«КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ: ЖАЙ-КҮЙІ, ТЕНДЕНЦИЯЛАРЫ, БОЛАШАҒЫ»

халықаралық ғылыми-тәжірибелік конференциясының материалдары

«ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ: СОСТОЯНИЕ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ»

материалы международной научно-практической конференции

Қарағанды, 2023 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ІІМ
Б. БЕЙСЕНОВ АТЫНДАҒЫ
ҚАРАҒАНДЫ АКАДЕМИЯСЫ

•

КАРАГАНДИНСКАЯ АКАДЕМИЯ
МВД РЕСПУБЛИКИ КАЗАХСТАН
ИМЕНИ Б. БЕЙСЕНОВА

«КИБЕРҚЫЛМЫСҚА ҚАРСЫ ІС-ҚИМЫЛ: ЖАЙ-КҮЙІ, ТЕНДЕНЦИЯЛАРЫ, БОЛАШАҒЫ»

халықаралық ғылыми-тәжірибелік конференциясының материалдары
(1 желтоқсан 2023 ж.)

«ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ: СОСТОЯНИЕ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ»

материалы международной научно-практической конференции
(1 декабря 2023 г.)

ҚАРАҒАНДЫ • 2023 • КАРАГАНДА

УДК 343
ББК 67.408
К 33

К33 Киберқылмысқа қарсы іс-қимыл: жай-күйі, тенденциялары, болашағы [Электрондық басылым]: халықаралық ғылыми – практикалық конференция материалдарының жинағы, Қарағанды қ., 1 желтоқсан 2023 ж. – Электрон. мәтіндік деректер. (3 mb). – Қарағанды: Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы, 2023. – 1 электрон. опт. диск (CD-R). - Жүйелік талаптар: IBM PC, 1 GHz; 512 mb жедел жады; 3 mb жедел жады; CD/DVD-ROM дисководы; Windows XP және одан жоғары операциялық жүйе; Adobe Reader 8.0 және одан жоғары. – Атауы экраннан.

К33 Противодействие киберпреступности: состояние, тенденции, перспективы [Электронное издание]: сборник материалов международной научно-практической конференции, г. Караганда, 1 декабря 2023 г. – Электрон. текстовые дан. (3 mb). – Караганда: Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2023. – 1 электрон. опт. диск (CD-R). – Систем. требования: IBM PC, 1 GHz; 512 mb оперативной памяти; 3 mb ОЗУ; CD/DVD-ROM дисковод; операционная система Windows XP и выше; Adobe Reader 8.0 и выше. – Загл. с экрана.

Жинақта «Киберқылмысқа қарсы іс-қимыл: жай-күйі, тенденциялары, болашағы» атты халықаралық ғылыми-практикалық конференцияға қатысушылардың ғылыми баяндамалары ұсынылған. Жинақта жарияланған материалдар құқық қолдану қызметін жүзеге асыратын органдардың қызметкерлерін, сондай-ақ жоғары оқу орындарының ғалымдарын, оқытушыларын, докторанттарын, магистранттары мен курсанттарын қызықтырады.

В сборнике представлены научные доклады участников международной научно-практической конференции «Противодействие киберпреступности: состояние, тенденции, перспективы». Материалы, опубликованные в сборнике, представляют интерес для сотрудников органов, осуществляющих правоприменительную деятельность, а также ученых, преподавателей, докторантов, магистрантов и курсантов высших учебных заведений.

Жинақтағы материалдар автордың редакциясымен берілді.
Материалы, публикуемые в сборнике, даны в авторской редакции.

ISBN 978-601-7264-91-8

УДК 343
ББК 67.408

Аблиязова Елена Борисовна,
ведущий научный сотрудник
к.ю.н., подполковник полиции, e-mail: abl-elena@yandex.ru
(Всероссийский научно-исследовательский институт МВД России, Российская Федерация)

О СПОСОБАХ ВИКТИМОЛОГИЧЕСКОЙ ПРОФИЛАКТИКИ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И ПРИМЕНЕНИЕМ МЕТОДОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

Аннотация. Публикация посвящена преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Автором анализируется работа мошеннического call-центра, который был обнаружен в г. Бердянске сотрудниками Росгвардии. Изучены сведения, собранные Сбербанком России, позволившие определить тип жертвы, наиболее подверженной влиянию методов социальной инженерии. Также предложен ряд мер, позволяющий организовать работу по защите граждан России от подобных преступных посягательств.

Ключевые слова: информационно-телекоммуникационные технологии, социальная инженерия, мошенник, call-центр, жертва, методы информирования, преступные посягательства, защита.

ON THE METHODS OF VICTIMOLOGICAL PREVENTION OF FRAUDULENT ACTIONS COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES AND THE USE OF SOCIAL ENGINEERING METHODS

Annotation. The publication is devoted to crimes committed using information and telecommunication technologies. The author analyzes the work of a fraudulent call center, which was discovered in Berdyansk by Rosgvardiya employees, which made it possible to collect data on victims to whom social engineering methods were applied and proposed ways to protect against such criminal encroachments.

Keywords: information and telecommunication technologies, social engineering, cheater, call center, victim, methods of informing, criminal encroachments, protection.

В России нет людей, которым хоть раз в жизни не звонили мошенники, представлявшиеся сотрудниками служб безопасности банков или правоохранительных органов и всегда их целью, было заставить человека самому сообщить сведения о своем финансовом положении. В подобных условиях важными становятся меры, направленные на совершенствование методов информирования населения о способах совершения преступлений, совершенных с использованием информационно-телекоммуникационных технологий и как от таких угроз, может, защитится рядовой гражданин. Все системы безопасности банков преж-

де всего направлены на защиту сведений, которыми они располагают, но в этой системе есть слабое звено – это человек, чьи сведения охраняются.

На территории России наблюдается рост числа преступлений, совершенных с использованием или применением информационно-телекоммуникационных технологий, которые реализуются методами социальной инженерии. Технические средства защиты не поддаются уговорам, но человек подвержен эмоциональным воздействиям, что и используют мошенники. В этом им помогают методы социальной инженерии, то есть способы психологического манипулирования людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

По данным Главного информационно-аналитического центра МВД России каждое третье преступление (33,3 %), зарегистрированное в январе-сентябре 2023 года, совершалось с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации (всего – 489,0 тыс.; +29,2 %). Больше половины таких преступлений (51,9 %) относятся к категориям тяжких и особо тяжких (253,7 тыс.; +26,8 %), более чем три четверти (77,2 %) совершалось с использованием сети Интернет (377,6 тыс.; +36,7 %), почти половина (45,0 %) – средств мобильной связи (220,3 тыс.; +46,7 %) [1].

ЦБ России сообщил, что в первом полугодии 2023 года злоумышленники, используя электронные средства платежей, похитили у банковских клиентов 8,1 млрд руб., при этом половина средств была похищена с помощью методов социальной инженерии [2].

Чаще всего мошенники используют методы – фишинг и вишинг. Цель у этих методов одна – это обманным путем выведать у жертвы конфиденциальные сведения, такие как пароли, номера банковских карт, коды подтверждения. Разница между фишингом и вишингом в том, что фишинг больше распространен в почтовых сервисах, социальных сетях и электронных платежных системах, а вишинг – это попытка выведать данные у жертвы при телефонном разговоре. И хотя мошенникам удается получить нужную информацию только в одном случае из ста совершенных звонков, в общем, такая преступная деятельность приносит прибыль в миллиарды рублей.

Впервые о мошеннических call-центрах заговорили в связи со звонками, которые совершали заключенные СИЗО и колоний. Сверхприбыли подобной преступной деятельности привлекли внимание организованных преступных сообществ Украины, неофициально г. Днепр считается столицей телефонного мошенничества [3]. Политические события 2014 года привели к прекращению взаимодействия между правоохранительными органами Украины и России. На Украине в результате политического и экономического кризисов стало наблюдаться снижение уровня жизни населения и как следствие высокий уровень криминализации общества. Высокий уровень коррупции дал возможность преступным call-центрам действовать, не опасаясь противодействия от государства. По оценке Сбера, на сегодняшний день общее количество таких центров по всей Украине превышает 3 000 [4].

Долгое время не было достоверных данных о внутренней структуре мошеннических call-центров, что затрудняло организацию мер по противодействию их деятельности. И когда в апреле 2022 года в рамках СВО в г. Бердянске сотрудники Росгвардии обнаружили брошенный call-центр [5], где сохранились компьютеры с информацией, то появилась возможность понять, как функционировала эта криминальная структура.

О масштабах криминальной деятельности можно судить по штатной численности call-центра, только в этом центре в сменном режиме работало около 300 сотрудников, которые совершали около 5 тыс. звонков в сутки. Роли всех сотрудников были четко распределены, и жертва в зависимости от степени внушаемости передавалась от сотрудников, которые осуществляли «холодный» обзвон к тем, кто уже завершал мошенническое списание средств со счетов человека. Для ведения разговора с потенциальной жертвой использовалось более 150 различных сценариев, также были обнаружены инструкции по ведению разговора, если человек сомневается и задает много вопросов. Понятно, что организовать подобную коммуникацию возможно только с привлечением людей, обладающих знаниями в сфере манипулятивных техник. Также в преступное сообщество входили группы технической поддержки, поиска баз данных для совершения звонков и тех, кто через интернет-сервисы получали сведения о конкретных лицах. Сложилась даже некоторая инфраструктура, обеспечивающая деятельность call-центров. Риелторы подыскивали помещения для офисов, отдельные фирмы занимались закупкой и настройкой оборудования и даже службы доставки были ориентированы исключительно на выполнение заказов тысяч сотрудников call-центров, чтобы процесс преступной деятельности не прерывался.

В действительности для проведения атак не нужен большой объем информации, достаточно сведений, которые человек сам о себе размещает в сети Интернет. Конечно, для массовых обзвонов необходимы большие массивы информации и мошеннические call-центры покупают базы данных мобильных операторов связи, банков, онлайн-магазинов в теневом сегменте сети Интернет (даркнет).

Несмотря на то, что от действий мошенников может пострадать любой человек вне зависимости от уровня доходов и социального статуса, но все-таки можно составить социальный портрет человека, наиболее уязвимого для обмана. В ноябре 2022 года Банк России провел опрос о степени удовлетворенности населения уровнем безопасности финансовых услуг, оказываемых организациями кредитно-финансовой сферы [6] и анализ полученных данных выявил социально-демографические характеристики людей, которым необходимо более внимательно относиться к вопросам безопасности, чтобы не стать жертвой мошенников.

Из числа опрошенных и сообщивших, что становились жертвами мошенников, женщины – 50,4 %, мужчины – 49,6 %. Три четверти пострадавших проживают в городах. Чаще всего жертвами мошенников становились люди в возрасте 25-44 лет (37,4 %), также значительное число жертв имеется среди людей в возрасте 45-64 лет (29,0 %), старше 65 лет обманутых оказалось значи-

тельно меньше (15,7 %) и самыми устойчивыми к мошенническим схемам оказались люди в возрасте 14-19 лет (10,3 %) и 20-24 лет (7,6 %). Если говорить об образовательном уровне лиц, поверивших в мошеннические схемы, то среднее образование имеют 48,0 %, высшее – 28,9 %, общее среднее – 23,1 %. Почти половина лиц, пострадавших от действий мошенников имеют средний уровень достатка (46,5 %), высокий уровень достатка имеют 27,7 % жертв и низкий – 25,8 %. Подавляющее большинство жертв – это трудоустроенные люди (59,4 %), учащиеся – 17,2 %, пенсионеры – 4,8 %, не работающие – 3,2 %, оставшаяся незначительная часть приходится на лиц, относящих себя к самозанятым, домохозяйкам, индивидуальным предпринимателям.

В ходе опроса задавался вопрос о способе мошенничества, было определено, что 60 % противоправных деяний совершены с помощью телефонных звонков и смс-сообщений, через мессенджеры мошенники установили контакт с жертвой в 12 % случаев, через социальные сети – 10 %, по электронной почте – 9 %, с помощью поддельных сайтов – 7 %, поддельные приложения банков использовались в 2 % случаев.

Анализ информации, содержавшейся в компьютерах call-центра из г. Бердянска, также позволяет определить круг жертв. Звонки осуществлялись преимущественно на номера телефонов столичного региона и Ленинградской области. В 60 % случаях жертвами становились женщины. Если говорить о возрасте жертв, то 44 % это люди 30-39 лет, 23 % – 20-29 лет, 19 % – 40-49 лет, 12 % – 50-59 лет, люди старшего поколения разговаривали с мошенниками всего в 2 % случаев.

Обобщив имеющиеся сведения о жертвах, можно представить кто в большей степени уязвим в результате мошеннических атак. Это жители крупных городов, имеющие средний или высокий уровень достатка. Невнимательными к деталям, указывающим на мошеннические схемы, в равной степени оказались как мужчины, так и женщины, но женщины более подвержены внушению, если в качестве канала воздействия мошенники использовали телефон. Неожиданными оказались данные о возрасте потерпевших. В отличии от устоявшегося мнения, что люди старшего поколения в большей степени страдают от действий мошенников, оказалось, что каждая вторая-третья жертва – это люди в возрасте от 25 до 45 лет.

Рассмотрев структуру преступной организации, использовавшей информационно-телекоммуникационные технологии и применявшей методы социальной инженерии, цель которой были совершения телефонных мошенничеств, можно определить ряд мер, которые должны иметь первоочередное значение. Особо важным является то обстоятельство, что меры, направленные на борьбу с мошенниками, должны носить системный характер. Ежедневно появляются новые мошеннические схемы. Лица, занимающиеся противоправной деятельностью, расширяют сферы применения своих преступных навыков и активно осваивают информационное пространство других стран, создавая тем самым предпосылки для создания международных преступных синдикатов.

Для успешного решения проблемы, связанной с мошенничествами необходимо активно работать в двух направлениях – это профилактика преступле-

ний, совершаемых с использованием информационно-телекоммуникационных технологий на государственном уровне и виктимологическая профилактика этих преступлений.

В части государственного уровня необходимо создать преграду для использования мошенниками банковской инфраструктуры, определить порядок использования SIP-телефонии, не оставлять безнаказанными факты нарушения законодательства в области связи, организовать взаимодействие между органами исполнительной власти, банками и операторами связи.

Учитывая, что криминальные доходы от деятельности телефонных мошенников получают организованные преступные группы, которые находятся вне юрисдикции России, то особое значение в системе противодействия приобретают меры виктимологической профилактики.

Защищаться от техник социальной инженерии сложно, но значительно снизить число обманутых можно, если человек будет понимать, что именно он является обязательным звеном в криминальной схеме и цель мошенника – именно от него самого получить конфиденциальную информацию. Суть социальной инженерии заключается в том, что человек должен поверить в выдуманную историю и, если один сценарий перестает приносить прибыль его легко меняют на другой.

В ходе проведения профилактических рейдов, ориентированных на информирование граждан о дистанционном мошенничестве, коммуникатор рассказывает какой-то сценарий, который в конкретный период времени массово использовали мошенники и люди проявляли бдительность, если сталкивались с подобным. Но стоило сценарию измениться, например, звонил не сотрудник банка, а сотрудник социальной защиты, число обманутых опять начинало увеличиваться.

В целях повышения эффективности виктимологической профилактики необходимо информировать людей о первоочередных мерах по защите от техник социальной инженерии. И первоочередной мерой является разъяснение людям раскрытие каких данных может причинить вред прежде всего им самим и не важно какой сценарий из арсенала социальной инженерии был применен.

Список использованной литературы

1. Состояние преступности в России за январь-сентябрь 2023 г. [Электронный ресурс] // https://xn--b1aew.xn--p1ai/reports/item/42989123.

2. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс] // URL: https://cbr.ru/statistics/ib/review_1q_2023/

3. Зампред правления СберБанка назвал город Днепр столицей телефонного мошенничества [Электронный ресурс] // URL: https://www.banki.ru/news/lenta/?id=10954136

4. Мошеннический колл-центр «Бердянск» [Электронный ресурс] // URL: https://www.sberbank.ru/common/img/uploaded/kibrary/investigations/berdyansk.pdf.

5. Обманывали россиян: сеть подпольных колл-центров мошенников раскрыли в Бердянске [Электронный ресурс] // URL: https://tvzvezda.ru/news/2022415259-KxrTx.html.

6. Обзор операций, совершенных без согласия клиентов финансовых организаций [Электронный ресурс] // URL: https://cbr.ru/analytics/ib/operations_survey_2022/.

Айтжанов Жасқанат Ерсайынович,
криминалистика кафедрасының аға оқытушы
з.ғ.м., полиция капитаны, e-mail: jasik_88_shet@mail.ru
(Қазақстан Республикасы ІІМ Б. Бейсенова атындағы Қарағанды академиясы, Қазақстан Республикасы)

АТЫС ҚАРУЫНЫҢ АТУҒА НЕМЕСЕ ЖЕКЕЛЕГЕН АТЫС ЖҮРГІЗУГЕ ЖАРАМДЫЛЫҒЫН ЗЕРТТЕУ ӘДІСТЕМЕСІНІҢ НЕГІЗДЕРІ

Аннотация. Атыс қаруын пайдаланумен жасалған қылмыстарды, оқыс жағдай да атылып қалу оқиғаларын тергеп – тексеру кезінде, сот баллистикалық зерттеудің объектісі болып табылатын қаруларды зерттеудің негіздері қарастырылған. Қарудың дұрыстығы немесе ақаулығы, атуға жарамдылығы, оның ішінде жекелеген оқ атуға жарамдылығы талқыланған.

Түйінді сөздер: атыс қаруы, баллистика, ақаулы, ақаусыз, криминалист – маман.

FUNDAMENTALS OF THE METHODOLOGY FOR STUDYING THE SUITABILITY OF FIREARMS FOR SHOOTING OR INDIVIDUAL FIRING

Annotation. When investigating crimes committed with the use of firearms, incidents and shootings, the court provides the basis for studying weapons that are the object of ballistic research. The accuracy or malfunction of the weapon, suitability for firing, including for individual firing, are discussed.

Keywords: firearms, ballistics, defective, defective, forensic specialist.

Атыс қаруының негізгі мақсаты нысананы зақымдау. Ол үшін қару мақсатына сай болуы, оның белгілі бір қасиеттерге ие болуы қажет, мысалы:

а) баллистикалық;

б) оңтайлылық;

в) қауіпсіз және т.б.

Жағдайлардың басым көпшілігінде зерттеуге зауыттық тәсілмен жасалған, белгіленген өндіріс технологиясына сәйкес қару ұсынылады.

Қару техникалық шарттарға сәйкес болған кезде, оның барлық механизмдері қалыпты жұмыс істейді, ал техникалық шарттардан ауытқуы жағдайында әртүрлі ақаулар пайда болуы мүмкін.

Кейбір ақаулар қарудың жұмысына әсер етуі мүмкін (мысалы, жауынгерлік серіппенің әлсіреуі), кей жағдай да қарудың қалыпты жұмысына тікелей әсер етпеуі мүмкін (тоттану, негізгі емес бөлшектерінің жарылуы: құндақ, саптың және т.б.).

Қару мен оқ - дәрілерді қолдануға қатысты жеке міндеттерді шешу кезінде келесілерді белгілеу ұсынылады:

– аталған қарудан атыстар жүргізу немесе оқ ату;

– аталған қарудың ағытқыш механизмін баспай оқ ату;

– аталған қарудан нысаналы атыс жүргізу;

– аталған патрондармен қарудан оқ ату;

– белгілі бір қашықтықтан, белгілі бір объектіге аталған қару үлгісінен оқ ату арқылы зақым келтіру.

Бұл міндеттерді шешу тек техникалық ақаусыздықты анықтау әдістерін қолдану негізінде мүмкін болады.

Ғылым мен техниканың әртүрлі салаларына қатысты ақаусыз ұғымы әртүрлі мағыналық мазмұнға ие.

Атыс қаруын өндіруші кәсіпорынға қатысты техникалық (зауыттық) ақаусыз деп атыс қаруының техникалық жағдаймен анықталған құрылымдық және баллистикалық өлшемдерге сәйкестігі түсіндіріледі.

Өндірушінің пайымдауы бойынша атыс қаруы шығарылған кезде ақаусыз болуы керек, яғни, барлық өлшемдік, құрылымдық және баллистикалық сипаттамаларға, жиынтыққа, әрлеуге және сыртқы құрылысына сәйкес келетін мемлекеттік немесе фирмалық стандарттар мен өндірістің техникалық шарттарының талаптарына сәйкес келуі қажет.

Бұл тұжырымдама бөлшектердің техникалық құжаттама талаптарына сәйкестігін қамтиды:

– бөлшектер жасалған материалдар;

– оларды термиялық және механикалық өңдеу технологиялары;

– әр бөлшектің өлшемдері;

– әр серіппенің күші;

– механизмдердің бөліктері мен бөлшектерінің өзара сәйкестігі және т. б.

Мұндай сипаттамаларды анықтау үшін тексерудің арнайы әдістері мен тәсілдері, бөліктері мен бөлшектерін тексеру әдістеріне сәйкестігі, тиісті бақылау – өлшеу жабдықтары туралы маманға техникалық терең білімі қажет.

Әрине, криминалистикалық бөлімшелерде мұндай жабдықтармен қамтамасыз етілмеген, ал криминалист – мамандардың аталған міндеттерді шешуге үшін арнайы білімі жоқ.

Әскери – техникалық тұрғыдан алғанда, атыс қаруы, егер оның жұмысына кедергі келтіретін немесе оны қиындататын ақаулары болмаса, жарамды болып саналады.

Бұл ретте қаруды пайдалану деп қарудың жауынгерлік қолданылуы және осы қарудың тұрақты жауынгерлік әзірлігін және оны техниканы дамытудың қазіргі деңгейінде жауынгерлік пайдаланудың барынша тиімділігін қамтамасыз ету үшін әскерлерде жүргізілуі тиіс ұйымдастырушылық - техникалық іс - шаралар кешені түсініледі.

Қаруды ақаусыз пайдалануға кедергі келтіретін ақаулар қару үлгілерінің әрқайсысын жөндеу жөніндегі нұсқаулықта көрсетілген. Егер ақаулар болса, күрделілігіне байланысты жөндеу немесе жарамсыздығын анықтау және жою қажет.

Ақаулар арасында, әскери - техникалық мағынада, тіпті қарудың әртүрлі бөліктеріндегі сандардың бір-біріне сәйкес келмеуі, бұл оларды жоюды және арнайы мөртабандармен немесе электрографиялық тәсілмен жаңа бірыңғай белгілерді енгізуді талап етеді. Сонымен қатар, қаруды пайдалану кезінде рұқсат етілген деп саналатын бірқатар ақаулар бар (мысалы, көздеу құрылғыларынан басқа, құндақ пен металл бөліктерінің жалпы тозуы және т.б.).

Көптеген бөліктер үшін, әсіресе ұңғылар, соққы - ағытқыш бөлшектері мен көру құрылғылары үшін олардың мөлшеріне, бекітудің беріктігіне, өзара әрекеттесуіне және т.б. қатысты қатаң талаптар қойылады.

Әскери – техникалық мағынада ақаусыз қару дәлдігі (шоғырлығы, дәлдігі және т.б.) қойылатын талаптарға сәйкес келуі керек.

Әскери – техникалық аспектідегі атыс қаруының ақаусыздығы тұжырымдамасының мазмұнына өндіруші кәсіпорынға қарағанда қатаң талаптар қойылады.

Әскери – техникалық белгілердің өзіндік ерекшелігі бар, онда оның құзыретіне жатпайтын, криминалист – маманда жоқ нұсқаулықтар мен жабдықтарды білуді талап етеді.

Тәжірибе көрсеткендей, криминалист – маман қойылған міндеттерді шешу үшін нормативтік - техникалық құжаттама талаптарының, сондай - ақ әскери - техникалық ғылымдар мен нұсқаулықтардың негізгі ережелерін білуі керек. Криминалистердің арасында ақаусыздық мәселесін түсіндіру өте қиын. Ақаусыздықты анықтауда екі жақты көзқарас бар.

Кейбір криминалистер (А.И. Устинов, И.А. Дворянский) атыс қаруының ақаусыздығы өндіруші шығарған кезде бағаланатын аспектіде қарастырады.

Сонымен, А.И. Устиновтың пайымдауынша «...техникалық шарттардың талаптарына сәйкес келетін қаруды ғана техникалық тұрғыдан ақаусыз деп санау керек. Техникалық шарттардың талаптарынан кез келген ауытқу қарудың техникалық ақаулығын көрсетеді».

Осы ұсталымға сүйене отырып, тіпті сырлы қаптаманың болмауы қарудан оқ атуға болатынына қарамастан қаруды техникалық тұрғыдан ақаулы етеді.

Екінші жағынан, ағытқыш ілмектің болмауы да ақау болып табылады. Бірақ мұндай ақаулықпен ату мүмкін емес.

Мұндай жағдайларда сот пен тергеу органдары үшін ақаулықтың мәнін қалыптастыру кезінде, қарудың атуға жарамдылығы туралы қорытынды шығаруда, қосымша түсінік қолданылуы тиіс.

Атыс қаруының техникалық ақаулығы туралы мәселені шешу кезінде, криминалист – маманда ғылым мен техниканың қажетті салаларында тиісті дайындықтың болмауына байланысты, оны анықтауға құқығы жоқ.

Мұны істеу қажет болған жағдайларда (мысалы, сапасыз өнім шығару фактілерін тергеу кезінде) баллист - маманның емес, техниктардың, қару - жарақ жасаушылар мен атыс қаруын жасаушылардың білімін пайдалану қажет.

Криминалистердің тағы бір тобы қарудың ақаусыздығы туралы мәселені криминалистикалық мағынада шешуді ұсынады.

Криминалистика саласының ғалымы Б.Н. Ермоленко, бөлшектердің жағдайына қарай, жалпы криминалистикалық зерттеумен қарудың техникалық жарамдылығы туралы мәселені криминалистикалық мағынада шешуді ұсынды. Бұл механизмдердің қалыпты өзара әрекеттесуін, сондай – ақ қаруды берік және қауіпсіз пайдалануды қамтамасыз етеді.

Бұл тәсіл яғни, қалыпты, атуға қауіпсіз әсер ететін ақаулардың болуы немесе болмауы, ақаусыз болып көрінеді, өйткені маман мұндай ақаусыз мәселесін шеше отырып, қарудың техникалық жағдайын арнайы білім көлемінде және одан ату өндірісін қамтамасыз ету тұрғысынан қарудың ақаусыздығы қызығушылық тудыратын, тергеу үшін маңызы бар сұрақтарды зерделейді.

Ақаулықтың криминалистикалық тұжырымдамасы, әскери-техникалық тұжырымдамамен тығыз байланыста болғанына қарамастан, олардың мазмұнымен айтарлықтай ерекшеленеді, демек, ақаусыздық немесе ақаулықты анықтайтын критерийлер.

Сонымен, криминалистикалық мағынада ақаулы - бұл қару, онда атыс өндірісі мен қаруды қалыпты пайдалануды қамтамасыз ететін бөлшектері жоқ немесе ақаулары бар.

Қосалқы бөлшектерінің шамалы ақаулары (тапанша сабының беттерінің сынуы, тапанша антабкасының жұлынуы және т.б.) немесе қосалқы бөлшектерінің болмауы (антабка, құндақ желкесі) қаруды криминалистикалық мағынада ақаусыз деп тануға әсер етпейді.

Жекелеген зауыттық бөлшектерді (шаппа, ағытқыш ілмек, соққыш, аңшылық мылтықтардың шүріппесі және т.б.) ауыстыру, егер бөлшек жеткілікті берік материалдан жасалған болса, ақаусыз орнатылған болса және қарудың нақты данасының тораптары мен механизмдерінің қалыпты өзара әрекеттесуін бұзбаса, қарудың ақаусыз жұмыс істеуіне әкелмейді. Бұл жағдайда маманға металдың қаттылығын, термиялық өңдеу түрін, бөлшектерді дайындау технологиясын және т.б. бағалау қажет.

Атыс өндірісіне әсер ететін бөлшектердің ақаусыз өзара әрекеттесуі де қаруды қалыпты пайдаланудың маңызды шарты болып табылады.

Бөлшектердің өзара әрекеттесуі қарудың нақты үлгісіне, жүйесіне, модельіне нормативтік – техникалық құжаттамамен (Техникалық жағдайы, Нұсқаулық, паспорт) реттеледі.

Жоғарыда айтылғандарға сүйене отырып, криминалистикадағы атыс қаруының дұрыстығы деп оның қауіпсіз және оңтайлылық ату өндірісін қамтамасыз ететін барлық механизмдердің, құрылғылардың және бөлшектердің елеулі ақаулары болмайтын және тиісті нормативтік - техникалық құжаттамаға сәйкес өзара іс-қимыл жасайтын жай-күйін түсіну керек.

Атыс қаруының дұрыстығы санаты ешбір жағдайда қолдан жасалған немесе қолөнерлік тәсілмен жасалған қаруға қолданылмауы тиіс. Атыс қаруының бұл түріне сәйкес келетін нормативтік - техникалық құжаттама жоқ.

Қолөнерлік немесе қолдан жасалған қаруларда нормаларды анықтау мүмкін емес, мысалы, жауынгерлік серіппенің қысылу нормаларын, механизм бөлшектерінің өзара әрекеттесуінің ақаусыздығын және басқа да мәселелерді анықтау.

Қайта жасалған атыс қаруының жарамдылығы туралы мәселені шешу оңайырақ болуы мүмкін.

Ұңғы, дүмбінің қысқартылуы, ұңғы құрылысы өзгертілген қару техникалық жағдайы талаптарына сәйкес келмейді.

Қайта жасалған қару бойынша жарамдылық мәселесі соққы - ағытқыш және сақтандыру тетіктерінің жарамдылығына қатысты шешілуі мүмкін.

Қарудың жарамдылығы туралы мәселе, әдетте, зауыттық тәсілмен жасалған, өзгертілмеген қаруға қатысты ғана шешілуі мүмкін.

Қарудың жарамдылығы туралы мәселені шешудің іс үшін маңызы жоқ, ал тергеу органдары мен сот ол туралы қарудың атуға жарамдылығына, белгілі бір жағдайларда одан кем дегенде жекелеген оқ ату мүмкіндігіне әсер етуі мүмкін ауытқуларға, не онымен жұмыс істеу кезінде қауіпсіздік дәрежесінің төмендеуі, оның абайсызда кісі өліміне немесе денеге зақым келтіру сияқты жазатайым оқиғасына әкелуі мүмкін. Зерттеуді тағайындаудың мәні кез-келген немесе белгілі бір нақты жағдайларда ату мүмкіндігін анықтау болып табылады.

Қарудың оқ атуға жарамдылығын анықтау міндетін тұжырымдауда екі ұғымды бөліп көрсету қажет: қарудың атуға жарамдылығы және қарудың жекелеген оқ атуға жарамдылығы. Бұл ұғымдар тәуелсіз мағынаға ие, сот пен тергеу үшін нақты ақпарат береді.

Қарудың атуға немесе жекелеген оқ атуға жарамдылығын анықтау іс жүзінде ұсынылған қаруды сот - баллистикалық зерттеу үшін міндетті болып табылады. Алайда, іс жүзінде жиі байқалатын бұл ұғымдарды араластыруға болмайды.

Қарудың атуға жарамдылығы деп оның қалыпты мақсатылы пайдаланылу мүмкіндігі, яғни құрылымында көзделген тәсілмен атыс жүргізу мүмкіндігі түсініледі:

а) жекелеген атыс жүргізетін атыс қаруы тек жекелеп оқ атуға мүмкіндік береді.

б) үздіксіз атыс жүргізетін қаруы – тек кезекпен атуға қабілетті

в) сериялық атыс жүргізетін қаруы – тек белгіленген сериялық оқ атуға мүмкіндік беретін ағытқыш механизмі бар автоматты қару

г) аралас атыс жүргізетін қаруы – атыстың бірнеше режимінде оқ атуға болатын қару

Мысалы, егер Калашников автоматынан жекелеген атыс жүргізу мүмкін болмаса, бірақ тек автоматты болса, онда қарудың белгілі бір атыс түріне жарамдылығы туралы айту керек.

Қарастырылмаған әдістер мен амалдарды қолдану арқылы, бірақ оның құрылысы үшін әдеттегі әдіспен емес, қарудан атуға болатындығы, қарудың жекелеген оқ атуға жарамдылығын білдіреді.

«Жекелеген оқ ату» және «бөлек оқ ату» ұғымдарын араластыруға болмайды. Жекелеген оқ ату қалыпты, берілген қару үшін көзделген, яғни оны

мақсатылы пайдалану мүмкіндігін қамтамасыз етеді, ал бөлек оқ ату ақаулы, қалыпты мақсатылы қолдануға жарамсыз қарудан жүзеге асырылады. Кемшіліктердің болуы мұндай қарудан әдеттегі әдістермен оқ атуға жол бермейді.

Оқ атуға жарамдылығы немесе жонылған оқпаны бар қарудан штаттан тыс патрондармен жеке оқ ату туралы мәселені шешкен кезде маман эксперимент жүргізуі керек. Егер қару механизмдерінің бөлшектері нормативтік - техникалық құжаттамаға сәйкес қалыпты түрде әрекет етсе, онда қару атуға жарамды. Бөлшектер мен механизмдердің өзара әрекеттесуі бұзылған жағдайда, штаттан тыс патрондарды қолдануға байланысты (мысалы, оқпаннан оқсауыттың шығарылмауы), қарудың жекелеген оқ атуға жарамдылығы туралы айту керек.

Қарудың жекелеген оқ атуға жарамдылығы туралы қорытынды тергеушілер мен сот үшін қарудың атуға жарамдылығы туралы тұжырыммен бірдей маңызға ие.

Сонымен қатар, егер қарудан жекелеген оқ ату үшін арнайы техникалар немесе дайындық қажет болса, онда оның тек жекелеген оқтарды шығаруға жарамдылығы туралы қорытынды тергеуші мен сотқа қылмыс құрамының субъективті жағын анықтауға мүмкіндік береді: ату кездейсоқ емес, тікелей ниетпен жасалған туралы.

Атыс қаруының сипатына байланысты атыс қаруының әртүрлі кемістіктері (ақаулық) оның атуға жарамдылығын белгілі бір дәрежеде шектеуі мүмкін (мысалы, қайтармалы серіппесі болмаған кезде Токарев тапаншасынан атуды әдеттегідей жүргізу мүмкін емес және т.б.) не орта және алыс қашықтықтағы нысаналы атуға (көздеу құрылғылардың болмауы немесе ақаулары болған кезде). Кейбір кемшіліктердің болуы қаруды әдеттегі техникамен атуға мүмкіндік бермейді, мысалы, ағытқыш тетігінің болмауы атыс қаруының ағытқыш ілмегін басып атуға мүмкіндік бермейді, бірақ шүріппені қайырып және күрт босатқан жағдайда атыс жүргізілуі мүмкін.

Басқа кемшіліктер соншалықты ауыр, оларды жоймай, қарудан ату мүмкін емес.

Соңғы жағдайда мүмкін екі нұсқа:

1) жөндеу нәтижесінде қаруды жарамды күйге немесе кем дегенде жекелеген оқтарды атуға келтірілуі мүмкін;

2) қаруды кем дегенде жекелеген оқ (күшті тоттанудан өзгерген, қарудың негізгі бөліктерін бұзылуы және т.б.) атуға жарамды күйге келтіруге болмайды.

Екінші нұсқада мәселені баллист-маман сәтті шеше алады және түбегейлі қиындықтар туғызбайды, ал біріншісінде бұл әлдеқайда күрделі.

Қаруды атуға жарамды күйге келтірудің нақты мүмкіндігін тек ескере отырып бағалауға болады:

а) криминалист - маманның атыс қаруының техникалық жай-күйі туралы, оны нақтылы емес тұлғаның техникалық жағынан жарамды күйге келтіру мүмкіндігі туралы деректері бар қорытындысы (қандай бөлшектер жетіспейді немесе қолда бар бөлшектер жөндеуді, не ауыстыруды талап етеді, ол үшін

қандай құралдар, материалдар, термиялық өңдеу, тиісті техникалық дағдылар мен біліктілік қажет);

б) кінәлі адамның қаруды жөндеу үшін тиісті біліктілігі мен дағдыларының болуы немесе болмауы;

в) кінәлі адамның техникалық құралдарының болуы немесе болмауы (металл өңдеу білдіктері, термиялық өңдеуге, құралдарға қол жетімділігі);

г) кінәлі адамның жөндеу жүргізу үшін біліктілігінің болмауы, осыған байланысты ол басқа адамдардың көмегіне жүгінеді, не кінәлі адамның біліктілігінің болуы, бірақ техникалық құралдарының болмауы, соның салдарынан ол тиісті біліктілігі мен техникалық құралдары бар адамдардан көмек сұрап жүгінген.

Жоғарыда аталған «б», «г» тармақтарында көрсетілген деректер тергеу жолымен белгіленеді, ал «а» тармағына қатысты кейбір ерекшеліктерді атап өту қажет. Криминалист - маман бар кемшіліктерді анықтап қана қоймай, оларды жою және қаруды атуға жарамды күйге келтіру жолдары мен құралдарын білуі керек.

Мұндай мәселелерді шешуде криминалист – маманға тек сот баллистикасы туралы ғана емес, сонымен қатар металды өңдеу технологиясы және басқа да техникалық ғылымдар туралы білім қажет.

Алёшина Анастасия Валерьевна,
адъюнкт, майор полиции, e-mail: aleshinaav02@yandex.ru
(*Воронежский институт МВД России, Российская Федерация*)

ПРОБЛЕМЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСЛЕДОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. Изучениеличностипреступниканеобходимо в практических целях для эффективной борьбы с преступностью. Подобное изучение позволяет выявить свойстваличности, которые должны стать объектом профилактического воздействия. Рассмотрениекриминологических характеристикквартирных воров 91 показывает, что, в основном, это молодые люди. На долю лиц в возрасте 18 – 24 лет приходится 37 %, в возрасте 25 –31 лет около 22 %.

Ключевые слова: преступление, преступник, личность, криминологическая характеристика, профилактическое воздействие, чужое имущество.

PROBLEMS OF PREVENTION OF PERSECUTION IN THE RUSSIAN FEDERATION

Abstract. The study of the criminal's identity is necessary for practical purposes in order to effectively combat crime. Such a study makes it possible to identify personality traits that should become the object of preventive action. Consideration of the criminological characteristics of apartment thieves 91 shows that, basically, these

are young people. The share of people aged 18 – 24 years' accounts for 37 %, about 22 % aged 25 – 31 years.

Keywords: persecution, prohibited act, criminalization, socially dangerous act, victim, prevention, criminal liability.

Повышенное внимание общественности к преследованию, как к социально-негативному явлению обусловлено изучением одного из самых быстроразвивающихся видов общественно опасной деятельности, не закрепленных российским уголовным законом. Преследование представляет собой умышленные и незаконные действия, которые направлены на притеснение другого человека и совершаются с целью насилия над психикой, вызывая тревожные чувства, опасность за свою жизнь [1, с. 140].

Это обстоятельство не в полной мере отражается в УК РФ и приобретает особую значимость в условиях фиксируемого криминологами существенного смещения насильственных форм воздействия с физической сферы в социально-психологическую сферу, появления новых видов социально опасного психологического воздействия на человека.

Преследование, которое выражается в форме психического насилия над человеком, является одной из наиболее острых социальных проблем, поскольку оно не только отражается непосредственно на самих жертвах, но и дестабилизирует общество в целом, несет угрозу социальному порядку, деструктивно влияет на институт семьи и нравственное состояние общества.

Преследование человека включает в себя следующие виды действий:

– нежелательное слежение за жертвой;

– нежелательное приближение или появление в таких местах, как дом жертвы, рабочее место или школа;

– нежелательное использование технологий сети интернет для мониторинга или отслеживания местоположения жертвы;

– незаконное вторжение в жилище жертвы или средство передвижения (автомобиль), с целью запугивания ее или целенаправленное оставление предметов или осуществление действий, чтобы дать понять, что преследователь находился в этом месте;

– использование технологий (например, скрытой камеры, диктофона, компьютерного программного обеспечения) для слежки за жертвой на расстоянии;

– нежелательные телефонные звонки, включая отправление голосовых сообщений;

– нежелательные текстовые сообщения, электронные письма, сообщения в социальных сетях или фотографий;

– нежелательные открытки, письма, цветы или подарки.

Ольгой Балуковой, жительницей г. Москвы, была подана жалоба в Европейский суд по правам человека (ЕСПЧ) о том, что в течение нескольких лет преследует бывший партнер, который избивал ее и угрожал убийством. Однако, государством защитных мер к гражданке Балуковой принято не было. Согласно жалобе, Ольга в 2018 г. рассталась со своим молодым человеком, близкие отношения с которым длились около трех лет. После расставания бывший парт-

нер до сих пор преследует ее: приходил к дому и месту работы, отслеживал местонахождение, угрожал избиением и даже убийством, распространял ее персональные данные и интимные фотографии в соцсетях. В документе указано, например, что только в 2019 году этот человек звонил Балуковой с 12 телефонных номеров, отправлял письма с девяти электронных адресов, а также угрожал, отправляя комментарии к денежным переводам по 1 руб. через приложение «Сбербанк онлайн». Он преследовал на автомобиле такси заявительницы, когда та возвращалась из аэропорта Домодедово после командировки.

Сотрудниками правоохранительных органов было возбуждено уголовное дело по ст. 119 УК РФ, Балукова была признана потерпевшей, преследователь по уголовному делу проходит свидетелем, однако факты угроз, нежелательных преследований все равно продолжаются, в связи с чем ей и было принято решение об обращении в ЕСПЧ. Ранее Балукова обращалась с ходатайством об избрании в отношении преследующего ее человека меры пресечения в виде «запрета определенных действий» (согласно ст. 105 УПК РФ), с просьбой запрета нахождения рядом с ее домом и офисом. По данному факту был получен отказ с формулировкой, что ее бывший партнер не является подозреваемым или обвиняемым по уголовному делу. Далее, 19 июня 2020 г. Балуковой подана жалоба в Басманный районный суд г. Москвы о нерассмотрении ее заявления о государственной защите, до настоящего времени она не рассмотрена. В жалобе в ЕСПЧ заявительница указывает, что в ее отношении нарушены статья Конвенции о правах человека, запрещающая пытки (ст. 3), о праве на частную жизнь (ст. 8), о праве на эффективное средство правовой защиты (ст. 13) и о запрете дискриминации (ст. 14) [2].

Одной из форм предупреждения и контроля преследования, а так же разновидностью оказания помощи лицам, подвергающихся психическому насилию, может служить профилактическая беседа с виновным, которая заключается в разъяснении лицу, в отношении которого применяются меры индивидуальной профилактики, его моральной и правовой ответственности перед обществом, государством, социальных и правовых последствий продолжения антиобщественного поведения, указанных в ч. 2 ст. 17 Федерального закона Российской Федерации от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации».

Сложности могут возникнуть и с квалификацией действий преследователя. Может быть непросто доказать, что преследователь осуществляет незаконный сбор данных о частной жизни пострадавшей. Факты преследований, такие как запись на камеру телефона или диктофон, скриншоты переписок, сохраненные письма, в совокупности помогут при обращении в правоохранительные органы для формирования доказательственной базы, которая не позволит принять незаконное решение об отсутствии преступления.

Преследование обычно связывают со слежкой, наблюдением или надзором, т.е. действиями, которые представляют всего лишь одну из разновидностей моделей поведения преследователя. Правоохранительные органы, обычно реагируют лишь на происшествия, где наступили общественно-опасные последствия, не изучая контекст, в результате которого эти события произошли. А

преследование отличается от большинства противоправных действий тем, что оно криминализирует «образ поведения», а не отдельное преступное деяние.

В США существуют запретительные приказы (которые также известны как «охранные приказы или ордеры») – это приказы, изданные судом для защиты отдельных лиц, предприятий или широкой общественности от вреда в случаях, когда есть обвинения в домашнем насилии, преследовании, нападении или сексуальном насилии [3]. В литературе можно встретить такие термины как «защитное или ограничительное предписание», «ограничительный судебный приказ», не смотря на разнообразие терминов они имеют цель – защитить жертв от любых видов насилия и преследований. Существующая практикаприменения охранных ордеров за рубежом также предусматривает такие ограничения, как запрет на употребление спиртных напитков и одурманивающих веществ, запрет на хранение и ношение оружия на период действия ордера (Республика Молдова, Республика Армения, Республика Таджикистан) [4, с. 139], [5, с. 203].

В связи с активно развивающимся распространением информационных технологий в современном мире, неизбежно, что преследователь воспользуется преимуществами сети Интернет как средством слежения, шпионажа, распространения порочащей информации, а также угроз различного характера. Взлом учетных записей в социальных сетях и мессенджерах, установка шпионского программного обеспечения на устройстве жертвы (или устройствах, принадлежащих детям), использование встроенного программного обеспечения для отслеживания (например, отслеживание местонахождения мобильного телефона или настройки местоположения в приложениях и геолокациях) позволяет преследователю перехватывать общение жертвы с другими людьми и узнавать, куда идет жертва и что она делает.

Поэтому проблемой, с которой сталкиваются пострадавшие от фактов преследования и решившие обратиться за помощью, является сложность функционирования правоохранительной системы и отсутствие оперативной реакции на поступившее заявление.

Подводя итог, сделанному выше и учитывая опыт зарубежных стран, видится необходимым ввести нормы, устанавливающие уголовную ответственность за преследование, которая должна найти свое отражение в главе 16 УК РФ «Преступления против жизни и здоровья».

Список использованной литературы

1. Криминология: учебное пособие / Под ред. В.Н. Бурлакова, Н.М. Кропачева. – СПб., 2018. – 304 с.

2. Страсбургский суд встал на защиту частной жизни [Электронный ресурс] URL: https://www.kommersant.ru/doc/4538452?utm_source=smi2_agr.

3. Legal Means for Prevention of Stalking [Электронный ресурс] // URL: https://www.legalmatch.com/law-library/article/legal-means-for-prevention-of-stalking.html.

4. Клоченко Л.Н. Психическое насилие: вопросы уголовно-правовой регламентации и квалификации: дис. канд. юрид. наук. – М., 2019. – 206 с.

5. Евсеева Я.В. Перспективы установления охранного (защитного) ордера, как инструмента превенции насилия в семье, в законодательстве Российской Федерации // Молодой ученый. – 2019. – № 48 (286). – С. 203–206.

Ахмадиев Асхат Бектурсынович,
старший преподаватель кафедры кибербезопасности
и информационных технологий
м.ю.н., подполковник полиции, e-mail: ahat.aytzhan.87@bk.ru

Искаков Куаныш Думанович,
старший преподаватель кафедры кибербезопасности
и информационных технологий
м.ю.н., капитан полиции, e-mail: ku.iskakov@kpa.gov.kz

(*Карагандинская Академия МВД Республика Казахстан, Республика Казахстан*)

ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В данной статье рассматриваются такие вопросы, как раскрытие и расследование преступления, которые совершаются с использованием ИТТ (информационно-телекоммуникационных технологий), с приведением различного рода примеров и конкретных ситуаций в быту и в жизни граждан.

Ключевые слова: информационно-телекоммуникационные технологии; расследование преступлений; мошенничество; способы совершения преступлений.

PROBLEMS OF DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Annotation: This article discusses issues such as the disclosure and investigation of crimes that are committed using ITT (information and telecommunication technologies), with the presentation of various kinds of examples and specific situations in everyday life and in the lives of citizens.

Keywords: information and telecommunication technologies; investigation of crimes; fraud; methods of committing crimes.

Преступность – это исторически изменчивое социальное и уголовно-правовое негативное явление, представляющее собой систему преступлений, совершённых на определённой территории в тот или иной период времени. Преступления можно выделить из общей массы преступлений как по формальному (установление за них уголовного наказания, запрет уголовным законом),

так и по материальному признаку (их высокая степень общественной опасности, значимость нарушений) закона и порядка, которые они создают [1, с. 262].

В нынешнее время наблюдается стремительный рост преступлений этого вида. С целью подмены официальных телефонных номеров банковских, социальных и других организаций злоумышленниками используются IP и SIP-телефония. Они размещают на интернет-ресурсах недостоверную информацию о продаже товаров, создают копии интернет сайтов, в том числе платежных систем. Преступники манипулируют потерпевшими, обращаясь к ним с просьбой займа денег под видом знакомых и родственников, попавших в сложную жизненную ситуацию.

Преступники, умело пользуясь доверчивостью граждан, стараются заполучить данные клиентов банков самыми различными способами, как правило, через прямой контакт с потенциальным потерпевшим.

Если человек сообщает мошенникам свои данные для проведения операций (номера карт, логины и пароли для входа в личный онлайн-кабинет, одноразовые СМС-пароли), то у злоумышленников появляется полный доступ к банковскому счету.

Ярким и частым примером являются случаи, когда к вам на телефон поступает либо СМС сообщение, либо звонок от сотрудника службы безопасности банка о том, что ваш счет заблокирован и Вам необходимо сообщить данные карты.

После этого, как гражданин сообщает эти сведения, преступники получают доступ к счету и переводят с него денежные средства.

В ряде случаев, под видом сотрудников служб безопасности банков, либо даже представляясь сотрудниками правоохранительных органов, мошенники просят своих жертв перевести деньги на «резервный счет» для их сохранности.

Конечно же, никакого резервного счета у банка нет и быть не может, мошенники пользуются доверчивостью граждан, которые в итоге сами переводят деньги на их счета.

Например, когда вам звонит мошенник, представившись сотрудникам банка и говорит что ваш счет пытались взломать и необходимо перевести деньги на другой счет, то есть резервный.

Данный вид преступления совершается при активном использовании подмены номера, что позволяет мошенникам имитировать звонки, к примеру, из Алматы, хотя сам человек при этом находится в другом городе. Это дает злоумышленникам возможность успешно маскироваться под сотрудников банковских организаций.

Во избежание таких случаев, даже если поступает звонок с номера телефона, похожего на номер банка, но при этом «сотрудник» просит сообщить конфиденциальную информацию, необходимо просто положить трубку и перезвонить в банк по номеру телефона, указанному на сайте банка или оборотной стороне банковской карты.

В зоне риска оказываются граждане, которые что-то продают или покупают на сайтах бесплатных объявлений или в социальных сетях, а также те, с кем мошенники вступают в переписку со странички «взломанного» друга.

Ни в коем случае нельзя соглашаться на перевод денежных средств за понравившуюся вещь на мобильный телефон продавца, так как, в большинстве случаев это элемент преступной схемы.

Также не стоит обращаться по объявлениям о товаре, цена на который явно занижена. Еще одним высокотехнологичным способом хищения является вирусное заражение компьютеров и мобильных телефонов. Наиболее подвержены вирусной атаке клиенты банков, использующие СМС-банкинг и мобильные банковские приложения на таких устройствах. Вирусы могут распространяться как через СМС, ММС-сообщения, так и через популярные мессенджеры, что резко снижает возможность их выявления со стороны операторов сотовой связи.

Преступления данного вида совершаются следующим образом, владелец смартфона получает сообщение, в тексте которого имеется ссылка, при открытии инициирующая загрузку вирусной программы. Как только вирус попадает в смартфон, он начинает рассылать СМС по контактным листам пользователя. Параллельно он делает запрос на номер СМС-банка и узнает баланс счета владельца смартфона. После этого вирусная программа переводит деньги на счета, подконтрольные злоумышленникам.

Вирус способен перехватывать входящие СМС-сообщения, поэтому владелец смартфона может не знать о снятии денег со счета, ведь оповещения о списаниях не доходят. Кроме того, вирус может открывать окна браузера, визуально похожие на окна авторизации банковских приложений, и при вводе данных своих карт пользователи отправляют средства напрямую мошенникам. В некоторых случаях вирус может блокировать смартфон. С целью защиты электронных устройств от вирусных атак, необходимо обеспечивать их антивирусной защитой.

Таким образом, если раньше преступникам требовалось получить физический доступ к деньгам жертвы, то теперь достаточно получить доступ к конфиденциальной информации. Именно при помощи такой информации, которую граждане зачастую сами охотно сообщают аферистам, последним удается удаленным способом похитить любые суммы денежных средств, вывести их на любые выбранные ими счета и обналичить в любой точке мира.

Реагировать на подобные звонки и сообщения следует спокойно и рассудительно, не поддаваться на уговоры, обязательно проверить информацию. Если вам сообщили о блокировке карты, необходимо обратиться в ближайшее отделение банка, либо по телефону, указанному на банковской карте.

При дистанционном общении важно учитывать, что, если с вас требуют предоплату для выполнения условий договора купли-продажи, устройства на работу, получения выигрыша, в отношении вас совершаются противоправные действия [2].

Однако при осуществлении раскрытия и расследования преступления сотрудники правоохранительных органов зачастую сталкиваются с такими проблемами, как:

1) идентификация владельца сим-карты, с чьего телефона был осуществлен звонок потерпевшему. Данная проблема возникает вследствие использова-

ния неавторизованных сим-карт или сим-карт с внесенными в учетные документы недостоверными сведениями;

2) установление региона нахождения абонента сотовой связи. С данной проблемой сталкиваются сотрудники следственных и оперативных подразделений вследствие отсутствия технической возможности эксплуатируемых систем подключения к ресурсам оператора связи;

3) установление личности абонента IP-телефонии. Проблема связана с отсутствием установленного порядка верификации предоставляемых сведений (как правило, регистрация абонентов производится формально при внесении платежа по присланным по электронной почте персональным данным или скан-копиям паспортов);

4) установление данных соединения о прохождении вызова от абонента IP-телефонии или социальных сетей, использующего VPN-сервисы и адресное пространство операторов связи и интернет-провайдеров стран, не поддерживающих международное сотрудничество правоохранительных органов;

5) установление данных об электронных платежах, совершаемых с использованием интернет-ресурсов.

Это не полный перечень технических проблем, с которыми сталкиваются правоохранительные органы в процессе раскрытия и расследования дистанционных преступлений, совершенных с использованием инновационных технологий. В целях повышения безопасности граждан от преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, целесообразно наладить межведомственное взаимодействие правоохранительных и контролирующих органов, банковских структур, операторов связи, провайдеров сети Интернет, СМИ и организаторов распространения информации. В связи со складывающейся криминогенной обстановкой необходимо пересмотреть концепцию подхода к решению данной проблемы и выработать соответствующую законодательную базу.

Таким образом, в аспекте повышения эффективности расследования указанных преступлений необходимо: проработать вопрос о заключении обязательных соглашений с банками, коммерческими организациями, предоставляющими услуги IP-телефонии, платежными системами, социальными сетями, операторами сотовой связи, провайдерами сети Интернет на предмет осуществления электронного документооборота с подразделениями МВД по направлению запросов и получению ответов в электронном виде посредством ведомственного сервиса электронного документооборота (СЭД) [3, с. 194].

Таким образом, перечень обозначенных вопросов в рамках раскрытия и расследования преступлений, совершаемых с использованием инновационных технологий, конечно же, не является исчерпывающим. Однако рассмотренный комплекс обстоятельств, способствующих совершению указанных преступлений, а также предложенные меры по раскрытию и расследованию данных преступлений помогут совершенствовать общественные отношения в данной области и снизить число таких преступлений на территории Республики Казахстан.

Список используемой литературы

1. Идрисова С.Ф. Современный концепт элитарной преступности // Актуальные проблемы российского права. – 2010. – № 1 (14). – С. 258–266.
2. Как защититься от телефонных мошенников? [Электронный ресурс] // URL: https://ivgazeta.ru/article/2022/11/29/kak_zashchititsya_ot_telefonyh_moshenikov.
3. Костенко Н.С., Семененко Г.М., Пшеничкин А.А. Основные проблемы раскрытия и расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, на современном этапе // Вестник Воронежского института МВД России. – 2020. – № 4. – С. 192–196.

Баймұханов Ербақыт Мухамедкалиевич,
кәсіби-психологиялық даярлық және ІІО басқару кафедрасының бастығы
с.ғ.к., полиция подполковнигі, e-mail: baimuhanov.e81@mail.ru
(*Қазақстан Республикасы ІІМ Б.Бейсенова атындағы Қарағанды академиясы, Қазақстан Республикасы)*

Кадырова Чолпон Айзабековна,
қоғамдық-саяси пәндер және психология кафедрасының бастығы
з.ғ.д., полиция полковнигі, e-mail: kchopa@inbox.ru
(Қырғыз Республикасы ІІМ полиция генерал-майоры Е.А. Алиев атындағы Академиясының, Қырғыз Республикасы)

ҚҰҚЫҚ ҚОРҒАУ ОРГАНДАРЫНДА КИБЕРПОЛИЦИЯ КАДРЛАРЫН ҚЫЗМЕТКЕ АЛУДАҒЫ ЖҰМЫСТЫ ҰЙЫМДАСТЫРУДЫҢ ЕРЕКШЕЛІКТЕРІ

Аннотация. Мақалада киберполиция қызметкерлерінің полиция органдарына қабылдау ерекшеліктері айтылады. Ондағы біліктілік мәселелері, бойларында қандай қасиеттер болу керек осы мәселелер кеңінен талқыланады.

Түйінді сөздер: кибер полиция, кадр деонтологиясы, этика, кадр қызметі.

Annotation. The article discusses the features of the admission of cyber police officers to the police authorities. It discusses the issues of qualification, what qualities they should have.

Keywords: cyber police, personnel deontology, ethics, personnel service.

Әр ұйымның кадрлық қамтуы мамандар іріктеу, яғни «ұйым қажет ететін маман негізіне ие» тұлғалар арқылы жүзеге асады. Мамандық белгі бойынша кадр таңдау, орналастыру, оқыту мен үйрету арқылы барлық жұмыс іске асады. Қажет етілетін мамандық қамту функциясынан кадр болжауы мен құру, оқыту, қайта даярлау, біліктілігін жоғарылату, кадрдың орнын ауыстыру шығады.

Ішкі істер органдар жүйесі қиын және түрлі жұмысты орындау әрі өзін қамтамасыз ету үшін мамандар молдығын қажет етеді.

Кейде «Ішкі істер органдарының қызметкері» мамандығы бар деген сөз естіп жатамыз. Әдетте, баспасөзде бұл ұғымды ішкі істер органдарда ең көп тараған мамандыққа қолданады (полиция қызметкеріне). Мамандық – жұмыс түрі, ал ПБ жүйесі бір адамды теориялық тұрғыдан да барлық қызмет түріне оқыта алмайды. «Теңіз флоты министрлігінің қызметкері», «Ауыр көлік министрлігінің қызметкері» және т.б. деген мамандық жоқ. Барлық бөлімшеде дәрігер, түзетуші, инженер және т.б. жұмыс істейді.

Қызметкер қызметі белсенді түрде этика деп аталатын ғылыммен оқытылады, онда үлкен орынды деонтологиялық кодекс орын алады. Мамандық қызметін реттейтін моральдық қызметін реттейтін моральдық бірлік пен ереже жиынтығы. Танымалы: медициналық этика, журналистика этикасы, полиция этикасы. Бұндай ереже жиынтығы белгілі мамандық иегер қызметін белгілейді, шектеу мен жұмыс уақытындағы істі белгілейді (мамандық құпия сақтауын).

Алдымен «кадр», «кадрмен жұмыс», «кадрмен жұмыс істеу жүйесі» түсінігінің мағынасын ашу қажет. Сондай-ақ «кадр» түсінігі белгілі бір жұмыспен біріктірілген адам жиынын білдіре алады, мысалы, механизатор кадры, техникалық кадр және т.б. Тар мағынада мекеме, ұйым, кәсіпорын кадры туралы айтуға болады. «Кадр» сөзі қызметкердің жеке белгісін айқындай алады, мысалы, жаңа және ескі кадр, маман тиістілігі, мысалы, инженер-техникалық кадр, медициналық кадр, басқару процесіндегі функцияның рөлінде (басқарма, орындау).

Қазіргі таңда кибер полиция қызметкерлерінің қызметіне сұраныс артып отыр. Өздеріңізге мәлім интернет алаяқтық және ақпараттық, сонымен бірге қаржы саласындағы алаяқтық та өршіп тұр.

Бастапқыда «кадр» сөзі тыныш уақытта қарулы күш орталығы, ең алдымен офицерлік корпусты белгілеген. Қазіргі кезде осы мағынада түсініледі.

«Ішкі істер органы кадры» терминін ішкі істер органы белгілеген штат санына сай және сол үшін ақшалай түрде төлемақы алатын, белгілі нормативті-қызметін атқаратын мамандар жинағын түсіну керек. Бұның негізіне мынадай критерий алынған: қызметтік жолы мен қызметкердің орындайтын міндетінің мазмұны; уақыт факторы – үнемді және уақытылы орындалу; құқықтық аспект – органдағы штат саны немесе ішкі жұмыс бөлімшесінде орындалған нормативті қызметтік міндеті; кәсіптік – негізгі мамандық негізінде қызметтік міндетті орындау; ынталандыру – жұмыс қызметі ынтыланады, яғни олар үшін қызметкер үнемі ақшалай қосымша ақы алады [1].

Ішкі істер органы қызметінде кадр түсінігіне арнайы лауазымға қатысты қосымша түсінік енгізу қажет. Нәтижесінде ішкі істер органы кадрында арнайы лауазым болады. Басқару және жай құрылым, курсанттар мен ҚР ІІБ арнайы оқу орындарындағы курсанттар кибер полиция мамандығына оқып жатыр.

Сондықтан ішкі істер органдарында кадр құрамы ішкі істер органы штатының аттестаттауымен айналысатын арнайы тұлғаларға байланысты.

Сондай-ақ кадр біліктілігінде тәжірибелік және теориялық қызығушылыққа ерекше мән беріледі, бұл өз құрамымен жұмыс істегенде өте маңызды.

Ішкі істер органының кадрын арнайы білім даярлығы бойынша бөлуге болады: жоғары білімі, орта, орта арнайы білімімен. Бұл бөлімді арнайы дайындығына қарай бөле аламыз, мысалы, заңгер, азаматтық оқу орындарын бітіргендер (университеттің заң факультетін бітіргендер, заң институты), ҚР ІІБ арнайы жоғары және орта оқу орындарын бітіргендер. Келесі бөлу белгісі қызметкердің жұмыс орнына байланысты. Ішкі істер органы штатының кадр орналасуына байланысты қызмет былай бөлінеді: қатардағы қызметкер, кіші, басқарма саптық бөлімше, инспекторы мен басқарма бөлімі.

Жұмыс саласына қарай кадр бөлінеді: қылмысты іздеу қызметкері, тергеу бөлімі, ДП, еңбекпен түзеу орыны қызметкері және т.б.

Қатысу мен шешім қабылдау жауаптылығына байланысты ішкі істер органы бөлінеді: басшылар, мамандар және техникалық орындаушылар.

Басшылар арнайы лауазымына байланысты кіші, орта, үлкен және жоғары болып бөлінеді.

Кадрмен жұмыс» сөзі шара ұйымдастыру мен техникалық әдісті, ішкі істер органында кадр функция жүйесін орындаумен байланыстының бәрін енгізеді.

«Кадрмен жұмыс» және «кадрмен жұмыс жүйесі» түсінігімен тығыз байланысты, оған негізгі элемент ретінде енеді.

«Кадрмен жұмыс жүйесі» кадрдың барлық сұрағын өзіне енгізеді. Шетел баспасөзінде «қызметкер жүйесі», «карьераны ұйымдастыру» түсінігі көп пайдаланылады, ал олар «кадрмен жұмыс жүйесі» түсінігінің синонимі [2].

Кадрмен жұмыс жүйесі қандай элементтен тұрады?

Орган мен бөлім құрылымы, олармен орындалатын функция түріне байланысты қызметкердің жалпы саны анықталады, олардың лауазым бөлімі, яғни штат болуы. Сондықтан жұмыстың жалпы саны, олардың мамандық даярлауы мен басшылық құрамы кадрмен жұмыс жүйесінің басты элементі. Бұл сатыда қызметкер саны, олардың дайындалу дәрежесі мен қызмет бабы анықталады.

Органның дұрыс дәрежеде жұмыс істеуі үшін оған кім керек деген сұрақпен қоса, олар қандай білім, тәжірибелі болу керегі анықталу керек: қызмет жұмысына сай болу үшін өзіндік сапа қандай дәрежеде болу қажет.

Кадрмен жұмыс жүйесінің екінші элементі негізгі кадр таңдау, орналастыру, қызметке даярлау. Бұл элемент кадрмен жұмыс жүйесінде ең маңызды.

Құқық қорғау органдары жүйесіндегі көтермелеу және жазалау.

Кадр іріктеу өзінің мағанасы бойынша белгілі лауазымға лайық нақты адам таңдаудан тұрады. Сондай-ақ кадр іздеу – қызметкер ұжымын құру. Қызметкер іріктеу мәселесі ұжым тұрғысынан жиналған қызметкер керекті лауазымға сай болмауы мүмкін, бірақ дұрыс орналасқанына байланысты сапалы жұмыс істеу мүмкін.

Кадрмен жұмыс жүйесінің маңызды элементінің бірі – қызметті белсенді шығармашылық жұмысқа жұмылдыру (моральдық және материалдық ынталандыру), қызметкерді ғылыми негізделген саралау, олардың: іскер, моральдық сапалы, еңбек тәртібін нығайту және қызметтің заңдылығын бекіту. Кадрмен жұмыс жүйесінің құрамдас бөлігі – жеке құрамды, маманды даярлау. Ол кадр даярлауынан тұрады. Жалпы алғанда, кадрмен жұмыс жүйесі элементінің сипаттамасы – осы. Олардың әрқайсысы өз кезегінде бірқатар элементтен тұрады.

«Кадрлық жұмыс» ұғымының түсінігінен шықсақ, оларға қойылған міндеттің орындалуын, басқарудың кадрлық қызметін, органның нормалық қызметінің және ішкі істер бөлімшесіне іріктеп алудың: орналастырып қою, оқудың және кадрдың тәрбиелеуі арқылы белгелі бір талапқа жауап беруін қамтамасыз ету сияқты тұрақты басқару функциясын анықтауға болады.

Басқару ғылымының әкімшілік құқықтан айырмашылығы, «кадрдың» кең ауқымды түсінігінен шығуы керек. Бұл түсінік келесі сипаттаманы береді:

– белгілі бір адамның еңбек функциясының тұрақты немесе уақытша орындауы;

– еңбек функцияның ресми нақтылы түрде әлеуметтік жүйе шегінде орындалуы;

– еңбек функцияның қызметтік лауазымды жағдайына байланыссыз кәсіби немесе мамандық негізі ретінде орындауы;

– еңбек қызметінің қайтарымды орындалуы.

Айтылғанға байланысты ішкі істер органының кадрлық қызмет жүйесі, қорғалатын қоғамдық тәртіп және қылмыстылықпен күресу саласындағы басқару үрдісі және жүйесін әлеуметтік жүйе міндетінің атқарылуымен және ҚР ішкі істер органын және оның құрылымдық бөлімшенің еңбек қызметін жүзеге асыру шегінде белгіленген талапқа жауап беретін қызмет ретінде анықталуы мүмкін.

«Кадр» және «кадрлық қызмет» түсінігімен қатар, басқару тәжірибесі және басқару ғылымы «кадрлық саясат», «кадрмен жұмыс», «кадр жұмысы» түсінігі кең қолданылады. Олардың ұқсастығына қарамастан, әрқайсысы кадрлық қызмет тұрғысын анықтай отырып, мазмұндық жүгі телуі болып табылады.

Кадрлық саясат – кадрды құру, қайта құру, пайдалану, таңдап алу стратегиясының қоғаммен жүзеге асуы, заңнамада және мемлекетте бекітіледі. Әрбір басқару жүйесі қажетті кадрлық саясаттың жоғары деңгейде болуы тиіс және осы кадрлық саясатын бастамасын алатын мемлекеттік кадрдың саясатын белгілеп, жүйеленетінін айта кету керек. Кадр саясатының мақсаты – ұзақ мерзімді тапсырманы орындау. Атап айтсақ:

– жақын арадағы жылдарға арналған штаттық сан, олардың құрамы және құрылымы;

– ҚР ІІМ жоғары оқу орнында жоғары және орта мамандығы жүйе бойынша дайындау және оқыту үрдісі;

– қойылған тапсырманы шешуді қамтамасыз ету шегінде ІІО құрылымы мен жүйесін жетілдіру; кадр жұмысының нормативті-құқықтық базасының дамытуы;

– ІІО кадрлық жұмысына ғылыми-зерттеу қызметтің мәселесі бойынша зерттеу;

– өкімет органымен әрекеттесу, жергілікті өзі-өзін басқару кадрлық саясаты кадр саны бойынша жоспарлау көрсеткіші бойынша сан белгілеу, кадр мәселесі ұзақ мерзімді жоспарсыз болса, мәнсіз [3].

«Кадрмен жұмыс» ұғымы шараның барлық кешенін белгілейді, бұл кадрлық қызметпен жүзеге асуымен байланысты. Кадрмен жұмыс – кадрлық саясатты жүзеге асырудың құралы. Онымен қол астындағылар үшін

жауаптылық шегінде барлық тұлға шұғылданады.

«Кадрлық жұмыс» «кадрмен жұмыс» ұғымына ұқсас, бірақ тарлау. Егер де кадрмен жұмысты кез келген бөлімнің басшысы мен ІІО кей қызметкермен жүргізілсе, кадрлық жұмыс кадр іріктеу мен тағайындау, арнайы кадрлық аппарат, басшы функциясы. Кадрлық жұмыс кадрмен жұмыс сияқты кадрлық саясат арқылы жүзеге асырылады.

Қарастырылған түсінік – кадрлық функциядағы бір-бірімен байланысты элемент. Олардың ішінде кадрлық басқару жүйесінің мазмұның «кадрмен жұмыс» түсінігін ашады. Кадрмен жұмыс әр жүйенің маңызды және мәнді бөлігі.

Басқару қаншалықты дамыған және заңды болса, жүйе мен оның басты бөлігі соншалықты тиімді болады.

Басқарманың кадрлық жүйесі қамтамасыз етушіге байланысты. Оның көмегімен жүйенің негізгі талабы орындалады. Кадрлық аппарат өзінің жұмыс аумағында салалық, функционалды, штатты қызмет пен өзінің кадр аппаратына қызмет көрсетеді [4, 121 б.].

Нәтижесінде, кадр қызметі басқарма қоластында олардың әрқайсысы олар баратын жүйесінің кадр саясатын жүргізуге қатысады, кадрмен жұмыс істейді және барлық жұмысты басқарады. Сондықтан кадр функциясы – басшының ажырамас жұмысының бөлігі.

Бұл аумақта басшы оған бағынышты кадр аппараты арқылы әдіс-операция жиынын жүргізеді, басқарма процесс мазмұнын: кадрмен жұмыс саласында басқарма гипотезасын ұсыну, ақпаратпен жұмыс, шешім қабылдайды, орындалуын қадағалайды және нәтижесін санайды. ғни басқа функция сияқты іске асады.

ІІО міндеттемені табысты орындауы кадрды құру, орналастыру, оқыту мен тәрбиелеуге, сондай-ақ жалпы біліміне және маман даярлығына, ойдың дұрыстығы, жалпы және құқықтық мәдениетіне, тәртібі мен орындау қабілетіне байланысты.

«Кадр таңдау» термині қызметке сай талапкердің лайық болуы, қызметті орындай алуы, даярлығын оқыту мен бағалау, салалық, функционалды және штабты ІІО бөлімі лауазымына сай болу дегенді білдіреді.

Таңдау жұмысы мынадай сатыдан тұрады:

– толтыру жұмысы қамтамасыз етілген тұлғалар арасында қойылған талапқа сай тұлға табу;

– бір немесе бірнеше талапкерді таңдау;

– қызметке талапкердің саяси, істік және өзіндік сапасын анықтау;

– ақпаратты өңдеу, жүйелендіру және саралау;

– талапкердің бұрынғы жұмыс орнында жұмыс істегеніне баға беру және жаңа жұмысты орындай алуын жобалау;

– талапкер талпынып жатқан лауазымға сәйкес келе алуын болжау үшін оның сапасы мен талабын салыстыру;

– бірнеше талапкерді салыстыру, олардың лауазым талабына сай екенін анықтау;

– талапкерге лауазымды беру және ҚР кадрына енгізу.

«Кадр таңдау» астында лауазымға сай барлық талапкер арасында мінезі мен құрамы бойынша келетінін таңдау. ІІО жүйесіне кәсіби таңдау әлеуметтік, медициналық белгісі мен білім деңгейі бойынша жүргізіледі.

Бұл шара ІІО-на таңдау жүргізу қамтамасыз етеді: моралдық ұстанымды, барынша дайын кадрды, оларға қойылған міндетті орындай алатын, мемлекет және қызмет құпиясын сақтай алатын. Оны арнайы кадр жоқ кезінде кадр аппарат басқармасы немесе ІІО басқармасы айналасады.

Медициналық белгі бойынша таңдау әскери-дәрігерлік комиссиямен жүр гізіледі, олар қызметке қабылданатындар немесе ҚР ІІБ жоғары немесе орта білім мекемесі оқуына түсушілерді қарайды. Кадр аппараты кадр таңдау мен орналастыру кезінде талапкердің жеке сапасы мен мінезіне назар аудару қажет. Бұл талап есептелуі талапкердің лауазымға сай екені туралы жобалап айтады. Бұдан басқа тек қана жеке белгіні ғана есте сақтамай, тұлға аралық және топта психологиялық ауа райын есептеу керек [5, 38 б.].

ІІО кадр лауазымға тағайындау арқылы толықтырылады. Тағайындау туралы шешімді басшы қабылдайды. Адамды бағалауда субъективизмді болдырмау үшін кей тұлғаға тиесілі, топтық шешім қабылдауды енгізу керек.

Психологтар айтуынша, адамға саяси, өзіндік, іскерлік бойынша баға бергенде тәуелсіз сипаттауды қолданған жөн, оның мағынасы бірнеше адам бірбірінен тәуелсіз белгіленген сызба бойынша бірнеше адамды сипаттайды.

ІІО кадрмен толықтыру мағынасы қажет етіліп отырған лауазыммен қамту қажет, қойылатын талапқа сай бола алатын. Кадрды орындарына қою негізі – басқарма аппарат бөлімшесіне қызметкерді дұрыс орналастыру. Кадрды таңдау туралы лауазымды толықтыру керектігі кезінде, ал орындарына тұрғызу күш қолдану кезінде сөз болады.

