АКАДЕМИЯ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ПРИ ГЕНЕРАЛЬНОЙ ПРОКУРАТУРЕ РЕСПУБЛИКИ КАЗАХСТАН

ВОПРОСЫ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ, СОВЕРШЕННЫХ В СЕТИ ИНТЕРНЕТ: ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ

Монография

Косшы, 2022

УДК 343.13
ББК 67.411
В __

Рецензенты: доктор юридических наук, профессор Ханов Т.А., доктор юридических наук, профессор Журсимбаев С.К.

Под общей редакцией проректора-директора Межведомственного научно-исследовательского института Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Шушиковой Г.К.

Вопросы расследования уголовных правонарушений, совершенных в сети Интернет: теоретические и практические аспекты: Монография / [Коллектив авторов]. Под общ. ред. Г.К. Шушиковой. – Косшы: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, 2022. – 110 с.

Монография посвящена актуальным проблемам уголовно-правового и процессуального урегулирования проблемных вопросов расследования уголовных правонарушений совершенных в сети Интернет. Авторами исследованы теоретические, нормативные, организационные и другие вопросы, направленные на недопущение нарушений прав человека.

С новых позиций рассматриваются вопросы применения международных правовых актов и их положений в национальном законодательстве, систематизации отдельных терминов в нормах уголовного закона.

Издание предназначено для сотрудников правоохранительных органов, а также для научных работников, преподавателей, докторантов, магистрантов и студентов вузов, в том числе ведомственных.

ISBN _____

УДК 343.13
ББК 67.411

Рекомендовано к опубликованию решением Учебно-методического совета Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан.

Сведения об авторах

Имангалиев Н.К., главный научный сотрудник Центра исследования проблем уголовной политики и криминологии Межведомственного научно-исследовательского института (далее - МНИИ) Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан (далее - Академия), кандидат юридических наук, ассоциированный профессор – *подразделы 1.3 (в соавторстве с Абдукадировой С.А.), 1.4. (в соавторстве с Алимкуловой С.А.), 2.4.*

Алимкулова М.А - *введение; подраздел 1.4 (в соавторстве с Имангалиевым Н.К).*

Абдукадирова С.А., старший научный сотрудник Центра координации исследований и изучения проблем правоохранительной деятельности МНИИ Академии, магистр юридических наук - *подразделы 1.3 (в соавторстве с Имангалиевым Н.К), 2.2, (в соавторстве с Тынышпаевой А.А.).*

Ажибаев М.Г., ведущий научный сотрудник Центра координации исследований и изучения проблем правоохранительной деятельности МНИИ Академии, магистр юридических наук - *подразделы 1.1, 2.1.*

Медиев Р.А., доцент Кафедры специальных юридических дисциплин Института послевузовского образования Академии, доктор Phd, ассоциированный профессор - *подраздел 1.2, 2.3.*

Тынышпаева А.А., кандидат юридических наук, доктор социологических наук - *подраздел 2.2, (в соавторстве с Абдукадировой С.А.).*

Содержание

Нормативные ссылки

Конституция Республики Казахстан (принята на республиканском референдуме 30.08.1995 года).

Уголовный кодекс Республики Казахстан от 03.07.2014 года №226-V ЗРК.

Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 года № 231-V ЗРК.

Кодекс Республики Казахстан об административных правонарушениях от 05.07.2014 года № 235-V ЗРК.

О правоохранительной службе: Закон Республики Казахстан от 06.01.2011 года №380-IV.

Об оперативно-розыскной деятельности: Закон Республики Казахстан от 15.09.1994 года № 154-XIII.

О Концепции правовой политики Республики Казахстан на период с 2010 по 2020 годы: Указ Президента Республики Казахстан от 24.08.2009 года №858.

Нормативные ссылки использованы по состоянию на 01.01.2021 года.

Термины и определения

Аккаунт - технология для соединения пользователя и информационного сервиса и/или компьютерной сети.

Активный цифровой след появляется, когда пользователь намеренно публикует свои персональные данные, чтобы рассказать о себе на веб-сайтах и в социальных сетях. Заинтересованные стороны пассивно или активно собирают эту информацию. В зависимости от объема этой информации можно без усилий собрать много данных о пользователе с помощью простых поисковых систем.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система.

Аутентификация информации - установление подлинности информации исключительно на основе внутренней структуры самой информации, независимо от источника этой информации, установление законным получателем (возможно арбитром) факта, что полученная информация наиболее вероятно была передана законным отправителем (источником) и при этом не была заменена или искажена.

APT-угроза, APT-атака - сложная, технологически продвинутая атака, направленная на получение конфиденциальных данных в течение длительного периода.

Аутсорсинг - выполнение отдельных задач проекта компании сторонними организациями, специализирующимися в этой области.

Безопасность информации - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение втайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Безопасность информационной технологии - защищенность технологического процесса переработки информации.

Безопасность оконечных - обеспечение безопасности устройств, находящихся в оконечных точках сети. К числу таких устройств относятся используемые сотрудниками мобильные устройства (планшеты, ноутбуки).

Биометрическая аутентификация - аутентификация, опирающаяся на уникальные биологические показатели человека. К основным биометрическим идентификаторам относятся отпечатки пальцев, рукописные подписи, образцы голоса, результаты сканирования сетчатки и радужной оболочки глаза, формы ладони или черт лица.

Бот-сети - так называют собрание подключенных к Интернету программ, которые могут взаимодействовать с другими аналогичными программами для выполнения определенных задач. Бот-сети бывают легальными и

нелегальными, и именно нелегальные чаще всего используются для рассылки спама или проведения DDoS атак. Они создаются троянцами или вредоносными программами и централизовано управляются «хозяином», за что бот-сети еще называют **зомби-сетями.**

Бра́узер, или **веб-обозрева́тель** (от англ. *web browser*, МФА; устар. **бро́узер**) – прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных и их каталогов; управления веб-приложениями; а также для решения других задач. В глобальной сети браузеры используют для запроса, обработки, манипулирования и отображения содержания веб-сайтов. Многие современные браузеры также могут использоваться для обмена файлами с серверами FTP, а также для непосредственного просмотра содержания файлов многих графических форматов (gif, ipeg, png, svg), аудио- и видеоформатов (mp3, mpeg), текстовых форматов (pdf, djvu) и других файлов.

Верификация (проверка) цифровой подписи документа - проверка соотношения, связывающего хэш-функцию документа, подпись под этим документом и открытый ключ подписавшего пользователя. Если рассматриваемое соотношение оказывается выполненным, то подпись признается действительной, а сам документ - подлинным, в противном случае документ считается измененным, а подпись под ним - недействительной.

Вирус - компьютерная программа, которая может тиражировать сама себя и таким образом переходить с одного компьютера на другой. Вирус – это код, который может внедряться в существующие на компьютере файлы, иногда с целью повреждения, а в некоторых случаях и уничтожения информации.

Взаимная (перекрестная) сертификация - двусторонний процесс сертификации двух доверенных удостоверяющих центров.

Владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносное ПО (вредоносные программы) - программное обеспечение, направленное на выполнение несанкционированных вредоносных действий на компьютере.

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях. К ВТСС относятся: телефонные средства и системы; средства и системы передачи данных, системы радиосвязи; средства и системы охранной и пожарной сигнализации; средства и системы оповещения и сигнализации; контрольно-измерительная аппаратура; средства и системы

кондиционирования; средства и системы проводной радиотрансляционной сети и приема программ радиовещания и телевидения (абонентские громкоговорители, системы радиовещания, телевизоры и радиоприемники и т.п.); средства электронной оргтехники; иные технические средства и системы.

Домен - онлайн-адрес сайта, место его размещения в интернете. С технической позиции доменный адрес - запись в базе данных. Когда пользователь указывает в поисковой строке доменное имя, компьютер понимает, какой сайт необходимо показать и по какому адресу отправить запрос.

Internet Protocol (**IP**, досл. «межсетевой протокол») – маршрутизированный протокол сетевого уровня стека TCP-IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является *адресация* сети.

Интернет-прова́йдер - организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги. К основным услугам интернет-провайдеров относятся: широкополосный доступ в Интернет, коммутируемый доступ в Интернет, беспроводной доступ в Интернет.

Контент - содержимое веб-страниц, соцсетей, каналов в мессенджерах и разных программ. Мы сталкиваемся с контентом ежедневно: это видео на YouTube, новости, посты в авторских каналах Telegram, статьи в корпоративных блогах.

Ку́ки (англ. *cookie*, букв. - «печенье») небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для аутентификации пользователя, хранения персональных предпочтений и настроек пользователя, отслеживания состояния сеанса доступа пользователя, сведения статистики о пользователях.

Логин –слово, которое будет использоваться для входа на сайт или сервис. Очень часто логин совпадает с именем пользователя, которое будет видно всем участникам сервиса, но иногда никнейм может задаваться отдельно.

Мобильный банкинг - услуга, предоставляемая банком или другим финансовым учреждением, которая позволяет его клиентам осуществлять финансовые транзакции удаленно с помощью мобильного устройства, такого как смартфон или планшет.

Мессенджер - программа (приложение) для смартфона или персонального компьютера, позволяющая мгновенно обмениваться с друзьями текстовыми сообщениями, телефонными звонками и разговаривать с использованием видеосвязи.

Никне́йм, (также сетевое имя) - псевдоним, используемый пользователем в Интернете, обычно в местах общения. Никнейм характеризует представившегося и является многофункциональным средством добавления выразительности в высказывания.

Номер IMEI (International Mobile Equipment Identity) - уникальное 15-значное число, которое присваивается каждому мобильному устройству, работающему в сетях GSM, UMTS, LTE, 5G. Номер **IMEI** состоит из нескольких блоков: первые 8 цифр **– код** Type Allocation Code (TAC), который показывает конкретную модель устройства.

Пароль (фр ***Parole*** - слово) **-** условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов, и предназначенный для подтверждения личности или полномочий. Если допустимо использование только цифр, то такую комбинацию иногда называют ПИН-кодом (от английской аббревиатуры PIN - персональный идентификационный номер).

Пассивный цифровой след - данные, собранные без ведома владельца. Также называют выхлопными данными.

Порт (англ. ***port***) - целое неотрицательное число, записываемое в заголовках протоколов транспортного уровня сетевой модели OSI (TCP, UDP, SCTP, DCCP).

Провайдеры SIP –организации, использующие для предоставления услуги IP-телефонии протокол **SIP -** и сегодня это наиболее выгодный и доступный способ связи. Еще одним преимуществом сотрудничества **SIP провайдером** является возможность совершать дешевые звонки на мобильные телефоны и межгород.

Руткит - набор программных средств, обеспечивающих: маскировку объектов; управление; сбор данных.

Сетевая модель OSI (The Open Systems Interconnection model) – сетевая модель стека (магазина) сетевых протоколов OSI/ISO. Посредством данной модели различные сетевые устройства могут взаимодействовать друг с другом. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Спам - массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получить. Распространителей спама называют спамерами.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа

Сессия (от лат. – sessio - заседание, англ. – session) – промежуток времени, охватывающий работу пользователя в **Интернете** с момента открытия первой и до последней ссылок. Рассчитывается как разница во времени между начальным и финальным запросами.

Cellebrite UFED – автономное устройство для снятия с мобильного телефона данных для расследования ИТ-инцидентов, как на месте происшествия, так и в криминалистической лаборатории. **UFED** расшифровывается как Universal forensic extraction device, универсальный прибор для извлечения криминалистических данных.

CVV2 (англ. *card verification value 2*) **–** трёхзначный код проверки подлинности карты платёжной системы Visa. Другие платёжные системы имеют схожие технологии, к примеру, аналогичный защитный код для карт MasterCard носит название *card validation code 2* (**CVC2**), защитный код для

платежной системы «МИР» получил название card verification parameter 2 (**CVP2**). Как правило, наносится на полосе для подписи держателя после номера карты либо после последних 4 цифр номера карты способом индент-печати. Используется в качестве защитного элемента при проведении транзакции в среде CNP (card not present).

Токен - устройство хранения криптографических ключей, аппаратный ключ.

Транспортировка ключа - защищенный процесс передачи ключа от одного пользователя к другому.

Хеш-функция, или функция свёртки - функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием.

Data Lake (Озеро данных) – метод хранения данных системой или репозиторием в натуральном (RAW) формате, который предполагает одновременное хранение данных в различных схемах и форматах. Обычно используется blob-объект (binary large object) или **файл**.

RAID *(*англ. *Redundant Array of Independent Disks)* массив - избыточный массив независимых (самостоятельных дисков) - технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности.

Хостинг-провайдер - организация, оказывающая профессиональные услуги хостинга или, иными словами, предоставляющая дисковое пространство и мощности сервера для размещения вашего сайта в Сети.

Фейк (англ. *Fake* - подделка) - что-либо ложное, недостоверное, сфальсифицированное, выдаваемое за действительное, реальное, достоверное с целью ввести в заблуждение.

Фейковый аккаунт - аккаунт, который является недостоверной копией аккаунта какого-либо пользователя, зарегистрировавшегося на том же ресурсе.

Резервные копии - копии файлов, которые сохраняются на сервере, жестком диске, компьютере или съемном диске на тот случай, если оригиналы окажутся утеряны.

Цифровой след (или *цифровой отпечаток*; англ. *digital footprint*) - уникальный набор действий в Интернете или на цифровых устройствах. Во Всемирной паутине «интернет-след», также известный как *«кибер-тень», «электронный след»* или *«цифровая тень»,* - это информация, оставленная в результате просмотра веб-страниц и сохраненная в виде куков. Термин обычно применяется к одному пользователю, но может также относиться к какой-либо коммерческой компании, организации или корпорации.

Электро́нная по́чта - технология и служба по пересылке и получению электронных сообщений между пользователями компьютерной сети.

Обозначения и сокращения

АПК	- Агентство по противодействию коррупции Республики Казахстан
АПО	- Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан
АРРФР	- Агентство по регулированию и развитию финансового рынка Республики Казахстан
АФМ	- Агентство по финансовому мониторингу Республики Казахстан
БРИКС	- Экономический союз пяти государств (Бразилия, Россия, Индия, Китай, Южная Африка)
ГК	- Гражданский кодекс Республики Казахстан
ГП	- Генеральная прокуратура Республики Казахстан
ЕК	- Европейская комиссия
ЕП	- Европейский парламент
ЕРДР	- Единый реестр досудебных расследований
ЕврАзЭС	- Евразийский экономический союз
ЕС	- Европейский Союз
ИИ	- искусственный интеллект
ИИН	- индивидуальный идентификационный номер
ИКТ	- информационно-коммуникационные технологии
КПСиСУ	- Комитет по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан
КУИ	- Книга учета информации
МВД	- Министерство внутренних дел Республики Казахстан
МЦРиАП	- Министерство цифрового развития и аэрокосмической промышленности Республики Казахстан
ООН	- Организация Объединенных Нации
ПК	- персональный компьютер
ПО	- программное обеспечение
РК	- Республика Казахстан
СЕ	- Совет Европы
СНГ	- Содружество Независимых Государств
СЭР	- Служба экономических расследований
УК	- Уголовный кодекс
УПК	- Уголовно-процессуальный кодекс
ШОС	- Шанхайская организация сотрудничества
ЭИЦД	- Электронный информационно-учетный документ
США	- Соединенные Штаты Америки

Введение

В статье 1 Конституции РК закреплено, что Республика Казахстан провозглашает себя демократическим, светским, правовым государством, высшими ценностями которого являются человек, его права и свободы [1].

В соответствии с Основным законом государства гарантией их защиты является действенный механизм, направленный на обеспечение прав человека.

Проводимая в нашей стране реформа по исполнению Национального плана развития Республики Казахстан до 2025 года [2] дала старт новым позитивным преобразованиям, комплексу мероприятий по совершенствованию защиты прав человека, одной из которых является борьба с киберпреступностью.

Широкое применение информационно-коммуникационных технологий во всех значимых сферах жизни общества стало неотъемлемой характеристикой современности.

Динамичное развитие общества привело к формированию в третьем тысячелетии единого мирового информационного пространства, основанного на развитии глобальных информационно-телекоммуникационных систем, использовании унифицированных международных протоколов информационного обмена и методов удаленного доступа к базам данных и знаний различного назначения.

На сегодняшний день в качестве технологической информационно-телекоммуникационной среды Интернет определяет новые способы совершения преступлений и соответственно технические средства, специфичные в процессе раскрытия и расследования преступлений.

Однако, в связи с высокими темпами развития глобализации общественной жизни произошел существенный рост количества правонарушений с использованием IT-технологий.

Согласно данным КПСиСУ, за период 2020-2021 годы в Казахстане число зарегистрированных преступлений, совершенных с использованием сети Интернет, выросло в 19 раз. В связи с чем возникает угроза нарушения работы информационных ресурсов государства, а также законных прав и интересов личности в информационной среде.

Под преступлениями, совершенными в сфере информационных технологий, следует понимать предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы информационной системы или сетей телекоммуникаций, причиняющие вред законным интересам собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина.

Доминирующее положение среди уголовных правонарушений, совершаемых в сети Интернет, занимают мошенничество (ст.190 ч.2 п.4 УК РК) и сбыт наркотических средств (ст.299-1 УК РК).

В связи с наблюдающимся ухудшением криминогенной ситуации в стране, обусловленной ростом киберпреступлений, необходимо повысить эффективность следственной практики по раскрытию и расследованию уголовных правонарушений в киберпространстве.

Следует отметить, что уголовные правонарушения, совершенные в сети Интернет, имеют свою специфику и носят латентный характер. Недостаточный уровень подготовки сотрудников правоохранительных органов по раскрытию и расследованию киберпреступлений способствуют уводу от ответственности виновных лиц и формированию атмосферы безнаказанности в этой сфере.

Выявление и расследование таких правонарушений затруднено сложностями проведения следственных действий, а сбор доказательств осуществляется новыми для следственной практики способами, имеющими недостаточную теоретико-методологическую проработку их основных аспектов.

В настоящее время наблюдается тенденция трансформации понятийного аппарата по вопросам противодействия уголовным правонарушениям, совершаемым в сети Интернет.

С целью повышения эффективности борьбы с преступлениями, совершаемыми с использованием компьютерных технологий, в УК РК была введена Глава 7, предусматривающая ответственность за уголовные правонарушения в сфере информатизации и связи.

Разнородность правового закрепления составов преступлений, совершенных посредством сети Интернет в уголовном законодательстве ставит проблему унификации правового пространства на государственном уровне.

Требуется дальнейшая разработка научно обоснованных рекомендаций как по применению теоретических и практических норм, так и по выработке предложений по дальнейшему совершенствованию мер по противодействию преступлений, совершенных посредством сети Интернет, а также приведение в соответствие понятийного аппарата, применяемого в уголовно-процессуальной сфере при расследовании указанной категорий дел.

Рассматривая ретроспективу преступного использования сети Интернет следует обратить внимание, что в развитых странах вопрос киберпреступности рассматривается и реализуется на протяжении более 20 лет.

Наиболее значимым на сегодняшний день результатом международного сотрудничества в борьбе с преступностью, связанной с использованием высоких технологий, является Конвенция Совета Европы о киберпреступности. В подготовке текста участвовали 43 государства - членов Совета, также Канада, Япония, США (имеющие статус наблюдателей) и Южно-Африканская Республика. В Конвенции закреплен механизм эффективного международного сотрудничества и координации при проведении расследований и уголовного преследования.

В свою очередь, возможности и перспективы принимаемых мер противодействия киберпреступности Казахстаном позволяют ему находиться в мировом сообществе на высоком уровне.

Изучение научной литературы свидетельствует о том, что отдельные стороны проблем выявления и расследования правонарушений, совершенных посредством сети Интернет, в частности методики выявления, способов расследования нашли свое отражение в работах отечественных ученых Б.Х. Толеубековой, С.Е. Каиржановой, А.А. Ешназарова, Л.А. Темиржановой, С.М. Мамбетова, Т.А. Ханова, Н.К. Имангалиева, А.Т. Завотпаевой, А.В. Сырбу и российских ученых В.А. Мещерякова, Гаврилина Ю.В., Аносова А.В., Баранова В.В., Н.П. Яблокова, Г.А. Густова, А.Т. Аристархова, С.Н. Чурилова, А.И. Трусова, Р.С. Белкина, Е.Н. Паршина, В.А. Образцова, С.П. Павликова и других.

Монография подготовлена с целью повышения эффективности расследования уголовных правонарушений, совершенных в сети Интернет, совершенствования действующего законодательства и деятельности правоохранительных органов, а также для использования при подготовке учебно-методических материалов профессорско-преподавательским составом ВУЗов.

Раздел I. Родовая криминалистическая характеристика уголовных правонарушений, совершаемых в сети Интернет

1.1 Понятие и содержание криминалистической характеристики уголовных правонарушений, совершаемых в сети Интернет

Ключевым элементом раскрытия уголовного правонарушения является криминалистическая характеристика преступления, представляющая собой воссоздание картины совершенного противоправного деяния, выявление связанных с этим деянием фактов, лиц, явлений.

Особое значение в данном контексте приобретают фундаментальные понятия и их содержание, используемые при описании криминалистической характеристики уголовных правонарушений, совершенных в сети Интернет.

Как отмечает Головин А.Ю.: «для существования и функционирования любой области научного знания необходим единый унифицированный объем понятий, описывающий системные процессы» [3]. Данное мнение, полагаем, подчеркивает важность применения унифицированных понятий в процессе научного познания.

Следует отметить, что с середины XX века и до настоящего времени учеными не выработано единое понятие криминалистической характеристики преступления, ведутся научные споры, выдвигаются научные гипотезы и мнения.

По мнению Яблокова Н.П., криминалистическая характеристика преступления представляет собой систему описания криминалистически значимых признаков вида, группы и отдельного преступления, проявляющихся в особенностях способа, механизма и обстановки его совершения. Криминалистическая характеристика преступления должна давать представление о преступлении, личности его субъекта и иных обстоятельствах, об определенной преступной деятельности, а цель криминалистической характеристики – обеспечение успешного решения задач по раскрытию, расследованию и предупреждению преступлений [4].

