разработка рекомендаций по эффективному выявлению и расследованию киберпреступлений.

В статье использованы методы аналитического и сравнительного анализа, изучение и обобщение научной литературы, нормативных правовых актов и практических материалов по теме кибератак. Вместе с тем, в данной статье применен качественный метод исследования путем проведения онлайн опроса граждан Казахстана. Также проведен анализ статистических данных, раскрывающих состояние преступности в сфере информатизации и связи в Республике Казахстан.

Полученные результаты могут быть использованы правоохранительными органами, экспертами в области кибербезопасности, а также разработчиками законодательных и нормативных актов для повышения эффективности противодействия кибератакам.

Кибератаки представляют собой сложную и многогранную угрозу, требующую комплексного подхода к их выявлению и расследованию. На основе анализа полученных данных сделан вывод об эффективности деятельности по совершенствованию деятельности правоохранительных органов и судебной системы в вопросах противодействия преступности в сфере информатизации и связи. Для эффективного противодействия этим преступлениям необходимо постоянное совершенствование методов работы правоохранительных органов и международное сотрудничество.

Ключевые слова: *киберпреступность, кибератаки, кибербезопасность, киберпространство, информационные технологии.*

FORENSIC CHARACTERIZATION OF CYBER ATTACKS

Kubanova Nurgul Baitokovna
Master of Jurisprudence, doctoral student of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov; Almaty c., Republic of Kazakhstan; e-mail: nurgul_kubanova@mail.ru; ORCID: https://orcid.org/0009-0006-1141-1165

Abstract. *In today's world, information technology plays a key role in the functioning of society. The development of the Internet and digital communications has opened up new opportunities, but has also led to an increase in the number of cyber-attacks that pose a serious threat to any organization, regardless of its size and industry. Cyberattacks are a specific type of crime that require special attention and approaches to solve and prevent them. Currently, law enforcement agencies face a number of serious problems in investigating cybercrime, which are discussed in this article.*

The main purpose of the article is to study the peculiarities of cyberattacks, analyze their characteristics, and develop recommendations for effective detection and investigation of cybercrime.

The article uses methods of analytical and comparative analysis, study and generalization of scientific literature, normative legal acts and practical materials on the topic of cyberattacks. At the same time, this article applies a qualitative method of research by conducting an online survey of citizens of Kazakhstan. In addition, the analysis of statistical data revealing the state of crime in the sphere of informatization and communication in the Republic of Kazakhstan was carried out.

The results obtained can be used by law enforcement agencies, experts in the field of cyber security, as well as developers of legislative and regulatory acts to improve the effectiveness of countering cyber attacks.

Cyberattacks are a complex and multifaceted threat requiring a comprehensive approach to their detection and investigation. On the basis of an analysis of the data obtained, it was concluded that it was effective in improving the activities of law enforcement agencies and the judicial system

in countering crime in the area of informatisation and communications. The effective countering of these offences requires the continuous improvement of law enforcement methods and international cooperation.

Keywords: *cybercrime, cyberattacks, cybersecurity, cyberspace, information technology.*

DOI: 10.52026/2788-5291_2025_80_2_278

Кіріспе

Қоғамның жалпы цифрлануы Қазақстан Республикасында да, бүкіл әлемде де киберқылмыстардың белсенді дамуына әкелді.

Жалпы алғанда, киберқылмыс ақпараттық технологияларды қылмыстық мақсатта пайдаланатын заңсыз әрекеттер ретінде қарастырылады [1, с. 79].

Айта кету керек, қылмыс жасау кезінде ақпараттық технологияларды қолдану адамның компьютерлік ақпаратты сақтау, өңдеу, беру немесе жою әдістері мен құралдарын мақсатты пайдалануы болып табылады, олардың көмегімен қылмыс жасау немесе қылмыс іздерін жасыру жеңілдетіледі [2, с. 9]. Ақпараттық технологияларды қолдана отырып қылмыс жасау тәсілдері қылмыс түріне байланысты әр түрлі болады. Сонымен қатар, тәжірибені талдау көрсеткендей, бұл әдістердің барлығын жалпылама түрде үш топқа бөлуге болады. Сонымен, қарастырылып отырған қылмыстар: әлеуметтік инженерия әдістерін, зиянды бағдарламалық қамтаманы, арнайы техникалық құралдарды қолдану арқылы жасалуы мүмкін [3, с. 73].