ІІО кадрдың толықтыру мен орналастыру ерекшелігі – әр қызметтің полиция сияқты болса да әлеуметтік ортаға басқарушы ретінде әсер етуі. Ал бұл үшін тиесілі сапа қажет, яғни лауазымға талапкерге ерекше талап қойылады.

ІІО-да талапкердің дайындығын бағалау үшін оның диалектикалық бірліктегі саяси және іс сапасы, моральдық бейнесі мен өзіндік мүмкіндігіне назар аудару керек [6, 217 б.].

ІІО кадрмен жұмыс істеу жағымды тәжірибеде жинақталды. Олардың топтасуы болашақ қызмет үшін таңдау ережесі мен кадр орналастыруын құрауға мүмкіндік береді. Оларға мыналар жатады:

1) болашақ қызметке талапкердің мінезінің сәйкес келуі;

2) қызметкер мен оның жақын көмекшісі сапасы бір-біріне үйлесімді;

3) тәжірибелі және жас кадрлардың ақылды үйлесімділігі.

Талапкердің болашақ жұмысына мінезі бойынша сәйкес келмеуі себебінің бастысы оның бұрынғы жұмыстағы тәжірибесі болашақ жұмыста табыстылықты кепілдемейді.

Салалық қызметке басшы таңдаған кезде ең алдымен келешек жұмысы бойынша білім мен тәжірибе барына назар аудару қажет. Бұл талап болғанмен, кейде оған назар аудармайды.

Мамандардың айтуынша бөлім басшысын тағайындаған кезде ол келесі талапқа сай болу керек:

1) жоғары заңгерлік білім, әсіресе ІІМ бағыты бойынша;

2) ІІО жұмыс тәжірибесі 10 жылдан кем емес, соның ішінде 4-5 жыл жедел-іздестіру жұмысында;

3) жедел бөлім басшы тәжірибесі болу керек, ал ол басқарған бөлім қылмысты сақтандыру мен ашу бойынша үнемі жоғары көрсеткіш көрсету керек;

4) қызметкердің үлкен саны бар жедел шараны ұйымдастыра және жүргізе білу қажет;

5) талдамалық жұмысқа бейімділік;

6) қызмет басшысы, қала, аудан басшылары, қарамағындылармен жақсы іскерлік қатынас құруы;

7) бағыныштыларды үнемді оқытып, оларға қамқорлық көрсету;

8) жеке құрамының тиімді жұмысын қамтамасыз етіп, топта дұрыс ахуал орнатып, қызмет тәртіптің бұзылуын және т.б. болдырмау керек;

9) өз мысалында бағыныштыларға жұмысқа адалдығын, тәртіп сақтаушылықты және заңға талаптылықты көрсету керек.

Мұндай белгіге ие болу үшін төменгі бөлімде жұмыс істеу қажет. Сондықтан басқару кадрмен жұмыс істегенде жұмыс баспалдағы бойынша «қарапайымнан киынға» көтерілу қағидасынан таймау керек.

Басшыны тағайындаған кезде қызмет ерекшелігін, нақты уақытта топ қандай күйде, бөлім ұзақ мерзім ішінде шешетін тапсырма ерекшелігін ескеру қажет. Басшы мен оның жақын көмекшілері бір-біріне сай болса, бұл өте жағымды [7, 83 б.].

Қорыта келгенде, басқарушының, еңбектің ғылыми ұйымдастырылуы толықтай ІІО кадр аппаратына жататынын белгілеу қажет. Осыған қоса кадр функциясының саяси мәні, оның басқа да функция орның анықтағанда әлеуметтік тәртіпті сақтауы мен қылмыспен күресу кадрлық аппараттың тиімді ұйымдасуы мен үнемді жетілуінсіз мүмкін емес [8, 19 б.].

Кадрлық мәселенің тиімді шешілуі орган мен қызмет басшыларының тәжірибелігіне байланысты, бірақ олардың барлығы бұған ие емес. Бұл кезде тәжірибелі және жас кадрдың үйлесімділігі өте маңызды.

Ішкі істер органдарының міндеті

Қазақстан халқына қызмет етуге тиісті ішкі істер органы қоғамдық қауіпсіздікті қамтамасыз ету мақсатында мынадай міндетті жүзеге асырады:

1) құқық бұзушылық профилактикасы;

2) қоғамдық тәртіпті сақтау;

3) қылмыстылықпен күрес;

4) қылмыстық жазаны және әкімшілік жазалауды орындау;

5) төтенше жағдайдың алдын алу және оларды жою, өрт қауіпсіздігін қамтамасыз ету, азаматтық қорғанысты ұйымдастыру.

Қазақстан Республикасының заңы және Қазақстан Республикасы Президентінің актісімен ішкі істер органдарына өзге де міндет жүктеледі.

Ішкі істер органдарының құзыреті.

Ішкі істер органы Қазақстан Республикасының заңнамасына сәйкес өздеріне жүктелген міндет шегінде:

1) құқық бұзушылық жасауға ықпал ететін себеп пен жағдайды анықтауға, зерделеуге, жоюға бағытталған шара кешенін жүзеге асырады;

2) қоғамдық тәртіпті сақтау жөніндегі шара кешенін жүзеге асырады;

3) жол жүрісіне және оның қауіпсіздігін қамтамасыз етуге мемлекеттік бақылау мен қадағалауды жүзеге асырады;

4) азаматтық және қызметтік қару мен оның патронының айналымына мемлекеттік бақылауды жүзеге асырады;

5) күзет қызметі саласында мемлекеттік бақылауды жүзеге асырады;

6) мемлекеттік күзетілуге жататын жеке тұлға мен объектіні күзетуді жүзеге асырады;

7) террористік тұрғыдан осал объектінің терроризмге қарсы қорғалуының жай-күйін бақылайды;

8) азаматтық, халықтың көші-қоны және босқындар саласындағы мемлекеттік саясатты іске асырады;

9) жеке басты куәландыратын құжатты дайындауды, сондай-ақ жеке сәйкестендіру нөмірінің ұлттық тізілімін жүргізуді жүзеге асырады;

10) лицензия және рұқсат беру қызметін жүзеге асырады;

11) әкімшілік құқық бұзушылық туралы іс бойынша іс жүргізуді жүзеге асырады;

12) қылмыстық құқық бұзушылықты ашуды және тексеруді жүзеге асырады;

13) жедел-іздестіру қызметін және жасырын тергеу әрекетін жүзеге асырады;

14) зерттеуді жүзеге асырады;

15) іздестіруді жүзеге асырады;

16) есірткі, психотроптық зат, прекурсор айналымы саласындағы мемлекеттік саясатты іске асыруды және олардың заңсыз айналымына және оларды теріс пайдалануға қарсы іс-қимылды жүзеге асырады;

17) қылмыстық процеске қатысушы адамдарды мемлекеттік қорғауды жүзеге асырады;

18) қылмыстық-атқару қызметі саласындағы мемлекеттік саясатты іске асырады, адамдарды ішкі істер органының арнаулы мекемесінде ұстауды жүзеге асырады;

19) мемлекеттік қызмет көрсетеді;

20) халықаралық ынтымақтастықты жүзеге асырады;

20-1) азаматтық қорғау саласындағы мемлекеттік бақылауды жүзеге асырады;

21) Қазақстан Республикасының заңында, Қазақстан Республикасы Президенті және Қазақстан Республикасы Үкіметінің актісінде көзделген өзге де өкілеттікті жүзеге асырады.

Пайдаланған әдебиеттер тізімі

1. ҚР ІІМ 2021 жылдың 26 ақпандағы «Қазақстан Республикасы Ішкі істер органдары жүйесіндегі тұрғын үй-жайды жалдау және жол жүру жөніндегі

қызметтік іссапарға арналған шығысты өтеу тәртібін бекіту туралы» № 111 бұйрығы.

2. ҚР ІІМ 2021 жылдың 17 наурыздағы «Қазақстан Республикасы Ішкі істер министрлігінің идеологиялық жұмысының тұжырымдамасын және Қазақстан Республикасы Ішкі істер органдарында идеологиялық жұмысты ұйымдастыру тәртібі туралы басшылықты бекіту туралы» № 155 бұйрығы.

3. ҚР ІІМ 2021 жылдың 01 сәуірдегі «ҚР Ішкі істер органдарына қызметке қабылдау, лауазымға тағайындау, ауыстыру, қызмет бойынша жоғарылату, демалыс беру, арнайы атақтар беру, қызметтен шығару және іс сапарға жіберу туралы Нұсқаулықты бекіту туралы» № 190 бұйрығы.

4. Артамонов В.С. Основы управления в органах внутренних дел: курс лекции. – М., 2012. – 249 с.

5. Кемел М., Бакирбекова А.М. Управление персоналом в государственной службе: учебное пособие. – Алматы: ЭКОНОМИКА, 2015. – 244 с.

6. Коренев А.П. Основы управления в ОВД: учебник. – М.: Щит-М, 2000. – 343 с.

7. Мишковсқая В.В. Основы управления в органах внутренних дел Республики Қазахстан: альбом-схем. – Караганды: Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, 2017. – 135 с.

8. Петрова О.В. Методология принятия управленческих решений: учебное пособие. – М.: Академия управления МВД России, 2020. – 92 с.

Баймырза Диана Қанатқызы,
магистрант факультета послевузовского образования
старший лейтенант полиции, e-mail: dikosya.99@mail.ru
(Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, Республика Казахстан)

ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОГО ФОРМАТА ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация. В данной статье автором рассматривается вопрос досудебного расследования в электронном формате. Особое внимание уделено применению данной формы расследования по киберпреступлениям. Автором были изучены виды преступлений в сфере информационных технологий и вопрос возможности проведения расследования по ним в электронном формате. Рассмотрены технические средства, соответствующие программы, платформы, используемые в расследовании. Целью данной работы является выявление проблемных аспектов использования электронного формата при расследовании киберпреступлений, а также установления главных проблемных вопросов противодействия киберпреступности в целом. В результате написания данной статьи предполагается внесение конкретных предложений по разрешению вышеуказанных проблем.

Ключевые слова: электронный формат, расследование киберпреступлений, технические средства, проблемы применения электронного формата, информационные технологии.

THE USE OF ELECTRONIC FORMAT IN THE INVESTIGATION OF CYBERCRIMES

Abstract. In this article, the author considers the issue of pre-trial investigation in electronic format. Particular attention is paid to the use of this form of investigation of cybercrimes. The author studied the types of crimes in the field of information technology and the question of the possibility of conducting an investigation on them in electronic format. Technical means, relevant programs, platforms used in the investigation are considered. The purpose of this work is to identify problematic aspects of the use of electronic format in the investigation of cybercrime, as well as to identify the main problematic issues of countering cybercrime in general. As a result of writing this article, it is expected to make specific proposals to resolve the above problems.

Keywords: electronic format, investigation of cybercrimes, technical means, problems of using electronic format, information technology.

21 век – век высоких технологий. Сегодня за очень короткие сроки происходят большие скачки в развитии человечества. Каждый день изобретаются новые информационные технологии. Главной целью каждого IT-продукта является упрощение жизни для людей. Тот или иной гаджет или приложение нацелено на выполнение некоторых функций, которые прежде люди выполняли вручную. Казалось бы, такого рода прогресс является очень полезным явлением для всего Мира. Но у информационного развития есть и отрицательные стороны. Наряду с другими технологиями развиваются и технологии совершения преступлений. Большое количество преступлений перешли в информационную среду. Сегодня их стали называть киберпреступлениями.

До сих пор в Уголовном кодексе нет определения «киберпреступление». В современной юридической литературе под «киберпреступлениями» понимают «преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами», «преступления в высоких компьютерных технологиях», «преступления в информационном пространстве» и т.д. [1]

В 2017 году в УПК РК была введена статья 42-1 «Формат уголовного судопроизводства» [2]. В ней говорится, что в Республике Казахстан с учетом мнения участников уголовного процесса судопроизводство может вестись в бумажном и (или) электронном форматах. Порядок ведения расследования уголовных дел в электронном формате регламентируется инструкцией [3].

Как сообщается Комитетом по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан, в электронном формате расследуется более 134 тыс. уголовных дел, что составляет более 90 % от общего

количества дел, находящихся в производстве органов досудебного расследования [4, с. 165].

Ведение электронного судопроизводства заключается в осуществлении досудебного расследования в электронном формате, в том числе путем ввода электронного документа либо вложения PDF-документа в ЕРДР на основании принятых должностным лицом процессуальных решений и действий, а также заполнения необходимых реквизитов электронных информационных учетных документов, подписываемых ЭЦП.

В условиях постоянно развивающихся цифровых технологий широкий спектр киберугроз может иметь серьезные последствия для бизнеса, если не защитить его должным образом. Понимание различных типов киберпреступлений (начиная с вредоносных программ и программ-вымогателей и заканчивая фишингом и кражей личных данных) – является первым шагом для обеспечения безопасности своей компании.

Виды киберпреступлений: фишинг, взлом (хакерство), криптоджекинг, спуфинг, программы-вымогатели, межсайтовый скриптинг, кража личности, мошенничество, вредоносные программы, социальная инженерия, взлом IoT-устройств, компьютерное пиратство, трояны, подслушивание (англ. «Eavesdropping»), DDoS-атаки, усовершенствованные постоянные угрозы (APT), Black Hat SEO. Самым распространенным среди киберпреступлений является так называемое интернет-мошенничество (п.4 ч.2 ст.190 УК РК) [5].

Если рассматривать вопрос расследования таких преступлений в электронном формате, то можно прийти к выводу, что, при наличии у преступников достаточных знаний, умений и навыков для совершения вышеуказанных деяний, у них наверняка может появится возможность взлома системы ЕРДР. В случае кибератаки на данную базу, у них может появиться возможность на удаление определенных материалов либо уголовных дел в целом, а также возможность изменения данных в электронных процессуальных документах. Конечно, Генеральная прокуратора позаботилась о безопасности системы ЕРДР от таких угроз, но все же риск остается. В таком случае может возникнуть необходимость расследования данной категорий уголовных дел именно в традиционном бумажном формате.

Очень тяжело квалифицировать вышеуказанные виды преступлений, так как данные деяния зачастую не подпадают под диспозиции статей УК РК. В некоторых статья УК просто имеется квалифицирующий признак «совершенное путем использования информационно-телекоммуникационных сетей Интернет» и т.п. Большинство представленных видов преступлений можно подвести под квалификацию как интернет-мошенничество.

Расследование данной категории преступлений проводится в основном в электронном формате. Связано это не только со спецификой самого преступления, но и с требованиями со стороны контролирующих и надзорных органов. В целом, сегодня уже смело можно утверждать, что интернет-мошенничества расследуются в электронном формате и довольно-таки успешно. В суд направляются многоэпизодные уголовные дела, по ним принимаются судебные решения.

Но если углубляться в суть данных преступлений, то назвать их именно интернет-мошенничеством очень сложно. Зачастую раскрываются именно простые мошенничества. Поводом для отнесения их именно к киберпреступлениям является форма контакта преступника и жертвы (посредством мессенджеров и мобильных приложений). Согласно УК, эти преступления подпадают под квалификацию именно как интернет-мошенничество. Исходя из этого статистические данные не совсем отражают действительность. Руководству страны докладывается криминогенная обстановка, где делается отметка на раскрытие киберпреступлений. Но по факту раскрытие именно настоящих киберпреступлений оставляет желать лучшего.

Стоит отметить, что расследование киберпреступлений предполагает собой наличие знаний в области информационных технологий и информационной безопасности. В следственно-оперативных подразделениях правоохранительных органов нашей страны большой дефицит кадров, которые так или иначе имеют познания в этой области. Для решения данной проблемы практически в каждом Департаменте полиции открылись специальные отделы – киберпол. Казалось бы, что пути решения насущных проблем были найдены. Но опять же, проблемы решаются только визуально. Стоит отметить квалификацию специалистов, работающих в киберполе. Как правило туда отправляют сотрудников из районных отделов полиции. Каждый руководитель районного отдела полиции не хочет отдавать своего ценного сотрудника, даже наоборот пытается избавиться от «балластов». Получается, в киберполе работают те лица, которые не нашли себе место в районном отеле. Данный пример не распространяется на все области. Но все же проблема с квалифицированными кадрами остается.

Настоящие IT-специалисты очень редко идут на работу в правоохранительные органы, в связи с тем, что оплата не соответствует труду. Обучать действующих сотрудников очень трудно, так как с возрастом восприятие современных технологий затрудняется. На базах академий МВД открыты специальные кафедры и полигоны, но имеется дефицит преподавателей-специалистов.

Для расследования киберпреступлений, в том числе в электронном формате, применяется практически та же техника, что и для расследования обычных преступлений. К таким приспособлениям относятся: Компьютер с двумя мониторами, МФУ, стиллус, сканнер и тд. и т.п. Особенностью раскрытия и расследования киберпреступлений является необходимость производить изъятие информационных ресурсов. Для этого также необходимы специальные носители. Также стоит отметить необходимость специальных программ по восстановлению удаленных файлов, программ по обходу вредоносных программ и т.п.

Подводя итоги данной работы, мы пришли к выводу, что вопрос расследования киберпреступлений в электронном формате плохо проработан с точки зрения организации работы, а также отсутствия тактики и методики расследования. Вопрос алгоритма расследования в электронном формате вполне сопоставим с расследованием обычных преступлений.

Исходя из вышеизложенного предлагаем:

– усилить подбор кадров для работы в киберполе;

– усилить подбор кадров для работы на киберкафедрах;

– усилить контроль над статистическими данными.

Рассмотреть вопрос об отнесении преступлений, совершенных путем использования мессенджеров и интернет-приложений к обычным преступлениям.

Рассмотреть вопрос о расследовании уголовных дел по киберпреступлениям только в бумажном формате, в целях профилактики кибератак на систему ЕРДР.

Список использованной литературы

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V // Казахстанская правда. – 2014. – 10 июля.

2. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V // Казахстанская правда. – 2014. – 9 июля.

3. Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате: приказ Генерального прокурора Республики Казахстан от 3 января 2018 г. № 2 // Эталонный контрольный банк НПА Республики Казахстан в электронном виде. – 2018.

4. Кочкина Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. С. 162–169.

5. Более 90 % уголовных дел расследуется в электронном формате [Электронный ресурс] // URL: https://www.zakon.kz/sobytiia/6022917-bolee-90-ugolovnykh-del-rassleduetsia-v-elektronnom-formate.html.

Басханов Ахмед Магомедович,
преподаватель кафедры уголовного права учебно-научного комплекса
по предварительному следствию в органах внутренних дел
капитан полиции, e-mail: axmed.basxanov.95@mail.ru

Грицианова Кристина Петровна,
слушатель факультета подготовки следователей
младший лейтенант полиции,

(Волгоградская академия МВД России, Российская Федерация)

ФЕНОМЕН «КИБЕРБУЛЛИНГ»: АКТУАЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Аннотация. Статья посвящена анализу понятия «кибербуллинг» и его форм. Данное негативное явление в настоящее время начало набирать обороты среди молодежи и, соответственно, становится объектом изучения правоведов. В работе анализируются аналитические данные, приведенные ВЦИОМ России, статистические данные МВД России. Авторами рассматриваются проблемы, которые появились в обществе и государстве, а также пробелы в законодательстве, сформулирована оригинальная позиция по урегулированию этих проблем.

Ключевые слова: кибербуллинг, троллинг, сталкерство, травля в интернете, кибербезопасность, законодательство, преступление.

THE PHENOMENON OF «CYBERBULLYING»: CURRENT PROBLEMS AND SOLUTIONS

Annotation. The article is devoted to the analysis of the concept of «cyberbullying» and its forms. This negative phenomenon has now begun to gain momentum among young people and, accordingly, is becoming an object of study for legal scholars. The paper analyzes the analytical data provided by VTSIOM of Russia, statistical data of the Ministry of Internal Affairs of Russia. The authors consider the problems that have appeared in society and the state, as well as gaps in legislation, and formulate an original position on the settlement of these problems.

Keywords: cyberbullying, trolling, stalking, harassment on the Internet, cybersecurity, legislation, crime.

Подключение к Интернету важно, поскольку оно обеспечивает как образовательные, так и социальные преимущества для молодежи. К сожалению, эти положительные качества уравновешиваются потенциально опасными последствиями. Наряду с улучшением коммуникации и демократизацией доступа к информации, Интернет позволяет людям скрываться за маской анонимности. Это создает совершенно новый набор рисков для детей, а зачастую и для взрослых. Это делает кибербуллинг темой, о которой должны знать все родители и опекуны. Стоит учитывать, что чаще всего издевательства происходят в школьные годы, когда молодежь не имеет представлений о толерантности и личном пространстве других людей. Эти инциденты могут варьироваться от простого оскорбления до более серьезных актов запугивания, таких как распространение слухов, преследование, угрозы и случаи нанесения физического вреда.

Кибербуллинг – это растущая социальная проблема, которая стала слишком распространенной в онлайн-сообществах. Исследования показывают, что каждый пятый подросток подвергался кибербуллингу, в то время как 59% подростков подвергались домогательствам в Интернете. И скорость, с которой происходят онлайн-издевательства, похоже, не снижается [1]. В разгар пандемии COVID-19 «кибербуллинг» усилился. Исследования показывают, что во время выполнения заказов на дому кибербуллинг увеличился на 70%, а токсичность на игровых платформах онлайн увеличилась на 40% [2]. Эти цифры показывают, что, несмотря на повышение уровня образования и совершенствование программ профилактики издевательств в школах, случаи киберзапугивания продолжают расти.

Поэтому правоохранительным органам необходимо сделать все возможное, чтобы предотвратить киберзапугивание [3].

Термин «кибербуллинг» был введен психологами в середине 1990-х годов для описания издевательств в онлайн-пространстве, как раз в то время, когда Интернет поразил массы. Кибербуллинг может принимать различные формы, начиная от оскорблений и преследования, шантажа, преследования, клеветы и

кражи личных данных. Все формы, упомянутые выше, могут нанести психологическую травму жертве.

Кибербуллинг оставляет жертвам мало возможностей для самозащиты. Кибербуллинг также может быть анонимным, не оставляя жертве возможности даже сообщить о преступнике правоохранительным органам. Кибербуллинг может продемонстрировать случаи издевательств сотням или, возможно, даже тысячам, в течение короткого периода времени, используя платформы социальных сетей.

Кибербуллинг в Интернете существует в различных формах и под разными названиями:

1. Троллинг. Это не совсем запугивание, а скорее своего рода «жесткий вызов» и «соревнование» в юморе. Как правило, троллю все равно, с кем и как долго «соревноваться». Если в ответ приходит более остроумное замечание или, если комментарий полностью игнорируется, «юморист» отправится в другое место в погоне за признательностью и признанием.

2. Прессинг. Также еще не является преследованием. Это единичная вспышка гнева по отношению к человеку, которая выражается оскорбительным комментарием или резкой критикой. Как правило, авторам таких грубых сообщений ответ не нужен. Они изливают свою реакцию на определенный продукт (например, сообщение, статью, видео, фотографию и т. д.) И двигаются дальше, немедленно забывая о вашем существовании [4, с. 218].

3. Преследование. Оно происходит от слова «ненависть» и обозначает полноценное преследование человека в онлайн-пространстве. Жертву буквально засыпают оскорбительными сообщениями и комментариями через социальные сети, мессенджеры, видеохостинги и т.д.

4. Сталкерство. Отличается от преследования тем, что издевательства происходят с явным сексуальным подтекстом. Человек начинает получать на электронную почту, в социальных сетях или на телефон в мессенджерах сообщения с фотографиями и видео сексуального характера, а также неуместные звонки и сообщения. Это может иметь место как форма мести, при которой бывший парень или девушка начинают угрожать загрузить фото или видео файлы интимного характера жертвы, чтобы все видели.

5. Диффамация (оскорбление). Это распространение недостоверной информации и слухов о жертве с целью нанесения максимального ущерба ее репутации. Для этой цели могут быть созданы специальные чаты, отфотошопленные изображения и сообщения с искаженной информацией.

6. Кража личных данных. Происходит путем взлома страницы пользователя или создания ее копии и распространения негативной ложной информации. Оскорбительные сообщения также могут быть отправлены друзьям, учителям (в случае школьников) от имени жертвы.

7. Бойкот. Часто происходит в реальной группе людей. Жертва исключается из публичных групп и чатов, лишая их возможности участвовать в обсуждениях и выражать свое мнение. Любая мелочь, которая отличает ребенка от остальной группы, может стать поводом для бойкота.

8. Публикация личной информации. Это относится к любой информации, опубликованной в Интернете о человеке, которая не является общедоступной и может иметь серьезные последствия для жертвы. Например, достаточно «слить» домашний адрес известного человека, чтобы причинить ему большие неприятности, вплоть до того, чтобы заставить его сменить место жительства. Более того, загрузка фотографий интимного характера или источника дохода в Интернете без разрешения человека тоже является формой издевательств.

9. Открытые атаки и угрозы причинения вреда. Это комментарии на страницах аккаунта в социальных сетях и сообщения, которые содержат описания физического насилия в прямой или косвенной форме, часто доходящие до попыток выследить жертву в реальном мире.

Конечно, многие воспримут данные формы смешными и не опасными, но, к сожалению, угрозы, которым могут подвергаться подростки имеют серьезные последствия: проблемы с психическим здоровьем, повышенный стресс и беспокойство, депрессию, жестокие действия и низкую самооценку. Кибербуллинг также может привести к длительным эмоциональным последствиям, даже если издевательства прекратились. Эти последствия киберзапугивания могут привести к стойкому чувству смущения. Онлайн-издевательства кажутся более постоянными, особенно когда они осуществляются через сообщения в социальных сетях, которые не сразу исчезают. Это может привести к подавляющему чувству незащищенности и дистресса.

Также за последнее десятилетие наблюдается тревожный рост числа подростковых самоубийств. Фактически, как показывают данные CDC, в 2020 году самоубийство было одной из четырех основных причин смерти людей в возрасте от 10 до 44 лет. Однако здесь есть небольшой прогресс: самоубийство было второй по вероятности причиной смерти среди 15-24-летних в 2019 году, но в 2020 году оно опустилось на третье место [5, с. 5].

В зависимости от способа кибербуллинга его участниками могут выступать люди различных возрастных групп.

Так, согласно исследованию РАЭК 2017 года, подростки 14-17 лет чаще других сталкиваются с «кибersталкингом» (44%), «хейтингом» (69%) и «троллингом» (65%). Молодежь же в большинстве своем становится свидетелями или жертвами «флейминга» (73%) [6]. Чаще всего «кибербуллинг» начинается в школьной среде. При этом прежде всего, огромный ущерб наносится психике подростка. Это может привести к такому серьезному последствию, как суицид. За первое полугодие 2021 года в России было зафиксировано 3064 попытки самоубийств и завершенных суицидов. Это на 43 процента больше, чем в 2020 году. При этом 80 % суицидов происходит из-за «кибербуллинга» [7].

Исследование, проведенное в 2022 году Институтом мозга «Lifespan», показало, что быть жертвой киберзапугивания соответствует увеличению частоты суицидальных мыслей, хотя быть преступником – нет. Это отражает исследование 2018 года, которое показало, что молодые люди в возрасте до 25 лет, ставшие жертвами киберзапугивания, в два раза чаще совершали самоубийства или причиняли себе вред другими способами [8].

Кроме того, исследование, представленное на собрании педиатрических академических обществ 2017 года, показало, что число детей, госпитализированных в больницы за попытку самоубийства или выражение суицидальных мыслей, удвоилось в период с 2008 по 2015 год [9].

Еще одна проблема связана с тем, что «кибербуллинг» может оставаться незамеченным в течение длительного времени и происходить анонимно, что делает его еще более опасным и трудным для выявления и пресечения.

Кроме того, в некоторых странах, включая Россию, отсутствует специальное законодательство, которое бы наказывало «кибербуллинг». Это может привести к тому, что жертвы остаются беззащитными и не могут обратиться за помощью к правоохранительным органам.

Итак, мы видим, что существуют различные формы «кибербуллинга» и имеют они разные названия. Стоит отметить, что в действующем Уголовном кодексе Российской Федерации отсутствует специальная норма, которая бы предусматривала ответственность непосредственно за «кибербуллинг».

Ответственность наступает лишь за определенные последствия – доведение до самоубийства, угроза убийством или причинением тяжкого вреда здоровью, клевета и т.д. Именно отсутствие специальной нормы, которая бы предусматривала ответственность за «кибербуллинг», является серьезной проблемой и пробелом в уголовном законодательстве России.

Полагаем, что необходимо выработать комплекс мер по профилактике и предупреждению данного явления среди молодежи. При этом считаем целесообразным сформулировать новое определение «кибербуллинга», адаптировав его под требования Федерального закона от 28.02.2023 № 52-ФЗ «О внесении изменений в Федеральный закон «О государственном языке Российской Федерации»», так как понятие «кибербуллинг» является заимствованным из иностранных источников.

Очевидно, что анализируемый в статье феномен требует более тщательного уголовно-правового и криминологического исследования.

Список использованной литературы

1. Федеральный закон от 28 февраля 2023 г. № 52-ФЗ «О внесении изменений в Федеральный закон «О государственном языке Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс] // URL: http://publication.pravo.gov.ru/Document/View/0001202302280028?index=0&rangeSize=1.

2. Статистика и аналитика России [Электронный ресурс] // URL: https://vegetarian.ru/articles/kiberbulling-chuma-tsifrovoy-tsivilizatsii.html.

3. Статистика и аналитика МВД России [Электронный ресурс] // URL: https://мвд.рф/dejatelnost/statistics.

4. Стукало И.С. Определение понятия кибербуллинга на основании исследований зарубежных и отечественных ученых // Молодой ученый. – 2020. – № 2 (292). – С. 218–220.

5. Баранов А.А., Рожина С.В. Психологический анализ причин подросткового кибербуллинга // Вестник удмуртского университета – 2017 − № 3. – С. 5–8.

6. ВЦИОМ. Новости: Кибербуллинг: масштаб проблемы в России [Электронный ресурс] // URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/kiberbulling-masshtab-problemy-v-rossii?ysclid=lhc25f8jcg815774599.

7. Статистика и аналитика России [Электронный ресурс] // URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/kiberbulling-masshtab-problemy-v-rossii.

8. Статистика и аналитика России [Электронный ресурс] // URL: https://raec.ru/activity/ analytics/9880/.

9. Статистика и аналитика России. [Электронный ресурс] // URL: https://raec.ru/activity/analytics/9880/.

Белоусова Анна Николаевна,
доцент кафедры уголовного права и криминологии
к.ю.н., доцент, e-mail: velanna22@mail.ru
(Воронежский институт МВД России, Российская Федерация)

Мисайлов Дмитрий Владимирович
e-mail: mitya.vladimirovich.93@list.ru
(Центральный филиал Российского государственного университета правосудия г. Воронеж, Российская Федерация)

МЕХАНИЗМ ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ С ИСПОЛЬЗОВАНИЕМ СОЦИАЛЬНЫХ СЕТЕЙ

Аннотация. В статье раскрываются психофизиологические особенности несовершеннолетнего возраста, обладающие виктимогенным характером, и криминогенность влияния социальных сетей на социализацию несовершеннолетних.

Ключевые слова: несовершеннолетние; виктимность несовершеннолетних; социальные сети, социализация несовершеннолетних, вовлечение несовершеннолетних в преступление.

MECHANISM OF INVOLVEMENT OF MINORS IN CRIMES COMMITTED USING SOCIAL NETWORKS

Annotation: The article reveals the psychophysiological features of minors, which have a victimogenic character, and the criminogenicity of the influence of social networks on the socialization of minors.

Keywords: minors; victimization of minors; social networks, socialization of minors, involvement of minors in crime.

В современных условиях цифровизации и коммуникации общества социальные сети и мессенджеры стали незаменимым инструментом работы, обучения и досуга. Стремительное развитие средств массовой информации, компьютерных технологий, сложная и постоянно меняющаяся эпидемиологическая ситуация в мире определили необходимость и незаменимость сети «Интернет». Развитие инфотелекоммуникационных сетей позволяет не взирая на расстояния и границы обмениваться информацией и документами, совершать финансово-экономические операции. Безграничные возможности Интернет-ресурсов становятся площадкой не только для развития созидательных, но и деструктивных форм деятельности. Сложности выявления и раскрытия «киберпреступлений», неразвитость методов их пресечения, расширение межрегиональных и международных связей всегда определяли латентность деяний, с использованием Интернет-ресурсов, и обусловливали их рост. Так, количество преступлений, совершаемых с использованием сети «Интернет», только в 2022 г. выросло на 8,4% по сравнению с предыдущим годом [1].

К числу наиболее уязвимых криминогенному воздействию групп населения относятся несовершеннолетние. Подростковый возраст, как этап социализации, значим формированием основ нравственных ценностей, развитием навыков саморегулирования и самоконтроля [2, с. 263]. Такие психологические особенности возраста как впечатлительность и эмоциональность, несдержанность и категоричность, доверчивость и самоуверенность, неуверенность и, вместе с тем, несамокритичность, обидчивость и равнодушие к переживаниям других очень ярко характеризуют эмоционально-волевую сферу личности несовершеннолетнего. В основе столь полярных реакций лежат физиологические особенности развития нервной системы и особые поведенческие механизмы, обусловленные гормональной перестройкой организма. Именно психофизиологические особенности влияют на восприятие и оценку окружающей действительности. Подростковое видение мира неоднозначно и противоречиво: стремясь к самостоятельности, демонстрируя упорстве несовершеннолетние нередко сами толком не знают, чего хотят, к каким жизненным и нравственным целям стремятся; интересуются всем новым и неизвестным, но проявляют неосмотрительность в обстановке опасности.

Внушаемость и ранимость, импульсивность и завышенная самооценка, необходимость самоактуализироваться и социальная незрелость определяют виктимогенность несовершеннолетнего возраста. В ситуации отсутствие четких нравственных принципов, жизненных целей и стереотипов поведения любое неблагоприятное внешнее воздействие сразу переходит в разряд криминогенного. И в одночасье эта группа населения из категории потерпевших может перерасти в категорию преступников. Не обладая в полной мере информацией о том, какие существуют опасности в виртуальном пространстве, а зачастую даже не осознавая, что стали жертвой преступления, подростки повторяют увиденное на экране, полагая, что это норма, правильный стереотип поведения.

Социальная и психологическая незрелость, специфические поведенческие реакции ставят несовершеннолетних в ситуациях морального выбора в сложное положение. Взрослый мир оперирует аргументами и правилами поведения, от-

личные от тех, которые прививают детям (терпимое отношение к еще недавно порицаемым неуважение к старикам и женщинам, сексуальной распущенности, вседозволенности). Такое несоответствие между образом идеальной модели мира (того, что внушают родители и педагоги) и самого себя в реальной действительности (того, как ведут себя окружающие) оставляют несовершеннолетних в растерянности – то, чему учились и к чему готовились, разбиваются о реальность и влечет разочарование и фрустрацию [3, с. 8]. Негативное мироощущение трансформируется в субъективное ощущение личной и социальной неадекватности. А для нормального духовного, нравственного и психического развития детям необходимо чувствовать радость, веселье, одобрение себя и своих достижений. К сожалению, родители и педагоги ежедневными требованиями и критическими замечаниями лишь обостряют ситуацию, вместо того чтобы разъяснять неодномерность и неоднозначность социальной жизни, учить разбираться в сложных социальных конструктах. Трудовая занятость родителей, распад традиционных государственной и общественной систем организации социально полезной занятости и досуга несовершеннолетних поставили в числе основных «воспитателей», источников нравов, вкусов и моделей поведения Интернет-ресурсы. Так, 97% несовершеннолетних пользователей Интернета заходили в сеть каждый день или почти каждый день [4]. Здесь следует понимать механизм преобладания этих коммуникативных ресурсов. Они доступны, просты для восприятия, не требуют интеллектуальных, нравственных, физических или материальных вложений и затрат, не контролируются взрослыми, а само их использование при неодобрении родителей повышает самооценку. К сожалению, они не оказывают культурно-просветительского воздействия, рекламируют материально-предметные ценности, легкую жизнь, беззаботное проведение досуга. По верному утверждению Е.О. Филипповой транслируемые передачи в формате ток-шоу не нацеливают на осознание и обдумывание происходящих событий, не стимулируют думать и сопоставлять транслируемое на экране и происходящее в реальной действительности, тем самым примитивизируют сознание [5, с. 258].

Незавершенность интеллектуального развития и необходимость на психофизиологическом уровне ощущения психологического комфорта определяет доминирование сиюминутных удовольствий, приоритет принципа «здесь и сейчас». Этим пользуются криминальные и околокриминальтные группы не обремененные моральными ограничениями и потому легко манипулирующие переживаниями подростка, не оценивают, не ругают, не контролируют, не воспитывают, не наставляют. И в подростковом сознании повышается их престиж. При такой моральной поддержке ребенка уже не интересуют другие социальные запреты, растет самосознание, собственная значимость, а социальные установки подавляются [2, с. 263].

Манипулирование неокрепшим детским сознанием происходит неприкрыто, с напором и динамизмом различных технических средств. Приоритетным инструментом выступают сфабрикованные факты о неправомерных действиях властей, о допустимости противоправного поведения для достижения «высших» целей, об агрессивном «общественном мнении» и т.п. Эти материалы не

только уничижают приоритетов власти или искажают действительность, но способствуют возникновению слухов и паники, что еще больше обостряет общественную обстановку и препятствует достижению государственно значимых целей. И это не всегда оппозиционные каналы, выступающие подстрекателями. Для дестабилизации обстановки используются коммуникационные чаты, социальные сети и чаты компьютерных игр при обязательном условии неразглашения и неиспользования защиты от старших, в том числе посредством сети Интернет. Социальные сети являются источником различных угроз, среди которых пропаганда потребления алкогольных напитков, наркотических средств и других психоактивных веществ, половой распущенности и порнографии, насилия и жестокости, агрессивного и суицидального поведения, пренебрежения и отрицания норм и правил человеческого общежития.

Повышенная возрастная восприимчивость, эмоциональность и внушаемость не позволяет объективно оценивать окружающую действительность. Так, например, организаторы и зачинщики массовых акций с выкладывали нп платформе TikTok видеоролики спризывам «погулять», которые посмотрели 19 до 34 млн. человек [6]. Если учесть, что основная аудитория и авторы мобильного приложения TikTok. – это подростки, то можно с уверенностью говорить, что все эти несколько миллионов человек – дети. Они до конца не осознают серьезности своих действий и последствий, что собираясь посетить то или иное мероприятия, могут оказаться в очень трудной ситуации – криминогенной или виктимогенной [7, с. 124].

Невежество или намеренное искажение информации вводит в заблуждение подростков. Они еще не в состоянии оценить авторитетность источников, разобраться в правдивости/лживости получаемых сведений. Недостоверность информации при низком уровне удовлетворения социальных потребностей, разжигание националистических чувств под прикрытием идей патриотизма являются благоприятной почвой для формирования искаженного, неадекватного общественного мнения. Да и сам по себе большой объем нерегламентированной и неконтролируемой информации расширяет опасность детского неблагополучия.

При отсутствии жизненного опыта и социальной незрелости детям требуется помощь в определении социальных ориентиров, стереотипов допустимого и верного поведения, смысле жизни и своего существования, определения вектора поступков. Во многих жизненных вопросах они не могут разобраться самостоятельно. Однако близкие взрослые не всегда находят время и силы для дружеского участия и поддержки. Следует постоянно напоминать родителям и педагогам о моральной ответственности за судьбы и умы наших детей, за формированием социальных ценностей, за выбор их жизненного пути. Однако, не всегда и старшее поколение понимает суть проводимых реформ и сами высказывают недоумение в различных их проявлениях. Следовательно, и населению следует разъяснять суть и значение принимаемых решений и проводимых реформ. В тех случаях, когда родителям просто не хватает аргументов, им необходимо оказать консультативную методическую помощь.

Полагаем, что у педагогов появились широкие возможности выявлять назревающие проблемы в подростково-молодежной среде. В условиях пандемии обучение организовывалось не только на образовательных платформах, но в социальных сетях и мессенджерах, где и сейчас зачастую продолжается общение с педагогами.

Большую значимость средств предупреждения встречи несовершеннолетнего с преступником в социальной сети имеют соответствующие настройки «приватности». Прежде всего, речь идет о средствах управления своим профилем в социальных сетях, ограничивающих объем размещаемой личной информации, доступ к ней со стороны посторонних лиц, позволяющих блокировать нежелательных собеседников и т.п.

Помимо технологических инструментов для несовершеннолетних пользователей, должны существовать и дополнительные средства защиты, используемые родителями (средства «родительского контроля»). Однако многие их них сами не знакомы с угрозами, которые таит для ребенка информационное пространство, и, следовательно, не знают, какие должны быть приняты профилактические меры. К последним стоит отнести работу с родителями подростков-пользователей Интернета по разъяснению угроз, важности установления на компьютере актуального антивирусного программного обеспечения, установления и настройки сетевого экрана, специального программного обеспечения, позволяющее контролировать и ограничивать деятельность ребенка в «Интернете», предоставления им алгоритма действий при попадании ребенка в зависимость от Интернет-ресурсов.

Список использованной литературы

1. Состояние преступности в Российской Федерации за январь-декабрь 2022 года // Официальный сайт Министерства внутренних дел Российской Федерации [Электронный ресурс] // URL: https://media.mvd.ru/files/application/4683439.

2. Щеголева А.Н. Механизм использования криминальной субкультурой психофизиологических особенностей несовершеннолетнего возраста // Вестник Воронежского института МВД России. – 2019. – № 2. – С.263–270.

3. Яковлев Н.П. Тюремная (пенитенциарная) субкультура как криминогенный фактор и перспективы нейтрализации ее негативного влияния: автореф. дис. … канд. юрид. наук. – Рязань, 2006. – 228 с.

4. Сайт о проектах фонда развития интернета [Электронный ресурс] // URL: http://www.fid.su/projects/research/.

5. Филиппова Е.О. Несовершеннолетняя преступность как объект криминологического исследования // Известия Оренбургского государственного аграрного университета. – 2015. – № 2 (52). – С. 258–260.

6. Полунин А.Бунт подростков: Навальный поднимает против Путина молодняк. Агитация на митинг 23 января заполонила соцсети [Электронный ресурс] // https://svpressa.ru/society/article/287755/.

7. Белоусова А.Н., Шевцова К.А. Современное состояние участия несовершеннолетних в преступлениях, посягающих на общественный порядок Со-

временное состояние участия несовершеннолетних в преступлениях, посягающих на общественный порядок // Вестник Воронежского института МВД России. – 2022. – № 1. – С. 124–130.

Власова Елена Львовна,
доцент кафедры административного права и административной деятельности ОВД
к.п.н., e-mail: vlasovael1963@gmail.com
(Восточно-Сибирский институт МВД России, Российская Федерация)

ПРОБЛЕМЫ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматриваются проблемы противодействия киберпреступности в реалиях сегодняшнего времени. В последнее время количество компьютерных преступлений, совершаемых под руководством транснациональных организованных преступных групп значительно увеличилось, однако, действующее законодательство не успевает подстраиваться под вызовы современности. Исходя из чего, предпринимается попытка усовершенствования уголовной ответственности за создание преступного сообщества в сфере компьютерной информации и вносится предложение по современному определению преступного сообщества.

Ключевые слова: цифровизация, информационно-телекоммуникационные технологии, интернет-пространство, киберпреступления, киберпреступность, кибергруппа, кибератака, кибероружие.

PROBLEMS OF DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Abstract. The article discusses the problems of countering cybercrime in the realities of today. Recently, the number of computer crimes committed under the leadership of transnational organized criminal groups has increased significantly, however, the current legislation does not have time to adapt to the challenges of modern times. Based on this, an attempt is being made to improve criminal liability for the creation of a criminal community in the field of computer information and a proposal is being made for a modern definition of a criminal community.

Keywords: digitalization, information and telecommunication technologies, Internet space, cybercrime, cybercrime, cyber group, cyberattack, cyberweapons.

Организованные группы и преступные сообщества (организации) активно адаптируются к новым условиям современной жизни, одним из существенных аспектов которой является стремление к тотальной цифровизации.

Данный факт не остается без внимания, как со стороны правоохранительных органов, так и со стороны криминальных структур, активно использующих возможности информационно-телекоммуникационных технологий в своих преступных целях. На современном информационном интернет-пространстве появился новый вид преступлений –киберпреступления и как следствие киберпреступность. Киберпреступность породила ранее не известные организованные преступные группы - кибергруппы, с целью совершения кибератак, то есть, создания, использования и распространения вредоносных компьютерных программ, вооруженные новым видом оружия – кибероружием, применяемым для нападений (кибератак) на граждан и организации [1, с. 142].

Число киберпреступлений в России выросло в 11 раз за последние 5 лет, их удельный вес в структуре преступности возрос с 1,8% до 25%, говорится в сообщении Генпрокуратуры. По данным ведомства, в прошлом году на преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходилось одно из четырех регистрируемых преступлений. Например, в 2020 году в России на кибермошенничество пришлось около 70% всех хищений, совершенных путем обмана или злоупотребления доверием, и составило более 510,4 тысяч.

В 2020 году было выявлено более 237 тыс. таких деяний, что на 73,4% больше, чем годом раньше. Понятно, что нельзя совершать такие преступления в одиночку, тут нужны и исполнители, и организаторы, и другие лица, например, предоставляющие базу персональных данных клиентов того или иного банка, работающих на постоянной и устойчивой основе.

На современном этапе, в организованных преступных кибергруппах устойчивость обеспечивается не иерархической структурой, как в классических формах организованной преступности, а партнерством и доверительными отношениями участников. Такие взаимоотношения приводят к устранению традиционных механизмов контроля и санкций к нарушителям, к гибкости и мобильности группы, способной в случае опасности мгновенно раствориться в сети «Интернет».

По мнению аналитиков, трансформация преступности с переходом в интернет-пространство произошла по причине глобальных изменений в экономике и политике к концу XX в, что повлекло появление новых рынков и технологий и немедленное приспособление преступности к новым социальным условиям. Приобретая черты транснациональности, организованная преступность вышла за пределы одной страны, что привело к усложнению структуры преступных формирований и увеличению числа их участников, руководитель в которых наделяется исключительно организаторскими функциями. Он уже не «условный» авторитет, а высокоинтеллектуальная личность, обладающая обширными связями не только на национальном, но, и международном уровне. Таким образом, произошла трансформация в так называемую «беловоротничковую» преступность» [2, с. 5].

Данное обстоятельство не могло не отразиться на криминологической характеристике личности «беловоротничкового» организованного преступника –

она стала другой. Наиболее значимыми в новой, изменившейся социальной среде стали два основных обстоятельства. Это, во-первых, «появление новых рыночных механизмов и отношений, основой формирования которых во многом стали криминальные капиталы»[76], сопровождавшиеся внедрением в сознание масс идеологии обогащения любым путем. В свою очередь это дало возможность «сконцентрировать в теневом секторе экономики значительные общенациональные средства»

И, во-вторых, нестабильность экономики на фоне всеобъемлющей цифровизации привела к новому виду преступлений, которые в настоящее время предусмотрены главой 28 Уголовного Кодекса Российской Федерации (далее УК РФ) «Преступления в сфере компьютерной информации», или «киберпреступность» [3, с. 123].

Приведем пример, в Екатеринбурге вынесли приговор Игорю Маковкину, создателю вредоносных компьютерных программ, в составе организованной группы, похитившему со счетов банков 1,2 млрд. рублей [4, с. 77].

В качестве примера также можно привести дело по обвинению А. и его супруги З., создавших транснациональную организованную преступную группу, состоящую из восьми лиц, обладающих навыками программирования и имеющих опыт создания вредоносных компьютерных программ. Подбор участников организаторы группы производили в ходе общения в сети «Интернет», при этом, для конспирации общение было анонимным. Указывая ложное географическое местоположение, пользователи, находящиеся в разных регионах России, Республики Казахстан и Латвии вошли в контакт, согласовали свои действия и приступили к реализации преступных планов, предложенных им организаторами [5, с. 93].

В настоящее время стремительно растет количество различных технических новинок, которые с успехом могут заменять привычное огнестрельное или холодное, газовое или пневматическое оружие. Развиваются биологическое оружие, робототехника, лазерное оружие. Существующие организованные преступные группы для достижения своих целей пользуются как оружием самыми последними новинками науки и техники. В такой ситуации им ничего не стоит обходить закон, узко трактующий понятие «оружие» и «вооруженность» [6].

В 2017 в России хакеры в целях нападений на граждан и организации использовали в качестве оружия вирусы-шифровальщики, способные останавливать операционную деятельность банков. По оценкам специалистов, доход хакеров от атак на банки уже перекрывает суммарный доход от остальных способов хищений. Международная компания Group-IB, специализирующаяся на предотвращении кибератак, зафиксировала нападения на 57 банков за короткий отрезок времени – 23 октября, 1 ноября и 15 ноября 2018 г. Хакерские группы, использующие разные способы кибератак, уже поделившие рынок интернет-пространства, получили у экспертов звучные имена: MoneyTaker (атакуют, в основном, системы межбанковских переводов), Silence (предпочитают банкоматы и системы карточного процессинга), Cobalt (специализируется на «бесконтактной» атаке на банкоматы, когда не повреждаются корпусы банкоматов, не используются скиммеры или банковские карты). Приходится сделать вывод,

что киберпреступность породила ранее не известный вид организованных преступных групп, вооруженных новым видом оружия – кибероружием, применяемым для нападений (кибератак) на граждан и организации. Представляется, что действующее законодательство пока не справляется с новыми угрозами, предъявленными обществу организованной преступностью, а специализированных органов нет, таким образом, данными преступлениями практически никто и не занимается. В настоящее время назрела необходимость в разъяснении изложенной проблемы в руководящем постановлении Пленума Верховного Суда РФ об ответственности за данный вид преступлений [7, с. 72].

В Главе 28 УК РФ «Преступления в сфере компьютерной информации» предусматривается повышенная ответственность в случае совершения данной категории преступлений в составе организованной группы. Организаторы и руководители групп хакеров должны нести ответственность за свои действия, сопоставимую с ответственностью создателей общеуголовных преступных организаций. Это, конечно, только одна из мер борьбы с современными организованными группами, но очень важная и актуальная. Другая проблема, вызванная трансформацией современных организованных преступных групп и их объединений, связана с господствующим в науке и практике мнением об иерархической структуре как характерном признаке преступного сообщества (преступной организации). Такое понимание обусловлено позицией законодателя, указавшего в определении данной формы соучастия на такой обязательный признак, как единое руководство структурированными организованными группами или объединениями организованных групп. Между тем, еще В.В. Казаневская отмечала, что «иерархическая структура - распространенный, но частный вид структуры» [5, с. 93].

Анализ современного состояния преступности приводит к выводу о том, что в действительности иерархический принцип построения преступных групп не является единственным. Суть иерархии — в вертикальном соподчинении подсистем и жестком характере отношений между ними. Социальные системы сегодняшнего дня, а в еще большей степени — дня завтрашнего, перестраиваются от иерархической формы организации к сетевой. Важнейшей чертой сетевых взаимодействий является то, что они позволяют выявить и согласовать интересы участников, сформулировать стратегическую цель и определить конечный результат взаимодействия, исходя из имеющихся потенциальных возможностей участников сети [8, с. 184].

В настоящее время мы являемся свидетелями стихийной перестройки структур организованной преступности, осваивающей более современные способы сетевых взаимодействий, что уже отмечено исследователями криминологами [9, с. 21].

В таких условиях задачей теории является разработка основных понятий и признаков новых сетевых форм организованной преступности, стихийно возникающих в криминальной реальности – это тоже относится к методам социально-криминологического характера. Все большая связь между киберпреступностью и организованной преступностью признается опасной тенденцией последнего времени, однако, уголовно-правовые нормы российского законода-

тельства не в полной мере учитывают это. В статьях Главы 28 УК РФ «Преступления в сфере компьютерной информации» в качестве квалифицирующего обстоятельства предусмотрено совершение преступлений группой лиц по предварительному сговору или организованной группой (ч. 3 статьи 272 и ч. 2 статьи 273 УК РФ). На наш взгляд, при этом не учитывается, что значительная часть компьютерных преступлений совершается не просто организованными группами, а объединениями таких групп, то есть преступными сообществами. [10, с. 45].

Однако в законе отсутствует специальная норма об ответственности за создание преступного сообщества в сфере компьютерной информации, что считаем пробелом в законодательстве [11, с. 59].

Таким образом, «социальные системы в настоящее время имеют тенденцию к структурной перестройке от иерархической формы организации к сетевой». Преступность, представляющая собой одну из негативных подсистем общества, развивается одновременно с ним, приспосабливая свои структурные характеристики к инновационным процессам, происходящим в обществе. Это выражается в стихийной перестройке структур организованной преступности и в переходе от иерархических форм к сетевым, получившим наибольшее распространение в киберпреступности. Уголовно-правовые меры противодействия преступности нуждаются в разработке новых понятий, соответствующих изменениям в способах формирования организованных групп и сообществ. В этих целях можно предложить следующее (рабочее) определение: преступное сообщество – это объединение организованных групп или структурированная организованная группа в составе нескольких лиц (не менее трех), которые объединились по иерархическому принципу (под единым руководством) либо по сетевому принципу (на основе комплементарности) с целью занятия преступной деятельностью. Предлагается дополнить Главу 28 УК РФ нормами об ответственности: «За создание организованной преступной группы (кибергруппы), с целью совершения кибератак (создания, использования и распространения вредоносных компьютерных программ), за создание преступного сообщества, имеющего цели совершения преступлений в сфере компьютерной информации, и за участие в таком сообществе Дополнить понятие преступного сообщества положениями, учитывающими сетевые способы организации преступных сообществ.

Список использованной литературы

1. Пырчев С.В. Тенденции организованной преступности в развивающемся цифровом мире // Труды Академии управления МВД России. – 2020. – № 2 (54). – С. 142–153.

2. Рябцев О.В. Сетевой принцип деятельности организаций закрытого типа в контексте угроз национальной и региональной безопасности России (на примере крымско-татарского национального движения): автореф. дис. … канд. политич. наук. – Ростов-на Дону, 2008. – 27 с.

3. Белоцерковский С.Д. Организованная преступность как специфический криминальный феномен // Пробелы в российском законодательстве. – 2017. – № 5. – С. 122–124.

4. Добрынина С. Расплата за вирусы // Российская газета. – 2018. – № 258. – С. 75–80.

5. Казаневская В.В. Философско-методологические основания системного подхода. – Томск: Изд-во Томского ун-та, 1987. – 247 с.

6. Меры борьбы с современным бандитизмом [Электронный ресурс] // URL:https://scicenter.online/kriminologiya-scicenter/meryi-borbyisovremennyim-61014.html.

7. Маркелов Р.И грянул взлом // Российская газета. – 2018. – № 259. – С. 70–74.

8. Василенко Н.В. Принципы сетевых взаимодействий в образовании // Международный журнал прикладных и фундаментальных исследований. – 2014. – № 4. – С. 183–185.

9. Агапов П.В., Александрова Л.И., Амирбеков К.И. Борьба с криминальными рынками в России: монография. – М.: Проспект, 2015. – 210 с.

10. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С. 45–49.

11. Глазкова Л.В. Бандитизм и преступные сообщества: вопросы разграничения. – М.: Юрайт, 2013. – 200 с.

Гончарова Мария Витальевна,
главный научный сотрудник
д.ю.н., доцент, полковник полиции, e-mail: maria-g2009@yandex.ru

Смирнов Владимир Георгиевич,
старший научный сотрудник
полковник полиции, e-mail: smvlag@rambler.ru

(Всероссийский научно-исследовательский институт МВД России, Российская Федерация)

ОСНОВНЫЕ ТЕНДЕНЦИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. В статье исследуются тенденции преступлений, совершаемых с использованием информационно-телекоммуникационных технологий на территории Российской Федерации, способы их совершения, обусловленые реализацией мероприятий федерального значения, направленных на противодействие указанному виду преступности.

Ключевые слова: преступления, совершаемые с использованием информационно-телекоммуникационных технологий; киберпреступления; тенденции; показатели; криминогенные факторы; органы внутренних дел; противодействие; предупреждение; меры.

THE MAIN TRENDS OF CRIMES COMMITTED ON THE TERRITORY OF THE RUSSIAN FEDERATION USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Annotation. The article examines the trends of crimes committed using information and telecommunication technologies on the territory of the Russian Federation, the ways of their commission, due to the implementation of federal measures aimed at countering this type of crime.

Keywords: crimes committed using information and telecommunication technologies; cybercrime; trends; indicators; criminogenic factors; internal affairs bodies; countering; prevention; measures.

С начала XXI века информационно-телекоммуникационные технологии все глубже проникают не только в повседневную жизнь граждан, но и в деятельность органов власти, предприятий и организаций. Произошло «переформатирование» социальных отношений, которые все больше и больше виртуализируются. Использование цифровых технологий позволяет в короткие сроки, без лишних затрат получать необходимые услуги и информацию, осуществлять экономические отношения, поддерживать деловые и личные контакты и многое другое.

Вместе с тем, такая всеобщая цифровизация несет в себе не только позитивные моменты, но и значительный негативный потенциал, прежде всего – криминальные риски и угрозы [1, с. 80–82].

Изучению различных аспектов проблемы преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, посвящали свои научные изыскания такие отечественные ученые, как И.Р. Бегишев, Я.И. Гилинский, Р.И. Дремлюга, Я.Г. Ищук, С.В. Иванцов, А.Г. Кибальник, С.Я. Лебедев, В.С. Овчинский (криминология цифрового мира), Т.В. Пинкевич, Э.Л. Сидоренко, Е.С. Смольянинов, Т.Л. Тропина, Е.А. Русскевич, Н.В. Щедрин и др.

По итогам 2022 г. количество зарегистрированных (+0,8 %; всего – 522 065) и уровень (с 352,9 в 2021 г. до 358,7 в 2022 г.) киберпреступлений, а также их доля в общей структуре преступности (с 25,8 % в 2021 г. до 26,5 % в 2022 г.) незначительно увеличились. Существенно увеличился ущерб от них. По преступлениям, выявленным органами внутренних дел (98,7 %), он составил 91 941 183 тыс. руб.

Но, поскольку киберпреступления являются высоколатентным видом преступности, статистические показатели не отражают их истинных размеров. В числе прочего об этом свидетельствует тот факт, что в истекшем году только мобильные продукты и технологии «Лаборатории Касперского» обнаружили

196 476 новых мобильных банковских «троянцев», что в два раза больше, чем в 2021 г. (всего – 97 661), и является максимальным значением за последние шесть лет [2].

Больше половины зарегистрированных киберпреступлений (52,1 %) относится к категориям тяжких и особо тяжких (272 233; –5,6 %).

В структуре киберпреступлений преобладают киберхищения (мошенничества (47,8 %; всего – 249 929) и кражи (21,8 %; всего – 113 530)) и преступления в сфере незаконного оборота наркотиков (15,7 %; всего – 82 661) (См. рис. 1).

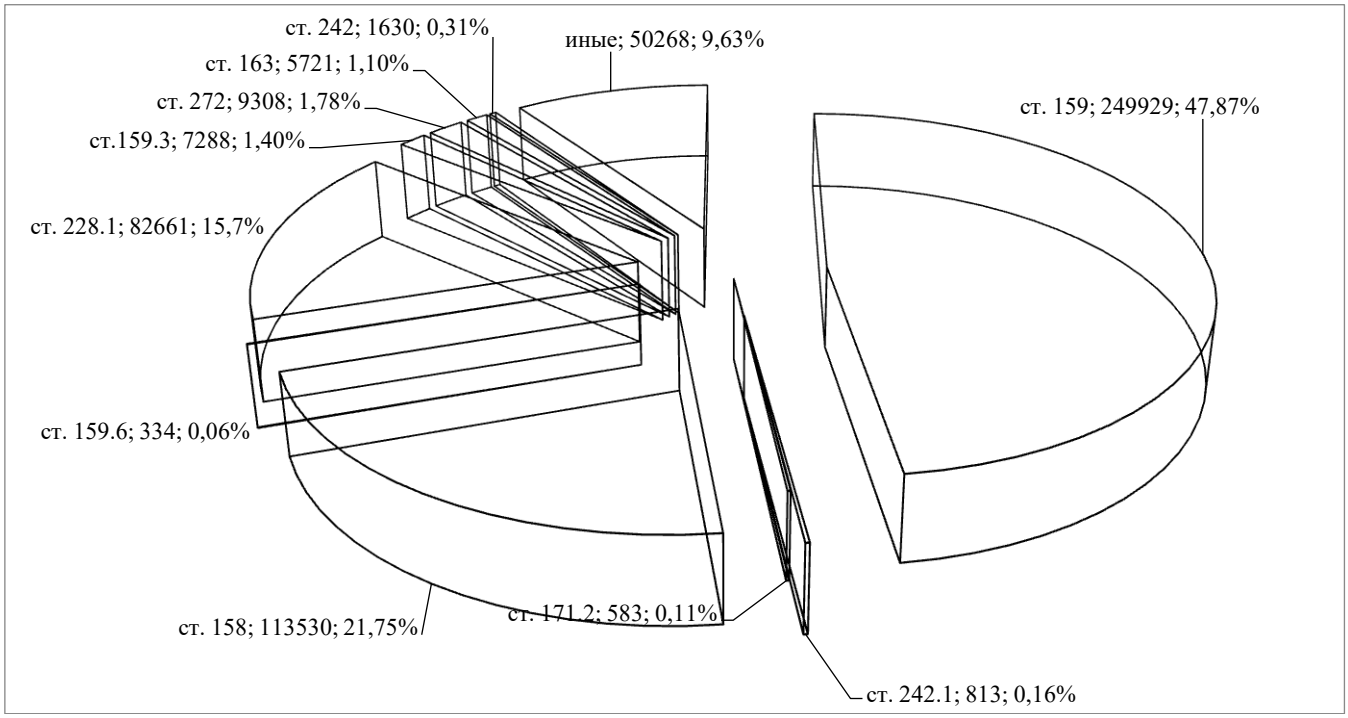


Рис. 1. Структура киберпреступлений в 2022 г.

Киберхищения в основном совершаются из-за рубежа. Подтверждением тому является существенное сокращение IT-мошенничеств с использованием электронных средств платежа (–29,0 %) и в сфере компьютерной информации (–22,5 %) после начала специальной военной операции (далее – СВО) [3].

Отмечается сохранение тенденции увеличения криминальной активности «телефонных» мошенников, в основном действующих с территории Украины. По данным ВЦИОМ, в 2022 г. с телефонным мошенничеством сталкивалось большинство россиян – 83 % (+7 п.п. к 2021 г.), из них 63 % (+6 п.п. к 2021 г.) указали, что им поступали звонки, а 20 % получали СМС-сообщения [4].

В России правоохранительные органы выстроили достаточно эффективную систему выявления мошеннических call-центров, вытесняющую владельцев этого «бизнеса» за пределы страны. Украина в этом смысле является максимально удобной, поскольку препятствий для такой деятельности практически не существует: международное сотрудничество правоохранительных органов фактически свернуто, любые «выпады», в том числе криминальные, в сторону России и ее граждан поощряются. Действуют целые организованные группы по 200-400 человек, иногда – до тысячи человек [5].

Вместе с тем риски дистанционных хищений напрямую сопряжены с фактами утечки персональных данных граждан.

Ключевыми факторами распространения наркотиков являются использование организованной наркопреступностью информационно-телекоммуникационных технологий и цифровизация наркоторговли. В 2022 г. практически каждое второе наркопреступление (46,5 %) совершалось с использованием сети Интернет.

IT-технологии активно применяются при совершении преступлений, связанных с экстремизмом, изготовлением и распространением порнографических материалов с изображением несовершеннолетних, с незаконной организацией и проведением азартных игр, оборотом оружия [6, с. 65].

Прирост числа киберпреступлений в два и более раз зафиксирован по преступлениям, связанным с незаконным оборотом оружия (+196,0 %: всего – 74) и неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации (+226,4 %; всего – 519), а также фактам содействия террористической деятельности (всего – 251) и заведомо ложных сообщений об акте терроризма (всего – 21 424), что обусловлено криминогенными факторами, обострившимися в период проведения СВО на Украине.

Значителен прирост числа вымогательств (+42,3 %; всего – 5 721), фактов неправомерного оборота средств платежей (+50,8 %; всего – 2 647), публичных призывов к осуществлению террористической деятельности, публичных оправданий терроризма или пропаганды терроризма (+55,6 %; всего – 490), изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних (+55,3 %; всего – 813) и неправомерного доступа к компьютерной информации (+45,6 %; всего – 9 308).

К наиболее распространенным способам совершения киберпреступлений относятся: с использованием информационно-телекоммуникационной сети «Интернет» (всего – 381 112; +8,4 %), при помощи средств мобильной связи (всего – 212 963; –2,1 %), расчетных (пластиковых) карт (всего – 127 149; –23,2 %) [7, с. 63–71].

Число выявленных за совершение киберпреступлений лиц продолжило увеличиваться, однако темпы прироста по сравнению с периодом пятилетней давности значительно снизились (См. табл. 1).

Таблица 1.

Динамика числа лиц, выявленных за совершение киберпреступлений

Показатели	**2018**	**2019**	**2020**	**2021**	**2022**
Лица, совершившие киберпреступления	24002	44158	65665	95370	96665
Прирост /снижение, %	–	84,0	48,7	42,2	1,4

Подавляющее большинство киберпреступников – мужчины (78,4%).

Наибольшую криминальную активность в киберпространстве проявляют лица возрастных групп 30-39 лет (34,3%) и 18-24 года (21,2%) (См. рис. 2).

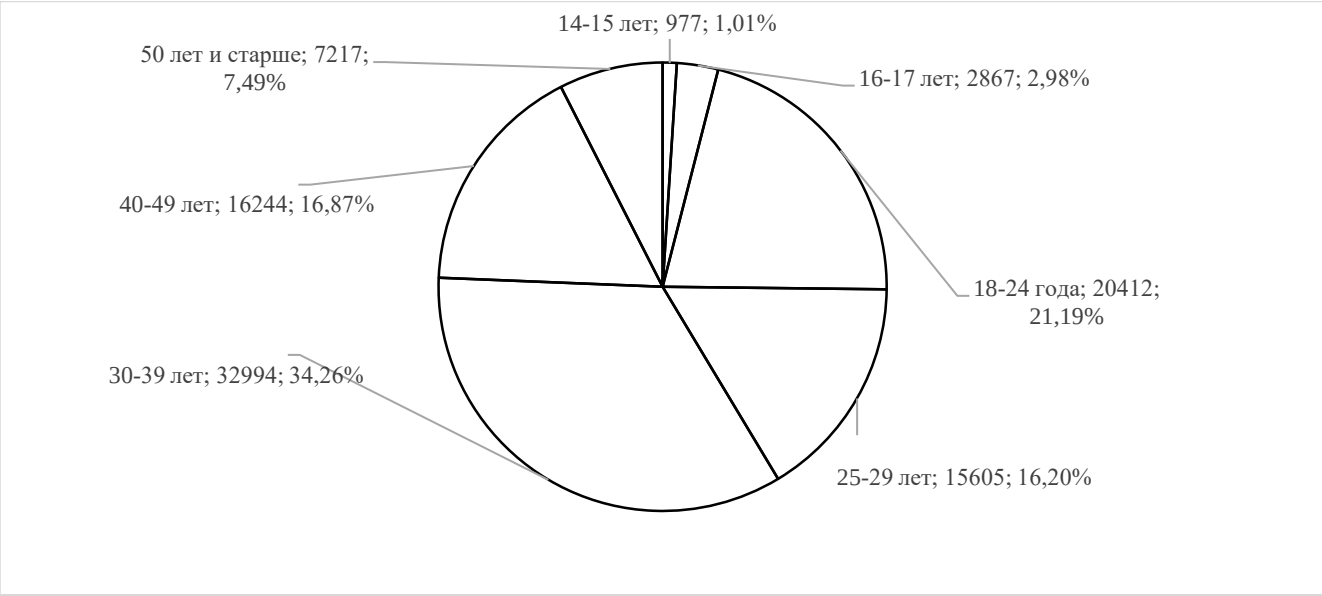


Рис. 2. Структура киберпреступников по возрасту в 2022 г.

Геополитические события, связанные с проведением СВО, повлияли на киберугрозы. С конца февраля 2022 г. российские организации, независимо от их величины, подвергаются беспрецедентным по своему размаху и интенсивности кибератакам, во основном со стороны Украины. Злоумышленники ориентированы строго на российские IP-адреса.

Наибольшее распространение получили DDoS-атаки[1], взлом крупных компаний с последующими кражами информации, а также дефейс[2] популярных ресурсов. Отмечается рост количества целенаправленных атак на государственный сектор, банковскую сферу, топливно-энергетический комплекс, IT-компании, научные институты и организации, связанные с оборонно-промышленным комплексом [8].

Частные лица в основном подвергались кибератакам через социальные сети и мессенджеры, направленными на сбор учетных данных и взлом аккаунтов, с последующим использованием в целях совершения преступлений против собственности [9, с. 8–10].

Анализ состояния и динамики киберпреступлений за пятилетний период, несмотря на указанные выше изменения правил статистического учета, демонстрирует последовательный рост их числа, обусловленный:

– расширением зоны проникновения Интернета. По данным отчёта Global Digital 2023 [10], уровень проникновения интернета в России достиг 88,2 %; 92 % пользователей интернета, используют для входа смартфоны; 73,3 % насе-

[1] DDoS-атака – распределенная атака типа «отказ в обслуживании» с одновременным использованием большого числа атакующих компьютеров, в том числе объединенных в ботсеть, целью которой, как правило, является воспрепятствование доступу легитимных пользователей к атакуемому ресурсу, частичное нарушение штатного функционирования информационной инфраструктуры и т.д.

[2] Дефейс (от англ. deface – «портить», «уродовать») – взлом сайта и публикация на нем сообщения злоумышленников.

ления России зарегистрированы в соцсетях; прирост скорости мобильного интернета составил 21,9%, мобильного трафика – 18 %;

– доступностью информации о способах совершения киберпреступлений;

– доступностью технических средств создания, хранения и обработки цифровой информации, а также снижением стоимости Интренет-подключения;

– недостаточной цифровой грамотностью населения;

– распространенностью программных средств анонимизации личности, обеспечивающих сокрытие информации о лице, совершающем противоправные действия с использованием сети «Интернет» (ремейлеры, анонимайзеры, VPN-сервисы, TOR-браузеры и др.) [11, с. 167];

– совершенствованием функциональности вредоносного программного обеспечения и способов его распространения. Все больше оно распространяется через легитимные каналы – официальные магазины приложений или рекламу в популярных приложениях.

Кроме того, информационно-телекоммуникационные технологии продолжают все глубже проникать не только в повседневную жизнь граждан, но и в деятельность органов власти, предприятий и организаций. Широкие возможности информационных технологий способствовали принятию на государственном уровне национальной программы «Цифровая экономика Российской Федерации» [12], фактически обязывающей принимать органы, организации и промышленные предприятия комплексные решения на базе цифровых продуктов, улучшающих или ускоряющих процессы жизнедеятельности, организационных и производственных процессов. На состояние киберпреступлений все это оказывает криминогенное влияние, поскольку чем выше уровень цифровизации, тем больше существует потенциальных возможностей для совершения рассматриваемых посягательств.

В 2022 г. Россия по уровню цифровизции государственного управления заняла 10 место в рейтинге 198 стран Всемирного банка GovTech Maturity Index 2022 и вошла в группу А – страны с самым высоким рейтингом [13].

На фоне пандемии коронавируса появилось множество разновидностей киберпреступлений, приобретших в сложившихся реалиях новый формат. В этой связи могут быть выделены следующие тренды:

– массовые кибератаки на инфраструктуру удаленного доступа или удаленную рабочую инфраструктуру;

– рост количества фишинговых атак и распространение вредоносных программ в связи с расширением цифровой аудитории;

– роста количества посягательств на криптовалюты;

– увеличение спроса на запрещенные товары и услуги (порнографическая продукция, кибер-секс, незаконный оборот наркотиков и др.[14, с. 185–198];

– атаки на цифровые платформы коммуникации, их взлом («Zoombombing»);

– рост числа криминальных проявлений в онлайн-играх[1];

[1] Преступные проявления в онлайн-играх связаны с распространением материалов экстремистского или сексуального характера, совершением финансовых махинаций, кражами персо-

– адаптация классических схем мошенничества при помощи методов социальной инженерии;

– активная эксплуатация в противоправных целях страхов населения (пандемии при организации онлайн-продаж поддельных лекарств, антисептиков, средств индивидуальной защиты, медицинских консультаций и онлайн-диагностики [15, с. 57–64]; потери денежных средств со счета банка, оказавшегося «под санкциями»; уголовной ответственности за якобы совершаемые переводы денежных средств в пользу ВСУ [16]);

– цифровизация наркоторговли;

– «хактивизм» – идеологически мотивированные киберпреступления;

– спекуляции на темы СВО и частичной мобилизации. Так, под видом повесток из военкоматов рассылались вредоносные электронные письма с целью краж документов и других файлов, данных для доступа к корпоративным почтовым ящикам [17].

Отмечается заметное снижение темпов прироста киберпреступлений (в 2019 г. – +68,5 %, 2020 г. – +73,4 %, 2021 г. – +1,4 %, 2022 г. – +0,8 %), что выступает следствием:

1) изменения онлайн-поведения пользователей Интернета.

Об этом свидетельствуют:

– сокращение времени нахождения в Интернете в результате более взвешенного подхода к его использованию[1];

– переход социальных сетей от простого средства коммуникации и развлечений до платформы, формирующей мировоззрение[2];

– более обдуманное отношение к выбору «подписок» и источников информации во избежание финансовых потерь, а также сохранения психического спокойствия;

– блокировка популярных информационных платформ, запрещенных в России в 2022 г. (Facebook, Instagram, Twitter и др.), а также закрытие сайтов отдельных средств массовой информации (сайты «Эхо» (проекта бывших журналистов «Эхо Москвы»), «Новая газета», проекта «Свободное пространство», изданий «Холод» и «Дискурс», немецкого таблоида Bild, литовского портала Delfi и интернет-издания «Полигон»);

2) дефицита серверных мощностей.