Густов Г.А. криминалистическую характеристику рассматривает как «основанное на практике правоохранительных органов и криминалистических исследованиях описание преступления как реального явления, имеющее своей целью оптимизацию процесса раскрытия и расследования преступления и решения задач правосудия» [5].

Аристархова А.Т. считает, что под криминалистической характеристикой преступлений понимается, в первую очередь, определенная совокупность взаимосвязанных криминалистически значимых информационных элементов, включающая в себя обобщенные и аналитически обработанные сведения о структуре и механизме преступной деятельности определенного вида, ориентированные на использование в процессе методического обеспечения процесса их раскрытия и расследования и непосредственное практическое использование по конкретным уголовным делам [6].

Указанные мнения ученых сходны в одном – криминалистическая характеристика преступления направлена на раскрытие и расследование совершенного уголовного правонарушения.

Это позволяет сделать вывод о том, что криминалистическая характеристика должна содержать в себе различные элементы, способствующие выявлению взаимосвязи между событиями, субъектами, объектами, предметами, обстановкой до совершения уголовного правонарушения, в процессе него, после его совершения. То есть, фактически содержать в себе все процессы, связанные с противоправным деянием, происходившие в рамках уголовного правонарушения на всех его стадиях.

При этом, важным является то, что в определениях криминалистической характеристики преступления содержатся уголовно-правовые, криминологические аспекты. В частности, это субъект, предмет и объект преступления, характеристика личности предполагаемого преступника и другие.

Это позволяет утверждать, что все составные части криминалистической характеристики детерминированы характеристиками совершения преступного деяния.

В научной среде по данному вопросу высказываются мнения относительно тождественности понятий «криминалистическая характеристика преступления» и «механизм преступления».

По данному вопросу поддерживаем мнение Чурилова С.Н., который анализируя соотношение понятий «криминалистическая характеристика преступления» и «механизм преступления», приходит к выводу о том, что эти понятия разнопланового характера, не совпадают, хотя и связаны между собой. По его мнению, понятие «механизм преступления» отражает преступление на уровне единичного явления, а понятие «криминалистическая характеристика преступления» относится «к массе преступлений одного вида или разновидности» [7].

Как и во многих других системах, основанных на научно-теоретических познаниях, значимость криминалистической характеристики преступлений определенного вида состоит не столько в выделении самих этих элементов как таковых, сколько в установлении взаимосвязей между выделенными элементами.

Целью исследования криминалистической характеристики является разработка достаточно логичных и обоснованных направлений по выстраиванию картины следственного поиска путем использования и корреляции выявленных взаимосвязей между разрозненными криминалистически значимыми элементами.

Это позволит при первичном построении следственных версий установить один или несколько элементов расследуемого преступления, которые помогут выявить другие, не установленные ранее элементы расследуемого события.

Не менее важным при раскрытии понятия криминалистическая характеристика преступления является детерминация понятия

«криминалистически важная информация», которая взята за основу многими учеными, в том числе, мнения которых приведены выше. Данная детерминанта позволит более ясно понять содержание криминалистической характеристики преступления, речь о котором в рамках данного подраздела будет изложена ниже.

Информация (от лат. informatio - осведомление, разъяснение, изложение, от лат. informare придавать форму) - в широком смысле абстрактное понятие, имеющее множество значений, в зависимости от контекста. В узком смысле этого слова - сведения (сообщения) независимо от формы их представления. В настоящее время не существует единого определения термина информация. С точки зрения различных областей знания данное понятие описывается своим специфическим набором признаков [8, С. 45].

В юридической литературе общее определение информации, в основу которого положено отражение как свойство материи, было впервые дано в 1976 году Трусовым А.И., который считал, что: «Информация охватывает отражение предметов и явлений в человеческом сознании, явлений и процессов друг в друге, вне связи с сознанием». В то же время, авторы, пытавшиеся дать определение данной универсальной категории, отмечали, что термин «информация» обладает широчайшим смысловым полем в связи с чем трудно поддается определению [9, С. 238].

При использовании понятия информация в криминалистической науке, она становится более конкретным, приобретает свойственные совершенному уголовному правонарушению следы.

Криминалистически значимая информация - это сведения, данные, имеющие отношения к раскрытию и расследованию преступления. Подразделяются на доказательственную информацию, содержащуюся в доказательствах, и ориентирующую - полученную из не процессуальных источников и доказательственного значения не имеющую; последняя может быть использована для выдвижения версий, определения направлений расследования, планирования следственных действий, прогнозирования возможной линии поведения участников расследования и т.п. Криминалистически значимой может оказаться любая информация любой природы [10, С. 15].

Белкин Р.С. дает следующее определение криминалистически важной информации: «Доказательства судебные, любые фактические данные, на основе которых в установленном законом порядке органы дознания, следователь, суд устанавливают наличие или отсутствие общественно опасного деяния, виновность лица, совершившего это деяние, и иные обстоятельства, имеющие значение для разрешения дела» [11, С, 72].

Иными словами, к криминалистически важной информации можно отнести все предметы, лица, события и т.д., связанные как прямо, так и косвенно с совершенным уголовным нарушением.

Например, следующее определение криминалистически важной информации дается в ст.111 УПК РК (Доказательства и доказывание).

«Доказательствами по уголовному делу являются законно полученные фактические данные, на основе которых в определенном настоящим Кодексом порядке орган дознания, дознаватель, следователь, прокурор, суд устанавливают наличие или отсутствие деяния, предусмотренного УК РК, совершение или несовершение этого деяния подозреваемым, обвиняемым или подсудимым, его виновность либо невиновность, а также иные обстоятельства, имеющие значение для правильного разрешения дела».

В этой же статье закреплены способы получения криминалистически важной информации. Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; протоколами процессуальных действий и иными документами [12].

Исходя из вышеизложенного, можно сделать вывод о том, что криминалистическая характеристика преступления - это комплекс взаимосвязанных научно-практических данных об уголовном правонарушении, в котором отражены присущие только ему сведения, факты, события, имеющие важное значение для его раскрытия и расследования.

Для следственной практики выработка соответствующей криминалистической характеристики уголовных правонарушений является важным условием для формирования методики расследования преступлений.

Ее важность заключается в создании научно-информационной основы для практической деятельности по раскрытию, расследованию и последующей профилактике.

Павликов С.Г. обоснованно отмечает, что практическое значение криминалистической характеристики преступления заключается в том, что ее изучение позволяет правильно диагностировать следственные ситуации, складывающиеся на первоначальном и последующем этапах расследования, определить направления расследования, выдвинуть следственные версии, определить оптимальные пути их проверки, принять правильные тактические решения [13, С. 46].

Методическое значение криминалистической характеристики определяется тем, что она аккумулирует в себе сведения о закономерностях отражения данного явления в носителях информации. Она характеризует не норму закона и законодателя, а преступную деятельность, как явление объективной действительности и субъекта ее совершившего. Преступление, проходя через волю и сознание, навыки преступника переносит на носителей информации различного рода сведения о нем, в силу чего становится намного богаче и сложнее [14, С. 337].

Данная точка зрения, полагаем, является следствием того, что процесс расследования заключает в себе методы научного исследования объективной реальности, такие как индукция и дедукция, анализ собранных данных и их сравнение с аналогичными преступлениями и другие. Целью же является одно

– воссоздание общей картины преступления и привлечение виновного к уголовной ответственности.

Содержание криминалистической характеристики может быть различным ввиду особой специфики, свойственной только определенной категории уголовных правонарушений.

Общие элементы криминалистической характеристики преступления будут рассмотрены в содержании.

Белкин Р.С., раскрывая содержание криминалистической характеристики, включает в нее следующие элементы:

- предметы преступного посягательства;
- типичные следственные ситуации, под которыми понимается характер исходных данных;
- способ совершения преступления;
- способ сокрытия преступления, маскировка;
- типичные материальные следы преступления и вероятные места их нахождения;
- характеристика личности преступника;
- характеристика личности потерпевшего;
- обстановка преступления (место, время и другие обстоятельства) [15, С. 312].

В совокупности, все вышеперечисленные сведения формируют информационную картину уголовного правонарушения, присущую определенным преступным деяниям.

Их сопоставление и анализ помогут реализовать весь потенциал следственных органов и обеспечат выбор наиболее верного, на наш взгляд, направления расследования.

Наибольшую практическую ценность данные сведения будут иметь при расследовании однотипных или серийных преступлений, имеющих сходную криминалистическую характеристику и только присущую им специфику.

Так, по мнению Давыдова Е.В., основными элементами, образующими криминалистическую характеристику актов терроризма, являются: приготовление к совершению преступления; способ сообщения о готовящемся или совершенном акте терроризма; способ совершения преступления; орудия и средства, применяемые при совершении преступления; характеристика личности террориста и террористического формирования; характеристика объектов преступного посягательства; материальные следы преступления и особенности механизма следообразования; типичные элементы обстановки (время, место и т. д.). К основным элементам криминалистической характеристики могут быть добавлены дополнительные - факультативные, характеризующие конкретное событие преступления [16].

В содержание криминалистической характеристики уголовных правонарушений, совершенных в сети Интернет, будут входить такие криминалистически важные элементы как способ, место, орудие преступления, обстановка и место его совершения, личность потерпевшего и совершившего уголовное правонарушение, способ сокрытия следов преступления.

При этом, несмотря на ряд определений, приведенных выше, понятие криминалистической характеристики носит обобщенный характер, так как в ее содержании в зависимости от вида и категории уголовного правонарушения может быть масса различных элементов, имеющих важное значение для раскрытия и расследования преступлений.

К основным элементам, составляющим содержание криминалистической характеристики, данного вида уголовных правонарушений, по нашему мнению, следует отнести: обстановку преступления, способ его совершения; типичные следы преступления, личность потерпевшего и преступника.

В зависимости от вида и характера уголовного правонарушения указанный перечень может быть расширен либо наоборот усечен путем исключения определенных элементов (например, при формировании криминалистической характеристики незаконного сбыта наркотических средств с использованием интернет-технологий должен быть исключен такой элемент, как личность потерпевшего).

Таким образом, содержание криминалистической характеристики для каждого вида преступлений будет сугубо индивидуальным.

Все обстоятельства произошедшего преступного деяния должны быть полностью исследованы.

Данное утверждение фактически носит нормативный характер и закреплено в ст.24 действующего УПК.

В частности, в ней указывается, что суд, прокурор, следователь, дознаватель обязаны принять все предусмотренные законом меры для всестороннего, полного и объективного исследования обстоятельств, необходимых и достаточных для правильного разрешения дела.

На практике, при начале расследования, в распоряжение следователя попадают данные, полученные в ходе первоначальных следственных действий, когда следователь еще не владеет достоверными данными о произошедших событиях, но уже получил определенное представление о них, опираясь на информацию, полученную из различных источников (свидетели, оперативная группа, сообщение дежурного сотрудника и т.д.).

Первое, что видит следователь, выезжая на место преступления - окружающая место преступления обстановка.

В теории уголовного права время, место, обстановка совершения уголовного правонарушения относятся к признакам объективной стороны преступления.

Совокупность условий, в которых протекало преступление, в криминалистике получило наименование обстановки совершения преступления или обстановки преступления.

Обстановка совершения преступления имеет важное криминалистическое значение, так как она самым тесным образом связана с вопросом оптимизации как практической, так и исследовательской деятельности криминалистической направленности.

В частности, структурирование данного понятия позволяет определить круг его составных элементов, а значит, и обстоятельств, подлежащих

выяснению по делу (время суток, день недели, месяц, место преступления, погодные условия, прилегающие к указанному месту коммуникации, наличие поблизости жилых, производственных объектов и т. д.).

Обстановка совершения преступления - это совокупность окружающих виновное лицо внешних обстоятельств, при которых совершается преступление. Это среда, ситуация, в которой совершается преступное деяние [17, С. 87].

Криминалистическое исследование обстановки совершения уголовного правонарушения, особенно в начале расследования, позволяет следственным работникам собрать большое количество информации и материалов.

Данные существенные сведения о возникшей до и в момент происшествия криминальной ситуации, выявление и анализ элементов обстановки дают весьма ценную криминалистическую информацию для выбора наиболее правильных путей и методов расследования, способствуют выдвижению конкретных следственных версий, которые бы скорректировали дальнейшее направление расследования.

В первую очередь, это касается сохранения и закрепления цифровых данных, которые в отличие от материальных следов могут самоуничтожиться или видоизмениться в течение определенного времени или вследствие команды данной злоумышленником, неосторожности самого потерпевшего, а также ввиду работы различных программ по безопасности, установленных на устройстве.

Анализ различных мнений по исследованию понятия и содержания обстановки совершения преступления, позволяет сделать вывод о том, что данное понятие многогранно.

Обстановка совершения уголовного правонарушения представляет собой систему различного рода взаимосвязанных между собой объектов, явлений и процессов, характеризующих условия места и времени совершения преступного деяния, различных обстоятельств, сложившихся как по воле виновного, так и без нее, влияющих на способ совершения и его механизм.

Например, в круг сведений, характерных для обстановки совершения преступлений террористического характера с применением взрывных устройств, входит широкий спектр данных, к которым можно отнести:

- сведения о взаимодействующих непосредственно до и в момент взрыва явлениях, процессах;

- данные об объектах и иных внешних и внутренних условиях, влияющих на возникновение и проявление разрушительных сил взрыва;

- примененные орудия преступления;

- негативные последствия преступного деяния и т.д.

Обстановка совершения уголовных правонарушений в сети Интернет, в свою очередь, более специфична, так как преступное действие осуществлено в цифровом пространстве, где имеют место свои законы, отличные от материального, привычного мира.

Особенностью их является то, что в результате использования информационных сетей (проводных и беспроводных технологий) в одном

преступлении одновременно могут быть задействованы множество компьютеров и гаджетов, находящиеся на определенном расстоянии друг от друга, возможно даже в разных государствах и соответственно часовых поясах.

Учитывая вышеуказанное, полагаем, что обстановка совершения преступления, на наш взгляд, является источником криминалистической информации, способным дать широкий спектр сведений для формирования криминалистической характеристики конкретного уголовного правонарушения.

То есть, обстановка совершения преступления представляет собой совокупность явлений, фактов и обстоятельств, материальных данных которые появляются в определенном месте и в определенное время.

Бессонов А.А. справедливо отмечал, что обстановка совершения преступления существует не сама по себе, а лишь во взаимосвязи с преступным деянием. Эта связь детерминирована при совершении умышленных деяний объектом (предметом) преступного посягательства как целью и (либо) личностью преступника, при совершении неосторожных деяний – природой объекта (предмета) посягательства и (или) личностью преступника [18].

Способ совершения преступления также занял одно из ключевых мест в содержании криминалистической характеристики уголовного правонарушения.

В частности, Зуйков Г.Г. рассуждал о способе совершения преступления как о системе действий по подготовке, совершению и сокрытию преступления, детерминированных условиями внешней среды и психофизиологическими свойствами личности, могущих быть связанными с избирательным использованием орудий или средств и условий места и времени.

По мнению Исакова А.В. под способом совершения преступления (в широком смысле, включая приготовление и сокрытие) понимается система объективно и субъективно детерминированных действий (бездействия) субъекта преступления, с помощью которых он достигает своей цели. Способ совершения преступления должен рассматриваться во взаимосвязи с механизмом общественно опасного деяния, включаться в обстановку преступления и увязываться с механизмом следообразования [19].

Изучение способа совершения уголовного правонарушения направлено на установление средств, которые используются злоумышленниками при совершении преступного деяния, причин и условий, определивших выбор конкретного способа совершения преступления.

Способов совершения уголовных правонарушений в сети Интернет множество и каждый день в мире появляются их новые разновидности.

К наиболее распространенным способам, можно отнести: разработку и рассылку различных вирусов (вредоносных программ, которые могут воровать данные, вымогать денежные средства за разблокировку информации); фишинг (получение конфиденциальной информации, например, с целью шантажа); мошенничество с использованием поддельных интернет-сайтов и т.д.

При этом, многие ученые-криминалисты считают, что действия по сокрытию преступления необходимо включать в понятие способа совершения преступления в случае, если подготовка, совершение и сокрытие преступления

осуществлялись по единому замыслу, а субъект преступления имел четкую программу по его сокрытию.

В других случаях способ сокрытия преступного деяния, представляет собой самостоятельную систему действий преступника, направленных на сокрытие следов своей деятельности путем утаивания, уничтожения, фальсификации и т.д.

Следует также отметить, что при описании способов совершения преступления рассматриваются типичные последствия (например, опустошенный банковский счет, пропажа личной информации с устройства), оставшиеся при этом следы (сообщения мошенников, сбои в работе компьютера или гаджета) и типичные места их локализации, которые в совокупности формируют следовую картину преступления.

Конечно, каждый вид уголовных правонарушений имеет присущую ему специфическую следовую картину. Следовая картина уголовных правонарушений, совершенных в сети Интернет, выражается в том, что привычные материальные и идеальные следы, хотя и присутствуют, но чаще всего имеют второстепенное значение.

Наибольшее значение в процессе выявления и расследования рассматриваемой группы преступлений имеют виртуальные следы, под которыми, по мнению Мещерякова В. А., следует понимать «любое изменение состояния автоматизированной информационной системы (образованного ею «кибернетического пространства»), связанное с событием преступления и зафиксированное в виде компьютерной информации (т.е. информации в виде, пригодном для машинной обработки) на материальном носителе, в том числе и на электромагнитном поле» [20, С. 7].

Особенностью таких следов является то, что их невозможно изъять в привычном материальном виде. Однако, в силу их важнейшего значения в процессе доказывания виртуальные следы требуют обязательного осмотра и фиксации. Любая противоправная деятельность является следствием антропогенной деятельности человека и содержит в себе следы личности, ее осуществившей.

В частности, это могут быть сведения о некоторых личных социально-демографических, нравственно-психологических признаках, подлежащих обязательному выяснению в рамках расследования, так как напрямую имеют отношение к установлению признаков состава уголовного правонарушения.

Для содержания криминалистической характеристики обобщение и анализ данных о личности преступника имеют особое практическое значение при расследовании, поскольку способствуют установлению его личности.

Необходимо учитывать, что даже в такой специфической сфере, как уголовные правонарушения, человек действует в качестве общественного субъекта. Поэтому к нему надо подходить как к носителю различных форм общественной психологии, приобретенных правовых, нравственных, этических и иных взглядов и ценностей, индивидуально-психологических особенностей. Все это в целом представляет собой источник преступного поведения, его субъективную причину, предопределяет необходимость изучения всей

совокупности психологических, социологических, правовых, медицинских (в первую очередь психиатрических) и других аспектов личности преступника [21, С. 4].

Лица, совершившие уголовные правонарушения в сфере информатизации и связи, несомненно, владеют навыками работы с компьютером на уровне продвинутого пользователя, соответственно могут являться активными участниками социальных сетей, форумов в сети Интернет по тематике совершенного преступного деяния, имеют в личном пользовании хорошую компьютерную технику, смартфон, подключенные к сети Интернет.

В свою очередь, потерпевшие, в основном, обычные пользователи гаджетов и сетей телекоммуникаций, не владеющие специальными знаниями по безопасной работе в сети, получая сообщения и ссылки из неизвестных источников, переходят по ним и попадают в ловушку злоумышленников.

Наибольшую ценность для формирования следовой картины в таком случае будет представлять информация, содержащаяся на устройстве потерпевшего, а не его показания.

Таким образом, говоря о криминалистической характеристике уголовных правонарушений, совершенных в сети Интернет, следует отметить следующее:

- криминалистическая характеристика должна содержать в себе различные элементы, которые позволили бы выявить взаимосвязь между событиями, субъектами, объектами, предметами, обстановкой до совершения уголовного правонарушения, в процессе него, после его совершения;

- в определениях криминалистической характеристики преступления содержатся уголовно-правовые, криминологические аспекты (субъект, предмет и объект преступления, характеристика личности предполагаемого преступника и другие);

- в содержание криминалистической характеристики будут входить такие криминалистически важные элементы как способ, место, орудие преступления, обстановка и место его совершения, личность потерпевшего и совершившего уголовное правонарушение, способ сокрытия следов преступления;

- особенностью является возможность использования злоумышленником множества устройств, установленных в различных местах и даже государствах;

- следовая картина уголовных правонарушений специфична, ввиду наличия следов уголовного правонарушения, содержащихся в цифровом виде на устройстве и/или в сети.

Проведя соответствующий анализ, пришли к выводу, что криминалистическая характеристика уголовного правонарушения, совершенного в сети Интернет содержит в себе научно-обоснованный инструмент когнитивной деятельности, обусловленный необходимостью обеспечения всестороннего, полного и объективного исследования обстоятельств совершенного противоправного деяния и решения задач по его раскрытию, а также реализации принципа неотвратимости наказания для виновных лиц.

1.2 Виды и способы совершения уголовных правонарушений в сети Интернет

По прогнозам Cybercrime Magazine, в 2022 году бюджеты на защиту данных достигнут 170 миллиардов долларов США. В сфере кибербезопасности будет работать 3,5 миллиона человек, а количество лиц совершающие правонарушения в сети Интернет (хакеров) в 2022 году достигнет 6 миллионов человек. В 2030 году 90% населения мира будут пользоваться интернетом [22].

Развитие всемирной системы объединённых компьютерных сетей выделяет основные три периода:

Первый период - большинство интернет сайтов были информационными, без каких либо интерактивных элементов. Пользователи не могли комментировать, обмен файловыми данными был длительным процессом, передача текстовых сообщений между пользователями равнялась нулю. Основным местом обмена информациями были специальные разделенные по темам форумы и чаты. Скорость работы сети была очень низкой. Интернет-трафик проходил по линиям телефонной связи и невозможно было одновременно находиться в сети и говорить по телефону.

Второй период - эпоха высокоскоростного интернета. Пользователи стали активно делиться фотографиями, мелодиями, видеороликами. Скачивание файлов стало быстрее. Интернет сайты начали наполняться пользовательскими веб-страницами, появились социальные сети и мессенджеры.

Третий период - эпоха, когда смартфоны с высокоскоростным интернетом стали доступными почти каждому пользователю и обеспечили его круглосуточное присутствие в сети интернет. Социальные сети почти полностью поглотили весь основной интернет. Стало возможным не только общаться, но и учиться, работать, смотреть фильмы, слушать музыку, заниматься творчеством и его продвижением [23].