Әлеуметтік инженерия әдістері ақпаратқа немесе жүйелерге рұқсатсыз қол жеткізу үшін адам факторын манипуляциялауға бағытталған кибершабуылдарды жүзеге асырудың негізгі құралдарының бірі болып табылады. Криминалистикалық талдауда олардың ерекшеліктерін ескеру маңызды, өйткені олар қылмыс механизміне, дәлелдемелік базаға және тергеу тактикасына әсер етеді. Әлеуметтік инженерия әдістері ақпараттық қауіпсіздіктің ең қуатты жүйелерін бұзуға қабілетті [4]. Іс жүзінде бұл әдістерді қолдану арқылы көбінесе төлем карталарының деректерін алаяқтықпен алып жатады. Пайдаланушыны алдау үшін, алаяқтар өздерін банк қызметкерлері ретінде таныстырып, қашықтықтан банктік қызмет көрсету жүйесінде операцияның жасалғанын растау үшін карта деректерін ұсынуды талап етеді. Алынған деректерді қылмыскерлер заңды банк картасын ұстаушының атынан заңсыз транзакциялар жасау үшін, негізінен жәбірленушілердің шоттарынан ақша қаражаттарын есептен шығару үшін пайдаланады.

Қазақстанда алаяқтық істерінің 80%-дан астамы әлеуметтік инженерия әдістерін қолдану арқылы жасалған. Сонымен қатар, біздің елде әлеуметтік инженерия дамуды жалғастыруда. Криминалистика тұрғысынан әлеуметтік инженерия әдістеріне қарсы тұру қылмыс механизмін, қылмыскердің сипаттамаларын және ол қолданатын әдістерді талдаумен байланысты. Алайда, криминалистикалық ғылым аясында әлеуметтік инженерия және оның қылмыстық іс-әрекетте қолданылатын әдістері туралы бірыңғай, кешенді білім жүйесі әлі қалыптаспағанын атап өткен жөн. Бұл ақпаратты жүйелеуде және осындай қылмыстарды тергеудің тиімді әдістерін жасауда белгілі бір қиындықтар туғызады.

Кибершабуылдар туралы қылмыстық істерді анықтау және қозғау бірқатар ерекшеліктерге ие және басқа қылмыстардың іс жүргізуінен ерекшеленеді. Мұндай қылмыстық істерді қозғау үшін көбінесе келесі бастапқы ақпараттар қажет:

1. ҚР ҚІЖК-нің 181-бабына сәйкес қылмыстық іс қозғаудың себептерінің бірі жәбірленушінің немесе оның өкілінің жасалған киберқылмыстар туралы арызы болып табылады. Көбінесе заңды тұлғалардың өкілдері емес, жеке тұлғалар құқық қорғау органдарына жүгінеді. Бұл ірі компаниялар мен құрылымдық бөлімшелер кибершабуылдар туралы ақпаратты, өз беделдерін түсірмеу мақсатында құқық қорғау органдарына жүгінбейді және өздерінің жеке қауіпсіздік қызметінің көмегімен жағдайды түзетуге тырысады. Нәтижесінде бұл қылмыстар жасырын болып қалады [5, с. 96].

2. Ақпарат жедел-іздестіру қызметін жүзеге асыру процесінде жедел түрде алынды. Бүгінгі таңда желілік ақпараттық кеңістік ақпараттық - іздестіру қызметін жүзеге асыру үшін аса маңызды рөл атқарады. Тергеудің бастапқы кезеңінде танымал әлеуметтік желілердің, соның ішінде провайдерлердің мамандарымен жоспарлы және үздіксіз өзара іс-қимыл орнату қажет. Бұл қылмыстық әрекеттерді анықтайтын және ашатын қызметкерлерге желілер, клиенттер және олардың белсенділік дәрежесі туралы маңызды ақпарат алуға мүмкіндік береді. Ішкі істер органдарында киберқылмыстарды ашумен «К» бөлімшесі айналысады. [6, с. 218]. Қазір-

гі таңда киберқылмысқа қарсы тұру үшін елімізде «Киберпол» жобасы енгізілді. Бұл жоба барлық өңірлер бойынша қызмет көрсетіп жатыр.

Материалдар мен әдістер

Зерттеудің құқықтық негізі Қазақстан Республикасының қолданыстағы Қылмыстық кодексі, Қазақстан Республикасының өзге де заңнамалық актілері, сондай-ақ киберқылмыс туралы статистикалық деректер болды. Ғылыми мақаланы дайындау кезінде киберқауіпсіздік саласындағы зерттеулер мен жарияланымдар талданды, зерттеудің жалпы ғылыми, сондай-ақ салыстырмалы-құқықтық зерттеу әдістері қолданылды.