В 2022 г. с российского рынка ушли, либо приостановили поставки, крупнейшие зарубежные компании – поставщики серверного и сетевого оборудова-

---

нальных данных, проведением нелегальных азартных игр, организацией «договорных» игр в киберспорте и др.

[1] В 2022 г. в среднем время нахождения в сети Интернет составляло 6 ч. 37 мин. в день (в 2021 г. – почти 7 ч.).

[2] На фоне сокращения общего количества времени онлайн, среднестатистический интернет-пользователь трудоспособного возраста тратит в день чуть больше 2,5 часов на социальные сети. Это всего на 3 минуты больше прошлогоднего, однако рост этого показателя фиксируется ежегодно. Цифры показывают, что типичный интернет-пользователь трудоспособного возраста ежедневно тратит на 30% больше времени на соцсети, чем на просмотр «традиционного» телевидения (эфирных и кабельных каналов).

ния Hewlett Packard Enterprise, Dell Technologies, Lenovo, MikroTik, Cisco, поставщик облачных сервисов Google Cloud, микрочипов – Intel и AMD, AWS, поставщики SSL-сертификатов DigiCert и Sectigo, хостинг-провайдеры Hostinger и Namecheap. Дефицит серверных мощностей препятствует развитию российского рынка IT-инфраструктуры. Создание российских решений в указанной области потребует времени [18];

3) последовательной реализацией МВД России мер повышения эффективности противодействия IT-преступлениям.

В структуре МВД России сформировано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий, на которое возлагаются функции координации деятельности в данной сфере [19]. С целью обеспечения надлежащего взаимодействия при выявлении, раскрытии и расследовании киберпреступлений в территориальных органах МВД России созданы и действуют на постоянной основе специализированные следственно-оперативные и рабочие группы.

В результате совместной работы МВД России и Роскомнадзора в Единый реестр запрещенной информации внесено свыше 83 тыс. сайтов и отдельных страниц, содержащих информацию о распространении наркотиков, пресечено распространение порядка 160 тыс. ложных и других запрещенных сведений, в том числе ориентированных на молодежь.

Усилия профильных ведомств и регуляторов финансового рынка позволили почти на 30% снизить массив краж с банковских счетов и мошенничеств с применением электронных средств платежа.

Наработанные средства и методы документирования IT-преступлений позволили повысить их раскрываемость, составившей 27,8 % (2021 г. – 23,4 %) [20];

4) роста затрат на ликвидацию последствий от киберпреступности и кибербезопасность.

По экспертным оценкам в мире эти затраты будут продолжать расти на 15% в год в течение следующих пяти лет, достигнув 10,5 трлн долларов ежегодно к 2025-му (по сравнению с 3 трлн долларов в 2015 г.).

Российский рынок информационной безопасности также демонстрирует ежегодный рост. В 2021 г. он составил 120-150 млрд рублей. Кроме того, сформировался новый тренд – более осознанное использование средств защиты, нацеленное на снижение малоуправляемых рисков, связанных с уязвимостями зарубежного программного и аппаратного обеспечения.

Одновременно атаки усложняются, а их криминальная «эффективность» повышается.

Пандемия COVID-19 ускорила развитие «цифровой» формы организованной преступности. Сформировался новый вид организованных преступных групп – кибер-ОПГ. Именно такими группами в числе других наиболее опасных преступлений совершаются атаки на критически важную государственную инфраструктуру.

До недавнего времени представители организованной преступности вовлекали высококвалифицированных IT-специалистов в определенные сферы своей

преступной деятельности [21, с. 53–56]. Сейчас появились и множатся группировки, специализирующиеся исключительно на киберпреступлениях. Все чаще их участники являются представителями разных стран. Ранее таким преступным объединениям препятствовало то, что в силу технического отставания ограниченный круг государств позволял формировать эффективные кибергруппировки. Криминогенное значение для разрастания подобных организованных форм киберпреступности имеют следующие обстоятельства:

– необходимый «инструментарий», часто вместе с инструкцией по эксплуатации, практически свободно можно приобрести на соответствующих форумах в Darkweb. Наличие понятной инструкции и популярность продажи (покупки) взлома как услуги максимально снижает технический порог «входа» в киберпреступность и, соответственно, размывает геолокацию кибергруппировок. Кибергруппировка может оказаться резидентом любой страны;

– сформировался устойчивый тренд на использование кибергруппировками инструментария друг друга, включая обмен, перепродажу и «шеринг»[1] технологических наработок. Нередки случаи заказов на разработку инструментов под конкретные задачи, а также слияний, поглощений и разделений кибергруппировок. В совокупности это приводит к совершенствованию способов киберпреступлений, их усложнению, практически исключающих возможности разоблачения;

– существуют специализированные компании, которые занимаются разработкой инструментария для проникновения в информационные системы. Особенно это развито в тех странах, где такая работа не подпадает под ограничения законодательства. Соответственно, этот инструментарий широко доступен для покупки и использования в противоправных целях [4, с. 17, 20-22].

Таким образом к числу основных тенденций киберпреступлений могут быть отнесены:

– ориентированность кибератак на российские IP-адреса;

– последовательный рост числа киберпреступлений с замедлением его темпов;

– развитие «цифровой» формы организованной преступности.

Развитие интеллектуальных систем, таких как «умные» здания, города и критически важной инфраструктуры, способствуют эволюции киберпреступлений. Серьезную криминальную угрозу несет морфическое вредоносное программное обеспечение на основе «роя», а также использование искусственного интеллекта в качестве кибероружия. В этих атаках используются «захваченные» устройства, разделенные на подгруппы, каждая из которых обладает специальным назначением и нацелена на сети или устройства. В процессе атаки они обмениваются данными в режиме реального времени для уточнения своей «роли» [22, с. 72–73].

Принимаемые меры противодействия киберпреступлениям пока не в полной мере результативны даже на фоне повышения грамотности населения и эффективности работы органов внутренних дел в указанной сфере. Уровень ки-

[1] Шеринг – передача во временное пользование за вознаграждение.

берпреступности продолжает оставаться высоким, результативность выявления, пресечения, раскрытия и расследования киберпреступлений – недостаточной. Во многом это обусловлено сохраняющимися криминогенными факторами, негативно влияющими на ситуацию в сфере киберпреступлений. В их числе:

– техническое и информационное обеспечение криминальных структур, позволяющее эффективно противостоять правоохранительным органам, а в отдельных случаях не попадать в поле их зрения, продолжая преступную деятельность;

– активная криминальная деятельность организованных преступных групп, действующих под контролем спецслужб;

– востребованность теневого сегмента сети Интернет, где возможен оборот всего перечня предметов, ограниченных либо изъятых из оборота, а также оказания запрещенных услуг;

– наличие теневых сервисов оборота криптовалюты, позволяющих скрытно выводить денежные средства за пределы Российской Федерации;

– отсутствие механизмов деанонимизации в теневом сегменте сети Интренет;

отсутствие оперативного доступа к информации, составляющей банковскую тайну, а также электронного документооборота с интернет-провайдерами, кредитными учреждениями и операторами сотовой связи, приводящее к устареванию запрашиваемой информации.

Позитивно повлиять на противодействие киберпреступлениям способны следующие факторы:

– «нарабатывание» практики применения изменений, внесенных в Федеральный закон «О связи», направленных на пресечение хищений с использованием сокрытия или подмены номера абонента [23];

– совершенствование технических средств защиты информации и мер технического противодействия киберпреступлениям [24, с. 662–665];

совершенствование нормативно-правового регулирования в части предоставления гражданам возможности самостоятельно устанавливать запреты и ограничения на онлайн-операции по своим банковским счетам;

– разработка и внедрение механизмов противодействия противоправному поведению сотрудников банков при оформлении кредитов, связанному с ситуациями, когда полученные денежные средства незамедлительно переводятся третьей стороне;

– введение ответственности для лиц, открывающих банковские счета на свое имя за вознаграждение в пользу третьих лиц;

совершенствование взаимодействия между МВД России и Банком России посредством законодательного закрепления оперативного обмена информацией о движении денежных средств по счетам при переводах без согласия клиента.

Антикриминогенным потенциалом обладает реализация:

– мер, предусмотренных в Указе Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [25], Приказе ФСБ России от 01.11.2022 № 543 «Об опре-

делении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250» [26];

– спецпроектов Минцифры, касающихся внедрения системы мониторинга фишинговых сайтов [27]; создания реестра недопустимых нарушений кибербезопасности [28]; информирующих пользователей о безопасном поведении в Интернете и киберугрозах, общих правил кибербезопасности [29], противодействия травли в сети, в том числе несовершеннолетних [30], качественной защиты аккаунтов [31];

– мер социально-экономической поддержки IT-специалистов [32] в частности касающихся расширения программы льготной ипотеки.

Повышению результативности противодействия киберпреступлениям будет способствовать дальнейшее совершенствование правовых механизмов. В этом смысле значимы изменения уголовного законодательства 2022 г., обусловленные необходимостью адекватной реакции на новые общественные отношения, возникающие и реализующиеся в условиях проведения СВО[1], направленные на обеспечение информационной безопасности России, а также принятие так называемого закона о «приземлении» иностранных IT-компаний, устанавливающего правовые основы деятельности иностранных юридических лиц, иностранных организаций, не являющихся юридическими лицами, иностранных граждан, лиц без гражданства, осуществляющих деятельность в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации [33].

Сохраняется потребность в квалифицированном кадровом обеспечении сферы информационной безопасности.

В краткосрочной перспективе прогнозируется незначительный рост числа киберпреступлений, что будет обусловлено, созданием дополнительных законодательных барьеров для совершения киберпреступлений, повышением уровня взаимодействия, профессиональной подготовки и технического оснащения субъектов противодействия таким преступлениям.

Список использованной литературы:

1. Антонян Ю.М., Афанасьева О.Р., Гончарова М.В. Преступность в России. – М.: Издательство «Юрлитинформ», 2023. – 272 с.

2. Мобильная вирусология 2022 [Электронный ресурс] // URL: https://securelist.ru/mobile-threat-report-2022/106860/.

3. Выступление В.А. Колокольцева на заседании Государственной Думы Федерального Собрания Российской Федерации в рамках «правительственного часа» [Электронный ресурс] // URL: https://мвд.рф/document/33200763.

4. Телефонное мошенничество – и как с ним бороться? Большинство россиян за последние полгода сталкивались с телефонными мошенниками, при

[1] Глава 28 УК РФ «Преступления в сфере компьютерной информации» дополнена ст. 274[2] «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

этом денежный ущерб понес каждый десятый [Электронный ресурс] // URL: https://wciom.ru/analytical-reviews /ana lit icheskii-obzor/telefonnoe-moshennichestvo-i-kak-s-nim-borotsja.

5. Охота на россиян. Как Украина превратилась в фабрику телефонных мошенников [Электронный ресурс] // URL: https: //aif.ru/ society/safety/ ohota_ na_rossiyan_ kak_ ukraina_ prevratilas_v_fabriku_telefonnyh_moshennikov.

6. Иващенко М. А. Новые формы организованной преступности: дис. … канд. юрид. наук. – М., 2022. – 217 с.

7. Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М.В. Гончарова, С.А. Невский, М.М. Бабаев, Р.В. Черкасов, Е.Б. Аблиязова, Е.М. Тимошина, Г.Ф. Коимшиди, Г.Э. Бицадзе. М.: ФГКУ «ВНИИ МВД России», 2023.

8. Фишинг, DDoS, дефейс: с какими ещё киберугрозами столкнулись российские компании в 2022 году [Электронный ресурс] // URL: //https://sber.pro /digital / publication / fishing-d-do-s-defejs-s-kakimi-eshhe-kiberugrozami-stolknulis-rossijskie-kompanii-v-2022-godu ? roistat _ visit =581417 (дата обращения: 21.03.2023).

9. Positive Research 2022: сборник исследований по практической безопасности. М., 2022.

10. Статистика интернета и соцсетей на 2023 год – цифры и тренды [Электронный ресурс]. URL: https: // www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2023-god-cifry-i-trendy-v-mire-i-v-rossii/.

11. Афанасьев П.Б., Шиян В.И. Состояние и тенденции киберпреступности на объектах транспортной инфраструктуры // Транспортное право и безопасность. – 2021. – № 4 (40). – С. 159–167.

12. О системе управления реализацией национальной программы «Цифровая экономика Российской Федерации: Постановление Правительства РФ от 02.03.2019 № 234: ред. от 13.05.2022 // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 07.03.2019.

13. Россия вошла в топ-10 стран по цифровизации госуправления [Электронный ресурс] // URL: https: // digital. gov. ru / ru / events / 42223 / ? utm_referrer = https % 3a % 2f %2 fyandex.ru %2f.

14. Хисамова З.И., Бегишев И.Р. Цифровая преступность в условиях пандемии: основные тренды // Russian Journal of Criminology. – 2022. – Vol. 16. – № 2. – С. 185–198.

15. Состояние преступности на территории Российской Федерации в условиях пандемии COVID-19 и тенденции ее развития до конца 2020 года: аналитический материал. М.: ФГКУ «ВНИИ МВД России», 2020.

16. 2 способа обмана: что придумали телефонные мошенники в 2023-м? [Электронный ресурс] // URL: https: // www.ixbt.com / live / offtopic/izmena-i-vash-schet-pod-sankciyami-telefonnye-moshenniki-v-2023g.html.

17. Мобилизовались: злоумышленники стали распространять вредоносное ПО под видом повесток [Электронный ресурс] // URL: https: // www.kaspersky.ru/about/press-releases/ 2022_ mo bilizovalis-zloumyshlenniki-stali-rasprostranyat-vredonosnoe-po-pod-vidom-povestok.

18. Рунет 2022: блокировка соцсетей, VPN-сервисы и запрет ЛГБТ-пропаганды. Ключевые цифры и события российского сегмента интернета [Электронный ресурс] // URL: https: //www. sostav.ru/publication/trendy-runeta-57912.html.

19. О внесении изменений в некоторые акты Президента Российской Федерации: Указ Президента Российской Федерации от 30 сентября 2022 г. № 688 // Официальный интернет-портал правовой информации http://pravo.gov.ru. 30.09.2022.

20. Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации 20.03.2023 [Электронный ресурс] // URL: https://мвд.рф/ (дата обращения: 21.03.2023).

21. Гончарова М.В., Шиян В.И. Состояние и тенденции современной киберпреступности // Вестник Академии Следственного комитета Российской Федерации. – 2021. – № 1 (27). – С. 53–56.

22. Кибермафия. Мировые тенденции и международное противодействие: монография / Ю.Н. Жданов, С.К. Кузнецов, В.С. Овчинский; вступ. ст. О.В. Храмова. – М.: Норма, 2022. – 182 с.

23. О связи: Федеральный закон от 07 июля 2003 г. № 126-ФЗ: ред. от 14.07.2022, с изм. и доп., вступ. в силу с 01.01.2023 // Собрание законодательства РФ. 14.07.2003. № 28. Ст. 2895.

24. Шиян В.И. Инновационные технические средства в сфере предупреждения преступности // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития: Материалы Международной научно-практической конференции, Москва, 17 октября 2019 года / Под общей редакцией А. М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – С. 662–665.

25. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 01 мая 2022 г. № 250 // Официальный интернет-портал правовой информации http://pravo.gov.ru. 01.05.2022.

26. Об определении переходного периода, предусмотренного подпунктом «б» пункта 5 Указа Президента Российской Федерации от 1 мая 2022 г. № 250: приказ ФСБ России от 01 ноября 2022 г. № 543 // Официальный интернет-портал правовой информации http:// pravo. gov.ru. 02.12.2022.

27. Минцифры запускает систему мониторинга фишинговых сайтов [Электронный ресурс] // URL: https://digital.gov.ru/ru/events/41620/.

28. Для госсектора открывается невозможное [Электронный ресурс] // URL: https://www.kommersant.ru/doc/5524837.

29. Как защитить себя и близких от киберугроз? КиберЗОЖ [Электронный ресурс] // URL: https://киберзож.рф/.

30. Кибербуллинг [Электронный ресурс] // URL: https://кибер-буллинг.рф/.

31. Выучи свою роль [Электронный ресурс] // URL: https://выучисвоюроль.рф/.

32. О внесении изменений в постановление Правительства Российской Федерации от 30 апреля 2022 г. № 805: постановление Правительства Российской Федерации от 23 января 2023 г. № 72 // Официальный интернет-портал правовой информации http://pravo.gov.ru. 30.01.2023.

33. О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации: Федеральный закон от 01 июля 2021 г. № 236-ФЗ // Официальный интернет-портал правовой информации http://pravo.gov.ru. 01.07.2021.

Горденко Александр Сергеевич,
преподаватель кафедры криминалистики, e-mail: alekgordenko@yandex.ru
(Омская академия МВД России, Российская Федерация)

ТИПИЧНЫЕ СПОСОБЫ СОВЕРШЕНИЯ ХИЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, В КОТОРЫХ ПОТЕРПЕВШИМИ ЯВЛЯЮТСЯ КРЕДИТНО-ФИНАНСОВЫЕ УЧРЕЖДЕНИЯ

Аннотация. В статье рассматриваются типичные способы совершения хищений с использованием информационно-телекоммуникационных технологий, в которых потерпевшими являются кредитно-финансовые учреждения. В качестве примеров к способам совершения данной категории преступлений приведены наиболее актуальные случаи из практики. В ходе исследования делается вывод, что классификация способов совершения хищений с использованием информационно-телекоммуникационных технологий не может носить исчерпывающего характера в силу многообразия таких способов, а также постоянного развития сферы информационно-телекоммуникационных технологий.

Ключевые слова: хищения, неправомерный доступ, информационно-телекоммуникационные технологии, распространение вредоносных программ.

TECHNOLOGIES, IN WHICH THE VICTIMS ARE CREDIT AND FINANCIAL INSTITUTIONS

Annotation. The article discusses typical methods of committing embezzlement using information and telecommunication technologies, in which the victims are credit and financial institutions. As examples of the methods of committing this category of crimes, the most relevant cases from practice are given. The study concludes that the classification of methods of committing theft using information and telecommunication technologies cannot be exhaustive due to the variety of such methods, as well as the constant development of the field of information and telecommunication technologies.

Keywords: embezzlement, unauthorized access, information and telecommunication technologies, malware distribution.

В настоящее время практические сотрудники правоохранительных органов все чаще сталкиваются с необходимостью расследования преступлений, совершённых с использованием информационно-телекоммуникационных технологий (далее – ИТТ), многообразие совершения которых постоянно растет. В случае расследования подобных преступлений, где потерпевшим является физическое лицо, у следователей и дознавателей уже выработался определенный алгоритм действий, позволяющий эффективно использовать ресурс правоохранительных органов в той или иной ситуации. Однако, если потерпевшим будет являться кредитно-финансовая организация (юридическое лицо), то расследование будет затруднено, поскольку количество заинтересованных лиц будет сокращено до минимума.

Отличительной чертой совершения преступлений в отношении кредитно-финансовых организаций, является тот факт, что у преступников зачастую отсутствует возможность изучить особенности поведения конкретного лица, т.к. потерпевшим будет являться не человек, а кредитно-финансовая организация, не имеющая каких-либо психологических уязвимостей, которыми, как правило, пользуются преступники. По этой причине, первично, хищения денежных средств у банков с использованием средств ИТТ разделяются на:

1) неправомерное воздействие, направленное на клиента необходимого банка (неправомерный доступ к личному кабинету);

2) кибератака направленная напрямую на серверы банковской организации.

Отметим, что при расследовании преступления совершенного первым способом, алгоритм действий правоохранительных органов, будет мало чем различаться от расследования аналогичного преступления, совершенного в отношении физического лица. Основным отличием будет отсутствие взаимодействия преступника с конкретным лицом, что весьма затруднит получение достаточного количества информации, представляющей интерес для расследования, в том числе и путем допроса потерпевшего. Поэтому следователю на первоначальном этапе расследования целесообразно учитывать информацию, полученную из финансово-кредитных организаций и операторов связи, а также сопоставлять сведения из иных источников.

Второй из указанных ранее способов совершения преступлений встречается реже и, как правило, требует тщательной подготовки со стороны преступника, однако ущерб от такого деяния, зачастую, будет гораздо больше, вплоть до банкротства юридического лица. Получить доступ к серверу такой организации удаленным способом крайне сложно, поскольку в силу специфики своей деятельности финансово-кредитные организации имеют достаточно серьезную защиту и при попытке получения доступа к системе извне, может сработать предупреждение, а система попросту отключится во избежание потенциальных финансовых потерь. Поэтому злоумышленники в подобных случаях используют самое незащищенное место такой системы – человека. Выяснив, кто из сотрудников финансово-кредитной организации работает в конкретном филиале на интересующей их должности, к примеру, главный бухгалтер или заместитель директора филиала, преступники предпринимают меры по размещению

вредоносного программного обеспечения на личные устройства данного сотрудника различными способами. Так как большинство лиц, как правило, используют как рабочих, так и в личных целях одни и те же электронные носители информации, например, флэш-карты, портативные жесткие диски, то с их помощью, после использования такого носителя на личном компьютере вредоносное программное обеспечение может быть доставлено на устройство, подключенное к внутренней сети финансово-кредитной организации. Далее, используя технологию удаленного доступа, злоумышленники будут способны осуществить достаточно широкий спектр неправомерных действий, направленных на их обогащение: хищение финансовых активов самой организации; хищение путем перевода денежных средств между счетами клиентов; шантаж и др. Рассмотрим каждый из возможных на этом этапе способов дальнейших действий преступников.

Первым способом, подлежащим рассмотрению, будет являться хищение финансовых активов финансово-кредитной организации. Осуществить подобного рода хищение преступникам возможно с помощью предварительного формирования поддельных платежных поручений, направляемых от имени клиентов данной организации в отношении третьих лиц. В качестве примера можно привести следующий случай. В феврале 2019 года на территории Омской области в отношении одного из региональных банков было совершено преступление вышеуказанным. Преступники осуществили неправомерный доступ к внутренней системе финансово-кредитной организации, после чего направили порядка 120 поддельных платежных поручений от имени её клиентов, суммами от 150 до 290 тысяч рублей каждое. Денежные средства были перечислены на более чем 90 расчетных счетов, оформленных в различных банках на физических лиц, проживающих на территории множества регионов Российской Федерации. Указанные транзакции были проведены через систему Центрального банка России. В результате указанного преступления финансово-кредитной организации был причинен ущерб на сумму, превышающую 20 миллионов рублей. В ходе расследования установлено, что похищенные денежные средства в течение суток были обналичены в банкоматах, расположенных в 12-ти различных субъектах Российской Федерации.

Вторым способом совершения вышеуказанной категории преступлений является хищение, совершенное путём перевода между счетами клиентов финансово-кредитной организации. Данный способ может использоваться злоумышленниками для маскировки своего проникновения в систему. Поскольку в первом случае велик риск быстрого обнаружения сомнительных операций сотрудниками Центрального банка Российской федерации злоумышленники могут сокрыть свое влияние на систему с помощью приобретения банковских карт, оформленных на третьих лиц, являющихся клиентами изначальной финансово-кредитной организации. После чего воспользовавшись доступом в личный кабинет клиента осуществить переводы похищенных денежных средств на любые иные счета, а также приобрести криптовалюту или обналичить в банкомате.

Третьим способом воздействия на систему финансово-кредитной организации с целью извлечения выгоды может являться вымогательство, выраженное в угрозе распространения сведений о клиентах данной организации, что может повлечь крупный репутационный ущерб. Данный способ совершения преступления зачастую обладает высокой латентностью, так как привлечение внимания со стороны правоохранительных органов к конкретной организации и последующие мероприятия также могут нанести ей дополнительный ущерб. Вследствие чего, потерпевшие от действий злоумышленников могут согласиться с их требованиями, и перечислить запрошенные денежные средства в целях урегулирования ситуации без привлечения помощи сотрудников правоохранительных органов. Данный способ представляет особую сложность, при выявлении, а также при последующем расследовании преступления.

Подводя итог, стоит отметить, что сегодня преступники изобретают все новые способы совершения хищений у кредитно-финансовых организаций с использованием информационно-телекоммуникационных технологий. Привести полную классификацию способов весьма затруднительно. Однако в целях противодействия такого рода преступности, сотрудникам правоохранительных органов необходимо повышать свою квалификацию в области информационно-телекоммнуникационных технологий для того чтобы эффективно осуществлять свои обязанности.

Дарменов Акынкали Даутбаевич,
начальник Карагандинской академии МВД Республики Казахстан
им. Б. Бейсенова, к.ю.н., генерал-майор полиции, a.darmenov@kpa.gov.kz
(Карагандинская академия МВД Республика Казахстан, Республика Казахстан)

ПРИНЦИПЫ УГОЛОВНОГО ПРАВА И ОСНОВАНИЯ ИХ УСТОЙЧИВОГО РАЗВИТИЯ

Аннотация. Научная статья представляет собой глубокий анализ основополагающих принципов уголовного права, рассматривая их актуальность. В статье автором особое внимание уделяется аспектам устойчивого развития принципов в контексте социокультурных и технологических изменений. Исследованием определено, что принципы уголовного права представляют собой фундаментальные нормы и основополагающие идеи, которые лежат в основе организации и функционирования уголовно-правовой системы в обществе.

Ключевые слова: принципы, уголовная ответственность, судебная система, правопорядок, наказание, основополагающие идеи, баланс интересов, общество.

PRINCIPLES OF CRIMINAL LAW AND THE BASIS FOR THEIR SUSTAINABILITY

Annotation. The scientific article is an in-depth analysis of the fundamental principles of criminal law, considering their relevance. In the article the author pays

special attention to the aspects of sustainable development of principles in the context of socio-cultural and technological changes. The study determines that the principles of criminal law are fundamental norms and fundamental ideas that underlie the organization and functioning of the criminal legal system in society.

Keywords: Principles, criminal responsibility, judiciary, rule of law, punishment, fundamental ideas, balance of interests, society.

Уголовное право играет важную роль в поддержании справедливости и правопорядка в современном обществе. Догматы уголовного права служат важнейшими руководящими принципами, которые определяют, как устроена и функционирует система уголовного правосудия. Рассмотрение принципов в правовой сфере представляет собой проблему, находящую постоянное внимание юристов различных областей права. Такая устойчивость в интересе к исследованию принципов и их сущности сохраняется на протяжении значительного времени. Мы полагаем, что их устойчивость обусловлена несколькими переменными, в том числе их уникальной структурной связью с содержанием соответствующей отрасли права. Их положение в правовой системе, придающее им исходный и векторный характер по отношению к другим нормам, обусловливает их специфику. Именно поэтому даже незначительные изменения общих или специальных норм в той или иной отрасли права требуют учета корректировки норм, называемых принципами права.

Еще одним фактором является постоянное проникновение зарубежных норм права, которые оказывают устойчивое влияние на национальное законодательство. Основной целью этого влияния является модификация отечественного законодательства с целью приближения его к международным нормам.

Уголовное законодательство Республики Казахстан основывается на Конституции Республики Казахстан и общепризнанных принципах и нормах международного права [1]. Конституция Республики Казахстан имеет высшую юридическую силу и прямое действие на всей территории Республики. В случае противоречий между нормами уголовного законодательства и Конституции Республики Казахстан действуют положения Конституции [2].

По мнению Е.А. Багуна, основополагающие принципы уголовного права – это идеи, которые служат ориентирами и закреплены в уголовном законодательстве, что делает их необходимыми для правоприменения. Данные идеи отражают социально-политические, экономические и интеллектуальные условия эволюции общества и его ценности [3, с. 23].

В то же время под принципами уголовного права В.Д. Филимонов понимает выраженные в уголовном законодательстве требования к созданию законов, их исполнению и поведению граждан. Данные требования обусловлены Конституцией, международными договорами о правах человека, целями борьбы с преступностью. Положения также служат для определения содержания всей или значительной совокупности правовых норм и объединения их в целостный свод уголовного права [4, с. 34].

По нашему мнению, принципы уголовного права представляют собой ключевые нормы, лежащие в основе структуры уголовной системы. Принципы

формируют основные положения гарантирования прав и свобод граждан в уголовном процессе.

Для принципов характерным является наличие только им присущих признаков, к которым следует отнести: отражение в концентрированной форме наиболее важных и прогрессивных сторон экономической, политической, идеологической и нравственной сфер общественной жизни; фиксацию (прямую или косвенную) в действующем законодательстве (прежде всего в Конституции); наличие значительной устойчивости и системообразующих свойств; копирование своеобразия национальной правовой системы; самостоятельное регулятивное значение; исполнение роли своеобразного руководящего начала для правотворческой, правоприменительной, правоохранительной, интерпретационной и иной юридически значимой деятельности [5, с. 51].

Учитывая скорость, с которой в современную эпоху меняются общество, культура и технологии, крайне важно, чтобы доктрины уголовного права оставались актуальными. В свете растущей глобализации и взаимодействия различных культурных контекстов уголовное право должно адаптироваться к этим изменениям, чтобы гарантировать эффективное регулирование межличностных отношений.

В частности, с развитием информационных технологий и цифровой среды появляются новые виды преступлений, такие как киберпреступления, нарушения прав интеллектуальной собственности и посягательства на цифровую безопасность. Для эффективного контроля над цифровой реальностью эти проблемы требуют не только адаптации ранее существовавших концепций, но и разработки новых методов в уголовном праве.

Требования современности не могут заставить основы уголовного права оставаться неизменными. В свете развивающихся условий эти принципы должны постоянно анализироваться и обновляться, чтобы обеспечить их устойчивость. Тщательный анализ влияния технологий и развития общества на уголовное право должен быть частью этого процесса. Например, опасения по поводу биотехнологий и искусственного интеллекта должны быть приняты во внимание в свете того, как быстро развиваются технологии. Какое влияние могут оказать новые технологии на такие понятия, как справедливость и определенность наказания? Какие моральные принципы следует принимать во внимание при использовании новых технологий в уголовном праве? Тщательное изучение этих проблем с учетом общественных норм и современных требований должно стать основой для формулирования руководящих принципов.

Восприятие и применение уголовного права существенно изменяется под влиянием социокультурных и технических преобразований. Изменение социальных норм и ценностей, в частности, является отражением социокультурных сдвигов и оказывает влияние на восприятие правосудия и применение закона. Технологические достижения, связанные с искусственным интеллектом, оказывают дополнительное давление на систему уголовного правосудия.

Применение новых технологий может привести к возникновению этических норм, требующих реформирования принципов уголовного права, чтобы

удовлетворить потребности современного общества, требующего справедливости и честности.

Эффективность и долговечность уголовного права напрямую зависят от его способности адаптироваться к изменениям в обществе и технологиях. Чтобы обеспечить правосудие и верховенство закона в современном обществе, уголовное право должно постоянно отслеживаться и корректироваться в соответствии с этими изменениями.

Изложенное позволяет констатировать, что основополагающие нормы, составляющие принципы уголовного права, играют важнейшую роль в создании справедливой и эффективной правовой системы. Их главная цель – поддержание стабильности и справедливости системы уголовного правосудия, которая призвана контролировать социальные взаимодействия и сдерживать преступную деятельность.

Важно помнить, что успешная адаптация системы уголовного правосудия к современным проблемам общества зависит от постоянного обновления основ уголовного права. Принципы должны постоянно обновляться, чтобы обеспечить их актуальность и эффективность в свете стремительного прогресса в социально-культурной, экономической и технологической сферах.

Основополагающие концепции уголовного права, закрепленные в Конституции и других законодательных документах, гарантируют обоснованность и конституционность уголовно-правовых норм, а также определяют направление деятельности по обеспечению правопорядка. Их постоянное обновление направлено на то, чтобы система уголовного правосудия соответствовала стандартам справедливости, эффективности и правовой законности. Оно основано на тщательном анализе социокультурных тенденций и технологических достижений.

Таким образом, основы уголовного права выступают одновременно и динамичными понятиями, способными подстраиваться под динамику общественных отношений, и структурными компонентами правовой системы. Система уголовного правосудия нуждается в частом обновлении, чтобы оставаться актуальной, справедливой и способной решать проблемы, с которыми сталкивается современное общество.

Список использованной литературы

1. Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V // Казахстанская правда. 2014. 9 июля.

2. Конституция Республики Казахстан: принята 30 августа 1995 г. на республиканском // Ведомости Парламента Республики Казахстан. – 1996. – № 4. – Ст. 217.

3. Уголовное право России. Общая часть: учебник для бакалавров / отв. ред. А.И. Плотников. – Оренбург: ООО ИПК «Университет», 2016. – 442 с.

4. Филимонов В.Д. Принципы уголовной права. – М.: АО «Центр ЮрИнфоР», 2002. – 139 с.

5. Большой юридический словарь / А.В. Малько и др.; под. ред. А.В. Малько. – М.: Проспект, 2009. – 702 с.

Джаксыбаев Асанали Сапаргалиевич,
доцент кафедры уголовного процесса
доктор философии (Phd), майор полиции, e-mail: asanali29@mail.ru

Хасенов Ербол Амантаевич,
заместитель начальника кафедры уголовного процесса
подполковник полиции, e-mail: erbolhasenov@mail.ru

(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ ЭЛЕКТРОННОГО ФОРМАТА ДОСУДЕБНОГО РАССЛЕДОВАНИЯ

Аннотация. В статье подробно рассмотрены ключевые вопросы внедрения, функционирования и дальнейшего совершенствования электронного формата расследования уголовных дел. Авторами исследованы и изучены процессуальные особенности и технические возможности работы единого реестра электронных досудебных расследований, кратко освещен исторический аспект. Статья содержит мнения и позиции практических работников по вопросам применения электронного формата уголовных дел, правовую статистику по отдельным процессуальным решениям. Основная роль в статье уделена дальнейшему совершенствованию электронного формата досудебного расследования с изложением конкретных предложений, реализация которых способна вывести уголовный процесс на новый технический уровень.

Ключевые слова: уголовный процесс, электронный формат досудебного расследования, электронное уголовное дело.

ISSUES OF IMPROVING THE ELECTRONIC FORMAT OF PRE-TRIAL INVESTIGATION

Annotation. The article discusses in detail the key issues of the introduction, functioning and further improvement of the electronic format of criminal investigation. The authors investigated and studied the procedural features and technical capabilities of the unified register of electronic pre-trial investigations, briefly highlighted the historical aspect. The article contains opinions and positions of practitioners on the application of the electronic format of criminal cases, legal statistics on individual procedural decisions. The main role in the article is given to the further improvement of the electronic format of pre-trial investigation with the presentation of specific proposals, the implementation of which is able to bring the criminal process to a new technical level.

Keywords: criminal procedure, electronic format of pre-trial investigation, electronic criminal case.

В марте 2017 г. Генеральной прокуратурой Республики Казахстан на межведомственном совещании правоохранительных и специальных органов пре-

зентован проект по внедрению электронного формата расследования и электронного уголовного дела.

Как тогда высказался председатель Комитета по правовой статистике и специальным учетам Б. Мусин: «на сегодняшний день даже по не представляющим особую сложность в расследовании преступлениям досудебное производство перегружено, на что затрачиваются огромные ресурсы, такие как человеческие, финансовые и временные. Более того, отсутствие возможности своевременного доступа к процессуальным материалам уголовного дела и делам участников процесса сохраняет риски фальсификации материалов, что не позволяет в полной мере обеспечить прозрачность взаимоотношений правоохранительных органов и населения страны» [1].

Такие инициативы надзорного органа были положительно встречены участниками межведомственного совещания. Для их полной реализации необходимо было внести ряд изменений в уголовно-процессуальное законодательство.

Презентуя в Мажилисе Республики Казахстан пакет нововведений, экс-заместитель Генерального прокурора республики М. Ахметжанов отметил основные цели реформ:

– усиление уровня защиты прав человека;

– повышение состязательности сторон;

– расширение судебного контроля;

– упрощение процедуры расследования;

– исключение дублирования и четкое распределение полномочий между органами следствия, прокуратурой и судом [2].

Уже в декабре 2017 года в Уголовно-процессуальный кодекс [3] внесены изменения [4], предоставляющие возможность проводить расследование в электронном формате.

Законодательство получило новую норму, которая предусматривает понятие «формат уголовного производства» (статья 42-1 УПК), который может быть бумажным или электронным.

Согласно данным Верховного Суда Республики Казахстан, первое электронное уголовное дело было рассмотрено в январе 2018 года [5]. Также уголовно-процессуальное законодательство содержит понятие электронного документа, являющегося документом, информация в котором предоставлена в цифровой форме и удостоверена электронной цифровой подписью (п.15 ст.7 УПК).

Электронными документами могут являться: заявление об уголовном правонарушении, гражданский иск, замечание на полный или краткий протокол судебного заседания, протокол главного судебного разбирательства, ходатайство прокурора о восстановлении срока на подачу апелляционной жалобы, запрос на истребование уголовного дела, ходатайство, протест или представление о пересмотре вступивших в законную силу судебных актов. В электронном формате могут быть оформлены доказательства: заключение эксперта, заключение специалиста.

Участники уголовного процесса вправе предоставлять лицу, осуществляющему досудебное расследование, документы в форме электронного документооборота. Кодекс содержит общие нормы о ведении досудебного рассле-

дования в электронном формате, все же детали и уточнения предусмотрены Приказом Генерального прокурора Республики Казахстан от 03.01.2018 года «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате».

Согласно положениям Инструкции, электронное расследование осуществляется в информационной системе «Единый реестр досудебных расследований» (ИС ЕРДР). Данная система имеет модуль «Электронное уголовное дело», целью которого является ведение и архивное хранение электронных уголовных дел [6].

Участники уголовного процесса о принимаемых решениях оповещаются посредством SMS-сообщений, что стало возможным благодаря соответствующему функционалу. Ознакомление с материалами дела, подача жалоб, ходатайств, заявлений производится удаленно с любого компьютерного устройства через функционал «Публичный сектор».

Процессуальные документы, соответствующие тем или иным решениям и действиям, формируются в системе автоматически в ходе заполнения лицом, ведущим уголовный процесс, соответствующих граф и реквизитов. В настоящее время более 90 % всех уголовных дел расследуется именно в электронном формате.

Преимуществами такого формата являются отсутствие бюрократии, исключение возможности манипуляции, подмены, сокрытия процессуальных документов, устранение коррупционных рисков. Лицо, проводящее расследование, освобождено от постоянных «хождений» по кабинетам начальства, прокуроров и судей, так как последние при поступлении жалоб и обращений от участников процесса имеют возможность изучить уголовное дело удаленно.

При традиционном бумажном формате немалая часть рабочего времени следователя затрачивалась на техническую работу – формирование и скрепление материалов уголовного дела, нумерация листов, составление и изменение описи и т.д. Электронный формат позволяет не отвлекаться на побочные дела и рутинную работу, так как материалы досудебного расследования формируются системой автоматически. Электронный формат позволил устранить устоявшуюся практику постоянного ксерокопирования процессуальных документов, представляемых для обоснования решений следователя перед прокурором и судом.

Как известно, с 2021 года отечественная система уголовного процесса перешла на трехзвенную модель расследования «следователь – прокурор –суд», где каждому ее участнику отведена исключительная роль: следователь принимает процессуальное решение, прокурор проверяет его обоснованность, суд же дает окончательную оценку по совокупности обстоятельств при рассмотрении дела по существу.

Важным вопросом в ее функционировании является необходимый уровень скорости документооборота между всеми звеньями. Электронный формат как раз предполагает такую оперативность, т.е. решения, принятые органом, мгновенно отражаются у надзирающего прокурора в специальных вкладках, соответствующих срокам их изучения.

Во избежание нарушений система электронного дела ведет отсчет времени нахождения уголовного дела у прокурора, заранее сигнализируя о приближающихся сроках. О результатах изучения уголовного дела (связанного с ним решения) прокурором следователь узнает посредством соответствующих вкладок базы. Таким образом, созданная система полностью исключает контактное взаимодействие государственных органов-участников процесса, что свою очередь сохраняет ценные временные ресурсы и снижает вероятность не процессуальных контактов.

В настоящее время в систему электронного уголовного дела включены органы прокуратуры, уголовного преследования (МВД, КНБ, АФМ, Антикоррупционная служба, подразделения дознания МО), суды. На данный момент проводится работа по слиянию и интеграции системы «Е-дело» с программой документационного обеспечения органов судебной экспертизы и банками второго уровня.

Как высказался бывший начальник Следственного Департамента МВД Республики Казахстан (в настоящее время – начальник Департамента полиции Карагандинской области) С. Адилов, «цифровизация уголовного процесса позволила решить ряд чувствительных для населения вопросов, а также упростить процедуру сбора доказательств и составление процессуальных документов. Программа «Е- уголовное дело» охватывает все стадии уголовного процесса: регистрация преступления, ход расследования и исполнение приговора. Это позволяет исключить фальсификацию материалов уголовного дела, а также снизить материальные затраты, связанные с расследованием и нагрузку на орган расследования [7].

«Электронный формат позволяет сократить сроки расследований и финансовые затраты, минимизировать риски фальсификации материалов и доказательств, предоставляет доступ к материалам в режиме онлайн, упрощает процедуру сбора доказательств и составления процессуальных документов, а также позволяет в полной мере обеспечить прозрачность взаимоотношений судебной системы, правоохранительных органов и населения страны» [8].

Б. Нургалиев считает, что внедрение электронного производства приблизило работу отечественных правоохранительных органов к общепринятым международным стандартам [9, с. 52].

Но, как и в любом деле, имеются вопросы, связанные с совершенствованием. По нашему мнению, цифровой процесс должен быть помощником следователя, автоматизировав ряд следственных действий и проверяя правильность принимаемых решений.

Так, следующей ступенью в совершенствовании уголовного процесса должен стать фунционал «умное» электронное дело. Его суть выражена во внедрении в логику базы алгоритмов, которые будут сопровождать действия требований уголовного и уголовно-процессуального законодательств.

К примеру, прекращение уголовного дела не допускается в отношении лица в течение срока давности привлечения к уголовной ответственности после освобождения от уголовной ответственности в связи с примирением сторон за ранее совершенное преступление (ст.68 УК) [10].

Однако как показывают статистические данные, следователями допускаются незаконные факты повторного примирения.

За 2022 год только по городу Караганде прокурорами ввиду неправильного применения статьи 68 Уголовного кодекса отказано в утверждении 12 решений о прекращении уголовных дел [11]. Очевидно, что причинами нарушений данных нарушений явились субъективные факторы. Мы полагаем, что электронное уголовное дело должно быть наделено интеллектом (логикой), позволяющим предостеречь сотрудника органа досудебного расследования от процессуальных ошибок. Например, в случае ввода следователем решения о прекращении дела логика базы проверяла бы историю привлечения подозреваемого к уголовной ответственности, не позволяя ввести информационно-учетный документ в случае повторного примирения.

Аналогичным образом, алгоритмы базы запрещали бы вводить решения о направлении уголовных дел прокурору в порядке согласительного производства по особо тяжким преступлениям, а также начинать или продолжать досудебные расследования по делам частно-публичного обвинения без вложения заявления потерпевшего.

В практической деятельности распространены случаи, когда органами досудебного расследования в нарушение требований Уголовно-процессуального кодекса прокурору в порядке согласительного производства в форме сделки о признании вины направлялись дела по особо тяжким преступлениям. Такие действия совершались в последний день отчетного периода в целях достижения ведомственных показателей по количеству направленных прокурору уголовных дел.

К примеру, в последний день первого квартала текущего года «*» отделом полиции города «*» прокурору с ходатайством о заключении процессуального соглашения в форме сделки о признании вины направлено 3 уголовных дела по особо тяжким преступлениям, из которых в двух делах отсутствовали ходатайства самих подозреваемых.

Данное обстоятельство привело к возвратам уголовных дел, а также к тому, что время изучения уголовного дела прокурором было включено в общий срок расследования, так как, согласно пп.4 п.3 ст.192 Уголовно-процессуального кодекса, время нахождения уголовного дела у прокурора не включается в срок досудебного расследования только при наличии ходатайства о заключении процессуального соглашения [3].

С учетом пересчета срока досудебного расследования было установлено, что допущено его нарушение, что вынудило орган досудебного расследования прекратить производства по реабилитирующим основаниям при наличии лиц, содержащихся под стражей.

Предлагаемые нами ограничения могут действовать по всем требованиям действующего законодательства. Полагаем, что данное новшество выведет электронное производство на новый уровень, исключит манипуляции и субъективный человеческий фактор в принятии значимых решений.

Список использованной литературы

1. В Генеральной прокуратуре РК презентована система электронного уголовного дела [Электронный ресурс] // URL: http://www.ratel.kz/kaz/v_genpro kurature_rk_prezentovana_sistema_ elektronnogo_ugolovnogo_dela.

2. Ахметжанов М.М. Поправки по вопросам модернизации процессуальных основ правоохранительной деятельности [Электронный ресурс] // URL: http://zhmb.kgd.gov.kz/ru/news/ popravki-po-voprosam-modernizacii-processualnyh-osnov-pravoohranitelnoy-deyatelnosti-9- 21495.

3. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан // URL: http://adilet. zan.kz/rus.

4. О внесении изменении и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности: Закон Республики Казахстан от 21 декабря 2017 г. № 118-VI ЗРК [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан // URL: http://adilet.zan.kz/rus.

5. В соответствии с обновленным УПК в Казахстане впервые рассмотрено «электронное уголовное дело» [Электронный ресурс] // Верховный Суд Республики Казахстан. – URL: http://sud. gov.kz/rus/news/v-sootvetstvii-s-obnovlennym-upk-v-kazahstane-vpervye-rassmotreno-elektronnoe-ugolovnoe-delo.

6. Приказ Генерального прокурора Республики Казахстан от 03.01.2018 года №2 «Об утверждении Инструкции о ведении уголовного производства в электронном формате» [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан // URL: http://adilet.zan.kz/rus.

7. Цифровизация уголовного процесса решит ряд чувствительных для населения вопросов [Электронный ресурс] // URL: https://www.inform.kz/ru/ cifrovizaciya-ugolovnogo-processa-reshit-ryad-chuvstvitel-nyh-dlya-naseleniya-voprosov-sanzhar-adilov_a3804021.

8. Как электронное производство упрощает процесс уголовных дел Электронный ресурс] // URL: https://aqmolanews.kz/ru/2023/04/13/kak-elektronnoe-sudoproizvodstvo-uproshaet-process-ugolovnyh-del/.

9. Нургалиев Б.Б. Новеллы уголовно-процессуального законодательства Республики Казахстан и его совершенствование // Хабаршы–Вестник. – 2019. – № 1. – С.52–55.

10. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.). [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан. – URL: http:// adilet.zan.kz/rus.

11. Отчет о работе прокурора по надзору за законностью уголовного преследования [Электронный ресурс] // URL: http://qamqor.gov.kz/.

Дырма Сергей Валерьевич,
старший преподаватель кафедры гуманитарных и социально-экономических дисциплин, майор полиции, e-mail: s.dyrma@mail.ru

Пироженко Илья Сергеевич,
e-mail: pirozhenkoilia@gmai.com

(Крымскоий филиал Краснодарского университета МВД России, Российская Федерация)

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье рассматриваются особенности социальной инженерии как угрозы информационной безопасности, а также способа совершения преступлений в сфере информационно-коммуникационных технологий. Рассмотрены меры, направленные на повышения эффективности противодействия социальной инженерии для снижения рисков утечки конфиденциальной информации.

Ключевые слова: информация, информационно-телекоммуникационные технологии, противодействие, социальная инженерия, информационная безопасность, защита информации, фишинг, психологическое воздействие.

SOCIAL ENGINEERING AS A THREAT TO INFORMATION SECURITY

Annotation. The article examines the features of social engineering as a threat to information security, as well as a method of committing crimes in the field of information and communication technologies. Measures aimed at increasing the effectiveness of countering social engineering to reduce the risks of leakage of confidential information are proposed

Keywords: information, information and telecommunication technologies, counteraction, social engineering, information security, information protection, phishing, psychological impact.

Еще в 19 веке известный англо-немецкий банкир, бизнесмен и финансист Натан Майер Ротшильд озвучил следующий афоризм «Кто владеет информацией – тот владеет миром» [4].

Даже непрофессиональный взгляд на динамику развития современного, в первую очередь информационного, общества позволяет заключить, что сказанное Ротшильдом нисколько не утратило значимости, а скорее приобрело все большую актуальность ввиду повсеместной цифровизации различных сфер жизни общества.

Повсеместная информатизации экономической и социальной сфер жизни общества на рубеже 21 века определяет необходимость защиты информации от различных видов угроз. Обеспечение информационной безопасности с каждым

годом становится все более актуальным для жизни граждан, экономической деятельности различных организаций, а также деятельности правоохранительных органов.

По данным лаборатории Касперского целевым кибератакам в 2021 году подвергались самые разные отрасли, больше всего их фиксировалось в государственных, промышленных, финансовых и ИТ-организациях [5].

Особое место среди целевых кибератак занимает социальная инженерия, которая по праву является одним из наиболее эффективных и опасных видов угроз, поскольку в бешенстве случаев позволяет злоумышленникам получить конфиденциальную информацию от граждан и (или) организаций не прибегая к использованию вредоносного программного обеспечения, которое может быть обнаружено системой информационной безопасности или антивирусным программным обеспечением.

Не вызывает сомнения тот факт, что с каждым годом количество преступлений против собственности, совершаемых с использованием информационно-коммуникационных технологий неуклонно растет. На наш взгляд, данная тенденция обусловлена как интенсификацией внедрения в жизнь человека современных информационных технологий, электронных средств платежа, онлайн-маркетинга и мобильных средств коммуникации, так и совершенствованием методик психологического воздействия на граждан со стороны злоумышленников.

Социальная инженерия в самом общем своем понимании представляет собой совокупность методик получения конфиденциальной информации, либо доступа к таковой посредством психологического воздействия на человека. Социальная инженерия часто рассматривается как «манипулирование поведением человека с помощью использования социальных и психологических навыков» [3, с. 135].

Изложенное позволяет подвести итог о том, что так или иначе в любой информационной системе одним из наиболее уязвимых элементов является человек. В отличие от программной защиты информационной системы какой-либо коммерческой организации человек далеко не всегда может обладать необходимыми морально-психологическими качествами, позволяющими эффективно противостоять методам психологического воздействия со стороны профессионально подготовленных злоумышленников.

Стоит отметить, что количество различных техник социальной инженерии, выделяемых специалистами в области информационной безопасности, достаточно велико. Выбор конкретной техники зависит от целей, преследуемых злоумышленником, а также от условий их применения. Предлагаем рассмотреть лишь некоторые из них.

Quid Pro Quo (от лат. qui pro quo – «кто вместо кого»). Особенность данной техники заключается в том, чтобы внушить объекту атаки (жертве), что возникли существенные проблемы, требующие немедленного разрешения. Например, проблемы с компьютером, банковским счетом или страховкой. Злоумышленник в ходе применения указанной техники старается запугать свою цель, убеждая в серьезности проблемы и фатальных последствиях. Способ убе-

ждения в данном случае является наиболее эффективным, поскольку осуществляется прямое воздействие на психику человека [2, с. 86].

В дальнейшем, после введения цели атаки (жертвы) в стрессовое зависимое состояние злоумышленник предлагает решение возникшей проблемы. Соответственно «решение» возникшей проблемы может сопровождаться необходимостью сообщить злоумышленнику логин или пароль к каким-либо информационным ресурсам, установить какое-либо программное обеспечение и т.п.

TailGatin является одной из наиболее творческих видов атак класса социальной инженерии. Представим, что злоумышленнику необходимо получить физический доступ в какое-либо помещение организации, не имея на то соответствующего разрешения.

Например, он может прийти в здание в костюме представителя службы доставки, клининговой компании, или же вообще представиться сотрудником атакуемой организации и вежливо попросить одного из сотрудников открыть ему дверь, поскольку свою карту-пропуск он якобы оставил дома и опаздывает на важную встречу и т.д. В дальнейшем злоумышленник, получив физический доступ в помещение организации может тайно загрузить в локальную сеть какое-либо вредоносное программное обеспечение.

Фишинг является самой известной техникой социальной инженерии, используемой злоумышленниками. Злоумышленник создает поддельный портал поддержки или веб-сайт уважаемой компании и отправляет ссылки своим целям по электронной почте, чтобы обманом заставить их раскрыть конфиденциальную информацию [1, с. 35].

Техника Road Apple (или «дорожное яблоко») предполагает использование физических носителей информации и создания ситуации, при которой жертва атаки проявила бы интерес к содержимому данного носителя информации и попыталась бы его изучить с использованием своего персонального компьютера. При загрузке информации с «подброшенного» носителя на персональный компьютер жертвы может быть загружено вредоносное программное обеспечение.

Подводя итог изложенному, следует отметить, что противодействие атакам класса социальной инженерии является важным компонентом обеспечения информационной безопасности государственных органов, коммерческих организаций и отдельных граждан.

По нашему мнению, система защиты от различных техник социальной инженерии представляет комплекс организационных, программных и технических мер, направленных на противодействие социальной инженерии по различным направлениям.

К числу организационных мер противодействия социальной инженерии, наряду с мероприятиями по разграничению доступа к информации для различных категорий сотрудников организации, можно отнести мероприятия по обучению сотрудников (граждан), их информированию о различных техниках и методах, в том числе психологического воздействия, со стороны потенциальных злоумышленников.

Использование программных средств защиты позволяет в отдельных случаях достаточно эффективно противодействовать фишингу и иным техникам социальной инженерии, предполагающим использование вредоносного программного обеспечения. Даже если гражданин (сотрудник) стал жертвой фишинга и перешел по отправленной злоумышленником ссылке, в ряде случаев необходимое программное обеспечение позволит предотвратить потенциальную угрозу информационной безопасности.

К числу технических мер, наряду с использование средств видеофикации в организациях можно отнести использование систем биометрической идентификации для входа в помещение организации или иного помещения, в котором осуществляется обработка конфиденциальной информации.

В заключении отметим, что совершенствование технических и программных средств защиты информации далеко не всегда является абсолютно надежным для решения вопросов обеспечения информационной безопасности. Наиболее уязвимым звеном системы обеспечения информационной безопасности является сам человек, поскольку воздействие на человеческую психику путем обмана и злоупотребления доверием во все времена было наиболее эффективным способом получения необходимой информации.

В целях минимизации риска утечки конфиденциальной информации также важно уделять внимание повышению уровня подготовки персонала организации в условиях возможного психологического воздействия со стороны потенциальных злоумышленников. Чем выше значимость и конфиденциальность информации, обрабатываемой сотрудниками организации, тем более системным должен быть подход к повышению уровня указанной подготовки в условиях моделирования потенциальных и возможных угроз.

Список использованной литературы

1. Пчелинцева Н.В., Ворошилова В.М., Чепраков И.В. Социальная инженерия как аспект информационной безопасности [Электронный ресурс] // Наука и образование. – 2023. – №1 // URL: https://cyberleninka.ru/article/n/sotsialnaya-inzheneriya-kak-aspekt-informatsionnoy-bezopasnosti.

2. Созаев С.С., Кунашев Д.А. Социальная инженерия, ее техники и методы ее противодействия // Вестник науки. – 2020. – № 2 (23). – С. 85–88.

3. Янгаева М.О. Социальная инженерия как способ совершения киберпреступлений // Вестник Сибирского юридического института МВД России. – 2021. – № 1 (42). – С.133–138.

4. Ротшильд Натан Майер [Электронный ресурс] // URL: https://ru.wikipedia.org/wiki/Ротшильд, _Натан_Майер.

5. «Лаборатория Касперского»: госучреждения, промышленность, ИТ и финансовый сектор чаще всего подвергаются целевым кибератакам[Электронный ресурс] // URL: https://www.security-center.ru/news/testy-i-otchety/laboratoriya-kasperskogo-gosuchrezhdeniya-promyshlennost-it-i-finansovyy-sektor-chashche-vsego-podve/?sphrase_id=1038605.

Ералина Саида Ермагамбетовна,
заместитель начальника Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова, к.ю.н., доцент, полковник полиции, s.eralina@kpa.gov.kz

Шульгин Евгений Петрович,
начальник кафедры кибербезопасности и информационных технологий к.ю.н., майор полиции, e.shulgin@kpa.gov.kz

(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

О ДЕЯТЕЛЬНОСТИ КАФЕДРЫ КИБЕРБЕЗОПАСНОСТИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАРАГАНДИНСКОЙ АКАДЕМИИ МВД РЕСПУБЛИКИ КАЗАХСТАН ИМ. Б. БЕЙСЕНОВА

Аннотация. В научной статье раскрывается деятельность кафедры кибербезопасности и информационных технологий. Важно отметить, что проведение данной конференции связано с празднованием годовщины создания данного структурного подразделения на базе Карагандинской академии МВД Республики Казахстан. Необходимость такого шага обусловлена стремительным развитием цифровых технологий и компьютеризации различных сфер деятельности. Кибербезопасность стала ключевым аспектом, требующим особого внимания и специализированного подхода, учитывая возрастающую сложность кибератак, утечек информации и других угроз, которые могут повлиять на стабильность и безопасность общества.

Ключевые слова: Республика Казахстан, кафедра, кибербезопасность, информационные технологии, обучение, учебные дисциплины, правоохранительная деятельность.

ON THE ACTIVITIES OF THE CYBERBESECURITY AND INFORMATION TECHNOLOGIES CHAPTER OF THE KARAGANDIN ACADEMY OF THE MIA OF THE REPUBLIC OF KAZAKHSTAN NAMED B. BEYSENOV

Annotation. The scientific article reveals the activities of the Department of Cyber Security and Information Technology. It is important to note that this conference is associated with the celebration of the anniversary of the establishment of this structural unit on the basis of the Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan. The necessity of such a step is due to the rapid development of digital technologies and computerisation of various spheres of activity. Cyber security has become a key aspect that requires special attention and a specialised approach, given the increasing complexity of cyber attacks, information leaks and other threats that can affect the stability and security of society.

Keywords: Republic of Kazakhstan, department, cyber security, information technology, training, academic disciplines, law enforcement.

Проводима научно-практическая конференция «Противодействие киберпреступности: состояние, тенденции, перспективы», приуроченная к годовщине со дня образования кафедры кибербезопасности и информационных технологий, является важным мероприятием, направленным на обмен опытом, представление новых научных исследований, а также обсуждение стратегий и методов в области кибербезопасности и информационных технологий. Участие в конференции предоставит ученым и практикующим специалистам возможность расширить свои знания, улучшить практические навыки и внести свой вклад в повышение уровня кибербезопасности как в регионе, так и в целом мире.

Учебный процесс, в сфере кибербезопасности приобретает стратегическую значимость в контексте противодействия киберпреступности [1, с. 83]. В условиях постоянного эволюционного развития информационных технологий и их широкого использования в различных сферах общества, обучение курсантов и действующих практических сотрудников в области кибербезопасности становится неотъемлемым элементом общенациональной стратегии обеспечения информационной стабильности.

Приступая к предмету научного исследования, следует начать с того, что в настоящее время наблюдается значительный рост количества уголовных правонарушений в сфере информационно-телекоммуникационных технологий. Для борьбы с подобного рода преступными проявлениями на базе Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова приказом Министерства внутренних дел Республики Казахстан № 966 от 15 декабря 2022 г. создана кафедра кибербезопасности и информационных технологий [2].

Деятельность кафедры направлена на подготовку кадров для оперативных, следственных и оперативно-криминалистических подразделений по выявлению, пресечению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Профессорско-преподавательским составом кафедры проводятся занятия на факультете профессиональной подготовки, факультете послевузовского образования, а также на факультете дополнительного образования (в рамках курсов повышения квалификации) по следующим направлениям и дисциплинам:

– Information and communication technologies;

– Раскрытие и расследование незаконного сбыта наркотических средств, совершенного с использованием сети Интернет;

– Особенности расследования мошенничества в сфере компьютерной информации;

– Основы информационной безопасности;

– Безопасность информационных систем;

– Организация реагирования на инциденты информационной безопасности;

– Цифровая криминалистика.

Целью кафедры является подготовка высококвалифицированных специалистов в раскрытии и расследовании уголовных правонарушений в информационном пространстве, имеющих глубокую теоретическую подготовку, получивших профессиональные знания и навыки по расследованию и раскрытию

преступлений в информационном пространстве, составлению процессуальных документов, применению действующего законодательства, регламентирующего вопросы досудебного расследования, дознания и судебного разбирательства.
Основная задача кафедры – организация и осуществление на высоком уровне учебной, воспитательной и научно-методической работы по раскрытию и расследованию уголовных правонарушений в информационном пространстве.
К проведению учебных занятий привлекаются практические сотрудники МВД Республики Казахстан, а также сотрудники IT-холлдинга «Kazdream Technologies» и «Seven Hills of Kazakhstan».

На кафедре имеется специализированная учебная аудитория – киберполигон «Kazdream Technologies». В ходе проведения учебных занятий используются цифровые инструменты IT-холдинга «Kazdream Technologies», которые направлены на оптимизацию стадии досудебного производства, среди которых:

1) CROSS – раскрытие преступлений посредством анализа сотовых данных;

2) Triton – инструмент визуального анализа больших данных;

3) IRIS – спецкомплекс по определению местоположения абонента сотовой связи;

4) Сыщик – автоматизация процесса по раскрытию преступлений, связанных с криминальными телефонами (в т.ч. раскрытие преступлений прошлых лет);

5) ARGUS – программный комплекс для оперативной разработки преступников в Интернете [3].

Также на базе кафедры имеется лаборатория цифровой криминалистики (Seven Hills of Kazakhstan) оборудованная инструментами, предназначенными для восстановления поврежденных цифровых устройств: паяльные станции, микроскопы, дымоуловители, лабораторные блоки питания, мультиметры, вакуумные сепараторы, наборы инструментов (более 40 позиций), наборы расходных материалов (более 40 позиций), а также аппаратно-программным комплексом по извлечению и анализу данных (MOBILedit Forensic) [4].

В учебном процессе акцентируется не только техническая компетентность, но и способность к критическому анализу, стратегическому мышлению и предвидению потенциальных угроз. Обучение включает в себя изучение современных методов киберзащиты, анализа уязвимостей, разработки и реализации превентивных мер, а также освоение этических и правовых норм, регулирующих деятельность в киберпространстве.

На базе кафедры функционирует группа киберволонтеров, представляющая собой добровольное объединение обучающихся Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова, направленное на противодействие распространению в сети Интернет противоправной информации и информации, способной причинить вред здоровью и развитию личности детей и подростков. Также группа киберволонтеров проводит большую разъяснительную и просветительскую работу с населением по профилактике киберпреступности.

Достигнутые результаты: в отдел по борьбе с киберпреступностью УКП ДП Карагандинской области предоставлена информация о более чем 1 000 слу-

чаях распространения в сети Интернет запрещенного контента; деятельность более 100 сайтов распространяющих в сети Интернет запрещенный контент заблокирована через платформу «Киберщит Казахстана»; киберволонтерами проводятся выездные занятия на тему: «Правда безопасного поведения в интернете и социальных сетях».

Таким образом, обучающиеся и практические сотрудники, прошедшие обучение в данной области, выступают в роли ключевых катализаторов инновационных подходов в предотвращении и реагировании на киберугрозы. Учебные программы на кафедре ориентированы на формирование специалистов, обладающих не только техническими навыками, но и способных к поиску новаторских решений, учету социокультурных аспектов и соблюдению этических стандартов в цифровом пространстве.

Список использованной литературы

1. Зегжда Д.П. Теоретические основы киберустойчивости и практика прогностической защиты от кибератак. – СПб.: ПОЛИТЕХ-ПРЕСС, 2022. – 490 с.

2. Кафедра кибербезопасности и информационных технологий [Электронный ресурс] // URL: https://kpa.gov.kz/kafedra-kiberbezopasnosti-i-informacionnyh-tehnologij/

3. IT-холдинг Kazdream Technologies [Электронный ресурс]: сайт IT-холдинга // URL: https://kazdream.kz/o-kompanii/

4. Seven Hills of Kazakhstan [Электронный ресурс]: сайт IT-компании // URL: https://www.sevenhills.kz/.

Исетова Жанна Муратовна,
старший преподаватель кафедры уголовного процесса
м.ю.н., майор полиции, zh.isetova@kpa.gov.kz
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

МЕТОДЫ ПРОФИЛАКТИКИ КИБЕПРЕСТУПЛЕНИЙ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. В статье обоснована необходимость предупреждения современных видов правонарушений, в частности с использованием информационных технологий.

Ключевые слова: борьба, досудебное производство, международные стандарты, предупреждение.

METHODS OF PREVENTION OF CYBERCRIME IN THE REPUBLIC OF KAZAKHSTAN

Annotation. The article substantiates the need to prevent modern types of offenses, in particular with the use of information technology.

Keywords: struggle, pre-trial proceedings, international standards, prevention.

Большими темпами происходит внедрение новых технологий, которые становятся неотъемлемой частью в жизни человечества.

Республика Казахстан выбрала активную позицию в вопросах использования электронно-информационных технологий, как в деятельности государственных органов, так и в иных сферах жизнедеятельности человека и общества.

Президент Казахстана Касым-Жомарт Токаев в своем выступлении на пленарном заседании форума Digital Bridge-2022 назвал пять приоритетов в цифровой трансформации страны. При этом отметил, что именно цифровая трансформация является определяющим фактором конкурентоспособности не только отдельных компаний, но и целых стран и регионов [1].

Современное время предполагает использование передовых технологий всеми гражданами нашей страны. Использование цифровых технологий предоставляет ряд преимуществ, среди которых: форсирование обмена информацией, упрощение доступа населения к государственным и коммерческим услугам, появление новых возможностей и дальнейшее развитие и создание цифровых продуктов.

В отличие от традиционных видов преступлений, история которых уходит в прошлое, киберпреступность явление новое и молодое. Именно такие свойства Глобальной сети, как быстрота и дешевизна трансакций, анонимность, трансграничность, создают уникальные условия для совершения новых видов преступлений и для качественного видоизменения традиционных [2].

Вопросы борьбы с киберпреступностью становятся все более актуальными. Необходимо понимать, что кибепреступность является достаточно новым «веянием» и меры борьбы с ней разрабатываются и будут разрабатываться.

В настоящее время существует большое количество различных видов и способов преступлений, совершаемых дистанционно с помощью информационных и компьютерных технологий [3].

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство. Большинство кибератак совершается киберпреступниками или хакерами с целью получения финансовой прибыли. Однако целью кибератак может быть и выведение компьютеров или сетей из строя – из личных или политических мотивов [4].

Основной мерой предупреждения уголовных правонарушений данного вида является информированность граждан о существующих видах и схемах киберпреступности, которые с каждым годом видоизменяются и становятся более изощренными [5, с. 62].

Список использованной литературы

1. 5 приоритетов цифровой трансформации Казахстана [Электронный ресурс] // https://digitalbusiness.kz.

2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.). [Электронный

ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан. – URL: http:// adilet.zan.kz/rus.

3. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан // URL: http://adilet. zan.kz/rus.

4. Что такое киберпреступность? Защита от киберпреступности [Электронный ресурс] // https://www.kaspersky.ru.

5. Ибадиллаұлы Ұ. Интернет-хищение чужого имущества: уголовно-правовые и криминологические аспекты: дисс. маг. … юрид. наук. – Косшы, 2022. – 102 с.

Канафин Арман Абайбекович,
Қазақстан Республикасы Б. Бейсенов атындағы
Қарағанды академиясы жоғары оқу орынан кейінгі білім беру факультетенінің
ғылыми-педагогикалық магистратураның магистранты, полиция майоры
(Қазақстан Республикасы ІІМ Б. Бейсенова атындағы Қарағанды академиясы, Қазақстан Республикасы)

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДЕ СЕРВИСТІК ТӘСІЛДЕРДІ ЕНГІЗУ

Аннотация. Полиция қызметтерінің сапасын арттыру. Ақпараттық қауіпсіздікті қамтамасыз ету. Полиция қызметіндегі шетелдік стратегиялар мен тәсілдер. Құқықтық саясат тұжырымдамасы. Фронт-лайн қызметкерлері қызметінің тиімділігін арттыру. Қолдау қызметтерінің жұмыс сапасын жетілдіру. Ақпараттық қауіпсіздік мәселелерін анықтау және талдау. Халықпен өзара іс-қимыл. ІІО бірыңғай ақпараттық кеңістігін қалыптастыру.

Түйінді сөздер: ақпараттық қауіпсіздік, полицияның сервистік моделі, сапалы қызметтер, құқықтық саясат тұжырымдамасы, фронт-лайн қызметкерлер, қолдау қызметтері, халықпен өзара іс-қимыл, ақпараттық кеңістік.

INTRODUCTION OF SERVICE APPROACHES TO ENSURING INFORMATION SECURITY

Annotation. Improving the quality of police services. Ensuring information security. Foreign strategies and approaches in policing. The concept of legal policy. Improving the efficiency of front-line employees. Improving the quality of work of support services. Identification and analysis of information security problems. Interaction with the population. Formation of a unified information space of the Department of Internal Affairs.

Keywords: information security, police service model, quality services, legal policy concept, front-line employees supporting services, interaction with the population, information space.

Қазіргі мемлекеттің полиция жүйесінің тиімді жұмыс істеуі, полиция қызметінің тиімділігі көбінесе полиция мен азаматтық қоғам институттарының өзара іс-қимылымен байланысты және қоғамның полицияға деген сенім деңгейінде көрінеді.

Полиция мен азаматтық қоғам институттарының өзара іс-қимылының серіктестік моделі дамыған заманауи мемлекеттерде әзірленген негізгі тұжырымдама болып табылады.

Қазақстандық полицияның жұмыстың сервистік моделіне көшуі туралы мемлекеттің басты стратегиялық құжаттарында айтылған. Мәселен, Қазақстан Республикасының 2025 жылға дейінгі ұлттық даму жоспарында (жалпыұлттық басымдық 4. Азаматтардың мүдделерін қорғаудағы әділ және тиімді мемлекет) қауіпсіз және құқықтық қоғам құру үшін полиция жұмысының күш көрсету моделінен құқық қорғау органдарының азаматтармен өзара іс-қимылының сервистік моделіне көшу көрсетілген [1].

Қазақстан Республикасында мемлекеттік басқаруды дамытудың 2030 жылға дейінгі тұжырымдамасына мемлекеттік басқарудың «адамға бағдарланған» моделін – «адамдар бәрінен бұрын» құру курсы бекітілген [2].

Қазақстан Республикасының 2030 жылға дейінгі құқықтық саясат тұжырымдамасында (5-бөлім. Құқық қорғау және сот жүйелері мен құқық қорғау институттарын дамытудың негізгі бағыттары) қоғамның, азаматтар мен бизнестің қажеттіліктеріне жауап беретін құқық қорғау жүйесінің сервистік моделін қалыптастыруға бағытталған құқық қорғау қызметін одан әрі жетілдіру қажеттілігі туралы айтылады [2].

Мемлекеттік органдардың, жеке және заңды тұлғалардың ақпараттық қауіпсіздігін қамтамасыз ету мониторингіне, сондай-ақ ақпараттық қауіпсіздік инциденттеріне, оның ішінде әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше немесе соғыс жағдайын енгізу жағдайларында алдын алу және жедел ден қою тетіктерін әзірлеуге көзқарастардың бірлігін қамтамасыз ету бұл маңызды элементтер емес.

Бүгінгі таңда қоғаммен қарым-қатынаста шет елдердің құқық қорғау органдарының басым идеологиясы полиция қызметіндегі ақпараттық құзыреттілік тұжырымдамасы болып табылады.

Сонымен, полицияның сервистік моделі – бұл полицияның идеологиясы мен ұйымдастырушылық стратегиясы азаматтарға сапалы полиция қызметтерін көрсетуге және қоғаммен серіктестікте қауіпсіздік мәселелерін шешуге бағытталған полиция қызметіне көзқарас деген түсінік беруге болады.

Қызмет көрсету моделінің мақсаты мен міндеттері. Мақсаты – бір нәрсенің бар болуының мақсаты мен мәні, оның болуының себебі. Полицияның сервистік моделі – қоғамның қауіпсіздігін қамтамасыз ету моделінің элементтерінің бірі. Олардың айтуынша, полицияның сервистік моделін енгізудің миссиясы немесе мақсаты қоғамдық қауіпсіздікті қамтамасыз ету болып табылады.

Тәжірибе көрсеткендей, басқа елдерден институционалдық модельдерді механикалық енгізу, егер олар мәдени, тарихи, экономикалық тұрғыдан бейімделмеген болса, табысқа кепілдік бермейді

Шетелдік тәжірибені зерттей отырып, ақпараттық қауіпсіздікке қатысты сервистік модельді дамытудағы үш негізгі векторды анықтауға болады.

Біріншісі – азаматтардың полицияға қол жеткізуін барынша жеңілдетуге бағытталған қадамдық қолжетімділік. Ол полиция пункттерін, мобильді бекеттерді оңтайлы орналастыруды, оларды материалдық-техникалық жарақтандыруды, ден қоюдың жеделдігін арттыруды, сондай-ақ цифрлық технологияларды қолдануды қамтиды.

Екіншісі – болатын қауіптерді уақтылы жою арқылы құқық бұзушылықтың алдын алу. Халықаралық тәжірибеде бұл проблемалар аналитикалық проблемалық – бағдарланған тәсіл арқылы шешіледі, мұнда полиция басқа мемлекеттік органдармен бірге қолайлы және қауіпсіз өмір сүру жағдайларын жасайды, сондай-ақ ақпараттық қауіпсіздік мәселелері бойынша хабардар етеді.

Үшіншісі – халықпен тығыз серіктестік, өйткені қауіпсіздік мәселелері жергілікті маңызға ие және оларды жергілікті қоғамдастықтың белсенді көмегімен ғана тиімді шешуге болады.

Әрине, осы модельдерді енгізу кезінде белгілі бір қауіптер болу мүмкін. Ең өзектілерінің бірі – бюрократиялық тәуекелдер. Атап айтқанда, кез-келген мәдени өзгерістер, полицияны модернизациялау және модельді енгізу, оның ішінде басқа мәдениетті енгізетін ақпараттық қауіпсіздікке қатысты бірқатар бюрократиялық тәуекелдерді болжайды:

– кәсіби қызғаныш; полиция бөлімшелері арасындағы ыңғайсыздық;

– билікке қол жетімділіктің төмендеуі;

– шешім қабылдау процесінің жоғарғы қолбасшылығына қол жетімділікті жоғалтудан қорқу;

– ақпарат алмасуға қарсылық;

– бірлескен жетістіктер табысқа жету;

– қызмет көрсетудің тұрақтылығын қамтамасыз ету үшін ең аз адами ресурстардың қанықтылығын азайту.