На сегодняшний день информация в сетях Интернета используется не только для оперативного оповещения, средством связи, создания новых знаний, инновационных изобретений, но и в противоправных целях. Такие понятия как «хищение - путем незаконного доступа в информационную систему», «интернет-мошенничество», «интернет-буллинг», «вовлечение в противоправную деятельность» прочно вошли словарь специализированных терминов.

Необходимо отметить, что вышеуказанные правонарушения совершаются с использованием сети Интернет, где, как отметил, профессор Перов В.А. «оставляют специфический «электронный» или как его еще называют в криминалистической литературе «цифровой след» [24, С. 18].

Также Перов В.А. указывает, что такие понятия как: «цифровой след», «киберпреступность» или «электронный след» единообразны. Например, в криминалистической литературе встречаются такие термины как: «электронно-цифровой», «виртуальный» следы, «цифровой отпечаток» [25, С. 21].

Ученые-криминалисты, исследуя данные понятия, отмечают, что термины «электронный след» и «цифровой след» имеют единообразные

определения, под которыми понимают некий набор действий на электронном устройстве в режиме онлайн через сети Интернет, в результате чего остается информация, являющаяся итогом совершения подобных действий.

Вышеуказанные обстоятельства полностью применимы к уголовным правонарушениям в сети Интернет. Отличия только в том, что цифровые следы могут возникнуть не только в результате противоправных действий людей, но и действий компьютерных систем, запрограммированных на автономный режим.

Согласно ст.18 Конституции РК каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и достоинства. Ограничения этого права допускаются только в случаях и в порядке, прямо установленных законом. Данная норма перешла и в цифровой мир.

Каждый гражданин тратит по несколько часов на социальные сети в Интернете, где остаются «цифровые следы» в веб-сайтах, когда смотрит и публикует картинки, фотографии, видео, ставят лайки и оставляет комментарии под ними. Данными «цифровыми следами» могут завладеть лица или группы лиц, находящиеся в Интернете и совершающие преступные действия – кражи личных данных, мошенничества и вымогательства.

В таблице 1 указаны виды, цели и способы совершения уголовных правонарушений в сети Интернет.

Виды	**Цель**	**Способы**
Хищение - путем незаконного доступа в информационную систему	персональный компьютер, смартфон, аккаунты для дальнейшего использования в хищении	отправка вредоносных файлов, ссылок на сайты
Интернет-мошенничество	денежные средства, материальные ценности, аккаунты	рекламные сообщения, предложения товаров и услуг, акции, выгодные предложения
Интернет-буллинг	личность, психика	сообщения, чаты, комментарии в аккаунте жертвы, закрытые сообщества
Вовлечение в противоправную деятельность	личность, психика	сообщения, чаты, закрытые сообщества

Таблица 1. Виды, цели и способы совершения уголовных правонарушений в сети Интернет

Рассмотрим основные виды и способы совершения уголовных правонарушений в сети Интернет и профилактические меры по ним.

Хищение - путем незаконного доступа в информационную систему

Преступник распространяет компьютерные вирусы, для получения личных данных пользователей (файлы персонального компьютера, информации, отправленные в интернете: например, пароли и данные платежной карты), получая доступ

к аккаунтам в социальных сетях и на сайтах, похищает цифровые денежные средства после блокировки компьютера.

Первый и наиболее распространенный тип вредоносного ПО – это вирусы. Для заражения компьютера вирусом, требуются действия пользователя. Вирус скрытно внедряется в программный код ПО или в файловые документы компьютера. При запуске ПО вирус переходит в активный режим и заражает компьютер.

Также для кибератак используется «троянский конь» – это кажущаяся безопасной программа, которая несет в себе вредоносный код. Часто внедряются в бесплатные программы, например, в компьютерные игры.

Типы вредоносного ПО

Программы-вымогатели - шифруют файлы на компьютере с последующим отображением сообщений с требованием выкупа за ключ для расшифровки.

Руткиты - используются для получения права администратора и удаленного управления компьютером.

Шпионские - ПО используется для сбора данных о пользователе и их отправки злоумышленникам без его ведома.

Червь - распространяется без участия пользователя, используя уязвимости легитимного ПО.

Интернет-мошенничество

Интернет-мошенничество – вид мошенничества с использованием Интернета. Оно включает в себя сокрытие информации или предоставление неверной информации с целью вымогательства у жертв денег, имущества и ценностей [26].

Например, интернет - пользователь получил денежный перевод, выиграл в Бинго, близкий родственник оставил завещание, последний день распродажи со скидкой 99%, эти и многие другие похожие сообщения рассылаются ежедневно. Электронная почта, социальные сети, интернет сайты, SMS – интернет - мошенники могут использовать любые доступные им социальные каналы коммуникаций, чтобы заманить в свои сети наивных пользователей.

Вариантов заманить беспечного пользователя социальных сетей очень много. Результат один - обманом получать от жертвы деньги или информацию. Интернет-пользователь и не заметит, как передает интернет-мошеннику номер банковской карты или перейдет по ссылке, через которую в компьютер проникнет вирус.

Криминалистическая характеристика интернет-мошенничества

- обещание быстрой и легкой выгоды (получения товара, денег, услуги);

- ограничение во времени (чтобы у потенциальной жертвы не было возможности обдумать все «за» и «против»);

- ограничение предложения («остался последний товар, последний день»).

В Казахстане к такой тактике во время объявленного карантина пандемии COVID-19 периодически прибегали интернет-мошенники, пытаясь продать гражданам сомнительные лекарственные препараты. На сайтах после долгого описания чудесного средства интернет-пользователям предлагали ввести

личные данные для бесплатного получения препарата. Впоследствии же оказывалось, что акция по безвозмездной раздаче закончилась, и гражданину все же придется заплатить [27].

Так, в Жамбылской области преступник позвонил по телефону жертве и сообщил о своем желании купить квартиру, объявление о продаже которой было размещено в интернете самим потерпевшим. В ходе переговоров мошенник обманом заполучил фото платежной карты и удостоверения личности жертвы. Затем, злоумышленник через личный кабинет в онлайн системе банка, получил доступ на депозитный счет потерпевшего, с которого похитил более 20.000.000 тенге путем их перевода на платежные карты подставных лиц. Такого рода преступления сложно раскрыть из-за законодательных ограничений в области банковской тайны в соответствии ч.1 ст.50 Закона «О банках и банковской деятельности» от 31.08.1995г. [28].

Ученый-юрист Шульгина И.В. в своих трудах отмечает, что: «… Типовые особенности личности интернет-мошенника по исследуемой категории дел позволяют правоохранительным органам в процессе проведения расследования определить круг подозреваемых в совершении преступления, разработать потенциальные модели их поведения, предугадать дальнейшие действия и сформировать алгоритм действий следствия в процессе раскрытия правонарушения и сбора доказательств, для их предъявления в суде» [29].

Отдельно стоит выделить интернет - мошенников, отправляющих ложные письма от различных сервисов или банков (фишинг). Эти письма вызывают доверие: в них есть логотип компании, фирменные цвета, обращение к жертве по имени. Поверив содержанию письма, жертва вводит на открывшемся сайте логин и пароль, навсегда потеряв доступ к аккаунту [30].

Интернет-буллинг

Буллинг (от английского bullying – «запугивание», «издевательство», «травля») – агрессивное преследование одного из членов коллектива (школьников или студентов) со стороны другого члена коллектива. Буллинг не всегда выражается в физической агрессии. Чаще всего речь идет о психологическом насилии в форме словесной травли (оскорбления, злые и непристойные шутки, насмешки), распространения слухов и сплетен, бойкота [31].

Травля во многих странах считается правонарушением и жертва буллинга может рассчитывать на помощь от родителей, учителей, правоохранительных органов. Главное – не молчать о проблеме.

Процесс интернет-буллинга начинается обычно с публикации поста, получения лайков и комментариев от друзей, где, в последующем, появляется незнакомый человек (точнее, аккаунт), который начинает оставлять издевательские сообщения, высмеивать, комментировать каждое действие, переходя на личности (пишет об особенностях, фигуре, имени, увлечениях), язвит в ответ на любое сообщение.

Данный процесс может продолжаться довольно долго – и не только в комментариях к посту или фотографии, но и в личных сообщениях. На языке интернета это называется «троллить», но в жесткой форме, когда шутки

переходят в травлю и преследование (буллинг), что может перейти уже к доведению человека до суицида.

В некоторых случаях в буллинге могут участвовать группа лиц. В этом случае жертве сложнее «спрятаться», находясь постоянно под ударом. В данном случае, приходится удалять аккаунт или менять имя в социальной сети.

Судебный практик Авганов С. отмечает, что «…блогеры, которые имеют число подписчиков свыше 3 000 подписчиков, должны быть приравнены к СМИ. В этом случае, к блогеру будут предъявлены требования такие, как запрет употребления нецензурной лексики, а также иные, которые предъявляются сейчас к СМИ. Поскольку неверно истолкованная свобода слова пользователями социальных сетей нарушает права других людей, которые подвергаются травле [32].

Вовлечение в противоправную деятельность

Не всех злоумышленников интересуют деньги и материальные ценности. Некоторые нацелены на личность потерпевшего, желание управлять ими.

Клубы общих интересов в социальных сетях, чатах и мессенджерах также могут представлять опасность. Современный интернет дает возможность находить единомышленников. Чем бы не интересовался интернет-пользователь, всегда найдутся в сети те, кто поддержит интерес в обсуждении самых разных тем. В этом случае, от общения в Интернете пользователь получает пользу и удовольствие. Однако, следует проявлять особую бдительность, если разговор в сообществе или в чате вдруг начнет уходить в сторону от главной темы.

Злоумышленники иногда маскируются под обычных интернет-пользователей, приходят в клуб общих интересов, участвуют в обсуждениях, знакомятся с участниками, а потом заводят разговоры на отвлеченные темы.

Незнание закона не освобождает от ответственности.

Так, распространители заведомо ложной информации привлекаются к ответственности по ст. 274 УК РК.

Например, 1 апреля 2017 года сайт azh.kz распространил информацию о том, что 20-летний житель г.Атырау Акылбек Копжасаров решил математическую задачу, которую ученые всего мира не могли решить много лет. Информационные порталы мгновенно переопубликовали сенсационную «новость». И несмотря на то, что сайт-первоисточник сразу же указал, что это первоапрельская шутка, сообщения о гениальном соотечественнике до сих пор размещены на некоторых казахстанских интернет-ресурсах. Чтобы убедиться в этом, достаточно вбить в поиск «Акылбек Копжасаров» [33].

Требуется критическое осмысление, основанное на понимании того, как работают современные цифровые технологии. Это позволит избежать манипуляций и сохранить независимость суждений и действий от указанных видов и способов совершения уголовных правонарушений в сети Интернет. В мире цифровых технологий такое мышление называют медиа-грамотностью или информационной гигиеной.

1.3. Анализ отечественного и международного законодательства в области защиты прав граждан от преступных посягательств в Интернете

С развитием информационных технологий защита личных, персональных данных стала еще более актуальной. Для решения проблем требуется правовое государственное регулирование (принятие соответствующих законов или корректировка имеющихся), а также межгосударственное сотрудничество в борьбе с преступностью в сети Интернет.

Накапливается международный опыт в сфере обеспечения информационной безопасности, особенно в рамках деятельности таких международных организаций, как ООН, СЕ, ЕС, БРИКС, ШОС, ЕврАзЭС, СНГ.

Резолюция Европейского парламента 1979 года «О защите прав личности в связи с прогрессом информатизации» определила основные идеологические направления регулирования этой сферы применительно к странам – членам Евросоюза, на основе которого приняты несколько важных постановлений и директив, защищающих данные о личности, подвергающиеся опасности в связи с развитием технического прогресса. К ним относятся рекомендации «О руководящих направлениях по защите частной жизни при межгосударственном обмене данными персонального характера», а также принципы «Регулирования сферы обеспечения конфиденциальности сведений» и другие.

В Конвенции СЕ «О защите физических лиц при автоматизированной обработке персональных данных» 1981 года дано определение персональных данных и заложены международные основы законной обработки персональных данных актуальных и по сей день (использование персональных данных только для определенных целей и в пределах определенных сроков, неизбыточность и актуальность обрабатываемых персональных данных и особенности их трансграничной передачи, защита данных, гарантированные права гражданина - обладателя личных данных).

В июне 1994 года СЕ принят план действий «Путь Европы в информационное общество», который предусматривал механизмы, направленные на создание условий по свободному доступу к информации, и одновременно, оберегающие личность и общество.

Положения Йоханнесбургских принципов 1995 года «Национальная безопасность, свобода выражения мнения и доступ к информации» также являются одним из основных актов регламентирующих вопрос свободы слова.

Множество проблем охвачены в директивах Европейского парламента и ЕС «О процедуре предоставления информации в области технических стандартов и регламентов, а также правил оказания услуг в информационном обществе», «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», «Об использовании персональных данных и защите неприкосновенности частной жизни в сфере телекоммуникаций», «О правовых основах регулирования электронных подписей в Сообществе», «О защите потребителей по договорам, заключаемым дистанционным способом».

С 2000 года приняты «Окинавская хартия» и итоговые документы Всемирной встречи на высшем уровне по вопросам информационного общества (2000г).

В декабре 2000 года принята Конвенция ООН против транснациональной организованной преступности, акцентирующая внимание на вопросах автоматизированного сбора и обработки данных о личности и ее жизни, норм их хранения, правил предоставления доступа к ним, прав и обязанностей собственников и операторов, требований к трансграничной передаче данных, и др.

Одним из важных международных документов также является Будапештская Конвенция Совета Европы о киберпреступности 2001 года. Она направлена на расширение международного сотрудничества и совершенствование методов расследования киберпреступлений. В ней имеются рекомендации для принятия на национальном уровне норм материального и уголовно-процессуального права по оказанию взаимной правовой помощи для стран, не имеющих договоров со странами, запрашивающими помощь.

Конвенция разделила киберпреступность на четыре группы: преступления против конфиденциальности, целостности и доступности компьютерных данных; преступления, связанные с использованием компьютерных средств; преступления, связанные с контентом (содержанием информации в сети); преступления, связанные с авторским правом и смежными правами.

Вместе с тем, дополнительным протоколом к Конвенции, касающимся криминализации актов расистского и ксенофобского характера, совершенных через компьютерные системы (Страсбург, 28.01.2003г.) утверждены преступления, посягающие на общественную безопасность, образовавшие пятую группу.

Учитывая сохраняющиеся политические, экономические, социальные связи, особое значение имеют соглашения, заключенные в этой сфере в рамках СНГ, в частности «Соглашения о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств-участников СНГ в сфере информатизации» (24.12.1999г.); «О принципах и формах взаимодействия государств-участников Содружества Независимых Государств в области использования архивной информации» (4.06.1999г.); «О сотрудничестве в области обеспечения международной информационной безопасности между правительствами государств-членов ШОС» (16.06.2009г.) и др.

Модельный закон «О персональных данных» принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств - участников СНГ в 1999 году Ассамблеей СНГ. Настоящий Закон определяет операции с персональными данными и их правовой режим с учетом общепризнанных норм международного права и обязательств по международным договорам. Он вводит термин «персональные данные» и закрепляет что к ним может относиться: вся информация о семье, карьере, бизнесе, счетах и вкладах, здоровье. Документ освещает стандарты регулирования обработки персональных данных, поясняет определение прав и обязанностей операторов.

Генеральной Ассамблеей ООН был принят ряд Резолюций, направленных, в том числе и на регулирование информационной сферы:

- Борьба с преступным использованием информационных технологий 2001 года;
- Стратегия в области информационно-коммуникационных технологий 2003 года;
- Расширение доступа к Интернету благодаря трансевразийской высокоскоростной информационной магистрали 2009 года.
- «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур» 2009 года;
- Довильская декларация 2011г. содержащая раздел об Интернете, в котором закреплены такие принципы как свобода, уважение частной жизни и интеллектуальной собственности, участие в процессе управления широкого круга заинтересованных сторон, кибербезопасность и защита от преступности.

В рамках инициативы «Европа - 2020» ЕС определил собственную Цифровую повестку дня (Digital Agenda) с обязательством выполнения широкого круга задач, как ориентирование на дальнейшую популяризацию Интернета и обеспечение кибербезопасности своих граждан.

На базе ЕС было создано Агентство по сетям и информационной безопасности (ENISA), которое проводит мониторинг мнений пользователей сети, в соответствии с этим вносит поправки в уже принятые проекты, которые в последующем становятся законами и соблюдаются странами ЕС.

В июне 2016 года Совет ООН по правам человека принял Резолюцию о «Продвижении, защите и осуществлении прав человека в Интернете».

Основным документом, регламентирующим вопросы защиты личных, персональных данных признается (Общий) Генеральный регламент о защите персональных данных (англ. General Data Protection Regulation, GDPR) - с помощью которого ЕП, Совет ЕС и ЕК усиливают и унифицируют защиту персональных данных всех лиц в ЕС.

Казахстан последовательно ведет работу по усилению защиты личных, персональных данных и информации с сети Интернет.

В мае 2013 года в РК принят Закон «О персональных данных и их защите» (далее - Закон о персональных данных), который регулирует общественные отношения в сфере персональных данных, устанавливает порядок сбора, обработки и защиты персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных. Особенности защиты персональных данных в электронной форме для государственных систем определены в Законе РК от 24.11.2015 года «Об информатизации», который закрепляет, что «информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, полученные или созданные обладателем информации, зафиксированные на любом носителе и имеющие реквизиты, позволяющие ее идентифицировать».

Принятие Закона «О персональных данных» было предусмотрено Планом нации - 100 конкретных шагов по реализации пяти институциональных реформ,

где любая информация, находящаяся в распоряжении государственных органов, будет охраняемой законодательством.

Кроме того, в мае 2013 года утверждены Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных и Правила определения собственником и (или) оператором перечня персональных данных.

В Казахстане постепенно внедряются нормы GDPR. В июле 2020 года вступили в силу изменения и дополнения, которыми определен уполномоченный орган, осуществляющий руководство в сфере защиты персональных данных МЦРИАП. Если собственник и/или оператор являются юридическими лицами, компаниям необходимо назначать лицо, ответственное за организацию работы с персональными данными, внесено новое понятие «сервис обеспечения безопасности персональных данных», обеспечено информационное взаимодействие собственников и/или операторов с субъектом персональных данных.

В 2021 году внесены изменения в Правила работы с персональными данными, в частности необходимо оповещение МЦРиАП об инцидентах в информационной безопасности, связанных с незаконным доступом к персональным данным.

Вместе с тем, в соответствии с нормами GDPR персональные данные должны быть интерпретированы настолько широко, насколько это возможно. Любая информация, позволяющая идентифицировать человека, вплоть до IP-адреса, цвета волос, вероисповедания, национальности.

В основе любых персональных данных лежит информация.

В РК термин «информация» и его модификации применяются в таких законах как: «О доступе к информации», «О техническом регулировании», «О государственных секретах», «О национальной безопасности», «О средствах массовой информации», «О связи». Используемая в отечественном законодательстве терминология информации соответствует международным стандартам, и не нуждается в какой-либо унификации [34, С. 32-33].

Вместе с тем, требуется кодификация норм права, регулирующих важнейшие общественные отношения в сфере информационно-коммуникационных технологий, предусматривающих фильтрацию контента, контроль используемых приложений и предупреждение о потенциальных угрозах.

Путем повышения осведомленности о рисках и стимулирования достаточного контроля со стороны родителей, не нарушающего при этом свободы выражения мнений, необходимо вести борьбу с торговлей детьми и их сексуальной эксплуатацией, работать над созданием для детей безопасной среды от киберпосягательств.

В этих целях, 2июля 2018 года в Казахстане принят Закон «О защите детей от информации, причиняющей вред их здоровью и развитию».

Основным политико-правовым актом, определяющим принципы и основные направления развития информационной безопасности, является Концепция кибербезопасности («Киберщит Казахстана» от 30.06.2017г.).

В 2019 году начался второй этап ее реализации. В нем определен ряд задач для обеспечения максимальной кибербезопасности, повышения осведомленности населения об имеющихся угрозах, увеличения количества специалистов в данной сфере, обновления образовательных программ, гармонизации международных стандартов, разработки национальных стандартов, создания оперативных центров информационной и кибербезопасности. Выполнение поставленных задач должно послужить модернизации казахстанского общества и внести вклад в реализацию Глобальной программы кибербезопасности ООН.

Несомненно, ратификация международных актов послужило поводом для включения ответственности за них в отечественное законодательство.

Следует отметить, что европейские законодатели по-разному именуют рассматриваемые преступления (к примеру, неправомерный доступ к информации, несанкционированный доступ, противозаконный доступ, самовольный доступ) что, впрочем, не меняет их сути.

Таким образом, в целях устранения пробелов и единообразного толкования понятийного аппарата, расширения определения персональных данных, создания безопасной среды для детей от киберпосягательств заинтересованным государственным органам предлагается рассмотреть вопрос о кодификации норм права в единый кодекс.

Указанные меры позволят систематизировать разрозненные и фрагментированные нормы закона, регулирующие общественные отношения в сфере информационно-коммуникационных технологии, безопасность и защиту информации, связи, обработки данных, цифровых активов, искусственного интеллекта, защиты прав субъектов персональных данных в единый нормативный документ.

Вместе с тем, к поставщикам информации, на примере GDPR, наряду с основными видами следует использовать и другие инструменты воздействия, как временное ограничение или полный запрет на обработку персональных данных.

1.4. Криминальная ситуация в сфере уголовных правонарушений, совершаемых в сети Интернет

В современном мире достижения научного и технического прогресса оказывают воздействие на все явления общественной жизни. Одним из негативных последствий является проникновение криминальных угроз в информационно-телекоммуникационную среду, в том числе в сеть Интернет.

В результате появляются новые виды общественно опасных деяний, связанных с информационными технологиями. Также они используются для совершения деяний, предусмотренных уголовным законодательством.