Зерттеу аясында Google платформасы арқылы әлеуметтік сауалнама жүргізілді. Алынған нәтижелер кибершабуыл болған жағдайда, азаматтардың құқық қорғау органдарына жүгіну кезінде кездесетін мәселелер анықталды және белгілі бір қорытынды жасауға мүмкіндік берді.

Нәтижелер мен талқылаулар

Киберқылмыстарды анықтаудың көптеген мәселелерінің бар екенін атап өткен жөн. Киберқылмысты анықтау және тергеуді бастау үшін болған іс-әрекет фактісін тіркеу қажет. Алайда, қылмысты анықтаудағы проблеманы жәбірленушілердің өздері жасайды, өйткені олардың кейбіреулері тиісті органдарға киберқылмыс туралы мәлімдемейді. Бұл жүргізілген сауалнаманың нәтижелерімен расталады. Сауалнамаға қатысқан респонденттердің тек 26% кибершабуыл болған жағдайда құқық қорғау органдарына жүгінетінін көрсетті. Құқық қорғау органдарына жүгінбеу себептерінің ішінде респонденттер келесі факторларды көрсетті: 10% құқық қорғау органдарына сенімсіздік және олардың тиімділігіне күмәндану; 14% беделді жоғалту немесе қылмыскерлерден кек алу сияқты мүмкін болатын жағымсыз салдардан қорқу; 5% мәселені өз бетінше немесе басқа әрекеттер арқылы шешу, мысалы, жеке қауіпсіздік қызметтеріне жүгіну; 22% құқық қорғау органдарына жүгіну рәсімдері туралы ақпараттың жеткіліксіздігі немесе өз құқықтарына сенімділіктің болмауы; 14% тергеу процесінің ұзақтығына байланысты, уақыт немесе ресурстардың жетіспеушілігі; 5% Құқық қорғау органдарына жүгінген кезде істің сәтті шешілуіне сенімді дәлелдердің немесе сенімділіктің болмауы; 4% басқа себептерді көрсетті (диаграмма 1). Кейде жеке тұлға қылмыстың құрбаны болғанын түсінбейді.

Киберқылмыс жағдайында құқық қорғау органдарына жүгіну немесе жүгінбеу тура-

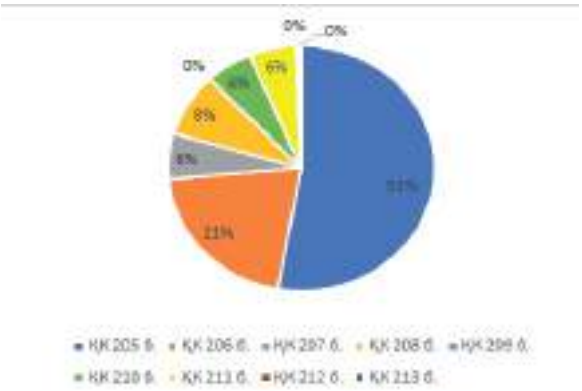
Диаграмма 1. Сауалнама нәтижелері: «Кибершабуылдар кезінде құқық қорғау органдарына бармаудың себебі мен факторларын көрсетіңіз»

лы шешімге әсер ететін факторлар туралы деректерді талдау нәтижесінде берілген салада сот төрелігіне қол жеткізуді қиындататын мыстық құқық бұзушылық тіркелген (кесте 1, диаграмма 2, диаграмма 3).

Киберқылмыс динамикасын зерттей оты-

Ақпараттандыру және байланыс саласындағы қылмыстық құқық бұзушылықтар	СДТБТ (ЕРДР) -да тіркелгендердің саны				Барлығы
	2020	2021	2022	2023	
ҚР ҚК 205 б.	37	46	43	32	158
ҚР ҚК 206 б.	9	9	15	29	62
ҚР ҚК 207 б.	4	0	10	4	18
ҚР ҚК 208 б.	4	9	6	6	25
ҚР ҚК 209 б.	0	0	0	0	0
ҚР ҚК 210 б.	4	4	5	4	17
ҚР ҚК 211 б.	4	5	5	3	17
ҚР ҚК 212 б.	0	0	1	0	1
ҚР ҚК 213 б.	0	1	0	0	1
Барлығы	62	74	85	78	299