Жұмысты қорытындылай келе, негізгі қорытындыларды бөліп көрсетуге болады: полиция қызметінің жоғары сапасын қамтамасыз ету үшін ең алдымен қызметкерлердің ақпараттық құзыреттілігін дамытуды және олардың өз жұмысына қанағаттануын арттыруды қамтамасыз ету қажет; фронт-лайн (яғни азаматтармен тікелей байланыста болатын) қызметкерлері қызметінің тиімділігін арттыру үшін саладағы қолдау қызметтерінің жұмыс сапасын жетілдіру қажет.

Пайдаланған әдебиеттер тізімі

1. Қазақстан Республикасында мемлекеттік басқаруды дамытудың 2030 жылға дейінгі тұжырымдамасын бекіту туралы Қазақстан Республикасы Президентінің 2021 жылғы 26 ақпандағы № 522 Жарлығы.

2. Қазақстан Республикасының құқықтық саясатының 2030 жылға дейінгі тұжырымдамасын бекіту туралы Қазақстан Республикасы Президентінің 2021 жылғы 15 қазандағы № 674 Жарлығы.

Кзылходжаева Айсәулем Амангелдіқызы,
соискатель института,
м.ю.н., e-mail: aisaylem@mail.ru
(Институт государства и права Национальной академии наук Кыргызской Республики)

ОБЗОР ОСНОВНЫХ ТЕХНОЛОГИЧЕСКИХ ДОСТИЖЕНИЙ В ОБЛАСТИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ЕЕ РОЛЬ В УСКОРЕНИИ И УСИЛЕНИИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Данная статья представляет обзор основных технологических достижений в области искусственного интеллекта (далее – ИИ) и анализирует их влияние на динамику преступной деятельности. В статье освещаются современные тенденции развития ИИ, включая машинное обучение, нейронные сети, обработку естественного языка и компьютерное зрение. Особое внимание уделяется роли искусственного интеллекта в ускорении и усилении правонарушений в данной области.

Автор рассматривает использование ИИ в киберпреступлениях, а также его влияние на различные аспекты преступной деятельности, включая планирование и выполнение преступлений. В статье также поднимаются вопросы этического и правового характера, связанные с применением ИИ в преступной среде, и обсуждаются возможные меры по предотвращению и борьбе с негативными последствиями технологического развития в контексте преступной активности. Исследуемая научная статья предоставляет читателям комплексный обзор взаимосвязи между технологическими достижениями в области искусственного интеллекта и преступной деятельностью, а также ставит вопросы о необходимости регулирования и ответственного использования технологий для обеспечения общественной безопасности.

Ключевые слова: искусственный интеллект, технологические достижения, киберпреступления, этика, правовые аспекты.

OVERVIEW OF MAIN TECHNOLOGICAL ADVANCES IN THE FIELD OF ARTIFICIAL INTELLIGENCE AND ITS ROLE IN ACCELERATING AND STRENGTHENING CRIMINAL ACTIVITIES

Annotation. This article provides an overview of the main technological advances in the field of artificial intelligence (hereinafter referred to as AI) and analyzes their impact on the dynamics of criminal activity. The article highlights current trends in AI development, including machine learning, neural networks, natural language processing and computer vision. Particular attention is paid to the role of artificial intelligence in accelerating and intensifying crime in this area. The authors examine the use of AI in cybercrime, as well as its impact on various aspects of criminal activity, including the planning and execution of crimes. The article also raises ethical and legal issues related to the use of AI in criminal environments, and discusses possible measures to prevent and combat the negative consequences of technological development in the context of criminal activity. The research article under study provides

readers with a comprehensive overview of the relationship between technological advances in artificial intelligence and criminal activity, and raises questions about the need for regulation and responsible use of technology to ensure public safety.

Keywords: artificial intelligence, technological advances, cybercrime, ethics, legal aspects.

В последние десятилетия искусственный интеллект (далее – ИИ) стал неотъемлемой частью нашей повседневной жизни, оказывая глубокое влияние на различные области, включая экономику, медицину и образование. Однако, несмотря на положительные достижения, технологии искусственного интеллекта также стали объектом внимания в контексте их возможного использования для преступных целей.

Одним из ключевых технологических достижений в области ИИ является разработка мощных алгоритмов машинного обучения, способных анализировать и обрабатывать огромные объемы данных с высокой точностью. Эти алгоритмы находят применение в различных задачах, начиная от распознавания образов и автоматизации производственных процессов до создания персонализированных рекомендаций в интернете. Однако, с ростом возможностей ИИ, появляется также потенциал для его злоупотребления в целях совершения преступлений. Автоматизация и улучшение алгоритмов таких технологий как распознавания лиц могут быть использованы для создания систем слежения и отслеживания, нарушающих частную жизнь граждан Республики Казахстан. Также, алгоритмы машинного обучения могут быть направлены на создание поддельных видео и звукозаписей, что усиливает риск манипуляций информацией и фальсификации событий. Исключительно важным является усиление мер безопасности и законодательства со стороны государства в ответ на данные вызовы. Актуальным вопросом в данном аспекте являются разработка эффективных систем защиты от злоупотреблений технологиями ИИ, а также усовершенствование методов аутентификации и авторизации [1].

Одной из ключевых проблем в области искусственного интеллекта является увеличение риска киберпреступности в связи с расширением возможностей алгоритмов машинного обучения. Это создает угрозы в сфере кибербезопасности, такие как более сложные кибератаки, фальсификация данных и генерация поддельных медиаконтентов, требуя постоянного совершенствования систем защиты и разработки этичных нормативов для применения искусственного интеллекта.

Кроме того, растущая зависимость от искусственного интеллекта в различных сферах общества вызывает заботы о потенциальных социальных и экономических последствиях. Возникают вопросы об автоматизации рабочих мест, неравенстве в доступе к новым технологиям, а также этических аспектах использования ИИ, включая вопросы прозрачности и ответственности за решения, принимаемые алгоритмами. Необходимо активное обсуждение и разработка стандартов, направленных на сбалансированное и этичное внедрение искусственного интеллекта в общественную жизнь [2].

Искусственный интеллект играет значительную роль в современном обществе, однако, также существует опасность использования ИИ для ускорения и усиления преступной деятельности. С одной стороны, применение ИИ в области кибербезопасности позволяет бороться с киберпреступлениями, выявлять уязвимости в системах безопасности и предотвращать хакерские атаки.

Искусственный интеллект может анализировать большие объемы данных, выявлять аномалии и предостерегать от возможных угроз. С другой стороны, киберпреступники также могут использовать технологии искусственного интеллекта для создания более сложных и совершенных атак. Алгоритмы машинного обучения могут быть применены для обхода систем безопасности, а также для создания фишинговых атак и мошенничества. Более тонкие и интеллектуальные методы могут делать преступные действия менее обнаружимыми [3].

Борьба с использованием ИИ в преступной деятельности требует постоянного развития технологий безопасности и этичных стандартов в области искусственного интеллекта.

Ответственное применение технологий, законодательство, и общественная осведомленность играют важную роль в предотвращении негативных последствий использования ИИ для преступных целей.

Для противостояния потенциальному ускорению и усилению преступной деятельности с применением искусственного интеллекта необходимо систематически развивать технологии безопасности, внедрять этические стандарты и законодательство, повышать уровень образования и осведомленности, стимулировать международное сотрудничество и разрабатывать специализированные «белые» технологии [4].

Первое, развитие технологий безопасности: важно постоянно совершенствовать технологии безопасности, в том числе искусственный интеллект, чтобы предотвращать злоупотребление. Создание более совершенных систем обнаружения и защиты может значительно уменьшить уязвимости, которые могут использоваться преступниками.

Второе, этические стандарты и законодательство: внедрение строгих этических стандартов и законодательства в области искусственного интеллекта может служить ограничителем для его злоупотребления. Регулирование использования ИИ в критических областях, таких как кибербезопасность, помогает предотвратить его применение в преступных целях.

Третье, обучение и осведомленность: повышение уровня осведомленности об угрозах, связанных с использованием искусственного интеллекта в преступной деятельности, является ключевым шагом. Обучение профессионалов в сфере кибербезопасности и общества в целом по управлению рисками и безопасному использованию технологий может смягчить потенциальные угрозы.

Четвертое, международное сотрудничество: преступления, связанные с использованием искусственного интеллекта, часто имеют международный характер. Поэтому сотрудничество между странами в области обмена информацией и координации действий на мировом уровне может эффективно противостоять глобальным угрозам.

Пятое, развитие «белых» технологий: специализированные разработки искусственного интеллекта, так называемые «белые» технологии, могут использоваться для предотвращения и выявления преступной деятельности. Активное развитие таких технологий способствует созданию мощных инструментов для борьбы с преступниками.

Интеграция развития технологий безопасности, внедрение этических стандартов, повышение образовательного уровня и осведомленности, активное международное сотрудничество, а также создание специализированных «белых» технологий в совокупности формируют более надежную систему защиты от возможного ускорения и усиления преступной деятельности, связанной с использованием искусственного интеллекта.

На основании вышеизложенного приходим, к выводам, что несмотря на потенциальные риски и вызовы, связанные с использованием искусственного интеллекта в преступной деятельности, важно признать, что ИИ также предоставляет ценные инструменты для борьбы с преступлениями и улучшения безопасности.

Эффективное сбалансированное регулирование, развитие этических стандартов, инновационные подходы к кибербезопасности и широкая осведомленность общества сыграют решающую роль в минимизации рисков и максимизации положительного воздействия искусственного интеллекта на общественную безопасность.

Отметим, что искусственный интеллект играет противоречивую роль в контексте преступной деятельности, предоставляя современным преступникам новые возможности и вызывая угрозы для общественной безопасности. Продвинутые алгоритмы машинного обучения и анализа данных могут использоваться для создания сложных киберпреступлений, обхода систем безопасности и даже для искусственного создания угроз.

Однако, разработка и внедрение эффективных систем безопасности, этических стандартов и законодательства, а также повышение осведомленности общества о потенциальных рисках, являются критическими шагами для сдерживания возможного ускорения и усиления преступной деятельности, подкрепленной искусственным интеллектом [5].

Вышесказанному относительно борьбы с использованием искусственного интеллекта для ускорения и усиления преступной деятельности, предлагаем следующие рекомендации:

1. Необходимо постоянно совершенствовать системы защиты, чтобы эффективно противостоять новым методам киберпреступников и адаптироваться к изменяющимся угрозам.

2. Существенное обновление правовых норм и установление четких этических стандартов способствует предотвращению злоупотреблений и несанкционированного использования технологий.

3. Широкая общественная осведомленность о рисках и возможностях искусственного интеллекта, а также обучение населения средствам кибербезопасности, создают более ответственное отношение к технологиям.

4. Совместные усилия государств и международных организаций в области обмена информацией и разработки общих стратегий обеспечивают эффективное противостояние трансграничным киберугрозам.

5. Специализированные технологии безопасности, направленные на предотвращение злоупотреблений и обеспечение защиты от киберпреступлений, являются важным компонентом общей стратегии борьбы с угрозами, связанными с искусственным интеллектом.

В заключение, следует отметить, что роль искусственного интеллекта в ускорении и усилении преступной деятельности представляет собой двусмысленный вызов для общества. В то время как ИИ может служить эффективным инструментом в борьбе с преступлениями, его потенциал для злоупотребления также велик. Необходимость постоянного совершенствования технологий безопасности, установления этических норм и законодательства, а также повышения осведомленности общества становится ключевой в создании устойчивого баланса между инновациями и защитой от потенциальных угроз, которые могут возникнуть в результате использования искусственного интеллекта в преступных целях.

Список использованной литературы

1. Artificial intelligence and crime: challenges and prospects [Электронный ресурс] // Technology and Security magazine. 2023. № 23 // URL: https://www.researchgate.net/publication/364011742_threats_and_opportunities_with_ai-based_cyber_security _intrusion_detection_a_review.

2. Hisham O. Khogali, Samir Mekid. The blended future of automation and AI [Электронный ресурс] // Examining some long-term societal and ethical impact features Technology in Society Volume 73, May 2023, 102232 // URL: https://www.sciencedirect.com/science/arti cle/pii/S0160791X23000374.

3. Janna Anderson, Lee Rainie. Improvements ahead [Электронный ресурс] // How humans and AI might evolve together in the next decade. Artificial intelligence and the future of humans. Pew research center. December 10, 2018 // URL: https://www.pewresearch.org/internet/2018/12/10/improvements-ahead-how-humans-and-ai-might-evolve-together-in-the-next-decade/.

4. Nadine Bachmann, Shailesh Tripathi, Manuel Brunner and Herbert Jodlbauer. The Contribution of Data-Driven Technologies in Achieving the Sustainable Development Goals. Center of Excellence for Smart Production, Research Group Operations Management, University of Applied Sciences Upper Austria, Wehrgrabengasse 1-3, 4400 Steyr, Austria [Электронный ресурс] // URL: https://www.mdpi.com/2071-1050/14/5/2497.

5. Keith Hayward, Matthijs Maas. Artificial intelligence and crime [Электронный ресурс] // A primer for criminologists. June 2020Crime Media Culture An International Journal 17(2) // URL: https://www.researchgate.net/publication/342551406_Artificial_intelligence_and_crime_A_primer_for_criminologists.

Киселёва Екатерина Валерьевна,
научный сотрудник центра по исследованию
проблем уголовной политики и профилактики преступности НИИ
магистр национальной безопасности и военного дела, майор полиции
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова,
Республика Казахстан)

К ВОПРОСУ ОБ ИНТЕРНЕТ-МОШЕННИЧЕСТВЕ И ЕГО ПРОФИЛАКТИКЕ

Аннотация. Профилактика правонарушений яляется одной из важнейших задач, стоящих перед государством и правоохранительными органами. В данной статье на основании статистического анализа, изучения зарубежного опыта, автором предлагается совершенствование законодательства, в частности ратифицировать Конвенцию о преступности в сфере компьютерной информации (ETS № 185), подписанную в Будапеште 23 ноября 2001 г., запретить реализацию и регистрацию SIM-карт вне офиса операторов сотовой связи, проводить биометрическую идентификацию при приобретении SIM-карт и сотовых телефонов. Данные предложения позволят снизить количество случаев интернет-мошенничества и уберечь людей от финансовых потерь и морального ущерба.

Ключевые слова: преступность, профилактика, интернет, мошенничество, закон, государственная политика.

ON THE ISSUE OF INTERNET FRAUD AND ITS PREVENTION

Annotation. Crime prevention is one of the most important tasks facing the State and law enforcement agencies. In this article, based on statistical analysis, studying foreign experience, the author proposes to improve legislation, in particular, to ratify the Convention on Computer Information Crime (ETS No. 185), signed in Budapest on November 23, 2001, to prohibit the sale and registration of SIM cards outside the office of mobile operators, to conduct biometric identification when purchasing a SIM-cards and cell phones. These proposals will reduce the number of cases of Internet fraud and protect people from financial losses and moral damage.

Keywords: crime, prevention, Internet, fraud, law, public policy.

В своем послании от 1 сентября 2022 года Президент Республики Казахстан Касым-Жомарт Токаев отметил, что: «Отдельное внимание следует уделить валу интернет- и телефонного мошенничества. Правоохранительным органам нужно усилить информационно-аналитическую работу по выявлению и нейтрализации подобных угроз. Следует также системно повышать правовую и финансовую грамотность граждан» [1].

В настоящее время очень быстро распространяются цифровые технологии. Одной из наиболее значимых и широко используемых технологий является сеть

Интернет, которая применяется во всех аспектах жизнедеятельности человека, включая хранение денежных средств на счетах в банках и дистанционное управление ими посредством компьютерных и мобильных технологий.

Интернет и информационные технологии способствуют развитию количества мошеннических действий в сети Интернет.

В соответствии со статьей 190 Уголовного Кодекса Республики Казахстан «Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» [2].

Основными составляющими мошенничества является обман и злоупотребление доверием. Согласно Словарю русского языка С.И. Ожегова, под обманом понимается намеренное искажение истины; ложное представление о чем-нибудь; неправда; введение в заблуждение, недобросовестный поступок по отношению к кому-нибудь; нарушение обещания и др.

Под злоупотреблением доверием понимается: злоупотребление – это проступок, состоящий в незаконном, преступном использовании своих прав, возможностей, а доверие – это уверенность в чьей-либо добросовестности и искренности [3].

По мнению ученых Красовской Н.Р., Гуляева А.А. кибермошенничество определяется как – активные действия в онлайн-формате с целью получения выгоды посредством манипуляций сознанием человека [4, с. 133].

Согласно Кембриджскому словарю делового английского языка кибермошенничество – это ситуация, в которой кто-то использует Интернет для незаконного получения денег, товаров и т. д. от людей путем их обмана [5].

Таким образом, кибермошенничество является сложным видом преступления. Киберпреступники постоянно придумывают новые способы обмана и используют передовые технологии для сокрытия своих преступлений. Кроме того, кибермошенничество часто имеет международный характер. Преступники могут находиться в других странах и использовать зарубежные серверы для совершения преступлений.

Это затрудняет расследование и требует сотрудничества правоохранительных органов разных стран.

Следует отметить, что существует множество видов и способов совершения кибермошенничества: фишинг, вишинг, смишинг, фарминг, компрометация деловой электронной почты, нигерийские письма или мошенничество «419» и т.д.

Чтобы оценить масштабность проблемы кибермошенничества, следует рассмотреть статистические данные. Данные официальной статистики за последние пять лет (в период с 2018 по 2022 гг.) о зарегистрированных преступлениях, предусмотренных п. 4 ч.2 ст. 190 УК РК, свидетельствуют об устойчивой тенденции к их росту. Всего зарегистрировано интернет-мошенничеств в 2018 –0,5 тыс.ед., в 2019 –7,8 тыс.ед., в 2020 –14,2 тыс.ед., 2021-21,4 тыс.ед., 2022-20,6 тыс.ед. [6].

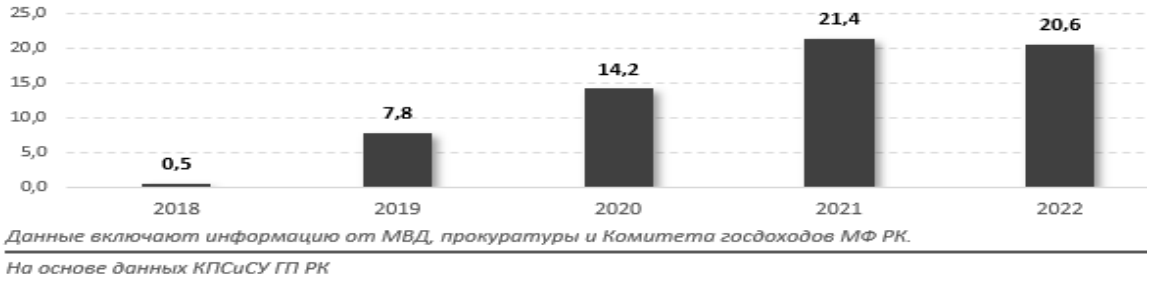


Рис. 1. Динамика зарегистрированных в ЕРДР преступлений,совершенных путем обмана или злоупотребления доверием пользователя информационной системы

Статистические данные показывают, что интернет-мошенничество продолжает быть серьезной проблемой в Республике Казахстан. Важно отметить, что это статистика показывает только официальные обращения в правоохранительные органы. Скорее всего, реальное число жертв цифровых мошенничеств выше, так как некоторые граждане не обращаются в правоохранительные органы, считая причиненный им ущерб незначительным.

Анализ законодательства зарубежных стран свидетельствует о том, что законы о киберпреступлениях на национальном уровне были проработаны еще в 70–80-х годах XX века. Первый федеральный закон, который установил уголовную ответственность за киберпреступления, был принят в Соединенных Штатах в 1977 году. В октябре 1984 года появилась новая редакция данного закона: новый акт назывался «Закон о компьютерном мошенничестве и злоупотреблениях» (Computer Fraud and Abuse Act). С тех пор в этот закон неоднократно вносились поправки – в 1989, 1994, 1996, 2001, 2002 и 2008 годах. Эти законопроекты были приняты в ответ на обеспокоенность тем, что преступления, связанные с использованием компьютеров, могут остаться безнаказанными, так как до принятия этих законов, компьютерные преступления преследовались по закону как «мошенничество с использованием почты и телеграмм», а это создавало проблему правильной квалификации совершенного деяния. В 2015 году был разработан новый закон с ужесточенными санкциями [7].

В Великобритании в 1990 году Парламентом Соединенного Королевства был принят первый такого рода законодательный акт, который называется «Закон о неправомерном использовании компьютеров» («Computer Misuse Act»). В законе «О терроризме» от 2000 года также затрагивается проблема кибепреступности [8].

Уголовный Кодекс Японии, Китая, Франции, Германии, Испании, Италии, Нидерландов и других стран мира также содержат специальные нормы, предусматривающие уголовную ответственность за преступления в сети Интернет.

В уголовных законодательствах зарубежных стран есть две тенденции криминализации таких деяний. В первом случае эти деяния определяются как отдельные самостоятельно совершенные преступления, во втором случае они дополняют составы уже существующих традиционных «некомпьютерных» преступлений, например, как в Уголовном кодексе Италии.

Резкого различия в классификации кибепреступлений в законах этих стран нет. Многие страны больше всего внимания уделяют организации предупреждения таких преступлений, нежели материальным нормам, предусматривающим ответственность.

Учитывая изученный международный опыт и то, что одним из самых действенных способов борьбы с преступностью является профилактика преступлений, полагаем о целесообразности разработать закон о профилактике правонарушений, совершаемых с использованием сетей телекоммуникаций, в том числе сети Интернет с целью установления единой государственной политики в области профилактики данных правонарушений. Так как на современном этапе развития социум зависит от информационных технологий и проблема профилактики данных правонарушений стоит остро. В данном законе по аналогии с Законом Республики Казахстан «О профилактике бытового насилия» от 4 декабря 2009 года, а также Законом Республики Казахстан «О профилактике правонарушений среди несовершеннолетних и предупреждении детской безнадзорности и беспризорности» от 9 июля 2004 года необходимо указать цели, задачи, принципы государственной политики, субъектов профилактики правонарушений, их полномочия и меры профилактики.

Следует отметить, что многие зарубежные страны ратифицировали Конвенцию о преступности в сфере компьютерной информации (ETS № 185), подписанную в Будапеште 23 ноября 2001 г. Это 26 государств-членов Совета Европы: Австрия, Албания, Армения, Бельгия, Болгария, Великобритания, Венгрия, Германия, Греция, Испания, Италия, Кипр, Македония, Молдова, Нидерланды, Норвегия, Польша, Португалия, Румыния, Украина, Финляндия, Франция, Хорватия, Швейцария, Швеция и Эстония. Кроме того, к ней присоединились Канада, Соединенные Штаты Америки, Южная Африка и Япония, также принимавшие участие в ее разработке.

Положения Конвенции нацелены на создание эффективного организационно-правового механизма сотрудничества между государствами – членами Конвенции, а также организациями и частными лицами. Основной идеей данного документа стало установление единообразного международного подхода к составам компьютерных преступлений, которые государства должны включить в свое национальное законодательство, а также разработка мер по предотвращению правонарушений, направленных против целостности, доступности, конфиденциальности информации, компьютерных систем, сетей, данных, а также неправомерного их использования.

Конвенция охватывает три основных направления:

– согласование национальных правовых норм, определяющих составы соответствующих преступлений;

– формирование процедуры расследования киберпреступлений;

– создание действенной системы межгосударственного сотрудничества в сфере противодействия киберпреступности [9].

Возможно, что присоединение Республики Казахстан к Конвенции Совета Европы о киберпреступности способствовало бы положительной оценке международным сообществом деятельности нашего государства в сфере обеспече-

ния информационной безопасности и противодействия компьютерной преступности. Представляется, что международное сотрудничество в сфере борьбы с компьютерной преступностью должно идти по пути расширения форм правовой помощи между государствами посредством заключения новых соглашений или внесения изменений в уже существующие, а также создания совместных институтов по взаимодействию в сфере борьбы с компьютерной преступностью и урегулированию разногласий, возникающих в процессе применения таких соглашений.

Кроме того, как свидетельствует анализ практической деятельности при совершении интернет-мошенничества для того, что бы скрыть свою личность, лоумышленники, посредством интернета покупают либо похищают данные лиц и регистрируют на них SIM -карты и сотовые устройства, что затрудняет поиск преступников. В целях повышения безопасности и предотвращения интернет-мошенничества, предлагается запретить реализацию и регистрацию SIM-карт вне офиса операторов сотовой связи. Законодательно закрепить обязательное предъявление документов удостоверяющих личность, фото/видеофиксации лица приобретающего SIM-карту, проводить биометрическую идентификацию при приобретении SIM-карт и сотовых телефонов. На наш взгляд высказанные предложения по совершенствованию законодательства Республики Казахстан позволят обеспечить надежную идентификацию пользователей и улучшить контроль над использованием мобильных услуг.

Также следует отметить, что помимо совершенствования нормативной базы необходимо на постоянной основе усиливать уровень обучения информационным технологиям в системе образования, то есть необходимо в школах обеспечить хорошее обучение пользованию информационными технологиями, готовить высокопрофессиональных специалистов в сфере информационных технологий, разрабатывать программы по профилактике виктимизации, направленные на формирование у населения навыков безопасного поведения в интернете, информировать людей о существующих способах обмана и способах защиты от них. Данные предложения позволят снизить количество случаев интернет-мошенничества и уберечь людей от финансовых потерь и морального ущерба.

Список использованной литературы

1. Послание Главы государства Касым-Жомарта Токаева народу Казахстана от 01 сентября 2022 г. «Справедливое государство. Единая нация. Благополучное общество» [Электронный ресурс] // URL: https://adilet.zan.kz/rus /docs/K22002022_2/.

2. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2023 г.). [Электронный ресурс] // Информационно-правовая система нормативных правовых актов Республики Казахстан. – URL: http:// adilet.zan.kz/rus.

3. Толковый Словарь Ожегова [Электронный ресурс] // URL: https://slovarozhegova.ru/word.php?wordid=9249.

4. Красовская Н.Р., Гуляев А. К вопросу о кибермошенничестве // Вестник Удмуртского университета. Социология. Политология. Международные отношения. – 2022. – Т. 6. – С. 133–138.

5. Кембриджский словарь делового английского языка [Электронный ресурс] // URL: https://dictionary.cambridge.org/ru/.

6. Анализ о состоянии преступности в стране проведен на основе сведений отчета КПСиСУ Генеральной прокуратуры РК. [Электронный ресурс] // URL: https://www.gov.kz/memleket/entities/pravstat.

7. Palmer C. C. Ethical Hacking // IBM Systems Journal. 2001. Vol. 40. № 3.

8. Уголовное право зарубежных стран: Общая и Особенная часть / Под ред. Н.Е. Крыловой. – М.: Юрайт, 2015. – 490 с.

9. Тарасов А.М. Структура и содержание конвенции по противодействию киберпреступлениям [Электронный ресурс] // URL: http://dx.doi.org/10.26583/bit.2018.4.05.

Конобеевских Владимир Валерьевич,
доцент кафедры автоматизированных информационных систем органов внутренних дел, к.т.н, e-mail: vkonobeevskikh@mail.ru
(Воронежский институт МВД России, Российская Федерация)

Мисайлов Дмитрий Владимирович,
e-mail: mitya.vladimirovich.93@list.ru
(Центральный филиал Российского государственного университета правосудия, г. Воронеж, Российская Федерация)

ОСНОВНЫЕ ТЕНДЕНЦИИ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ С ПОМОЩЬЮ СЕТИ ИНТЕРНЕТ

Аннотация. В статье авторами раскрываются основные тенденции совершения преступлений против детей подростков в России с помощью сети Интернет на основе проведенного анализа материалов правоприменительной практики, научный и иных публикаций из открытого доступа.

Ключевые слова: ребенок, несовершеннолетний, подросток, дети, вовлечение в совершение преступления, взрослый вовлекатель, совершеннолетнее лицо, профилактика, предупреждение, Интернет, виртуальное пространство, криминогенные факторы, киберпреступность, информационная безопасность, вредоносный контент, педагогические работники, полиция, родители, семья, школа, криминогенная ситуация.

THE MAIN TRENDS IN THE COMMISSION OF CRIMES AGAINST MINORS USING THE INTERNET

Annotation. In the article, the authors reveal the main trends in the commission of crimes against adolescent children in Russia using the Internet based on the analy-

sis of materials of law enforcement practice, scientific and other publications from open access.

Keywords: child, minor, teenager, children, involvement in the commission of a crime, adult, adult, prevention, prevention, Internet, virtual space, criminogenic factors, cybercrime, information security, malicious content, teaching staff, police, parents, family, school, criminogenic situation.

В современном мире информационные технологии и сеть Интернет развиваются стремительно, и Российская Федерация не исключение. В повседневную жизнь прочно вошли современные средства связи – мобильные телефоны, смартфоны, планшетные компьютеры и т.д. Конечно, все это не может не приводить к глобальным изменениям, которые затрагивают практически все сферы жизни современных людей. Так, например, ставшее в последнее время популярным виртуальное пространство позволяет людям реализовывать различные виды активностей без личных встреч – онлайн. Планировать рабочие совещания (в режиме видеоконференцсвязи), организовывать досуг (онлайн-игры), удовлетворять различные повседневные потребности (интернет-магазины, 3D-моделирование пространств и т.д.). Однако мы не можем не обратить внимание на то, что наряду с весьма широкими возможностями, которые дает людям онлайн-пространство, оно может одновременно нести и вред. Особенно очевидны опасности для тех категорий граждан, которые в силу возраста (несовершеннолетние, престарелые лица) или иных (психологических, физических) возможностей не могут в полной мере отдавать отчет всем своим действиям. Специалисты выражают обеспокоенность тем, что молодое поколение с каждым годом проводят все больше времени в сети Интернет. По этой причине подрастающее поколение стали традиционно называть «цифровым поколением». Именно представители «цифрового поколения» являются одной из основных групп риска, в которой формируется зависимость от сети Интернет и технических средств, при помощи которых обеспечивается доступ к нему.

Группой исследователей во главе с Г.У. Солдатовой был проведен опрос молодого населения России (1056 представителей во возрасте 14-18 лет), по результатам которого было выявлено, что каждый второй представитель данной группы ежедневно проводит в Интернете более шести часов. Каждый четвертый, одновременно с этим, ежедневно уделяет Интернету более девяти часов [1, с. 12]. Исследователи обращают особое внимание на то, что подростки в последние годы изменили направление своей коммуникативной активности – они все больше стали осуществлять ее в интернет-пространстве. Этот аспект представляется важным по той причине, что в подростковом возрасте ведущим типом деятельности является именно коммуникации, личностное общение. Соответственно, прямо пропорционально возрастают угрозы стать жертвой различных криминальны посягательств в интернет-пространстве.

Вместе с тем, говоря о преступлениях, которые совершаются в отношении детей и подростков с помощью Интернет, нельзя не отметить их высокую латентность и, одновременно с этим, низкую раскрываемость, которые в конечном счете приводят к крайне негативным последствий для жизни и благополу-

чия несовершеннолетних, ставших жертвами данных преступлений [2, с. 28]. По данному поводу следует упомянуть доклад, подготовленный специалистами Всероссийского научно-исследовательского института МВД России в 2021 г.: «…современное состояние преступности помимо прочего характеризуется высокой адаптированностью к новейшим достижениям научно-технического прогресса, перерождением в новых формах, методах и способах совершаемых преступных посягательств в сферах, сложных для осуществления социального контроля» [3, с. 72]. В данном докладе также отмечается, что не более 25% преступлений, которые были совершены с использованием сети Интернет, были в последствии раскрыты правоохранительными органами. Подростки так же становятся жертвами данных преступлений. Однако помимо риска стать непосредственно жертвой преступления, которое также может быть выражено в сексуальных домогательствах, существует и более серьезный риск – риск вовлечения подростка в систематическую (организованную) преступную деятельность, а также в различные деструктивные сообщества, в результате чего подросток становится уже не жертвой преступления, а преступником.

Развитие современных технологий значительно расширило количество способов, при помощи которых может реализовываться преступная деятельность. Лицу, совершающему преступление, сейчас стало значительно проще сохранять свою анонимность. Возможности поиска потенциальных жертв для преступника год от года становятся все шире. Более того, у взрослых преступников постоянно появляются все новые возможности, при помощи которых они могут оказывать психологическое воздействие на потенциальных жертв среди детей и подростков. «По характеру посягательства действия киберпреступников условно можно подразделить на две большие группы: преступления, посягающие на личные права ребёнка, и преступные деяния, направленные на вовлечение несовершеннолетних лиц в преступление» [4, с. 78]. К примеру, «новую технически оснащенную площадку для своей реализации в виртуальном пространстве получила и практика буллинга, а также различных форм его проявления в подростковой среде» [5, с. 215].

Причем все аще стали проявляться случаи, когда жертв буллинга продолжают притеснять не только в реальной жизни, но и в онлайн-пространстве. Данное проявление получило название «happy slapping» – видеосъемка процесса избиения жертвы другими подростками и последующее размещение такого видео в сети Интернет. Кроме того, актуальной в настоящее время является также проблема аутодеструктивного и суицидального поведения подростков. В данной сфере Интернет так же играет весьма значительную роль. Подростки в большинстве своем являются легковнушаемыми, а в Интернете в свободном доступе есть весьма большой массив информации, в том числе и суицидогенной. Кроме того, в сети Интернет есть множество онлайн-площадок, на которых подростки могут найти сообщества единомышленников по различным вопросам, в которых они будут делиться друг с другом своими переживаниями. В таких сообществам преступникам значительно проще найти себе потенциальную жертву.

Общение в виртуальном пространстве значительно облегчает поиск единомышленников, в том числе и при наличии суицидальных мыслей, а также поиск потенциальных жертв. Следовательно путь от мысли о суициде к его исполнению при использовании сети Интернет становится только короче.

Нельзя не обратить внимание на то, что, помимо указанного выше, Интернет несет в себе и иные опасности. Так, весьма серьезной опасностью является перенасыщенный контент, размещенный в сети. Значительная часть информации, содержащаяся в Интернете, может нанести значительный вред психике подростков, оказать негативное влияние на развитие детей. Законодатель в настоящее время принимает ряд мер по защите детей и подростков от неблагоприятного контента, который может оказать на них негативное влияние. Так, в 2010 г. был принят Федеральный закон № 436-ФЗ от 29 декабря 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию». В этом законе предусматривается «отнесение информационной продукции к одной из пяти категорий, и запрещающий ее распространение среди детей в зависимости от их возраста».

Запретительные меры являются не единственными в работе, которую законодатель ведет в целях профилактики и предотвращения распространения контента, который может оказать негативное влияние на психику представителей «цифрового поколения». Важную роль в профилактической деятельности законодателя играет профилактика распространения негативного контента. Такого рода деятельность направлена на достижение основной цели – создания условий, при помощи которых будет повышаться общий уровень культуры и информационной безопасности в онлайн-среде, в которой преобладает молодежь. Работа в этом направлении заключается в «ранней профилактике экстремизма, дискриминации по социальным, религиозным, расовым, национальным и другим признакам» [6].

Следует подчеркнуть, что в настоящее время на практике в большинстве случаев киберпреступления, совершаемых против несовершеннолетних лиц, являются тяжкими или особо тяжкими преступными деяниями. При этом все большую популярность приобретают такие направления преступной деятельности в сети Интернет как кибермошенничество, кибертерроризм, а также различные действия, которые направлены на сексуальную эксплуатацию детей, продажа несовершеннолетних лиц через «тёмный интернет» (Даркнет).

С технической точки зрения, важным также является тот аспект, что для совершения преступлений преступники часто используют специально устанавливаемые программы (VPN), которые позволяют им скрывать свой IP-адрес компьютера и действовать через так называемую теневую сторону интернета. Особенностью использования теневой стороны интернета является то, что идентифицировать такого пользователя весьма сложно. VPN-программы позволяют сохранять анонимность пользователя, скрывать его реальное местоположение, подменяя его другим (зачастую – другой страной), засекречивать данные, передаваемые пользователем. Совокупность данных факторов снижает вероятность успешного раскрытия совершенного преступления, а зачастую и вовсе делает это невозможным [7, с. 55].

В качестве еще одного характерного признака преступления, совершаемых в сети Интернет необходимо отметить значительное сокращение промежутков времени между совершаемыми преступлениями. В первую очередь это связано с предыдущим отличительным признаком – преступник напрямую с жертвой не контактирует, а совершает все свои действия дистанционно. Сокращается время приготовления к совершению преступления: преступнику не нужно планировать место совершения преступления, подготавливать орудия, с помощью которых будет совершено преступление и т.д.» [8, с. 170].

При этом действия лиц, совершаемых такого рода преступления, направленны на вовлечение в них детей и подростков, и предполагает изменение идеологических, моральных, этических и других ценностных установок личности. В конечном счете такая криминальная деятельность способствует общему омоложению преступности. В итоге такого рода преступления могут представлять весьма серьезную угрозу не только для национальной безопасности государства, но и для международного сообщества.

Список использованной литературы

1. Рязова Г.У. Особенности межличностных отношений российских подростков в социальных сетях // Национальный психологический журнал. – 2023. – № 31 (57).

2. Кирова А.В. Участие несовершеннолетних лиц в совершении интернет-преступлений // Вестник Барнаульского юридического университета. – 2022. – № 9.

3. Гаврилин Ю.В. О научных подходах к проблеме использования информационно-телекоммуникационных технологий в преступных целях: научно-практическое пособие. – М.: Академия управления МВД России, 2021.

4. Алферова О.О. Киберпреступность, направленная против несовершеннолетних // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 7.

5. Сысоева Н.Н. Актуальные вопросы противодействия кибersталкингу среди несовершеннолетних в информационно-телекоммуникационной сети Интернет // Вестник Воронежского института МВД России. – 2021. – № 4.

6. Об утверждении основ государственной молодежной политики Российской Федерации на период до 2025 г.: постановление Правительства РФ от 29.11.2014 г. № 2403-р // Собрание законодательства РФ. – № 134. – Ст. 87.

7. Яновский Р.Б. К вопросу об анализе практики правового регулирования цифровой среды и предотвращения киберпреступлений // Вестник Санкт-Петербургской юридической академии. – 2022. – № 7.

8. Миронова К.С. Совершение преступлений несовершеннолетними в интернет среде // Вестник Барнаульского юридического института МВД России. – 2022. – № 8.

Корнаухова Наталья Геннадьевна,
заместитель начальника кафедры оперативно-разыскной деятельности
и специальной техники
к.ю.н., e-mail.ru: pongo_07@mail.ru
(Волгоградская академия МВД России, Российская Федерация)

Реент Ярослав Романович,
преподаватель цикла Центра профессиональной подготовки УМВД России
(Ханты-Мансийский автономномный округ – Югре, Российская Федерация)

ОСОБЕННОСТИ СТАДИИ ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. На сегодняшний день развитие информационно-коммуникационных технологий достигло того уровня, при котором значительное количество сфер жизни стало невозможным без использования последних. Повсеместная цифровизация общества сопряжена с ростом числа уголовно-правовых рисков практически во всех сферах общественной жизни. Авторами рассмотрены проблемы, с которыми сталкиваются практические работники в процессе раскрытия и расследования преступлений указанной категории.

Ключевые слова: компьютерная информация, уголовное дело, мошенничество, преступление, мессенджеры, цифровизация, хищения, банковские карты.

FEATURES OF THE STAGE OF INITIATION OF A CRIMINAL CASE IN THE DISCLOSURE AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES

Annotation. To date, the development of information and communication technologies has reached a level at which a significant number of spheres of life have become impossible without the use of the latter. The widespread digitalization of society is associated with an increase in the number of criminal law risks in almost all spheres of public life. The authors consider the problems faced by practitioners in the process of disclosure and investigation of crimes of this category.

Keywords: computer information, criminal case, fraud, crime, messengers, digitalization, theft, bank cards.

На сегодняшний день, в связи с тем, что общепризнанное определение преступления, совершенного с использованием ИКТ отсутствует, соответственно и отсутствует официальная статистика данной категории преступлений. Однако в ведомственной статистике присутствуют показатели количества совершенных преступлений в сфере компьютерной информации (далее – КИ) и

преступлений, совершенных с использованием информационно-коммуникационных технологий (далее - ПСИИКТ).

В 2023 г. в Российской Федерации зарегистрировано уже 489077 тыс. (+29,2 % к АППГ) ПСИИКТ [1]. Наиболее широкое распространение в настоящее время получили преступные деяния с использованием банковских карт, сети «Интернет», средств мобильной связи и КТ. Получили распространение мошенничества, сопровождающиеся внесением в единые государственные реестры фиктивных сведений о юридических лицах и индивидуальных предпринимателях, в результате которых злоумышленники приобретают возможность завладения имуществом, активами физических и юридических лиц. Значительное число «дистанционных мошенничеств» совершается лицами, отбывающими наказания в местах лишения свободы. Большое количество краж данного вида совершено с использованием мобильной связи, банковских карт и КТ. Рассматриваемые преступления все чаще совершаются технически оснащенными преступниками (в том числе международными), характеризуются усложненными способами их подготовки и сокрытия, созданием и использованием вредоносных программ [2].

Следует отметить, что раскрываемость рассматриваемой группы преступлений довольно низка. Одной из причин данных низких показателей, очевидно, является несовершенство работы сотрудников, производящих предварительное следствие на стадии сбора материала. Специфика стадии возбуждения уголовного дела обусловлена особенностью данного вида преступления, что определяет последовательность действий сотрудника полиции при обнаружении признаков состава преступления. Выявленные признаки оказывают влияние на выбор сил и средств, а также ход всего дальнейшего расследования.

Анализ следственно-судебной практики и научных работ позволяет сделать вывод, что типичными поводами для возбуждения уголовного дела по ПСИИКТ являются:

– заявление от физических лиц или представителей юридических лиц (около 80 %);

– сообщение о совершенном или готовящемся преступлении, полученное из иных источников, оформленное рапортом об обнаружении признаков преступления, составляемым сотрудником органа дознания или следователем, осуществляющим проверку сообщения о преступлении (около 20 %) [3, 173; 88].

Согласно ч. 2 ст. 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления. Нельзя не отметить, что в уголовно-процессуальном законе отсутствует требование об обязательности выяснения уже на стадии возбуждения уголовного дела всех обстоятельств происшедшего события, содержащего признаки преступления. На данной стадии достаточным будет установление фактов, указывающих на наличие признаков преступления, выяснение же конкретных обстоятельств преступления и лиц, виновных в его совершении, возможно только после возбуждения уголовного дела в ходе предварительного расследования [4].

При рассмотрении вопросов организации взаимодействия служб и подразделений при расследовании ПСИИКТ, необходимо рассмотреть деятельность сотрудников, осуществляющих дознание на стадии проверки поступившей информации.

В рамках проверки сообщения о хищении денежных средств с использованием ИКТ необходимо выяснить следующие обстоятельства:

– способ совершения и сокрытия хищения;

– существует ли вероятность списания денежных средств с банковского счета потерпевшего в результате действия, не связанного с хищением;

– наличие вредоносных программ на техническом устройстве пострадавшего лица;

– сведения о лицах, причастных к хищению денежных средств;

– наличие сведений об отправке, рассылке файлов вредоносного программного обеспечения;

– наличие факта воздействия из вне на сетевой ресурс для выведения его из строя и штатной работы;

– наличие сетевых запросов на техническое устройство пострадавшего лица, обработка которых привела к выведению его из строя.

Наряду с преступлениями против личности и общественной безопасности, так же значительной цифровизации стали подвержены преступления в сфере незаконного оборота наркотиков (далее – НОН). В этом направлении выделены следующие проблемы:

1. Ряд мессенджеров осуществляют шифрование сообщений, вследствие чего отслеживание передаваемой информации вызывает технические сложности. При отправке мгновенного сообщения, программным обеспечением, благодаря специальным алгоритмам формируется уникальный ключ, который хранится на устройствах отправителя и получателя, а не на серверах. Этот процесс делает труднодоступной информацию для третьих лиц.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» [5] показал свою неэффективность в части следующих своих положений:

– установлен запрет на использование программного обеспечения, позволяющего получать доступ к Интернет-ресурсам, запрещенным в РФ;

– большинство популярных Интернет-ресурсов в России игнорируют требование федерального закона относительно хранения сведений о персональных данных пользователей, равно как и о передаваемой ими информации.

3. В цифровом пространстве существует возможность создания произвольного образа личности, который формируется целым комплексом псевдоиндификаторов. Своей целью злоумышленники ставят анонимизацию своей реальной личности, которая позволяет последним создавать псевдоличности, которые в последующим используются в противоправной деятельности.

4. Вышеупомянутый ФЗ «Об информации, информационных технологиях и о защите информации» в ст. 10.1 и ФЗ «О связи» [6] в ст. 44 накладывают обязательства на операторов связи достоверно устанавливать сведения, позволяющие идентифицировать абонента. Однако эффективный механизм контроля

этого процесса на сегодняшний день отсутствует, не редки факты реализации сим-карт лицам, без установления личности последних, равно как и по утраченным законным пользователями документов.

5. Так же следует отметить, что на сегодняшний день в вышеуказанных законодательных актах отсутствуют конкретные сроки предоставления информации по запросам операторами связи. Этот факт негативно сказывается на оперативности принимаемых действий, направленных на пресечение преступных деяний.

6. На сегодняшний день все большее распространение получает использование криптовалют при взаиморасчетах по факту незаконного сбыта наркотиков. Происходит конвертация денежных средств в виртуальную валюту, которая на сегодня не подконтрольна уполномоченным государственным органам. Это обстоятельство в значительной мере способствует легализации доходов, полученных преступным путём. Последующие действия по отмыванию таких денежных средств происходит путём последовательных платежей с применением электронных средств, что прерывает связь между полученным доходом и совершенным противоправным деянием.

7. Анонимность в сети зачастую реализуется посредством технологии «луковой» маршрутизации, позволяющей создать защищенное подключение. Происходит разбитие сетевых запросов на множество фрагментов и пересылка их через различные виртуальные туннели.

В качестве рекомендаций для решения проблемы анонимности в сети, хотелось бы озвучить предложение, которое неоднократно освещалось рядом исследователей, а именно возложить на провайдеров – поставщиков трафика обязанность блокировать доступ к Интернет-ресурсам, которые обеспечивают сокрытие личности в сети. Также видится целесообразным введение обязательной идентификации пользователей при входе в глобальную сеть.

Нельзя не подчеркнуть, что значительно повысит эффективность противодействия НОН устранение технологического отставания правоохранительных органов от современного уровня развития ИКТ [7, с. 122-129].

Таким образом, повышение эффективности деятельности органов внутренних дел по противодействию преступлениям, совершенным с использование ИКТ, обеспечивается комплексной слаженной деятельностью подразделений и служб территориальных органов МВД России, по ключевым направлениям, обозначенным в настоящей статье. При этом, ограниченный объем публикации не позволяет отразить весь спектр направлений, за организацию которых отвечает начальник территориального органа. Вместе с тем, ключевые из них нашли в ней свое отражение.

Список использованной литературы

1. Состояние преступности в России за 2019 год [Электронный ресурс] // Министерство внутренних дел Российской Федерации: краткая характеристика состояния преступности в Российской Федерации за январь-август 2023 года // URL: https://xn-b1aew.xn-p1ai/reports/item/41741442/.

2. Информационно-аналитические материалы Следственного департамента МВД России за 2020 г. [Электронный ресурс] // URL: https://мвд.рф/mvd/structure1/Departamenti/Sledstvennij_departament

3. Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дисс. …канд. юрид. наук. – Иркутск, 2017. – 211 с.

4. Обзор судебной практики Верховного Суда Российской Федерации № 3. 2017. (утв. Президиумом Верховного Суда РФ 12 июля 2017 г.) [Электронный ресурс] // СПС Консультант плюс 2020.

5. Об информации, информационных технологиях и о защите информации: федеральный закон от 27 июля 2006 г. № 149-ФЗ // СЗ РФ. – 2006. – № 31 (ч.1). – ст. 3448.

6. О связи: федеральный закон от 7 июля 2003 г. № 126 // СЗ РФ. – 2003. – № 28. – Ст. 2895.

7. Гаврилин Ю.В. Противодействие цифровой трансформации наркопреступности // Труды Академии управления МВД России. – 2020. – №4 (56). – С. 122–129.

Кочкина Мария Сергеевна,
адъюнкт, e-mail: mari.koshkina.98@bk.ru
(Воронежский институт МВД России, Российская Федерация)

О НЕОБХОДИМОСТИ ЗАЩИТЫ НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД НРАВСТВЕННОМУ РАЗВИТИЮ

Аннотация. В настоящей статье рассмотрена общественная опасность сети Интернет для несовершеннолетних, в которой размещается порнографическая информация, причиняющая вред их нравственному и духовному развитию. Раскрываются некоторые причины и условия в связи, с которыми несовершеннолетние становятся потребителями порно-контента. Автором предлагаются меры по обеспечению информационной защищенности несовершеннолетних от порнографии в сети Интернет.

Ключевые слова: порнография, порно-контент, эротика, законодательство о порнографии, оборот порнографии, порнографические материалы и предметы, уголовное законодательство о порнографии.

ABOUT THE NECESSITY TO PROTECT MINORS ON THE INTERNET FROM INFORMATION HARMFUL TO MORAL DEVELOPMENT

Abstract. This article examines the social danger of the Internet for minors, which contains pornographic information that is harmful to their moral and spiritual development. Some reasons and conditions are revealed in connection with which minors become consumers of porn content. The author proposes measures to ensure the information security of minors from pornography on the Internet.

Keywords: pornography, porn content, erotica, legislation on pornography, circulation of pornography, pornographic materials and objects, criminal legislation on pornography.

В современных условиях вседоступности любого вида информации распространенность порнографии приобрела статус глобальной проблемы. Нельзя сказать, что она носит локальный характер. Вопрос настолько широкомасштабен, что его актуальность одинакова для стран с разным уровнем социально-экономического развития, отличной друг от друга бытовой культурой и религией. Любой пользователь сети Интернет за считанные секунды может найти порнографический сайт и получить к нему беспрепятственный доступ, вне зависимости от своего возраста.

Самой уязвимой категорией Интернет-пользователей являются несовершеннолетние, так как даже не прибегая к какому либо поиску в сети Интернет, а просто находясь в ней они имею возможность столкнуться с данными, которые могут напугать, навредить психическому и морально-нравственному развитию (например, информация порнографического характера; сцены насилия; склонение к самоубийству; реклама наркотических средств или одурманивающих веществ и т.д.).

Информация порнографического характера наносит вред всем возрастным категориям интернет-пользователей. Наиболее негативное воздействие приходится на восприятие несовершеннолетних, в силу отсутствия у них понятия о нормальной сексуальной жизни, не до конца сформированных жизненных ценностей, эмоциональной и психической неустойчивости, обусловленных сильными гормональными перепадами. Поэтому, транслируемые часто в порно-роликах насилие, жестокость, извращенные формы половых актов (оральный, анальный, групповой секс), постоянная смена половых партнеров и др., может приняться несовершеннолетним зрителем за норму, в следствии чего произойдет недопустимая подмена понятий. Просмотр порнографии ведет к подрыву авторитета семейных ценностей в социуме и способствует его моральному разложению. Часты случаи, когда подростки начинают просматривать порно-ролики для эмоциональной разрядки в пубертатном периоде, что в последующем может привести к их бесконтрольному просмотру и порно-зависимости, которая чревата разными побочными эффектами, в том числе компульсивным нарушением сексуального поведения [1].

Категория «порнография» не закреплено в Российском законодательстве, также не существует четко выделенных критериев, позволяющих отграничить порнографию от эротики. Поэтому, многие ученые из различных сфер (социологии, сексологии, психологии, различных отраслей права), предлагают свой категориальный аппарат в зависимости от специфики их деятельности.

Эксперты называют следующие существенные признаки порнографии:

– ставит на первый план макро-плановое исполнения секса;

– сосредотачивается на инструментализации полового акта;

– абсолютно бездумно направлена на возбуждение сексуальной потенции;

– порнография не знает ограничений;

– что бы быть или казаться разнообразной и использовать возбуждающий эффект особенного, порнография основное внимание уделяет отличиям от нормы;

– имеет своим содержанием различные формы насилия и апеллирует к жестокости и грубости;

– преимущественными потребителями порно-контента являются мужчины;

– в ней устранен момент интимности, делается открытым то, что не предназначено для сторонних глаз [2, с. 115].

В контексте рассматриваемой темы несовершеннолетний выступает в роли жертвы, которая потребляет и усваивает порно-контент. Причем, попасть на порно-сайт несовершеннолетний пользователь может как целенаправленно, ища желаемую ссылку, так и по ошибке – кликнув случайно по всплывающим окнам, нативной рекламе, которая появляется на видео-хостингах, в социальных сетях, может прийти в спам-сообщении.

Ключевыми причинами, по которым несовершеннолетние просматривают порно являются: возрастные особенности, которые происходят с подростками. Видоизменение собственного тела, гормональные всплески, которые приходятся, как правило на возраст 12-17 лет; зарождение интереса к противоположному полу, первые романтические отношения, в которых тинейджер может ощущать чувство полового влечения формирует в нем интерес к сексуальной жизни в целом. Как правило, малый процент от общего числа несовершеннолетних захочет ознакомиться с научной, психологической и социологической литературой, объясняющей и описывающей физиологические процессы, которые происходят с несовершеннолетними во время полового созревания, раскрывающей с научной точки зрения что такое половой акт. Сниженное чувство контроля, своеобразие поведения подростков толкает их на удовлетворение своего интереса путем просмотра воочию, при помощи порно-сайтов, которые в последующем приобщают подростков к их постоянному использованию. Потребность в удовольствии при незавершенности интеллектуального развития, недостаточности знаний, несформированности взглядов и отсутствии социального опыта, жизненных ценностей, целей и способов их достижения смещаются в сторону психологического комфорта, сиюминутных наслаждений [3]. Отсутствие заинтересованности Интернет-провайдеров в действительном ограничении несовершеннолетних от информации, доступ к которой им запрещен (несовершенство механизмов идентификации возраста, которые создают лживый облик защищенности и недоступности, так, например, каждый нажимающий на порно-сайте на кнопку «Да, мне исполнилось 18 лет» беспрепятственно получает доступ к порно-контенту); размещение нативной рекламы, содержащей в себе порнографический контекст (предложения перейти по ссылке чтобы попасть в приватный чат, где распространяются порно-ролики), реклама порно-симуляторов, все это размещается даже на обычных новостных сайтах.

Порнография спекулирует на дефиците новизны – показывает сексуальную жизнь в извращенной форме, нарушает принятые в обществе запреты. Она нравственно растлевает несовершеннолетних, оказывает пагубное влияние на их духовное и моральное развитие, дегуманизирует институт семьи и часто создает неправильное представление у подростков о половой жизни. Порнография непрерывно транслирует вульгарность, цинизм и натурализм, которые в последующем (в случае постоянного просмотра или использования порнографии) могут стать бессознательной ассоциацией у подростков к любому половому акту.

Основными условиями просмотра информации порнографического характера среди несовершеннолетних выступают: отсутствие полового воспитания подростков как родителями, так и образовательными учреждениями. Тема полового созревания и секса является табуированной в большинстве семей, немногие родители готовы откровенно и доверительно рассказать об этом своему чаду.

Давление сверстников внутри подростковой группы – еще одно распространенное условие. Любой подросток характеризуется в силу его возраста еще неокрепшей психикой, высокой степенью подверженности общественному мнению, желанием угодить большинству, потребностью отнесения себя к какой-либо группе, поэтому несовершеннолетние могут потреблять порноконтент «за компанию».

Для обеспечения информационной защищенности несовершеннолетних от порнографии в сети Интернет, по нашему мнению, необходимо:

– усложнение механизма попадания на порно-сайты за счет установления обязательной идентификации пользователя через мессенджеры/социальные сети, иные приложения, где возраст пользователя подтвержден изначально;

– установление родителями на компьютерах и мобильных устройствах детей программ-блокировщиков, которые позволяют фильтровать доступ к Интернет-ресурсам;

– контроль родителями подростков их аккаунтов на предмет нахождения на устройстве порнографического контента или иных цифровых следов, свидетельствующих о факте поиска или просмотра вышеназванного (чаты, история поиска, закладки, фотогалерея и т.д.);

– соблюдение родителями несовершеннолетних «цифровой гигиены», которая бы включала в себя удаление истории поиска в браузерах в случае, если поисковые запросы могут нанести вред психике или морально-нравственному развитию несовершеннолетнего, осуществление выхода из своих аккаунтов в социальных сетях.

Список использованной литературы

1. Бэрон Р., Ричардсон Д. Агрессия. – СПб: Питер, 2001. – 352 с.

2. Михайлова М.В., Шишкина С.Г. Иллюстративный фактор в разграничении понятий «Эротика» и «Порнография» // Приволжский научный вестник. – 2013. – №9 (25). – С. 115–120.

3. Противодействие распространению криминальной субкультуры среди несовершеннолетних / Р.Б. Иванченко, О.А. Садыкова, А.Н. Щеголева, Е.А. Буданова, А.В. Польшиков. – Воронеж: Воронежский институт МВД России, 2019. – 35 с.

Курумбаева Айнур Бекежановна,
докторант факультета послевузовского образования
майор полиции, e-mail: ainura77707@mail.ru
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

ВИКТИМОЛОГИЧЕСКИЕ АСПЕКТЫ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ СИСТЕМ

Аннотация. В настоящее время наблюдается значительный рост преступлений с использованием информационных систем. Статья посвящена рассмотрению вопросов, касающихся виктимологической характеристики мошенничества, совершаемого с использованием информационных систем. Особое внимание обращается на личность потерпевшего, его демографическую характеристику, пол, возраст, правовую просвещенность, психофизические свойства, социальный статус и социальное положение, а также – на перспективные направления изучения вышеуказанной темы.

Ключевые слова: виктимология, характеристика жертвы, мошенничество в сфере информационных систем, качества личности.

VICTIMOLOGICAL ASPECTS OF FRAUD USING INFORMATION SYSTEMS

Annotation. Currently, there is a significant increase in crimes involving information systems. The article is devoted to the consideration of the victimological characteristics of fraud committed using information and information systems. Particular attentionis paid to the personality ofthe victim, his demographic characteristics, gender, age, le-gal enlightenment, psychophysical properties, social status and social status, as well as to promising areas for studying the above topic.

Keywords: victimology, victim characteristics, fraud in the field of information information systems, personality quality.

В настоящее время наблюдается значительный рост преступлений с использованием информационных систем. С переходом к смешанной экономике и на фоне стремительно развивающихся информационных систем, правовой механизм защиты населения от преступных посягательств мошенников ослабевает, а способы их совершения прогрессируют и трансформируются. Согласно статистическим данным, на территории Республики Казахстан в январе–августе 2022 года произошло существенное увеличение зарегистрированных преступ-

лений в IT-сфере. За 8 месяцев 2022 года правоохранители выявили 180153 (+66,8 %) преступлений, совершенных с использованием информационных систем или в сфере компьютерной информации. При этом доля таких преступлений от числа всех зарегистрированных в Казахстане составляет 4,4 %: т.е., каждое двадцатое [1].

По данным Генпрокуратуры Республики Казахстан, наиболее часто совершаются такие кибер преступления, как: неправомерный доступ к компьютерной информации, распространение вирусных программ и спама, мошенничество в сфере компьютерной информации. Увеличение мошенничеств, совершаемых с использованием информационным системным способом, связано с легкой доступностью и популяризацией цифровых технологий, а также свидетельствует о недостаточной защищенности граждан от посягательств на их собственность (телефонные вирусы, лживые SMS-просьбы о помощи, продажа товаров, не соответствующих действительности).

В юридической литературе на протяжении длительного периода времени обсуждается рациональное и правильное определение понятия жертва. Большинство ученых считают, что жертвой преступления могут быть только физические лица, которым преступлением причинен моральный, физический или имущественный вред (узкое, операционное определение) [2, с. 8].

Канадская ученая М. Барель определяет жертву как лицо, перенесшее посягательство на основные права, ввиду сознательного воздействия другого лица [3, с. 342]. В.Е. Христенко утверждает, что жертва – это человек, который утратил значимые для него ценности ввиду воздействия на него другим лицом (стороной взаимодействия), группой людей либо определенными событиями и обстоятельствами [4, с. 53]. Согласно Декларации основных принципов правосудия для жертв преступлений и злоупотребления, под «жертвой» необходимо понимать лицо, которому индивидуально или группой лиц причинен вред, включая физический, моральный, эмоциональный, материальный, а также, существенное ущемление основных прав в результате действия или бездействия независимо от того, был ли установлен, арестован, передан суду или осужден правонарушитель, а также - независимо от родственных связей между правонарушителем и жертвой [6]. Рассматриваемые позиции, бесспорно, внесли существенный вклад в виктимологическую науку, но, главным образом, не содержат в себе общепризнанной позиции по определению понятия «жертва мошенничества в сфере IT-технологий».

Анализируя виктимологическую литературу, мы можем предположить, что под жертвой мошенничества в сфере IT-технологий следует понимать лицо или группу лиц, являющихся активными пользователями информационных систем; любого возраста и пола; характеризующихся легковерностью, корыстью, эгоистичностью, несообразительностью; чаще всего, использующих незащищенное программное обеспечение, понесших имущественный и (или) моральный вред от противоправного деяния в сети Интернет или посредством информационных систем, независимо от того, признаны ли они в установленном порядке потерпевшими от данного преступления или нет. Изучение и анализ личности жертвы следует начинать с ее социально-демографической характеристики: уста-

новления пола, возраста, рода занятий, уровня образования, места жительства. Наибольшее количество пострадавших от рассматриваемого преступления составляют женщины, так как они чаще идут на контакт и при принятии решений руководствуются чувствами и эмоциями, в то время как мужчины более рациональны.

В результате изучения и анализа архивных уголовных дел о мошенничестве, совершаемых с использованием информационных систем на территории Республики Казахстан, нами выявлено:

1. Жертвами рассматриваемой категории преступлений были как мужчины, так и женщины. Но стоит отметить абсолютное преобладание женщин среди потерпевших, ввиду более высокой активности и эмоциональности.

2. Большинство жертв – лица от 45 до 58 лет (28 %). Среди других возрастных групп потерпевшие разделились следующим образом: до 18 лет – 8 %, до 30 лет – 17 %, 31–35 лет – 21 %, 36–40 лет – 5 %, 41–45 лет – 21 %.

3. Правовая просвещенность либо безграмотность оказали значительное влияние на уровень виктимности потенциальной жертвы. Обычно, жертвами преступлений становились лица, имеющие низкий уровень правовой грамотности. Однако следует заметить, что определенная доля потерпевших от данных преступлений – это люди с высшим образованием, что объясняется широким кругом их деловых контактов и стабильным материальным положением.

4. Психофизические свойства личности также влияли на степень ее виктимности. Характеры жертв информационно-телекоммуникационного мошенничества, работавших в незащищенном от вирусов и спама киберпространстве, отличались чрезмерной доверчивостью, легкомысленностью, некой суеверностью, некомпетентностью, неопытностью и незнанием элементарных мер интернет – безопасности.

5. Социальный статус и социальное положение является одной из основных характеристик структуры личности потерпевшего. Люди преклонного возраста большую часть жизни проживали при другом социально-экономическом строе, когда сомнений в надежности банковской системы, а также, системы социальной помощи и обеспечения быть не могло. С прогрессом общества данная категория людей, познавая мир новых технологий посредством всемирной глобальной сети интернет, забывает об элементарных мерах предосторожности.

Злоумышленники активно пользуются доверчивостью и наивностью граждан, выдавая себя за дружелюбного продавца с «накрученным» рейтингом, собирателя средств на лечение тяжелобольного родственника, предсказателя судьбы, снимателя порчи, сглаз и много другое.

6. Одиночество и социальная изолированность. Как правило, жертвами, чаще всего, становились разведенные либо овдовевшие лица, которым, в силу своего одиночества, не с кем обсудить насущные проблемы.

7. Подверженность финансовому стрессу. Лица, в силу своего неудовлетворительного материального положения (имеющие кредиты, ипотеки, краткосрочные займы), начинали искать дополнительные пути заработка с целью досрочного погашения долга. Как правило, обращаясь к сети Интернет, они находили массу вариантов, но, следуя по пути наименьшего сопротивления, стано-

вились жертвами фишинга, онлайн-казино, фальшивых интернет магазинов с повышенным кешбеком, «магических кошельков» и других преступных махинаций.

Анализируя личность жертвы, необходимо также учитывать ее психологическое состояние: агрессивное или провоцирующее; правомерное или противоправное; слабовольное или устойчивое и др. Данные характеристики составляют психологический аспект виктимности жертвы. Изучение роли жертвы в механизме преступления направлено на решение общетеоретических проблем криминологического плана либо разработку и создание виктимологических теорий, учитывающих специфику рассматриваемых видов преступлений или потерпевших от них [5, с. 50]. Необходимо отметить, что на возможность стать жертвой влияют как объективные признаки (пол, возраст, образование), так и субъективные (к ним относятся внутренние характеристики – доверчивость, мнительность, сострадание, желание обогатиться и др.). Лица, в большей степени, сострадающие тяжело больным детям, животным и другим нуждающимся, становятся «живой мишенью» различного рода размещений, «благотворительных акций» в сети интернет, а также, посредством телекоммуникационной связи. Большое влияние на виктимность личности оказывает совокупность факторов, конкретизирующих человека, а именно: профессиональная активность, подверженность новым течениям в культуре и технике, и др.

Говоря о характере и степени выраженности качеств личности, можно выделить несколько типов жертв:

1. Виктимно-универсальный. Жертвы характеризуются повышенной уязвимостью, а также, типичной для них как активностью виктимного поведения, так и пассивностью.

2. Виктимно-избирательный. Жертве свойственна повышенная уязвимость, а традиционные формы поведения обусловливают ее виктимную предрасположенность во взаимодействии с характером конфликтных ситуаций.

В качестве примера можно привести коммерческую деятельность в сети Интернет, когда лицо с высокой виктимностью занимает управляющую должность, но, в силу неадекватного поведения, получает имущественный ущерб.

3. Виктимно-ситуативный. Жертва обладает невысоким уровнем виктимности (примерно, средним), потерпевшим становится вследствие сложившихся в совокупность ряда ситуативных факторов.

4. Виктимно-случайный. Сочетание и слияние случайных обстоятельств определяют характеристику жертвы.

5. Виктимно-профессиональный. Виктимность жертв связана с их трудовой (рабочей) деятельностью [6, с. 58].

Приходится констатировать, что правоохранительным органам сложно эффективно противостоять современнейшим методам и формам мошенничества, совершаемого с применением информационных систем.

Практика правоприменения свидетельствует о том, что значение виктимологической характеристики недооценивается правоприменителями, не ведется анализ и учет данных, касающихся жертв рассматриваемых преступлений. Одной из основных причиной малоэффективной борьбы с рассматриваемым явле-

нием выступает недостаточная научная проработка, пересечение и смешение понятий, отсутствие научных концепций, которые, в своей совокупности, определяют феномен жертвы информационных систем мошенничества.

На основании изложенного, можно сделать вывод о том, что к виктимологической характеристике жертвы корыстных преступлений, совершаемых с использованием информационных систем, относятся: ее возраст и пол, финансовое состояние, место и характер работы, морально-психологическое состояние, социальное положение, уровень образования. Безусловно, изучение указанных особенностей личности жертвы является важным условием развития виктимологии, снижения уровня потенциальных жертв и эффективным средством предупреждения преступлений.

Список использованной литературы

1. Статистические данные о зарегистрированных преступлениях на территории Республики Казахстан [Электронный ресурс] // Официальный сайт Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан. – Информационный сервис. – URL: https://www.qamqor.gov.kz.

2. Ривман Д.В. Виктимологические факторы и профилактика преступлений: учебное пособие. – Л., 1975. – 154 с.

3. Baril M. La criminologieet la Justice a l'heure de la victime // Revue Internationale de criminologie et de Police technique. – 1981. – № 4. – P. 340–345.

4. Христенко В.Е. Психология поведения жертвы. – Ростов н/Д: Феникс, 2004. – 411 с.

5. Ривман Д.В. К вопросу о социально-психологической типологии потерпевших от преступлений // Виктимологические проблемы борьбы с преступностью. – Иркутск, 1988. – С. 48–57.

6. Калинина С.Б. Психологические особенности женщин – жертв домашнего насилия // Психология. – Пермь, 2010. – № 19. – С. 54–60.

Маликов Жандос Анарбекұлы,
жоғары білім беру факультетінің докторанты
з.ғ.м., полиция капитаны, e-mail: malikov-zhandos@mail.ru
(Қазақстан Республикасы ІІМ Б. Бейсенова атындағы Қарағанды академиясы, Қазақстан Республикасы)

ИНТЕРНЕТ ЖЕЛІСІНДЕГІ БАЛА ҚЫЛМЫСТАРЫ

Аннотация. Соңғы уақыттарда әлеуметтік желілердің веб-сайттары-жаңа құралдарды пайдаланған кезде, балалар мен интернетке қатысты соңғы оқиғалар мен жаңалықтар балалардың желіде болған кездегі осал тұстары көбейіп келе жатыр. Қылмыстық жүйе осы жағдайлардың салдарларынан балалар тарапынан заң бұзушылық әрекеттер орын алған сәттерде бірқатар дилеммаларға тап болып отыр, өйткені балалар өз әрекеттері үшін заңды

жауапкершілікке тартылмайтын кәмелетке толмағандар институты аясына топтастырылады. Сонымен қатар мақалада балалар әлеуметтік медиа вебсайттарын пайдалану кезінде кездесетін мәселелер қарастырылады. Қай уақыттарда балалармен жасалған әрекет немесе әрекетсіздіктер құқық бұзушылық әрекет немесе қылмыс санатына жатқызылатыны туралы түсіндіріледі. Осы құжатта интернет пен балаларға қатысты құқықтық мәселелерді реттеудегі шиеленістер көрсетілген.

Түйін сөздер: киберқауіпсіздік, балалар, кәмелеттік жас, қылмыстық заңнама, Интернет.

CHILD CRIME ON THE INTERNET

Annotation. Recently, social media websites-using new tools, the latest events and news related to children and the Internet-have become increasingly vulnerable when children are online. The criminal system faces a number of dilemmas at the time of the commission of offenses by children due to the consequences of these circumstances, since children are grouped within the institution of minors who are not legally responsible for their actions. The article also examines the problems that children face when using social networking sites. At what time the actions or omissions committed with children are explained by the fact that the offense is classified as an action or crime. This document highlights the tension in the regulation of legal issues related to the Internet and children.

Keywords: cybersecurity, children, adults, criminal law, Internet.

Көп жағдайда қоғам барлық балаларды қараусыз қалудан, қатыгездіктен немесе сырттан келетін зиянды әрекеттерден қорғауға ғана назар аударады да, ал соның ішінде басқа адамдарға зиян келтіруге немесе мүліктік зиян келтіруге қатысатын балаларды қорғау мәселелері назардан тыс қалып жатады. Бұл тұста балалардың Интернетті пайдалану әсеріне қатысты өсіп келе жатқан алаңдаушылыққа назар аудару аса маңыздырақ. Осылайша, Интернеттегі баланың теріс қылықтарын құқық бұзушылық ретінде қарастыруға бола ма, жоқ па, дәлірек айтсақ, ересек адам жасаған жағдайда еш күмәнсіз қылмыстық әрекет болап саналатын құбылыс -балалар жасаған уақытта қандай әрекеттер санатына жатқызылады деген сияқты сұрақтар зерттеледі.

Ақырында, материал Үкімет (Ішкі істер министрлігі тарапынан) пен қоғамдастықтың, атап айтқанда ата-аналар мен мұғалімдердің, саясат пен нормативтік құқықтық ережелердің балаларды қорғаудың ғана емес, сонымен бірге олардың ел азаматтары ретіндегі мүмкіндіктерін кеңейтудің тетігін қамтамасыз етуде маңызды рөл атқаруы керек деп болжайды. Бұған құқықтық сананы насихаттау және балаларды интернеттегі іс-әрекеттеріне жауапкершілікпен қарауға және заңға, этикаға және моральға құрметпен қарауға үйрету арқылы қол жеткізуге болады. Қоғам мүшелерінің, әсіресе ата-аналар мен мұғалімдердің, соның ішінде полиция қызметінің портфелінде интернет қауіпсіздігіне алаңдаушылық артып келеді. Өйткені көптеген

артықшылықтарға қарамастан, Интернет қазіргі таңда кез-келген адам, тіпті бала немесе жас адам жасай алатын қылмыс құралына да айналып отыр.

Интернеттің күрделі бөлігі-бұл анонимді пайдаланушыны білдіреді, бұл жастың бұрмалануын оңай тудыруы мүмкін. Осылайша, жасты тану өте қиын, өйткені пайдаланушылардың нақты жасын анықтай алатын арнайы құрал немесе құрылғы жоқ. Тіпті растау үшін несие картасы қажет коммерциялық сайттарда да жасты манипуляциялау үрдісі байқалады. Компьютерлік ойындар, теледидар және Интернет балалар арасындағы әлеуметтік байланыстардың әлсіреуіне әкелді деген хабарламалар бар. Егер нақты әлеуметтік байланыстар болмаса, балалардан нақты өмірлік тәжірибе мен жұмсақ дағдыларды, мысалы, қарым-қатынас дағдыларын немесе тіпті дұрыс пен бұрысты ажырата алатын жеке қасиеттерді қалай күтуге болады. Неміс авторы Harmut von Henting жаңа медиа шындықтың біртіндеп жойылуына әкелді деп мәлімдеді [1]. Кейбір жағдайларда балалар компьютерлік ойындар сияқты интернетті пайдалануға тәуелді болуы мүмкін және олар шынайы өмірді сезінудің орнына іс жүзінде қиялдауға мүмкіндік алады. Алайда, Интернетті пайдалануға қарапайым тәуелділік мұндай әрекет басқа адамның құқықтарына қол сұғылмайынша немесе заңмен танылған мүлікке зиян келтірмейінше қиындық тудырмауы мүмкін. Қоғам мүшелері интернеттің зиянды әсеріне алаңдайды, бұл жазықсыз баланың құқық бұзушыға айналуына әкелуі мүмкін. Ең нашар жағдайда, Интернетке тәуелділік, онлайн ойындар және әлеуметтік медиа балаларды кибербопсалау, кибер-қудалау, кибер-груминг, жеке басын куәландыратын мәліметтерді әшкерелеу әрекеттерін қамтитын алаяқтық, кибер әрекеттердің көмегімен өз-өзіне қол жұмсау және т. б. сияқты киберқауіпсіздікпен байланысты құқық бұзушылықтарға итермелеуі мүмкін. Құзырлы органдар, олардың іс жүзінде киберқауіпсіздікпен байланысты қылмыстар жасап жатқанын білмей немесе түсінбей отырғанына қарамастан, оларды белгілі бір дәрежеде жергілікті заңдарға сәйкес жауапқа тартуы мүмкін. Олардың әрекеттерінің нәтижесінде олар өздерінің болашағына қауіп төндіруі мүмкін. Қылмыстық заңнама әрқашан осындай заң бұзушылар кәмелетке толмаған, сондықтан көптеген жолдармен өздері үшін заңды жауапкершілікке тартылмаған кезде не істеу керектігі туралы дилеммаға тап болып отыр. Көбінесе қоғам балаларды қараусыз қалудан, қатыгездіктен немесе зиян келтіруден қорғауға назар аударады, бірақ көбінесе балалардың өздерін қорғауды елемейді. Бұл бірдей маңызды және интернетті күнделікті пайдалану контекстінде қарастырылуы керек. Осылайша, «Интернеттегі баланың теріс қылықтарын девиантты әрекет ретінде қарастыруға бола ма» деген сұрақ девиантты әрекеттің мағынасын талдау арқылы зерттеледі.