К данным деяниям можно отнести незаконное завладение персональными данными, банковскими реквизитами, например, данными платежных карточек (фишинг) физического лица для хищения чужого имущества, взлом паролей, распространение вредоносных вирусов, а также разного рода информации (сведения, затрагивающие честь и достоинство личности, тайну частной жизни, материалы экстремистско-террористической направленности, возбуждающие межнациональную и межрелигиозную вражду, порнографического характера и т.п.).

Число преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей и по оценкам Интерпола темпы роста преступности в сети Интернет являются самыми стремительными на планете [35, С.367].

Такие виды уголовных правонарушений отмечаются транснациональностью, неперсонофицированностью и экспоненциальным ростом, хотя сам механизм совершения преступления не требует больших усилий, затрат и глубоких технических познаний. Достаточно иметь компьютер, программное обеспечение и подключение к информационной сети.

В настоящее время существуют специальные площадки, где можно приобрести программное обеспечение, номера похищенных кредитных карт, идентификационные данные пользователей, услуги по электронному хищению и совершению атак на компьютерные системы.

Поэтому преступные деяния, совершаемые при помощи информационно-телекоммуникационных технологий, условно можно разделить на деяния, обусловленные взаимодействием человека и техники, либо взаимодействием человека с человеком с помощью технических средств.

Вторая модель взаимодействия представляет наибольшую угрозу для безопасности личности, общества и государства, поскольку представляет организованную преступность в сетях Интернет. Ее жертвами могут быть как отдельные граждане, так и целые государства. Одним словом безопасность пользователей одновременно может оказаться в зависимости от небольшой группы преступников.

Как ранее отмечалось, свыше 80% преступлений в сети Интернет совершаются в организованной форме, со сложившимися черными рынками киберпреступности в области создания вредоносных программ, компьютерных вирусов, управления бот-сетями, сбора персональных и финансовых данных, продажи данных и получения денег за финансовую информацию.

Во многих странах резкий всплеск количества подсоединений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах граждан, сокращением расходов в частном секторе и снижением финансовой ликвидности.

По данным Рейтинга хостинга веб-сайтов:

1. Ежедневная цена глобальной киберпреступности к 2025 году достигнет $10.5 трлн.;

2. Доходы от киберпреступности превысят в 5 раз доходы от глобальных транснациональных преступлений вместе взятых;

3. Рынок кибербезопасности будет стоить до 2024 года $ 300 млрд. [36].

Характерной особенностью киберпреступности является ее высокая латентность, в том числе из-за отсутствия должной реакции со стороны жертв преступлений, а также возможности совершения данных деяний незаметно для потерпевшего с использованием компьютерных технологий.

Низкий уровень выявляемости данных правонарушений связан с их трансграничным характером, и с тем, что правоохранительные органы РК работают преимущественно с отечественными Интернет ресурсами. В то же время, зарубежные интернет-ресурсы продолжают совершать незаконные действия, входящие в объективную сторону уголовных правонарушений на территории Казахстана.

В качестве примера указанных незаконных действий можно привести мошеннические операции, совершаемые путём выставления счетов за неоказанные услуги (кремминг) либо финансовые пирамиды.

Поэтому, для обладания полной и достоверной информацией о преступности в целом, и киберпреступности в частности, в первую очередь необходим организованный сбор данных обо всех преступлениях, совершаемых с использованием информационных технологий, что позволит эффективно и упорядоченно структурировать данные по всем видам преступлений.

Действующий УК РК содержит Главу 7, предусматривающую ответственность за уголовные правонарушения в сфере информатизации и связи.

Согласно статистическим данным в период с 2015 по 2020 годы зарегистрировано 694 уголовных правонарушения в сфере информатизации и связи (2015 г. – 176, 2016 г. – 132, 2017 г. – 107, 2018 г. – 72, 2019 г. – 108, 2020 г. – 62) с устойчивой тенденцией их ежегодного снижения на - 64% (с 176 – 2015 г. до 62 – 2020 г.) (таблица 2).

№	Статья УК РК	2015	2016	2017	2018	2019	2020	2021
1.	Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть (ст.205)	50	44	53	28	59	37	46
2.	Неправомерные уничтожение	14	9	22	13	6	9	9

	или модификация информации (ст.206)							
3.	Нарушение работы информационной системы или информационно-коммуникационной сети (ст.207)	9	11	7	5	6	4	
4.	Неправомерное завладение информацией (ст.208)	14	20	4	11	16	4	9
5.	Принуждение к передаче информации (ст.209)	1	0		1			
6.	Создание, использование или распространение вредоносных компьютерных программ и программных продуктов (ст.210)	61	24	11	4	4	4	4
7.	Неправомерное распространение электронных информационных ресурсов ограниченного доступа (ст.211)	19	17	7	7	8	4	5
8.	Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (ст.212)	4	2	1	1	2		
9.	Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (ст.213)	4	5	2	2	7		1

Таблица 2. Уголовные правонарушения в сфере информатизации и связи

При этом, приведенные статистические показатели не отражают все многообразие уголовных правонарушений, совершенных посредством сети Интернет, так как значительное число уголовных правонарушений находится в различных главах Особенной части УК.

Так, в ежеквартальный отчет, охватывающий 9 составов преступлений (ст.205, 206, 207, 208, 209, 210, 211, 212, 213 УК РК), не вошли такие преступления как: понуждение к половому сношению, мужеложству, лесбиянству или иным действиям сексуального характера - (ст.123 УК РК), развращение малолетних - (ст.124 УК РК), оскорбление - (ст.131 УК РК), вовлечение несовершеннолетнего в совершение уголовных правонарушений - (ст.132 УК РК), нарушение частной

жизни и законодательства РК о персональных данных и их защите - (ст.147 УК РК), незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений - (ст.148 УК РК), пропаганда или публичные призывы к развязыванию агрессивной войны - (ст.161 УК РК), разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни - (ст.174 УК РК), пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя РК - (ст.179 УК РК), сепаратистская деятельность - (ст.180 УК РК), кража - (ст.188 УК РК), мошенничество - (ст.190 УК РК), причинение имущественного ущерба путем обмана или злоупотребления доверием - (ст.195 УК РК), незаконные получение, разглашение или использование сведений, составляющих коммерческую либо банковскую тайну, налоговую тайну, полученную в ходе горизонтального мониторинга, тайну предоставления микрокредита, тайну коллекторской деятельности, а также информации, связанной с легализацией имущества - (ст.223 УК РК), пропаганда терроризма или публичные призывы к совершению акта терроризма (ст.256 УК РК), распространение заведомо ложной информации - (ст.274 УК РК), незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка либо сбыт наркотических средств, психотропных веществ, их аналогов - (ст.297 УК РК), склонение к потреблению наркотических средств, психотропных веществ, их аналогов - (ст.299 УК РК), пропаганда или незаконная реклама наркотических средств, психотропных веществ, их аналогов, прекурсоров - (ст.299-1 УК РК), незаконный оборот ядовитых веществ, а также веществ, инструментов или оборудования, используемых для изготовления или переработки наркотических средств, психотропных веществ, их аналогов или ядовитых веществ - (ст.301 УК РК), за исключением доведения до самоубийства - (ст.105 УК РК) и вовлечение несовершеннолетнего в занятие проституцией (ст.134 УК РК).

Таким образом, с целью совершенствования информационно-аналитического обеспечения деятельности по противодействию уголовным преступлениям, совершаемым в сети Интернет, сбора и систематизации криминологически значимой информации, анализа, классификации, определения реальной картины состояния дел и перспективного прогнозирования развития ситуации КПСиСУ предлагается внести соответствующие изменения в Правила приема и регистрации заявлений, сообщений и рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований, утвержденные приказом ГП РК от 19 сентября 2014 года №89 (далее - Правила).

В частности, предлагается внести в форму отчета №1-М «О зарегистрированных уголовных правонарушениях» (далее – Отчет №1-М) в раздел «Всего правонарушений» строку «совершено посредством сети Интернет», что позволит определить общее число правонарушений, совершенных в сети Интернет.

Кроме этого, имеются существенные несоответствия в определении понятийного аппарата, а именно в несовершенстве действующего уголовного

законодательства, в котором отсутствует регламентация ответственности за совершение преступлений с использованием сети Интернет, а официальное закрепление получила только ограниченная группа деяний, для которой используется термин «в сфере информатизации и связи».

Разнородность правового закрепления составов преступлений посредством сети Интернет в уголовном законодательстве Казахстана поднимает проблему унификации правового поля.

Отсутствие нормативной правовой базы и единого подхода к определению понятийного аппарата рассматриваемой совокупности общественно опасных деяний существенно осложняют эффективное противодействие преступлениям, совершаемым посредством сети Интернет.

Так, анализ отчета 1-М «О зарегистрированных уголовных правонарушениях» за период 2015-2020 г.г. случаев регистрации уголовных правонарушений, совершенных посредством использования сетей телекоммуникации, в том числе сети Интернет показал, что за шесть лет их регистрация в Казахстане увеличилась в 1,7 раза (с 16 576 в 2015 году до 29 161 в 2020 году).

В разрезе уголовных правонарушений увеличение отмечается по таким составам как:

- незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сетям телекоммуникаций (ст.148 ч.2 УК РК);
- кража путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций (ст.188 УК РК);
- мошенничество путем обмана или злоупотребления доверием пользователя информационной системы (ст.190 ч. 2 п.4 УК РК);
- причинение имущественного ущерба путем обмана или злоупотребления доверием путем незаконного доступа в информационную систему либо изменения информации, передаваемой по сетям телекоммуникаций (ст.195 ч.3 п.3 УК РК);
- пропаганда терроризма или публичных призывов к совершению акта терроризма с использованием сетей телекоммуникации (ст.256 ч.2 УК РК);
- распространение заведомо ложной информации с использованием сетей телекоммуникаций (ст.274 УК РК);
- незаконное распространение порнографических материалов или предметов (ст.311 УК РК);
- изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних либо их привлечения для участия в зрелищных мероприятиях порнографического характера (ст.312 УК РК);

Данное указывает на значительный рост правонарушений с использованием сети Интернет, в связи с чем, необходимо проведение качественных исследований, направленных на выявление драйверов

преступности, то есть изучение причин и условий их совершения.

Рассмотрим наиболее распространенные уголовные правонарушения, совершаемые посредством сети Интернет.

Одним из таких является мошенничество. В ст.190 УК РК законодатель предусмотрел квалифицированный состав – мошенничество, совершенное путем обмана или злоупотребления доверием пользователя информационной системы (п.4 ч. 2 ст.190 УК), которого не было в УК РК 1997 года.

В 2018 году в приказ Генерального Прокурора РК от 29.08.2016 года №14 отчета формы 1-М были внесены изменения, связанные с разграничением мошенничеств в зависимости от способа их совершения. Это позволило выявить реальную криминогенную ситуацию с регистрацией мошенничеств.

Так, по статистическим данным в 2018 году было зарегистрировано 517 фактов интернет-мошенничества.

В разрезе регионов наибольшее количество регистрации за 2018 год отмечено в городе Нур-Султан – 238 фактов, в Костанайской – 83 и Восточно-Казахстанской областях – 74.

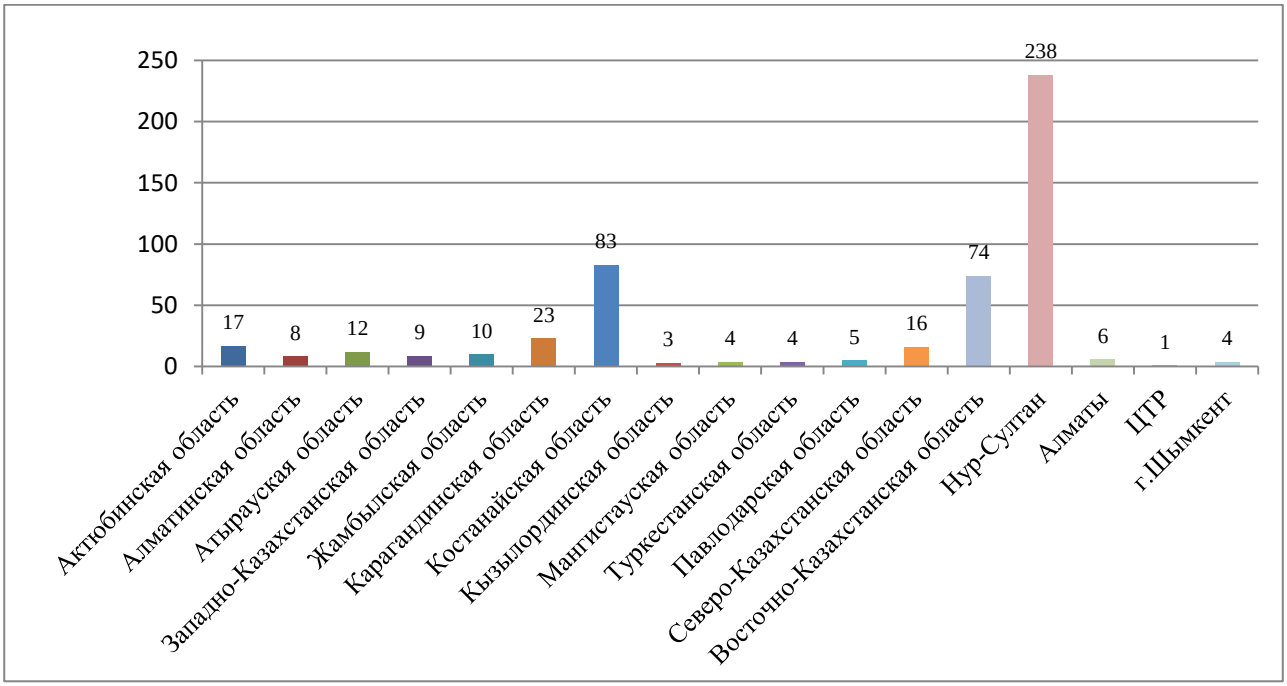

Рисунок 1. Регистрация интернет-мошенничеств в разрезе регионов (2018г.)

По итогам 2019 года зарегистрировано 7 769 фактов интернет-мошенничества.

По сравнению с 2018 годом отмечен рост интернет - мошенничества с 517 до 7 769 (1 402%).

Наибольший рост количества регистрации по интернет-мошенничествам за 2019 год произошел в городе Нур-Султан – 1 711, в Восточно-Казахстанской – 834 и Карагандинской областях – 785 .

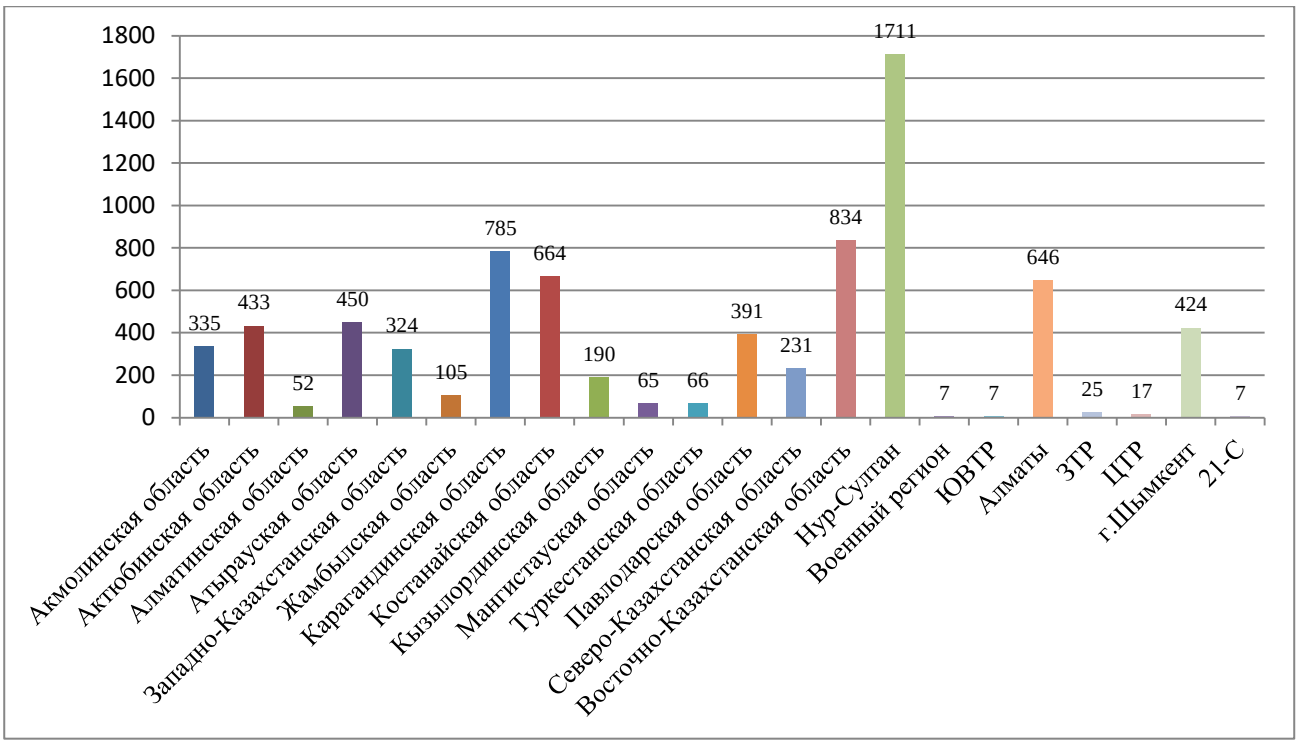

Рисунок 2. Регистрация интернет-мошенничеств в разрезе регионов (2019г.)

Пик регистрации по данной категории преступлений пришелся на 2020 год.

Так, по итогам 2020 года было зарегистрировано 14 220 случаев интернет-мошенничеств.

По сравнению с 2019 годом рост составил с 7 769 до 14 220 (83%).

Наибольший рост наблюдался в г.Нур-Султан – 2 773 , г.Алматы – 1 658 и в Карагандинской области 1 591.

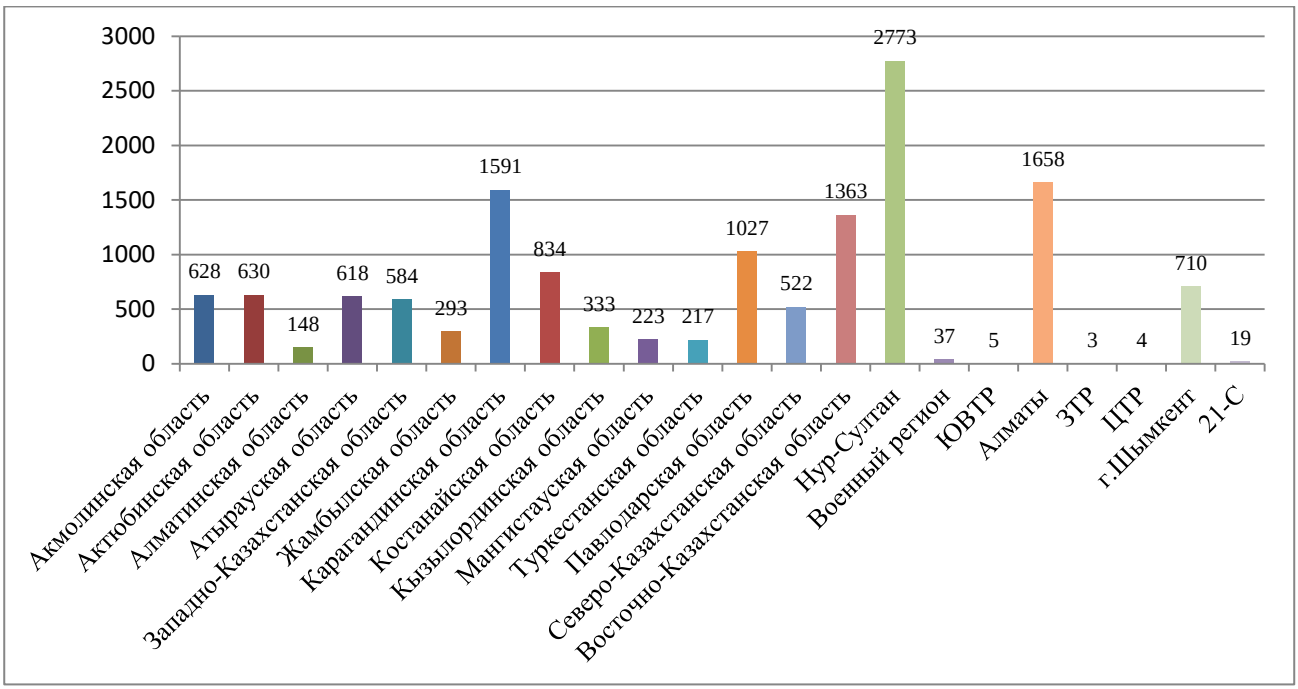

Рисунок 3. Регистрация интернет-мошенничеств в разрезе регионов за 2020 год.