Кесте 1. Тіркелген киберқылмыстар туралы мәліметтер



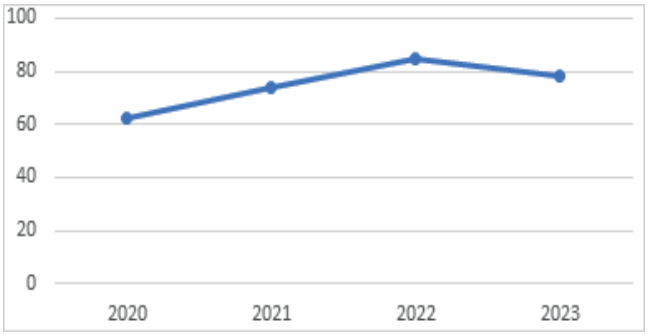


Диаграмма 2. 2020-2023 ж. аралығында тіркелген киберқылмыстар туралы мәліметтер
Диаграмма 3. 2020-2023 ж. аралығындағы киберқылмыстардың динамикасы

бірқатар проблемалар бар екендігі көрінеді. Респонденттердің құқық қорғау органдарына жүгінбеуінің негізгі себептеріне құқық қорғау органдарының тиімділігіне сенімсіздік, жағымсыз салдардан қорқу, мәселені өз бетінше шешуге деген ұмтылыс және жүгіну рәсімдері туралы жеткіліксіз хабардар болу жатады.

Статистикалық деректерді талдау көрсеткендей, 2020 жылдан 2023 жылға дейінгі кезеңде Қазақстан Республикасында ақпараттандыру және байланыс саласында 299 қылрып, ҚР ҚК 7-тарауында көзделген келесі баптар киберқылмыстың ең көп таралған түрі болып табылатынын атап өткен жөн: 205-бап. Ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге құқыққа сыйымсыз қол жеткізу; 206-бап. Ақпаратты құқыққа сыйымсыз жою немесе түрлендіру; 208-бап. Ақпаратты құқыққа сыйымсыз иеленіп алу[1].

Бұл жерде киберқылмыстардың 85-90% жасырын екенін ескеру қажет. Киберқылмыстың таралуының шынайы ауқымын анықтау

[1] *Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V Қылмыстық кодексі (2024.01.05. берілген өзгерістер мен толықтырулармен). // URL: https://online.zakon.kz/Document/?doc_id=31575294 (жүгінген күні: 05.06.2024).*

үшін ақпарат алудың жаңа әдістері мен көздерін пайдалану қажет [7, с. 32].

Ақпараттық-телекоммуникациялық технологияларды пайдалана отырып, құқыққа қайшы әрекеттер жасайтын қылмыскерлер әрқашан, шартты түрде айтқанда, ақпараттық қауіпсіздікті қамтамасыз етудің уәкілетті субъектілері қабылдайтын құқықтық және техникалық шаралардан «бір қадам алда» жүреді. Екінші жағынан, киберқылмыстардың көбеюі жүргізілген зерттеулерге сәйкес, киберқылмыс құрбандарының едәуір бөлігі өз тәжірибесін отбасымен, достарымен немесе құқық қорғау органдарымен бөліспейтіндігіне байланысты [8, p. 219]. Осылайша, ақпараттық технологияларды қолдану арқылы жасалған қылмыстардың саны, басқа ауыр қылмыстардың санынан асып түседі [9, с. 68].

Интернет-қылмыстарды ашу үшін, құқық қорғау органдарының шетелдік байланыс провайдерлері мен интернет-ресурстар иелерінің меншігіндегі ақпаратпен жедел алмасу қажеттілігі туындайды. Бүгінгі таңда осы саладағы халықаралық ынтымақтастықты көздейтін жалғыз құжат Еуропа Кеңесінің компьютерлік қылмыстар жөніндегі Конвенциясы болып табылады[2].

Киберқылмыстардың криминалистикалық сипаттамасының ерекше элементінің бірі – із болып табылады. Қылмысты тергеудің криминалистикалық тактикасының өзіндік ерекшеліктері бар: киберқылмыс іздерін жинау кезінде қылмыс іздерін жинаудың стандартты криминалистикалық әдістері де, мысалы, IP мекенжайлары туралы ақпарат алуға мүмкіндік беретін компьютерлік-техникалық сараптама да қолданылады [10, с. 111].