Бала және интернет туралы түсінік.

Балалардың ойнақылық, кәсіпкерлік, осалдық, нәзіктік және өмірлік маңызды шешімдер қабылдаудағы қабілетсіздік сияқты белгілі бір сипаттамалары бар екені белгілі. Швед ғалымы U.Sjöberg жүргізген зерттеулер Интернетті балалар мен жасөспірімдерге арналған ойын алаңы ретінде қарастырады, онда олар өздерінің жеке ерекшеліктерімен айналыса алады [2]. Бала сөзінің тұжырымдамасын және оның Интернетпен байланысын, сондай-ақ

баланың сипаттамалары олардың киберкеңістік қауымдастығындағы өкілдігі мен өзара әрекеттесуіне қалай әсер ететінін түсіну маңызды. Екінші жағынан, балалар американдық белгілі саяси қайраткер Бэнджамин Франклин айтқан көптеген топтарды білдіреді. Ол бұл топтарды төрт түрлі кезеңге бөледі: әр түрлі қажеттіліктер, құқықтар мен міндеттер жүктейтін жөргектегі кезең, нағыз балалық кезең, жасөспірім кезең және ертерек ер жеткен кезең. Демек, балалар баланың өз іс-әрекеттері үшін қаншалықты жауапты болуы мүмкін екендігі туралы күрделі пікірталас болып табылады, өйткені олар әртүрлі жауапкершілік деңгейлерін білдіреді. Біз жауапкершілікті интернетке қатысты дұрыс және бұрыс нәрсемен байланыстырамыз. Ағылшын тумасы, бала құқықтарын қорғаушы маман Эндрю Бейнэм балалар туралы “Егер олардың «құқықтары» болса, онда олардың да жауапкершілігі бар ма?” – сұрақ туғызады [3].

Технология біздің өмірімізге әсер етті және кейбір жағдайларда бұл бізді ненің дұрыс, ненің бұрыс екенін, әсіресе балаларымызды оқытуда, ажыратуда дилемма тудырады. Осы орайда тағы бір британдық автор С.Бандалли — дұрыс пен бұрысты ажырату туралы ілім сәтсіздікке ұшырайды деген кең қоғамдық консенсус бар деп мәлімдейді [4]. Біздің дұрыс пен бұрысты қабылдауымызға көбіне қоғамның сенімдері, нормалары мен өмір салты әсер етеді және олардың орындалуын қамтамасыз ету үшін заң енгізіледі. Егер біздің балаларымызға дұрыс пен бұрысты үйрету сәтсіз болса, біз балаларды интернетте моральдық тұрғыдан дұрыс нәрсені түсінбегені үшін жазалауымыз керек пе? Біздің дәлеліміз-интернеттің дамуы балаларды ненің дұрыс, ненің бұрыс екенін ажыратуда одан әрі шатастырады. Осы жас құқық бұзушыларды қорғауды қарастырған кезде өте сақ болу керек-олардың мүдделеріне сәйкес келетін заңды жауап қандай? Тағы да, С.Бандалли өзінің ««Doli incapax» (қылмыс жасауға қабілетсіздік) презумпциясын жою және балалардың қылмыстық әрекеттерін криминализациялау» – деген еңбегінде бұзақылық және ауыр құқық бұзушылық туралы айтады – бұл күрделі тұжырымдамалық мәселелер, ал қылмыстық құқықтың өзінде көптеген моральдық дилеммалар бар.

Балалар мен интернетке қатысты әртүрлі мәселелерді қарастыратын зерттеуші маман, Лондон Экономика мектебінің (LSE) профессоры Соня Ливингстонның тәжірибесі туралы онлайн түрде балаларға кең ауқымды зерттеу жүргізілген екен. Екінші жағынан, Соня Ливингстон компьютерлер біздің әлеуметтік және психологиялық өміріміздің бір бөлігі болып табылатын құрал екендігі туралы жазады – деп атап өтеді американдық ізденуші Шэрри Тёркл [5].

Ш. Тёркл өзінің «Экрандағы өмір технологиясы» кітабында өзгерістерді тек не істеп жатқанымызда ғана емес, сонымен бірге қалай ойлайтынымызда да кездеседі деп саралайтын көзқарас танытады. Басқа кітапта өзімен бірге былай деп жазды: «Неліктен біз технологиядан көбірек және бір-бірімізден аз күтеміз, онда технологияның дамуының адамның әлеуметтік мінез-құлқына жағымсыз әсерін бағалана түседі» [6]. Шынында да, технологияның, жасанды интеллекттің, сондай-ақ басқа да құбылыстар мен заттар интернеттің дамуы қоғамның өмір салтын өзгертуден аулақ бола алмайды. Дегенмен, ақылды адам

технологияның толқынына, әсіресе жас ұрпаққа берілмегені үшін бірдей қорғап, қолдауы керек. Қазіргі әлемде біз желі қолданушылары Интернетті жауапсыз пайдаланған кезде моральдық және этикалық аспектілердің әлсіреуіне куә болып отырмыз. Балаларды интернеттегі құрбандықтан қорғауға баса назар аударатын әдебиеттерге қарамастан, ұмытпау керек тағы бір аспект-интернетті пайдаланатын балалар мен жастарды этика мен адамгершілікке үйрету. Қазіргі әлемде адамгершілікті оқыту өте қиын болуы мүмкін, балалар интернетте және тіпті ұялы телефондардан-ақ онлайн режимде барлық ақпаратты демде қабылдап ала алады.

Балалар қылмысының анықтамасы.

Кейбір елдердің юрисдикцияларында құқық бұзушылық әрекеттің заңды анықтамасы жоқ. Мысалы, құқық бұзушы Кембридж сөздігінде көптеген адамдар үшін заңсыз немесе қолайсыз мінез-құлықпен айналысатын, әдетте жас адам ретінде анықталады. Оларды әдетте кәмелетке толмаған қылмыскерлер деп атайды. Ағылшын Оксфорд сөздігінде құқық бұзушы бейнесі қылмыс жасауға бейім жас жігіттің, әсіресе кішкентайлардың типтік мінез-құлқы ретінде анықталады [7]. Ал Малайзияда "Кәмелетке толмағандардың заңсыздығы" термині жастардың заңсыз әрекеттерінің кейбір түрлеріне сілтеме жасау үшін қолданылады [8]. АҚШ-та мұны кәмелетке толмағандар жасаған әрекет ретінде анықтайды, ол үшін ересек адам қылмыстық сотта жауапқа тартылуы мүмкін, бірақ кәмелетке толмағандар жасаған әрекет кәмелетке толмағандар сотының қарауына жатады [9]. Зерттеуіміздің дәйектілік деңгейін көтеру мақсатында басқа да мемлекеттер мәліметтеріне тоқтала кетсек, дәл осы анықтаманы Үндістан істері бюросы, Ішкі істер Министрлігі және 1908 жылғы канадалық Кәмелетке толмағандар туралы Заң қолданады (кейінірек ол ауыстырылды, 1984). Содан кейін 1984 жылғы Заң 2003 жылдың 1 сәуірінде күшіне енген кәмелетке толмағандарға қатысты қылмыстық сот төрелігі туралы Заңмен ауыстырылды (Канада Әділет министрлігі, 2016). Жоғарыда айтылғандардың бәрінен қорытынды жасауға болады: бала жасаған құқық бұзушылық тек жаңылыстырылған баланың құқық бұзушылық әрекеті ретінде қарастырылуы керек, бірақ қылмыс ретінде емес.

Кәмелетке толмағандардың құқық бұзушылық әрекеттері екі санатқа бөлінеді; біріншіден, тиісті құқықтық жүйелерге сәйкес заңмен тыйым салынған және жазаланатын әрекеттер немесе әрекетсіздіктер. Екіншіден, мәртебелік құқық бұзушылықтар деп аталатын әрекеттер, егер олар кәмелетке толмаған адам жасаса, құқық бұзушылыққа айналатын кейбір мінез-құлықтарды білдіреді [8]. Сонымен қатар кәмелетке толмағандар арасындағы қылмыс тұжырымдамасы заңмен құқық бұзушылық (қылмыстық заңнаманы бұзу) және құқық бұзушылық мәртебесі (кәмелетке толмағандар туралы заңдарды бұзу) ретінде анықталған әрекеттерге әкелетіні атап көрсетіледі. Әдеби дереккөздердің көпшілігінде кәмелетке толмағандар арасындағы балалар қылмысы мен құқық бұзушылықтар заңға сәйкес 18 жасқа толмаған балалар ретінде анықталған кәмелетке толмаған құқық бұзушылардың бір тобы ретінде қарастырылады. Тағы бір мысал ретінде айта кететін болсақ, Малайзия Заңы өз ережелерінде «бала» сөзі ретінде барлық кәмелетке толмағандарды қолданады

[9]. Алайда, Америка Құрама Штаттарының «Кәмелетке толмағандардың әділдігі мен қауіпсіздігі үшін күрес» басқармасы (OJJDP) жас қылмыскерлерді немесе құқық бұзушылықтарды екі санатқа бөледі, атап айтқанда; 13 жасқа дейінгі және 13 жастан асқан балалар [10].

13 жасқа толмаған балалар жасаған құқық бұзушылық әрекеттерді жасаған фигуранттар ғана кәмелетке толмаған құқық бұзушылар болып саналады. Сонымен қатар, кәмелетке толмағандар жасаған заңсыз әрекет осы жастан асқан адам кәмелетке толмаған қылмыскер ретінде жіктеледі [11].

Олар жас қылмыскерлерді осы екі топқа жіктеу керек деген қорытындыға келді, өйткені олардың пікірінше, ерте жаста жасалған заңсыз әрекет жасөспірім болған кезде ауыр және зорлық-зомбылыққа бейім кәмелетке толмаған құқық бұзушыларға айналу қаупін арттырады [12]. Осылайша, қылмыскерге немесе құқық бұзушыға (құқық бұзушы қыз балаға) қатысты "құқық бұзушылық" сөзіне артықшылық беріледі. Бұл әлдеқайда дұрыс, өйткені балалар табиғаты мен жасы бойынша әдетте қылмыс жасай алмайды деп саналады. Олар осал немесе сырттан келетін жағымсыз әсерлер мен қысымға сезімтал. Facebook, Instagram, Twitter, Tik-Tok, Telegram және Вконтакте сияқты әлеуметтік медиа сайттардың пайда болуымен бұл жасына қарамастан желі қолданушыларына Интернеттің жағымды жақтарын ашатыны сөзсіз. Көптеген зерттеушілер ұзақ уақыт бойы құқық бұзушының өміріндегі әлеуметтік және экономикалық өзгерістермен, әсіресе қираған үй теориясымен, соның ішінде неке сапасы мен ата-ана тәрбиесімен байланысты екенін Флауэрс атап өтті [13]. Бұл 1980 жылдардағы жағдай болды. Ақпараттық технологиялар дәуіріндегі қоғамның қазіргі кездегі қиындықтары тек осы теориямен шектелмейді. Клиникалық психологтың айтуы бойынша құқық бұзушылық мінез-құлқының себебі қоғамның әртүрлі топтары, соның ішінде ажыраспаған отбасылар мен кәсіби отбасылар болып табылады [14].

Қылмыстық сот төрелігі жүйесі әрқашан заңды бұзушылар кәмелетке толмаған, сондықтан көптеген жолдармен өздері үшін заңды жауапкершілікке тартылмаған кезде не істеу керектігі туралы дилеммаға тап болды. Көбінесе қоғам балаларды қараусыз қалудан, қатыгездіктен немесе зиян келтіруден қорғауға назар аударады, бірақ көбінесе балалардың өздерін зиян келтіруден қорғауды елемейді. Бұл бірдей маңызды және балаларды құқық бұзушылықтар жасаудан сақтандыру мақсатында интернетті күнделікті пайдалану контекстінде қарастырылуы керек. Қылмыстық жауапкершіліктің негізі үш міндеттемені талап етеді. Біріншіден, жасалған әрекет заңсыз болуы керек. Екіншіден, бұл заңсыз әрекет ізгі ниетпен жасалған болу керек. Үшіншіден, бұл әрекетті дұрыс пен бұрысты ажырата алатын ересек және есі дұрыс адам жасауы керек. Осы тұжырымдамаға сүйене отырып, егер балалар қылмыс жасаса, олардың бойында осы міндеттемелер табылмағандықтан және табылмайтындықтан олар жауапқа тартылмайды.

Бала және қылмыстық жауапкершілік.

Сонымен, қылмыстық жауапкершіліктің ең төменгі жасын талдау бала қылмыскер бола ала ма, балалардың интернеттегі теріс қылықтары олардың заң алдындағы жауапкершілігін қалай тудырады деген сұрақты анықтау үшін

маңызды? Біріккен Ұлттар Ұйымының 1989 жылғы Бала құқықтары туралы Конвенциясының (БҰҰ БҚК) 1-бабы балаларды 18 жасқа дейінгі адамдар ретінде айқындайды. Алайда, БҰҰ БҚК мемлекетке кәмелетке толған жасты белгілеуге мүмкіндік береді. Сонымен қатар, қылмыстық процестегі балаларға қатысты іс-қимыл нұсқаулары сот төрелігі жүйесі және БҰҰ-ның кәмелетке толмағандар арасындағы қылмыстың алдын алу жөніндегі нұсқаулықтары ("Эр-Рияд нұсқаулары') қылмыстық жауапкершіліктің басталу жасына қатысты кейбір ұсыныстарды қамтиды. «Бейжің ережелері, 2.2 (А) ережесі» кәмелетке толмағандарға қатысты сот төрелігін жүзеге асырудың мынадай минималды стандартты ережелерін (БҰҰ, 1985) атап өтті:

– «Кәмелетке толмаған-бұл тиісті құқықтық жүйелерге сәйкес ересек адамның мінез-құлқынан өзгеше түрде құқық бұзушылық үшін жауапқа тартылуы мүмкін бала немесе жасөспірім». Бұл кәмелетке толмағандарға қатысты сот төрелігінің дұрыс орындалуын қамтамасыз ету үшін жасалады. Тағы да, бұл ережеде әр түрлі мемлекеттер анықтаған ең төменгі жасты сақтау үшін балалардың қылмыстық жауапкершілігінің стандартты ең төменгі жасы туралы нақты айтылмайды, бұл әдетте балалардың эмоционалды, психикалық және интеллектуалдық жағдайына, сондай-ақ мемлекеттің экономикалық, саяси, әлеуметтік және мәдени даму мәртебесіне байланысты.

Біріккен Британ Корольдігінде 10-14 жас аралығындағы балаларға арналған ағылшын заңнамасына сәйкес қабілетсіздік үлесінің презумпциясы балаларға үлкен тәуелсіздік пен олардың моральдық пайымдауға қабілетті екенін мойындауға мүмкіндік береді және сонымен бірге оларға дұрыс емес әрекеттері үшін жауапқа тартылуға мүмкіндік береді. Сонымен қатар, және 2003 жылғы қоғамға қарсы мінез-құлық туралы Заң сияқты заңдар балаларды зұлымдық жасауға қабілетті және назар мен бақылауға мұқтаж деп санайды, ал жастар қоғамның үйлесімділігіне қауіп төндіретін қауіпті топ ретінде қарастырылады [15]. Екінші жағынан, мемлекет қылмыстық заңның кейбір нормаларын сақтауға және ата-аналарға олардың балаларының мінез-құлқы, 2003 жылғы ағылшынның әлеуметтік мінез-құлқына қарсы актісінде көрсетілгендіктен санкциялар салуға міндетті. Интернет шекараны мойындамайтын және байланыс пен ақпарат таратудың ескі дәстүрлі тәсілдерін өзгерткен жаһандық құбылыс жасау үстінде. Нәтижесінде, заң қоғамды қылмыстық және заңсыз әрекеттерден қорғау құралы ретінде үлкен қиындықтарға тап болады, әсіресе егер мұндай әрекеттерді бала жасырын және тіпті онлайн форматта жасаса.

Балалар және әлеуметтік медиа: мәселелер мен сот процестері. Реттеудегі әлеуметтік желілердің құқықтық мәселелерін талқылау кезінде құжатта балаларға қатысты сұрақтар екі аспектке бағытталған: біріншіден, Интернеттегі балаларды құрбан ету, екіншіден, интернетті пайдалану кезінде өзін қоғамға қарсы ұстайтын балалар [16]. Интернеттегі балаларды құрбан етуге байланысты туындайтын құқықтық мәселелер өте кең. Дегенмен, алаңдаушылық тудыратын тағы бір аспект-балалардың, әсіресе жасөспірімдердің Интернеттегі қоғамға қарсы мінез-құлқы. Л.Дж. Сталанс пен М.А.Финн Интернет киберқылмыс түрлеріне қатысты ауытқулар мен заң бұзушылықтарға жол береді деп

мәлімдейді [17]. Медицина ғылымдарының докторлары М.Л.Се мен Мак Шейнс жүргізген зерттеуде интернеттегі девиантты мінез-құлықтың жеңілдетілген және кеңейтілген жіктелуіне және құқық бұзушылардың, бандалардың жеке бастарын зерттеуге негізделген, онлайн параметрлерге келетін болсақ, балалар мен жасөспірімдер интернетте серуендеу кезінде кездесетін мәселе кейде ата-аналардан жасырылуы мүмкін [18]. Зерттеу Интернеттегі жастардың қауіпсіздігі туралы үшінші сауалнаманың (YISS-3) деректеріне негізделген, 10-17 жас аралығындағы 1560 интернет қолданушысы мен олардың қамқоршыларының бүкіл ел бойынша өкілдік үлгісі бар телефон сауалнамасы. Жастардың интернеттегі жағымсыз тәжірибеге реакциясы жағымсыз тәжірибенің түріне, олардың ренжігеніне немесе оқиғадан туындаған басқа да жағымсыз реакцияларды сезінуіне және белгілі бір дәрежеде жастардың басқа сипаттамалары мен оқиғаларына байланысты өзгереді. Қытай Халық республикасының Фудань Университетінің профессоры Тянь Лу мырза Интернеттегі құқық бұзушылық ниетіне әкелетін психологиялық факторларды зерттеді [19].

Ұлыбританияда жүргізілген тағы бір зерттеуде «Проблемалы онлайн жастар топтары» (TOYG) деп аталатын топ Ұлыбританияның үш аймағындағы субъектілерден жиналған мәліметтерге негізделген [20]. Бұған білім беру, жұмысқа орналасу немесе кәсіптік оқытумен (NEETs) айналыспайтын жастар кіреді. Ол өзінің зерттеуінде осы жастардың интернетте тролль жасауының себептерін зерттейді. Интернет-тролльдер жалпы қоғам үшін үлкен проблемаға айналуда. Осылайша, мұндай мәселені шешу үшін қосымша құқықтық механизм қажет.

Қазіргі уақытта балалар интернеттегі «Заңсыз және қорлайтын» мазмұнға ұшырайды. Тағы бір маңызды мәселе-балалардың порнографиялық материалдарды көруі, ал ең нашар жағдайда балалар, әсіресе жасөспірімдер Интернетте сексуалдық суреттерді орналастырады. Сонымен қатар, қазіргі жастардың WhatsApp, WeChat және Twitter-ді, Telegram әлеуметтік желілерінде жиі отыруы – тек Интернет тәуелділікке ғана емес, сонымен қатар жыныстық тәуелділікке де ұшырау қаупін туындап отыр. Интернеттің жағымды жақтарынан басқа, Интернет қазір желіде тұрған гангстеризмді тарату құралына айналуда.

Мысалы, Джордано Н. Наварроның АҚШ-тың Солтүстік Каролина штатындағы орта мектеп оқушылары арасында жүргізілген сауалнамада киберқауіпсіздік пен Интернетке тәуелділіктің байланысын зерттейді [21]. Күнделікті газеттерде кеңінен жарияланған киберқауіпсіздік, кибербуллинг, кибер-құдалау, және кибер-бопсалау сияқты онлайн қылмыстардың көбеюіне қарамастан, Интернеттегі балалар қылмысы мен онлайн БАҚ туралы арнайы зерттеулер әлі де өте шектеулі. Интернеттегі қылмыстар мен әрекеттерді реттеу туралы Заң мен саясаттың жоқтығын жедел назар аударуды қажет ететін негізгі мәселелер ретінде қарастыруға болады.

Малайзия мемлекетінің өкілдері Нисрина Абиада мен Фарханд Зия Мансурдың материалдарында айтылғандай, мұсылман және мұсылман емес болсын, жалпы алғанда әлемдегі барлық елдерде балаларды қорғау саласында

әлі де көптеген олқылықтар бар [22]. Балаларға қатысты қылмыстың қатты қарқынмен дамуын қарастыра отырып, ол жәбірленуші немесе қылмыскер ретінде болсын, балалардың құқық бұзушылықтары мен қылмыстық жауапкершілігі мәселелері ықпал ететін факторларды зерттеумен бірге қайта қаралуы мүмкін. Мүмкін, ислам құқығының кәмелетке толу жасын анықтауға арналған жалпы басшылығы баланың қабілеттілігі мен жетілуіне байланысты қылмыстық жауапкершілік мәселесін шешуді қамтамасыз ете алады. Баланы тәрбиелеу үшін бүкіл құзырлы органдар мен тұлғалардың қажырлы еңбегі қажет.

Алдын алу емдеуден гөрі жақсы болғандықтан, отбасылық институттар мен қоғам мүшелері балаларды «нақты әлемге» бағыттап, қолдауы керек, өйткені «Киберәлемдегі» бейтаныс адамдар баланың интернеттегі құқық бұзушылықтарына байланысты оның болашағына үлкен қауіп төндіруі мүмкін. Заң Интернетте ғана емес, нақты әлемде де құқық бұзушылықтар жасауға бейім осал балаларға жәрдемдесу және бейімделу құралы ретінде қарастырылады. Заңсыз әрекеттер, әсіресе әлеуметтік медиа сайттарында жиі кездесетіндіктен, балаларымызды құрметтеп, цифрлық азаматтықты қалыптастыру үшін онлайн байланыста таратылуы керек әдеп, этика және мораль сияқты жұмсақ дағдыларды үйрету маңызды; жауапкершілік мәдениеті онлайн және балалар мен жастарға таңдау, бақылау және қорғау жүйесі жұмыс істеп тұрған кезде медиа контент пен қызметтердің кең ауқымын бағалау, бағдарлау және құру мүмкіндігін беру. Тұтастай алғанда, Үкімет пен қоғамдастық, атап айтқанда ата-аналар мен мұғалімдер мен полиция саясат пен тиісті ережелердің балаларды қорғаудың ғана емес, сонымен бірге олардың ел азаматтары ретіндегі мүмкіндіктерін кеңейтудің тетігін қамтамасыз етуде маңызды рөл атқаруға арналған, бұған құқықтық сауаттылықты насихаттау және балаларды өздеріне үлкен жауапкершілікке тәрбиелеу арқылы қол жеткізуге болады, сондай - ақ заң мен адамгершілікті құрметтеу де басты алғышарттардың тізбегіне енгізілу қажет.

Пайдаланған әдебиеттер тізімі

1. Harmut von Henting, as quoted by Crofts, T. _Doli Incapax: Why Children Deserve Its Protection‘. Murdoch University Electronic Journal of Law, available at http://www.murdoch.edu.au/elaw/issues/v10n3/crofts103nf.html.
2. Sjöberg, U. (1999). The rise of the electronic individual: A study of how young Swedish teenagers use and perceive Internet. Telematics and Informatics, 16(3), 113–133.
3. Bainham, A. (1998). Changing families and changing conceptsreforming the language of family law. Child & Fam. LQ, 10, 1.
4. Bandalli, S. (1998). _Abolition of the Presumption of Doli Incapax and the Criminalisation of Children‘, The Howard Journal, Vol 37, No, 2, May 1998.
5. Sherry Turkle, (1995), _Life on the Screen: Identity in the Age of the Internet‘, Touchstone Edition, New York.

6. Turkle, S. (2001). Foreword: All MOOs are Educational—the Experience of" Walking through the Self. High wired: On the design, use, and theory of education MOOs.

7. English Oxford living Dictionary, 2017 see https://en.oxforddictionaries.com.

8. Nasimah Hussin, (2007), Juvenile Delinquency in Malaysia: Legal Framework and Prospects for Reforms, IIUM Law Journal, 15(2).

9. United States Office of Juvenile Justice and Delinquency Prevention (OJJDP) see: https://www.ojjdp.gov.

10. Child Act 2001 (Amendment 2016).

11. Snyder, H. N., Espiritu, R. C., Huizinga, D., Loeber, R., & Petechuk, D. (2003). Prevalence and development of child delinquency. Child delinquency bulletin series, March 2003.

12. Loeber, R., Farrington, D. P., & Petechuk, D. (2003). Child delinquency: Early intervention and prevention. Washington, DC: US Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention.

13. Flowers, R. B. (1986). _Children and criminality: The child as victim and perpetrator‘ (Vol. 13). Greenwood Publishing Group.

14. Azlina@Roszy AG, _Gajet@Gen α,‘ paper presented at Simposium Penyelidikan dan Meja Bulat, Putrajaya, May, 17, 2017.

15. Fionda, J. (1999). Crime and Disorder Act 1998: New labour, old hat: Youth justice and the Crime and Disorder Act 1998. Criminal Law Review, (Jan), 36-47.

16. Utusan Borneo (Sabah). 23 Nov 2016, "Awasi Anak Untuk Elak Jadi Mangsa Pelaku Jenayah Seks'; Sinar 10 October 2016.‖Kanakkanak Jadi Hamba Seks Kenalan WeChat".

17. Stalans, L. J., & Finn, M. A. (2016). Understanding How the Internet Facilitates Crime and Deviance. 11.

18. Hsieh, M.L, Mc Shanes, MD and Williams, MF (2016) _Juveniles in Cyberspace Issues in Enforcement and Parental Control in Understanding Juvenile Justice and Delinquency‘, McShane, and Cavanaugh, M (eds) USA: Praeger.

19. Lu, Tian, et, al (2016) _Psycological factors lead to Delinquency Intention on Online Peer-to-Peer Landing Platform, A Survey Evidence‘, PACIS 2016 Proceedings.191. Available at http://aisel.aisnet.org/pacis2016/191 Lu Tian.

20. J. Bishop, (2014) _Digital teens and the _Antisocial Network‘: Prevalance of troublesome Online Youth Groups and Internet trolling in Great Britain‘ 5(3) International Journal of E-Politics.

21. Navarro, J. N., Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2016). Addicted to the Thrill of the Virtual Hunt: Examining the Effects of Internet Addiction on the Cyberstalking Behaviors of Juveniles. Deviant Behavior, 37(8), 893-903.

22. Nisrine Abiad and Farkhanda Zia Mansoor (2010) _Criminal Law & the Rights of the Child in Muslim States‘. British Institute of International Comparative Law: London.

Маликова Наталия Валерьевна,
доцент кафедры уголовного процесса
к.ю.н., доцент, e-mail: natali-malikova@yandex.ru

Арсланова Альбина Ринатовна,
доцент кафедры уголовного процесса
к.ю.н., e-mail: alya.arslanova@inbox.ru

(Уфимский юридический институт МВД России, Российская Федерация)

ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Аннотация. В статье рассматривается способ совершения преступления в электронных или информационно-телекоммуникационных сетях как системообразующий фактор в сфере формировании принципиально новых критериев построения криминалистической методики расследования преступлений.

Ключевые слова: информационно-телекоммуникационные сети, Интернет, методика, способ совершения преступления, электронно-информационное пространство.

THE USE OF THE INTERNET AND INFORMATION TECHNOLOGY AS A WAY OF COMMITTING CRIMES

Annotation. The article considers the method of committing a crime in electronic or information and telecommunication networks as a backbone factor in the formation of fundamentally new criteria for constructing a forensic methodology for investigating crimes.

Key words: information and telecommunication networks, Internet, methodology, method of committing a crime, electronic information space.

Исследование общего фона развития преступности в Российской Федерации проходит на основании статистических данных федеральных органов исполнительной власти и сформированных на их основе итоговых отчётов о состоянии преступности как за конкретный промежуток времени, так и за несколько лет. Так, из итогового отчета МВД России по состоянию преступности за период январь-июнь 2023 год, отмечается, что за данный отчетный период число преступлений, совершенных с использованием информационно-телекоммуникационных технологий возросло на 27,9 % [1].

Многообразие способов совершения рассматриваемых преступлений также имеет тенденцию к увеличению, объектом их преступного посягательства, могут быть широкого спектра общественные отношения. Кроме того, субъектами преступления и потерпевшими могут становиться самые разные категории социальных слоев населения. Вместе с тем элементом, объединяющим все эти деяния, является способ их совершения. Он обусловлен тем, что преступления

могут совершаться в информационно-телекоммуникационных сетях (включая сеть Интернет). Что в общем своем виде позволяет указать на ряд важных аспектов, одинаково характеризующих указанные преступления и в итоге говорить о том, что их алгоритм расследования во многом совпадает. К ним относятся: 1) отсутствие непосредственного физического контакта (взаимодействия) субъекта деяния с потерпевшим или предметом преступного посягательства в связи с удаленным характером совершения преступления; 2) возможность действовать обезличено или под различными ник-неймами преступника, что так же обеспечивается действиями в сети.

Системообразующий фактор, а именно – совершение преступления в электронных или информационно-телекоммуникационных сетях позволяет с научной точки зрения говорить о формировании принципиально новых критериев построения криминалистической методики расследования преступлений.

Это не означает, что сложившееся к настоящему времени понимание криминалистической методики становится не актуальным. Наоборот, в построении криминалистической методики, не отвергая сложившиеся положения, технические аспекты сети, только лишь являются причиной для формирования новых подходов дел.

Знания об особенностях работы сети, и оставления в ней следов, могут позволить квалифицированно подходить к раскрытию и расследованию конкретного преступления, вне зависимости от подследственности и объекта преступного посягательства

Для того, чтобы иметь представление о формировании не только комплекса электронных следов, но и об алгоритме по индивидуализации субъекта преступления, личность которого сокрыта техническими свойствами сетей необходимо обратить внимание на порядок доступа в сеть Интернет, оставляемые при этом электронные следы и раскрыть основные понятия, необходимые для понимания механизма преступлений.

Доступ в сеть Интернет как правило осуществляется:

1) посредством услуг субъектов предпринимательской деятельности (провайдер), оказывающих услуги передачи информации через сети электросвязи;

2) посредством услуг операторов сотовой связи.

Алгоритм доступа в сеть Интернет одинаков как для преступника, так и для законопослушного гражданина. При подключении через провайдера или через ОСС, формируется запрос на сервер указанных поставщиков услуг. Сервер на этот запрос выделяет IP-адрес (код технического устройства в сети) и этот адрес закрепляется за MAC-адресом конкретного технического устройства, через который и осуществляется доступ в сеть. Для понимания, раскроем ряд понятий:

1) MAC-адрес (Media Access Control – управление доступом к среде) – уникальный идентификатор, присваиваемый производителем оборудованию, оснащенному сетевой картой. Этот номер используется для идентификации устройства в сети. Стоит учитывать, что несмотря на привязку MAC-адреса к физическому местоположению технического устройства с которого производится доступ в сеть Интернет, это не следует считать неоспоримым доказатель-

ством виновности лица, пользующегося соответствующим роутером, смартфоном или компьютером (ноутбуком, нетбуком, планшетом). Это связано с тем, что преступник может продать, подарить, выкинуть техническое устройство и в дальнейшем его будет использовать другое лицо;

2) IP-адрес (Internet protocol address – адрес Интернет-протокола) – уникальный код компьютера в сети Интернет. Он автоматически назначается клиенту провайдером или ОСС, состоит из четырех десятичных чисел со значениями от 0 до 255, разделенных точками (xxx.xxx.xxx.xxx, например 123.122.12.74). Начало адреса определяет сеть, в которой расположен адресуемый компьютер, а крайний правый блок – роутер, компьютер и т.д. в этой сети.

Таким образом, предлагаемая методика основывается не только на закономерностях совершения какого-либо конкретного преступления, позволяющего выявить типы преступников, типичные версии, но и на технических особенностях обращения компьютерной информации, взаимодействия в сети электронных носителей и закономерностях фиксации следов деяния вне зависимости от вида преступления, личности преступника, потерпевшего и причин совершения деяния. И причиной этого является то, что механизм преступления в основной своей части протекает не в реальном мире, а в виртуальном. Естественно, запускает этот механизм человек в реальном мире, но сама процедура, приводящая к последствиям реализуется в электронно-информационном пространстве.

Список использованной литературы

1. Краткая характеристика состояния преступности в Российской Федерации за январь - июнь 2023 года): [сайт]. URL:https:// https://xn--b1aew.xn--p1ai/reports/item/40116049/ (дата обращения: 21.10.2023 года).

Момбеков Бекнур Бауржанович,
магистрант факультета послевузовского образования
подполковник полиции, e-mail: bekabm_777@bk.ru
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

НЕЗАКОННЫЙ ОБОРОТ НАРКОТИКОВ В СЕТИ ИНТЕРНЕТ

Аннотация. Научная статья посвящена одной из актуальнейших проблем современности – наркотикам. От пагубного влияния, которых страдает уже не одно поколение слабовольных личностей. Несмотря на то, что повсеместная цифровизация и использование Интернета имеют множество преимуществ, важно отметить, что преступники воспользовались этими достижениями для расширения сети распространения наркотиков. Это говорит о том, что борьба с подобными негативными социальными проявлениями становится еще более актуальной и сложной.

Ключевые слова: противодействие, наркотики, Интернет, правоохранительная деятельность, цифровизация.

DRUG TRAFFICKING ON THE INTERNET

Annotation. The scientific article is devoted to one of the most urgent problems of our time – drugs. More than one generation of weak-willed individuals suffers from the harmful effects of drugs. Despite the fact that ubiquitous digitalization and the use of the Internet have many advantages, it is important to note that criminals have taken advantage of these achievements to expand the network of drug distribution. This suggests that the fight against such negative social manifestations is becoming even more urgent and complex.

Keywords: counteraction, drugs, Internet, law enforcement, digitalization.

Интернет играет большую роль в жизни современного общества. В контексте современного общества, Интернет превратился в ключевой элемент повседневной жизни, оказывая глубокое воздействие на различные сферы человеческой деятельности. Однако, следует подчеркнуть, что несмотря на свою значимость, он стал источником неоднозначных явлений, в частности, в сфере соблюдения законности. На сегодняшний день, одной из актуальных проблем, связанных с деятельностью интернет-пользователей, является незаконное распространение наркотических средств, психотропных веществ и их аналогов.

Экспансия интернета стала основой для глобальной трансформации коммуникации и информационного обмена. Вмешательство сети в различные сферы повседневной жизни отразилось на характере преступной деятельности, в том числе и в области незаконной торговли наркотиками. Нарушители законов вследствие высокой степени анонимности и обширного охвата Интернета могут проводить свои операции как на национальном, так и на международном уровне, что создает сложности для правоохранительных органов [1, с. 118].

Эксплуатация сети для распространения наркотических средств и психотропных веществ требует всестороннего анализа. Важно изучить механизмы, через которые осуществляется эта незаконная торговля, а также выявить особенности, которые делают ее более устойчивой и трудноразграничимой для пресечения. Неотъемлемой частью научного исследования является оценка влияния подобных преступных действий на общество и здоровье граждан. Взаимосвязь между распространением наркотиков через Интернет и общественным здоровьем требует глубокого анализа данных и статистических показателей. Результаты подобных исследований могут выступить основой для разработки эффективных стратегий противодействия данному явлению.

Раскрывая многогранность проблемы распространения наркотиков через Интернет, следует отметить, что существует множество ухищрений, которые преступные элементы используют для достижения своих целей в этой области. Рассмотрим разнообразные методы распространения наркотических веществ, в которых злоумышленники активно применяют современные технологии и ресурсы виртуальной среды [2, с. 552].

Первым и, возможно, наиболее широко используемым методом является пользование популярными социальными сетями. Интерактивность и массовость таких платформ предоставляют возможность незаконным дистрибьюто-

рам наркотиков скрыть свою деятельность среди многочисленных пользователей, создавая видимость обыденности и нормальности. Это особенно опасно, учитывая, что в данной среде активными пользователями являются и дети, и подростки, находящиеся в группе риска в силу их уязвимости и недостаточного опыта в сфере оценки подобных рисков.

Приватные веб-сайты и виртуальные магазины также представляют собой эффективные инструменты для распространения наркотиков. Здесь преступники могут действовать в условиях повышенной анонимности, продают наркотические вещества под прикрытием легальных товаров, искусно маскируя свою деятельность. Этот метод обеспечивает тщательную утайку и обход законодательных ограничений, что увеличивает сложность борьбы с незаконной торговлей.

Особое внимание следует уделить тому факту, что дети и подростки активно участвуют в интернет-пространстве, и они являются целевой аудиторией для преступных схем распространения наркотиков. Злоупотребление информацией о положительных эффектах наркотиков и навязывание идеи «легальных порошков» представляет собой серьезную угрозу для формирования и стабильности ментального состояния молодежи. Более того, возможность приобретения психотропных и наркотических средств в интернете сопровождается аспектом доступности и недороговизны, что может создавать дополнительные стимулы для молодежи в поиске подобных средств.

Наверняка найдется не так много людей, которые бы не слышали о вреде употребления наркотиков. И большинство подростков до определенного возраста пребывают в твердой уверенности, что наркомания – это плохо, наркотики разрушают жизнь, а потому принимать их (и даже просто пробовать) нельзя. Так происходит до тех пор, пока подросток не попадает в компанию, где ему предлагают попробовать «легкие» наркотики. Мнимые друзья подначивают, насмехаясь, но одновременно уверяя, что никакого вреда синтетические наркотики организму не приносят – только удовольствие. Не желая отставать от товарищей, подросток делает первый шаг и зачастую уже не может остановиться.

В контексте рассмотрения наркотиков, охватывающего широкий спектр веществ, способных оказывать воздействие на нервную систему и вызывать привыкание, оказывается целесообразным подчеркнуть, что данный термин охватывает различные химические соединения. Тем не менее, в современном дискурсе наркотики, в первую очередь, ассоциируются с теми веществами, которые обладают высокой активностью воздействия на центральную нервную систему, влекущую за собой развитие сильной физической или психологической зависимости [3, с. 39].

Из вышесказанного следует выделить категорию синтетических наркотиков, представляющих собой относительно новое исследование в области химических веществ, созданных искусственным путем. Особенно актуальным в данном контексте является отмеченное воздействие этих веществ на мозговую деятельность, что влечет за собой возникновение значительной степени зависимости. Значимость синтетических наркотиков заключается в их способности по-

ражать центральную нервную систему с необыкновенной силой, предоставляя плачевные перспективы для здоровья людей.

Отметим, что сравнение воздействия синтетических наркотиков с традиционными наркотическими веществами, такими как героин, позволяет выделить угрозу, исходящую от последних. Несмотря на широкую известность и распространенность героина, синтетические наркотики, обладая более выраженной активностью, представляют собой более опасный аспект в плане здоровья человека. Подчеркивается, что данная опасность превосходит те, которые связаны с употреблением героина и подобных веществ, требуя тщательного научного исследования для полноценного понимания масштабов угрозы.

При рассмотрении данной проблемы выделяются несколько ключевых аспектов, воздействующих на эффективность противодействия этому виду преступности.

В первую очередь, следует обратить внимание на проблему скрытности и анонимности участников наркокартелей и других преступных группировок. Данные аспекты создают серьезные трудности для правоохранительных органов, снижая возможности выявления и пресечения противоправных деяний. Необходимость разработки и внедрения технологических решений для преодоления анонимности становится одним из важных направлений в борьбе с наркотической преступностью.

Второй важный аспект заключается в технических сложностях, требующих специализированных знаний. Современные технологии, такие как криптовалюты и защищенные каналы связи, используются наркокартелями для уклонения от преследования. Развитие компетенций в области кибербезопасности и киберкриминалистики становится важным элементом в противостоянии техническим аспектам наркотической преступности.

Третий аспект касается необходимости международного сотрудничества. Преступные сети действуют глобально, и успешная борьба с ними требует координации усилий между различными странами. Развитие механизмов международного сотрудничества и обмена информацией становится неотъемлемой частью стратегии борьбы с наркотической преступностью.

Четвертый аспект связан со сбором и анализом данных. В контексте наркотической преступности эффективный анализ больших объемов информации становится критическим для выявления связей и паттернов в деятельности преступных организаций. Развитие методов анализа данных и использование современных технологий обработки информации способствует улучшению результатов в этой области.

Наконец, не следует пренебрегать юридическими аспектами и вопросами этики и конфиденциальности, которые возникают в рамках правоохранительной деятельности. Разработка баланса между необходимостью борьбы с преступностью и соблюдением прав и свобод граждан представляет собой сложную задачу, требующую внимательного рассмотрения и проработки [4, с. 9].

В контексте скрытности и анонимности участников незаконного оборота наркотических средств, существует неотложная необходимость в разработке и внедрении передовых технологий и методов идентификации. Данные инстру-

менты должны обеспечивать высокий уровень приватности для законопослушных граждан, сохраняя при этом эффективность действий правоохранительных органов. Развитие криптографических технологий и алгоритмов, способных обеспечить баланс между конфиденциальностью и безопасностью, представляется приоритетным направлением исследований.

Обобщая вышеизложенное, можно заключить, что проблема распространения наркотиков через Интернет является сложным социальным и технологическим явлением. Ее решение требует комплексного исследования, включающего в себя анализ технических механизмов, социальных взаимосвязей и психологических аспектов. Развитие эффективных стратегий противодействия данному явлению необходимо основывать на глубоком понимании всех перечисленных факторов и их влияния на современное общество, особенно на молодое поколение.

Список использованной литературы

1. Бряндина А.С. Криминологические аспекты распространения наркотиков в сети Интернет // В мире научных открытий. – 2009. – № 1 (1). –С. 116–119.

2. Токманцев Д.В., Пахорукова Ю.Е. Состав сбыта наркотиков с использованием сети интернет: проблемы конструкции и пути совершенствования // Современные научные исследования и инновации. – 2016. – № 3 (59). – С. 551–553.

3. Битов А.А. сравнительный анализ некоторых средств противодействия раскрытию преступлений в сфере незаконного оборота наркотиков, совершаемых с использованием сети Интернет // Пробелы в российском законодательстве. – 2023. – Т. 16. – № 4. – С. 38–41.

4. Волкова О.В., Дроздова Е.А., Высоцкий В.Л. Оперативно-разыскное обеспечение противодействия преступности, связанной с незаконным сбытом наркотиков бесконтактным способом // Наркоконтроль. – 2022. – № 3. – С. 7–10.

Мукатаев Талгат Маратович,
старший научный сотрудник Межведомственного научно-исследовательского института, советник юстиции, 7171140@prokuror.kz.
(Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан)

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ВОЗМОЖНОСТИ ЕГО ПРИМЕНЕНИЯ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация. Статья подготовлена по результатам внутреннего анализа сотрудника Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан. В статье описано определение искусственному интеллекту, наиболее доступному к пониманию для не IT-специалистов. Приведены примеры прогрес-

сивного применения в зарубежных странах, возможностях использования ИИ в уголовном процессе и охране общественного порядка.

Ключевые слов: внутренний анализ, искусственный интеллект, уголовный процесс, правоохранительная деятельность, правопорядок.

ARTIFIKAL INTELLIGENCE AND THE POSSIBILITIES OF ITS APPLICATION IN LAW ENFORCEMENT

Abstract. The article is prepared on the basis of the results of internal analysis of the employee of the Interdepartmental research institute of the Academy of law enforcement agencies at the Prosecutor General's Office of the Republic of Kazakhstan. The article describes the definition of artificial intelligence, the most accessible to understanding for non-IT specialists. Examples of progressive use in foreign countries, the possibilities of using AI in criminal proceedings and the protection of public order are given.

Keywords: internal analysis, artificial intelligence, criminal proceedings, law enforcement, law and order.

Интеллектуальные системы уже продолжительное время сопровождают нас во многих сферах жизнедеятельности и их сосуществование с человеком для многих развитых стран стало обыденностью и ключевым технологическим трендом, фактически дав начало четвертой промышленной революции. В качестве эффективного инструмента повышения уровня технологического прогресса получает развитие искусственный интеллект (далее – ИИ), дающий прорыв в науке, космонавтике, военной промышленности, в политике и в других областях жизнедеятельности.

Одновременно ИИ в научном мире вызывает как интерес – в возможностях повышения эффективности в различных сферах деятельности, так и опасения – в виде угрозы по вытеснению человека с рынка труда и его порабощению будущими разработками из-за потери контроля над ИИ, которые возникают не только у ученых, но и у руководителей государств.

Информация о сферах применения и правовом регулировании ИИ достаточно широко освещается в средствах массовой информации, проводятся международные форумы, конференции и т.д., многие так или иначе уже встречались с ними.

Вместе с тем, при всеобщем обсуждении об ИИ не все понимают что он из себя представляет.

Понятие «Искусственный интеллект» относится к передовому машинному интеллекту и не имеет сегодня общепринятого международного определения, но встречающиеся варианты схожи. В науке отсутствие общей дефиниции объясняется различными существующими подходами к установлению его сущностных характеристик.

Сам ИИ позиционирует себя как машину способную воспринимать окружающую среду и реагировать на нее самостоятельно, с выполнением решений подобно человеку без вмешательство самого человека.

Для более точного и верного восприятия определения ИИ полагаем правильным объяснить – что это такое. Для этого выбран наиболее доступный к пониманию для не IT-специалистов пример.

ИИ моделирует человеческий интеллект, но только в IT-технологиях с установленными программами по выполнению задач, решение которых требуют человеческого интеллекта.

ИИ можно характеризовать как систему алгоритмов, позволяющих компьютеру обрабатывать большое количество информации.

Разработчик в своих алгоритмах задает пошаговые последовательные действия (сложения, умножения, деления, вычитания и т.д.), позволяющие внесение изменений и приводящие к правильному результату.

При этом ИИ используются нейросети, способные выполнять целый набор различных сложных задач.

Нейросети в свою очередь представляют вид машинного обучения, имитирующую (схожую) работу человеческого мозга, с заранее большим количеством разрешенных задач и работают посредством системы соединенных и взаимодействующих между собой простых блоков математических операций, моделирующих искусственные нейроны.

Принято считать, что такие сети не программируются, а обучаются.

Нейросеть разгадывает ожидающий от нее результат, с помощью отдельного алгоритма, указывающего на правильность решения. В ходе обучения у нейросети формируются свои пути к правильному решению.

При неправильном решении алгоритмы указывают на ошибочность вывода. Вместе с тем необходимо отметить, что и сам разработчик не всегда может понять принцип решения, т.к. нейросеть сама образует свои связи в принятии заключения.

Таким образом, алгоритм приходит к выводу через последовательность заданных разработчиком шагов, нейросеть же выбирает ожидаемый от нее ответ по своим, не поддающегося на сегодняшний день изучению человеком принципам.

Сама нейросеть не может видеть, она считывает поступившие числа и формирует итоговые, также числа. На выходе результаты вырабатываются, но никак не посредством понятного для человека мышления.

Необходимо учитывать, что нейросети работают лишь посредством работы алгоритмом заданных человеком, при этом она не может думать подобно человеческому мышлению, искусственное сознание здесь отсутствует.

Вопросы сфер применения и разработки законодательных норм достаточно освещаются в СМИ, но не наблюдается широкого применения ИИ в уголовном процессе. В этой связи хотелось бы сегодня немного акцентировать внимание на возможности применения ИИ уголовно-правовой сфере.

Среди технологий с использованием ИИ, есть алгоритмы, нацеленные на обнаружение подозрительных или украденных транспортных средств; программы машинного распознавания образов; использование программ распознавания голосов; программы контент- и латентно-семантического анализа, делающие возможным на основе содержательного исследования письменных или

аудиотекстов устанавливать психологическое состояние их автора, а также скрытые смыслы, заложенные в сообщении; сбор, хранение и интеллектуальный анализ информации с целью превентивного выявления даже слабых сигналов, указывающих на всплеск уличной преступности, неконтролируемых волнений, беспорядков и актов вандализма; биометрические методы, позволяющих обнаруживать подозрительное поведение по микромоторике мускулов лица, движению тела; автоматизированный комплекс поиска и анализа контента детской порнографии в Сети; интеллектуальные программы, помогающие выявлять аномалии при проведении финансовых транзакций; камеры с ИИ для прогнозирования преступлений.

При этом, задачей сегодняшнего дня является возможность использования ИИ при расследовании.

Д.В. Бахтеевым описано, что «деятельность следователя, в свою очередь, может быть представлена в качестве нелинейного комплекса операций по решению задач раскрытия и расследования преступлений, характеризующегося динамичностью и претерпевающего воздействие случайных и псевдослучайных факторов, которые затрудняют быстрое и эффективное познание обстоятельств, составляющих предмет доказывания [1, с. 44]. Соответственно актуален вопрос создания программных комплексов, чьи возможности сложной эвристической (использование опыта и практических навыков в процессе принятия решения) обработки информации максимально приближены к возможностям криминалистического мышления следователя.

Для целей правовых отраслей знания, в том числе криминалистики, искусственные нейронные сети можно рассматривать как программные или аппаратные комплексы простых обработчиков данных, способные обмениваться друг с другом сигналами и при достаточно развитой структуре и настроенной логике взаимодействия решать сложные задачи. Специфику искусственных нейронных сетей обусловливают простота каждого их элемента (искусственного нейрона), их взаимозаменяемость и взаимосвязь. Каждый кластер информации, загружаемый в сеть, сопоставляется с другими кластерами, на основе чего генерируется решение задачи. Рабочая искусственная сеть может содержать десятки и сотни слоев (уровней оценки и проверки), обеспечивающих комплексное рассмотрение любых факторов, что позволяет решать крайне сложные задачи, в том числе по раскрытию и расследованию преступлений.

Основным качеством искусственных нейронных сетей, выгодно отличающим их от большинства более привычных программных комплексов, является их способность к адаптивному ситуационному обучению. Это выражается в том, что создатель сети задает общие правила анализа данных и предоставляет данные для обучения. Последние должны быть непротиворечивыми и предельно достоверно отображать характеристики анализируемого процесса или явления.

К таким данным можно отнести сведения о раскрытых и нераскрытых преступлениях, механизме и обстановке их совершения, наличию и характеристике связей между преступником и потерпевшим и т.д.

Работа искусственной нейронной сети основана на интеллектуальном эвристическом анализе данных, который гораздо более эффективен, чем методы математической статистики, используемые в большинстве криминалистических программных комплексов. В этом отношении искусственные нейронные сети гораздо ближе к человеческому мозгу, поскольку способны выявлять скрытые, неочевидные связи и закономерности подобно тому, как талантливый следователь может связать в единую картину разрозненные обстоятельства совершения преступления, известные следствию.

Следующее качество искусственных нейронных сетей, закономерно вытекающее из предыдущего, заключается в их устойчивости к информационным шумам, в том числе дезинформации, за счет комплекса эвристических операций по обработке загружаемых сведений. Этим же фактором обусловлено низкое число ошибок и его дальнейшее снижение по мере наращивания информации в сети (обучения) и уточнения алгоритмов обучения и извлечения данных.

Обучаемость может рассматриваться одновременно как достоинство и недостаток искусственных нейронных сетей. Преимущество заключается, как уже было сказано, в поступательном снижении числа ошибок и накапливании сетью «опыта» решения разнообразных задач. Однако оборотной стороной медали выступают низкая скорость обучения и необходимость загрузки в сеть большого объема информации.

Для создания подобной системы «должна быть проведена значительная работа по обработке материалов уголовных дел по отдельным видам преступлений с целью их анализа и выделения исходной информации, включающей: обстановку совершения преступления, способ совершения преступления, типовые следы, обстоятельства, подлежащие установлению, информацию о личности потерпевшего и преступника». Информация, загружаемая в сеть, должна быть проверенной и внутренне непротиворечивой.

Кроме того, необходима тщательная разработка системы приоритетов (весов), согласно которым искусственная нейронная сеть будет осуществлять моделирование и оценку разнообразных вариантов решения поставленных задач. Для определения направления поиска разумным представляется использование математического аппарата Байесовского поиска, позволяющего рассчитывать множество переменных и их зависимостей, к примеру, вероятность правдивости отдельных показаний в зависимости от сложившейся следственной ситуации и других показаний, имеющихся в деле.

Процесс создания искусственной нейронной сети состоит из ряда этапов.

На первом этапе происходят сбор и обобщение данных, которые впоследствии будут использованы для обучения сети. При этом необходимо загружать данные в сеть таким образом, чтобы несвязанные кластеры информации нельзя было перепутать. В частности, искусственная нейронная сеть в процессе обучения должна четко различать орудие непосредственного совершения преступления (например, при убийстве – нож) и средство обеспечения совершения преступления (например, веревка, с помощью которой ограничивалось сопротивление потерпевшего). В противном случае возможна неверная интерпретация данных и, как следствие, ошибка при анализе ситуации.

Значительные сложности могут возникнуть именно на этом этапе, поскольку для создания достаточного массива данных требуются анализ и трансформация в цифровую форму предельно детализированных материалов по сотням (а желательно тысячам и десяткам тысяч) схожих уголовных дел, что к настоящему времени является трудновыполнимой, хотя и решаемой задачей.

На втором этапе осуществляется выбор топологии (внутренней архитектуры) искусственной нейронной сети и подбор параметров обучения; формируется «скрытый слой». К примеру, сеть, ориентированная на поиск признаков серийности или объединение разнородных эпизодов преступления, должна содержать правила синтеза или дифференциации информационных кластеров. Также сеть может быть настроена либо на постоянное обновление алгоритмов обучения путем вмешательства оператора сети (разработчика), либо на самостоятельное развитие по заранее заданным параметрам. В основе «скрытого слоя» искусственной нейронной сети, обученной или обучаемой решать криминалистические задачи, должны быть учтены основные методы криминалистического мышления: как чисто логические (анализ, синтез, традукция, индукция и т.д.), так и психологические и эвристические (сомнение, уверенность и пр.).

На третьем, заключительном, этапе подготовки искусственной нейронной сети происходит непосредственно обучение, за которым следует проверка его адекватности, т.е. соответствия целям создания сети. Проверка должна основываться на примерах, не включенных в массив для обучения, поскольку работоспособность искусственной нейронной сети можно оценить только в «полевых» условиях.

Проведенный анализ показал, что возможности искусственных нейронных сетей могут быть реализованы в следующих частных и общих направлениях уголовного процесса:

1. Оценка исходной информации по уголовному делу в целях выдвижения простых и комплексных следственных версий, определения направлений их проверки.

2. Моделирование события преступления и его следовой картины на основе неполных данных и предшествующего «опыта», охватывающего большой массив уголовных дел.

3. Выявление признаков серийности в условиях информационной недостаточности и предложение вариантов действий следователя по проверке перспективных следственных версий.

4. Увеличение эффективности почерковедческих и габитоскопических исследований: к настоящему времени наиболее перспективным направлением развития искусственных нейронных сетей считается распознавание образов, что может позволить, к примеру, автоматизацию выявления признаков подлога документов.

5. Поиск недоступных криминалистическому программному обеспечению компьютерных файлов, сокрытых, например, при помощи стеганографии или альтернативных потоков данных (ADS) (Harris 2007), установление первичного источника информации в сети Интернет.

6. Дополнительная оценка достаточности собранных доказательств для предъявления обвинения.

7. Прогнозирование совершения преступления в будущем, на основе анализа признаков совершенных преступлений с точки зрения их локализации, социальных характеристик участвующих лиц, средств массовой информации (Norton 2013).

8. Стратегическое планирование, к примеру построение логических моделей, отражающих: вероятность развития оперативной обстановки в каком-либо регионе, на территории отдельной страны или ряда государств; возможность проявления активности крупных организованных криминальных структур, в том числе международных, террористических и др.; перспективы возникновения новых каналов незаконной поставки наркотиков, оружия, иных объектов, изъятых из гражданского оборота; новых потоков незаконной миграции.

Р.С. Белкин подчеркивает, что «рядовой следователь без обширного профессионального опыта, в условиях дефицита времени и экстремальной ситуации не в состоянии воспроизвести в памяти десятки страниц книжной методики в качестве оперативного руководства к действиям». Он предлагает разработать лаконичные, четкие и ясные алгоритмы действий следователя, их варианты для выбора в зависимости от следственной ситуации.

Представляется, что ИИ, по сути, и сам может выступить важным помощником следователя.

Однако любые типы ИИ, которые могут быть использованы при раскрытии и расследовании преступлений, должны быть апробированы, а сама возможность их применения – закреплена в уголовно-процессуальном законодательстве.

Искусственные нейронные сети могут быть адаптированы для решения специфических криминалистических задач, например анализа материалов уголовных дел для выявления следственных ошибок процессуального и тактического характера, вычленения из массива расследуемых дел признаков серийности, объединения преступлений по схожим признакам. В ближайшем будущем вполне возможна интеграция рассмотренной технологии в криминалистическую практику, однако для этого требуется дальнейшее изучение архитектуры и возможностей искусственных нейронных сетей, в том числе учеными-криминалистами» [1, с. 47].

Мы понимаем, что разработчиками и потребителями движет живой человеческий интерес к новым технологиям, быстрый результат, надежда на то, что ученые создадут системы (ноу-хау) раскрывающие горизонты будущего. При этом все также понимают о возможности непрогнозируемых последствий, в т.ч. использование ИИ с нарушением прав человека, которое уже «излучает» ИИ.

В Казахстане разработка регуляторных норм в сфере реализации инновационных проектов, в т.ч. ИИ уже начата.

На сегодняшний день анализ показывает, что при наличии прорывных проектов развития ИИ не изучена его природа, правовые и этические аспекты (в т.ч. правосубъектность ИИ), не дано четкого юридического определения ИИ.

Между тем на необходимость выработки норм регулирующих применение ИИ все чаще обращают внимание. На октябрь-ноябрь месяцы 2023 года порядка 120 стран приняли индивидуальные (внутри страны) законодательные акты, а также попытки международного регулирования в этой области – первым были приняты в январе 2017 года (США) «Азиломарские принципы ИИ».

Таким образом сегодня отсутствует консолидированная международная правовая позиция, национальные правовые нормы по возможности принятия результатов работы той или иной системы ИИ не только в качестве доказательств в уголовном процессе, (разработанной для использования в уголовно-правовой сфере, автономной, либо гибридной - с участием человека), но и в целом в промышленном масштабе в различных областях жизнедеятельности.

Данная работа подразумевает необходимость дальнейшего исследования возможностей ИИ экспертами в этом направлении деятельности, разработку машинных систем, не совершающих недопустимые ошибки, разработку общих правовых норм по использованию ИИ, в т.ч. ответственность разработчика за возможный вред, причиненный при его использовании.

Следующий этап правовой работы – внесение соответствующих изменений в отраслевые законы (уголовно-процессуальное, гражданско-процессуальное, о национальной безопасности и т.д.).

Необходимость проведения данных работ в уголовно-правовой сфере продиктована тем, что принятие решений системами ИИ в рамках, к примеру, только досудебного производства и в суде, предусматривает прямые последствия, затрагивающие установленные Конституцией права и свободы граждан.

Список использованной литературы

1. Бахтеев Д.В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Российское право: образование, практика, наука. – 2018. – № 2. – С. 43–49.

Мясникова Татьяна Васильевна,
преподаватель кафедры криминологии и уголовно-исполнительного права
e-mail: mtv24.01@mail.ru
(Уральский юридический институт МВД России, Российская Федерация)

ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ В КИБЕРПРОСТРАНСТВЕ

Аннотация. В настоящей статье рассматриваются вопросы о состоянии организованной киберпреступности на современном этапе развития общества. Проводится анализ причин и условий, влияющих на увеличение количества данного вида преступлений. Анализируются существующие меры профилактики, предупреждения и пресечения анализируемого явления, а также выделяются наиболее эффективные из них.

Ключевые слова: кибепреступления, организованная преступность, информационно-телекоммуникационные технологии, детерминанты кибепреступности, предупреждение преступлений, общественная опасность.

ORGANIZED CRIME IN CYBERSPACE

Annotation: This article examines questions about the state of organized cybercrime at the present stage of development of society. An analysis of the causes and conditions influencing the increase in the number of this type of crime is carried out. Existing measures of prevention, warning and suppression of the analyzed phenomenon are analyzed, and the most effective of them are highlighted.

Key words: cybercrime, organized crime, information and telecommunication technologies, determinants of cybercrime, crime prevention, public danger.

С течением времени и стремительным развитием информационно-телекоммуникационных технологий многие сферы жизнедеятельности человека начинают функционировать за рамками «реальной» жизни, всё больше уходя в виртуальное пространство. Преступная деятельность, напрямую зависящая от условий существования социума, также активно предпринимает попытки осуществления запрещенной активности в различных её проявлениях в сети «Интернет».

В Указе Президента Российской Федерации от 2 июля 2021 года № 400 «О Стратегии национальной безопасности Российской Федерации» указано, что к числу важных для мирового сообщества направлений следует относить обеспечение равной и неделимой безопасности для всех государств, в том числе в Европе, урегулирование конфликтов, борьбу с терроризмом, экстремизмом, наркобизнесом, организованной преступностью, распространением инфекционных заболеваний, обеспечение международной информационной безопасности, решение экологических проблем [1].

Исходя из вышесказанного, актуальность выбранного направления исследования подтверждается вдвойне. Помимо этого следует отметить, что наиболее серьезной категорией криминальных деяний является организованная преступность в силу повышенной степени общественной опасности, а использование информационно-телекоммуникационных технологий для достижения преступного умысла способствует рассматриваемой категории преступлений оставаться незамеченной и недостигаемой для правоохранительных органов.

В условиях глобализации совершение преступлений посредством информационно-телекоммуникационных технологий не вызывает сложностей, поскольку доступность, открытость и повсеместность различных устройств с выходом в сеть «Интернет» является неотъемлемой частью жизни общества на современном этапе. Поэтому, наравне с пресечением и профилактикой преступлений в сети «Интернет» стоит и предупреждение организованной преступности.

Немаловажным аспектом соотношения рассматриваемых социально-негативных явлений, выступают статистические данные за последние 3 года, представленные в таблице [2].

Таблица 1

Вид преступления / Год		2022 год	2021 год	2020 год
Количество зарегистрированных преступлений		1966795 преступлений (на 1,9 % меньше, чем в 2021 году)	2004404 преступлений (на 1,9 % меньше, чем в 2020 году)	2044221 преступлений (на 1 % больше, чем в 2019 году)
Организованная преступность	Преступления, совершенные группой лиц	102482 преступлений (на 11,6 % больше, чем в 2021 году)	91791 преступлений (на 0,9 % меньше, чем в 2020 году)	92643 преступлений (на 3 % меньше, чем в 2019 году)
	Преступления, совершенные в группе лиц по предварительному сговору	72558 преступлений (на 8,4 % больше, чем в 2021 году)	66929 преступлений (на 6,3 % меньше, чем в 2020 году)	71460 преступлений (на 5,4 % меньше, чем в 2019 году)
	Преступления, совершенные организованной группой или преступным сообществом (преступной организацией)	27207 преступлений (на 22,7 % больше, чем в 2021 году)	22172 преступлений (на 25,1 % больше, чем в 2020 году)	17727 преступлений (на 8,8 % больше, чем в 2019 году)
Преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации		522065 преступлений (на 0,8 % больше, чем в 2021 году)	517722 преступлений (на 1,4 % больше, чем в 2020 году)	510396 преступлений (на 73,4 % больше, чем в 2019 году)

Исходя из представленных данных, можно сделать вывод, что, не смотря на общую тенденцию снижения преступности за последние два года, уровень преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации неизменно растет. Организованная преступность в самом опасном и устойчивом проявлении также ежегодно увеличивает область своей деятельности. Сопоставляя данные виды преступлений, можно предположить, что киберпространство с его активным распространением во всех сферах жизни человека привносит не только положительные изменения, но и становится источником концентрации организованной преступности.

Повышенная общественная опасность заключается и в сращивании двух преступных проявлений в одно, именуемое организованная кибепреступность. Уровень угроз в информационном пространстве повышается с каждым днем, число рисков увеличивается, а негативные последствия киберпреступлений носят глобальный масштаб. Исходя из этого, предупреждение организованной преступности в сфере информационно-телекоммуникационных технологий и в сфере компьютерной информации становится одним из актуальных направлений на сегодняшний день.

Для выработки эффективных мер противодействия рассматриваемому явлению, необходимо установить детерминанты, обуславливающие его появление. В первую очередь стоит сказать, о периоде короновирусной инфекции в 2019 году, когда уровень преступности в сфере информационно-

телекоммуникационных технологий и в сфере компьютерной информации достиг показателей, превышающих предыдущий год на 73,4 % [2]. Обществу пришлось в срочном порядке переводить трудовую, финансовую, образовательную и другие сферы в режим «онлайн», не имея при этом необходимых знаний об основах безопасности в сети «Интернет». В жизни преступных формирований также произошли изменения, способствующие созданию кибер-ОПГ для нападения, совершения атаки на критически важную инфраструктуру государства. Более того, такая деятельность стала осуществляться как самостоятельно, так и с привлечением высококвалифицированных IT-специалистов, которые переходили на криминальную сторону в силу повышенного вознаграждения за свои знания. Так, утечка профессионалов в киберпространстве стала ещё одной причиной, усложняющей борьбу с преступностью.

Несмотря на возвращение к привычному образу жизни в «офлайне», IT-технологии основательно закрепились в функционировании общества, как и организованная преступность. Способности компьютеризации стали активно применяться при совершении преступлений, связанных с экстремизмом, изготовлением и распространением порнографических материалов с изображением несовершеннолетних, с незаконной организацией и проведением азартных игр, оборотом наркотических средств и оружия. Проведение специальной военной операции, безусловно, сказывается на уровне организованной преступности, в том числе связанной с незаконным оборотом оружия и идеологическими преступлениями.

Информационные технологии допускают различные способы совершения преступлений, в том числе с использованием сети «Интернет», пластиковых карт, средств мобильной связи, программных средств или компьютерной техники, фиктивных электронных платежей и т.д. Преступления, совершаемые организованной группой или преступным сообществом, в свою очередь, могут выражаться в использовании любого из перечисленных способов. В качестве примера можно проанализировать приговор Октябрьского районного суда г. Кирова, в соответствии с которым гражданин А. осужден за незаконный сбыт наркотических средств, с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»), в значительном размере, организованной группой.

Исходя из установленных судом обстоятельств, гражданин А. разработал план совершения преступлений, согласно которому путем заказа в сети «Интернет», решил приобретать наркотические средства, получать их через тайники и в почтовых отправлениях и хранить в недоступном для посторонних лиц месте, с использованием реагента получать готовые к употреблению наркотики в виде курительных смесей, а затем расфасовывать наркотические средства по полимерным пакетам и сверткам, после чего размещать их в сокрытые места в г. Кирове, а информацию о тайниках с наркотиками передавать покупателям после поступления оплаты на электронные счета. Непосредственную продажу наркотических средств А. решил осуществлять через организованный им Интернет-магазин, при этом использовать различные учетные записи в программе «Telegram», а для оплаты покупателями наркотических средств использовать

электронные счета «QIWI Кошелек» неосведомленных о преступной деятельности лиц. В соответствии с разработанной гражданином А. схемой, распространение наркотических средств должно было осуществляться организованной группой лиц, с распределением ролей: организатора, оператора, фасовщика и закладчиков [3].

Данный пример является далеко не единичным случаем слияния организованной преступности и IT-технологий. В современных условиях существует множество сайтов, на которых распространяют наркотические средства, психотропные вещества, их прекурсоры, оборот которых запрещен на территории Российской Федерации. Такая ситуация является типичным способом незаконной реализации товаров, оборот которых подлежит контролю со стороны государственных органов.

Подводя итог проведенному исследованию, стоит раскрыть вопрос о мерах противодействия рассматриваемым криминальным явлениям. Для эффективной борьбы с организованной преступностью в кибепространстве необходимо регулярно проводить обучающие мероприятия и информировать население о потенциальных угрозах в области безопасности информации, о способах совершения рассматриваемых преступлений, о преступных сообществах, реализующих свою деятельность на просторах сети «Интернет». Также внедрять в деятельность организаций занятия по виктимологической профилактике такого рода преступлений.

Помимо этого, важно уделить внимание надежности паролей и шифрованию данных, чтобы предотвратить несанкционированный доступ к личной информации. В следующую очередь, необходимо обозначить обязательность использования защитного программного обеспечения для защиты компьютеров и мобильных устройств от вирусов, шпионского программного обеспечения и других угроз. Также возникает потребность в мониторинге сетевой активности с целью обнаружения любых потенциальных угроз и преступлений. И в заключении следует сказать о сотрудничестве с правительственными и кибербезопасностными организациями для обмена информацией о новых угрозах и для выявления и пресечения преступлений в сфере информационно-телекоммуникационных технологий.

Список использованной литературы

1. О Стратегии национальной безопасности Российской Федерации [Электронный ресурс]: указ Президента Российской Федерации от 2 июля 2021 г. № 400 // Официальный интернет-портал правовой информации. Государственная система правовой информации. – URL: http://pravo.gov.ru.

2. Состояние преступности в России // Министерство внутренних дел Российской Федерации [Электронный ресурс] // URL: http://www.мвд.рф.

3. Приговор Октябрьского районного суда г. Кирова от 11 октября 2022 г. [Электронный ресурс] // Судебные и нормативно-правовые акты РФ // URL: https://sudact.ru/regular/doc/QfdjN3V9rHbV.

Намысов Ерлан Думанович,
заместитель начальника Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова, полковник полиции, e-mail: ynamysov@inbox.ru
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

О ЛИЧНОСТИ ПРЕСТУПНИКОВ, СОВЕРШИВШИХ ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Аннотация. В рамках современной криминологии и социологии особое внимание уделяется изучению личности преступников, занимающихся мошенничеством в виртуальной среде. Исследование интернет-мошенничества важно, поскольку оно показывает, как преступность эволюционировала в соответствии с новыми технологическими вызовами. В исследовании обращено внимание на специфические черты тех, кто совершает мошенничество в Интернете. Во время анализа учитывались социальные, психологические и криминологические черты этих преступников, а также то, как эти элементы взаимодействуют между собой.

Ключевые слова: криминология, интернет-мошенничество, личностные характеристики, мотивации преступников, виртуальная среда, социальные сети, предотвращение преступлений.

ON THE IDENTITY OF PERPETRATORS OF INTERNET FRAUDS

Annotation. Within modern criminology and sociology, particular attention has been paid to the study of the identity of criminals who engage in fraud in virtual environments. The study of Internet fraud is important because it shows how crime has evolved to meet new technological challenges. The study draws attention to the specific traits of those who commit fraud on the Internet. During the analysis, the social, psychological and criminological traits of these criminals were taken into account, as well as how these elements interact with each other.

Keywords: criminology, Internet fraud, personal characteristics, motivations of criminals, virtual environment, social networks, crime prevention.

Наиболее концентрированной и информативной частью криминологических данных, позволяющей установить наиболее важные выводы, закономерности и корреляции, является личность преступника в каждом конкретном сегменте преступности. Криминологи начинают свои исследования с предпосылки, что личность преступника представляет собой некий фундаментальный компонент преступного деяния. Соответственно, та или иная закономерность, выявленная в качественно-количественных характеристиках собирательного «портрета» личности преступника, диагностирует как значимые аспекты исследуемого сегмента криминальной действительности, так и является основой для поиска эффективных направлений профилактического воздействия. Кроме того, закономерности и тенденции позволяют оценивать криминологические про-

цессы в футурологическом аспекте (в рамках прогнозирования преступности). Категория «личность преступника» преимущественно является объектом криминологических исследований, хотя и не является монополией исключительно данной отрасли знания. Так, например, П.С. Дагель совершенно справедливо отмечал значение данной категории в рамках уголовно-правового поля, называя в ее качестве совокупности социально-политических, психических и физических признаков лица, совершившего преступление, имеющей уголовно-правовое значение [1, с. 53].

Действительно, в рамках уголовно-правового анализа лица, совершившего преступление (помимо необходимости установления у него необходимых признаков субъекта преступления) нередко возникает необходимость оценки параметров, которые имеют значение отягчающих иди смягчающих уголовную ответственность и наказание обстоятельств. Так, к примеру, несовершеннолетний возраст преступника имеет характер универсального свойства, имеющего не только криминологическое, но и уголовно-правовое значение.

Аналогично, факт наличия судимости за предшествующие преступные посягательства также в значительном количестве случаев имеет пересечения в уголовно-правовом и криминологическом учете. Вместе с тем, криминологические параметры категории «личность преступника» являются более широкими, поскольку в отношении многих из них уголовное право имеет индифферентное отношение (например, в контексте рода профессии, семейного положения, гражданства и т.д.). Личность преступника в рамках криминологических исследований обладает одновременно и конкретностью (в сравнении с другими качественно-количественными показателями преступности), и абстрактностью (поскольку представляет собой итоговый, собирательный результата всей совокупности криминологической информации о лицах, совершивших преступления определенного вида).