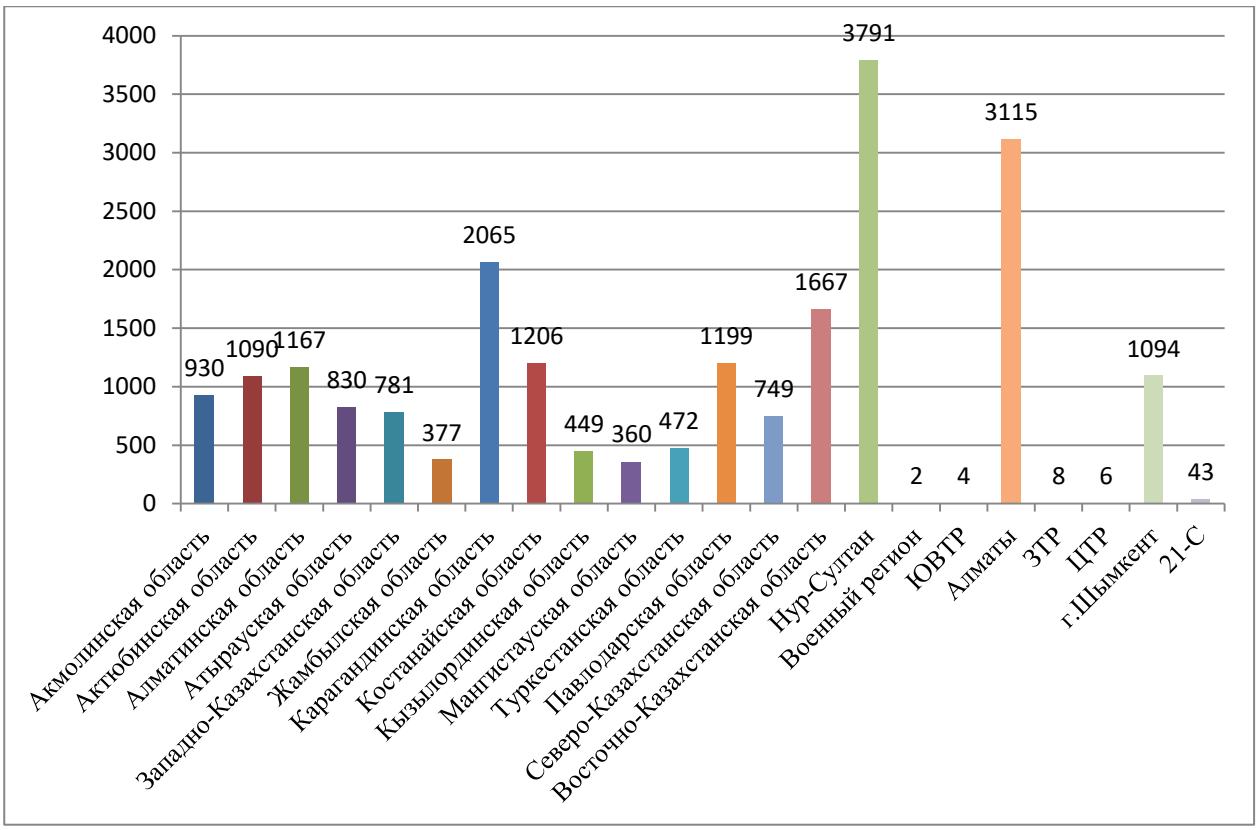

Рисунок 4. Регистрация интернет-мошенничеств в разрезе регионов за 2021 год.

Сегодня к наиболее распространенным видам мошенничества в Интернете относятся: фишинг; работа с платежными пластиковыми карточками; сделки на рынке ценных бумаг; онлайн аукционы и онлайн торговля; деловые возможности; «надомная работа»; сделки с мобильной сотовой связью и др.

Специалисты компании Dr.Web, отмечают, что фишинг (phishing) представляет собой технологию Интернет мошенничества, заключающуюся в хищении личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт-счетов и прочие сведения физического либо юридического лица.

С помощью спам рассылок или почтовых червей потенциальным жертвам отправляются подложные письма якобы от имени легальных организаций, в которых их просят зайти на фиктивный сайт такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию, используемую впоследствии для хищения денег со счета жертвы и в других преступлениях.

К примеру, в Акмолинской области мошенник по телефону связался с жертвой и сообщил последней о том, что она вправе получить «Президентскую премию». Далее, злоумышленник уговорил открыть карт-счет в одном из банков второго уровня. Затем, получив от жертвы сведения о номере ее платежной карты, убедил последнюю «привязать» ее на номер своего мобильного телефона. В результате, преступник похитил с депозита потерпевшей 10 млн. тенге.

Большинство мошенников, как правило, обладают достаточно глубоким

уровнем знаний в различных областях человеческой жизнедеятельности, в том числе психологии, экономике, юриспруденции, информационных технологиях.

Соответственно обман может совершаться в активной форме: путем рассылок спамерских писем, непосредственной работой мошенников в чатах, на сайтах и т.д. с использованием юридических документов.

Например, злоупотребляя доверием строительной компании, мошенник от ее имени начинает в сети Интернет предлагать к реализации строящиеся квартиры, используя настоящие правоустанавливающие документы данной компании. Действуя мошенническим способом от имени данной компании, мошенник заключает действительные инвестиционные договора под будущие квартиры, получает по этим договорам наличные средства, однако никаких работ по названным договорам не выполняет, скрывается с наличными средствами, чем причиняет значительный ущерб потерпевшим.

Не исключается и пассивная форма обмана, которую следует охарактеризовать как умолчание об истине.

Одни обстоятельства, в отношении которых обманывает преступник, непосредственно служат мнимым основанием для передачи имущества. Другие обстоятельства, не являясь основаниям для передачи денежных средств, используются преступником для того, чтобы создать предпосылки для другого обмана либо вызвать доверие к себе, а затем с большой легкостью обмануть или злоупотребить доверием потерпевшего. Они также входят в содержание мошеннического обмана, т.к. потерпевший учитывает эти обстоятельства, когда принимает решение о передаче имущества.

Так, в сети Интернет очень часто предлагается купить различные коды-доступа для скачивания фильмов, музыкальных файлов, картинок и т.д. При этом предлагается отправить SMS-сообщение на определенный номер. Расписывается также, из какой страны, на какой номер необходимо отправить данное сообщение.

После отправки SMS-сообщения зачастую приходит ответ, что код доступа будет отправлен клиенту после получения подтверждения оплаты. В последующем никаких кодов доступа не приходит, а со счета клиента списываются денежные средства.

Потерпевший, доверившись ложному намерению преступника, предоставляет последнему код доступа к персональным банковским данным и лишается денежных средств.

Часть правонарушений совершается с использованием «интернет-магазинов» под предлогом продажи автомобильных запчастей или иных потребительских товаров либо с использованием социальных сетей через создания «аккаунтов» от имени знакомых с дальнейшей просьбой перечисления денег на номер мобильного телефона, «Киви-кошельки» либо другие средства электронной оплаты.

Продолжаются случаи хищения денег под предлогом оказания услуг по выдаче кредита либо денежных займов под низкие проценты в «онлайн режиме».

Указанные в таких объявлениях контактные телефоны в основном являются разовыми и отключаются после совершения преступлений. В большинстве случаев Интернет-мошенничества совершаются посредством интернет сайтов, таких как: OLX.kz, kolesa.kz, krisha.kz.

Стоит отметить, что в целом рост регистрации мошенничеств обусловлен увеличением интернет-мошенничества и негативной практикой регистрации фактов неисполнения договорных обязательств.

Несмотря на то, что преступники оставляют следы при пользовании различными приложениями в сети Интернет, их практически невозможно вычислить ввиду того, что правонарушение может быть совершено из любой точки мира. Кроме того, злоумышленники скрывают свои персональные данные (регистрируются под вымышленными анкетными данными, используют программы-анонимайзеры, скрывающие географическое местоположение в сети), что затрудняет их поиск.

Более того, если они используют точки публичного доступа к сети Интернет, или незащищенные беспроводные сети, анонимные интернет-сервисы, то установление их личности представляет дополнительную сложность.

Раскрытие преступлений осложнено также и тем, что с технической точки зрения в Интернете отсутствуют наработанные механизмы контроля, которые могли бы использовать органы внутренних дел.

В феврале 2021 года в нескольких регионах страны обратились с заявлением в правоохранительные органы более 16 000 потерпевших, ставших жертвами махинации ломбардов. При этом, количество вкладчиков превышает 42 тысячи. В большинстве случаев, граждане лишились последнего жилья и крупных денежных средств.

В ходе расследования установлено, что с сентября 2019 года в 14 регионах республики одновременно начали свою деятельность ранее зарегистрированные ТОО «Гарант 24 Ломбард», ТОО «ESTATE Ломбард», ТОО «Выгодный займ» и ТОО «Нур-Али Капитал» (в городах Нур-Султан, Алматы, Шымкент, ВКО, ЗКО, Атырауской, Актюбинской, Жамбылской, Карагандинской, Костанайской, Туркестанской, Мангистауской, Кызылординской и Павлодарской областях).

Схема отъема имущества и денежных средств у граждан была построена на открытии и функционировании региональных представительств в 14-ти регионах республики, с обустройством офисов, набором штата сотрудников и назначением лжедиректоров предприятий.

Для привлечения граждан к своей деятельности в мессенджерах Инстаграм и WhatsApp руководителями ТОО созданы чаты, где регистрировались все вкладчики для получения информации по своим сделкам. Выкупали движимое и недвижимое имущество по завышенной стоимости, либо в рассрочку. В последующем, только в течение 3-5 месяцев клиентам выплачивали небольшую сумму сделки, а полученное имущество реализовывали третьим лицам ниже рыночной стоимости.

Кроме этого, указанные компании принимали вклады в качестве депозита от 30 до 40% ежемесячно. Все денежные средства инкассировались в головной

офис наличными и нарочно.

15 февраля 2020 года руководители данных ТОО практически одновременно прекратили свою деятельность и с похищенными денежными средствами пострадавших скрылись за пределами страны [37].

В период коронавирусной пандемии мошенниками причинен ущерб на сумму свыше 304 млрд тенге, из которых государству причинен ущерб на сумму 33 млрд тенге, физическим и юридическим лицам 271,8 млрд тенге.

В ходе расследования возмещено 68,1 млрд. тенге (государству 26,1 млрд, юридическим лицам 23,5 млрд, физическим лицам 18,5 млрд.).

Однако, в разделе №4 «Сведения об установленной сумме материального ущерба и его возмещаемости по оконченным уголовным делам» отчета 1-М отсутствуют данные о сумме материального ущерба и его возмещаемости по оконченным уголовным делам, в том числе о мошенничестве, совершаемых посредством сети Интернет.

В этой связи, полагаем целесообразным КПСиСУ разработать механизм внесения в ЭИУД формы ЕРДР-2, в реквизит №23 «ущерб» дополнительного показателя «посредством сети Интернет».

Указанные меры ввиду значительного роста регистрации правонарушений, совершенных в сети Интернет и невозвратности похищенных средств позволят разграничить сумму ущерба киберпреступлений от общей суммы ущерба уголовных правонарушений.

Следующим видом уголовных правонарушений совершаемых в сети Интернет по количеству регистрации в ЕРДР является незаконный оборот наркотических средств.

При этом преступность в сфере незаконного оборота наркотических средств выделяется по ее отличительным признакам, родовым и видовым, позволяющим говорить о ней как о самостоятельном виде преступности, которым является преступная деятельность лиц, совершающих преступления в сфере незаконного оборота наркотических средств с использованием компьютерных технологий.

В настоящее время интернет-ресурсы являются основной площадкой для распространения наркотических средств, психотропных веществ и прекурсоров, путем «закладок».

В современном толковом словаре криминалист Бегалиев Е.Н. дает следующее понятие: «закладка - предварительно оговоренное (условное) место транзитного хранения наркотических средств, психотропных веществ и прекурсоров, используемое сбытчиком для передачи дозы/партии потребителю [38].

Ключевым преимуществом закладки является бесконтактный сбыт и приобретение, что негативно влияет на процесс выявления и раскрытия таких преступлений.

«Закладку» можно рассматривать в качестве способа совершения сбыта наркотических средств, потому что поставка продукции покупателю осуществляется через курьера и основной целью является получение денежных средств способом перевода на карт-счета.

Правоохранительными органами РК проводится мониторинг различных Интернет-ресурсов, социальных сетей и работа по недопущению трафаретной рекламы. Всего по Казахстану выявлено более тысячи интернет адресов, с помощью которых производилась реализация наркотических средств, в том числе и синтетических.

Методы распространения наркотических средств становятся все сложнее, что создает определенные трудности для выявления и предупреждения этих преступлений.

Все действия, связанные с поиском клиентов с помощью «смс-переписки» в мобильных приложениях и социальных сетях, производством закладок осуществляются курьерами. Для переводов денежных средств с помощью электронных платежных систем используются подставные лица, на которых регистрируются данные счета.

Следует отметить тот факт, что лица, занимающиеся расследованием данного рода преступлений, а также работники судебной системы в большинстве своем не обладают специальными познаниями в области новых компьютерных технологий, что создает определенные трудности при квалификации и расследовании таких деяний.

Выявление и расследование в большинстве случаев осуществляют сотрудники, имеющие высшее юридическое образование (в соответствии с квалификационными требованиями), специализирующиеся на расследовании общеуголовных преступлений, в том числе в сфере коррупции и экономики.

Отсутствие у следственных работников правоохранительных органов Казахстана специальных познаний в расследовании уголовных дел данной категории, недостаточный уровень навыков у сотрудников оперативных подразделений не позволяет своевременно раскрывать преступления, устанавливать доказательства и привлекать к ответственности виновных лиц.

УПК РК (ст.ст.79, 80) позволяет привлекать лиц с IT-образованием лишь в качестве экспертов или специалистов для дачи заключения или технического сопровождения отдельных процессуальных действий, которые не заинтересованы в исходе дела и не уполномочены осуществлять расследование.

С учетом наблюдаемого роста уголовных правонарушений, совершаемых в сети Интернет, принимаемые государством меры в данной области явно недостаточны. Данная проблема обозначена в Послании Президента народу Казахстана в сентябре 2021 года, в котором отмечена необходимость усиления отечественного IT-сектора с взращиванием 100 тысяч молодых IT-специалистов [39].

В настоящее время вопросы противодействия уголовным правонарушениям в сфере информатизации и связи, преступлениям, совершаемым с использованием информационных технологий (незаконное распространение порнографии, развращение детей через Интернет, борьба с распространением контрафактной продукции, сбыт специальных технических средств, электронные хищения, в т.ч. интернет-мошенничества), мониторинг, выявление и пресечение распространения противоправного контента в сети Интернет возложены на Центр по борьбе с киберпреступностью Департамента

криминальной полиции МВД РК, количество сотрудников которого не позволяет обеспечить принятие действенных мер со стороны государства по обеспечению противодействия значительному росту уголовных правонарушений, совершаемых в сети Интернет, проникновению криминальных угроз в информационно-телекоммуникационную среду, в том числе транснационального характера.

В связи, с чем, в целях повышения эффективности противодействия уголовным правонарушениям в сети Интернет, усиления специального подразделения и исключения выполнения не свойственных задач, предлагается создание на базе МВД РК самостоятельного подразделения по борьбе с киберпреступностью.

Подразделению следует придать функции по реализации государственной политики в сфере борьбы с киберпреступностью, межведомственной координации в области предупреждения, раскрытия и расследования, общеуголовных киберпреступлений, проведения исследований электронно-цифровых доказательств, противодействия преступлениям с использованием сети Интернет, взаимодействия с частным сектором (провайдеры, банковский сектор, ВУЗЫ, научное сообщество, правообладатели и др.) и международного взаимодействия.

Таким образом, в целях повышения эффективности противодействия преступлениям, совершаемым в сети Интернет либо с его использованием, предлагается:

- усовершенствовать действующую статистическую отчетность, что позволит определить общее число правонарушений, совершенных в сети Интернет и разграничить сумму ущерба от киберпреступлений;
- рассмотреть вопрос о создании центров подготовки специалистов по противодействию киберпреступлениям в учебных заведениях правоохранительных органов республики, что ускорит процесс укомплектованиях компетентными и профессиональными сотрудниками.
- создать в МВД самостоятельное подразделение по борьбе с киберпреступностью.

РАЗДЕЛ II. Вопросы расследования уголовных правонарушений, совершенных в сети Интернет

2.1 Исследование дефиниций, применяемых в отечественном законодательстве по уголовным правонарушениям в сети Интернет

Широкое применение в повседневной деятельности человека компьютеров и сети Интернет развивает новые виды экономической активности.

Благодаря цифровым и сетевым инструментам, в мире активно развиваются электронные торговые площади, происходит переход на цифровые бизнес процессы. В цифровую эволюцию включены такие социально значимые сферы как здравоохранение, образование, наука, судопроизводство.

Государственные органы используют достижения информационных технологий для организации оперативного управления и повышения качества услуг, предоставляемых населению.

Применение компьютерных технологий во всех сферах общественной жизни является необходимым условием для перехода к высокотехнологичному обществу XXI века.

Однако прогресс и результаты цифровизации используются как в благих целях, приносящих обществу пользу, так и при совершении различного рода правонарушений.

Серьезную угрозу для стабильности государства представляют уголовные правонарушения, связанные со взломом компьютерных сетей государственных органов, банков, различных организаций, предоставляющих услуги населению.

С использованием компьютерных технологий могут совершаться как уголовные правонарушения, предусмотренные главой 7 УК РК («Уголовные правонарушения в сфере информатизации и связи»), так и более распространенные их виды (кража, мошенничество, распространение наркотиков и т.д.).

Важную роль в противодействии уголовным правонарушениям играет введение новых составов уголовных правонарушений соответствующих реалиям сегодняшнего времени, в том числе своевременная выработка единообразно трактуемых юридических терминов, применяемых в уголовном законодательстве.

В юридической науке вопросы выработки новых понятий и употребления юридической терминологии рассматриваются как проблемы языка законодательства.

Норма права, из которой состоит любой правовой акт, является ядром нормативного регулирования и ее построение основано на специальных ключевых словах - юридических терминах, предназначенных для точного и ясного изложения его текста.

По мнению Алексеева С.С. юридический термин - это выраженное непосредственно в тексте акта словесное обозначение определенного понятия. Относясь к средствам словесно-документального изложения, термины вместе с

тем служат исходным материалом для строительства норм, их общностей [40, С. 49].

Большой юридический словарь дает следующее определение юридических терминов - это словесные обозначения государственно-правовых понятий, с помощью которых выражается и закрепляется содержание нормативно-правовых предписаний государства [41, С. 702].

То есть, юридическому термину и соответственно нормативному правовому акту присущ особый стиль изложения, который именуется официально - деловым или официально-документальным.

Аналогичная идея прослеживается в ст.24 Закона РК от 6 апреля 2016 года «О правовых актах», в которой определено, что текст нормативного правового акта излагается с соблюдением норм литературного языка, юридической терминологии и юридической техники, его положения должны быть предельно краткими, содержать четкий и не подлежащий различному толкованию смысл. Текст нормативного правового акта не должен содержать положения декларативного характера, не несущие смысловой и правовой нагрузки.

Необходимость совершенствования терминологии и соответственно понятийного аппарата свойственна любой области науки и практики. Это в первую очередь связано с возросшим количеством информации, получаемой и обрабатываемой человеком в современном обществе, что пропорционально ведет к возрастанию числа используемых терминов и необходимости формулировки и внедрения в законодательство новых важных дефиниций, используемых ежедневно, но еще не включенных в соответствующие нормативные правовые акты.

Анализ норм действующего УК РК показал, что в нем содержится 32 статьи, связанные с совершением уголовных правонарушений в сети Интернет.

Подобные термины содержатся в статьях УК РК: 105 «Доведение до самоубийства», 131 «Оскорбление», 132 «Вовлечение несовершеннолетнего в совершение уголовных правонарушений», 134 «Вовлечение несовершеннолетнего в занятие проституцией», 147 «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите», 148 «Незаконное нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», 161 «Пропаганда или публичные призывы к развязыванию агрессивной войны», 174 «Разжигание социальной, национальной, родовой, расовой, сословной или религиозной розни», 179 «Пропаганда или публичные призывы к захвату или удержанию власти, а равно захват или удержание власти либо насильственное изменение конституционного строя Республики Казахстан», 180 «Сепаратистская деятельность», 188 «Кража», 190 «Мошенничество», 195 «Причинение имущественного ущерба путем обмана или злоупотребления доверием», 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций», 206 «Неправомерные уничтожение или модификация информации», 207 «Нарушение работы информационной системы или сетей телекоммуникаций», 208 «Неправомерное

завладение информацией», 209 «Принуждение к передаче информации», 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов», 211 «Неправомерное распространение электронных информационных ресурсов ограниченного доступа», 212 «Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели», 223 «Незаконные получение, разглашение или использование сведений, составляющих коммерческую либо банковскую тайну, налоговую тайну, полученную в ходе горизонтального мониторинга, тайну предоставления микрокредита, тайну коллекторской деятельности, а также информации, связанной с легализацией имущества», 256 «Пропаганда терроризма или публичные призывы к совершению акта терроризма», 274 «Распространение заведомо ложной информации», 297 «Незаконные изготовление, переработка, приобретение, хранение, перевозка в целях сбыта, пересылка либо сбыт наркотических средств, психотропных веществ, их аналогов», 299 «Склонение к потреблению наркотических средств, психотропных веществ, их аналогов», 299-1 «Пропаганда или незаконная реклама наркотических средств, психотропных веществ или их аналогов, прекурсоров», 301 «Незаконный оборот ядовитых веществ, а также веществ, инструментов или оборудования, используемых для изготовления или переработки наркотических средств, психотропных веществ, их аналогов или ядовитых веществ», 373 «Публичное оскорбление и иное посягательство на честь и достоинство Первого Президента Республики Казахстан – Елбасы, осквернение изображений Первого Президента Республики Казахстан – Елбасы, воспрепятствование законной деятельности Первого Президента Республики Казахстан – Елбасы», 375 «Посягательство на честь и достоинство Президента Республики Казахстан и воспрепятствование его деятельности», 376 «Посягательство на честь и достоинство депутата Парламента Республики Казахстан и воспрепятствование его деятельности», 378 «Оскорбление представителя власти».

Изучение данных норм показало, что в них наиболее часто употребляются такие термины как:

1. сети телекоммуникаций (в ст.ст. 105, 131, 132, 134, 147, 148, 161, 174, 179, 180, 188, 195, 205, 206, 207, 208, 209, 210, 256, 274, 373, 375, 376, 378 – всего в 24 из 32).

Согласно ст.2 Закона РК от 5 июля 2004 года «О связи» сеть телекоммуникаций – совокупность средств телекоммуникаций и линий связи, обеспечивающих передачу сообщений телекоммуникаций, состоящая из коммутационного оборудования (станций, подстанций, концентраторов), линейно-кабельных сооружений (абонентских линий, соединительных линий и каналов связи), систем передачи и абонентских устройств.

2. сеть Интернет (в ст.ст. 105, 132,134 – всего в 3 из 32).

В соответствии со ст.1 Закона РК от 24 ноября 2015 года «Об информатизации» «Интернет – всемирная система объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов».

3. средства массовой информации (в ст.ст. 131, 147, 161, 174, 179, 180, 256, 274, 299-1, 373, 375, 376, 378 – всего в 13 из 32).