Киберкеңістіктегі цифрлық іздерді анықтау хаттамада осы фактілердің сипаттамасымен жазылады, мұнда жадыда анықталған құрылғы туралы мәліметтер; құрылғы кімге тиесілі; интернетпен, жергілікті немесе басқа желілермен байланысы бар ма; оның жедел жүйесінің сипаттамасы; файлдарды орналастыру, құру және өзгерту; іздердің сипаттамасы жазылады. Файлдардың, әкімшілік журналдардың қасиеттерін көрсете отырып, экранды суретке түсіргеннен кейін объектінің өзі алынады, содан кейін оны зерттейді [11, с. 43]. Киберқылмыстар қылмыстың трансұлттық түрі болғандықтан, жалпы алғанда, киберқылмыс жасау өте оңай, бұл үшін физикалық қатысу қажет емес және әрекет өте тез жасалады.

Киберқылмыстарды тергеу және ашу, сондай-ақ оларға қарсы тұру кезінде киберқылмыстың ерекшелігіне байланысты келесі мәселелер туындайды:

1. Киберқылмыстар трансшекаралық сипатқа ие: кез-келген аумақтық шекараның болмауына байланысты қылмыскер әлемнің кез-келген жерінде бола алады және қылмыстық әрекеттерді жүзеге асыру үшін бірнеше компьютерлерді олардың бір-бірінен орналасқан жеріне қарамастан қолдана алады, яғни қашықтан әрекет ете алады. Кеңістіктік аспектіден басқа, уақыт өте маңызды. Бірқатар компьютерлік бағдарламалардың жұмысы құрылғыда орнатылған уақытпен байланысты болғандықтан және қылмыскер оны өзгерте алатындықтан, бұл қарастырылып отырған қылмыстарды тергеуде айтарлықтай қиындықтар туғызады. Осыған сүйене отырып, қылмыстың орны мен уақытын анықтау өте қиын және көбінесе мүмкін емес [12, с. 114]. Бұған айқын мысал ретінде «Cobalt» деп аталатын трансұлттық қылмыстық ұйымның банктерге жасаған кибершабуыл фактілері бойынша қылмыстық істі тергеуді келтіруге болады. Алматы прокуратурасының мәліметінше, «Карбанак/Кобальт» - бүкіл әлемдегі банктерге шабуыл жасайтын трансұлттық қылмыстық ұйым. Олардың есебінде әлемнің 40 еліндегі 100-ден астам қаржы ұйымдарын тонаған, келтірілген шығын шамамен 1 миллиард долларды құрайды[3].

Әр түрлі елдердің құқық қорғау органдары арасындағы ынтымақтастықты күшейту маңызды. Бұған киберқауіптер туралы ақпарат алмасу, киберқылмыстардың алдын алу және тергеу бойынша бірлескен операциялар және халықаралық құқықтық құралдар шеңберіндегі әрекеттерді үйлестіру кіреді.

2. Техникалық мәселелер бар: іздерді табу әдістерін таңдау процесі; сандық дәлелдемелерді сақтау және талдау; қылмыскерлердің IP мекенжайын қадағалау; бағдарламалық жасақтаманың осалдығы. Ақпаратты шифрлау құралдарын кеңінен енгізу және қолдану, бақылау тетіктерінің болмауы, желідегі анонимділік және т.б. Мысалы, көптеген бөлімшелерде компьютерлерде және басқа құрылғыларда ескірген операциялық жүйелер мен бағдарламалық қамтамасыз ету қолданылады. Сондай-ақ сот сараптамаларын дайындауға, тағайындауға және жүргізуге байланысты белгілі бір проблемалар бар. Киберқылмысқа сапалы қарсы тұру жоғары

[2] *В Казахстане раскрыли только 22% киберпреступлений в этом году. В МВД рассказали о сложностях в расследовании. // URL: https://kz.kursiv.media (дата обращения: 16.05.2024)7*

[3] *Кибератака на банки: в Агентстве рассказали, как расследовали хищения на 2 млрд тенге. // URL: https://online.fingramota.kz/ru/news/view/6125 (дата обращения: 16.05.2024).*

техникалық жабдықты қажет етеді, бұл қылмыстарды анықтау, сараптамалық зерттеулер жүргізу үшін қажет. Сандық дәлелдемелерді анықтау, жинау, сақтау үшін көптеген мамандандырылған құралдарды тиімді қолдану киберкеңістік саласындағы сараптамалық зертханалардың сапалы жұмысына әкеледі. Осылайша, заманауи техника мен жабдықтардың санын едәуір кеңейту қажет. Тергеушілер, егер ерекше күш жұмсалса, киберқылмыстың іздерін құрылғылардың жадысынан табуға болатындығын түсінуі маңызды.