При этом она не может исследоваться в отрыве от понятия «личность» вообще, поскольку «любое преступление определяется в итоге всей предшествующей жизнью преступника, теми его личностными чертами и качествами, которые сформированы в процессе воспитания и которые в конкретной, порой весьма сложной или конфликтной ситуации и предопределяют выбор общественно опасного варианта поведения» [2, с. 21]. Личность преступника формируется «в недрах» личности человека, а криминальное поведение фактически есть «не что иное, как реализация вовне (объективизация) определенных сторон, свойств внутреннего мира данной личности» [3, с. 58]. К настоящему времени в криминологической теории сложился консенсус относительно отрицания возможности признания той или иной формы криминальной предрасположенности личности к совершению конкретного преступного посягательства.

Как указывает Ю.М. Антонян, личность преступника следует оценивать как «совокупность психологических социально значимых негативных свойств психики человека, развившихся в процессе многообразных и систематических взаимодействий с другими людьми» [4, с. 113].

Соответственно, в качестве аксиомы выступает тезис о том, что личность преступника – это социальный продукт, который находится в симбиотической

связи объективных обстоятельств и субъективны качеств, и является результатом более или менее длительной негативной детерминации социального характера. Действительно, именно личность преступника неизбежно занимает центральную позицию в механизме совершения конкретного преступления (или преступности определенного рода).

Свойства личности, которые в своей совокупности приводят к детерминации криминального поведения, являются одновременно и предшествующим, и итоговым фактором криминологического анализа. Именно по этой причине исследование личности преступника в рамках того или иного сегмента преступности традиционно является одним из центральных элементов анализа, благодаря которым общая «картина» приобретает более живое, конкретное наполнение. В конечном итоге, преступность в целом (равно как и отдельные ее сегменты) – это совокупность криминальных актов конкретных людей, обладающих социально-демографическими и нравственно-психологическими характеристиками.

Соответственно, признаки отдельно взятой личности преступника, в зависимости от кратности их воспроизводства при анализе структуры личности других лиц, совершивших аналогичное преступление, позволяют констатировать частоту повторения тех или иных свойств, которые, в конечном итоге, выявляют основные акценты, характеризующие «среднего» преступника в рамках того или иного сегмента преступности. В рамках криминологического анализа речь всегда идет о «среднестатистическом» преступнике, т.е. о том наборе наиболее типичных, часто повторяющихся свойств, которые могут быть отнесены к подавляющему большинству случаев совершения преступлений анализируемого вида. В целом, персонология в рамках криминологических исследований не является типичным методом анализа, поскольку задачами криминологии является оценка криминальных явлений в массе (равно как и личности преступника).

В редких случаях портрет отдельно взятого преступника может представлять познавательно-иллюстративный интерес, однако это следует отнести к исключениям, поскольку, как правило, предполагает те или иные экстраординарные криминальные способности личности, критическое множество потерпевших, исключительный талант маскировки, причинение тотально вредных последствий и т.д.

Следует, вместе с тем, отметить, что в сегменте информационной преступности (в том числе, и интернет-мошенничеств) вопросы персонологии могут иметь гораздо более выраженное прикладное значение, нежели в рамках других сфер криминальной действительности.

Так, в отличие от резонансных серийных преступлений, связанных с убийствами, половыми посягательствами, где личность преступника вызывает интерес с точки зрения тех или иных социальных отклонений и перверсий, в контексте «громких» интернет-мошенничеств ситуация имеет иной характер. Связано это с тем, что беспрецедентные суммы ущерба, авантюрные схемы масштабных обманов нередко причиняются людьми, не имеющими выраженных специфических характеристик. Это может быть просто грамотный сотрудник

фирмы, обнаруживший «лазейки» в системе безопасности или обычный человек со склонностью к обману и риску, пользующийся расчетами в информационной системе. Так, например, в сети Интернет можно встретить значительное количество описаний весьма наглых и успешных интернет-мошенников, которые успевают присвоить огромные денежные суммы до того, как будут обнаружены и привлечены к ответственности.

Нередко это прием так называемых дипфейков, когда мошенник формирует обманную схему на том, что выдает себя за наследника известного финансового магната либо лицо, известное своей благотворительной деятельностью и т.д. [5]. Одним из ставших типичными способов является манипуляция с платежными картами, когда мошенникам удается менять лимит средств и в последующем получать денежные суммы (хотя в данном случае в большей степени речь идет о тайном способе хищения) [6].

Подобные ситуации не являются редкими, однако «популярность» приобретают в случаях, когда суммы похищенных средств достигают беспрецедентных масштабов. Имеют место и такие формы интернет-мошенничества, которые могут причинить не только имущественный, но и физический вред. Так, к примеру, известен случай семьи архиепископа Гренона, которая под видом чудодейственного лекарства от различных неизлечимых болезней реализовывала через сайт препарат MMS, фактически соответствующий по своему составу бытовому отбеливающему средству.

Причем, в период пандемии COVID-19 продажи средства резко возросли. Выявить факт мошенничества в данном случае удалось с помощью деятельности агента по киберпреступности США [7].

Социальный контекст играет ключевую роль в формировании мотиваций и поведения преступников. Индивидуумы, занимающиеся интернет-мошенничеством, часто находятся в условиях, где отсутствует стабильность и доступ к легальным источникам дохода. Также важным является изучение воздействия социальных сетей и виртуальных сообществ на формирование криминального поведения.

Психологический аспект личности преступника важен для понимания механизмов принятия решений и разработки стратегий обмана. При анализе психологических характеристик следует обратить внимание на уровень эмпатии, способность к манипуляции и стрессоустойчивость, поскольку эти качества могут быть ключевыми в контексте совершения интернет-мошенничеств.

Криминологический анализ подразумевает изучение динамики криминальной активности, предшествующих преступлению, а также факторов, способствующих его совершению. Важно выявить теоретические модели, которые могут объяснить вовлечение личности в интернет-мошенничество, такие как теория дифференциальной ассоциации или теория социального контроля.

Таким образом, анализ личности преступников, совершивших интернет-мошенничество, требует комплексного подхода, учитывающего социальные, психологические и криминологические аспекты, что позволяет не только лучше понять мотивации и динамику деятельности данных субъектов, но и разрабо-

тать эффективные стратегии предотвращения и борьбы с интернет-мошенничеством.

Список использованной литературы

1. Дагель П.С. Учение о личности преступника в советском уголовном праве. – Владивосток: Изд-во Дальневост. ун-та, 1970. – 132 с.

2. Орлова Ю.Р., Гусева О.Н. Криминологические особенности личности несовершеннолетних женского пола, совершивших корыстно–насильственные преступления // Юридическая психология. – 2008. – № 4. – С. 19–23.

3. Мерзлов Ю.А. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2015. – № 4(7). – С. 56–61.

4. Антонян Ю.М. Личность преступника. Криминология: учебник / под ред. В.Н. Кудрявцева, В.Е. Эминова. 4-е изд., перераб. и доп. – М.: Норма, 2009. – 207 с.

5. Самые знаменитые мошенники современных соцсетей [Электронный ресурс] // URL: https://dzen.ru/a/Y2487HOtlCRzL_vb.

6. 10 крупнейших интернет-афер всех времен [Электронный ресурс] // URL: https://fishki.net/1688180-10-krupnejshih-internet-afer-vseh-vremen.html.

7. Самые громкие преступления цифровой эпохи: подборка Bloomberg [Электронный ресурс] // URL: https://trends.rbc.ru/trends/industry/60ec49bc9a7947fb7b4a0ac8.

Обухова Софья Александровна,
адъюнкт, e-mail: sofya_obukhova@mail.ru
(Воронежский институт МВД России, Российская Федерация)

ВИКТИМОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ПОВЕДЕНИЯ ЖЕРТВ СЕКСУАЛЬНОГО НАСИЛИЯ

Аннотация. В представленной статье рассматриваются основные аспекты виктимного поведение потенциальных и реальных жертв насильственных преступлений против половой неприкосновенности и половой свободы личности на основе комплексного анализа статистических данных и изучения теоретических основ криминологии.

Ключевые слова: сексуальное насилие, жертва, виктимология, виктимное поведение, половая свобода, половая неприкосновенность, криминология, насильственные преступления, негативные проявления, предупредительная деятельность, профилактическая работа.

VICTIMOLOGICAL FEATURES OF BEHAVIOR OF VICTIMS OF SEXUAL VIOLENCE

Anotation. The presented article examines the main aspects of the victim behavior of potential and actual victims of violent crimes against sexual integrity and sexual freedom of the individual based on a comprehensive analysis of statistical data and the study of the theoretical foundations of criminology.

Keywords: sexual violence, victim, victimology, victim behavior, sexual freedom, sexual integrity, criminology, violent crimes, negative manifestations, preventive activities, preventive work.

Виктимологические особенности поведения жертв противоправных посягательств заслуживают особого внимания ученых в области криминологии для грамотной разработки и применения в практической деятельности. Для того, чтобы перейти к детальному рассмотрению виктимного поведения лиц, ставших жертвами насильственных преступлений против половой неприкосновенности и половой свободы личности, необходимо пояснить что же представляет собой виктимология как наука, что позволит выявить сущность виктимного поведения жертв деяний, которые запрещены действующим уголовным законом под угрозой наказания.

Следует заметить, что самостоятельной наукой виктимология не является, она выступает неотъемлемым составным элементом криминологии, но многие ученые сходятся во мнении, что она представляет собой достаточно перспективное направление развития научной криминологической мыслии, при условии оказания должного внимания ее развитию, может выделиться в самостоятельную область научного знания.

так, виктимология как наука представляет собой систему положений и разрабатываемых на их основе теорий, в том числе и прогностического характера, о роли лица, ставшего жертвой преступного посягательства, в механизме совершения конкретного деяния [1, с. 167].

Отличительной чертой виктимного поведения является осуществление потенциальной жертвой преступления каких-либо активных действий, которые служат сигналом преступнику для совершения правонарушения, или же, наоборот, бездействие в конкретной ситуации. Необходимо отличать виктимное поведение от провокации другого лица к совершению преступления, так как потенциальный потерпевший зачастую даже не осознает, что своими действиями привлекает внимание антисоциального субъекта.

Также многие криминологи, изучающие вопросы виктимологии, выделяют параллельный вид поведения индивида – нейтральное, которое представляет собой такое поведение лица в конкретной жизненной ситуации, не способное спровоцировать другое лицо на совершение в отношении него преступления. Ярким примером является попытка завладеть оружием сотрудника полиции, где поведение первого безупречно.

Виктимное поведение в зависимости от ряда как личностных, так и внешних факторов может быть устойчивым и ситуационным, которое проявляется лишь единожды под давлением обстоятельств и вовсе не свойственно конкретной личности. Следовательно, поведение жертвы в конкретной ситуации, наряду с множеством иных факторов, перечисленный выше перечень которых не

является исчерпывающим, напрямую влияет на формирование криминогенной ситуации.

Анализ трудов ученых в области уголовного права и криминологии, а также наук психологического профиля показал, что существует небезосновательное мнение о возможности потенциальной жертвы насильственных половых преступлений избежать попадания в ситуацию криминогенного характера, при условии, что она понимает как грамотно себя вести.

Выделяют два вида типичного поведения потенциальных жертв преступлений против половой неприкосновенности и половой свободы личности:

а) нейтральное поведение – такой тип поведения личности, который характеризуется отсутствием явных признаков, привлекающих правонарушителя, но при этом все же становится жертвой противоправного посягательства;

б) негативное поведение – поведение потенциального потерпевшего, которое становится причиной привлечения внимания криминальных элементов, но, тем не менее, не является асоциальным [2, с. 176].

Виктимогенная ситуация может складываться под влиянием многих аспектов, но, согласно мнению ученых, основная роль отводится физиологическим свойствам, личностным характеристикам и особенностям поведения не только потенциальной жертвы, но и преступника [3, с. 408]. Одним из подобных факторов является возрастная группа, к которой относится лицо, причем это касается не только преступника, но и потерпевшей. Согласно данным статистики в подавляющем большинстве случаев изнасилование совершается мужчинами в возрасте от 20 до 35 лет. Жертвой же, как правило, являются женщины, которые входят в возрастную категорию от 25 до 40 лет, что составляет в среднем 51% от всех зарегистрированных случаев изнасилования. Также отдельную возрастную группу жертв рассматриваемого вида преступлений составляют лица, не достигшие совершеннолетнего возраста.

На основании проанализированных статистических данных МВД России, можно сделать вывод, что наиболее часто негативное поведение жертвы проявляется в возрасте до 25 лет, а это более 90% от общего числа потерпевших с негативным поведением. Причем вызывает особую обеспокоенность то, что подавляющее большинство жертв указанной основной категории, создающие своим поведением наиболее «благоприятный» климат для действий преступника – это несовершеннолетние девушки. Немаловажный признак, влияющий на виктимное поведение потенциальной жертвы – уровень образования, культурного развития и досуговые предпочтения. Это обусловлено тем, что вышеперечисленные качества напрямую влияют на жизненные цели, установки и моральные принципы человека, что формирует его социальное поведение, в том числе и в предкриминогенных ситуациях.

Культурное развитие конкретной личности, которое, по сути, в основном и формирует досуговые предпочтения человека, также играет огромную роль, так как потенциальная жертва рассматриваемого преступления элементарно имеет меньше шансов оказаться в месте с повышенной криминогенной обстановкой [4, с. 110].

Одним из оснований в выборе преступником жертвы выступает репутация последней. Анализ данных социологических исследований свидетельствует о том, что 27% мужчин, осужденных за изнасилование, выбирали женщин с отрицательной общественной характеристикой. Основанием такой характеристики, в первую очередь, является неразборчивость женщины в половых связях либо занятие проституцией.

Неразборчивость девушек, на наш взгляд, обусловлена двумя основными аспектами. Первый – это пробелы в воспитании, которые приводят к отсутствию «здоровой» подозрительности, и, следовательно, к легким знакомствам с противоположным полом, которое сопровождается посещением наедине с потенциальным преступником мест, наиболее характерных для совершения изнасилования. По статистике большинство, а именно более 58% изнасилований происходят на улице в темное время суток, второе место занимает жилище преступника (около 32%), третье – жилое помещение потерпевшей (приблизительно 6%), четвертое – совместная жилплощадь преступника и жертвы, что характерно для, так называемых, «бытовых» изнасилований (около 4%). Второй аспект носит положительную характеристику поведения жертвы и заключается в чрезмерной доверчивости, как правило, в силу молодого возраста, либо социальной «неиспорченности» и наивности.

Особое внимание заслуживает состояние опьянения, в котором зачастую находятся жертвы насильственных преступлений против половой неприкосновенности и половой свободы личности. В подавляющем большинстве случаев согласно данным социологических исследований и официальной статистики более трети потерпевших находились в состоянии алкогольного опьянения [5, с. 7].

Таким образом, усматривается необходимость усиления мер профилактического характера в борьбе с насильственными посягательствами на половую неприкосновенность и половую свободу личности, в которые, на наш взгляд, обязательно должна входить разработка рекомендаций по поведению при попадании человека в виктимогенную ситуацию, которые могут увеличить его шансы на благополучный выход из сложившейся обстановки.

Список используемой литературы

1. Варчук Т.В. Виктимология: учебное пособие: доп. МВД РФ; рек. УМЦ. – М: ЮНИТИ, 2015. – 191 с.

2. Лелеков В.А. Ювенальная криминология: учебник – М.: ЮНИТИ-ДАНА: Закон и право, 2015 – 311 с.

3. Алексеев А.И. Криминологическая профилактика: теория, опыт, проблемы – М.: Норма, 2001. – 481 с.

4. Полубинский В.И. Криминальная виктимология: монография. – М.: Всероссийский научно-исследовательский институт, 2008. – 208 с.

5. Ривман Д.В. Виктимология. – Санкт-Петербург: Юрид. центр Пресс, 2000. – 331 с.

Овсянников Андрей Викторович,
старший преподаватель кафедры оперативно-разыскной деятельности
и оперативно-технических мероприятий органов внутренних дел
e-mail: andrej.ovsyannikov.340@mail.ru
*(Тюменский институт повышения квалификации сотрудников МВД России,
Российская Федерация)*

ПРОВЕДЕНИЕ ОПЕРАТИВНО-ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ С УЧЕТОМ СОВРЕМЕННОГО СОСТОЯНИЯ НЕЗАКОННОГО ОБОРОТА НАРКОТИКОВ

Аннотация. В статье представлен анализ современного состояния незаконного оборота наркотиков в Российской Федерации. Отражена статистическая отчетность состояния преступности в сфере незаконного оборота наркотических средств и психотропных веществ, а также основные формы ее проявления. С учетом состояния современной наркопреступности определены меры, направленные на реализацию мероприятий по предупреждению, пресечению, мониторингу и профилактике правонарушений в сфере незаконного оборота наркотиков.

Ключевые слова: незаконный оборот наркотиков, профилактика, наркомания, наркотизм, антинаркотическая политика.

CARRYING OUT OPERATIONAL AND PREVENTIVE MEASURES TAKING INTO ACCOUNT THE CURRENT STATE OF DRUG TRAFFICKING

Anotation. The article presents an analysis of the current state of drug trafficking in the Russian Federation. The statistical reporting of the state of crime in the field of illicit trafficking of narcotic drugs and psychotropic substances, as well as the main forms of its manifestation, is reflected. Taking into account the state of modern drug crime, measures have been identified aimed at implementing measures to prevent, suppress, monitor and prevent offenses in the field of drug trafficking.

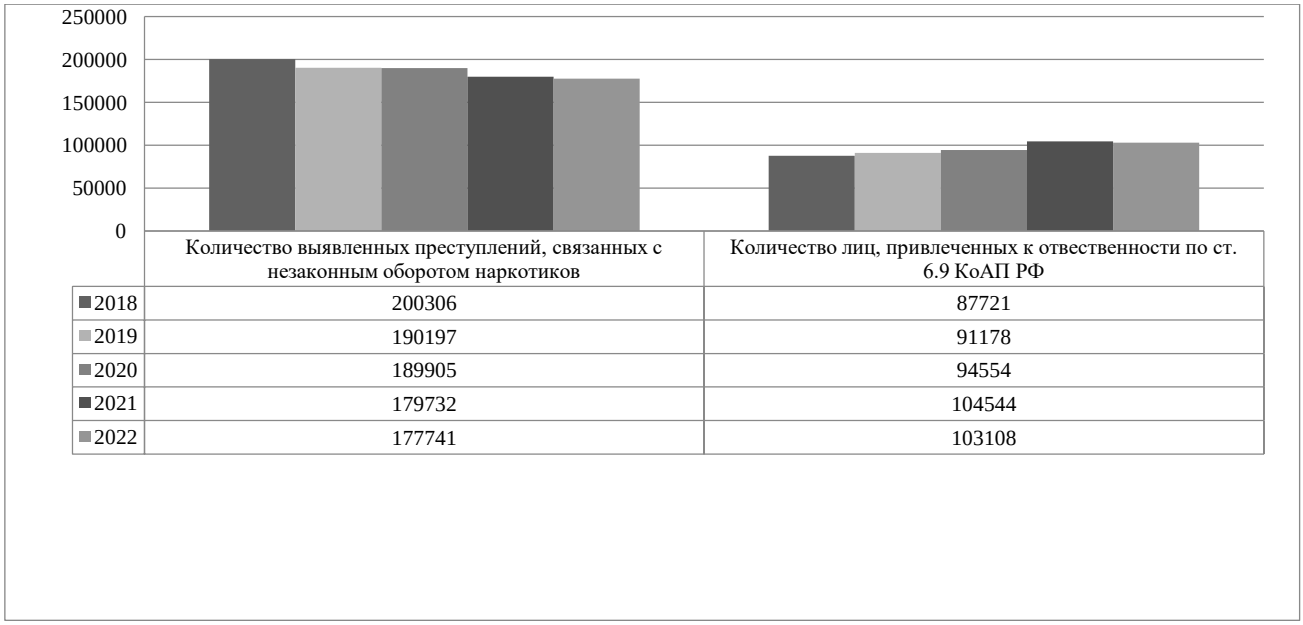
Keywords: drug trafficking, prevention, drug addiction, narcosis, anti-drug policy.

В современном мировом сообществе существуют различные взгляды на проблему не медицинского потребления наркотических средств, психотропных веществ и их аналогов, а также новых потенциально опасных психоактивных веществ (далее – наркотики). Опираясь на исторические и культурные прецеденты, религиозные и политические режимы, каждое государство самостоятельно определяет приоритетные направления в противодействии незаконному обороту наркотиков.

Отличительной чертой незаконного оборота наркотиков является его транснациональный характер. Международные сделки с наркотиками оказывают значительную финансовую поддержку экстремисткой и террористической

деятельности, способствуют затягиванию вооруженных конфликтов, а также оказывают дестабилизирующие воздействие на социальное и экономическое развитие государств.

Согласно статистическим данным Главного информационного центра Министерства внутренних дел Российской Федерации, на протяжении последних лет в Российской Федерации прослеживается тенденция к незначительному снижению числа зарегистрированных преступлений в сфере незаконного оборота наркотиков, так в 2018 году – 200306 преступлений; 2019 – 190197; 2020 – 189905; 2021 – 179732; 2022 – 177741 [1]. Однако в указанный период стоит обратить внимание на показатель выявленных административных правонарушений, предусматривающих ответственность за потребление наркотиков без назначения врача: 2018 год – 87721; 2019 – 91178; 2020 – 94554; 2021 – 104544; 2022 – 103108 (См.: рис.1). На наш взгляд, состав указанного административного преступления является не менее общественно опасным деянием, чем уголовно наказуемое. Разница заключается лишь в размере массы, изъятого у потребителя наркотического средства, психотропного вещества, либо нового потенциально опасного психоактивного вещества.



	Количество выявленных преступлений, связанных с незаконным оборотом наркотиков	Количество лиц, привлеченных к ответственности по ст. 6.9 КоАП РФ
2018	200306	87721
2019	190197	91178
2020	189905	94554
2021	179732	104544
2022	177741	103108

Рис. 1. Тенденции развития незаконного оборота наркотиков в Российской Федерации в 2018-2022 годах

В последние годы преступность в сфере незаконного оборота наркотиков претерпела значительные изменения, причем как количественные, так и качественные. В соответствии с тенденциями развития современных IT-технологий, произошел резкий скачек количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, так в период с 2019 по 2022 год количество возросло на 77,3 % с 294409 до 52206 соответственно [1]. Незаконный оборот наркотиков стал одним из основных видов противоправной деятельности в Российской Федерации максимально использующий возможности

современного развития IT-технологий. Следует отметить, что количество выявленных преступлений, только по ст. 228.1 Уголовного кодекса Российской Федерации (указанная статья предусматривает ответственность за незаконные производство, сбыт или пересылку наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылку растений, либо их частей, содержащих наркотические средства или психотропные вещества), совершенных с использованием информационно-телекоммуникационных технологий, составило: 2018 год – 18918; 2019 – 24817; 2020 – 47060; 2021 – 51444; 2022 – 62209 [1].

Еще одним показателем изменения наркоситуации в Российской Федерации можно считать изменение количества и видов, изъятых из оборота наркотиков и их прекурсоров. В 2018 году всего из оборота изъято 20,5 тонны наркотических средств, доля синтетических наркотиков от общего числа изъятых, составила 20 % или 4,1 тонна, в 2022 году всего изъято – 26,4 тонны, из которых синтетические наркотики составили 51,9 % или 13,7 тонны. Аналогичная ситуация и по изъятым прекурсорам наркотиков 1,2 тонны в 2018 году против 15 тонн в 2022 году [2].

Необходимо подчеркнуть, что потребление наркотиков по-прежнему больше распространяется среди молодежи (например, для указанной категории характерно потребление синтетических наркотиков, чем потребление наркотиков опийной группы путем внутривенных инъекций), чем среди взрослого населения, и носит более массовый характер. Данные доводы находят свое подтверждение в научном исследовании проведенным в 2022 году Национальный медицинский исследовательский центр психиатрии и наркологии им. В.П. Сербского Минздрава России, о том, что в последние годы на фоне общей заболеваемости наркоманией, выросло число лиц, у которых заболевание приобретено в следствии употребления психостимуляторов, а также употреблением других наркотиков и сочетанием наркотиков разных групп [3, с. 36].

На наш взгляд, с учетом современных тенденций развития наркоситуации, необходимо уделять большее внимание первичной профилактики не медицинского потребления наркотиков. В дополнении к основным первичным мерам профилактического воздействия, к которым можно отнести размещение социальных плакатов, баннеров и видеороликов, на объектах инфраструктуры, проведение разъяснительных бесед в образовательных организациях, проведения тестирования на наркотики и т.п., необходимо активно и наступательно проводить, в том числе оперативно-розыскные мероприятия в сети Интернет. На наш взгляд, профилактические мероприятия в сети Интернет целесообразно проводить адресно, в отношении конкретного пользователя. При этом сотрудники оперативных подразделений, осуществляющие оперативно-розыскную деятельность, могут проводить профилактическую работу на примере способов воздействия на пользователя, используемых в маркетинге. Примером тому может служить контекстная реклама, которая на основании запросов в поисковых системах (например, Яндекс и Google), предлагает пользователям товары и услуги, к которым он проявил интерес. Правоохранительные органы в свою очередь оказывают профилактическое воздействие (например, в виде наглядного

баннера, памятки с указанием видов и размеров ответственности, за противоправную деятельность в сфере незаконного оборота наркотиков), при проявлении пользователя интереса к теме наркотиков в поисковых системах. На наш взгляд, указанный подход в профилактике незаконного оборота наркотиков, с учетом современных тенденций, является актуальным и требует дополнительной проработки.

Список используемой литературы

1. Официальный сайт МВД России [Электронный ресурс]. URL: https://мвд.рф.

2. Доклад о наркоситуации в Российской Федерации 2018, 2022 год. // Государственный антинаркотический комитет: официальный сайт. URL: https://xn----7sbabhak4bqktigbdqi0yka.xn--p1ai/index.php?option=com_content&view=article&id=2008:-------2022-&catid=99:--2023-&Itemid=143.

3. Киржанова В.В., Григорова Н.И., Бобков Е.Н., Киржанов В.Н., Сидорюк О.В. Состояние и деятельность наркологической службы в Российской Федерации в 2021 году: Аналитический обзор. – М.: ФГБУ «НМИЦ ПН им. В.П. Сербского» Минздрава России, 2022. – 202 с.

Прокопова Анна Алексеевна,
доцент кафедры уголовно-правовых дисциплин
к.ю.н., e-mail: anya.prokopova@gmail.com
(АНО ВО «Национальный институт бизнеса», г. Москва, Российская Федерация)

ТРАНСФОРМАЦИЯ ПРОЦЕССУАЛЬНОЙ ФОРМЫ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В статье рассматривается варианты интенсификации процесса расследования уголовных дел, что позволит при тех же ресурсах за счет оптимального, разумного их использования вскрыть дополнительные резервы ускорения процессуальной формы. Основная нагрузка при интенсификации уголовного судопроизводства ложится на организацию работы органов уголовного преследования, в этом наиболее эффективно может помощь новейшие информационные технологии.

Ключевые слова: дифференциация уголовно-процессуальной формы, научно-технические средства, Республика Казахстан, уголовный процесс, ускоренные производства, цифровизация.

TRANSFORMATION OF THE PROCEDURAL FORM IN THE CONTEXT OF DIGITALIZATION OF CRIMINAL PROCEEDINGS

Annotation. The article discusses options for intensifying the process of investigating criminal cases, which will allow, with the same resources, through their optimal, reasonable use, to reveal additional reserves for speeding up the procedural

form. The main burden when intensifying criminal proceedings falls on the organization of the work of criminal prosecution bodies; the latest information technologies can most effectively help with this.

Key words: differentiation of the criminal procedural form,scientific and technical means, The Republic of Kazakhstan, criminal process, accelerated production, digitalization.

Рациональность и процессуальная экономия стала основным вектором развития уголовного процесса последнего десятилетия на всем постсоветском пространстве. Законодатель пытается сконструировать новые механизмы расследования преступлений, чтобы сократить трудозатратность процесса в целях обеспечения жизнеспособности системы уголовного судопроизводства.

Ускорение досудебного производства достигающееся за счет сокращения его уголовно-процессуальной формы, посредством урезания предела доказывания, изъятия части процедурных механизмов, а также наличиетребования о согласие подозреваемого с виной либо обвинением, часто влияет на качество расследования и создает риски нарушения прав участников ускоренных производств.

Историческая тенденция к унификации уголовно-процессуальной формы, отойти от экстенсивного пути (изъятие процессуальных гарантий) и обратится в сторону интенсификации уголовного процесса. Процессуальная форма еще имеет резервы совершенствования за счет отказа от бюрократических процедур, не снижающих уровень гарантий правосудия и прав человека, в том числе за счет внедрения современных информационных технологий [1, с. 295-299].

Интенсификация предполагает достижение наибольшего эффекта при тех же ресурсах за счет оптимального, разумного их использования, отыскания в них дополнительных резервов. Значительная нагрузка по интенсификации уголовного судопроизводства ложится на организацию работы, именно в этой части должны сказать решающее слово новейшие информационные технологии [2, с. 50-55].

Примером, в данном случае, может случить уголовное судопроизводство Республики Казахстан, где в течение последних лет проводятся широкомасштабные реформы, которые в том числе коснулись и внедрение в процесс расследования инновационных технологий.

В Уголовно-процессуальном кодексе 2014 г. (далее - УПК РК) [3] появился новый вид допроса с использованием научно-технических средств в режиме видеосвязи (дистанционный допрос) [4, с.173].

Это обусловлено необходимостью разрешения проблем несвоевременности явки (доставки) свидетелей в установленное время, что зачастую является причиной затягивания расследования уголовных дел и, как следствие, нарушения прав и законных интересов участников процесса, а также уменьшения временных и материальных затрат на извещение свидетелей, находящихся на значительном удалении от места расследования уголовного дела, организацию командировок и выезд лица, производящего расследование, к месту нахождения потерпевшего (свидетеля).

Дистанционный допрос является разновидностью допроса, производимого в режиме реального времени с отдаленным присутствием допрашиваемого посредством научно-технических средств в режиме видеосвязи, при котором возможен обмен аудио- и видеоинформацией [5, с. 20-23].

Основной целью дистанционного допроса является получение в кратчайшие сроки и без значительных материальных затрат показаний свидетеля и потерпевшего, которые находятся в отдалении от места производства досудебного производства. Допрос организовывается заинтересованным следователям, путем направления отдельного поручения в местонахождения необходимого участника процесса (ст. 213 УПК РК). Допрос осуществляется в общем порядке с учетом особенностей технических средств, применяемых в ходе следственного действия. Данный вид допроса возможен для производства в рамках оказания правовой помощи по уголовным делам на основании международных договоров (ст. 576 УПК РК).

Дистанционный допрос значительно сокращают время на организацию и проведения допроса лично следователем (выезд в командировку) либо по поручению (длительное ожидание, некачественный результат), что во много ускоряет ход расследования.

Еще одной инновацией досудебного производства в Республике Казахстан, стал электронной формат судопроизводства, который в 2017 г. [6] был официально закреплен, наравне с бумажным.

Как отмечал генеральный прокурор РК Жакип Асанов, «Цифровизация уголовного процесса позволит решить ряд чувствительных для населения вопросов, а также упростить процедуру сбора доказательств и составления процессуальных документов, снизить риски фальсификации материалов дела и их утери, а также материальные затраты и нагрузку на следственные и судебные органы» [7].

Электронный формат расследования осуществляется на базе (модуля) «Е-уголовное дело» в системы Единого реестра досудебных расследований (ЕРДР). Модуль содержит алгоритмы действийпо формированию уголовного дела, с момента начала расследования до момента исполнения приговора. Работа с системой осуществляется посредством заполнения определенных электронным шаблонов (бланков), позволяющих прикреплять сведения о полученных доказательствах включая фото, аудиозаписи, видеоизображения, а также иные файлы и программные продукты, которые не возможно в последующем удалить.

Такой механизм направлен на максимальную прозрачность расследования, возможность доступа к материалам дела его участников и прокурора для ознакомления и изучения, а также исключение случаев фальсификации документов и потери уголовных дел.

В настоящий момент в электронном формате расследуется большее количество угоовных дел, так за 10 месяцев 2023 г. из 147 529 уголовных дел которые находились в производстве 134 009 дела, расследовались в электронном формате (90%). Распространение применения электронного формата хорошо видно на приведенном графике № 1.

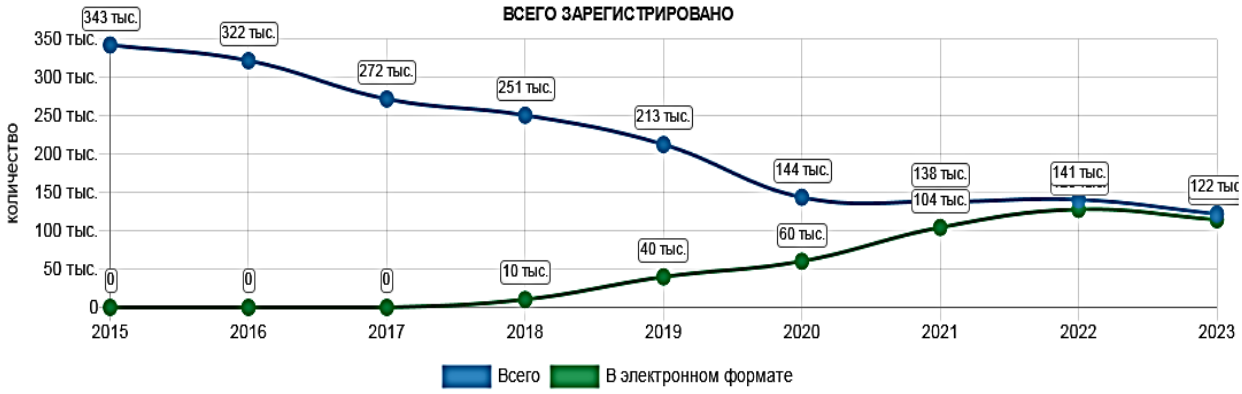


График 1. Количество зарегистрированных досудебных расследований.

Апробации нового формата расследования показала, что ускорение досудебного производства при расследовании в уголовных дел в электронном формате достигается путем сокращение сроков, при:

– направление ходатайств лицом, осуществляющим досудебное производство в прокуратуру, суд;

– передаче материалов досудебного расследования в органы прокуратуры и суда, для согласования решения о применении мер пресечения и разрешения на проведение отдельных следственных действий;

– направление материалов досудебного расследования прокурору, судье для рассмотрения по существу поступившие в рамках расследования жалобы, ходатайства и т.д.;

– ознакомление с материалами уголовного дела, путем одновременного прочтения всеми участникам досудебного расследования без привязки по времени и месту.

Все эти действия теперь возможно осуществлять, не выходя из кабинета, при помощи возможностей программного обеспечения. Однако на данный позитивный процесс накладываются сложности, связанные с процессом внедрения трехзвенной модели судопроизводства, которая перераспределила ответственность между органами уголовного преследования и прокуратурой. Сейчас оперативности расследования мешает выстроившейся процесс скрытого, межведомственного согласования процессуальных решений, выносимых в электронном формате. Данные действия обосновываются желанием избежать ухудщения показателей работы в случае допущения исполнителями решений ошибок, которые не возможно исправить после официального внесения документа в модуль «Е-уголовное дело».

Еще одним новшеством уголовного процесса Казахстана стала возможность составления краткого протокола следственного действия, если его ход и результаты полностью фиксируются с помощью средств звуко-, видеозаписи (ч.3 ст. 199 УПК РК) [8].

Предполагается, что данный формат позволит значительно оптимизировать сроки расследования, обеспечит прозрачностьрасследования уголовных дел,

исключит бюрократическую волокиту, минимизирует коррупционные и фальсификационные риски, а также обеспечит защиту прав и законных интересов участников досудебного расследования.

Сейчас еще трудно говорить о результатах данного нововведения. Стоит понимать, что данных формат доказательственного процесса потребует от исполнителя высокого уровня профессионализма, владения методическими приемами производства следственных действий и работы с техническими средствами, а также поддержаниях на высоком техническом уровне итоговых материалов (качество звука, -видео, отсутствие монтажа, ретуши и т.д.).

Резюмируя, стоит отметить, что процесс реализации инновационных технологий в уголовном судопроизводстве сопряжен с необходимостью вложения значительных финансовых средств, а так же созданием информационной среды способной обеспечить надлежащий уровень защиты процессуальной информации.

Таким образом, использование цифровых технологий и научно-технических средств в досудебном производстве с учетом всех достоинств и недостатков вполне действенно может ускорить процесс расследования без создания угрозы нарушения прав и законных интересов его участников.

Современные технологии призваны упрощать жизнь во всех ее сферах, уголовное судопроизводство не должно становиться исключением. Рационализация досудебного производства средствами современных технологий наиболее оптимальный способ ускорения на современном этапе развития уголовного процесса.

Список использованной литературы

1. Прокопова А.А. Применение цифровых технологий и научно-технических средств как рациональный вектор ускорения досудебного производства // Российская правовая система в условиях четвертой промышленной революции: материалы XVI Международной научно-практической конференции (Кутафинские чтения): в 3 ч. – М. – 2019. – Ч. 3. – С. 295–299.

2. Победкин А.В. Этико-аксиологические риски моды на цифровизацию для уголовного судопроизводства (об ошибочности технологичного подхода к уголовному процессу) // Вестник Московского университета МВД России. – 2020. – № 3. – С. 50–55.

3. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V // Казахстанская правда. – 2014. – 10 июля.

4. Ахпанов А.Н. Депонирование показаний потерпевшего и свидетеля в уголовном процессе Республики Казахстан// Вестник Омского университета. Серия «Право». – 2015. – № 4 (45). – С. 173–179.

5. Прокопова А.А. Особенности использования научно-технических средств в режиме видеосвязи: процессуальные и криминалистические аспекты: учебно-практическое пособие. – Караганда, 2017. – 80 с.

6. О внесении изменении и дополнений в некоторые законодательные акты Республики Казахстан по вопросам модернизации процессуальных основ правоохранительной деятельности [Электронный ресурс]: закон Республики Ка-

захстан от 21 декабря 2017 г. № 118-VI ЗРК // Информационно-правовая система нормативных правовых актов Республики Казахстан. – URL: http://adilet.zan.kz/rus.

7. Уголовные дела в электронном формате апробируют в Казахстане. Информация сайта «InformБюро» [Электронный ресурс] – URL: https://informburo.kz/novosti/ugolovnye-dela-v-elektronnom-formate-aprobiruyut-v-kazahstane.html.

8. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам прав человека в сфере уголовного судопроизводства, исполнения наказания, а также предупреждения пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения [Электронный ресурс]: закон Республики Казахстан от 17 марта 2023 г. № 212-VII – URL: // https://online.zakon.kz.

Sitebekov Aidar Mutalikovich,
Head of the Almaty academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Makan Esbulatov

Kadyrova Rashida,
Head of cybersecurity and information technologies department

Endybaiuly Erlan,
Docent of cybersecurity and information technologies department

Akezhan Sabibolda,
Lecturer of cybersecurity and information technologies department

(Almaty academy of the Ministry of Internal Affairs M. Esbolatova)

DIGITAL SOVEREIGNTY AS A FUNDAMENTAL TOOL IN CYBERSPACE

Annotation. A sovereign state is an independent state “recognized within its borders by the international community” and exercising “administrative power and jurisdiction” over its population. However, in the digital universe, this concept is not so easily defined. While digital sovereignty generally refers to the fact that a state (government) or organization must establish its authority to exercise its powers in cyberspace, it also focuses on more tangible issues such as technological dependence or control over users' personal data. In fact, the digital sovereignty movement, which launched about a decade ago, aims to reclaim a share of the power exercised in the digital space.

Keywords: cybersecurity, digital assets, cyber threats, information security, information protection, digital law.

In the early days of digital technology, its proponents sought to create power free of governments. Published in 1996, the Declaration of Independence of Cyberspace defines that governments have no power in this ecosystem.

The sovereignty of governments has been quickly undermined by the rise of digital globalization, which ignores borders and laws and allows powerful web players to set their own rules and even be classified as “fully digitized countries.” Several examples support this theory.

A case in point is Denmark's appointment of a special GAFA Ambassador in 2017 [1]. Another example is the term "colonization" (admittedly consensual), which is increasingly used to describe the attitude of these multinational corporations towards «real» countries.

The concept of 'digital sovereignty' emerged from this observation in the 2000s.

The term has since been taken up by politicians such as French Interior Minister Michèle Alliot-Marie, who in 2009 emphasized the need to “guarantee digital sovereignty” and “extend the scope of the rule of law to the digital space.”

In 2013, the Snowden case (the revelation of mass eavesdropping by the NSA) highlighted the risks associated with failing to govern digital spaces [2].

Then, in 2015, the Facebook-Cambridge Analytica scandal highlighted the multinationals' fraudulent use of users' personal data. Such large corporations have shown indifference to the issue of privacy.

Digital independence is now a well-established concept. This is reflected in specific decisions taken at the European level, which are aimed at developing sovereign cloud solutions and local search engines (including the French company Qwant) [3].

These decisions are also encouraging European companies to seek independence [4] from large multinational web players, opting instead for national solutions.

This applies to companies' use of sensitive data. And this is the cornerstone issue of digital sovereignty from an organizational perspective.

Identifying Digital Independence Issues

A company's efforts to create effective digital independence pose two major challenges: one is strategic [5] and the other is ethical.

While the pandemic has further increased companies' dependence on multinational cloud solutions, now, more than ever, they must develop digital autonomy in the quest to control their data (their own and that of their customers).

This is because these leading web players are subject to regulations that may conflict with the strategic interests of the organizations that use them.

As an example, GAFAM must comply with extraterritoriality rules such as the Cloud Law. The latter allows the US government to access data [6] hosted by national companies, even if their servers are located outside the United States.

As a result, the confidentiality of such data is in no way guaranteed. Considering that 92% of data produced in the West is hosted in the United States, these laws pose a threat to business interests [7].

Digital sovereignty also extends to individuals, with an emphasis on preserving the right to privacy. This is especially true in cases where the data entrusted to operators is confidential, including bank details, medical information, financial data.

Moreover, this issue concerns not only the rules of extraterritoriality or transborderness [8]. Once organizations collect data, they have the ability to sell it to advertisers or politically motivated institutions.

Take, for example, the Cambridge Analytica scandal [9], where voters' personal data was used to influence voting intentions.

Given that users are increasingly concerned about how their personal data is processed (69% of French people are concerned about how their data is used), companies should make protecting such information a priority [10].

Considering the various issues at stake, a key question arises: why should companies focus all their efforts on digital sovereignty? There are several answers.

Firstly, to protect your data. This is especially true for companies processing sensitive data in sectors such as defense, healthcare, security, banking and insurance, and industrial. However, all personal data is at risk if it is stolen, altered or misused. As stated in this article, there is absolutely no way to guarantee privacy when it is hosted by Big Tech giants [11]. Conversely, data in Europe is protected by continental laws, including the European Union's General Data Protection Regulation (GPDR).

Secondly, provide guarantees to users. The French are fully aware of the problems associated with the processing of their data: 49% of French people already wonder about the country in which their personal data is stored. 44% of French people trust a French or European player to manage their data (and only 2% trust their data to an American player). Finally, 66% of French people said they would be willing to give up a digital service if they expressed doubt about the use and storage of their data. A guiding principle based on the desire to ensure effective digital independence is inevitably becoming an outstanding quality for companies.

Third, reduce dependence on foreign decisions and resulting changes (from the point of view of domestic policy or for the purpose of applying national legislation). In turn, the decision to work with local players provides advantages such as proximity, attentiveness, efficiency and security [12].

It is obvious that information sovereignty is associated with the processes of informatization of society. Their consequence is the reaction of the legislator, following the path of active development of legal regulation of the sphere of information relations. This gives grounds to talk about the inclusion in the content of state sovereignty of such a component as information sovereignty [5, 6], which is already literally expressed in the legislation and official acts of some states2. In addition to the information sovereignty of the state, the information sovereignty of the individual is also distinguished, understood by analogy with the sovereignty of the individual [13, 7] as a designation of a certain degree of independence of a person from the state and from other people in the field of information relations.

The issue of digital sovereignty in the context of global social change means that there is a shift in the definition of sovereignty, which moves into a new sphere, and becomes a tool for establishing a dominant position at both the institutional and individual levels. The legal codification of this shift may either represent an attempt to maintain the existing status quo for the state and the individual, or create a formally legal means of transferring sovereign attributes to new participants.

From a political point of view, this also means that in the future it is possible to reconsider the functions of the state, including the exercise of power and its social purpose. At the personal level, this can lead to the loss of the individual's ability to define his personal characteristics as an expression of his autonomous existence and worldview.

Thus, we can conclude that the problem of digital sovereignty of the state and the individual has a deep semantic aspect, since the state, as the bearer of sovereignty, cannot exist without sovereign individuals - the individuals who make up its population and its government. This process of formally establishing digital sovereignty in modern conditions includes a wide range of possible scenarios, ranging from a revision and reassessment of the relationship between different types of sovereignty and ending with the possible disappearance of sovereignty as a key category of social order. In addition, there is a need to consider a new type of sovereignty - neurosovereignty, in the context of the implementation of digital technologies.

List of used literature

1. Sivash E.M. Questions of sovereignty are in the acts of Great French Revolution and the Holy Alliance.Problemy zakonnosti, 2011, (115): 228–237.
2. Bredikhin AL, Protsenko ED Principles and properties of State sovereignty. Akademicheskij yuridicheskij zhurnal, 2016, (3): 4–12.
3. Reut O. Ch. Adjectives of sovereignty. Sovereignty as an adjective. Polis. Political Studies, 2007, (3): 115–124. DOI: 10.17976/jpps/2007.03.09
4. Tokarev VA to the issue of the concept of the "sovereignty holder" (comparative legal analysis). Izvestiia vuzov. Pravovedenie, 2016, (3): 130–139.
5. Zorina EG Informational sovereignty of contemporary state and the main instruments of its ensuring. Izv. Saratov. Univ. (NS), Ser. Sociology. Political Science, 2017, 17(3): 345–348. DOI: 10.18500/1818-9601-2017-17-3-345-348
6. Matuzov NI to the question of the sovereignty of the individual. Pravovedenie, 1994, (4): 3–14.
7. Chernyak L.Yu. On the concept information sovereignty: theoretical and comparative and legal aspects. Siberian Law Herald, 2012, (3): 117–122.
8. Mass media and Internet: legal regulation problems, comp.Monakhov VN Moscow: EKOPRINT, 2003, 320.
9. Terenteva L.V. Concept of sovereignty in the conditions of global and information communication processes. Pravo. Zhurnal Vysshey shkoly ekonomiki, 2017, (1): 187–200. DOI: 10.17323/2072-8166.2017.1.187.200.
10. Simonov V.A. Sovereignty: the problems of subjects. Herald of Omsk University. Series «Law», 2016, (1): 54–68.
11. Bredihin AL, Protsenko ED Sovereignty as a legal category. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, 2011, (9): 142–151.
12. Boltanova ES, Imekova MP Genetic information in the system of objects of civil rights. Lex russica, 2019, (6): 110–121. DOI: 10.17803/1729-5920.2019.151.6.110–121.

13. Ruzanova VD Legislation in the field of personal data as an institution of information legislation. Iuridicheskii vestnik Samarskogo universiteta, 2019, 5(2): 15–22. DOI: 10.18287/2542-047X-2019-5-2-15-22.

Саниязова Еркемай Казбековна,
аспирант кафедры уголовного процесса и судебных экспертиз
e-mail: erkem_84@mail.ru
(Кыргызский национальный университет им. Ж. Баласагына, Кыргызская Республика)

ТАКТИКА ПРОИЗВОДСТВА ВЕРБАЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ КИБЕРПРАВОНАРУШЕНИЙ

Аннотация. Статья рассматривает тактику производства вербальных следственных действий, особенно допроса и очной ставки, в контексте расследования уголовных киберправонарушений. Автор обращает внимание на важность учета специфики механизма таких преступлений и подчеркивает роль специалистов в области телекоммуникаций и компьютерных технологий. Особое внимание уделяется различиям в допросах подозреваемых, обвиняемых, потерпевших и свидетелей, а также влиянию интеллектуального противодействия со стороны уголовных киберправонарушителей. Статья также затрагивает вопросы обработки информации, обнаруженной на носителях программного обеспечения, и управления временными ограничениями в информационном киберпространстве.

Ключевые слова: уголовные киберправонарушения, вербальные следственные действия, допрос, очная ставка, тактика расследования.

TACTICS OF VERBAL INVESTIGATIVE ACTIONS DURING THE INVESTIGATION OF CRIMINAL CYBER OFFENSES

Annotation. The article examines the tactics of conducting verbal investigative actions, especially interrogation and confrontation, in the context of the investigation of criminal cyber offenses. The author draws attention to the importance of taking into account the specifics of the mechanism of such crimes and emphasizes the role of specialists in the field of telecommunications and computer technology. Particular attention is paid to differences in the interrogation of suspects, accused, victims and witnesses, as well as the impact of intelligent counteraction by criminal cyber offenders. The article also touches on the issues of processing information found on software media and managing time constraints in information cyberspace.

Keywords: criminal cyber offenses, verbal investigative actions, interrogation, confrontation, investigative tactics.

С каждым годом уровень киберугрозы повышается, и преступники все более изощренно используют технологии для осуществления киберправонарушения. Это включает в себя кражу личных данных, финансовые мошенничества, кибершпионаж и другие формы киберпреступлений. В связи с этим, важно развивать и совершенствовать методы расследования уголовных киберпреступлений, включая вербальные следственные действия. Особенности киберпреступлений требуют от следователей не только глубоких знаний в области информационных технологий, но и умения эффективно взаимодействовать с цифровым пространством.

Одним из основных следственных действий как допрос и очная ставка подозреваемых (обвиняемых), в том числе при расследовании киберправонарушений, проводятся в соответствии со ст. 210 (Общие правила производства допроса), ст.218 (Очная ставка), а также в соответствии со ст. 215 УПК Республики Казахстан [1], если указанные следственные действия проводятся с участием несовершеннолетних.

Допрос и очную ставку при расследовании уголовных киберправонарушений можно отнести к одним из самых сложных следственных действий.

Среди ученых-юристов существует разногласие в трактовке понятия «очная ставка». Одна группа исследователей рассматривает очную ставку как особый вид допроса. Например, профессор М.Ч. Когамов, принадлежащий к этой группе, определяет очную ставку как продолжение и вариацию допроса, при этом она проводится с участием двух равноправных участников – допрашиваемых лиц [2, с. 125].

Другая группа ученых рассматривает очную ставку как самостоятельное следственное действие. Например, В.Е. Коновалова определяет очную ставку как особый вид следственного процесса, целью которого является сбор доказательств в рамках дела. Это действие заключается в одновременном допросе двух лиц (двух свидетелей, двух обвиняемых, свидетеля и обвиняемого) судебно-следственными органами. Основная задача очной ставки, согласно В.Е. Коноваловой, заключается в устранении существенных противоречий, выявленных в показаниях этих лиц, с целью достижения объективной правды [3, с. 23].

На основе вышеизложенных точек зрения, в контексте расследования уголовных киберправонарушений можно классифицировать очную ставку как одно из вербальных следственных действий, рассматривая ее как специфичную форму допроса. Этот вид действия представляет собой одновременный допрос двух ранее допрошенных лиц (подозреваемых, обвиняемых), в показаниях которых выявлены значительные противоречия.

Необходимо подчеркнуть, что подготовка к проведению допроса и очной ставки в рамках расследования уголовных киберправонарушений требует учета специфических нюансов. Пренебрежение этими особенностями может стать причиной возникновения трудностей у следователя и препятствовать эффективному проведению указанных следственных действий. Тактика проведения допроса в уголовных делах данной категории напрямую зависит от уникальности механизма совершения уголовных киберправонарушений, а также от положительных и отрицательных факторов, влияющих на этот процесс. Важно учи-

тывать, что допрос потерпевших и свидетелей по уголовным делам об уголовных киберправонарушениях отличается от допроса подозреваемых и обвиняемых. Особенности, связанные с механизмом преступления, оказывают влияние на выбор тактических методов проведения допроса.

Допрос (включая очную ставку) представляет собой эффективное средство для решения определенных тактических задач с точки зрения криминалистики:

– распознании лживых сведений, предоставляемых лицом, противодействующего следствию;

– проверки выдвинутых версий; определение прочности позиций, занятых допрашиваемыми на следствии;

– выявления ранее неизвестных обстоятельств, включая неизвестные эпизоды преступной деятельности, и т.д. [4, с. 160].

Как справедливо отмечает профессор П.В. Костин «преступления в сфере компьютерной информации в изолированной форме представляют собой редкое исключение, поскольку они чаще всего совершаются совместно с другими общественно опасными деяниями и обладают факультативным характером. Это объясняется тем, что при использовании компьютерной информации в качестве инструмента для совершения другого преступления, сама эта информация становится объектом общественно опасного деяния» [5, с. 6].

Для обеспечения информационной составляющей допроса в ходе досудебного расследования уголовных киберправонарушений требуются компетенции в области компьютерных технологий и глубокие знания нормативно-правовой базы, регулирующей нарушенные права. Например, М.А. Романенко «аргументируя важность проведения допроса при расследовании уголовных нарушений авторских прав в сфере программного обеспечения, выделяет, что в подготовке к допросу необходимо особое внимание уделять изучению законодательства, регулирующего предмет преступного посягательства, а также подготовке вопросов, охватывающих как событие уголовного правонарушения, так и сущность контрафактности копий и исходного материала» [6, с. 155].

В подготовительной фазе допроса, с целью ясного понимания обстоятельств совершенного уголовного киберправонарушения, следователь должен обратить внимание на специализированную литературу, посвященную использованным технологиям в уголовных киберправонарушениях, а также проконсультироваться с ИТ-специалистом, изучив справочники по компьютерной терминологии. Считаем мнение М.М. Менжеги обоснованным, поскольку она указывает на трудности, с которыми сталкивается следователь, не обладающий специфическими знаниями. Например, такому следователю может быть сложно самостоятельно различить сбой в работе оборудования или случайную ошибку от последствий действия вирусов. Также возможно затруднение в выявлении противоречий и лжи в показаниях, поскольку следователь может быть намеренно дезориентирован вопросами относительно значений терминов и возможностей устройств. В ходе расследования специалист по технологиям может предоставить поддержку следователю, помогая разрешить технические вопросы, такие как определение наличия копирования или модификации информации в процессе выполнения определенных действий, и другие аспекты [7].

Подобную точку зрения высказывают и А.Н. Яковлев с Н.В. Олиндер [8, с. 47], которые утверждают, что при расследовании уголовных преступлений, совершенных с использованием электронных платежных средств и систем, при проведении допроса (очной ставки) подозреваемых (обвиняемых) ими вероятно используются жаргонизмы и термины, понимание которых может быть неясным и непонятным для следователя. Однако эти термины могут указывать на конкретные методы совершения уголовных преступлений. Избавиться от таких недопониманий в ходе допроса (очной ставки) без участия специалиста практически невозможно.

Фактором, положительно влияющим на выбор тактики производства допроса, является наличие определённого объёма информации об уголовно-наказуемом событии, полученного из различных (процессуальных и не процессуальных) источников, например, оперативно-розыскных мероприятий и т. п. Кроме того, содержание преступного деяния таково, что при выяснении обстоятельств его совершения необходимо наличие знаний об особенностях механизма преступления, которые зависят от применяемых для его реализации орудий и средств (компьютерно-технические средства) [9, с. 72].

Широкий доступ к информации, особенно для тех, кто прекрасно разбирается в информационно-коммуникационных технологиях и особенностях работы в сетях телекоммуникаций, предоставляет обширные возможности для самообразования. Это включает в себя поиск информации о методах и тактике деятельности правоохранительных органов.

Данная ситуация часто приводит к конфликтам во время допросов подозреваемых по уголовным киберправонарушениям. В большинстве случаев допрашиваемые отказываются давать показания или предоставляют ложные сведения, минимизируя свою вину или вообще отрицая свою причастность к преступлению.

Уголовные киберправонарушения, как правило, характеризуются тщательным планированием. В случае обнаружения и доставления злоумышленника в органы для проведения следствия и допроса, он может обладать информацией о том, что известно следствию. В связи с этим преступник внимательно разрабатывает правдоподобную ложную версию. Дополнительно, он активно внедряет в эту версию специфическую терминологию, что дополнительно усложняет задачу следователя в выявлении лжи.

Поэтому следователю необходимо тщательно обдумать тактику, используемую во время допроса (очной ставки), и особенности документирования данного следственного действия. Вовлечение специалиста непосредственно в проведение следственного действия позволит: корректно формулировать вопросы на основе полученной информации в ходе допроса (очной ставки); обращать внимание на обстоятельства, которые могут быть искажены допрашиваемыми намеренно или по невнимательности; выбирать точные формулировки, которые вносятся в протокол следственного действия, и в некоторых случаях помогут установить психологический контакт с допрашиваемыми.

В ходе допроса подозреваемого применяется следующий подход: вначале предъявляются общие вопросы, такие как навыки и уровень компьютерной

грамотности, место работы, наличие компьютера дома и на работе, а также обязанности, связанные с рабочей деятельностью (в случае, если преступление связано с работой). Также освещаются цели и мотивы допрашиваемого, вопросы о возможном скрытии преступления и тому подобные. После этого следователь переходит к конкретным вопросам, касающимся непосредственно совершенного уголовного киберправонарушения.

В ходе расследования уголовных киберправонарушений, направленных против собственности, следователю необходимо выяснить следующее у подозреваемого: используемые программные и технические средства при совершении преступления; методы преодоления систем безопасности; способы получения несанкционированного доступа к компьютерной информации; методы скрытия неправомерного доступа; частоту и количество совершенных посягательств; использование служебного положения в процессе преступления; возможное групповое совершение преступления и методы снятия и обналичивания похищенных средств.

При расследовании дел о создании и использовании вредоносных программ следователь должен задать ряд дополнительных вопросов: была ли программа создана лично подозреваемым или заимствована из других источников; на каком оборудовании происходило разработка программы; для какой операционной системы предназначалась данная вредоносная программа; какие последствия должны были произойти от использования этой программы; каким образом предполагалось использование вредоносной программы; сколько и какие компьютеры были заражены; каким образом происходило заражение и другие уточняющие вопросы [10, с. 156].

На основании вышеизложенного отметим, что при проведении допроса (очной ставки) с обвиняемыми в уголовных киберправонарушениях особенно важно учитывать психологические особенности участников данных следственных действий. Необходимы навыки применения законных методов психологического воздействия на участников, а также контроль за их эмоциональным состоянием и взаимным психологическим воздействием, которое может оказываться как на самого следователя, так и на других участников.

Таким образом, важная тактическая информация о личности уголовного киберправонарушителя (-ей) в процессе допроса (очной ставки) должна включать в себя следующие сведения:

– уровне их технической подготовленности и компьютерных навыков; мотивах совершения уголовного киберправонарушения;

– их дифференциации в зависимости от локализации их преступной деятельности;

– информации размещённой в социальных сетях о самом себе; психологическом состоянии или информационных болезнях (зависимостях, фобиях).

Тактика проведения допроса в уголовных делах данной категории непосредственно определяется особенностями механизма совершения уголовных киберправонарушений, а также различными позитивными и негативными факторами.

Исходя из вышесказанного, можно заключить, что для следователя оптимальным будет выбор тактики проведения вербальных следственных действий (допроса, очной ставки) на основе:

1. Разумное использование и привлечение к специализированным знаниям в области телекоммуникационных систем, компьютерных технологий и компьютерной техники;

2. Применение знаний юридической психологии при анализе личности уголовного киберправонарушителя;

3. Учета особенностей интеллектуального противодействия со стороны уголовного киберправонарушителя(-ей);

4. Анализа содержания информации, обнаруженной на конкретном носителе программного обеспечения и специальных компьютерных программах;

5. Способности эффективно управлять временными ограничениями и быстро меняющейся обстановкой в информационном киберпространстве.

При этом необходимо учитывать различия в проведении допроса среди подозреваемых и обвиняемых по сравнению с потерпевшими и свидетелями в уголовных делах о киберправонарушениях. Особенности, связанные с механизмом совершенного уголовного правонарушения, будут влиять на выбор тактических приемов при проведении допроса.

Список использованной литературы

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V // Казахстанская правда. – 2014. – 10 июля.

2. Когамов М.Ч. Комментарий к Уголовно-процессуальному кодексу Республики Казахстан 2014 года. – Т. 2. – Особенная часть. – Алматы, 2015. – 1016 с.

3. Коновалова В.Е. Тактика производства очной ставки. – Харьков, 1955. – 38 с.

4. Образцов В.А., Топорков А.А. Подготовка и производство очной ставки // Следственные действия. Криминалистические рекомендации. Типовые образцы документов. – М., 2001. – 501 с.

5. Костин П.В. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики: автореф. ... канд. юрид. наук. – Н. Новгород, 2007. – 31 с.

6. Романенко М.А. Расследование преступных нарушений авторских прав в сфере программного обеспечения: монография. – Омск: Изд-во Омского гос. ун-та, 2008. – 246 с.

7. Менжега М.М. Методика расследования создания и использовании вредоносных программ для ЭВМ. – М.: Юрлитинформ, 2010. – 179 с.

8. Яковлев А. Н., Олиндер Н. В. Особенности расследования преступлений, совершенных с использованием электронных платежных средств и систем: научно-методическое пособие. – М, 2012. – 182 с.

9. Смирнова И.Г., Коломинов В.В. Тактические особенности производства осмотра по делам о мошенничестве в сфере компьютерной информации // Уголовное производство: процессуальная теория и криминалистическая практика:

материалы III международной научно-практической конференции, 24-25 апреля 2015 г., г. Симферополь-Алушта / отв.ред. М.А. Михайлов, Т.В. Омельченко. – Симферополь: КФУ им. В.И. Вернадского, 2015. С. 72–75.

10. Романенко М.А. Расследование преступных нарушений авторских прав в сфере программного обеспечения: монография. – Омск: Изд-во Омского гос. ун-та, 2008. – 246 с.

Сапарғалиев Жандос Нурбекович,
киберқауіпсіздік және ақпараттық технологиялар кафедрасының оқытушысы
з.ғ.м., полиция подполковнигі, e-mail: zh.sapargalyiev@mail.ru
(Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясы, Қазақстан Республикасы)

МОБИЛЬДІ ҚҰРЫЛҒЫЛАРДЫ ҚАРАП-ТЕКСЕРУМЕН АЛУДЫҢ ЕРЕКШЕЛІКТЕРІ

Аннотация. Ғылыми мақалада автор ұялы телефондардан деректерді талдау және ақпаратты қалпына келтіру сарапшы мен тергеуші қызметінің ажырамас құрамдас бөлігі болып табылады деген қорытындыға келеді. Бұл процедуралар дұрыс орындалса, құнды дәлелдемелерді бере алады және қылмыстық тергеуге көмектеседі.

Түйін сөздер: деректерді талдау, ақпаратты қалпына келтіру, ұялы телефондар, тергеуші, дәлелдеме, тергеу.

MOBILE DEVICE REVIEW FEATURES

Annotation. In the scientific article, the author comes to the conclusion that data analysis and recovery of information from mobile phones are integral components of the activities of an expert and investigator. When carried out correctly, these procedures can provide valuable evidence and assist in criminal investigations.

Keywords: data analysis, information recovery, mobile phones, investigator, evidence, investigation.

Ұялы байланыс желілерінің қарқынды дамуына және абоненттер санының күрт өсуіне байланысты соңғы жылдары «телефондық алаяқтық» фактілерінің саны белсенді өсуде және бұл қылмыстық әрекеттің жасалу механизмі өзгерістерге ұшырауды.

Бүгінгі таңда осы қылмыстардың келесі түрлері кең тарап жатыр:

1) қалалық телефонға немесе ұялы телефонға қоңырау алаяқ телефон шалып туысы немесе танысы, полиция қызметкері, күзетші және т.б. болып сөйлеседі, отбасы мүшесі жасаған құқық бұзушылық туралы хабарлайды, жанжалды шешу үшін ақша төлеуді ұсынады. Қылмыстың құрбаны көбінесе

егде жастағы әйелдер. Ақшаны қылмыстық топтың мүшесі немесе курьер (көбінесе такси жүргізушісі) алады;

2) қылмыскерлер ұялы телефонға қоңырау шалып немесе SMS - хабарлама жіберіп, жәбірленушіге ойнаған жүлденің «ұтысы» туралы хабарлайды және салықты, оны жеткізгені үшін ақшаны және т. б. төлеуді ұсынады;

3) хабарланатын СМС-хабарламаларды жіберу жүзеге асырылады пайдаланушының банктік карточкасы қылмыстық қол сұғушылық әрекеттері нәтижесінде бұғатталғаны туралы ақпарат және көрсетілген нөмір бойынша банк қызметкерімен байланысу ұсынылады. Банктің жалған қызметкері жәбірленушіге картаның паролін ашу үшін банкомат арқылы қандай комбинацияларды енгізу керектігін нұсқайды. Бұл ретте ақша қаражаты алаяқтың немесе оның сенімді тұлғасының шотына аударылады.

Мұндай қылмыстың субъектісі болып бұрын сотталғандармен IT мамандығы бар адамдар болып табылады.

Бұндай алаяқтық қылмыстарды тергеу кезінде маңызды дәлелдеме болып жәбірленушілерге хабарласу және СМС-хабарламаларын жолдау үшін пайдаланған ұялы телефондар болып табылады.

Олар иелері туралы және олардың байланыстары, өткен байланыс сеанстары, жіберілген және қабылданған хабарламалар туралы ақпаратты және өзге де криминалистикалық маңызы бар мәліметтерді қамтуы мүмкін және бас бостандығынан айыру орындарында және тінту жүргізу кезінде режимдік іс-шаралар нәтижесінде табылуы мүмкін.

Қазақстанда 2022 жылдың соңында 25,1 млн абонент тіркелді-бұл өткен жылмен салыстырғанда 3,3%-ға артық. Бұл дүниежүзілік желіге қол жеткізудің негізгі көзі болып табылатын Қазақстан Республикасындағы мобильді интернет. Мәселен, егер 2022 жылдың соңына қарай елде тіркелген интернеттің 2,9 млн абоненті болса, онда интернетке қол жеткізе алатын ұялы байланыс абоненттерінің саны бір жылда 3,1%-ға, 17,4 млн-ға дейін өсті. Қазақстандықтармен еліміздің қонақтарын мобильді байланыспен «Kcell» (Kcell және Activ сауда белгілері), «Мобайл Телеком-Сервис» (Tele2 мен Altel сауда белгілері) және «Кар-Тел» (Beeline сауда белгісі) үш оператор қамтамасыз етеді [1].

Мобильді құрылғы деп - қуат көзінен автономды жұмыс істейтін (мысалы, егерде өзінің аккумуляторлы батарейінен жұмыс істесе) және оның сенсорлық дисплей түріндегі типтік басқару органы мен шағын габаритті өлшемдері бар кез келген құрылғы түсіндіріледі. Біздің жағдайда құрылғының Интернет желісіне қосылуына мүмкіндік беретін GSM немесе Wi-Fi типті модульдердің болуы ерекше маңызды [2].

Қарастырылып отырған қылмыстық әрекеттер компьютерлік ақпаратты беру арқылы жасалатындықтан, цифрлық іздер түріндегі дәлелдемелік ақпараттың айтарлықтай үлесі электрондық тасымалдағыштарда сақталады. Сандық іздер адамның Интернет желісіндегі белсенді әрекетінен, әлеуметтік желілерде сөйлескенде, фотосуреттерді орналастырғанда, белгілі бір мазмұнды контентті жүктегенде, тауарларға, қызметтерге, хабарландыруларға ақы төлегенде және т. б. әрекеттерінен пайда болады [3].

Телефондарды алу және тексеру кезінде тактикалық ұсыныстарды ескеру қажет. Тергеуші (анықтаушы) алынатын объектілермен кез-келген әрекеттен аулақ болу керек, оның салдарын алдын-ала қарастыра алмауы мүмкін.

Алынған байланыс құралдарындағы ақпараттың тұтастығын және басқа іздерді қамтамасыз ету маманның кәсібилігіне байланысты, оның қатысуын мүмкіндігінше қамтамасыз ету қажет.

Алынатын байланыс құралдарының мазмұнын осы үшін арналмаған компьютерлік техниканы пайдалана отырып қарауға, әсіресе олармен қандай да бір іс-әрекеттер жасауға (оларға кез келген файлдарды жазуды жүзеге асыруға, қоңырау шалуға, смс-хабарламалар жіберуге) жол берілмейді.

Осы тергеу әрекетін жүргізу барысында материалдық іздер де (саусақ іздері, микрообъектілер және т. б.), сондай-ақ виртуалды (есірткі жарнамасы бар сайттарға кіру, пайдаланушының хат алмасу мұрағаты, электрондық төлем жүйелерінің шоттарын басқару, геолокация және т. б.) табылуы мүмкін, бұл толыққанды дәлелдемелік базаны қалыптастыруға ықпал етеді және оны пайдаланушыны ғана емес, сонымен қатар қылмыс жасауға қатысы бар басқа адамдарды әшкерелейді.

Қарап-тексеруді жүргізу кезінде арнайы білімі бар және арнайы бағдарламалық қамтамасыз етулермен жұмыс істей алатын арнайы білімі бар маманды пайдалануғада болады [4].

Процессуалдық тұрғыдан деректерді құрылғылардан әртүрлі жолдармен алуға болады:

– оқиға болған жерде қарауды жүргізу арқылы;

– қылмыстық іс аясында алынған құрылғыны қарап-тексеруді жүргізу кезінде;

– сот сараптамасын тағайындау және жүргізу арқылы.

Қарап-тексерулер жүргізу кезінде қажетті арнайы білімі бар, сондай-ақ мамандандырылған бағдарламалар мен аппараттық-бағдарламалық кешендерді пайдалана алатын маманды тартуға болады.

Тергеушінің ұялы телефонды қарап-тексеруі – бұл құрылғыдан дәлелдер алу үшін әртүрлі әрекеттерді орындау процесі. Негізгі мәселе – деректерді бастапқы күйінде тоқтату және бұзбау үшін процедураны сақтау. Ол үшін тергеушінің жеткілікті білімі болуы керек, сонымен қатар арнайы ұсыныстарды басшылыққа алуы керек.

Ұялы телефонды қарап-тексеру кезінде тергеуші заңдылық қағидаттарын сақтауға, құпиялылық пен жеке өмірге қол сұғылмаушылық құқығын ескеруге міндетті. Ұялы телефон қылмыстық істің бір бөлігі ретінде тінту қажет болған жағдайларда тергеу судьясынан қарап-тексеру жүргізуге санкцияның болуы тиіс. Мұндай құжаттарсыз тексеру заңсыз болуы мүмкін және пайдаланылған дәлелдер жарамсыз болуы мүмкін.

Тергеушінің ұялы телефонды қарап-тексеру процедурасы: тергеуші ұялы телефонды қарап-тексерген кезде алынған ақпараттардың тұтастығы мен дұрыстығын сақтау үшін белгілі бір сақтық шараларын сақтауы керек. Ұялы телефонды тексеру кезінде тергеуші келесі әрекеттерді басшылыққа алуы керек:

1. Ұялы телефонның сыртқы жай-күйін тексеру: тергеуші көрінетін зақымданулардың немесе сыртқы түрінің өзгеруінің бар-жоғын жазып, телефонның күйін тексеріп, құжаттауы керек.

2. Телефонның маркасымен моделін анықтау: тергеуші алынған ақпаратты одан әрі анықтау және өңдеу үшін телефонның маркасы мен моделін бекітуі керек.

3. SIM-картаны алу және арнайы құрылғыларға қосу: тергеуші ұялы телефоннан SIM картасын алып, оны әрі қарай зерттеу және деректерді алу үшін арнайы құрылғыларға қосуы керек.

4. Деректерді алу және талдау процесі: тергеуші ұялы телефоннан мәтіндік хабарлар, байланыс деректері, фотосуреттер және т.б. сияқты деректерді алу үшін арнайы бағдарламалық құралды пайдалануы керек. Алынған мәліметтер құжаттандырылып және өзгеру мен бүлінуден қорғалуы керек.

5. Жүргізілген қарап-тексеру туралы есеп жасау: телефонның физикалық жағдайы, алынған SIM-карта, алынған деректер және тергеуге пайдалы болуы мүмкін кез келген басқа ерекшеліктер туралы ақпаратты қоса алғанда, ұялы телефонды қарап-тексеру туралы тергеуші егжей-тегжейлі есеп жасауы керек.

Ұялы телефонға қарап-тексеруді жүргізу үшін тергеуші келесі құралдарды дайындауы керек:

Пинцет – SIM-картаны мұқият алу үшін немесе басқада ұсақ заттарды құрылғыдан алу үшін пайдаланылады.

Микросхемалық оқу құрылғысы (картридер) – SIM картадағы және ұялы телефонның ішкі жадында сақталған ақпараттарға қол жеткізуге мүмкіндік береді.

Тиісті бағдарламалық қамтамасыз етулері бар компьютер - ұялы телефоннан ақпаратты талдауға және алуға мүмкіндік береді.

Фото және видеоаппарат – құрылғының күйін және оның жағдайын бекіту үшін қолданылады [5].

Ұялы телефонды қарап-тексеру процедурасы келесідей жүргізілуі керек:

– ұялы телефонды барлық жағынан және экраннан, сондай-ақ оның ішіндегісін, соның ішінде ашық қосымшалар немесе хабарламаларды фотоға түсіру керек;

– мүмкіндік болса, құрылғының SIM картасын немесе басқа да элементтерін бөлшектеу және алу процесін көрсететін бейнежазба түсіру;

– SIM картаны және басқада іздерді құрылғыдан бүлдірмей іздерді алу үшін пинцетті пайдаланған дұрыс;

– қажет болса, SIM картадағы немесе ұялы телефонның ішкі жадында сақталған ақпаратты алу үшін чипті оқу құралын (картридер) пайдаланыңыз.