В ст.1 Закона РК от 23 июля 1999 года «О средствах массовой информации» «средство массовой информации - периодическое печатное издание, теле-, радиоканал, кинодокументалистика, аудиовизуальная запись и иная форма периодического или непрерывного публичного распространения массовой информации, включая интернет-ресурсы».

4. электронные информационные ресурсы (в ст.ст. 147, 148, 211, 297, 299, 299-1, 301 - всего в 7 из 32).

Согласно ст.1 Закона РК от 24 ноября 2015 года «Об информатизации» «электронные информационные ресурсы – информация в электронно-цифровой форме, содержащаяся на электронном носителе и в объектах информатизации».

«Объекты информатизации – электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура».

5. информационная система (в ст.ст. 147, 148, 188, 190, 195, 205, 206, 207, 208, 209, 210 – в 11 из 32).

Согласно ст.1 Закона РК от 24 ноября 2015 года «Об информатизации» «информационная система – организационно-упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач».

6. критически важные объекты информационно-коммуникационной инфраструктуры (в ст.ст. 205, 206, 207, 208, 209, 210 – в 6 из 32) – согласно ст.1 Закона РК от 24 ноября 2015 года «Об информатизации» «объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, «электронного правительства».

«Объект информационно-коммуникационной инфраструктуры – информационная система, технологическая платформа, аппаратно-программные комплексы, серверные помещения (центры обработки данных), сети телекоммуникаций, а также системы обеспечения информационной безопасности и бесперебойного функционирования технических средств».

Некоторые термины, используемые в УК РК, встречаются лишь в одной статье:

1. аппаратно-программный комплекс (в ст.212).

Согласно ст.1 Закона РК от 24 ноября 2015 года «Об информатизации» «аппаратно-программный комплекс – совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа».

2. интернет-ресурс (в ст.212).

«Интернет-ресурс – информация (в текстовом, графическом, аудиовизуальном или ином виде), размещенная на аппаратно-программном комплексе, имеющем уникальный сетевой адрес и (или) доменное имя и функционирующем в Интернете» (ст.1 Закона РК «Об информатизации»).

3. электронный носитель (в ст.210).

«Материальный носитель, предназначенный для хранения информации в электронной форме, а также записи или ее воспроизведения с помощью технических средств» (ст.1 Закона РК «Об информатизации»).

4. программный продукт (в ст.210).

«Самостоятельная программа или часть программного обеспечения, являющаяся товаром, которая независимо от ее разработчиков может использоваться в предусмотренных целях в соответствии с системными требованиями, установленными технической документацией» (ст.1 Закона РК «Об информатизации»).

5. абонентское устройство (в ст.210).

«Средство связи индивидуального использования, формирующее сигналы электрической связи для передачи или приема заданной абонентом информации и подключаемое к сети оператора связи» (ст.2 Закона «О связи»).

Следует отметить, что практически во всех анализируемых статьях, совершение уголовных правонарушений, с использованием цифровых технологий влечет более суровую уголовную ответственность путем включения их в части 2 или 3 указанных статей.

Только в 10 статьях из 32, указанные выше термины включены также в 1 часть (в ст. ст.174, 205, 206, 207, 208, 209, 210, 211, 212, 223).

Вместе с тем, возникает вопрос о необходимости употребления определенных дефиниций, без разброса синонимичных терминов по 32 статьям.

Так, в статьях 105, 132, 134 УК РК используется такое определение преступного деяния как «**совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет».**

Обратив внимание на определение главных составных частей можно сделать вывод о том, что **сеть Интернет** согласно приведенному законодательному определению, **представляет собой систему объединенных сетей телекоммуникаций.**

Профессор Пиголкин А.С., говоря о требованиях к терминам в языке законодательных актов, отмечал следующие их характеристики:

«- точное и недвусмысленное отражение содержания обозначаемого правового понятия, недопустимость использования неясных, многозначных, расплывчатых и нечетко оформленных терминов;

- использование терминов в их прямом и общеизвестном значении; - простота и доступность терминов;

- отказ от употребления устаревших и активно неиспользуемых в литературном языке слов и словосочетаний;

- отказ от употребления канцеляризмов, словесных штампов, слов и оборотов бюрократического стиля; - использование, как правило, общепринятых и устоявшихся в литературном языке терминов, имеющих широкое применение;

- устойчивость, стабильность в использовании юридических терминов;

- благозвучие и стилистическая правильность юридических терминов;

- отказ от чрезмерного употребления терминов-аббревиатур и сокращений, образовавшихся из двух или более слов;

- присвоение сходных наименований, по возможности однокоренных, близким по содержанию правовым понятиям для обеспечения единства терминологии;

- максимальная краткость формирования терминов» [42].

Полагаем, что добавление законодателем слов «в том числе сети Интернет» в статьях 105, 132, 134 УК РК излишне и фактически дублирует понятие «сети телекоммуникаций», которым охватывается Интернет как сеть телекоммуникаций, в связи с чем, предлагаем его исключить.

Следует обратить внимание на вопрос формулирования законодателем составов некоторых уголовных правонарушений из числа проанализированных.

Анализ содержания 32 статей УК РК показал, что в некоторых используются терминологические обороты, которые по нашему мнению требуют пересмотра ввиду узкого их определения.

В ст.ст.131, 161, 174, 256, 274, 373, 375, 376, 378 УК РК при определении состава уголовного правонарушения в качестве квалифицирующего признака используется понятие «**совершенное с использованием средств массовой информации или сетей телекоммуникаций».**

В то же время, в ст.ст.105, 132, 134 УК РК законодателем используется такой квалифицирующий признак как «совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет».

В этом случае подобный подход ограничивает правоприменителя и сужает сферу применения указанной нормы к подобным деяниям, что не совсем верно.

Интернет состоит из сайтов, на которых его владельцами размещается различная информация, а пользователи находят на них требующийся им контент.

Интернет сайт – это интернет-ресурс, который включает в себя объединенные ссылками и общей структурой документы (веб-страницы). Они обязательно имеют уникальное доменное имя (адрес), которое официально регистрируется на юридическое или физическое лицо [43].

Интернет-ресурс, в свою очередь, относится к средствам массовой информации согласно Закону РК от 23 июля 1999 года «О средствах массовой информации».

Более логичным, по нашему мнению, для законодателя является использование расширенного подхода, примененного в статьях 131, 161, 174, 256, 274, 373, 375, 376, 378 УК РК.

В частности, в качестве квалифицирующего признака в пп.4 ч.2 ст.105, ч.2 132, пп.1-1 ч.3 134 УК РК использование оборота **«с использованием средств массовой информации или сетей телекоммуникаций»**.

Предлагаем пп.4 ч.2 ст.105, ч.2 132, пп.1-1 ч.3 134 УК РК изложить в следующей редакции:

- пп.4 ч.2 ст.105 УК РК.

То же деяние, совершенное:

«4) посредством использования средств массовой информации или сетей телекоммуникаций».

- ч.2 132 УК РК.

«То же деяние, совершенное родителем, педагогом либо иным лицом, на которое законом РК возложены обязанности по воспитанию несовершеннолетнего, или посредством использования средств массовой информации или сетей телекоммуникаций».

- пп.1-1 ч.3 134 УК РК.

«1-1) посредством использования сетей телекоммуникаций, в том числе сети Интернет средств массовой информации или сетей телекоммуникаций».

В некоторых статьях УК РК используются термины «посредством использования» (105, 132, 134, 297, 301) «с использованием» (131, 161, 174, 179, 180, 256, 274, 299-1, 373, 375, 376, 378), «путем» (147, 148, 188, 190, 223).

Согласно Толковому словарю русского языка Ожегова С.И. «посредством» означает «при помощи чего-нибудь, каким-нибудь способом, используя что-нибудь» [44].

Следовательно, данные термины являются синонимами и не противоречат друг другу.

Предлагается пересмотреть использование данных терминов для их единообразного применения.

В качестве альтернативы, предлагаем закрепить во всех указанных статьях, где применены термины «с использованием» и «путем» термин «посредством» как наиболее логичный и соответствующий юридическому языку.

Как указывает Петров Е.П.: «При формулировке того или иного понятия в нормативном акте необходимо придерживаться однозначности, четкости, полноты одних и тех же юридических терминов, используемых в различных нормативно-правовых актах с тем, чтобы не исказить смысл и язык самих юридических норм в тесте законодательных актов» [45].

Как показало изучение терминов, применяемых в вышеуказанных статьях, не все они регламентированы действующим законодательством.

В частности, отсутствуют дефиниции таких терминов как: компьютер (ст.210 УК РК), компьютерная программа (ст.210 УК РК), информационно-коммуникационная сеть (ст.212 УК РК), компьютерная система (ст.223 УК РК), компьютерная сеть (ст.223 УК РК).

То есть, законодатель предусмотрел, например, в ч.1 ст.210 УК РК ответственность за создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью нарушения работы компьютера, компьютерной программы.

При этом, им не дано определение понятиям «компьютер», «компьютерная программа», что затрудняет правоприменительную практику. В каждом конкретном случае правоприменителю необходимо установить, на основе собственного представления, опыта является то или иное оборудование, файл, информация и т.д. «компьютером», «компьютерной программой» и, соответственно, можно ли привлекать к уголовной ответственности лицо по данной статье или нет.

Генеральный секретарь ООН Гуттериш А. в своем докладе «Противодействие использованию информационно-коммуникационных технологий в преступных целях» (30.07.2019 года) подчеркнул, что одной из проблем, с которыми сталкиваются государства в борьбе с использованием информационно-коммуникационных технологий в преступных целях, являются трудности, возникающие при обновлении нормативно-правовой базы в отношении технического прогресса. Постоянное обновление уголовно-правовой базы с точки зрения как существа, так и процедур сопряжено с многочисленными трудностями, которые носят более серьезный характер в странах с кодифицированными правовыми системами [46].

Данный вывод справедлив ввиду необходимости постоянного мониторинга национального уголовного законодательства на предмет его способности противодействовать новым и «совершенствуемым» преступным сообществом уголовным правонарушениям и способам их совершения.

Хотя многие термины и являются общераспространенными, внесение их в уголовное законодательство в качестве квалифицирующих признаков требует их соответствующей расшифровки ввиду отсутствия технического образования у многих правоприменителей, в том числе, которые опираются лишь на терминологию, закрепленную в законодательстве.

Существенной функциональной чертой терминов, используемых в нормативных правовых актах, является то, что они отражают официальную волю законодателя, оказывая тем самым определенное воздействие на субъекты правовых отношений.

Информационным образом репрезентировать эту волю для соответствующего восприятия могут только правовые термины. Создание, унифицирование и жесткое регламентированное использование специального терминологического фонда нормативно-правовой информации обусловлено, таким образом, самой природой права, его социальным назначением, необходимостью обеспечения правильного наименования и понимания его различных структурных элементов, адекватной репрезентации многоаспектных логических и иных связей и взаимоотношений между ними, конкретной содержательной определенностью нормативных предписаний, их функциональной стабильностью и эффективностью [47, С. 181].

Основополагающим элементом развития эры высоких технологий стал компьютер, разработанные программы для его функционирования и расширения возможностей его применения в различных сферах общественной жизни.

При этом, несмотря на широкое распространение компьютеров и его программ, данные термины в национальном законодательстве не закреплены.

В научно-технической литературе имеется масса определений компьютера и компьютерных программ, информационно-коммуникационной сети, компьютерной системы, компьютерной сети. Все они схожи и перечислять их не имеет смысла, так как технические термины в данном случае имеют международно-применимый характер и не зависят от применяемого в государстве права.

Компью́тер - устройство или система, способная выполнять заданную, чётко определённую, изменяемую последовательность операций. Это чаще всего операции численных расчётов и манипулирования данными, операции ввода-вывода информации [48].

Компьютерная программа (программное обеспечение), набор расположенных поэтапно команд, позволяющих компьютеру выполнить поставленную задачу [49].

В ст.1261 Гражданского кодекса Российской Федерации (далее - ГК РФ) закреплено понятие «программа для ЭВМ» (электронно-вычислительная машина), фактически являющееся синонимом понятия компьютерная программа.

Так, программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения [50].

Полагаем, что данное определение достаточно полно отражает сущность понятия «компьютерная программа» и с исключением термина ЭВМ как устаревшего с заменой его на понятие «компьютер» может быть применено в условиях казахстанского правового поля.

Переходим к термину «информационно-коммуникационные сети» (ч.1 ст.212 УК РК), не регламентированному в отечественном законодательстве.

Согласно диспозиции ч.1 ст.212 УК РК уголовную ответственность влечет «заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытой информационно-коммуникационной сети, для размещения интернет-ресурсов, преследующих противоправные цели».

Из данной нормы следует, что информационно-коммуникационная сеть служит местом для размещения интернет-ресурсов.

Интернет-ресурс может функционировать лишь в сети Интернет, что логично и соответствует его определению, закрепленному в ст.1 Закона РК «Об информатизации».

Интернет, в свою очередь, представляет собой всемирную систему объединенных сетей телекоммуникаций и вычислительных ресурсов для передачи электронных информационных ресурсов.

Как отмечает профессор Борчашвили И.Ш., под «открытой информационно-коммуникационной сетью следует понимать сеть Интернет» [51, С. 397].

То есть, информационно-коммуникационная сеть фактически является сетью телекоммуникаций.

Для реализации принципа единообразия применяемых терминов в УК РК предлагаем ч.1 ст.212 изложить в следующей редакции:

«- Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытых **сетях телекоммуникаций,** для размещения интернет-ресурсов, преследующих противоправные цели».

Другими терминами, требующими правовой регламентации, являются «компьютерная система» и «компьютерная сеть», указанные в ч.1 ст.223 УК РК.

В Конвенции о компьютерных преступлениях (принята Советом Европы, в г. Будапешт 23.11.2001 года) **компьютерная система** означает любое устройство или группу взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных [52].

Полагаем, что имплементация термина из указанной Конвенции и других международных актов в национальное законодательство в целом будет иметь положительный эффект и свидетельствовать о приверженности Казахстана международным стандартам противодействия преступности и защиты прав человека от преступных посягательств

Компьютерная сеть - система, состоящая из компьютеров и компьютерных устройств (принт-серверов, серверных веб-камер и др.), которые взаимодействуют по единым правилам, определённым сетевыми протоколами. Компьютерная сеть предназначена для совместного пользования различными сервисами (электронной почтой, поисковыми системами и др.), информационными ресурсами, программами (например, программами серверов приложений) и аппаратными средствами (жёсткими дисками, принтерами и др.) [53].

Проведенное изучение дефиниций, применяемых в отечественном законодательстве по уголовным правонарушениям в сети Интернет, показало, что национальное законодательство содержит часть используемых в УК РК понятий, но в то же время единообразного подхода при использовании терминов нет.

Это создает риски различного толкования и нарушает принцип единообразного применения норм права, когда для обозначения одних и тех же понятий должны использоваться одни и те же термины.

Таким образом, выработанные предложения будут способствовать систематизации и единообразному применению законодательства, позволят

избежать нарушений законности при осуществлении досудебного расследования.

Учитывая изложенное, предлагается следующее:

Первое. В ст.ст.105, 132, 134 УК РК используется квалифицирующий признак как **«совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет».**

При этом, **сеть Интернет** согласно ст.1 Закона РК «Об информатизации» представляет собой сеть телекоммуникаций**.**

Предлагаем исключить в данных статьях слова «в том числе сети Интернет», как оборот речи, не несущий смысловой нагрузки.

Второе. Используемый в ст.ст.105, 132, 134 УК РК квалифицирующий признак **«совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет»** ограничивает правоприменителя, сужая сферу применения данной нормы к подобным деяниям.

В целях расширения сферы действия данной нормы предлагается в качестве квалифицирующего признака в пп.4 ч.2 ст.105, ч.2 132, пп.1-1 ч.3 134 УК РК использовать оборот **«с использованием средств массовой информации или сетей телекоммуникаций»**.

Третье. В целях единообразного применения терминов, их логического построения и изложения юридическим языком, используемых в УК РК речевых оборотов, в ст.ст.131, 161, 174, 179, 180, 256, 274, 299-1, 373, 375, 376, 378 УК РК, где применяется термин «с использованием» и в ст.ст.147, 148, 188, 190, 223 УК РК - «путем», использовать термин «посредством» как наиболее соответствующий требованиям юридической техники.

Четвертое. Ввиду отсутствия в действующем законодательстве соответствующих дефиниций, предлагается дополнить ст.3 УК РК следующим:

а) **Компью́тер** - устройство или система, способная выполнять заданную, чётко определённую, изменяемую последовательность операций. Это чаще всего операции численных расчётов и манипулирования данными, операции ввода-вывода информации.

б) **Компьютерная программа** - представленная в объективной форме совокупность данных и команд, предназначенных для функционирования компьютера и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для компьютера, и порождаемые ею аудиовизуальные отображения.

в) **Компьютерная система** - любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

г) **Компьютерная сеть** - система, состоящая из компьютеров и компьютерных устройств (принт-серверов, серверных веб-камер и др.), которые взаимодействуют по единым правилам, определённым сетевыми протоколами.

Пятое. Установлено, что понятие «информационно-коммуникационная сеть», закрепленное в ч.1 ст.212 УК РК фактически является сетью телекоммуникаций.

В этой связи, в целях реализации принципа единообразия применяемых терминов в УК РК, предлагаем ч.1 ст.212 изложить в следующей редакции:

«- Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в **сетях телекоммуникаций,** для размещения интернет-ресурсов, преследующих противоправные цели».

Процесс эволюции закона сложен и не может быть окончен на каком-то конкретном этапе. Отечественное законодательство поступательно развивается с учетом мировых трендов законодательной техники.

Множество явлений и предметов постоянно нуждаются в нормативной конкретизации и закреплении вследствие развития общественных отношений. Как показал анализ, данная работа требует от законодателя постоянного совершенствования и унификации имеющихся норм.

Давид Р. отмечал: «Закон в силу самой строгости его изложения представляется лучшим техническим способом установления четких норм в эпоху, когда сложность общественных отношений выдвигает на первый план среди всех аспектов правильного решения его точность и ясность» [54].

Закон является юридическим инструментом по разрешению различных социально-экономических, политических вопросов в государстве.

Особую важность в процессе законотворчества приобретает совместная работа ученых и правоприменителей по наполнению нашего законодательства четкими и ясными нормами, направленными на обеспечение конституционных прав человека, так как законы не должны стоять на месте, постоянно совершенствуясь в соответствии с изменяющимися потребностями общества.

2.2. Проблемы выявления уголовных правонарушений в сети Интернет

Уголовные правонарушения, совершаемые в сети Интернет, вместе с бурным развитием научно-технического прогресса с каждым днем приобретают все более изощренные и опасные формы, в том числе и транснационального характера.

Наряду с этим, происходит изменение мотивации соответствующей противоправной деятельности, активно осваиваются ее новые формы и расширяется география совершаемых уголовных правонарушений. Отмечается усиление организованности криминальных структур, использующих возможности Интернета в преступной деятельности.

Правоохранительные органы все чаще имеют дело с профессиональными преступниками, с высоким уровнем технической подготовленности и упорством в достижении цели. Будучи осведомленными о формах и методах работы органов они оказывают активное «интеллектуальное» сопротивление раскрытию преступлений.

Наиболее заметную роль играют хакерские сообщества, имеющие особую криминогенную среду, способную продуцировать значительное число латентных преступлений. Оно имеет сложную организацию и характеризуется специфическими механизмами взаимодействия участников, неизвестными ранее формами организации групповой противоправной деятельности.

В сети Интернет преступники способны воплощать в жизнь целый ряд различных незаконных операций одновременно в нескольких информационных системах. То есть, дистанционно совершают действия направленные на информационные объекты, находящиеся на значительном расстоянии, перемещаясь в физическом пространстве.

Таким образом, «размывается» физическое место совершения преступления и нарушается пространственная локализация.

Сложность обнаружения действий компьютерного преступника и его возможности совершать преступления в киберпространстве, не имеющем государственных временных границ, многократно увеличивают степень общественной опасности таких деяний [55, С. 36].

Следует отметить, что сетевая социальная среда крайне разнородна, и определенная ее часть разделяет общественно опасные взгляды. Комфортные условия, предоставленные в сетевом пространстве, приводят к появлению в нем многочисленных криминальных сетевых ресурсов. Растет число сайтов, принадлежащих организованным преступным формированиям (ОПФ), через которые они обмениваются информацией, пытаются популяризировать свои идеи.

Наряду с этим, формируются рынки и секторы теневой преступной экономики как детская порнография, сбыт наркотических средств, рекомендаций по их изготовлению, торговля оружием, похищенными номерами кредитных карт и др.

В Интернете размещаются видеосъемки реальных сцен насилия, распространяются общественно опасные разъяснения по изготовлению взрывчатых и отравляющих веществ, описываются способы совершения суицида, пропагандируются экстремизм, разврат, каннибализм и т.п.

По данным Министерства информации и общественного развития РК в период с 2017 года по 1 квартал 2021 года наибольшее количество совершаемых через сеть противоправных деяний зафиксированы по следующим направлениям:

1. Пропаганда терроризма, экстремизма;

2. Распространение порнографии;

3. Пропаганда наркотических средств, психотропных веществ, их аналогов и прекурсоров;

4. Распространение информации, пропагандирующей суицид (таблица 3) [56].

Годы	Пропаганда терроризма, пропаганда экстремизма	Распространение порнографии	Пропаганда наркотических средств, психотропных веществ, их аналогов и прекурсоров	Распространение информации, пропагандирующей суицид
2017	79186	2562	2097	923
2018	148998	1346	945	354
2019	56428	3779	1851	133
2020	72025	2125	1068	87
2021	231140	6760	1754	28

Таблица 3 Совершаемые в сети противоправные деяния

Наряду с этим, реальную угрозу интересам общества несет и размещение в Интернете вредоносных программ, устройств компьютерного взлома, методических рекомендаций по применению хакерского инструментария, а также продажа запрещенных к обороту специальных технических средств.

Сетевые сообщества, размещающие подобные сведения в Интернете, непременно должны попадать под контроль правоохранительных органов.

Вместе с тем, росту уголовных правонарушений, совершаемых в сети Интернет, способствуют и такие проблемы, как низкая правовая грамотность населения, работников сферы ИКТ и руководителей организаций по вопросам информационной безопасности и программного обеспечения.