Технологияның қарқынды дамуын ескере отырып, киберқылмыскерлер шабуыл әдістерін үнемі жетілдіріп отырады. Сондықтан құқық қорғау органдарының қызметкерлері киберқауіпсіздік және криминалистика саласындағы дағдылар мен білімдерді үнемі жаңартып, дамытып отыруы керек. Тәжірибе көрсеткендей, тек заңгерлік білімнің болуы киберкеңістіктегі қылмыстарды тергеуде және алдын алуда тиімді нәтиже бермейді.

3. Құқықтық қиындықтарға біліктілік, қылмыс жасау фактісін анықтау, қылмыс жасаған адамдар немесе адамдар тобы, қылмыстың тәсілі мен себебін анықтау, тергеу үшін құқық қорғау органдары қолданатын әдістерді анықтау, заңнамадағы олқылықтар және т.б. себеп болуы мүмкін. Заңнаманы, үнемі өзгеріп отыратын киберқылмыстарға бейімдеу маңызды. Бұл киберқылмыс үшін жазаны қатаңдатуды, құқық қорғау органдарының киберқауіпсіздік саласындағы өкілеттіктерін кеңейтуді және мемлекеттік органдар мен жеке сектор арасындағы ынтымақтастық тетіктерін жақсартуды қамтуы мүмкін.

Қорытынды

Жоғарыда айтылғандарды ескере отырып, киберқылмыс қоғамда, мемлекетте және әлемде болып жатқан әлеуметтік, саяси, экономикалық, психологиялық және басқа факторлардың салдарынан туындайды деген қорытынды жасауға мүмкіндік береді [13, с. 234]. Соңғы жылдары криминалистикалық әдебиеттерде осы қылмыстарды тергеу әдістемесіне баса назар аударылғанына қарамастан, осы салада әлі де бірқатар шешілмеген және пікірталас тудыратын мәселелер бар. Киберқылмыскерлердің криминалистикалық сипаттамасы ерекше орын алады, өйткені бұл мәліметтер, тергеу бағытын анықтауға және қылмыскерлерді іздеуге қажетті маңызды криминалистикалық ақпараттан тұрады. Олардың кәсіби қасиеттері, компьютерлік техниканы, компьютерлік бағдарламаларды және т. б. білу дәрежесі туралы ақпарат ерекше маңызды [14, с. 99]. Әдетте, заңды тұлғаға қатысты киберқылмыстар жасалған жағдайда, қылмыскер немесе сыбайлас осы мекеменің қызметкері болып табылады [15, с. 57].

Киберқылмыспен күресудің күрделілігі киберқылмыс жасаған адамның жеке басына, жеке тұлғаның ерекшеліктеріне, қылмыстарды анықтауға және ашуға бағытталған жедел-іздестіру іс-шараларына, сондай-ақ оларды жүргізу нәтижелерін заңдастыру мүмкіндіктеріне байланысты болады [16, с. 15]. Қорытындылай келе, кибершабуылдарды жақсарту механизмінде әлеуметтік инженерия әдістері шешуші рөл атқаратынын атап өткен жөн. Талдау көрсеткендей, оларды криминалистикалық біліммен жіктеу адам факторын манипуляциялаудың қолданыстағы бағыттарын жүйелеуге ғана емес, сонымен қатар мұндай жағдайларды тергеу мен алдын алудың тиімді әдістерін жасауға мүмкіндік береді. Сонымен қатар, ұсынылған тәсіл киберқылмыстың әлеуметтік-психологиялық аспектілерін зерттеуге, сондай-ақ кибершабуылдарға қарсы іс-қимыл құралдарын жетілдіруге негіз бола алады.