Ұялы телефонды компьютерге қоспас бұрын, құрылғының жұмысына және мәліметтердің сақталу қауіпсіздігіне әсер етпейтін құрылғының бүтіндігін және сыртқы зақымдарының жоқтығын тексеріңіз.

Ұялы телефонды компьютерге қосыңыз және оның мазмұнына қол жеткізу үшін тиісті бағдарламалық жасақтаманы іске қосыңыз.

Бағдарламалық қамтамасыз ету нұсқауларын орындау арқылы ұялы телефоннан барлық қажетті деректерді көшіріңіз және сақтаңыз.

Қажет болса, алынған деректерді талдаңыз және тергеу үшін пайдалы ақпарат алыңыз.

Тергеуші ұялы телефонды қарап-тексеруді аяқтағаннан кейін хаттама толтырып, алынған құрылғы мен деректердің сақталуын қамтамасыз етуі керек.

Ұялы телефондағы дәлелдерді іздеу, алу және бекіту: тергеу әрекеттері аясында тергеушімен қылмысқа қатысы бар ұялы телефонға қарап-тексеру жүргізіп дәлелдемелерді іздеуі, алуы және бекітуі қажет.

Ұялы телефонды тексеру кезінде тергеуші келесі ұсыныстарды ескеруі керек: тексеруді бастамас бұрын тергеуші құпия сөзді беру немесе құрылғының құлпын ашу туралы талап бар-жоғын анықтауы керек.

Тергеуші ұялы телефонды тексермес бұрын арнайы пломбаларды пайдаланып мөрлеп, нөмірлеуі керек.

Тексеру кезінде тергеуші құрылғыдағы деректердің бүлінуіне немесе өзгеруіне жол бермеу үшін мұқият болуы керек. Ол сенсорлық экрандарға зақым келтірмеу үшін фарфор пинцет сияқты ұялы телефондарды тексеруге арналған арнайы құралдарды қолдана алады.

Ұялы телефонда сақталған барлық қосымшаларды, хабарламаларды, фотосуреттерді, бейнежазбаларды және басқа деректерді егжей-тегжейлі тексеру қажет.

Ұялы телефоннан табылған маңызды дәлелдердің сол ұялы телефоннан табылғанын дәлелдеу мақсатымен, тергеуші фотосурет пен бейнежазба жүргізуі керек.

Жүргізілген тергеу шараларын растау үшін ұялы телефонды қарау уақыты мен күні, сондай-ақ тексеру кезінде жасалған барлық әрекеттер туралы ақпаратты жазу маңызды.

Ұялы телефонды тексергеннен кейін тергеуші оны арнайы қорғаныс пакетіне салып (фарадей сөмкесі), сараптама жүргізу үшін зертханаға жібермес бұрын мөр басуы керек.

Қажет болған жағдайда тергеуші ұялы телефонды егжей-тегжейлі зерттеу және цифрлық дәлелдерді алу үшін цифрлық криминалистика саласындағы сарапшылардан көмек сұрай алады.

Жоғарыда аталған барлық әрекеттерді орындау кезінде тергеуші ұялы телефоннан табылған дәлелдердің қауіпсіздігі мен дұрыстығын қамтамасыз етеді, бұл қылмыстық құқықбұзушылықты сәтті тергеудің маңызды элементі болып табылады.

Деректерді талдау және ақпаратты қалпына келтіру.

Деректерді талдау процесінде тергеуші әртүрлі әдістерді қолдана алады, соның ішінде метадеректерді талдау, келген-кеткен хабарламаларды, контактілер мен қоңырауларды талдау, фотосуреттер мен видеожазбаларды талдау, орнатылған қосымшалар мен интернеттегі әрекеттерін талдау.

Ақпаратты қалпына келтіру.

Жойылған файлдарды қарауды, қол жетімді емес жад аймақтарынан деректерді алуды, бүлінген файлдар мен кескіндерді қалпына келтіруді және жойылған іздеу және интернетті қарау тарихын қалпына келтіруді қамтуы мүмкін.

Деректерді сәтті талдау және ақпаратты қалпына келтіру үшін тергеуші арнайы бағдарламалық және аппараттық құралдарды қолдануы керек, сонымен қатар тиісті білім мен дағдыларға ие болуы керек. Мұндай жұмыс мұқият болуды, дәлдікті және әр жағдайға ерекше көзқарасты қажет етеді.

Деректерді талдау және ақпаратты қалпына келтіру айтарлықтай уақытты қажет ететінін және тергеушінің барлық әрекеттерін мұқият құжаттауды қажет ететінін ескеру маңызды. Деректерді дұрыс және толық талдау істе дәлел ретінде пайдаланылуы мүмкін маңызды фактілер мен жағдайларды анықтауға мүмкіндік береді.

Ұялы телефонды қарап-тексеру бойынша ұсыныстар.

Ұялы телефонды қарап-тексеру кезінде тергеуші келесі әдістерді ұстануы керек:

1. Тексеруді бастамас бұрын тергеуші материалдардардың толық көлемімен танысып, мобильді құрылғыда қандай ақпарат болуы мүмкін екендігі туралы алдын ала білуі керек.

2. Ұялы телефонды қарап-тексеру заңнамада көзделген барлық ережелер мен талаптарды сақтай отырып, сондай-ақ тұтастық пен құпиялылық қағидаттарын сақтай отырып жүргізілуі тиіс.

3. Қарап-тексеруден бұрын тергеуші пароль, деректерді шифрлау немесе биометриялық аутентификация сияқты қосымша қорғаныс механизмдерінің жоқтығына көз жеткізуі керек.

4. Қарап-тексеру кезінде тергеуші ұялы телефондағы барлық файлдар мен қосымшаларды мұқият және әдістемелік түрде зерттеп, фотосуреттерге, хабарламаларға және әлеуметтік желілердегі жазбаларға ерекше назар аударуы керек.

5. Ұялы телефонды тексеру кезінде тергеушінің барлық әрекеттері тексеруді жүргізу уақыты мен әдістемесі, сондай-ақ қаралған ақпарат көрсетіле отырып құжатталуы тиіс.

6. Ұялы телефонды қарап-тексергеннен кейін тергеуші қарап-тексеру фактісін арнайы хаттамада қолымен және толық жазумен куәландыруы тиіс, ол іске қоса тіркелуі тиіс.

7. Ұялы телефонды тексеру нәтижелері Қазақстан Республикасы ҚПК баптарында және басқа да нормативтік актілерде көзделген барлық ережелерді сақтай отырып, сот талқылауында дәлел ретінде ұсынылуы мүмкін.

Қорытындылай келе, деректерді талдау және ұялы телефоннан ақпаратты қалпына келтіру тергеушімен эксперт жұмысының ажырамас бөлігі болып табылады. Бұл процестерді дұрыс жүргізу маңызды дәлелдер алуға және қылмыстарды тергеуге көмектеседі.

Пайдаланған әдебиеттер тізімі

1. Более 25 млн абонентов сотовой связи зарегистрировано в Казахстане на конец 2022 года // https://turanpress.kz/obschestvo/6360-bolee-25-mln-abonentov-sotovoi-svjazi-zaregistrirovano-v-kazahstane-na-konec-2022-go.html.

2. Воронкова Д.К., Манучарян А.К. Осмотр и судебная экспертиза мобильного устройства в рамках расследований по уголовным делам // International Journal of Humanities and Natural Sciences, vol.7-2. С. 119–120.

3. Имангалиев Н.К. Правовые и организационные вопросы расследования уголовных правонарушений, совершенных в сети Интернет // Хабаршы— Вестник. 2022. № 1 (75). С. 37–41.

4. Вехов В.Б. Особенности следственного осмотра сотового радиотелефона // Расследование преступлений: проблемы и пути их решения. – 2015. – № 4. – С. 170–172.

5. Осмотр мобильного телефона следователем: образец, инструкция, правила // https://metiz-krepej.ru/minecraft/osmotr-mobilnogo-telefona-sledovatelem-obrazec-instrukciya-pravila.

Саранчин Дмитрий Владимирович,
старший преподаватель кафедры оперативно-разыскной деятельности
и оперативно-технических мероприятий органов внутренних дел
t14235dmitry@yandex.ru
(Тюменский институт повышения квалификации сотрудников МВД России, Российская Федерация)

ОРГАНИЗАЦИЯ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В КОНТЕКСТЕ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

Аннотация. Реализация личных прав и свобод возможна в достаточной степени только в условиях правового государства с высокоразвитыми органами власти. В первую очередь это касается правоохранительных органов, призванных защищать общественные и личные интересы от нарушений. Противодействие легализации (отмыванию) доходов, полученных преступным путем, такая категория дел, которая часто выходит за пределы одного государства. Соответственно, требуется запрашивать информацию об активах и банковских счетах, находящихся за границей.

Ключевые слова: обеспечение безопасности, противодействие легализации (отмыванию) доходов, международные организации, финансовый мониторинг, правоохранительные органы, международные договора, международные стандарты, денежные средства.

ORGANIZATION OF INTERNATIONAL COOPERATION IN THE CONTEXT OF COUNTERING THE LEGALIZATION (LAUNDERING) OF PROCEEDS FROM CRIME

Anotation. The realization of personal rights and freedoms is possible to a sufficient extent only in a State governed by the rule of law with highly developed authorities. First of all, this concerns law enforcement agencies designed to protect pub-

lic and personal interests from violations. Countering the legalization (laundering) of proceeds from crime is a category of cases that often goes beyond the borders of one state. Accordingly, it is required to request information about assets and bank accounts located abroad.

Keywords: security; countering the legalization (laundering) of income; international organizations; financial monitoring; law enforcement agencies; international treaties; international standards; money.

Обеспечение безопасности, как известно, – одна из основных потребностей человека. Реализация личных прав и свобод возможна в достаточной степени только в условиях правового государства с высокоразвитыми органами власти. В первую очередь это касается правоохранительных органов, призванных защищать общественные и личные интересы от нарушений. Следует отметить, что противодействие легализации (отмыванию) доходов, полученных преступным путем, такая категория дел, которая часто выходит за пределы одного государства. Соответственно, требуется запрашивать информацию об активах и банковских счетах, находящихся за границей. Информацию (например, о правах на землю, автомобилях, а также корпоративную информацию) посредством запросов об оказании взаимной правовой помощи.

1. Международные организации в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Наиболее важным направлением международного взаимодействия является участие государств в международных организациях, одна из задач которых – противодействие отмыванию преступных доходов и финансированию терроризма:

– ФАТФ (Группа разработки финансовых мер по борьбе с отмыванием денег). ФАТФ была учреждена США, Японией, Германией, Великобританией, Францией, Италией, Канадой и Европейской комиссией во время Парижской встречи на высшем уровне в июле 1989 г. по инициативе Президента Франции. В настоящее время членами ФАТФ являются 31 страна и 2 международные организации. Россия была принята в постоянные члены ФАТФ на пленарном заседании ФАТФ в июне 2003 г.

ФАТФ постоянно осуществляет:

– взаимные оценки в странах – членах ФАТФ на предмет соответствия национальных законодательств и действующей практики в области борьбы с отмыванием денег рекомендациям ФАТФ;

– исследования по выполнению своих рекомендаций (составляемые по итогам этих мероприятий отчеты и доклады руководство организации направляет странам-участницам для передачи своим компетентным органам);

– изучение в методологических и практических целях ситуации в странах, которые активно используются международной организованной преступностью для отмывания преступных доходов;

– организацию и проведение на регулярной основе в различных странах мира конференций, симпозиумов и семинаров по финансовым, юридическим и законодательным проблемам;

– публикацию перечня несотрудничающих стран и территорий в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

2. Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ). По инициативе России сформирована шестого октября 2004 г. Данная инициатива одобрена ФАТФ, МВФ, Всемирным банком и рядом государств.

ЕАГ является региональной группой по типу ФАТФ. Государствами - членами ЕАГ являются: Белоруссия, Казахстан, Китай, Кыргызстан, Россия, Таджикистан и Узбекистан. Среди наблюдателей можно выделить: Армению, Афганистан, Великобританию, Германию, Грузию, Италию, Молдову, США, Турцию, Украину, Францию, Японию, Литву, а также ФАТФ, Управление ООН по наркотикам и преступности, Всемирный банк, Международный валютный фонд, Исполком СНГ, ЕврАзЭС, Интерпол, Совет Европы (МАНИВЭЛ), ОБСЕ.

Основные задачи ЕАГ:

– содействие в распространении международных стандартов в сфере противодействия отмыванию денег и финансированию терроризма с учетом особенностей регионов;

– разработка и проведение совместных мероприятий в пределах компетенции подразделений финансовой разведки;

– оценка эффективности мер, принимаемых в целях противодействия отмыванию преступных доходов и финансированию терроризма;

– координация программ сотрудничества с международными организациями, рабочими группами и заинтересованными государствами;

– анализ тенденций (типологий) в сфере легализации преступных доходов и финансирования терроризма;

– обмен опытом противодействия таким преступлениям и оказание технического содействия государствам-членам.

3. Последней из наиболее известных международных организаций является Комитет экспертов Совета Европы по оценке мер противодействия легализации преступных доходов (далее – МАНИВЭЛ).

Российская Федерация – член МАНИВЭЛ, который действует по мандату Совета Европы и одновременно является региональной ФАТФ, отчитываясь перед ФАТФ.

В состав МАНИВЭЛ входят страны Совета Европы, не являющиеся членами ФАТФ. Страны Совета Европы, бывшие членами Комитета, но впоследствии ставшие членами ФАТФ, также имеют право остаться членами Комитета.

Каждая из стран-участниц представлена в Комитете тремя экспертами. Одна из основных форм работы Комитета – проведение взаимных оценок стран-участниц на основе Рекомендаций ФАТФ.

4. Содружество Независимых Государств (СНГ). В рамках деятельности Содружества Независимых Государств был принят ряд важных правовых актов, способствовавших развитию национальных систем финансового мониторинга на территории государств – бывших союзных республик:

– Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступностью (Москва, 25 ноября 1998 г.);

– Модельный закон «Об основах законодательства об антикоррупционной политике» (принят на XXII пленарном заседании МПА СНГ 15 ноября 2003 г.);

– Модельный закон «О борьбе с коррупцией» (принят на XIII пленарном заседании МПА СНГ 3 апреля 1999 г.);

– Модельный закон «О противодействии легализации (отмыванию) доходов, полученных незаконным путем» (принят на XII пленарном заседании МПА СНГ 8 декабря 1998 г.).

Среди функций Росфинмониторинга в сфере международного сотрудничества также необходимо выделить взаимодействие с компетентными органами иностранных государств на стадиях сбора информации, предварительного расследования, судебного разбирательства и исполнения судебных решений.

Росфинмониторинг в сфере финансового мониторинга предоставляет соответствующую информацию компетентным органам иностранных государств по их запросам или по собственной инициативе в соответствии с международными договорами Российской Федерации.

Передача компетентным органам иностранного государства информации, связанной с выявлением, изъятием и конфискацией доходов, полученных преступным путем, осуществляется в том случае, если она не наносит ущерба интересам национальной безопасности Российской Федерации и может позволить компетентным органам этого государства начать расследование или сформулировать запрос.

Информация, связанная с выявлением, изъятием и конфискацией доходов, полученных преступным путем, предоставляется по запросу компетентного органа иностранного государства при условии, что она не будет использована без предварительного согласия соответствующих органов государственной власти Российской Федерации, предоставивших ее, в целях, не указанных в запросе.

В свою очередь, органы государственной власти Российской Федерации, в том числе Росфинмониторинг, вправе направлять в компетентные органы иностранных государств запросы о предоставлении необходимой информации и давать ответы на запросы, сделанные указанными компетентными органами согласно международным договорам Российской Федерации.

Органы государственной власти Российской Федерации, осуществляющие деятельность, связанную с финансовым мониторингом, направившие запрос, обеспечивают конфиденциальность предоставленной информации и используют ее только в целях, указанных в запросе.

Росфинмониторинг в соответствии с международными договорами Российской Федерации и федеральными законами исполняет запросы компетентных органов иностранных государств, связанные с противодействием легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

В Российской Федерации в соответствии с международными договорами Российской Федерации и федеральными законами признаются вынесенные су-

дами иностранных государств и вступившие в законную силу приговоры (решения) в отношении лиц, имеющих доходы, полученные преступным путем.

В соответствии с заключенными Российской Федерацией международными договорами в России признаются и исполняются вынесенные судами иностранных государств и вступившие в законную силу приговоры (решения) о конфискации находящихся на территории Российской Федерации доходов, полученных преступным путем, или эквивалентного им имущества.

В заключении можно сделать вывод, что противодействие легализации (отмыванию) доходов, полученных преступным путем, в рамках одного государства малоэффективно. Правоохранительным органам будет полезна предварительная информация, полученная от прочих государственных органов, которая может быть полезна для восстановления маршрута движения денежных средств, а использование такого института как международные организации повышает ее эффективность.

Список использованной литературы

1. Протокол «О сотрудничестве между Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств-участников Содружества Независимых Государств и Совет руководителей подразделений финансовой разведки государств – участников Содружества Независимых Государств. М., 17 июня 2014 г.

2. Концепция развития сотрудничества министерств внутренних дел (полиции) государств – участников Содружества Независимых Государств на период до 2020 г. Астана, 10.09.2013 г.

Свиридова Жибек Сергеевна,
магистрант факультета послевузовского образования
капитан полиции, e-mail: sviridovazs@mail.ru
(Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, Республика Казахстан)

КВАЛИФИЦИРУЮЩИЕ ПРИЗНАКИ ВОВЛЕЧЕНИЯ В ЗАНЯТИЕ ПРОСТИТУЦИЕЙ И ОРГАНИЗАЦИИ ИЛИ СОДЕРЖАНИЯ ПРИТОНОВ ДЛЯ ЗАНЯТИЯ ПРОСТИТУЦИЕЙ ИЛИ СВОДНИЧЕСТВО

Аннотация. Правовая природа фактических обстоятельств, признаваемых в законе квалифицирующими, содержит свойство влиять на степень общественной опасности деяния. Система квалифицирующих признаков надстраивает над ней свой ряд отличительных качеств, содержанием которых являются интегративные свойства квалифицирующих признаков как признаков состава уголовного правонарушения. К ним, в частности, относится способность квалифицирующих признаков влиять на квалификацию содеянного и изменять пределы наказания.

Ключевые слова: Квалифицирующие признаки, уголовное правонарушение, сеть Интернет, вовлечение в занятие проституции, организация или содержание притонов, сводничество, вебкам.

QUALIFYING SIGNS OF INVOLVEMENT IN PROSTITUTION AND THE ORGANIZATION OR MAINTENANCE OF BROTHELS FOR PROSTITUTION OR PANDERING

Annotation. The legal nature of the factual circumstances recognized as qualifying in the law contains the property of influencing the degree of public danger of the act. The system of qualifying features builds over it its own number of distinctive qualities, the content of which are the integrative properties of qualifying features as signs of the composition of a criminal offense. These include, in particular, the ability of qualifying signs to influence the qualification of the deed and change the limits of punishment.

Keywords: qualifying signs, criminal offense, Internet, involvement in prostitution, organization or maintenance of brothels, pimping, webcam.

Квалифицированным составом уголовного правонарушения признается состав, предусматривающий отягчающие обстоятельства, наличие которых влечет повышенное наказание по сравнению с ответственностью за уголовное правонарушение, образующее основной состав. Иногда по степени тяжести совершаемого уголовного правонарушения и, соответственно, усиления наказания законодатель выделяет разновидности квалифицированного состава в виде составов уголовных правонарушений с особо отягчающими обстоятельствами.

Квалифицирующие признаки отражают внутривидовые различия, то есть различия между преступлениями одного вида, а не между преступными деяниями вообще [1, с. 72–73]. Придавая содеянному новое качество, квалифицирующие признаки изменяют законодательную оценку поведения виновного ввиду значительного изменения степени его общественной опасности, что получает свое внешнее выражение в иной квалификации, отличной от той, которая имеет место при отсутствии квалифицирующих признаков [2, с. 13].

Квалифицирующие признаки состава преступления следует отличать как от отягчающих, так и от смягчающих вину обстоятельств. Основное различие между ними заключается в том, что квалифицирующие признаки – это средство законодательной дифференциации ответственности и наказания. Смягчающие или отягчающие вину обстоятельства – это способ индивидуализации наказания. Они представляют суду возможность варьировать выбор вида и размера наказания в пределах санкции статьи, уменьшая его или увеличивая. Квалифицирующие признаки существенно повышают общественную опасность любого противоправного деяния.

Законодатель в качестве квалифицирующих признаков вовлечения в занятие проституцией, в ч. 2 ст. 308 УК Республики Казахстан предусмотрел следующие признаки: группой лиц по предварительному сговору либо неодно-

кратно, и в ч. 3 деяния совершенные частью первой или второй, совершенные преступной группой.

В ст. 309 УК Республики Казахстан организация или содержание притонов для занятия проституцией и сводничество, законодатель предусмотрел следующие квалифицирующие признаки: группой лиц по предварительному сговору, неоднократно, сопряженное с вовлечением несовершеннолетнего в занятие проституцией и в ч. 3 совершенные преступной группой [3, с. 176].

Рассмотрим каждый из вышеуказанных признаков в отдельности.

Проведенный анализ судебно-следственной практики дает нам основание утверждать, что определенная категория лиц, осужденных за рассматриваемое преступление, имела более широкие по сравнению с другими частными лицами возможности по вовлечению в занятие проституцией и по организации или содержанию притонов для занятия проституцией или сводничество.

Неоднократность отнесена к числу квалифицирующих признаков в связи с тем, что совершение одним и тем же лицом преступления два и более раза указывает на повышенную степень общественной опасности личности преступника, свидетельствует о наличии у него сформировавшихся антиобщественных установок, что, соответственно, влечет предусмотренные законом неблагоприятные правовые последствия.

В соответствии с ч. 1 ст. 12 УК Республики Казахстан, неоднократностью уголовных правонарушений признается совершение двух или более деяний, предусмотренных одной и той же статьей или частью статьи Особенной части настоящего Кодекса. Преступление и уголовный проступок не образуют между собой неоднократность.

Согласно ч. 2 ст. 12 УК Республики Казахстан уголовное правонарушение не признается совершенным неоднократно, если за ранее совершенное уголовное правонарушение лицо было осуждено либо освобождено от уголовной ответственности по основаниям, установленным законом[3, с. 30].

По сути, аналогичные разъяснения по данному вопросу содержатся в Нормативном постановлении Верховного Суда Республики Казахстан «О квалификации неоднократности и совокупности преступлений» от 25 декабря 2006 г.: «2. Неоднократность предполагает совершение одним и тем же лицом нескольких преступлений, предусмотренных одной и той же статьей или одной и той же частью статьи Особенной части УК. Уголовное правонарушение не признается совершенным неоднократно, если за ранее совершенное уголовное правонарушение лицо было осуждено, либо освобождено от уголовной ответственности по основаниям, установленным законом. Преступление и уголовный проступок не образуют между собой неоднократность» [4].

В соответствии с ч. 3 ст. 12 УК РК, не признается неоднократным продолжаемое уголовное правонарушение, то есть уголовное правонарушение, состоящее из ряда одинаковых противоправных деяний, которые охватываются едиными умыслом и целью и образуют в целом одно уголовное правонарушение. На данное обстоятельство также акцентирует внимание Нормативное постановление Верховного Суда Республики Казахстан «О квалификации неоднократности и совокупности преступлений» от 25 декабря 2006 г. [4].

Рассмотренные квалифицирующие признаки являются одинаковыми как в ст. 308 так и в ст. 309 УК РК, исключение составляет п. 3 ч. 2 ст. 309 УК «Организация или содержание притонов для занятия проституцией и сводничество» сопряженное с вовлечением несовершеннолетнего в занятие проституцией.

Вовлечение несовершеннолетнего в занятие проституцией является наиболее аморальным и более общественно опасным уголовно наказуемым деянием, так как причиняется физический или моральный вред молодому поколению.

Под вовлечением в занятие проституцией следует понимать целенаправленные действия вовлекающего по формированию у несовершеннолетнего желание (намерения, стремления) и готовности участвовать в занятии проституцией. При этом действия взрослого лица как указывается в п. 24 Нормативного постановления Верховного Суда от 11.04.2002 г. «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий», должны носить активный характер и могут сопровождаться применением психического или физического воздействия (побоев, уговоров, угроз и запугивания, подкупа, обмана и т.д.) [5].

В отличие от ст. 308 УК Республики Казахстан, в рассматриваемой норме потерпевшим является несовершеннолетний, т.е. лицо не достигшее 18 лет, которого вовлекли в занятие проституцией. Согласно ч. 2 ст. 31 УК Республики Казахстан уголовное правонарушение признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении уголовного правонарушения.

Преступление, совершенное преступной группой, дается в п. 24 ст. 3 УК Республики Казахстан, где говорится о том, что преступная группа – это организованная группа, преступная организация, преступное сообщество, транснациональная организованная группа, транснациональная преступная организация, транснациональное преступное сообщество, террористическая группа, экстремистская группа, банда, незаконное военизированное формирование.

Об организованности и устойчивости «преступной группы» могут свидетельствовать, в частности, такие признаки, как «стабильность их состава и организационных структур, сплочённость их членов, подчинение групповой дисциплине и указаниям, организатора и руководителя, постоянство форм и методов преступной деятельности, планирование и тщательная подготовка преступления, распределение ролей между соучастниками, обеспечение заранее мер по сокрытию преступления и сбыта имущества, добытого в результате преступной деятельности и т.п.».

В судебной практике вывод об устойчивом характере группы обосновывается также длительностью и многоэпизодностью преступной деятельности. Все участники «преступной группы» несут ответственность как исполнители, независимо от того, какую роль они играли при совершении уголовного правонарушения. Руководитель преступной группы (их создатель, разработчик преступных планов) должен нести ответственность за все совершенные группой уголовные правонарушения, если они охватывались его умыслом.

Если уголовное правонарушение совершено «преступной группой», то действия организатора, руководителя и членов преступной группы, участвовавших в вовлечении в занятия проституцией, организации или содержании притонов для занятия проституцией следует квалифицировать по совокупности статей, предусматривающей ответственность за вовлечение в занятия проституцией, организации или содержании притонов для занятия проституцией совершенное преступной группой (ч. 3 ст. 308 УК Республики Казахстан или ч. 3 ст. 309 УК Республики Казахстан) и соответствующей части ст. 262 УК Республики Казахстан, как создание и руководство организованной группой, преступной организацией, а равно участие в них. Такой вывод вытекает из анализа ч.ч. 4-5 ст. 31 УК Республики Казахстан, где говорится: «лицо, создавшее преступную группу либо руководившее ею, подлежит уголовной ответственности за организацию преступной группы и руководство ею в случаях, предусмотренных соответствующими статьями Особенной части УК, а также за все совершенные преступной группой преступления, если они охватывались его умыслом. Другие участники преступной группы несут уголовную ответственность за участие в ней в случаях, предусмотренных соответствующими статьями Особенной части Уголовного кодекса, а также за преступления, в подготовке или совершении которых они участвовали».

Как показало проведенное исследование, участники организованной группы содержателей притонов при осуществлении преступной деятельности распределяют между собой роли. Так, одни члены группы занимаются подбором помещения для организации притона, приискивают клиентов, другие вовлекают лиц в занятие проституцией. Таким образом, каждый из членов организованной преступной группы выполняет свою определенную роль в совершении преступления.

В последние годы «уличная» и «квартирная» проституция перешла в массажные салоны и оказывается под видом услуг эротического массажа или «body» массажа.

Организаторами салонов создаются определенные условия для этого, в частности, на выбор клиента предоставляются массажистки, обеспечивается уединение в отдельной комнате, предусматривается выполнение программ в обнаженном виде, соприкасающиеся с эрогенными частями тела клиента, допускаются действия сексуального характера руками, грудью и другими частями тела в целях доведения клиента до полного удовлетворения.

По факту, данные сексуальные услуги, оказываемые в салоне, являются завуалированной проституцией, которая выдается за эротический массаж без использования прямого полового сношения, вместе с тем, за дополнительную плату возможно получить и услуги интимного характера.

В целях получения большего дохода, организаторы открывают сети массажных салонов как в пределах одного города, так и по республике, активно размещая объявления в интернете и социальных сетях об оказании услуг разного вида эротического массажа.

Кроме того, как показывает практика организаторы арендуют под массажные салоны частные дома и квартиры в многоэтажных домах, где работая круглосуточно, нарушают тишину и общественный порядок.

Организация и деятельность таких массажных салонов сопутствует преступлениям, связанным с торговлей людьми, при этом, ничем не регулируется и не предусматривает никакой ответственности.

Кроме этого, действует большой сегмент сайтов с услугами вебкам («проституция онлайн» с использованием веб камер). Вебкам-бизнес – сфера бизнеса, построенная на общении веб-модели и наблюдателя в онлайн-видео-чате. Общение обычно происходит на платной основе, что является основной целью организаторов.

Как правило, администраторы портала размещают рекламные ссылки на Telegram и WhatsApp каналах, при вербовке обещают высокий доход с привлекательными условиями, гибким графиком работы, возможностью работать онлайн, в том числе для граждан других государств, что будет исключать возможность встретить знакомых или близких людей. Основной аргумент приводится на отсутствие физического контакта и независимость от места проживания.

Вместе с тем, по факту, в Telegram имеются каналы под названием «Слив видео вебкам моделей», что не исключает возможности дальнейшего шантажа девушек с принуждением их к такой работе. Кроме того, для вовлечения и принуждения девушек используются наркотические средства или психотропные вещества, их аналоги. В этой связи, требуется принятие мер по введению ответственности за вовлечение в занятие проституцией, организацию и содержание притонов для эротического массажа или «body» массажа, а также услуги вебкам («проституция онлайн» с использованием веб камер). Анализ показывает, что на территории Республики Казахстан действует большое количество сайтов, предлагающих интим-услуги.

Как правило, это сайты, куда желающие могут отправить анкету с объявлением об оказании интимных услуг разного характера. Не смотря на кажущиеся эффект частных анкет за большинством таких объявлений стоят преступные группы. Одно и то же объявление практически представляет несколько совершенно разных девушек, что рассеивает сомнения о частном характере анкет.

Сайты работают с повышенным уровнем безопасности и анонимности и рекламируют интимные услуги, в том числе и жертв торговли людьми широкой аудитории на сотнях и тысячах платформ, являясь теневым бизнесом и принося колоссальные доходы организаторам. Работа по актуализации страниц ведется постоянно, на страницах появляется новый контент, напоминая о своих услугах, ответы на заявки приходят незамедлительно. К примеру, @znakomstva_kazakhstana имеет 57 тыс. подписчиков, @brightgirls7 – 13 тыс. подписчиков и т.д., число подписчиков таких страниц постоянно растет.

Создание в интернете таких платформ не предусматривает никакой ответственности, подзаконные акты прописывают только блокирование сайтов.

Ежегодно блокируется по несколько тысяч сайтов порнографического характера (2019 г. - 3 069, 2020 г. - 1 638, 2021 г. – 5 416, 7 мес. т.г. 1 333).

Ряд каналов блокируется, но блокировка решает проблему только отчасти – новые страницы создаются практически сразу же, продолжая свою работу.

В этой связи, предлагаем в ч, 2 ст. 308 УК вовлечение в занятие проституцией и в ч. 2 ст. 309 УК РК организация или содержание притонов для занятия проституцией или сводничество, ввести квалифицирующий признак «посредством использования сетей телекоммуникаций, в том числе сети Интернет.

Список использованной литературы

1. Кудрявцев В. Н.Общая теория квалификации преступления. – М., 1972. – 352 с.

2. Кругликов Л. Л., Савинов В. Н. Квалифицирующие обстоятельства: понятие, виды, влияние на квалификацию преступлений. – Ярославль, 1989. – 210 с.

3. Уголовный кодекс Республики Казахстан. Практическое пособие – Алматы, «Издательство «Норма-К», 2023». – 276 с.

4. Нормативное постановление Верховного Суда Республики Казахстан «О квалификации неоднократности и совокупности преступлений» от 25 декабря 2006 г. https://adilet.zan.kz/rus/docs/P06000011S_

5. Нормативное постановление Верховного Суда Республики Казахстан «О судебной практике по делам об уголовных правонарушениях несовершеннолетних и о вовлечении их в совершение уголовных правонарушений и иных антиобщественных действий» от 21.04.2002 г. https://adilet.zan.kz/rus/docs/P02000006S_.

Солодина София Антоновна,
адъюнкт, e-mail: olgasonia1999@gmail.com
(Воронежский институт МВД России, Российская Федерация)

ЭЛЕКТРОННО-ЦИФРОВЫЕ СЛЕДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЭКОНОМИКИ

Аннотация. В настоящей статье рассматривают вопросы, связанные с преступлениями, совершаемых с использованием технических средств связи, информационно-телекоммуникационных технологий и компьютерной техники. В статье указаны некоторые особенности описания и значение электронно-цифровых следов, связанные с цифровыми технологиями в экономике.

Ключевые слова: информация, информационно-телекоммуникационные технологии, расследование преступлений, цифровые следы, интернет, право, преступник, экономика.

ELECTRONIC AND DIGITAL TRACES OF ECONOMIC CRIMES

Anotation. This article discusses issues related to crimes committed with the use of technical means of communication, information and telecommunication technologies and computer equipment. The article points out some features of the de-

scription and significance of electronic digital traces associated with digital technologies in the economy.

Keywords: information, information and telecommunication technologies, crime investigation, digital traces, internet, law, criminal, econimic.

Результатом каждого выхода пользователя в сеть «Интернет» с помощью компьютера, планшета, мобильного телефона или других цифровых устройств является образование следов его пребывания в указанной сети и речь эта идет о следах преступления. Данная категория используется для анализа взаимовлияния преступной деятельности и деятельности по расследованию преступлений.

Прежде всего, следует обратиться к вопросу понимания термина «следы преступления». Рассматривая следы преступления в широком смысле, имеются в виду обусловленные преступным событием все возможные модификации, любые отображения, любая информация. Иными словами, это любые (материальные, идеальные) изменения окружающей действительности, возникшие в связи с совершением преступных действий (подготовкой, совершением и сокрытием) и отражающие сущность и специфические особенности данного преступного события. Узкое понятие «следы преступления» означает следы-отображения как материально зафиксированные отражения внешнего строения одного объекта на поверхности другого объекта в результате их контактного взаимодействия.

По преступлениям следовая картина весьма специфична, поскольку формируется как традиционными (материальными и идеальными) следами, так и электронно-цифровыми.

След в преступлениях в сфере экономики представляет собой преобразования объектов материальной и виртуальной природы, обусловленные приложением к этим объектам воли преступника [1, с. 89].

Признавая решающую роль электронно-цифровых следов, кратко охарактеризуем традиционные следы, свойственные преступлениям в сфере информационных технологий.

Идеальными следами выступают мысленные образы, возникшие в связи с совершением преступления и зафиксированные в сознании и памяти преступника, потерпевшего, свидетелей. Процессуально идеальные следы отображаются в протоколе следственных действий [2, с. 84].

Несмотря на осуществление основного объема преступных действий в информационном пространстве (электронно-цифровом поле, внутри компьютерной системы или системы мобильной связи), рассматриваемые преступления оставляют и малочисленные материальные следы.

Материальными следами являются любые объекты материального мира, взаимодействующие на физическом или химическом уровне (в частности, следы рук, документы, орудия преступления) и воспринимаемые через органы чувств.

Можно выделить три группы материальных следов:

− следы-отображения (следы пальцев рук, следы ног, зубов, следы от инструментов и другие);

− следы-вещества (потожировое вещество преступника, оставленное на предметах обстановки преступного события, а также микрообъекты, запаховые следы);

− следы-предметы (программное обеспечение (ПО), средства компьютерной техники, средства кодирования и уничтожения информации; денежные средства, счета в банках, записные книжки и др.).

Прежде чем перейти к анализу нетрадиционных следов преступлений рассматриваемой категории, следует отметить, что среди исследователей данная разновидность следов получает различные наименования, в частности, электронные, виртуальные, цифровые, компьютерные, электронно-цифровые. Подобное многообразие терминологии объясняется тем, что до настоящего времени в науке единого подхода к пониманию следов в сфере экономики не сформировано.

Стоит учитывать, что такие следы остаются не только в результате компьютерных преступлений, но и любых других видов преступных деяний, совершенных с использованием информационных технологий.

Электронно-цифровые следы являются типичными для исследуемых преступлений. Образование данных следов происходит в процессе взаимодействия не имеющих формы информационных объектов в электронно-цифровой среде [3, с. 131].

Понятие электронно-цифровых (виртуальных) следов появилось в связи с тем, что специфика информационных технологий, применяемых на разных этапах криминальной деятельности, независимо от желания пользователя приводит к возникновению информации, которая может быть использована в целях расследования преступлений.

Считаем важным обратить внимание на то, что преступления в сфере информационных технологий оставляют различные электронно-цифровые следы.

Так, при свершении преступлений с использованием мобильных телефонов остаются следы в виде компьютерной информации коммутаторов сотовой связи, фиксирующих абонентскую активность, исходящие и входящие соединения. В данном примере в качестве электронно-цифровых следов рассматриваются сведения о местонахождении и соединениях абонента, следы в терминалах и банкоматах, SIM-карты, сами мобильные средства сотовой связи, а также прочие объекты, в которых может содержаться информация о месте пребывания преступника, способе совершения им преступления, переводе денежных средств.

Различные виды электронно-цифровых следов, могут находиться на сервере и в компьютерных системах мошенника и его жертвы. Подобные следы сохраняются на серверах и интернет-сайтах, мобильных и других электронно-цифровых устройствах потерпевшего и преступника.

Программные и технические средства образуют единую компьютерную систему, содержащую информацию в электронно-цифровой форме. Следовательно, информация, отображенная на носителях в результате использования сети Интернет, имеет значение электронно-цифрового следа.

Представляется важным обратить внимание на то, что для установления пользователя сети «Интернет» необходимо исходить из анализа пользовательских следов, но при этом обязательно учитывать алгоритмизированные следы. Только при соблюдении этого правила, по нашему глубокому убеждению, может быть точно установлен интернет-пользователь.

Специфика механизма образования пользовательских следов состоит в закономерности их формирования уже на этапе подключения к сети Интернет с помощью электронно-цифрового устройства. Данному сетевому подключению присваивается IP-адрес (уникальная символьная комбинация).

IP-адрес служит для идентификации электронно-цифрового устройства в интернете или локальной сети.

IP-адрес – это идентификатор, с помощью которого может передаваться информация между электронно-цифровыми устройствами в сети. Данный идентификатор содержит информацию о местоположении устройства и позволяет обеспечивать доступность его для связи.

Одним из главных свойств IP-адреса пользователя является его способность сохраняться в прежнем состоянии при переходе на другой ресурс и фиксироваться на сервере провайдера, обеспечивающего подключение, и администратора соответствующего Интернет-ресурса.

Еще одним свойством IP-адрес является его скрытость от пользователя.

Пользователь совершает различные действия на социальных ресурсах сети Интернет с присвоенным IP-адресом, в частности регистрируется на этих ресурсах, публикует там информацию, отправляет файлы.

Домен (доменное имя, доменный адрес) предполагает название сайта, его уникальный «адрес». Это определенная буквенная последовательность, обозначающая имя сайта или используемая в именах электронных почтовых ящиков.

Таким образом, можно заключить, что в сети Интернет пользователь и его компьютерное устройство оставляют следы в виде IP-адреса, логина, доменного имени.

На машинных носителях компьютерной информации остаются электронно-цифровые следы в виде:

1) изменений файловой структуры, системных областей носителей информации, постоянной энергонезависимой памяти;

2) изменений настроек компьютера и отдельных компьютерных программ;

3) нарушения работы компьютера и установленных на нем программ;

4) воздействия на конфиденциальную компьютерную информацию и систему ее защиты;

5) проявлений действия вредоносных компьютерных программ, в частности, видео- и аудио-эффекты, сообщения, выводимые на печатающее устройство.

Итак, можно сделать следующие вывод, что типичными для исследуемых преступлений являются электронно-цифровые следы, которые образуются в процессе взаимодействия информационных объектов, не имеющих формы, в электронно-цифровой среде. Понятие «электронно-цифровые следы» представляет собой информацию о событиях (действиях), отображенных посредством

электромагнитных взаимодействий в материальной среде в связи с ее возникновением, обработкой, хранением и передачей в телекоммуникационной сети, или передаваемые по каналам связи с помощью электромагнитных сигналов.

Список используемой литературы

1. Каминский А.М. Криминалистическая категория «след преступления» в анализе правонарушений в сфере компьютерной информации // Цифровой след как объект судебной экспертизы: материалы Международной научно-практической конференции. – М.: РГ-Пресс, 2020. – С. 85–90.

2. Першин А.Н., Сидорова К.С. Криминалистические основы установления пользователя информационно-телекоммуникационной сети Интернет // Вестник Университета имени О.Е. Кутафина. − 2019. − № 3. − С. 82–94.

3. Комиссарова Я.В. Понятие и классификация следов в криминалистике // Вестник Университета имени О.Е. Кутафина. − 2019. − № 3. − С. 131−141.

Спан Мадина Айткеновна,
докторант, советник юстиции, e-mail: mmakonti@mail.ru
(Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан)

О РЕАЛИЗАЦИИ ПРОЕКТА ПО СОЗДАНИЮ БУМАГИ С ВСТРОЕННЫМ ИНТЕГРИРОВАННЫМ ЧИПОМ

Аннотация. Настоящая статья посвящена вопросам изучения проблем использования фиктивных счет-фактур. Автором разработан проект по созданию бумаги с встроенным интегрированным чипом. Указанный проект позволит исключить факты использования фиктивных счет-фактур, путем чипирования бланка. Указанный бланк бумаги будет использовать как обычная бумага. Предложенный проект по использованию чипированной бумаги не имеет аналогов в Республики Казахстан.

Ключевые слова: бумага, чип, счет-фактура, модель, проект, безопасность, цифровые технологии.

ABOUT THE IMPLEMENTATION OF THE PROJECT TO CREATE PAPER WITH A BUILT-IN INTEGRATED CHIP

Annotation. This article is devoted to the study of the problems of using fictitious invoices. The author has developed a project to create paper with a built-in integrated chip. This project will eliminate the facts of using fictitious invoices by chipping the form. The specified blank paper will be used as plain paper. The proposed project on the use of chiped paper has no analogues in the Republic of Kazakhstan.

Keywords: paper, chip, invoice, model, project, security, digital technologies.

На данном этапе социально-экономического развития происходят глобальные перемены, связанные с цифровизацией экономики. В результате внедрения и широкого использования цифровых технологий возникают новые угрозы экономической безопасности как для государства, так и для его граждан.

В целях сокращения фактов уклонения от уплаты налогов необходимо, чтобы предприниматели отражали в декларациях фактическое осуществление финансово-хозяйственной операции. Отсутствует о фактическом совершении финансово-хозяйственной операции.

В настоящее время достаточно актуальной является проблема уклонения налогоплательщиков от уплаты налогов, а именно одним из способов уклонения от уплаты налогов является использование фиктивных счет-фактур.

Данный вопрос является актуальным и обсуждаемым среди научных исследований отечественных и зарубежных исследователей: Э.Р. Нуриманова, Е.В. Печерица [1], Ш.И. Алибеков [2], А.Ю. Головина [3] и др.

«Подделка документов широко используется при совершении налоговых преступлений. В результате подделка и использование заведомо подложных документов при совершении налоговых преступлений ставят перед правоприменительной практикой вопрос о необходимости пресечения совершения подобных преступлений» [4, с. 4].

Полезная модель относится к цифровым документам и предназначено для исключения фактов использования фиктивных счет-фактур.

Бумагу с встроенным чипом предполагается использовать в предпринимательской деятельности.

В процессе развития цифрового пространства одним из незаменимых алгоритмов функционирования правоохранительных органов, полагаем должны быть технологии чипирования бумаги, для сдачи отчетности счета-фактур.

Целью заявленной полезной модели является исключение фактов использования фиктивных счет-фактур, повышения качества работы уполномоченных органов в борьбе с теневой экономикой.

Техническим результатом заявляемой полезной модели является:

1. Разработка чипированной бумаги позволит вести учет коммерческих операций между продавцом и покупателем, а также исключит:

– изготовления фиктивных счет-фактур;

– получение фиктивно подтвержденных налоговых вычетов;

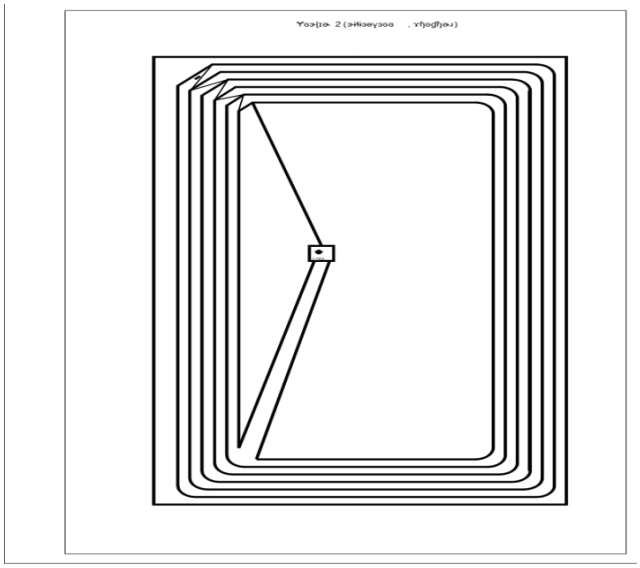
– причинение материального ущерба государственному бюджету.

2. Повышение эффективности работы уполномоченных органов по защите материальных интересов государства, а также в противодействии экономическим преступлениям, связанными с выпиской фиктивных счет-факту;

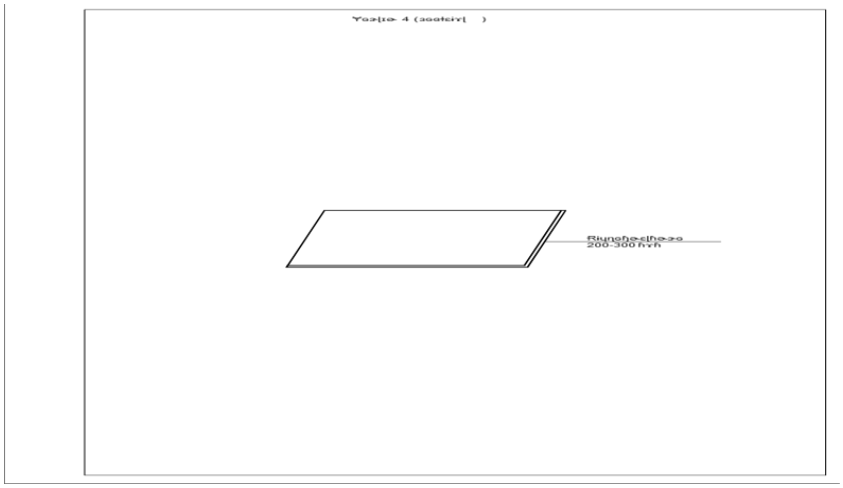
Описанные результаты достигаются путем встраивания RFID-чипа в лист бумаги, который не влияет на поверхность бумаги. При этом свойства ровной и бумаги сохраняются.

Такая бумага ничем не отличается от обычной и не требует для работы с ней специального оборудования. Нужная информация просто передается на встроенный в бумагу чип: (для подобного кодирования компания должна разработать специальную машину и учебные материалы).

На фиг. 1 показана бумага с встроенным интегрированным чипом (вид сверху).



Фигура 1 (Вид сверху)



На фиг. 2 бумага с встроенным интегрированным чипом (вид сбоку)

Согласно фиг. 1 и 2 бумага с встроенным интегрированным чипом собрана следующим образом.

Бумага с встроенным интегрированным чипом состоит из следующих структурных элементов: 1 – чип; 2 – субстрат; 3 – антенна (1); 4 – антенна (2).

Все составляющие компоненты устанавливаются в лист бумаги, при этом толщина бумаги не меняется и позволяет использовать ее как обычную бумагу.

Необходимо отметить, что встраиваемый чип достаточно тонкий и практически не заметен, его толщина составляет 200–300 мкм.

Каждая RFID-метка содержит уникальный идентификационный код, электронный серийный номер, который может быть считан дистанционно. Но, помимо простой идентификации, RFID-метки обеспечивают дополнительный уровень безопасности.

Эксплуатировать бумагу с встроенным интегрированным чипом предполагается в предпринимательской деятельности, при совершении сделок и для

подтверждения проведённых операций. Аналогичной модели, как предлагаемая бумага с встроенным интегрированным чипом, не существует.

По результатам проведенной работы автором получен патент на полезную модель под названием: «Бумага с встроенным интегрированным чипом» № 8624 от 10.11.2023 г.

Список используемой литературы

1. Нуриманова Э.Р., Печерица Е.В. Способы подлогов электроных финансовых документов и методы их выявления // Здоровье – основа человеческого потенциала: проблемы и пути их решения. – 2020. – №3. – С. 1422–1427.

2. Алибеков Ш.И. Установление фиктивных и подложных документов в процессе судебно-бухгалтерской экспертизы // Вестник Бурятского государственного университета. – 2012. – №2. – С. 31–35.

3. Головин А. Ю. Криминалистическая характеристика преступлений как категория современной криминалистики // Известия Тульского государственного университета. – 2012. – №1-2. – С. 43–55.

4. Кузнецов А.П., Князьков А.А. Бухгалтерские и иные документы как предмет налоговых преступлений: дискуссионные вопросы правоприменительной практики // Актуальные вопросы борьбы с преступлениями. – 2017. – № 1. – С. 4–8.

Тагаева Асель Манаповна,
начальник кафедры гражданско-правовых дисциплин
к.ю.н, доцент
(Академия МВД Киргизской Республики им. генерал-майора милиции Э. Алиева)

РОЛЬ ОВД КР В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Развитие мира на современном этапе имеет непосредственное влияние на состояние и уровень информационной безопасности. Значительно возрастает роль информационных отношений, которые являются одним из ключевых звеньев деятельности правоохранительных органов и институтов гражданского общества, связанных с созданием, хранением, преобразованием и использованием информации.

Ключевые слова: развитие, информационная безопасность, информационные отношения, правоохранительные органы, гражданское общество.

ROLE OF THE KR ATS IN ENSURING INFORMATION SECURITY

Annotation. The development of the world at the present stage has a direct impact on the state and level of information security. The role of information relations, which is one of the key links in the activities of law enforcement agencies and civil society institutions related to the creation, storage, transformation and use of information, is significantly increasing.

Keywords: development, information security, information relations, law enforcement agencies, civil society.

Процесс развития информационно-коммуникационных технологий стал определяющим фактором их глобального внедрения и использования во всех сферах жизни, что предъявляет особые требования к регулированию и решению вопросов в сфере информационной безопасности.

Информационная безопасность Кыргызской Республики является одной из составляющих национальной безопасности Кыргызской Республики и влияет на состояние защиты национальных интересов Кыргызской Республики в различных сферах жизнедеятельности общества и государства. Деятельность ОВД КР в современных условиях неразрывно связана с использованием высоких технологий. Как отмечает Е.Н. Завгородний: «в настоящее время происходит активное создание новых и модернизация ныне эксплуатируемых информационных ресурсов, централизация и подведение под единый формат представления и формирования разрозненных банков данных, которые позволяют сотрудникам ОВД различных направлений деятельности своевременно получать актуальные сведения, необходимые для выполнения своих функциональных обязанностей». Существующие проблемы и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных вызовов и направлены не только против физических лиц, бизнеса, государственных органов, но и против государства в целом.

Угрозы в деятельности ОВД по обеспечению информационной безопасности принято классифицировать на внешние и внутренние. Внешние связаны с разведывательной деятельностью иностранных государств и функционированием на территории Кыргызской Республики филиалов различных организаций и торговых представительств, которые пытаются получить несанкционированный доступ к информационным объектам или данным, которые находятся под охраной ОВД КР. По нашему мнению, сюда же следует отнести деятельность криминальных структур, которые также делают попытки получить такого рода данные. К внутренним угрозам информационной безопасности ОВД относят:

Нарушение руководителями и сотрудниками подразделений ОВД КР регламента хранения, обработки и распространения информации. Такие нормы специально разработаны для работы с охраняемыми данными как для информации, хранящейся на электронных носителях, так и для бумажных экземпляров.

Умышленные действия персонала, которые направлены на незаконное завладение, несанкционированный доступ, изменение или уничтожение информации. Непреднамеренные ошибки, в силу халатного отношения к выполнению профессиональных обязанностей по обеспечению информационной безопасности, которые привели к нарушению целостности и нормам распространения защищаемых данных. Неисправность технических средств обработки данных, нерегулярное обслуживание техники, которые впоследствии повлекли за собой утечку охраняемых данных.

Анализ выявленных угроз позволяет сформулировать следующие предложения по совершенствованию деятельности органов внутренних дел в сфере обеспечения информационной безопасности:

1. Ввести обязательное обучение основам информационной безопасности сотрудников ОВД КР, получивших доступ к секретной информации в силу занимаемой должности.

2. Ввести специальный курс «Информационная безопасность» для изучения лиц, проходящих первоначальную подготовку и сотрудников, проходящих профессиональную подготовку и переподготовку.

3. При увольнении сотрудника из ОВД КР немедленно аннулировать его право доступа к информационным ресурсам, с подписанием акта о неразглашении сведений, ставших известными в силу профессиональной деятельности.

4. В целях подготовки IT-специалистов высокого уровня, организовать их обучение в учреждениях соответствующего профиля, с предварительным подписанием трудового договора или контракта с указанием обязательного срока дальнейшего прохождения службы в ОВД КР.

Перечень предложенных средств не является исчерпывающим. Необходимо совершенствование организации деятельности ОВД КР, а также объединение усилий всех участников, заинтересованных в обеспечении информационной безопасности на национальном уровне: правоохранительных органов, предпринимательской среды, институтов гражданского общества.

Тафинцев Павел Анатольевич,
старший преподаватель кафедры кибербезопасности
и информационных технологий,
м.ю.н., майор полиции, p.tafintsyev@kpa.gov.kz
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

Фидель Петр Михайлович,
доцент кафедры административного права
и административной деятельности ОВД,
к.ю.н., подполковник полиции
(Восточно-Сибирский институт МВД России, Российская Федерация)

ОТДЕЛЬНЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ СЛЕДОВАТЕЛЯ ПРИ ОБНАРУЖЕНИИ И ИЗЪЯТИИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

Аннотация. В данной статье рассматриваются некоторые особенности работы лица осуществляющего досудебное расследование по обнаружению и фиксации электронно-цифровых следов в рамках расследования уголовных дел, подробно анализируются специфические методы и инструменты, применяемые следователем при обнаружении и фиксации цифровых следов, а также их признаки и значения в уголовном деле.

Ключевые слова: электронно-цифровые следы, фиксация цифровых следов, обнаружение цифровых следов на носителях информации.

CERTAIN ASPECTS OF THE INVESTIGATOR'S ACTIVITY IN THE DETECTION AND SEIZURE OF DIGITAL EVIDENCE

Annotation. This article discusses some features of the work of a person conducting a pre-trial investigation on the detection and fixation of electronic digital traces in the investigation of criminal cases, analyzes in detail the specific methods and tools used by the investigator in the detection and fixation of digital traces, as well as their signs and meanings in a criminal case.

Keywords: electronic digital footprints, fixation of digital footprints, detection of digital footprints on media.

В настоящее время уголовные правонарушения, совершаемые в сети Интернет осваивают все новые формы, используя в большинстве случаев бесконтактные способы оплаты товаров и услуг. Электронно-цифровые следы играют все более важную роль в расследовании уголовных правонарушений. В современной цифровой эпохе, почти каждое уголовное правонарушение имеет связь с электронными устройствами и сетевыми технологиями. Лицо осуществляющее досудебное расследование по обнаружению и фиксации электронно-цифровых следов играет ключевую роль в раскрытии уголовного правонарушения.

Наилучшим вариантом для более грамотной фиксации в рамках проведения проверки, оперативно-розыскных мероприятий, направленных на выявление информации доказательственного характера, является участие специалистов в области информационной безопасности [1]. Всеобъемлющая цифровизация человеческой жизнедеятельности не могла не отразиться на таком негативном социальном явлении, как преступность, а, следовательно, и на способах противодействия этому явлению. Развитие компьютерных технологий, мобильной связи, сети Интернет по всему миру привело к тому, что современный человек уже не мыслит себя без использования электронных технических средств и тех возможностей, которые они дают. Соответственно, каждый пользователь сети оставляет следы своих действий и присутствия, даже если они носят правомерный характер. Данные следы называются цифровыми.

Сегодня преступления, совершаемые с использованием компьютерных и сетевых компьютерных технологий, показывают невероятный рост, что, несомненно, является большой угрозой для рядовых граждан и головной болью для правоохранительных органов. Каждый день мы сталкиваемся с угрозой стать жертвой интернет-мошенничества, информационной блокады, компьютерного шпионажа, фишинга и других преступлений в сфере информатизации и связи. Причины тому различные: распространенность средств информатизации, смещение фокуса бизнеса на предоставление услуг в дистанционном формате, слабое знание гражданами основ информационной безопасности и, соответственно, смещение интересов преступных элементов в информационную сферу [2].

В случае обнаружения цифровых следов на носителе информации, необходимо обязательное привлечение специалиста в области информационной безо-

пасности. Обнаружение цифрового следа требует соблюдения процессуальной части его изъятия в соответствии с уголовно-процессуальным законодательством Республики Казахстан, а также принятия всех необходимых мер по обеспечению информационной безопасности с целью сохранения значения цифрового следа для уголовного дела.

Кроме того, необходимо соблюдать надежную и последовательную цепочку доказательств. Это означает что каждый этап проведения следственного действия должен быть отражен в протоколе в соответствии с уголовно-процессуальным законодательством Республики Казахстан и зафиксирован таким образом чтобы избежать подделки или изменения доказательств.

Также существуют различные инструменты и программы, которые специализированны для фиксации и изъятия цифровых следов. Это могут быть средства восстановления данных, программы для анализа метаданных, программы для определения законных прав на доступ к информации и другое. Применение таких программ облегчает процесс фиксации и изъятия цифровых следов и улучшает его эффективность, но при этом нельзя забывать в случае применения данных программ в обязательном порядке это должно быть отражено в протоколе следственного действия.

Один из важных аспектов фиксации и изъятия цифровых следов – это сохранение исходных данных в неизменном состоянии. Цифровые следы могут быть легко модифицированы или удалены, поэтому необходимо применять специализированные методы сохранения целостности данных, чтобы минимизировать риск потери или искажения информации имеющая значение для расследования дела. В целом, фиксация и изъятие цифровых следов – это сложный и многогранный процесс, который требует соблюдения норм и правил, наличия специальных навыков и использования специализированного программного обеспечения.

Список использованной литературы

1. Колычева А.Н. Фиксация доказательственной информации, хранящейся на ресурсах сети интернет: дис. … канд. юрид. наук. М., 2018. 199 с.

2. Полевик И.А. Понятие цифровых следов преступления [Электронный ресурс] // URL: https://legalbook.ru/765-ponjatie-cifrovyh-sledov-prestuplenija.html.

Толепбергенов Абилгазы Сматович,
магистрант факультета послевузовского образования
полковник полиции
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Казахстан)

ОБ АКТУАЛЬНОСТИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ ГОСУДАРСТВА

Аннотация. Успешное современное государство не только учитывает потребности и обстоятельства настоящего, но и должно извлекать уроки из про-

шлого, даже если оно было неудачным. Это предполагает признание ошибок прошлого, которые привели к потере государственности, поражению в военных и экономических состязаниях, неблагоприятным исходам операций государственных структур. Для того чтобы прошлое никогда не повторилось, необходимо изучать его опыт.

Ключевые слова: оперативно-розыскная деятельность, развитие, противодействие, эволюция, оптимизация.

ON THE RELEVANCE OF OPERATIONAL AND INVESTIGATIVE ACTIVITIES AT THE CURRENT STAGE OF STATE DEVELOPMENT

Annotation. A successful modern state not only takes into account the needs and circumstances of the present, but must also learn lessons from the past, even if it was unsuccessful. This implies recognizing the mistakes of the past, which led to the loss of statehood, defeat in military and economic competitions, unfavorable outcomes of operations of state structures. In order to ensure that the past is never repeated, it is necessary to study its experience.

Keywords: operational and investigative activity, development, counteraction, evolution, optimization.

Обсуждая вопросы, связанные с выработкой стратегической перспективы в построении государства, необходимо углубиться в анализ органических компонентов, которые формируют его основу. Помимо традиционных аспектов, таких как развитие национальной экономики, создание эффективной финансовой и налоговой системы, а также организация вооруженных сил, критическую роль в структуре государства играют правоохранительные органы. Эффективное управление ими и максимальное использование их потенциала являются неотъемлемой частью успешной реализации внутренней политики государства, особенно в контексте их оперативно-розыскной деятельности.

Формирование правоохранительных органов несет в себе более широкий смысл, чем просто создание структуры для обеспечения общественной безопасности. Это стратегический элемент, который должен быть органично вписан в общую концепцию развития государства. Оперативно-розыскная деятельность этих органов становится ключевым инструментом для осуществления контроля и поддержания законности в обществе [1, с. 76].

Неотъемлемой частью формирования стратегии государства является внимание к процессу управления правоохранительными органами. Эффективное руководство должно учитывать сложившиеся вызовы и угрозы, а также обеспечивать интеграцию правоохранительных структур в общую систему государственного управления. Ключевыми аспектами являются координация деятельности органов, оптимизация использования ресурсов и обеспечение высокого профессионализма сотрудников [2, с. 193].

Важным моментом является также умелое использование потенциала правоохранительных органов в рамках внутренней политики государства. Опера-

тивно-розыскная деятельность становится инструментом, способствующим противостоянию преступности, обеспечению национальной безопасности и соблюдению прав граждан.

В контексте оперативно-розыскной деятельности представляется важным выделить акцент на фундаментальных этапах этого процесса, начиная от получения информации и заканчивая принятием соответствующих мер на основе анализа предоставленной достоверной информации. Всесторонний анализ оперативной работы, таким образом, включает в себя комплексный подход к информационному процессу, который предполагает накопление, обработку, анализ и последующее использование данных в целях эффективной борьбы с преступностью.

Оперативные подразделения, прежде всего, ориентированы на выявление, предотвращение и раскрытие преступлений. Непреложным условием для выполнения данной задачи является наличие оперативных данных о преступнике и преступлении. Без этого компонента невозможно рассматривать успешное выполнение поставленных перед оперативными структурами задач.

Анализ эффективности оперативно-розыскной деятельности включает в себя не только технические и технологические аспекты, но и фокусируется на чрезвычайной важности полного и всестороннего освещения деятельности субъекта правонарушения. Это становится неотъемлемой частью процесса предотвращения противоправного поведения. Всестороннее изучение преступника, включая его характер, мотивацию и методы деятельности, предоставляет оперативным подразделениям ключевые инсайты для эффективного контроля и нейтрализации преступных угроз [3, с. 703].

Предварительная информация о преступлении и его исполнителе, являющаяся базой для последующего успешного расследования, выступает в качестве стартовой точки для оперативных мероприятий. Она служит основой для формирования стратегии и тактики борьбы с преступностью, а также обеспечивает преемственность в оперативных действиях, предлагая подробный обзор источников преступной деятельности.

В контексте совершенствования механизмов противостояния преступности и защиты граждан от уголовных посягательств, имеет смысл уделить внимание наращиванию эффективности негласной поисковой работы оперативных подразделений. Особое значение приобретает использование возможностей оперативно-технических структур, что предполагает внедрение современных технологий и методик для усовершенствования тактики раскрытия и расследования преступлений.

Негласная поисковая работа, в качестве ключевого элемента в оперативной деятельности, требует тщательного анализа и оптимизации. Оперативные подразделения должны активно внедрять передовые технологии для максимизации эффективности своей работы. Это включает в себя использование современных информационных систем, технических средств наблюдения, аналитических инструментов и других средств, обеспечивающих эффективное и целенаправленное сбор и анализ информации.

На сегодняшний день существует активный стремительный прогресс в области оперативно-технических возможностей. Применение передовых технологий, таких как системы искусственного интеллекта, биг-дата анализ, и кибернетические средства, предоставляет уникальные возможности для более точного и оперативного реагирования на преступные явления. Важным аспектом в этом контексте является не только внедрение новых технологий, но и обеспечение необходимой квалификации оперативных сотрудников для использования современных инструментов [4, с. 176].

Законодательство, на своей стороне, направлено на активное развитие новых подходов и методов работы оперативных подразделений, что включает в себя не только адаптацию к современным вызовам и угрозам, но и внедрение передовых форм и методов, которые были успешно апробированы как в отечественной, так и зарубежной оперативной практике.

Стратегия обновления тактики и методики работы подразумевает постоянное изучение и внедрение передовых научных и практических достижений в области борьбы с преступностью.

В свете современных вызовов и динамичного развития информационных технологий, оперативно-розыскная деятельность приобретает новые масштабы и направления, особенно в контексте противодействия киберпреступности. Актуальность данной темы усиливается не только быстрым технологическим прогрессом, но и постоянно увеличивающимся уровнем сложности кибератак, ставящих под угрозу информационную безопасность общества.

Оперативно-розыскная деятельность, направленная на противостояние киберпреступности, требует от оперативных подразделений не только высокой квалификации, но и постоянного адаптивного подхода. Важным компонентом становится понимание не только традиционных форм преступности, но и особенностей виртуального пространства, где киберпреступники оперируют с использованием сложных технологий и алгоритмов.

Существующая реальность вынуждает оперативные структуры активно внедрять современные методы анализа и мониторинга цифровых следов, тем самым эффективно выявляя и предотвращая кибератаки. Развитие оперативно-розыскной деятельности в сфере киберпреступности требует глубокого понимания технических особенностей современных киберугроз, а также умения оперативников оперировать информацией в виртуальном пространстве.

Одним из важных аспектов в этом контексте является сотрудничество с экспертами в области кибербезопасности и специалистами по анализу цифровых данных. Интеграция современных методов кибераналитики, использование средств машинного обучения и искусственного интеллекта позволяют повысить эффективность оперативных мероприятий в борьбе с киберпреступностью [5, с. 319]. Кроме того, неотъемлемой частью оперативно-розыскной деятельности в контексте киберпреступности становится обеспечение информационной безопасности, как на государственном, так и на корпоративном уровне. Разработка и внедрение превентивных мер, обучение персонала в области кибергигиени, а также регулярное обновление технических средств защиты становятся необходимыми шагами в обеспечении устойчивости киберпространства.

С увеличением зависимости общества от цифровых технологий и Интернета, проблема киберпреступности становится более острой и сложной. Оперативно-розыскная деятельность в этом контексте требует не только совершенствования методов анализа и пресечения кибератак, но и развития специализированных компетенций у оперативных сотрудников.

Оперативные подразделения, занимающиеся борьбой с киберпреступностью, должны активно внедрять передовые методы кибераналитики, что включает в себя мониторинг сетевого трафика, анализ цифровых следов, и применение интеллектуальных систем для обнаружения нештатных ситуаций в сети.

Таким образом, оперативно-розыскная деятельность в контексте противодействия киберпреступности предполагает комплексный подход, включая технические, правовые и организационные аспекты. Современные оперативные структуры должны постоянно совершенствовать свои методы и инструменты, чтобы эффективно противостоять быстро развивающимся угрозам в виртуальном мире.

Список использованной литературы

1. Левашов С.А. Оперативно-розыскная деятельность как вид правоохранительной деятельности // Студенческий вестник. – 2021. – № 19-3 (164). – С. 76–77.

2. Османов А.А., Дациева Х.Г. Связь и соотношение уголовно-процессуальной и оперативно-розыскной деятельности в раскрытии и расследовании преступлений // Закон и право. – 2022. – № 4. – С. 192–194.

3. Прудников С.С., Парфенов А.В. Некоторые аспекты организации оперативно-розыскной деятельности органов внутренних дел в особых условиях // Научный аспект. – 2023. – Т. 6. – № 6. – С. 700–706.

4. Коныш С.П. Проблемные вопросы оперативно-розыскной деятельности: с учетом анализа законодательства стран ближнего зарубежья // Закон и право. – 2022. – № 3. – С. 174–177.

5. Вытовтов А.Е. Значение результатов оперативно-розыскной деятельности как средств доказывания в уголовном судопроизводстве // Проблемы экономики и юридической практики. – 2020. – Т. 16. – № 2. – С. 317–321.

Тугелбаев Улан Еркинович,
преподаватель кафедры кибербезопасности и информационных технологий
м.ю.н., капитан полиции, kpa.ulan.20@gmail.com
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова, Республика Каахстан)

ОСОБЕННОСТИ ПРОФИЛАКТИКИ НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ, С ИСПОЛЬЗОВАНИЕМ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Аннотация. В статье рассматриваются уголовные правонарушения, связанные с незаконным оборотом наркотических средств, психотропных веществ,

совершаемых посредством использования электронных информационных ресурсов. Анализируется статистика количества лиц, занимающихся распространением наркотических средств с использованием телекоммуникационных систем. Автором представлены актуальные пути совершенствования профилактических мероприятий по предупреждению преступлений в сфере незаконного оборота наркотических средств, с использованием телекоммуникационных систем.

Ключевые слова: незаконный оборот наркотических средств, профилактика, сеть Интернет, уголовные правонарушения, ответственность.

FEATURES OF PREVENTION OF ILLICIT DRUG TRAFFICKING, USING TELECOMMUNICATION SYSTEMS

Annotation. The article deals with criminal offenses related to the illicit trafficking of narcotic drugs and psychotropic substances committed through the use of electronic information resources. The statistics of the number of persons involved in the distribution of narcotic drugs using telecommunication systems are analyzed. The author presents current ways to improve preventive measures to prevent crimes in the field of illicit drug trafficking using telecommunication systems.

Keywords: illicit drug trafficking, prevention, Internet, criminal offenses, liability.

Одним из значимых негативных факторов, оказывающих влияние на здоровье нации и нормальное позитивное развитие современного казахстанского общества, демографическое положение, экономическое состояние, политику и в целом на правопорядок, является наркотизация населения, особенно несовершеннолетних и молодежи [1].

Вместе с тем, активное освоение высоких технологий, открытость Казахстана мировому сообществу привели к незащищенности детей от противоправного контента в информационно-телекоммуникационной сети Интернет, усугубили проблемы, связанные с торговлей детьми, бесконтактным незаконным оборотом наркотиков, детской порнографией, педофилией и проституцией. Информационная база сети Интернет с каждым годом только увеличивается, а сам интернет для некоторых пользователей становится зависимостью. Это обусловлено тем, что виртуальная реальность действует на психику в семь раз сильнее, чем наркотические средства.

По данным Департамента по противодействию наркопреступности МВД Республики Казахстан в 2022 году заблокировали 1493 сайта и задержали 632 человека, занимающихся распространением наркотических средств с использованием телекоммуникационных систем. Это администраторы и создатели чат-ботов, фасовщики, закладчики, организаторы нарколабараторий и трафаретчики [2]. Также установлены 84 интернет-магазина и чат-бота в мессенджерах. С начала 2023 года список заблокированных пополнили еще 69 интернет-платформ, где распространяли запрещенные вещества.

Для повышения эффективности борьбы с наркобизнесом по поручению Главы государства разработан соответствующий Комплексный план по борьбе с наркоманией и наркобизнесом в Республике Казахстан на 2023 – 2025 годы. Его основными целями являются снижение оборота особо опасных видов наркотиков, в том числе синтетических, внедрение системы раннего выявления и учета наркозависимых, повышение компетенции и укрепление материально-технической базы уполномоченных органов [3].

Неслучайно, несмотря на огромные усилия и экономические затраты, приведшие к улучшению физического, психического и нравственного здоровья молодежи Казахстана, реальное количество преступлений в сфере незаконного оборота наркотиков, их тяжесть и число несовершеннолетних, принимающих участие в их совершении, незначительно, но ежегодно только возрастает. В настоящее время наркотизм в подростковой и молодежной среде рассматривается как социальное бедствие и ключевой детерминант корыстной и корыстно-насильственной преступности. При этом в сфере здравоохранения данная проблема способствует смертности населения и препятствует реализации комплексных государственных социально-экономических, демографических и миграционных программам по увеличению средней продолжительности жизни и естественному приросту населения нашей страны, социально-экономическому развития страны, страдает репродуктивная способность будущих поколений.

В современных условиях быстрого развития высокотехнологичных средств массовой информации нередки случаи вовлечения несовершеннолетних в незаконный оборот наркотических средств, психотропных веществ или их аналогов посредством сети Интернет. Подростки гораздо более информированы о возможностях сети Интернет и других средств массовой коммуникации, и это обстоятельство активно используется лицами, вовлекающими несовершеннолетних в сферу незаконного оборота наркотиков. С учетом расширения сферы криминального бизнеса в глобальной компьютерной сети Интернет (появления возможности практической неограниченных возможностей сбыта с помощью сети «Интернет», современных анонимных мессенджеров, таких как Viber, WhatsApp, Telegramm, VPN) такие показатели являются катастрофическими.

Перечень уголовных правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ, совершаемых посредством использования электронных информационных ресурсов:

1) незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка либо сбыт наркотических средств, психотропных веществ, их аналогов посредством использования электронных информационных ресурсов (п. 5 ч. 3 ст. 297 УК);

2) склонение к потреблению наркотических средств, психотропных веществ, их аналогов посредством использования электронных информационных ресурсов (п. 3 ч. 2 ст. 299 УК);

3) пропаганда или незаконная реклама наркотических средств, психотропных веществ или их аналогов, прекурсоров с использованием средств массовой

информации или электронных информационных ресурсов (п. 4 ч. 2 ст. 299-1 УК).

Предупреждение уголовных правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ, совершаемых посредством использования электронных информационных ресурсов – деятельность правоохранительных, иных государственных органов по своевременному обнаружению и устранению либо нейтрализации (обезвреживанию, взятию под оперативный контроль) причин и условий, способствующих совершению таких уголовных правонарушений.