Выявление, изучение, фиксация и изъятие в установленном законом порядке цифровых объектов, следов и информации из мобильного устройства позволяют:

- напрямую изобличать лицо в совершении преступления;

- косвенно указывать на линию поведения лица, возможную причастность его к совершенному преступлению;

- способствовать установлению иных обстоятельств, имеющих значение для уголовного дела.

Вместе с тем, компьютерная информация может быть как носителем следов совершенного уголовного правонарушения, так и непосредственно являться их следами. В сфере высоких технологий компьютерная информация легко передается, копируется, блокируется или модифицируется с беспрецедентной скоростью и на значительном расстоянии.

Как отмечает Мещеряков В.А., для таких следов характерны «специфические свойства, определяющие перспективы их регистрации, извлечения и использования в качестве доказательств, при расследовании совершенного преступления.

Во-первых, «виртуальные следы» существуют на материальном носителе, но не доступны непосредственному восприятию. Для их извлечения необходимо обязательное использование программно - технических средств. Они не имеют жесткой связи с устройством, осуществившим запись информации, являясь «виртуальным следом, … весьма неустойчивы, и могут быть легко уничтожены.

Во-вторых, благодаря своей природе получаемые «виртуальные следы» внутренне ненадежны, так как их можно неправильно считать» [57, С. 74].

Несмотря на это можно констатировать, что при расследовании преступлений, совершенных с использованием компьютерных сетей могут использоваться их следы, представляющие собой сведения о прохождении информации [58] по проводной, радио-, оптической и другим электромагнитным системам связи (электросвязи), то есть данные о состоявшихся сеансах связи или переданных сообщениях, либо «данные о потоках» или «данные о потоках информации».

К примеру, отсутствие прямого или удаленного доступа к устройствам, на которых хранятся данные, и проведение необходимых следственных действий является актуальной проблемой сотрудников правоохранительных органов при выявлении уголовных правонарушений.

Когда данные хранятся на большом сложном оборудовании, к примеру, на оборудовании крупного поставщика интернет-услуг, то доступ к ним иногда и вовсе невозможен без содействия и помощи со стороны его владельцев.

Электронные доказательства, указывающие на совершение уголовных правонарушений в сети Интернет и являющиеся основанием для проведения досудебного расследования, аккумулируются в регистрационных данных и системных журналах, находящихся в распоряжении компаний-поставщиков хостинговых услуг.

Правоохранительные органы с их ограниченными ресурсами просто не в состоянии охватить совершаемые каждую минуту в сети Интернет обмен информацией и транзакций в веб-пространстве. Не все данные в сети Интернет являются общедоступными, и для получения к ним доступа необходимы регистрационные данные. В случаях, когда для совершения преступления используются закрытые каналы связи (например, электронная почта), то, пока лицо, имеющее доступ к такому каналу, не обратится в правоохранительные органы,

у них практически нет шансов отследить эти действия или получить необходимые доказательства.

Также имеются сложности при установлении лиц, совершивших уголовные правонарушения в сети Интернет. Зачастую, все, что известно о подозреваемом, - это его IP-адрес, MAC - адрес (Адрес управления доступом к среде (Media Access Control address) - это уникальное число, которое идентифицирует устройство в сети), адрес электронной почты, доменное имя или интернет-псевдоним («ник»).

Для идентификации физического лица по IP-адресу специалисту нужны данные, которые находятся в распоряжении поставщика интернет-услуг. Поставщики интернет-услуг (электронной почты, хостинговых услуг) зачастую являются единственным источником информации, которая помогает установить связь между виртуальной личностью правонарушителя и конкретным физическим лицом.

В связи с чем, независимые владельцы данных часто оказываются ключевым звеном в расследовании.

Базы данных, которые могут использоваться в качестве электронных доказательств, принадлежат не только правоохранительным органам и государственным организациям, но и множеству частных компаний, обеспечивающих работу сети Интернет. Из-за отсутствия централизованной информации об идентификационных данных пользователей поставщикам интернет-услуг довольно сложно выработать единые стандарты обмена данными. Каждый использует свои собственные методы фиксации запрашиваемых данных, определения приоритетности запросов на предоставление данных и борьбы с правонарушителями в сети.

При необходимости, с соблюдением установленной законом процессуальной формы, они могли бы передаваться представителям органов дознания или предварительного следствия для целей, связанных с расследованием преступлений.

Наиболее распространенным способом совершаемых уголовных правонарушений в сети Интернет являются такие виды, как:

- получение частичной или полной предоплаты за товар или услугу по объявлениям, размещенным на торговых интернет-площадках (OLX, Kolesa.kz, Krisha.kz и т.д.) и в социальных сетях (Instagram, Facebook, VKontakte и т.д.);

- оформление фиктивных онлайн-займов через сайты микрокредитных организаций («Деньги-населению», «Займер», «Тенго», «Финкап», «Смарт-Финанс» и др.).

В одном случае, после обманного завладения персональными данными, преступники оформляют онлайн-кредит и получают полный доступ к управлению банковской картой и депозитами. Далее деньги через банкинг переводятся на сторонние счета, в т.ч. за рубеж.

В другом, мошенник звонит владельцу интернет-объявления и предлагает произвести продавцу оплату по его банковским реквизитам. После получения необходимых данных (Ф.И.О., ИИН, номер удостоверения личности и т.д.), которые продавец передает добровольно, на него оформляется кредит.

Зарегистрированы факты мошенничества под предлогом выгодного вложения денег в различные проекты (инвестиции, ставки, игры и т.д.). Такие преступления совершаются через группы и чаты социальных сетей и мессенджеров.

Совершаются мошеннические хищения со счетов пластиковых карт посредством создания или подключения к личному кабинету. При этом, граждане добровольно передавали мошенникам либо вводили на «фишинговых» сайтах свои персональные данные.

В большинстве случаев преступники представлялись сотрудниками служб безопасности банков и похищали деньги со счетов граждан путем подключения к мобильному банкингу с последующим переводом на счета зарубежных банков, в т.ч. российских, белорусских, украинских и др.

Справочно: почти треть (2822) оставшихся в 2020 году нераскрытыми интернет-мошенничеств совершена с территорий государств постсоветского пространства (Россия, Беларусь, Украина) [59].

Выявление уголовных дел по фактам интернет-мошенничеств также осложнено продолжительными поисковыми мероприятиями владельцев сим-карт, с которых произведен звонок и «интернет-адресов» подозреваемых.

В ходе расследования правоохранительными органами направляются запросы в компании сотовой связи, в оперативно-технические подразделения и отдельные поручения в иные регионы для установления владельцев сим-карт.

Однако, в большинстве случаев, для совершения уголовных правонарушений данной категории используются «сайты однодневки», при регистрации доменного имени вносятся вымышленные данные.

Направляются санкционированные постановления в банки второго уровня о выемке транзакции по банковским счетам, на которые потерпевшими перечисляются денежные средства.

Проблема заключается в том, что банки не дают полных ответов на постановления следователя, это создает дополнительные трудности в расследовании, а именно:

- сообщается о перечислении денежных средств на другие карты банка или счета, при этом полные номера счетов и карт не указываются;

- сообщается о перечислении денежных средств на номера телефонов сотовых компаний, однако номера и данные сотовых компании не предоставляются;

- денежные средства перечисляются на счета зарубежных банков, установить принадлежность которых невозможно.

При этом, для получения исходных данных подозреваемых затрачивается большое количество времени, за которые последние успевают поменять платежные карты, мобильные устройства, создать новые сайты и т.д.

Справочно: после получения необходимых сведений (посредством запроса, санкционированного прокурором) требуется выемка документов (договоров банковского займа, залога недвижимого имущества, кредитного досье и т.д.), содержащих банковскую тайну.

В ряде случаев возникает необходимость в получении из банков второго уровня информации о передвижении денежных средств (по одному или нескольким

банковским счетам), IP-адресах (при online-переводах), абонентских номерах (привязанных к банковским счетам), местонахождении банкоматов, через которые обналичены похищенные денежные средства, а также фото и видеоизображений с камер банкоматов.

Вместе с тем, имеются проблемы в получении санкций о выемке сведений с банков второго уровня, и вопросы взаимодействия с администрациями интернет сайтов, социальных сетей, мессенджеров (ВКонтакте, Facebook, Watsapp, Одноклассники, Инстаграмм, Mail.ru) находящимися за пределами страны, которые не имеют своих представительств на территории РК:

- Администрированием чатов в социальных сетях, через которые осуществляется сбыт, занимаются «боты», то есть фактически чаты страницы не зарегистрированы на конкретных лиц, которых можно установить (в основном в социальной сети «Телеграмм»).

- Использование прокси - серверов, не позволяют установить IP-адреса возможных создателей чатов, через которых осуществляется сбыт наркотических средств.

Также имеются проблемы при выявлении и расследовании уголовных правонарушений в сети Интернет, связанных с незаконным оборотом наркотических средств, психотропных веществ и их аналогов совершенных «бесконтактным» способом.

На это влияют следующие факторы:

- низкий уровень модерации и мониторинга в социальных сетях групп, чатов, через которые осуществляется сбыт наркотических средств, позволяет сбытчикам беспрепятственно создавать интернет-магазины для реализации наркотических средств;

- в основном, уголовные правонарушения данной категорий совершаются организованной преступной группой, в которой имеются организатор, модератор чатов, сайтов, исполнители (закладчики), фасовщики, лаборатория и т.д.

Отличительной особенностью преступлений, связанных с незаконным сбытом наркотических средств, совершаемых с использованием сети Интернет, является то, что в них нет личности потерпевшего. Объясняется это тем, что при покупке и других незаконных действиях с наркотиками лицо само нарушает соответствующие нормы права и становится преступником.

Правоохранительными органами в настоящее время устанавливаются и привлекаются к уголовной ответственности только исполнители (закладчики). Организаторы сбыта продолжают свою преступную деятельность, привлекая новых участников в виде исполнителей.

Так, в сентябре 2021 года в г.Шымкенте на видных местах были развешаны объявления предлагающие работать наркокурьером. Причем расклейщики не побоялись камер уличного наблюдения. Зарплату пообещали приличную – около 300 тыс. тенге в неделю. Номер для связи был указан иностранный и оплату обещали в иностранной валюте [60].

Установить активных участников, тем более организаторов преступной группы, составляют особую сложность из-за:

- невозможности установления организаторов сбыта, отслеживающих поступление денег на электронные кошельки, криптовалюты и руководящих преступной деятельностью наркогруппы;

- сложности в документировании преступной деятельности лиц, путем проведения НСД-1, в связи с бесконтактным способом сбыта психотропных веществ, а также изъятием денежных средств, израсходованных в ходе проведения НСД (деньги переводятся на электронные кошельки либо на криптовалюты и нет возможности их изъятия).

Указанное создаёт определенные сложности при проведении профилактики преступлений данной категории.

В деятельности правоохранительных органов возникают проблемы в процессе осуществления оперативно-розыскной деятельности и в процессе доказывания по данной категории преступлений. Отсутствие или устаревшие методы решения указанных проблем, методик противодействия преступности представляет собой растущую угрозу правовой безопасности личности, общества и государства [61, С. 272].

В ряде стран на технические службы связи и интернет-провайдеров законодательно возложена обязанность, сохранять в определенном порядке «исторические данные», которые могут быть важны для расследования преступлений. Во многих странах это запрещено, а в некоторых закон об этом умалчивает, оставляя службам связи самим решать эти проблемы в зависимости от технологических потребностей, интересов частных лиц и развития рынка, что, естественно, создает дополнительные сложности для правоохранительной деятельности в этой сфере.

Не менее важна проблема недостаточной эффективности системы международной взаимной правовой помощи для решения вопросов, связанных с киберпространством, в частности, ввиду ее медлительности.

Средний срок обработки запроса об оказании взаимной правовой помощи в связи с вопросами кибербезопасности составляет от 6 месяцев (по информации Республики Чехия средний срок среди государств - членов Совета Европы составил 21 месяц) [62].

К примеру, США сталкиваются с проблемами, стремясь удовлетворить тысячи просьб других стран об электронных доказательствах; зачастую эти проблемы возникают из-за того, что страны не понимают требований или не предоставляют достаточной информации для соблюдения правовых стандартов США. Ввиду недостаточности информации, содержащейся в просьбах об оказании взаимной правовой помощи, власти США вынуждены запрашивать разъяснения и дополнительную информацию у зарубежных партнеров, что приводит к задержкам в выполнении этих запросов.

Для решения указанных проблем необходимо:

- изменить порядок регистрации пользователей в платежной системе Киви-кошелек (Казахстан) и обязательным условием для создания кошелька определить регистрацию пользователя (для всех регистрирующихся), путем внесения личных данных, ИИН, и адреса прописки (есть сложность установления IP-адресов);

- упростить процедуры получения информации о транзакциях через Киви-кошелек, без санкционирования постановления в следственном суде, путем запроса в рамках уголовного дела.

В целях противодействия мошенничеству в банковской сфере (в т.ч. в сфере кредитования) создана межведомственная рабочая группа (МВД, Нацбанк, АРРФР) по вопросам дополнительной идентификации получателей займов, блокирования незаконных переводов, механизма оперативного взаимодействия государственных органов по пресечению и предотвращению хищений.

С АРРФР осуществляется обмен информацией о микрокредитных организациях (не соблюдающих требования по выдаче займов), способах, схемах и инструментах, используемых для совершения мошенничеств. Прорабатывается вопрос межведомственного мониторинга фиктивных финансовых операций, а также алгоритм оперативного приостановления вознаграждения, неустойки и списания задолженности по таким операциям.

Вместе с тем, существует ряд проблемных вопросов, которые требуют совместного решения и принятия дополнительных мер реагирования.

Так, в целях минимизации рисков хищения денежных средств (правовые и технические аспекты) компетентным государственным органам (АРРФР, МТ) совместно с Ассоциацией «Цифровой Казахстан» необходимо принять дополнительный комплекс мер по урегулированию интернет-торговли.

Вследствие отсутствия единой базы данных о наличии банковских счетов и движении по ним денежных средств, возникают сложности при получении сведений о наличии банковских счетов (запросы направляются во все банки второго уровня республики).

В результате чего теряется оперативность в получении подобных данных, раскрытие и расследование таких уголовных дел затягивается.

Ввиду трансграничности (с использованием сети Интернет), а также малоэффективности существующих механизмов международного обмена оперативной информацией и международными запросами такие дела остаются нераскрытыми.

Необходима проработка вопроса взаимодействия органов внутренних дел (полиции) и международного сообщества по раскрытию преступлений в сфере информационных технологий, в том числе интернет-мошенничеств.

Сходные проблемы существуют и при использовании преступниками и их жертвами зарубежных социальных сетей и мессенджеров, которые находятся вне юрисдикции РК и информация об интересующих пользователях может быть получена на основании международного следственного поручения.

На данном этапе своего развития правоприменительная практика остро нуждается в совершенствовании оперативно-розыскных, криминалистических приёмов и способов выявления и раскрытия преступлений, совершаемых посредством интернет-ресурсов [63, С. 8].

В целях создания эффективного механизма противодействия теневому обороту наркодоходов посредством «электронных кошельков» и пресечения распространения новых психоактивных веществ с использованием виртуальных платежных систем, предлагается поручить Национальному банку

РК внести изменения в Закон РК от 26 июля 2016 года «О платежах и платежных системах» в части отказа в оказании услуг не идентифицированным пользователям электронных платежных систем.

Процесс идентификации пользователей предлагается осуществлять по аналогии с процедурой прохождения регистрации в онлайн-режиме в банковских и сервисных мобильных приложениях («Kaspi», «InDriver» и др.).

Таким образом, в целях совершенствования правоприменительной практики расследования уголовных правонарушений совершаемых в сети, предлагается активизировать деятельность по ратификации Конвенции Совета Европы «О компьютерных преступлениях» («Будапештская конвенция», 2001г.). Имплементация положений Конвенции и приведение национального законодательства в соответствие с международными нормами позволит расширить сферы взаимодействия правоохранительных органов Казахстана с зарубежными коллегами по раскрытию уголовных правонарушений, совершаемых в сети Интернет.

Результаты проведенного социологического опроса показали следующее.

59% респондентов ответили, что, в основном используют Интернет в целях ознакомления с новостями, 19% для использования видео порталов (YouTube, ТикТок, Likee и т.д.), мессенджеров (ватсап, соц.сети, фейсбук, вконтакте и др.), для электронных платежных систем (Webmoney, Яндекс.Деньги, PayPal, онлайн покупки и др.), 4% для использования систем файлообменов BitTorrent (Rutracker.ru, Torrent.ru и т.д.).

На основании полученных данных:

1. Определен уровень осведомленности населения об угрозах информационной безопасности. Так, только 22% опрошенных дали положительный ответ, что позволяет делать вывод о необходимости усиления государством политики информирования граждан и использовать для этого наиболее эффективные методы и способы, которые были бы более удобные для респондентов.

2. Составлен социально-психологический портрет и выявлены особенности психологии поведения жертвы. 39% участников подвергались преступлениям, совершаемым посредством сети Интернет, не подвергались 37%, остальной процент респондентов впервые слышат об этом или не знают вообще.

При этом большинство опрошенных являются жителями областных, районных центров, городов, использующие Интернет для ознакомления с новостями, а новостные каналы периодически освещают факты правонарушений, совершаемых с использованием сетей телекоммуникаций.

45% затруднялись с ответом по какой причине они стали жертвой интернет-преступности, 33% затруднились с ответом. Просьбы, угрозы и требования со стороны преступников оказались в меньшинстве.

По мнению опрошенных, желающие получить легкие деньги (48%) и доверчивые люди (36%) чаще всего подвергаются интернет-мошенничеству.

Из числа подвергшихся интернет-преступности людей 63% смогли вовремя понять и отреагировать на действия злоумышленников. Однако 37%

все же доверяются и оказываются жертвами преступности. 75% никаких потерь не понесли, а остальные затруднились с ответом.

3. Из ответов лиц, подвергшихся интернет-мошенничеству следует, что большинство мошенников устанавливают контакт с жертвой обращаясь к ней лично, но сами не представившись. В остальных случаях обращаются лично, называя имена (своё или жертвы).

Для привлечения потенциальных жертв преступники чаще всего пользуются такими методами как приглашение на сайты с тематиками, которые могут заинтересовать их (47%) или такими способами как взлом сайтов и мессенджеров (24%). 15% атаками вредоносных вирусов (спам), 14% звонками и сообщения на телефоны. Преступники чаще обращаются с предложениями, чтобы заинтересовать потенциальную жертву (33%).

4. Около половины (47%) всех ответивших подвергались интернет-мошенничеству, вдвое меньшее (18%) неправомерному доступу к информации, практически одинаковое количество столкнулись с вредоносными программами (14%) и (13%) бесконтактной торговлей наркотиками и распространением порнографии. Еще 7% сталкивались с неправомерным завладением информацией.

Относительно видов интернет-мошенничества самой распространенной и более чаще встречающейся оказалась кража пароля от учетной записи пользователя (10%), по 8% спам и SMS-оплата.

С такими видами, как фальшивые извещения о выигрыше в лотерее, фишинг мошенничеством в виде рекламы товаров и услуг, попрошайничество, тайпсквоттингом, имитаторы вирусов и антивирусов, взлом сайтов, мошенничество с платежными системами знакомы, но не сталкивались.

В связи с пандемией и развитием интернет-пространства, в сети распространяется такой вид преступности, как предложения работы по распространению запрещенных наркотических препаратов и психотропных веществ. 91% опрошенных не сталкивались с подобным предложением, 6% респондируемых отказались, испугавшись подозрительного предложения и 3% подумали, что это розыгрыш.

5. Одним из проблемных вопросов является латентность уголовных правонарушений, совершенных в сети Интернет. Эту же картину можно видеть и по результатам опроса.

Так, 91% респондентов не обращались в правоохранительные или уполномоченные органы, а остальные не хотят иметь дело с правоохранительными органами.

Вместе с тем, многие (45%) считают, что проблема роста интернет-преступности заключаются в ненадлежащем противодействии соответствующих органов, а все больше мошенников владеют IT-технологиями (39%). И только 10% считают, что виноват сам пользователь.

Также 87% опрошенных не известны факты привлечения к ответственности интернет-преступников, и только в 13% случаев опрошенные осведомлены о подобных фактах.

6. По мнению 75% опрошенных, более эффективными действиями правоохранительных органов является привлечение специалистов и экспертов в области IT-технологий, фиксация всех значимых, по мнению жертвы, обстоятельств преступления (13%) и повышение эффективности сотрудничества с другими органами (12%).

Наиболее эффективными мерами со стороны государства для предупреждения интернет-преступности могут стать всплывающие информационные (рекламные) окна в сети Интернет (38%) и посвящение специальной рубрики в программе новостей (32%).

Возможно, есть необходимость обратить внимание государства на этот вопрос и рассмотреть способы использования рекламных окон для повышения осведомленности граждан об интернет-преступлениях и понижения уровня интернет-преступности.

Уровень осведомленности населения об угрозах информационной безопасности низкий, что позволяет сделать вывод о необходимости усиления государством политики в части осведомления граждан и использовать для этого наиболее эффективные методы и способы, которые были бы более удобными для граждан.

Для предупреждения интернет-преступности и повышения уровня осведомленности уполномоченным органам необходимо рассмотреть вопрос о возможности размещения соответствующей информации в сети Интернет и посвящение специальной рубрики в программе новостей. Информационные окна возможно будут полезны для любого пользователя сети.

Анализируя ответы респондентов, можно сделать вывод о том, что 33% лиц, даже будучи осведомленными о рассматриваемых угрозах, проявили неосторожность и не перепроверили информацию (предложение), которую представил им злоумышленник.

Тем самым, подтверждается гипотеза о том, что преступник тщательно изучает данные (соц.сети, подписки, круг интересов, друзей и т.д.) о жертве, прежде чем обращаться лично с каким-либо предложением или просьбой, хорошо разбирается в психологии поведения.

Около 50% всех жертв, которые подверглись интернет-мошенничеству, вступали в контакт с преступниками через сообщения или по телефону.