Кибершабуылдар анықтау мен тергеуге кешенді көзқарасты қажет ететін күрделі және көп қырлы қауіп болып табылады. Жаһандану және технологиялардың қарқынды дамуы жағдайында құқық қорғау органдары өздерінің жұмыс әдістерін үнемі жетілдіріп, трансшекаралық кибершабуылдарға неғұрлым тиімді қарсы тұру үшін әртүрлі елдердің құқық қорғау органдары арасында халықаралық ынтымақтастық пен ақпарат алмасуды дамыту керек. Құқық қорғау органдарының қызметкерлері үшін киберқауіпсіздік және кибершабуылдарды тергеу әдістері бойынша арнайы курстар мен тренингтер әзірлеп, қызметкерлердің киберқауіптердің жаңа түрлері және оларды анықтау, талдау және алдын алу әдістері туралы білімдерін үнемі жаңартып отыру, сондай-ақ желілік трафикті талдау, кибершабуылдарды бақылау және анықтау үшін блокчейн және жасанды интеллектке негізделген заманауи құралдар мен технологияларды енгізіп техникалық базаны жетілдіру қажет. Қазіргі заманғы қауіптер мен кибершабуыл әдістерін дәлірек көрсету үшін қолданыстағы заңдарды бейімдеу және жаңарту, сондай-ақ киберқылмыс үшін жазаны күшейту сипаттамасы осы қылмыстардың табиғатын тереңірек түсінуге және олардың алдын алу мен ашудың тиімді стратегияларын жасауға мүмкіндік береді.

ӘДЕБИЕТ

1. Мамаева Л.Н., Шульдякова В.В., Удалов Д.В. Влияние глобальных угроз на национальную экономическую безопасность // Вестник Саратовского государственного социально-экономического университета. - 2018. - № 5 (74). - С. 77–80.

2. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительная практика: дис. … канд. юрид. наук. - М., 2015. – 222 с.

3. Захаров Д.Н., Щерба В.В. Особенности расследования киберпреступлений // Вопросы кибербезопасности. - 2017. - № S2 (20). - С. 72-76.

4. Ламинина О.Г. Возможности социальной инженерии в информационных технологиях // Гуманитарные, социально-экономические и общественные науки. - 2017. // URL: https://cyberleninka.ru/article/n/vozmozhnosti-sotsialnoy-inzhenerii-v-informatsionnyhtehnologiyah (дата обращения: 16.05.2024).

5. Темиралиев Т.С., Омаров Е.А. Проблемы противодействия преступлениям, совершенным с применением информационных систем, и пути их решения. // Вестник Института законодательства и правовой информации Республики Казахстан. – 2019. – №1 (55) - С. 93-99.

6. Григорьева А.Е. Выявление и расследование интернет-мошенничества на первоначальном этапе. // Аграрное и земельное право. - 2022. - №12 (216). // URL: https://cyberleninka.ru/article/n/vyyavlenie-i-rassledovanie-internet-moshennichestva-na-pervonachalnom-etape (дата обращения: 28.04.2024).

7. Протасевич А.А., Зверянская Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Всероссийский криминологический журнал. - 2011. - №3. - С. 28-33.

8. Jansen J., Leukfeldt E.R. Coping with cybercrime victimization: An exploratory study into impact and change // Journal of Qualitative Criminal Justice and Criminology. - 2018. -Volume 6. - Issue 2. - P. 205–228.

9. Мамаева Л.Н., Бехер В.В. Угрозы кибербезопасности в цифровом пространстве // Вестник Саратовского государственного социально-экономического университета. - 2019. - № 4 (78). - С. 68–70.

10. Аносов А.В. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч. 1. – С. 208.

11. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. - 2012. - № 8. - С. 43-45.

12. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. - 2013. - С. 114-116.

13. Сладченко Н.С. Криминалистическая характеристика киберпреступности на территории РФ // Международный журнал гуманитарных и строительных наук. - 2021. - №10-2(61). - С. 232-237.

14. Савельева М.В., Смушкин А.Б. Криминалистика. Учебник. – М.: «Деловой двор», 2009. – 324 с.

15. Клещёва, А.С. Криминалистическая характеристика личности преступника, совершающего преступления в области компьютерной информации / А.С. Клещёва. — Текст: непосредственный // Молодой ученый. — 2018. — № 37 (223). — С. 57-60. // URL:https://moluch.ru/archive/223/52669/ (дата обращения: 26.04.2024).

16. Фурнелл С., Доулинг С. Киберпреступность: портрет ландшафта // Журнал криминологических исследований, политики и практики. - 2019. - Т. 5. -№ 1. - С. 13–26.

REFERENCES

1. Mamaeva L.N., Shuldyakova V.V., Udalov D.V. Vliyanie globalnyh ugroz na natsionalnuyu ekonomicheskuyu bezopasnost // Vestnik Saratovskogo gosudarstvennogo sotsialno-ekonomicheskogo universiteta. - 2018. - № 5 (74). - S. 77–80.