Основные угрозы (причины и условия), способствующие совершению уголовных правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ посредством использования электронных информационных ресурсов:

– отсутствие необходимых международных и национальных правовых институтов, а также механизмов правового эффективного правового регулирования интернет-пространства;

– отсутствие у уполномоченных достаточных технических возможностей по контролю над пользователями электронных информационных ресурсов (сети Интернет);

– наличие широких возможностей цифровой конспирации, сокрытия цифровых следов незаконных действий в сети Интернет, чем активно пользуются лица, вовлеченные в цифровой наркобизнес;

– широкие возможности организации транснациональных схем сбыта наркотических средств посредством использования конфиденциальных цифровых ресурсов (программ обмена сообщениями Telegram, WhatsApp и т.д.);

– высокий уровень конспирации в структуре и организации деятельности преступных групп в сфере цифрового наркобизнеса (зачастую участники не знакомы друг с другом, не осведомлены о личности соучастников, их местожительстве и местонахождении);

– ограниченные технические и кадровые возможности правоохранительных органов в организации эффективного контроля интернет-пространства, своевременного выявления, пресечения и раскрытия цифровых наркопреступлений.

– интенсивное развитие химических и фармацевтических технологий в области производства и оперативной модификации синтетических наркотических средств, психотропных веществ и их аналогов.

Меры предупреждения уголовных правонарушений, связанных с незаконным оборотом наркотических средств, психотропных веществ, совершаемых посредством использования электронных информационных ресурсов:

– организация профилактической пропаганды о вреде наркотических средств и психотропных веществ для здоровья граждан (особенно среди целевых групп потенциальных потребителей – в организациях с высокой концентрацией молодежи) с привлечением СМИ и молодежных блогеров;

– внедрение технологий анализа больших данных (Big Data) в сфере выявления и пресечения цифровых наркопреступлений; общее усиление аналитиче-

ской работы по выявлению закономерностей в сфере деятельности преступных групп, осуществляющих наркопреступления с использованием цифровых технологий;

– организация и активное развитие волонтерского движения в сети Интернет по выявлению фактов цифровой наркопреступности (с привлечением популярных в молодежной среде блогеров и активистов);

– вовлекать работников химического и фармацевтического сектора к деятельности по противодействию изготовления наркотических средств и психотропных веществ (прежде всего, синтетического происхождения);

– организовывать рейдовые, оперативно-поисковые мероприятия по выявлению, пресечению фактов сбыта и приобретения наркотических средств, психотропных веществ по методу «тайниковых закладок».

В современных условиях для повышения эффективности борьбы с фактами преступного вовлечения подростков в сбыт наркотиков посредством сети Интернет, рекомендуется:

– во-первых, снизить возраст уголовной ответственности за сбыт наркотиков до 14 лет (внести изменения в ч. 2 ст. 15 УК РК), одновременно установив пожизненное лишение свободы в качестве уголовного наказания взрослым лицам (от 18 лет) за совершение любых наркопреступлений по УК РК. Только так можно кардинально переломить ситуацию с наркоугрозой для детей;

– во-вторых, сотрудникам территориальных отделов ювенальной полиции рекомендуется активизировать внимание на мониторинге информационных ресурсов сети Интернет (изучение страниц социальных сетей на предмет наличия контента, свидетельствующего о склонности подростка к наркотизации), создавая команды волонтёров в общеобразовательных организациях, высших учебных заведениях, которые совместно с педагогами, психологами, социальными службами, сотрудниками ювенальной полиции и общественными организациями будут проводить мониторинг аккаунтов социальных сетей и выявлять факты противоправных действий в сфере незаконного оборот наркотиков;

– в-третьих, недостатки правового регулирования отдельных вопросов противодействия распространению в информационном пространстве сети Интернет запрещенной информации указывают на необходимость принятия нормативного правового акта, который будет устанавливать требования к интернет-компаниям по осуществлению ими мониторинга контента сети и удалению вредной информации из интернета, а также обяжет операторов мобильной связи разграничить пользователей по возрастному критерию (до 18 лет и старше) с одновременным ограничением для первой возрастной категории доступа к сайтам криминогенного характера.

Список использованной литературы

1. О наркотических средствах, психотропных веществах, их аналогах и прекурсорах и мерах противодействия их незаконному обороту и злоупотреблению ими: Закон Республики Казахстан от 10 июля 1998 г. № 279-I // Ведомости Парламента Республики Казахстан. – 1998. – № 17-18. – Ст. 221.

2. МВД: Более 1500 сайтов с рекламой наркотиков заблокировали в Казахстане [Электронный ресурс] // URL: https://bizmedia.kz/2023/02/27/mvd-bolee-1500-sajtov-s-reklamoj-narkotikov-zablokirovali-v-kazahstane/.

3. Об утверждении Комплексного плана по борьбе с наркоманией и наркобизнесом в Республике Казахстан на 2023-2025 годы [Электронный ресурс]: постановление Правительства Республики Казахстан от 29 июня 2023 г. № 508 // URL: https://adilet.zan.kz/rus/docs/P2300000508.

Тусупбеков Қайрат Рысбекович,
жедел-іздестіру қызметі кафедрасының аға оқытушылары
полиция подполковнигі

Исмаилов Ғани Мейрханович,
жедел-іздестіру қызметі кафедрасының оқытушылары
полиция подполковнигі, e-mail: ord.feliks@bk.ru

(*Қазақстан Республикасы ІІМ Б. Бейсенова атындағы Қарағанды академиясы, Қазақстан Республикасы*)

ЖАСАНДЫ ИНТЕЛЛЕКТІҢ ЖЕДЕЛ–ІЗДЕСТІРУ ҚЫЗМЕТІНДЕГІ БОЛАШАҒЫ

Аннотация. Аталған мақалада жедел-іздестіру қызметі қызметінің алдында тұрған міндеттерді шешу барысында жасанды интеллект жүйесін дамытуды алға қойған мәселердің бірі болып отыр. Қазіргі цифрлық даму заманында қылмыстарды ашуда, ескертуде жасанды интеллек жүйесін алға қойып отырмыз. Жедел-іздестіру қызметінде жасанды интеллектің алатын орны, ол негізінен ақпараттарды жинау, сақтау және оларды өңдеу үшін қолданылады, яғни бұл дегеніміз ақпараттық-аналитикалық болжамдарды құрып, бағыт-бағдар беру болып табылады.

Түйінді сөздер: жедел-іздестіру қызметі, жасанды интеллект, ішкі істер органдары, қылмыстық құқық бұзушылықтар, есептеу платформасы, биометриялық мәліметтер.

THE FUTURE OF ARTIFICIAL INTELLIGENCE IN OPERATIONAL SEARCH ACTIVITIES

Annotation. In this article, one of the issues that raised the development of an artificial intelligence system in the process of solving the tasks facing the activities of the operational-search service is considered. In modern times of digital development, we are putting forward artificial intelligence systems in solving crimes and warning. The place occupied by artificial intelligence in operational-search activities is mainly used for collecting, storing information and processing it, that is, it means creating and guiding information and analytical forecasts.

Keywords: operational-search activities, artificial intelligence, internal affairs bodies, criminal offenses, computing platform, biometric data.

Қазіргі уақытта ғылым мен техниканың заманауи дамуы қылмыспен күресу құралдары мен әдістерінің өзгеруіне әкеледі. Біздің еліміздің әртүрлі қызмет салаларында жасанды интеллект жүйесін (бұдан әрі – ЖИ) дамыту оның өзектілігінің, тиімділігінің және соның салдарынан ЖІҚ жүзеге асыру кезінде ІІО пайдалану үшін қажеттілігінің артып келе жатқанын көрсетеді.

Мемлекет басшысы Қ-Ж. Тоқаев Digital Bridge форумында сөйлеген сөзінде: «Жасанды интеллект енді ғылыми фантастика емес, ол біздің шындыққа айналды. Біздің көз алдымызда жаңа дәуір басталды. Жасанды интеллект технологиясының әсері электр қуаты мен интернеттің ашылуы сияқты революциялық болып табылады. Оның адам өмірінің форматын толығымен өзгертуге, процестерді автоматтандыруға және ауқымды айтарлықтай экономикалық құндылық жасауға мүмкіндігі бар. Сарапшылардың кейбір бағалаулары ЖИ-дің жаһандық экономикаға әлеуетті үлесі жаһандық жалпы ішкі өнімнің төрттен бірін құрауы мүмкін дейді» [1].

Жасанды интеллект (ЖИ) – бұл нақты, алдын ала белгіленген функцияларды орындауға және есептерді шешуге арналған есептеу платформасы, кез келген – визуалды, акустикалық, мәтіндік және т.б. ақпаратты цифрға айналдыру құрылғысы, бұл цифрды статистика және дискретті Есептеу математикасы әдістерімен өңдеу және адамға интуитивті түрде жауап алу [2, 63 б.].

Дәл осы жасанды интеллект ақпараттарды жинауға, сақтауға және өңдеуге негіз болады. ЖИ технологиясының мүмкіндіктерін белсенді түрде енгізілуі тиіс салалардың бірі ол жедел-іздестіру қызметі болып табылатынына күмән жоқ.

Қазіргі уақытта әлемде ЖИ-ің дамуының екі негізгі бағыты бар [3].

Бірінші бағыты – «әмбебап» (күшті) жасанды интеллект деп аталады, ол адамды толығымен алмастыра алады, қазіргі уақытта әлі зерттелуде және оны қолдану перспективалары толығымен анық емес.

Екінші бағыты – «әлсіз» деп аталатын жасанды интеллект, оның негізінде толық автоматтандырылған жүйелер жасалады, ол соңғы уақытта өте қарқынды дамып келеді. Осы бағыт аясында ЖИ адамды алмастырмайды, бірақ матрицалық және статистикалық әдістер негізінде тануға, қарым-қатынас орнатуға байланысты нақты мәселелерді шешеді.

Жедел-іздестіру қызметіне қатысты ЖИ-ің мүмкіндіктері негізінен ақпаратты жинау, сақтау және өңдеу үшін қолданылады; әртүрлі аналитикалық және болжамды модельдерді құру, сондай-ақ байланыс пен өзара әрекеттесуді қамтамасыз ету.

Қарқынды дамып келе жатқан әлемде ЖИ қылмысқа қарсы күресте ЖІҚ-ің тиімді құралына айналады. Бұл, ең алдымен, жасанды интеллектке пара беру немесе оны бір нәрсеге сендіру, анықталған қылмысты жасыру мүмкін еместігімен байланысты. ЖИ қабылдаған шешімдерді өзгерту немесе қайта конфигурациялау, қиын нақты алгоритмдерге байланысты.

Мұндай жүйелер басқа елдерде өздерінің тиімділігін көрсетті. Қазіргі уақытта АҚШ жасанды интеллект зерттеулерінде әлемдік көшбасшы болып табылады. АҚШ полициясының аналитикалық-жағдайлық орталықтарында фотосуреттер, дауыстық деректер және т.б. сияқты әртүрлі мәліметтерді қамтитын тұлғалар туралы ақпаратты жинақтау, сақтау және өңдеу үшін бағдарламалық-аппараттық орта жабдықталған.

2007 жылы Нью-Йоркте 100-ден астам шашыраңқы деректер көздерін біріктіретін орталықтандырылған қоғамдық қауіпсіздік операциялық орталығы құрылды. Бейнебақылау камералары, патрульдік машиналар, полицияға қоңырау шалу және т.б. сияқты әртүрлі көздерден алынған ақпарат орталыққа келіп, әмбебап форматқа айналады. Содан кейін бұл ақпарат массиві талданады, құрылымдалады және пайдаланушылардың сұраныстарына сәйкес таратылады. Өңдеушілердің айтуынша, бірыңғай ақпарат қоймасын құру қаладағы қылмысты төмендетуге мүмкіндік берді. Сонымен қатар, ақпарат көздерінен жедел маңызды деректерді іздеу сервисі құрылды, олар өздерінің бытыраңқылығына, әртүрлі нысандары мен үйлесімсіздігіне байланысты бұрын құрылымдалмаған: азаматтардың өтініштері, полицияның түрлі есептері, 911 нөміріне келіп түскен телефон қоңырауларының жазбалары, қамауға алу хаттамалары және т.б.

Бұл деректердің барлығы біріктірілмегендіктен олардағы қажетті мәліметтер мен өзарақатынастарды анықтау қиынға соқты. Орталықты құрудың нәтижесінде полиция жұмысының тиімділігін арттырды [4, 100 б.].

ЖІҚ-ін жүзеге асыру кезінде ЖИ-нің аналитикалық және болжамды мүмкіндіктері өте өзекті болып табылады.

Сонымен, АҚШ-тың көптеген қалаларында (мысалы, Лас-Вегаста) қылмысты анықтайтын және ықтимал уақыты мен орнын болжайтын деректерді талдау жүйелері енгізілген. Жасалған қылмыстар туралы есептерді пайдалана отырып, құқық бұзушылық жасау ықтималдығы жоғары аймақтарды анықтайды, бұл учаскелерді картада бөледі және жергілікті полиция қызметкерлеріне жолдайды [5].

ЖІҚ-де жасанды интеллект мүмкіндіктерін пайдаланудың тағы бір перспективалық бағыты басқа елдерде тиімді жұмыс істейтін технологиялар болып табылады, бұл нақты уақыт режимінде қылмыстардың алдын-алу және алдын-алу бойынша аналитикалық әрекеттерді автоматты түрде орындауға мүмкіндік береді. Атап айтқанда, АҚШ-та қылмыстарды интеллектуалды ескертетін жүйе, «Domain Awareness» қызмет етеді.

Ол көшедегі камералардан, құқық қорғау органдарының сенсорларынан, радарларынан ақпараттарды жинап және талдайды. Сонымен қатар нақты уақыт режимінде күдіктілерді ұстау кезін немесе олардың басқа әрекеттерін, сондай-ақ бір қарағанда анық емес нәрселерді түсіріп тіркеуге мүмкіндік береді [6].

ЖІҚ саласында ЖИ технологияларын тиімді қолдану қылмыстарға, оның ішінде ақпараттық-телекоммуникациялық технологияларды пайдалана отырып жасалатын қылмыстарға неғұрлым сапалы және тиімді қарсы іс-қимылды қамтамасыз етуге мүмкіндік береді.

Сонымен бірге, жалпы құқық қорғау қызметінде және атап айтқанда, ЖІҚ-де ЖИ жүйелерінің жұмыс істеуі толығымен жүйелі емес және бірқатар мәселелерді шешуді талап етеді.

Мәселен, қылмыстарды ашу процесіне Қазақстан Республикасы ІІМ АТҚД (ДИТС), жедел бөліністер және ЖКД (жедел-криминалистикалық департамент) қазіргі уақытта ашық, сақтаумен және жүйелеумен айналысатын барлық есептерді, жүйелендіретін, сақтайтын, жасырын және ашық тіркеулерді талдау жүргізу мақсатында бірге интеграциялау қажет.

Сонымен қатар, олар Интернет желісіндегі автоматтандырылған іздеу және талдау жүйесін елеулі дамытуды, содан кейін оны жасалған қылмыстар мен іздеуде жүрген адамдар туралы қолда бар ақпараттар массивімен салыстыру қажет.

Нақты уақыт режимінде азаматтарды биометриялық мәліметтер (саусақ іздері мен алақан іздері, түрлері, суреттері мен көздің ірисі, татуировкалар, тыртықтар, дауыстық файлдар және т.б.) бойынша сәйкестендіруге немесе олардың мінез-құлқын болжауға қабілетті кешенді жүйелерді дамыту қылмыстарды ашуда ЖІҚ автоматты түрде пайдалануы керек.

Сонымен қатар, коммерциялық және мемлекеттік құрылымдарда қолда бар ЖИ жүйелерін ЖІҚ-ің мақсаттары үшін (банктер, әлеуметтік желілер, мессенджерлер, интернет-провайдерлер, медициналық мекемелер және т.б.) пайдалану қажет.

Бұл ретте осы секторды нормативтік реттеу, адамның құқықтары мен бостандықтарын сақтауға, деректердің ағып кетуіне жол бермеуге және ЖИ шешімін қабылдау процестерін бақылауға мүмкіндік беретін тиімді бақылау жүйесін белгілеу қажет.

Пайдаланған әдебиеттер тізімі

1. «Новая эра». Токаев поручил создать все условия для развития ИИ в Казахстане [Электрондық ресурс] // URL: https://tengrinews.kz/kazakhstan_news/novaya-era-tokaev-poruchil-sozdat-usloviya-razvitiya-ii-513271/.

2. Овчинский В.С., Ларина Е.С. Искусственный интеллект. Большие данные. Преступность. – М.: Книжный мир, 2018. – 416 с.

3. Овчинский В.С., Маслов А.А., Бабушкин А.А. О перспективах использования технологий искусственного интеллекта в оперативно-розыскной деятельности органов внутренних дел: науч. доклад (ВНИИ МВД России, 2020).

4. Жданов Ю., Овчинский В. Полиция будущего. – М., 2018. – 166 с.

5. Жданов С. Вы арестованы за намерение. Как новейшие цифровые разработки помогают предсказывать и предотвращать преступления [Электрондық ресурс] // НОЖ. URL: https://knife.media/predict-crime/.

6. Domain Awareness System [Электрондық ресурс] // Tadviser. URL: https://www.tadviser.ru/index.php/Продукт:Domain_Awareness_System.

Тюрина Ирина Николаевна,
старший преподаватель кафедры уголовного права и криминологии
к.ю.н., e-mail: vuzmvd@mail.ru
(Воронежский институт МВД России, Российская Федерация)

СПЕЦИАЛЬНЫЕ МЕРЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ И ПОЛОВОЙ СВОБОДЫ НЕСОВЕРШЕННОЛЕТНИХ

Аннотация. В статье рассматриваются наиболее эффективные меры по предупреждению и профилактике преступлений против половой свободы и половой неприкосновенности несовершеннолетних. Предлагаются изменения в действующем законодательстве с применением наиболее действенных специальных мер предупреждения данных видов преступлений.

Ключевые слова: половые преступления, несовершеннолетние, специальные меры предупреждения, половая свобода, половая неприкосновенность.

SPECIAL MEASURES FOR THE PREVENTION OF CRIMES AGAINST THE SEXUAL INTEGRITY AND SEXUAL FREEDOM OF MINORS

Annotation. The article discusses the most effective measures for the prevention and prevention of crimes against sexual freedom and sexual integrity of minors. Amendments to the current legislation are proposed with the use of the most effective special measures to prevent these types of crimes.

Keywords: sexual crimes, minors, special preventive measures, sexual freedom, sexual inviolability.

В современном государстве регистрируется значительное количество преступлений против половой свободы и половой неприкосновенности несовершеннолетних. В борьбе с данными видами преступлений необходим особый подход и выбор специализированных мер по предупреждению и предотвращению противоправных деяний.

При выборе специальных мер предупреждения преступлений необходимо отталкиваться от конкретной специфики рассматриваемых преступлений. Именно анализ специфики и причин и условий этой преступности (имеющихся детерминантов) является положительной предпосылкой выбора правильных специальных мер и дальнейшего успешного предупреждения преступлений.

Общие меры предупреждения преступлений являются более абстрактными и обобщенными в отличии от специальных мер, которые направлены на решение конкретных проблем, устранение причин и условий преступности [1, с. 50].

Говоря о «половых преступлениях», в частности совершаемых в отношении несовершеннолетних лиц, основным фактом, на который следует обратить внимание является то, что данные преступления совершают лица обладающими определенными психическими отклонениями – расстройствами сексуального влечения.

Рассмотрим наиболее оптимальные и эффективные, на наш взгляд, специальные меры предупреждения «половой» преступности, совершаемых в отношении лиц, не достигших восемнадцатилетнего возраста.

Оказание лицам, страдающих психическим отклонением, таким как расстройство сексуального влечения, помощи специалистами, обладающими психологическими и/или психиатрическими знаниями.

В данном пункте стоит затронуть необходимость несколько ужесточить принимаемые в отношении указанной категории преступников карательных мер. Например, в отношении лиц, совершивших посягательство на половую свободу или неприкосновенность несовершеннолетних, по решению суда могут быть применены принудительные меры медицинского характера, но в отношении вменяемого лица они могут применяться исключительно в период отбывания наказания. После истечения данного срока лицо подлежит освобождению. Считаем, что эту норму уголовного законодательства необходимо изменить и принудительные меры медицинского характера применять в отношении лиц с расстройством сексуального предпочтения до момента, когда специалисты смогут утверждать, что лицо больше не нечет опасности для общества: оно либо окончательно излечилось, либо вероятность рецидива минимальна и практически отсутствует.

В отношении педофилов, которые уже проходили подобное лечение в специализированных учреждениях, но после его окончания, окунувшись в привычную среду, где на них не оказывается никакого влияния (медицинских работников) и их действия ничем и никем не ограничиваются, снова поддаются соблазну и становятся на преступный путь, совершая рецидив. Эффективными мерами предупреждения нам видятся:

1. Применение к ним принудительных мер медицинского характера пожизненно.

2. Применение менее гуманной меры – химической кастрации.

3. Составление программ, носящих сексуально-просветительский и воспитательный характер, а также использование этих программ в реальной жизни.

Рассматривая данную меру предупреждения «половой» преступности, можно выделить несколько направлений в зависимости от лиц, осуществляющих эти программы.

К первому направлению относят проведение подобных мероприятий в рамках школы, когда учителя проводят беседы со своими подопечными на информационных или классных часах, а также выделяя для этого отдельные занятия.

Ко второму направлению относят проведение бесед с сотрудниками правоохранительных органов, в рамках которых они в большей мере отражают правовой аспект данной тематики. Так как многие подростки могут сами спровоцировать совершение в отношении них преступлений в силу незнания закона. Например, подобные ситуации часто происходят в рамках 134 статьи УК РФ, в которой предусмотрены различные действия сексуального характера с несовершеннолетними с условием их добровольного согласия.

К третьему направлению относят сексуальное воспитание в рамках семьи. Это, как нам кажется, наиболее важное и значимое направление, так как семья и то, что она дает ребенку, является основополагающим в его развитии. Ведь это сведения, получаемые не от незнакомых людей, к которым у них возможно нет доверия и веры, а от близких и родных, которые не в коем случае не обманут и не пожелают плохого.

Исходя из анализа судебной практики и теоретических данных несовершеннолетние лица, с которыми проводились подобные беседы, и освещалась данная тема со стороны родителей, обладали более устойчивым психическим состоянием, нежели лица, получаемые все сведения самостоятельно из Интернет-ресурсов или от сверстников.

Осуществлении предупреждения виктимности, также посредством проведения бесед и освещения этих вопросов при помощи средств массовой информации (СМИ).

Данная мера заключается в том, что лицам, которые являются потенциальными жертвами рассматриваемой нами категории преступлений, рассказывается какого поведения, каких жизненных ситуаций стоит избегать, чтобы не привлечь к себе внимания потенциальных преступников. Среди таких правил можно выделить следующие: избегать незнакомых компаний и общения с незнакомыми людьми (особенно в позднее (темное) время суток), передвижение на попутках, употребление алкоголя или наркотических веществ и общение с лицами их употребляющих, прогулки или иное нахождение на улице в ночное время.

4. Принятие изменений в уголовном законодательстве, и введение в действие новых нормативных правовых актов в данной области.

Среди возможных изменений мы можем предложить следующие:

1) ужесточение применяемых мер за совершение «половых» преступлений в отношении несовершеннолетних;

2) применение принудительных мер медицинского характера для лиц, имеющих расстройство сексуального предпочтения, и после отбытия наказания;

3) регламентация в законодательстве правил более строгого и тщательного проведения надзора за данной группой преступников после их освобождения сотрудниками правоохранительных органов [2, с. 47].

5. Принятие мер, способных снизить уровень латентных преступлений в области «половых преступлений».

Для осуществления данной цели необходимо донести до общества, что «половые» преступления ни в коем случае нельзя скрывать, о них нельзя умалчивать, ведь это ведет лишь к увеличению количества таких преступлений. С помощью бесед с сотрудниками правоохранительных органов, через СМИ, через информационные стенды и любыми другими способами требуется донести до людей, что умалчивание приводит к тому, что преступник остается на свободе и чувствует определенную безнаказанность, так как будет предполагать что и следующие его жертвы не обратятся к сотрудникам полиции.

Также одной из проблем является отношение общества к жертвам «половых» преступлений, на них сваливается негатив и зачастую даже порицание.

Следствием является то, что потерпевшим стыдно рассказывать о случившемся. Ликвидировать данную проблему не так легко, ведь нельзя так просто изменить мировоззрение общества, но пропаганда и освещение данных вопросов со временем может дать определенный результат.

Еще одним важным фактором является деятельность сотрудников полиции при проведении расследования подобных заявлений, необходимо быть тактичным и деликатным при работе с потерпевшим, так как это в целом лицо с еще неустоявшейся психикой в силу несовершеннолетнего возраста, так еще и подвергнувшееся стрессовой ситуации из которой не так легко выйти (иногда лицо не в состоянии выйти из этого состояния самостоятельно, без помощи специалиста).

В заключении хотелось бы отметить, что предупредительная работа не будет приносить желаемой эффективности без использования сексологических и сексопатологических результатов. Конечно предупредительные меры не должны ограничиваться исключительно рекомендациями сексопатологов, предупредительная работа носит комплексный характер и должна включать в себя все имеющиеся разновидности мер.

Список использованной литературы

1. Кутуев Э.К. Деятельность государственных структур в сфере профилактики сексуального насилия // Мир юридической науки. – Санкт-Петербург: ООО «МНИОЦ», 2019. – № 4. – С. 50–53.

2. Антонян Ю.М. Криминальная сексология / Ю.М. Антонян, А.А. Ткаченко, Б.В. Шостакович. – М, 2009. – С. 47–49.

Урстенова Дарина Данияровна,
преподаватель кафедры кибербезопасности и информационных технологий
магистр национальной безопасности и военного дела, d.urstenova@kpa.gov.kz
(Карагандинская академия МВД Республика Казахстан им. Б. Бейсенова Республика Казахстан)

КАРДИНГ: ЭВОЛЮЦИЯ КИБЕРУГРОЗ В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. Кардинг, вид мошенничества с использованием платежных карт, переживает значительные трансформации. Современные киберпреступники сосредотачивают свои усилия на взломе банковских счетов физических и юридических лиц через интернет, обеспечивая высокую прибыль при сопоставимых затратах времени и усилий. В статье рассматриваются эволюция кардинга и современные тенденции, а также выделяются две основные группы кардерских методов: скимминг и дистанционный доступ к данным."

Ключевые слова: кардинг, мошенничество с использованием платежных карт, эволюция киберпреступности, безопасность онлайн-банкинга, техники скимминга, дистанционный доступ к данным, тенденции финансового мошен-

ничества, проблемы кибербезопасности, риски цифровой экономики, несанкционированные транзакции.

CARDING: EVOLUTION OF THREATS IN THE ERA OF DIGITAL ECONOMY

Annotation. Carding, a form of fraud involving the use of payment cards, is undergoing significant transformations. Contemporary cybercriminals concentrate their efforts on gaining access to the bank accounts of individuals and businesses online, ensuring substantial profits with comparable time and effort expenditures. This article explores the evolution of carding and current trends, highlighting two main carding methods: skimming and remote data access

Keywords: carding, payment card fraud, cybercrime evolution, online banking security, skimming techniques, remote data access, financial fraud trends, cybersecurity challenges, digital economy risks, unauthorized transactions.

Киберпреступность, рассматриваемая с юридической, практической и политической точек зрения, представляет прямую угрозу для прав человека, общества и государства. Она становится особенно опасной в свете того, что современное развитие общества невозможно без использования телекоммуникационных систем. Наши дни – это эпоха цифрового прогресса, где, помимо новых возможностей, присутствуют и новые риски. Развитие цифровых технологий создает уникальную платформу для преступной деятельности, что обуславливает перенос преступности в киберпространство. Это требует не только изменений в работе правоохранительных органов, но и пересмотра научных исследований в данной области, учитывая особенности киберпространства.

Благодаря технологическому прогрессу, киберпреступность обычно ассоциируется с преступлениями, в которых компьютерные сети используются для незаконных целей, таких как кража конфиденциальных данных, мошенничество, отмывание денег и детская порнография. С развитием технологий появляются новые формы киберпреступлений, совершаемых преступниками.

Один из видов мошенничества с участием дропперов, дроповода и торпеды это Кардинг.

Кардинг (от англ. carding) – вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем [1].

Кардинг сильно изменился в настоящее время. Киберпреступники теперь направляют все свои усилия на получение доступа к банковским счетам физических и юридических лиц через Интернет. Это обеспечивает большую прибыль при сопоставимых затратах по времени и силам.Это дает возможность получить большую прибыль при сравнимых затратах времени и усилий.

Кардинг можно разделить по способу доступа к данным на две большие группы:

1. Скимминг.

2. Дистанционно.

Скимминг (Skimmin,от английского «to skim»– бегло прочитывать, скользить)– вид мошенничества с банковскими картами, который представляет собой считывание информации с их магнитной полосы с помощью специального технического устройства или скиммера [2].

Для считывания данных применяют скиммеры (Skimmer)– специальные устройства, которые крепятся непосредственно к банкомату, а также к любому принимающему слоту картоприемника .

В настоящее время первая категория лиц сталкивается с трудностями в легком доступе к банковским картам из-за усовершенствованных систем безопасности банкоматов и самих карт. Это свидетельствует о том, что безопасность банковских карт и банкоматов значительно улучшилась и стала более надежной. Кроме того, физическое вмешательство преступника представляло собой значительный риск, поэтому с течением времени преступники, стремясь к анонимности, перешли в онлайн-пространство, где существуют методы шифрования данных, предотвращающие их идентификацию.

При обсуждении дистанционного кардинга следует отметить, что он имеет множество подгрупп, в которых киберпреступники занимаются различными видами незаконной деятельности.

Основными направлениями являются сбор материала, вещевой кардинг и кардинг авиабилетов/отелей. Различие между всеми видами кардинга через Интернет (кроме сбора материала) заключается в том, как мошенник получает похищенные деньги после всех операций. Главным направлением кардинга является «сбор материала», который представляет собой незаконное получение информации о реквизитах банковских карт и счетов преступником или преступной группой.

Существует множество способов, но наиболее распространенным способом совершения такого рода преступлений является так называемый «фишинг» – один из видов интернет-мошенничества, подразумевающий под собой получение данных карты от самого хозяина.

Преступник создает, например, зеркальный сайт, внешне похожий на сайт банка или интернет-магазина, но доменное имя зеркального сайта будет незначительно отличаться, в результате ничего не подозревающий пользователь вносит все данные карты на сайт, и у злоумышленника появляются в распоряжении все реквизиты карты.

Кроме создания зеркальных сайтов широкое распространение имеют интернет-рассылки по типу: банк просит указать реквизиты карты для верификации, укажите данные карты для получения государственной субсидии, выигрыша и так далее

После получения информации с банковских карт есть несколько отличающихся друг от друга способов ее реализации.

Однако у них есть общее – реализация полученных в ходе преступления данных и денежных средств осуществляется только через даркнет (сеть

интернет-ресурсов, обеспечивающих своим пользователям полную анонимность, благодаря нестандартным протоколам шифрования информации).

Злоумышленники «сливают» полученные незаконным путем данные банковских карт другим пользователям даркнета за определенную плату, которая в подавляющем большинстве случаев представляет собой криптовалюту, особенностью которой является невозможность проследить ее движение между пользователями, что делает расследование киберпреступлений крайне затруднительным.

Касаемо создания поддельных банковских карт, злоумышленники нередко производят их сами. В даркнете закупаются «болванки» пластиковых карт нужного банка с магнитной полосой, после чего, используя энкодер – устройство, записывающее информацию на магнитную полосу и позволяющее выгравировать различные элементы на карте, производится запись на магнитную полосу информации банковской карты, похищенной у потерпевшего, а также наносятся все реквизиты банковской карты.

На данном этапе для своей безопасности Кардеры передают поддельные банковские карты подставным лицам (торпедам). Это позволяет им избежать прямого контакта с незаконными операциями и снизить риск попадания под следствие. Однако это также увеличивает риск обнаружения мошенничества, так как торпеды могут быть пойманы и раскрыть информацию о Кардерах. В конечном итоге, это демонстрирует, что Кардеры готовы идти на большие риски ради своей безопасности и прибыли.

Подводя итог, следует отметить, что с каждым годом схемы кардинга становятся все более сложными, что создает трудности в разработке четких алгоритмов расследования таких преступлений. Тем не менее, важно уметь выявлять цифровые следы, оставленные преступниками из-за их неосторожности в некоторых случаях.

В связи с этим представляется необходимым внедрение информации о основных методах совершения кардинга, социальной инженерии, технологии поиска OSINT (open source Intelligence) в учебные программы по курсу «Криминалистика» для образовательных учреждений высшего и среднего профессионального уровня. Это также включает в себя обучение будущих сотрудников органов дознания и предварительного следствия методам обнаружения электронных следов и подходам к расследованию преступлений, связанных с банковскими картами. Такие усилия помогут повысить уровень знаний в области информационных технологий и научат получать необходимую информацию через сеть Интернет.

Список использованной литературы

1. Что такое кардинг (Carding) и почему все о нем говорят? И как на этом заработать? [Электронный ресурс] // URL: https://medium.com/@markmark1_23715/.

2. Считать и украсть: как работает скимминг банковских карт [Электронный ресурс] // URL: https://trends.rbc.ru/trends/industry/612d019d9a79470c54677745?from=copy.

Холиков Шухрат Абдухамидович,
старший преподаватель кафедры информационных технологий
подполковник, vtingru@yandex.com
(Университет общественной безопасности Республики Узбекистан)

КИБЕРУГРОЗЫ И КАК ЗАЩИТИТЬ СВОИ ДАННЫЕ

Аннотация. В статье рассматривается понятие киберугрозы, вредоносная деятельность, последствия кибератак и обстоятельства возникновения киберугроз.

Ключевые слова: киберугрозы, кибератаки, киберриск, вредоносная программа, сеть, злоумышленник.

CYBER THREATS AND HOW TO PROTECT OWN DATA

Abstract. The article discusses the concept of a cyber threat, malicious activity, the consequences of cyber attacks and the circumstances of the emergence of cyber threats.

Keywords: Cyber threats, cyber attacks, cyber risk, malware, network, attacker.

«Киберугрозы», угроза кибербезопасности определяется как любое вредоносное действие, направленное на причинение вреда, кражу или нарушение работы данных и цифровой жизни в целом. Компьютерные вирусы, утечки данных и атаки типа «Отказ в обслуживании» (DoS) – все это примеры таких атак. Чтобы действительно понять понятие киберугроз, необходимо углубиться в историю кибербезопасности. Опасности и последствия этих угроз продолжают расти по мере того, как мы ориентируемся во все более взаимосвязанном мире. Итак, давайте посмотрим, что такое киберриски и как их избежать.

Киберугроза – это вредоносная деятельность, совершаемая с целью уничтожения, кражи или нарушения работы данных и цифровой жизни в целом. Примерами таких рисков являются компьютерные вредоносные программы, утечки данных и атаки типа «отказ в обслуживании» (DoS). Поскольку мы все больше зависим от технологий, киберугрозы прогрессируют и становятся все более распространенными, представляя значительный риск для людей и предприятий. Понимание киберрисков – это первый шаг к защите от них [1].

Каковы последствия кибератак? В последние годы кибератаки становятся все более распространенными. Никто не застрахован от опасности кибератаки, от крупных предприятий до правительственных учреждений. Опасности, связанные с утечками данных и кибератаками, возрастают по мере того, как все больше конфиденциальной информации хранится и передается онлайн.

Вот некоторые из последствий кибератаки:

– отключения электроэнергии;

– отказ военной техники;

– нарушения секретов национальной безопасности;

– кража ценных и конфиденциальных данных (например, медицинских записей, кода sw);

– сбои в работе компьютерных и телефонных сетей;

– парализация целых систем;

– шифруйте важную информацию, делая ее недоступной.

Типы кибератак. Кибератаки принимают различные формы, каждая со своим набором методов и целей. Мы составили список из 7 лучших киберугроз, которые могут подвергнуть риску ваш бизнес. Понимание этих типов кибератак является важным первым шагом в защите себя и своей компании от возможных опасностей.

Вредоносное ПО. Программное обеспечение, которое выполняет вредоносную задачу на целевом устройстве или в сети, например, повреждает данные или захватывает систему.

Мобильные устройства также уязвимы для вредоносных атак, как и другое компьютерное оборудование. Злоумышленники могут внедрять вредоносное ПО в загружаемые приложения, мобильные веб-сайты или фишинговые электронные письма и текстовые сообщения. После взлома мобильное устройство может предоставить злоумышленнику доступ к личной информации, данным о местоположении, финансовым счетам и многому другому. Вот несколько распространенных типов вредоносных программ:

– Virus;

– Worm;

– Trojan;

– Spyware (Шпионское ПО);

– Ransomware (Программа-вымогатель);

– Phishing (Фишинг);

– Spear Phishing (Фишинг с использованием шпионских программ);

– Adware (Рекламное ПО);

– Rootkit (Руткиты);

– Keylogger (Кейлоггер);

– Botnet (Ботнет);

– Fileless Malware (Вредоносное ПО без файлов);

– Mobile Malware (Вредоносное ПО для мобильных устройств) [2].

Это происходит, когда злоумышленник устанавливает позицию между отправителем и получателем электронных сообщений и перехватывает их, возможно, изменяя при передаче. Отправитель и получатель считают, что они общаются друг с другом напрямую. MitM-атака может использоваться в вооруженных силах, чтобы сбить противника с толку.

Атака типа «отказ в обслуживании» или распределенная атака типа «отказ в обслуживании» (Denial of Service attack or Distributed Denial of Service Attack – DDoS).

Атаки на устройства Интернета вещей (Attacks on IoT Devices).

Утечки данных (Data Breaches).

SQL Injection.

Атаки с использованием паролей (Password Attacks).

Причины кибератак:

1) понимание причин кибератак является важным шагом в разработке успешных методов предотвращения и смягчения последствий;

2) человеческая ошибка;

3) устаревшее программное обеспечение;

4) неадекватная аутентификация;

5) спонсируемые государством кибератаки, направленные на кражу интеллектуальной собственности, получение военного или политического преимущества или разрушение необходимой инфраструктуры;

6) атаки, осуществляемые одной страной против другой, часто с целью нарушения работы или нанесения ущерба важнейшей инфраструктуре, такой как электросети или банковские системы;

7) поставщики технологий со слабым уровнем безопасности [3].

Наиболее распространенные источники угроз кибербезопасности. Киберугрозы исходят из самых разных мест, людей и контекстов. К злоумышленникам относятся: лица, создающие векторы атак с помощью собственных программных средств; преступные организации, которые управляются как корпорации, с большим количеством сотрудников, разрабатывающих векторы атак и осуществляющих их; национальные государства; террористы; промышленные шпионы; организованные преступные группировки; недовольные инсайдеры; хакеры; конкуренты по бизнесу [4].

Национальные государства являются источниками многих наиболее серьезных атак. Существует несколько различных версий киберугроз со стороны национальных государств. Некоторые из них являются элементарным шпионажем – попыткой узнать государственные секреты другой страны. Другие направлены на разрушение.

Многие киберугрозы покупаются и продаются в “темной паутине”, неорганизованном, но широко распространенном криминальном сегменте Интернета. На этом онлайн-рынке начинающие хакеры могут приобрести программы-вымогатели, вредоносное ПО, учетные данные для взломанных систем и многое другое. Темная паутина служит множителем угроз, поскольку один хакер может продавать свое творение снова и снова.

Как предотвратить киберугрозы: защита ваших конфиденциальных данных. Защита вашей конфиденциальной информации как никогда важна в постоянно развивающемся мире киберугроз. Последствия одной утечки данных могут быть катастрофическими, что скажется на вашей конфиденциальности, финансовой стабильности и репутации. К счастью, существует множество стратегий, которые вы можете использовать для защиты своих ценных данных. Вот несколько важных шагов, которые следует рассмотреть:

1. Регулярно обновляйте: обновляйте свою операционную систему, программное обеспечение и приложения с помощью последних исправлений безопасности. Хакеры часто используют устаревшие системы, поэтому важно регулярно проверять наличие обновлений и устанавливать их.

2. Надежная аутентификация: используйте надежные, уникальные пароли для каждой из ваших онлайн-учетных записей. Рассмотрите возможность

использования менеджера паролей, который поможет вам отслеживать сложные пароли. Включайте двухфакторную аутентификацию (2FA), когда это возможно, для дополнительного уровня безопасности.

3. Безопасные сети: избегайте использования общедоступных сетей Wi-Fi для конфиденциальных транзакций. Если вам необходимо использовать общедоступный Wi-Fi, используйте виртуальную частную сеть (VPN) для шифрования ваших данных и сохранения их конфиденциальности.

4. Брандмауэр и антивирусное программное обеспечение: Используйте брандмауэр для блокирования несанкционированного доступа к вашему компьютеру. Установите проверенный антивирус и антивирусное программное обеспечение для обнаружения и удаления вредоносного ПО.

5. Будьте осторожны с попытками фишинга: скептически относитесь к неожиданным электронным письмам, особенно к тем, в которых запрашивается личная информация или предлагается перейти по ссылке. Проверьте личность отправителя, прежде чем отвечать или переходить по каким-либо ссылкам.

6. Ограничить доступ: Ограничьте доступ к вашим конфиденциальным данным. Делитесь ими только с теми, кому это абсолютно необходимо, и обязательно отмените доступ, когда в этом больше не будет необходимости.

7. Шифрование конфиденциальных данных Шифрование данных: особенно когда они хранятся на портативных устройствах, таких как ноутбуки или USB-накопители, которые могут быть легко потеряны или украдены.

8. Регулярные резервные копии: регулярно создавайте резервные копии ваших важных данных на внешний диск или облачное хранилище. Это гарантирует, что у вас будет копия ваших данных на случай кибератаки, например, вымогательства.

9. Обучение сотрудников: Если вы ведете бизнес, обучайте своих сотрудников рискам киберугроз и способам их предотвращения. Это включает в себя безопасное использование Интернета, распознавание попыток фишинга и сообщение о любых подозрительных действиях.

10. План реагирования на инциденты: Разработайте план реагирования на инциденты, чтобы вы знали, какие шаги предпринять в случае утечки данных. Это должно включать в себя, с кем связаться, как локализовать нарушение и как уведомить затронутых лиц.

11. Будьте в курсе: Будьте в курсе последних киберугроз и стратегий предотвращения. Присоединяйтесь к форумам, подписывайтесь на новостные рассылки или следите за экспертами по кибербезопасности в социальных сетях [5].

Помните, что кибербезопасность – это непрерывный процесс, требующий постоянной бдительности для эффективной защиты ваших конфиденциальных данных.

Наконец, киберугрозы вызывают реальную озабоченность в современной цифровой среде, и к ним нужно относиться серьезно. Они могут оказать серьезное влияние на любого человека, от частных лиц до корпораций и правительств. Тем не менее, предотвращение имеет важное значение, и есть несколько мер, которые могут быть использованы для уменьшения опасности

кибератаки. Помните, что ответственность за кибербезопасность несет каждый. Быть в курсе новейших рисков и принимать меры предосторожности для защиты себя и других может помочь в предотвращении киберугроз и гарантировать более безопасную цифровую среду. Мы все можем помочь сохранить наш цифровой мир в безопасности, работая сообща и серьезно относясь к кибербезопасности.

Список использованной литературы

1. Lawrence C. Miller. Cybersecurity survival guide. – 2023. – 363 p.

2. Michael Kofler, Klaus Gebeshuber, Peter Kloep, Frank Neugebauer, André Zingsheim, Thomas Hackner, Markus Widl, Roland Aigner, Stefan Kania, Tobias Scheible, Matthias Wübbeling «Hacking and Security. The Comprehensive Guide to Penetration Testing and Cybersecurity». – 2023. – 1143 p.

3. 10 most common types of cyber attacks [Электронный ресурс] // URL:https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/.

4. Prevent Cyber Attacks: Strategies to Protect Your Digital Assets [Электронный ресурс] // URL: https://www.sprintzeal.com/blog/prevent-cyber-attacks.

5. Preventing Malicious Actors at the Perimeter [Электронный ресурс] // URL: https://www.linkedin.com/pulse/preventing-malicious-actors-perimeter-onefirewall-alliance/.

Чернышев Дмитрий Борисович,
старший преподаватель кафедры уголовного права
к.ю.н., e-mail: sledstvieNT404@mail.ru
(Уральский юридический институт МВД России, Российская Федерация)

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ «ИСКУССТВЕННОГО ИНТЕЛЛЕКТА» ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация. В статье приводится анализ возможностей использования технологий искусственного интеллекта при организации деятельности следователя по раскрытию и расследованию уголовных дел. Рассматриваются основные направления совершенствования технического и программного обеспечения следственных подразделений, направленные на автоматизацию и оптимизацию процессов.

Ключевые слова: искусственный интеллект, цифровая криминалистика, расследование.

THE USE OF «ARTIFICIAL INTELLIGENCE» TECHNOLOGIES IN THE INVESTIGATION OF CRIMES

Annotation. The article provides an analysis of the possibilities of using artificial intelligence technologies in organizing the activities of an investigator for the

disclosure and investigation of criminal cases. The main directions of improving the technical and software of investigative units aimed at automating and optimizing processes are considered.

Keywords**:** artificial intelligence, digital forensics, investigation.

Современные компьютерные технологии, затрагивающие все стороны жизни современного постиндустриального общества, последовательно проникают в следственную деятельность. Как специфическая форма человеческой деятельности, имеющая собственные потребности, она требует разработки и внедрения собственных программных инструментов. Внедрение таких технологий в криминалистическую деятельность осуществляется в двух аспектах – как совершенствование материально-технических средств, находящихся в распоряжении следователя, и использование программного обеспечения в практической деятельности.

Д.В. Бахтеев в своих исследованиях оценивает возможности использования технологий искусственного интеллекта в нескольких направлениях: для сбора и анализа статистики, для облегчения выполнением следователей рутинных технических задач, для проведения исследований и экспертиз, и т. д. [1, с. 89].

В настоящее время в практической деятельности следователей применение искусственного интеллекта как правило выражается в разработке и внедрении систем программирования принятия решения. Указанная система включает в себя три основных компонента.

В первую очередь – это автоматизация процесса сбора, обработки и хранения информации. Применяемые технические средства должны иметь возможность аккумулировать данные, полученные в результате осмотра мобильных телефонов, размещенные в открытом доступе данные государственных учреждений, в частности – Бюро кредитных историй [2], таможенных органов, Базы данных о компаниях и частных предпринимателях [3], и т. д. Ряд ученых к таким базам относит также цифровизованные материалы уголовных дел, предоставляемые в подразделения оперативно-розыскной информации, в основном – электронные протоколы следственных действий, сведения, полученные от мобильных операторов.

Отдельное место занимают сведения, содержащиеся в социальных сетях. В качестве примера программного обеспечения, позволяющего анализировать большие массивы данных социальных сетей, можно отметить приложения «Октопус», «Платформа ПСКОВ», осуществляющие сбор сведений с использованием возможностей API-интерфейса [4, с. 978]. В целом основной функционал подобных программ позволяет осуществлять сбор и анализ сведений из открытых источников. Перспективным направлением видится интеграция указанных технологий с криминалистическими базами данных, и цифровыми материалами уголовных дел. Главным условие этого является обеспечение надлежащего уровня безопасности от несанкционированного доступа.

Второй компонент включает в себя совокупность программ, осуществляющих построение и анализ связей межу данными внутри одного массива и между различными базами. Данная функция позволяет осуществлять построе-

ние «эгосети» объекта анализа, включающей «мосты-связи» между элементами сети, устанавливать связи уровня – юридическое лицо – физическое лицо.

В исследовании, проведенном А.Г. Себякиным, приводятся результаты исследования взаимодействия фигурантов нескольких уголовных дел, базой которых послужили сведения о контактах, извлеченные из их мобильных телефонов, что позволило выявить дополнительных фигурантов [5].

Последний компонент предназначен для объединения возможностей двух предыдущих в единой информационной системе, находящейся в распоряжении следователя, оснащенная соответствующим интерфейсом (т.н. «пользовательский модуль»), позволяющая облегчить выполнение текущих рутинных задач. Помимо перечисленных модулей, она позволяет автоматизировать ряд технических операций, в частности формирование типовых запросов и поручений, методическая поддержка при проведении отдельных следственных действий, учет изъятых предметов и документов, формирование обвинительного заключения и оформление материалов уголовного дела.

В качестве положительного опыта применения таких технологий можно отметить разработанную К.А. Нелюбиным регуляционную базу данных, содержащую основные элементы криминалистической характеристики убийств [6, с. 4].

Безусловно, существующие сегодня программы позволяют выработать лишь высоко вероятностную версию пути раскрытия преступления, возможный круг источников, и требующую перспективного моделирования со стороны следователя [7]. Соответственно, они направлены прежде всего на методическую поддержку деятельности следователя, а не программирование расследования как информационного процесс [8, с. 45].

В связи с этим встает вопрос о способности технологии искусственного интеллекта заменить следователя.

Полагаем, что существующие технические возможности, как и перспективные разработки программного обеспечения могут лишь автоматизировать отдельные этапы проведения предварительного следствия. В связи с тем, что согласно ст. 17 УПК РФ оценка доказательств на предмет допустимости, относимости, достоверности, а в совокупности – достаточности для принятия процессуального решения осуществляется следователем на основе внутреннего убеждения и совести, коими не обладает ни одна существующая программа, полагаем, что роль личности следователя в расследовании уголовных дел останется решающей.

Список использованной литературы

1. Бахтеев Д.В. О связи криминалистики и технологии искусственного интеллекта // Сибирские уголовно-процессуальные и криминалистические чтения. – 2022. – № 1 (35). – С. 88–93.

2. Центральный банк Российской Федерации: официальный сайт [Электронный ресурс] // URL: https://www.cbr.ru.

3. Открытые официальные государственные базы данных Российской Федерации [Электронный ресурс] // URL: https://ba-za.net/otkrytye-ofitsialnye-gosudarstvennye-bazy-dannyh-rf.

4. Орехва А.В., Кириллов Д.С., Малахов С.В. Описание и сравнение API для работы с графиками котировок // Инновации. Наука. Образование. – 2022. – № 53. – С. 978–979.

5. Себякин А.Г. Искусственный интеллект в криминалистике: система поддержки принятия решений // Baikal Research Journal. – 2019. – Т. 10. – № 4. – DOI: 10.17150/2411-6262. 2019.10(4).21.

6. Нелюбин К.А. Некоторые вопросы создания и использования электронной базы данных на основе криминалистической характеристики убийств // Российский следователь. – 2014. – № 13. – С. 3–5.

7. Бахтеев Д.В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений: дисс. … док. юрид. наук. – Екатеринбург, 2022. – 504 с.

8. Бахтеев Д.В. О некоторых цифровых технологиях и их воздействии на следственную деятельность // Библиотека криминалиста. Научный журнал. – 2018. – № 3. – С. 45–49.

Шаухар Данияр Қанатұлы,
магистрант факультета послевузовского образования
старший лейтенант полиции, d.shauhar@kpa.gov.kz
(Карагандинская академия МВД Республики Казахстан им. Б. Бейсенова, Республика Казахстан)

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ В РАМКАХ ВНЕДРЕНИЯ ТРЕХЗВЕННОЙ МОДЕЛИ УГОЛОВНОГО ПРОЦЕССА

Аннотация. В данной статье автором рассматривается вопрос противодействия киберпреступности в рамках внедрения трехзвенной модели уголовного процесса. Особое внимание уделено сущности трехзвенной модели, как гаранта соблюдения прав и свобод человека и гражданина. Автором также были рассмотрены формы киберпреступности. Изучена стратегия борьбы с киберпреступностью в свете реформирования уголовного судопроизводства. Целью написания данной статьи является выявление причин и условий совершений киберпреступлений на фоне реформы правоохранительной системы и системы правосудия Республики Казахстан, а также внесение предложений по противодействию данному виду преступности.

Ключевые слова: противодействие киберпреступности, расследование киберпреступлений, трехзвенная модель, уголовное судопроизводство.

COUNTERING CYBERCRIME AS PART OF THE IMPLEMENTATION OF A THREE-TIER MODEL OF THE CRIMINAL PROCESS

Annotation. In this article, the author examines the issue of countering cybercrime within the framework of the introduction of a three-tier model of criminal procedure. Special attention is paid to the essence of the three-tier model as a guarantor of respect for human and civil rights and freedoms. The author also considered the forms of cybercrime. The strategy of combating cybercrime in the light of criminal justice reform has been studied. The purpose of writing this article is to identify the causes and conditions of cybercrime against the background of the reform of the law enforcement system and the justice system of the Republic of Kazakhstan, as well as to make proposals to counter this type of crime.

Keywords: countering cybercrime, investigation of cybercrimes, three-tier model, criminal proceedings.

1 сентября 2020 г. в Послании народу «Казахстан в новой реальности: время действий» Глава государства поручил поэтапно внедрить в стране трехзвенную модель уголовного процесса. Такая система действует в развитых странах Организации экономического сотрудничества и предусматривает следующую организацию процесса. Орган уголовного преследования выявляет преступления, устанавливает причастных лиц и собирает улики.

Прокурор дает оценку собранным доказательствам, пресекает нарушение прав участников уголовного процесса, не допускает вовлечение добросовестных граждан в уголовный процесс и поддерживает государственное обвинение в суде.

Суд занимается санкционированием следственных действий, рассмотрением жалоб и назначением наказания. Мировая практика показывает, что разграничение полномочий уполномоченных органов позволяет максимально обеспечить защиту прав граждан на всех стадиях уголовного процесса. Разграничение создаёт правозащитный барьер, ограждая от необоснованных незаконных решений. Каждая из стадий трёхзвенной модели служит фильтром, через который должно пройти уголовное дело, перед тем как будет рассмотрено судом.

Касым-Жомарт Кемелевич Токаев подчеркнул: «Такой подход укрепит систему сдержек и противовесов, создаст на каждом этапе эффективные фильтры. Еще раз подчеркиваю: законность и справедливость должны быть обеспечены по умолчанию. Нужно помнить, что от ошибок в уголовных делах зависят судьбы людей» [1].

Если разбираться в корне, то можно прийти к выводу, что на протяжении всего времени существования уголовный процесс Республики Казахстан и так был построен по трехзвенной модели. Фактически идет не перевод системы уголовного судопроизводства на трехзвенную модель, а реформа этих самых трех звеньев и системы взаимодействий каждого звена друг с другом. По нашему мнению ключевым и связующим звеном становится прокуратура. Большинство решений необходимо будет согласовывать с прокурорами.

С политикой внедрения трехзвенной модели судопроизводства с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом. Законом существенно расширены полномочия осуществляющего надзор, а также процессуального прокурора, что фактически

свело на нет и без того формально закрепленную в законе процессуальную самостоятельность следователя [2].

Переход на трехзвенную модель уголовного процесса по плану состоит из двух основных этапов. В настоящее время приводится в жизнь первый этап.

С 1 января 2021 г. прокурор уполномочен согласовывать следующие процессуальные решения:

– о признании в качестве подозреваемого (ст.64, 202 УПК);

– о квалификации деяния (ст. 64, 203 УПК);

– о прерывании сроков досудебного расследования (ст. 192 УПК);

– утверждение протокола об уголовном проступке (ст.65, 528 УПК);

– утверждение постановления о прекращении производства по делу, (ст. 192, 289-290 УПК);

– утверждение постановления о применении приказного производства (ст.629-2, 629-3 УПК).

Безусловно, надзор со стороны прокурора необходим. Но при этом следует избегать излишней бюрократизации и мелочной опеки, фактически снимая ответственность следователя за принятие ключевых решений, ограничивающих конституционные права лиц, вовлеченных в процесс расследования. Полагаем, что вынесение постановления о признании лица подозреваемым – прерогатива следователя, не требующая согласования с прокурором, поскольку это вероятностное решение, правильность которого еще предстоит установить путем производства его допроса и других следственных или негласных следственных действий. Другое дело – согласование прокурором постановления о квалификации деяния подозреваемого, виновность которого подтверждается всей совокупностью собранных следователем доказательств. Но при этом сама процедура, регламентированная ст. 203 УПК РК, требует внесения поправок, соответствующих общепризнанным теоретическим постулатам. В частности, согласие прокурора с квалификацией деяния фактически означает начало официального (государственного) обвинения конкретного лица, которое должно иметь статус уже обвиняемого, а не подозреваемого [3].

Мы полностью согласны с мнением профессора Ахпанова А.Н. и доцента Хана А.Л. Согласование признания лица в качестве подозреваемого требует затраты дополнительных временных ресурсов. Возникает вопрос, как происходит согласование данного решения в ночное время либо в случаях нетерпящих отлагательства. Законодатель предусмотрел право следователя выносить в неотложных случаях постановление о признании лица подозреваемым с последующим обращением к прокурору за получением согласия (п.1-1, 4 ч.1 ст.64 УПК РК). Например, когда необходимо безотлагательно допросить подозреваемого, а согласование с прокурором сразу организовать невозможно (в ночное время, ввиду отдаленности места производства неотложных следственных действий, ввиду отсутствия доступа к ИС ЕРДР – отсутствие электроэнергии, отсутствие или неполадки с интернетом, перезагрузки ИС ЕРДР и т.п.) [4].

Что касается остальных вышеуказанных положений, то считаем их обоснованными. Данные нововведения позволят разделить ответственность за принятие данных решений между органами прокуратуры и органами предвари-

тельного расследования, что, в свою очередь положительно отразится на качестве следственной работы и прокурорского надзора.

Следует отметить и положительные стороны трехзвенной модели уголовного судопроизводства Республики Казахстан. Анализ деятельности прокуратуры города Алматы показал, что с момента внедрения трехзвенной модели значительно улучшилось качество досудебного расследования. Так, прекращаемость дел снизилась на 37,5% (с 8 до 5 тысяч), количество прерываний сократилось на 38,5% (с 13 до 8 тысяч), а выявляемость неправильной квалификации увеличилась в 15 раз (с 6 до 89) [5].

Несмотря на то, что имеется положительная правовая статистика, налицо реальный факт распространения киберпреступности. Данная категория преступлений сегодня является самой распространенной и самой латентной. Несмотря на большое количество заявителей, львиная доля пострадавших от киберпреступлений так или иначе скрывают об этом. Но даже в этом случае правоохранительным органам очень тяжело бороться с подобными преступными проявлениями.

Главной причиной укрытия подобных преступлений является стыд со стороны жертв. Зачастую они просто не хотят разглашать тайну своей личной жизни, а кто-то просто стесняется подавать заявление в связи с тем, что не хочет казаться глупым. Например, даже среди сотрудников полиции имеется большое количество пострадавших от интернет-мошенников. Их логику укрытия данных фактов можно легко объяснить. Так как они сами являются представителями правоохранительных органов, а также, нередко, сами работают именно по линии интернет-мошенничества, было бы позорно оказаться среди потерпевших.

Также среди интернет-мошенников очень много фактов обмана именно связанных с сексуальной жизнью жертв. Например, интернет-мошенница вступает в виртуальный половой акт с пострадавшим, а после вымогает деньги за нераспространение интим-ролика с его участием.

Еще очень много фактов мошенничества среди объявлений. Речь идет не о стандартных объявлениях на сайтах рекламы, таких как КОЛЕСА.КЗ, ОЛХ и т.п. Речь идет о запрещенных сайтах, с размещением анкет с интим-услугами. Сейчас мошенники проникли и в эту итак преступную сферу. Мошенниками здесь могут являться не только женщины, но и мужчины, а также несовершеннолетние.

На сайте, таком как кыздар.нет, выкладывается объявление-анкета. Дальше, когда по данному объявлению звонят, а зачастую пишут в мессенджерах потенциальные клиенты, им предлагается произвести предоплату для производства записи на определенное время. После того, как клиент проводит перевод (на неизвестную карту, без имени), его тут же блокируют в телефоне и мессенджере. Обманутый человек далее ничего не может сделать с данной ситуацией. Обращаться в правоохранительные органы глупо и стыдно. Никто не хочет компрометировать себя как пользователя интим услуг, особенно люди, состоящие в браке, либо люди с хорошей репутацией.

Несмотря на вышеуказанное информация о пользователях таких услуг просочилась в сеть. Сегодня в мессенджере WhatsApp широко распространены

файлы с опубликованной клиентской базой LoveAika, которая занималась сводничеством «Элитных моделей». Также в данных списках имеется полная база самих девушек, оказывающих интим-услуги.

Указанные данные должны были использоваться в доказывании по делу о сводничестве. А граждане, чьи данные были распространены, должны привлекаться в качестве участников расследования. Сразу налицо нарушение прав граждан, как участников уголовного процесса. С 1 января 2024 года будет проведен заключительный этап внедрения трехзвенной модели уголовного процесса. Несмотря на это не соблюдается главный принцип трехзвенной модели – соблюдение прав и свобод граждан. Безусловно все виновные лица понесут наказание. Но где же был прокурорский надзор во время распространения данных расследования?

Подводя итоги данной работы, отметим, что законодатель Республики Казахстан в очередной раз показал свой реформаторский характер. В Казахстане не боятся своевременно и резко отвечать на требования времени. С другой стороны, возникает вопрос об обоснованности внесенных изменений. Учитывая вышеуказанное, считаем, что внедрение трехзвенной модели действительно необходимо. Несмотря на критику со стороны представителей науки и следственного аппарата государственных органов, положительных тенденций у данной модели больше. Единственное, мы не согласны с согласованием признания лица в качестве подозреваемого, считаем, что данное положение следует исключить либо переработать (например, признание лица в качестве подозреваемого необходимо согласовывать по уголовным делам особо тяжкой категории). Также стоит уделить особое внимание на соблюдение прав граждан в режиме реального времени. Привлекать к ответственности должностных лиц, нарушивших права и свободы граждан, не будет необходимым, если будет работать превентивный механизм. Таким механизмом должен выступать прокурор, который должен не допускать подобные проявления в их зародыше.

Список использованной литературы

1. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 г. № 231-V // Казахстанская правда. – 2014. – 10 июля.

2. Послание Главы государства Касым-Жомарта Токаева народу Казахстана «Казахстан в новой реальности: время действий» (г. Нур-Султан, 1 сентября 2020 г). – Доступ из справ.-правовой системы «Параграф».

3. Ахпанов А.Н., Хан А.Л. Проект Закона РК «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам внедрения трехзвенной модели с разграничением полномочий и зон ответственности между правоохранительными органами, прокуратурой и судом» [Электронный ресурс]: взгляд со стороны. URL:https://online.zakon.kz/Document/?doc_id=33889622.

4. Ахпанов А.Н., Хан А.Л. Новые подходы к институту обвинения в уголовном судопроизводстве Республики Казахстан // Вестник Барнаульского юридического института МВД России. – 2021. – № 2 (41). – С. 70–71.

5. Трехзвенная модель уголовного процесса в Казахстане оправдывает себя [Электронный ресурс] // URL: https://www.zakon.kz/redaktsiia-zakonkz/5074134-trehzvennaya-model-ugolovnogo-protsessa.html.

Югай Людмила Юрьевна,
доцент кафедры профилактики правонарушений
д.ю.н., e-mail: yugai.lyudmila@mail.ru

Иминов Абдурасул Абдулатипович,
начальник кафедры информационных технологий
к.ф.-м.н., доцент, e-mail: iminovabdurasul1970@gmail.com

(Академия МВД Республики Узбекистан)

АКТУАЛЬНЫЕ ВОПРОСЫ ПОДГОТОВКИ КАДРОВ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ В КИБЕРПРОСТРАНСТВЕ

Аннотация. В статье раскрывается современное состояние и тенденции развития киберпреступности, что обусловливает необходимость специализированной подготовки кадров по противодействию данному виду преступлениям. Рассматривается передовой зарубежный опыт в данной сфере, а также опыт Академии МВД Республики Узбекистан. На основе анализа мнений ученых и зарубежного опыта формируются предложения по совершенствованию данного направления деятельности.

Ключевые слова: киберпреступность, виртуальное пространство, образование, специальность, информация, информационная безопасность, искусственный интеллект.

CURRENT ISSUES IN TRAINING PERSONNEL TO COMBAT CYBERCRIME

Annotation. The article reveals the current state and development trends of cybercrime, which necessitates specialized training to combat this type of crime. The advanced foreign experience in this area, as well as the experience of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, is considered. Based on an analysis of the opinions of scientists and foreign experience, proposals are formed to improve this activity area.

Keywords: cybercrime, virtual space, education, specialty, information, information security, artificial intelligence.

Цифровая трансформация общества и государства влечет за собой рост новой высокотехнологичной преступности, появление её новых видов и способов совершения. В сферу оказания государственных и банковских услуг, судебно-правовой сферы, медицины, систему обороны и во многие другие направления

жизни общества динамично внедряются информационные технологии, искусственный интеллект и машинное обучение, что обусловливает необходимость особого внимания вопросам обеспечения информационной безопасности, а также учета рисков и угроз злонамеренного использования, хищения, кражи данных, криптопреступности, мошенничества в информационном пространстве и многое другое.

Киберпреступность породила ранее неизвестный вид банд – организованные преступные группы, вооруженные новым видом оружия – кибероружием, применяемым для нападений (кибератак) на граждан и организации [1].

А.В. Симоненко отмечает выраженную экспансию организованной преступности в киберпространстве. В частности, преступными сообществами создаются интернет-ресурсы для осуществления и координации криминальной деятельности, осуществляется проникновение в легальный интернет-бизнес, освоение новейших информационных технологий для наращивания объемов и повышения эффективности преступлений [2, с. 6–14].

Несомненно, данная категория преступлений требует особой подготовки кадров для правоохранительных органов, которые будут заниматься их расследованием. Традиционный формат подготовки специалистов, направленный на охват юридических дисциплин в данном случае, не позволит решать все поставленные задачи.

Профессиональная подготовленность сотрудников государственных и правоохранительных органов, служб обеспечения информационной безопасности организаций и учреждений требует комплекса знаний как юридических, так и технических дисциплин в сфере обеспечения информационной безопасности. При этом, В.А. Северин отмечает тенденции ведомственного и корпоративного подхода к процессам подготовки кадров, а также необходимость комплексного единого подхода к подготовке кадров [3, с. 16–20].

Практически все государства мира уделяют особое внимание подготовке специалистов по противодействию киберпреступности. В ЕС, США, КНР, Индии, Южной Корее, России, Беларуси, Казахстане и многих других государствах ведется подготовка специалистов по обеспечению информационной безопасности, радиоразведке, выявлению и оперативно-техническому обеспечению раскрытия, расследования и профилактики киберпреступлений, компьютерной экспертизе при расследовании преступлений [4].

К примеру, опыт Московского университета МВД России имени В.Я. Кикотя, Краснодарского университета МВД России, Воронежского института МВД России, Санкт-Петербургского университета МВД России, Алматинской академии МВД Республики Казахстан и ряда других учебных заведений, показывает целесообразность создания отдельного Факультета, на базе которого будет осуществляться подготовка указанных специалистов.

Должны отметить, что в Республике Узбекистан подготовка базовых специалистов в области обеспечения информационных технологий и информационной безопасности осуществляется в Ташкентском университете информационных технологий имени Мухаммада аль Хорезми и Университете Инха. При этом, специалистов с базовым юридическим образованием готовят Ташкент-

ский государственный юридический университет, Университет мировой экономики и дипломатии, Исламский университет, Академия МВД, Институт СГБ и несколько факультетов других ВУЗов.

Исходя из потребностей правоприменительной практики, возникает необходимость создания программы повышения квалификации и переподготовки кадров, осуществляющих оперативно-розыскные мероприятия, дознание и следствие по преступлениям, связанным с информационной безопасностью и киберпреступностью в целом.

Начиная с 2021 г. для курсантов Академии МВД было организовано факультативное обучение по курсам «Организация противодействия киберпреступности», «Методы проведения оперативно-розыскных мероприятий при раскрытии киберпреступлений», организованные с привлечением специалистов всех структур МВД, задействованных в борьбе с киберпреступностью.

Вместе с тем, на сегодняшний день в соответствии с Постановлением Президента Республики Узбекистан от 25 июля 2022 года, а также на основании приказа Министерства внутренних дел Республики Узбекистан от 29 августа 2022 года «Об организации системы подготовки кадров по направлению информационной безопасности в качестве эксперимента в 2022 г.» Академией МВД Республики Узбекистан была сформирована отдельная учебная группа, обучающаяся по направлению 60420100 – Юриспруденция (в сфере информационной безопасности).

Среди преподаваемых дисциплин:

– Основы и технологии программирования. Системы управления базами данных;

– Основы информационной безопасности. Криптография и криптоталиль. Безопасность программного обеспечения;

– Компьютерные сети и сетевая безопасность;

– Компьютерная графика;

– Основы цифровой криминалистики;

– Технические и программные основы кибербезопасности в IIO;

– Технологии искусственного интеллекта;

– Социальная инженерия.

Курсанты группы, проходящих обучение по данному направлению, ежедневно во второй половине дня проходят практическую стажировку в Управлении по борьбе с преступлениями в сфере информационных технологий ГУВД г. Ташкента.

В качестве эксперимента в Академии была сформирована «Группа мониторинга Интернета». Данная группа выявляет интернет-ресурсы, содержащие запрещенный законодательством контент, а также проводит ряд иных мероприятий по противодействию киберпреступности.

Начиная с января 2022 года по сегодняшний день Группой было выявлено более 2,5 тыс пропагандирующих магазины по продаже наркотиков и интимные услуги, религиозный экстремизм, идеи фанатизма и терроризма в Интернете, из которых соответствующими практическими подразделениями было заблокировано свыше 2,3 тыс.

Кроме того, Академия МВД Республики Узбекистан осуществляет тесное сотрудничество с международными организациями в рамках организации и проведения научно-практических мероприятий, направленных на повышение квалификации профессорско-преподавательского состава и курсантов Академии в сфере противодействия киберпреступности.

В частности, Организация по безопасности и сотрудничеству в Европе (ОБСЕ) с июня по ноябрь 2023 г. провела в Академии МВД курс вебинаров по темам, посвященным программам – вымогателям, мошенничеству в сфере онлайн-платежей, криминальным схемам Dark web, а также преступлениям, связанным с криптовалютой.

13-14 ноября 2023 г. Управление ООН по борьбе с терроризмом, Региональный центр ООН по превентивной дипломатии для Центральной Азии, Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма, Федеральная служба по финансовому мониторингу Российской Федерации, а также Институт стратегических и межрегиональных исследований при Президенте Республики Узбекистан и Служба государственной безопасности организовали проведение в Академии для слушателей магистратуры и профессорско-преподавательского состава региональную консультацию на тему «Противодействие использованию криптовалют при финансировании терроризма».

Вместе с тем, должны отметить, что киберпреступность динамично распространяется во всем мире и на сегодняшний день вопрос совершенствования подготовки кадров по её противодействию приобретает особую актуальность. Исходя из вышеуказанного в Академии МВД Республики Узбекистан предлагается:

С учетом передового зарубежного опыта необходимо создание специализированного факультета по подготовке специалистов по противодействию киберпреступности.

В составе данного факультета предусмотреть кафедры киберправа, информационной безопасности, специальных информационных технологий и естественнонаучных дисциплин, а также Центра цифровой криминалистики.

В обучение специалистов по направлению противодействие киберпреступлениям необходимо включить дополнительно учебные дисциплины, которые предусмотрены учебным планом аналогичных зарубежных ВУЗов.

Срок обучения в бакалавриате предусмотреть 4 года. На сегодняшний день срок обучения в бакалавриате по всем специальностям Академии МВД Республики Узбекистан составляет 3 года.

К учебному процессу на Факультете привлечь специалистов Центра кибербезопасности, ГЭКЦ, Управления уголовно-правовой статистики и оперативно-справочных учетов МВД Республики Узбекистан, ГУП «Центр кибербезопасности», Ташкентского университета информационных технологий имени Мухаммада аль Хорезми, Инха и других специализированных ВУЗов.

В целях организации соответствующего уровня учебного процесса данных специалистов необходимо обеспечить необходимую материально-техническую базу (киберлабораторию, киберполигон, оснащенные необходимым современ-

ным компьютерным и серверным оборудованием, а также программным обеспечением, включающим технико-криминалистические средства обнаружения и фиксации электронных и цифровых следов, предусматривающих функции фиксации и исследования цифровых следов, в том числе сети Darknet).

Привлечь IT-парки для создания образовательных онлайн-платформ, учебных и методических материалов для подготовки курсантов Факультета.

Список использованной литературы

1. Крупные атаки хакеров в 2001–2016 годах [Электронный ресурс] // Информационное агентство России ТАСС. URL: https://tass.ru/info/1408961.

2. Симоненко А.В. Актуальные вопросы подготовки кадров для противодействия киберпреступности // Вестник Краснодарского Университета МВД России. – 2021. – № 4 (54). – С.6–14.

3. Северин В.А. Комплексный подход подготовки кадров для обеспечения кибербезопасности: вызовы и проблемы // Лоббирование в законодательстве. – 2023. – Т. 2. – № 2. – С. 16–20.

7. Расулев А.К. Турсунов А.С. Противодействие киберпреступности – требование времени [Электронный ресурс] // URL: https://iiv.uz/ru/news/ counteracting-cybercrime-is-a-requirement-of-the-time.

МАЗМҰНЫ • СОДЕРЖАНИЕ • CONTENTS

Киберқылмысқа қарсы іс-қимыл: жай-күйі, тенденциялары, болашағы [Электрондық басылым]: халықаралық ғылыми – практикалық конференция материалдарының жинағы, Қарағанды қ.

2023 жылғы 01 желтоқсан

Жауапты редактор
з.ғ.к., доцент
О.Т. Сейтжанов

Редакторлар
Е.П. Шульгин
А.Б. Ахмадиев

Техникалық редактор
П.А. Тафинцев

Қазақстан Республикасы ІІМ Б. Бейсенов атындағы Қарағанды академиясының киберқауіпсіздік және ақпараттық технологиялар кафедрасы

Формат 60×84$^{1}/_{8}$.
Электрондық басылым
Шартты баспа табақ 26,51.

Противодействие киберпреступности: состояние, тенденции, перспективы [Электронное издание]: сборник материалов международной научно-практической конференции, г. Караганда

01 декабря 2023 жылғы

Ответственный редактор
к.ю.н., доцент
О. Т. Сейтжанов

Редакторы
Е.П. Шульгин
А.Б. Ахмадиев

Технический редактор
П.А. Тафинцев

Кафедра кибербезопасности и информационных технологий Карагандинской академии МВД Республики Казахстан им. Б. Бейсенова

Формат 60×84$^{1}/_{8}$.
Электронное издание
Усл. печ. л. 26,51.