2. Safonov O.M. Ugolovno-pravovaya otsenka ispolzovaniya kompyuternyh tehnologiy pri sovershenii prestupleniy: sostoyanie zakonodatelstva i pravoprimenitelnaya praktika: dis. … kand. yurid. nauk. - M., 2015. – 222 s.

3. Zaharov D.N., Shherba V.V. Osobennosti rassledovaniya kiberprestupleniy // Voprosy kiberbezopasnosti. - 2017. - № S2 (20). - S. 72-76.

4. Laminina O.G. Vozmozhnosti socialnoi inzhenerii v informatsionnyh tehnologiyah // Gumanitarnye, socialno-ekonomicheskie i obshhestvennye nauki. - 2017. // URL: https:// cyberleninka.ru/article/n/vozmozhnosti-sotsialnoy-inzhenerii-v-informatsionnyhtehnologiyah (data obrashhenija: 16.05.2024).

5. Temiraliev T.S., Omarov E.A. Problemy protivodejstviya prestupleniyam, sovershennym s primeneniem informatsionnyh sistem, i puti ih resheniya. // Vestnik Instituta zakonodatelstva i pravovoi informatsii Respubliki Kazahstan. – 2019. – №1 (55) - S. 93-99.

6. Grigoryeva A.E. Vyiavlenie i rassledovanie internet-moshennichestva na pervonachalnom etape. // Agrarnoe i zemelnoe pravo. - 2022. - №12 (216). // URL: https://cyberleninka.ru/ article/n/vyyavlenie-i-rassledovanie-internet-moshennichestva-na-pervonachalnom-etape (data obrashhenija: 28.04.2024).

7. Protasevich A.A., Zverjanskaya L.P. Borba s kiberprestupnostyu kak aktualnaya zadacha sovremennoi nauki // Vserossiyskiy kriminologicheskiy zhurnal. - 2011. - №3. - S. 28-33.

8. Jansen J., Leukfeldt E.R. Coping with cybercrime victimization: An exploratory study into impact and change // Journal of Qualitative Criminal Justice and Criminology. - 2018. -Volume 6. - Issue 2. - P. 205–228.

9. Mamaeva L.N., Beher V.V. Ugrozy kiberbezopasnosti v tsifrovom prostranstve // Vestnik Saratovskogo gosudarstvennogo sotsialno-ekonomicheskogo universiteta. - 2019. - № 4 (78). - S. 68–70.

10. Anosov A.V. Deyatelnost organov vnutrennih del po borbe s prestupleniyami, sovershennymi s ispolzovaniem informatsionnyh, kommunikatsionnyh i vysokih tehnologiy: uchebnoe posobie: v 2 ch. / [A. V. Anosov i dr.]. – M.: Akademiya upravleniya MVD Rossii, 2019. – Ch. 1. – C. 208.

11. Smushkin A.B. Virtualnye sledy v kriminalistike // Zakonnost'. - 2012. - № 8. - S. 43-45.

12. Polyakov V.V. Obstanovka sovershheniya prestupleniy v sfere kompyuternoi informatsii kak element kriminalisticheskoi harakteristiki // Izvestiya Altaiskogo gosudarstvennogo universiteta. - 2013. - S. 114-116.

13. Sladchenko N.S. Kriminalisticheskaya harakteristika kiberprestupnosti na territorii RF // Mezhdunarodnyi zhurnal gumanitarnyh i stroitelnyh nauk. - 2021. - №10-2(61). - C. 232-237.

14. Savelyeva M.V., Smushkin A.B. Kriminalistika. Uchebnik. – M.: «Delovoj dvor», 2009. – 324 c.

15. Kleshhyova, A.S. Kriminalisticheskaya harakteristika lichnosti prestupnika, sovershayushhego prestupleniya v oblasti kompyuternoj informatsii / A.S. Kleshhyova. — Tekst: neposredstvennyi // Molodoi uchenyi. — 2018. — № 37 (223). — S. 57-60. // URL: https://moluch.ru/archive/223/52669/ (data obrashhenija: 26.04.2024).

16. Furnell S., Douling S. Kiberprestupnost: portret landshafta // Zhurnal kriminologicheskih issledovaniy, politiki i praktiki. - 2019. - T. 5. -№ 1. - S. 13–26.