Те же участники, которые не подвергались преступным посягательствам, не знают о них, если даже сталкивались или становились жертвой, не включают себя в категорию жертвы.

Обращения в уполномоченные и правоохранительные органы заканчивались лишь получением рекомендаций по безопасному использованию сети Интернет. В итоге, это, приводит к высокому уровню латентности, так как 91% пострадавших не обращались в указанные органы.

Однако, имеется категория лиц, которые не прочь заработать легкие деньги, что может быть связано с поведением самого человека (жадность, алчность, азарт) либо его низкой социальной обеспеченностью.

Возможно, некоторые из участников опроса или их знакомые, близкие сталкивались с такими видами преступности, как утечка персональных данных.

В связи с чем, не доверяют сотрудникам государственных органов и сомневаются в их честности или возможности оказать реальную помощь.

Для решения указанных проблем необходимо следующее:

- упростить процедуры получения сведений о транзакциях через Киви-кошелек, без санкционирования постановления в следственном суде, а по запросам в рамках уголовного дела;

- принять дополнительный комплекс мер по урегулированию интернет-торговли для минимизации рисков хищения денежных средств (правовые и технические аспекты) компетентным государственным органам (АРРФР, МТ) совместно с Ассоциацией «Цифровой Казахстан»;

- внести изменения в Закон РК «О платежах и платежных системах» в части отказа в предоставлении услуг не идентифицированным пользователям электронных платежных систем для создания эффективного механизма противодействия теневому обороту наркодоходов посредством «электронных кошельков» и пресечения распространения новых психоактивных веществ с использованием виртуальных платежных систем;

- активизировать деятельность по ратификации Конвенции Совета Европы «О компьютерных преступлениях» («Будапештская конвенция», 2001г.), для улучшения взаимодействия органов внутренних дел (полиции) с международным сообществом по раскрытию преступлений в сфере информационных технологий, в том числе интернет-мошенничеств.

2.3 Вопросы производства следственных действий по уголовным правонарушениям, совершенным в сети Интернет

Уголовные правонарушения в области информатизации и связи являются одним из активно прогрессирующих видов виртуальной преступности в условиях нашего социума и массового распространения устройств (гаджетов), облегчающих жизнь человека.

Сегодня с помощью любых персональных устройств (компьютеров, гаджетов) и различного рода программ для обработки информационных данных совершаются преступные посягательства на личные данные граждан РК, охраняемые Законом РК «О персональных данных и их защите» [64], основанные на Конституции РК.

Актуальностью темы монографии, является то, что уголовные правонарушения, совершаемые в сети Интернет несут в себе реальную опасность, поскольку их несвоевременное пресечение приводит к появлению у правонарушителя чувства безнаказанности в интернет-среде и дает возможность оттачивать свои навыки «хакерства», далее в будущем способствующие совершению более тяжких преступлений.

Отметим, что процесс по раскрытию и расследованию правонарушений реализуется в рамках факторов объективной действительности, в настоящем времени, места, взаимодействия субъектов с различным процессуальным статусом. При подготовке отдельных методик расследования правонарушений первостепенным является использование ситуационного подхода.

Некоторые положения касательно характеристики ситуаций, попадающих в орбиту изучения криминалистики, исследовались в трудах ученых криминалистов Видонова Л.Г., Селиванова Н.А., Лузгина И.М., Яблокова Н.П., Каневского Л.Л., Облакова А.Ф. и других.

Профессор Волчецкая Т.С. впервые в криминалистической ситуалогии определила следственную ситуацию как «степень информационной осведомленности следователя о правонарушении, а также состояние процесса расследования, сложившееся на любой определенный момент времени, анализ и оценка которого позволяют следователю принять наиболее целесообразные по делу решения» [65, С. 134].

Основным видом изложения тактики первоначальных следственных действий является описание типизации следственных ситуаций. Тем не менее, наряду с общими научными взглядами по вопросам понятия методики расследования правонарушений, рассматриваемые при построении тактики первоначальных следственных действий, в юридической науке нет единого понятия «типичная» и «типовая», сопоставительно к характеристике следственных ситуаций, которая приводит к разночтению данных понятий.

Ушаков Д.Н. в своем Толковом словаре русского языка, слово «типовой» трактует как «являющийся образцом, типом, стандартом для ряда явлений, случаев; типовой договор; типовая модель». Термин «типичный» определяет как «наделенный характерными особенностями, свойственными какому-нибудь типу, легко подводимый под тип; типичная ошибка невежды» [66].

Подобное объяснение вышеуказанных толкований имеется и в других словарях.

Согласно определениям понятий типичных и типовых следственных ситуаций, склоняемся к термину «типичный», как соответствующий определенному типу и индивидуализирующий ситуацию.

Хотя Волчецкая Т.С. отметила, что «в информационной структуре типичной ситуации преобладают общие, часто повторяющиеся черты, в отличие от типовой ситуации» [65, С. 160].

Рассмотрим вопросы расследования и производства типичных следственных ситуаций по уголовным правонарушениям, совершаемым в сети Интернет, путем обмана или злоупотребления доверием пользователя информационной системы (ст.190 ч.2 п.4 УК РК) (далее - интернет - мошенничество).

Необходимо отметить, что данные монографии могут быть использованы и в иных следственных ситуациях, таких как:

- установление лиц, причастных к незаконному обороту наркотических средств;

- установление сбытчиков похищенного (при продаже в интернет - сервисах «OLX», «kolesa.kz» и т.д.);

- установление лиц, причастных к пропаганде терроризма или публичным призывам к совершению акта терроризма;

- установление лиц, причастных к разжиганию социальной, национальной, родовой, расовой, сословной или религиозной розни;

- розыск преступников и без вести пропавших лиц.

Типичные следственные ситуации и первоначальные следственные действия для закрепления доказательств при расследовании интернет-мошенничества.

Ситуация первая. Интернет - мошенничество через сайты объявлений. Интернет мошенник – продавец.

Интернет-мошенник размещает на сайтах объявлений («OLX», «krisha.kz», «kolesa.kz» и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг, за которые в последующем получает предоплату, тем самым похищая деньги.

В данной ситуации следователю первоначально необходимо допросить потерпевшего и свидетелей, для установления криминалистически значимой информации, которая в дальнейшем даст возможность планировать процесс расследование интернет - мошенничества.

В этой связи необходимо установить:

- абонентский номер интернет-мошенника, по которому связывался с потерпевшим и свидетелем.

- какую услугу предлагал интернет-мошенник, и на каких сайтах размещал объявления.

- сведения по банковской карте или электронному кошельку интернет-мошенника, по которому были переведены денежные средства.

Затем, следователю необходимо составить отдельное поручение на проведение оперативно-розыскных мероприятий (далее - ОРМ), в соответствии с которым оперативным подразделениям необходимо провести следующие ОРМ:

- *по абонентскому номеру:*1) установить и допросить владельца абонентского номера и продавца Sim-карты; 2) провести анализ детализации звонков и расположения базовых станций; 3) установить лиц, ранее судимых и проживающих в данном секторе.

- *по информациям о сайтах разместившие объявления:*1) установить электронную почту, указанные при регистрации на сайтах объявлений; 2) установить IP-адрес устройства (гаджета), с которого было подано объявление; 3) провести анализ дополнительных объявлений, установленных при помощи Cookie.

- *по банковской карте или электронному кошельку интернет-мошенника, по которому были переведены денежные средства:*1) провести анализ передвижения денежных средств; 2) в случае снятия денежных средств, запросить видео с камеры банкомата; 3) в случае покупки в интернет магазинах, запросить данные по оплате банковской картой или услугой «мобильного банкинга».

Далее, в зависимости от сложившейся следственной ситуации следователь определяет перечень следственных действий, необходимых для качественного закрепления и фиксации доказательств.

Ситуация вторая. Интернет-мошенничество через сайты объявлений. Интернет-мошенник – покупатель.

Интернет-мошенник звонит по объявлению потерпевшего, размещенному на сайте («OLX», «krisha.kz», «kolesa.kz» и т.д.) и говорит, что желает приобрести его товар и готов внести задаток, для чего просит продиктовать контрольные данные по банковской карте и поступивший код. Получив данные сведения, осуществляет перевод через онлайн сервисы или совершая покупку. Или же интернет-мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банкинг, и в последующем похищая денежные средства.

В данной ситуации, при допросе потерпевшего и свидетелей, следователю необходимо установить:

1. абонентский номер интернет – мошенника;

2. информацию по объявлению интернет-мошенника, размещенную на сайтах;

3. банковские карты или электронные кошельки интернет-мошенника, по которому были переведены денежные средства.

Затем следователем выносится отдельное поручение оперативным подразделениям на проведение ОРМ по вышеуказанному алгоритму и определяются следственные действия необходимые для качественного закрепления доказательств.

Ситуация третья. Интернет - мошенничество со взломом страниц социальных сетей.

Интернет-мошенник покупает в сети Интернет взлом страницы социальной сети (Vk.com, ok.ru, drugvokrug.ru и др.) или осуществляет его

самостоятельно. В последующем пишет всем друзьям из списка сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.).

При допросе потерпевшего и свидетелей следователю необходимо установить:

1. период взлома и переписки в социальной странице потерпевшего;

2. банковские карты или электронные кошельки интернет-мошенника, по которому были переведены денежные средства.

Ситуация четвертая. Интернет - мошенничество, совершенное с использованием интернет сайтов (интернет-магазинов).

Интернет-мошенник создает либо покупает интернет-сайт по продаже товара различной тематики. Регистрирует несколько виртуальных номеров (8-800-…) у SIP-провайдера и указывает их на сайте в качестве контактов. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта.

При допросе потерпевшего и свидетелей следователю необходимо установить:

1. услуги SIP-провайдера по виртуальному номеру интернет – мошенника;

2. доменное имя, и хостинг арендованного сайта;

3. организацию арендодателей хостинга.

Ситуация пятая. Интернет - мошенничество, совершенное под предлогом заказа банкета (или связь с курьером).

Интернет-мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу банкета, заказу крупной партии товара или прочих услуг. Далее он сообщает адрес, где бы он хотел встретиться с представителем компании и спрашивает его телефон. В последующем он связывается с представителем и просит последнего по пути пополнить счет абонентского номера (или банковской карты) на неопределенную сумму, которую он отдаст при встрече.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить:

1. абонентский номер интернет–мошенника;

2. банковские карты или электронные кошельки интернет-мошенника, по которому были переведены денежные средства.

Ситуация шестая. Интернет-мошенничество, совершенное под предлогом разблокировки банковской карты или предотвращения списания денежных средств.

Интернет-мошенник осуществляет рассылку SMS-сообщений с текстом о списании денежных средств или блокировке банковской карты. В данном сообщении указывает другой абонентский номер (иногда виртуальный 8-800-…), который может проинформировать о произошедшем. Потерпевший звонит по данному номеру, после чего интернет-мошенник просит сообщить контрольные данные банковской карты.

При допросе потерпевшего и свидетелей следователю необходимо установить:

1. абонентский номер интернет – мошенника;

2. банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства;

3. услуги SIP-провайдера по виртуальному номеру интернет - мошенника.

Ситуация седьмая. Интернет-мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду.

На стационарный или абонентский номер потерпевшего звонит интернет-мошенник, который обращается под видом родственника (привет мама, привет бабушка и т.д.). Сообщает, что попал в ДТП или сбил человека, либо с кем-то подрался и т.д., а после передает трубку сотруднику полиции, который за отдельную плату предлагает решить вопрос об отказе в составлении протокола или регистрации уголовного дела.

Аналогично при допросе потерпевшего и свидетелей следователю необходимо установить:

1. абонентский номер интернет–мошенника;

2. банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Ситуация восьмая. Интернет-мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы.

На стационарный или абонентский номер потерпевшего звонит интернет-мошенник, который, представляется сотрудником правоохранительных органов. Сообщает, о задержании группы мошенников, продававших некачественные БАДы, и о необходимости оплаты государственной пошлины или налогового сбора для получения компенсации.

При допросе потерпевшего и свидетелей следователю необходимо установить:

1. абонентский номер интернет–мошенника;

2. банковские карты или электронные кошельки интернет-мошенника, по которому были переведены денежные средства.

Ситуация девятая. Интернет-мошенничество, совершенное с использованием вредоносных программ на ОС «Android».

Потерпевшему на сотовый телефон с операционной системой «Android» с неизвестного номера приходят SMS-сообщения с текстом: «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка: https://www.olx.kz/FriZksk)», или SMS-сообщение с текстом: «Смотри, как мы здорово получились на этой фотографии. Ссылка www. URL/ZreizE1eaAa». Потерпевший проходит по данной ссылке, в результате чего загружает на свой телефон вирус (чаще всего используются вирусы под названием «Triada», «Marcher», «Loki», «Faketoken»), предоставляющий злоумышленнику доступ к SMS-командам. В дальнейшем интернет мошенник похищает деньги, путем направления сообщений на номер «800».

Аналогично при допросе потерпевшего и свидетелей следователю необходимо установить:

1. абонентский номер интернет–мошенника;

2. банковские карты или электронные кошельки интернет- мошенника, по которому были переведены денежные средства.

Ситуация десятая. Интернет-мошенничество, совершенное с использованием социальных сетей (интернет-магазин «Instagram»).

Интернет-мошенник создает страницу или группу в социальной сети, позиционирующую себя как интернет-магазин. В последующем принимает покупателей, получая от них денежные средства за покупку товара с сайта.

В данной ситуации при допросе потерпевшего и свидетелей следователю необходимо установить:

1. название сайта или интернет-магазина;

2. банковские карты или электронные кошельки интернет - мошенника, по которому были переведены денежные средства.

Организация производства отдельных следственных действий при расследовании интернет-мошенничества.

Основными следственными действиями, необходимыми при расследовании интернет-мошенничества, совершенные в сети Интернет являются:

- осмотр (места происшествия, предметов и документов);
- обыск (в жилище, в ином помещении, личный);
- выемка (предметов - электронных носителей информации, электронной почтовой корреспонденции);
- допрос (обвиняемого, подозреваемого, потерпевшего, свидетеля, эксперта, специалиста);
- негласные следственные действия;
- далее по обстоятельствам.

Организация осмотра (места происшествия, предметов и документов).

Особое значение осмотра места происшествия как первоначального следственного действия, заключается в том, что это самое близкое во времени и в пространстве соприкосновение следователя с событием преступления [67].

Сущность рассматриваемого следственного действия заключается в непосредственном исследовании следователем (дознавателем) и другими участниками осмотра обстоятельства места происшествия (таблица 4), в условиях которого выявляются, изучаются, фиксируются и изымаются в установленном законом порядке материальные объекты и следы, с целью получения сведений, имеющие значение для раскрытия и расследования уголовного дела, а также событий, содержащих признаки преступления.

Осмотр (места происшествия, предметов и документов) при расследовании интернет-мошенничества позволяет установить ряд важных обстоятельств	Целью осмотра (места происшествия, предметов и документов) при расследовании интернет-мошенничества являются
имеются ли на месте осмотра следы события, подлежащего расследованию	поиск средств мобильной связи
если да, то содержит ли событие признаки хищения	поиск специальных технических средств, для негласного получения информации с технических средств

кто принимал участие и какую функцию выполнял при подготовке, совершении и сокрытии хищении	поиск вредоносных программ на компьютерных носителях информации
какие носители информации, содержащие следы события, подлежащего фиксацию и изъятию, имеются на месте происшествия	поиск электронных записей, находящихся в памяти компьютера или иного аппаратного средства, содержащих криминалистический значимые сведения
какие технические средства, компьютерные программы и документы использовались для доступа к предмету посягательства и совершения незаконных действий с ним	поиск имен, адреса, телефоны, сетевые псевдонимы, сетевые адреса, даты, PIN-коды, реквизиты доступа к электронным счетам, названия вредоносных компьютерных программ и других идентификационно-справочных информации
кто мог стать очевидцем подготовки, совершения или сокрытия хищения и т.п.	поиск методических рекомендаций и цифровых видеофильмов, раскрывающих способ преступления

Таблица 4 Фиксация и изъятие материальных объектов и следов

Специфика осмотра предметов (документов) при расследовании интернет-мошенничеств заключается в том, что осмотру подлежат, как правило, не только файлы, содержащие текстовые или графические документы, подготовленные пользователем, но и служебные журналы системных и прикладных программ, применяемых для осуществления транзакций. Это предполагает использование в ходе осмотра современных экспертных аппаратно-программных комплексов (например, BELKASOFT) [68], оснащенных необходимым экспертным программным обеспечением, позволяющих быстро находить требуемые файлы и интерпретировать их содержимое.

При осмотре места происшествия могут находиться такие носители информации как накопитель на жёстких магнитных дисках (винчестер), флэш-карты памяти в разнообразном исполнении. Целесообразно указывать факт их наличия в протоколе осмотра с указанием следующих данных:

- место нахождения носителя информации;
- его идентифицирующие типы;
- индивидуализирующее название;
- маркировочные обозначения, серийные номера.

Также, на месте происшествия, кроме персонального компьютера, могут находиться мобильные телефоны (таблица 5), на носителях которых могут остаться следы события преступления. Такая техника описывается в протоколе осмотра с указанием сведений, аналогичных сведениям, приводимым при обнаружении носителей информации.

Рекомендации по осмотру обнаруженного и (или) изъятого средства сотовой связи (мобильного устройства)		
первый этап внешний осмотр	второй этап конструктивный осмотр	третий этап осмотр информационной среды
наружное строение и состояние мобильного устройства	идентификационный номер, объем, цвет и родовой материал корпуса флэш-карты Micro-SD	записная книжка
марка, модель, тип, форма аппарата, цвет корпуса, размер	идентификационный номер, объем, цвет и родовой материал корпуса SIM-карты	входящие и исходящие звонки и SMS-сообщения GSM связи
наличие объективов тыльной и (или) лицевой фото/видеокамеры	логотип оператора сотовой связи SIM-карты	входящие и исходящие звонки и SMS-сообщения WhatsApp и Viber связи

(вспышки)		(чаты)
фирменное наименование, логотип		Email, Gmail, голосовая почта
разъем Mini(Micro)USB, зарядное устройство, стереонаушники		фото-, видеофайлы
повреждения (сколы, царапины, потертости)		текстовый процессор Word, PDF файлы
отсутствие должных элементов		диктофонные записи
наличие дополнительных атрибутов (чехол, брелок, гарнитуры, полимерные наклейки, надписи, инкрустации драгоценными металлами)		органайзер

Таблица 5 Техника, описываемая в протоколе ОМП

Если в ходе осмотра следователю удалось включить мобильный телефон и получить доступ к сведениям, которые в нем находятся, в протоколе осмотра в хронологическом порядке фиксируются все производимые в дальнейшем действия с устройством.

Нередко возникают ситуации, в которых в ходе производства первоначальных следственных действий изымается сразу несколько мобильных устройств во включенном состоянии. Выключать их в таких случаях до осмотра нецелесообразно (отключение может произойти при извлечении SIM-карты), т.к. при последующем включении потребуются коды блокировки (PIN-код), которые могут быть известны только его последнему пользователю (подозреваемому, свидетелю или потерпевшему).

Отказ вышеуказанных в предоставлении информации по разблокировке телефона может исключить возможность оперативного полноценного исследования его информационного содержимого (записной книжки, входящих, исходящих звонков, SMS-сообщений GSM, WhatsApp и Viber связи, E-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера). Поэтому важно отметить, что если к моменту осмотра мобильное устройство было включено, то конструктивный осмотр следует проводить только после изучения его информационной среды.

Осмотр информационной среды необходимо начать с указания в протоколе осмотра процедуры разблокировки клавиатуры мобильного устройства, перечисления графических и текстовых элементов, которые отобразились на его экране после разблокировки. Затем осуществляется проверка IMEI-номера мобильного устройства нажатием комбинации клавиш *#06# (15-ти значный номер должен отобразиться на экране телефона).

Если мобильное устройство не защищено паролем, то в протоколе осмотра последовательно указывается информационное содержимое (список контактов, сообщений, наличие изображений, фотографий, видеороликов и т.д.) (таблица 6).

Рекомендации описательной части протокола осмотра информационной среды обнаруженного и (или) изъятого средства сотовой связи (мобильного устройства)
- при описании определенного контакта указывается его вид звонков (входящий, исходящий, непринятый), время, длительность, данные абонента, с которым осуществлен контакт, а также его абонентский номер

- при описании SMS-сообщений исключается указание длительности, но включает текстовое содержание SMS-сообщений (GSM, WhatsApp и Viber связи)
- при описании графических изображений, фотографий, необходимо указывать того, что или кто изображен, тип, размер, время создания файла
- при описании видеофайлов, необходимо указывать того, что или кто изображен, тип, размер, время создания файла и их длительность

Таблица 6 Информация, описываемая в протоколе осмотра незащищённого паролем мобильное устройство

В настоящее время сотрудники правоохранительных органов обеспечиваются специальной высокотехнологичной криминалистической техникой, позволяющей извлекать полную информацию (включая онлайн) из мобильных устройств, а также электронных накопителей (карт памяти, SIM-карт и др.) в ходе досудебного расследования. Например: универсальное устройство извлечения судебной информации (UFED - Universal Forensic Extraction Device, мобильный криминалист МК Enterprise, XRY, MOBILedit и др.).

При этом, данная криминалистическая техника позволяет работать почти с любой моделью мобильных устройств, планшетов, навигаторами и персональными компьютерами, в том числе с поврежденными устройствами, на основе любой операционной системы, а также позволяет войти в операционную систему в обход системы распознавания паролей и логинов, работать с мобильными устройствами без аккумулятора, либо отдельно с SIM-картой.

Поэтому, если доступ к информационной среде мобильного телефона затруднен, то для участия к осмотру необходимо привлечь специалиста (ч.6 ст.220 УПК РК), имеющего навыки пользования данными устройствами.

Выявление, изучение, фиксация и изъятие в установленном порядке цифровых объектов, следы и информация из мобильного устройства позволяют:

- напрямую изобличать лицо в совершении преступления (интернет мошенничества);

- косвенно указывать на линию поведения лица, возможную причастность его к совершенному преступлению (интернет-мошенничество);

- способствовать установлению иных обстоятельств, имеющих значение для уголовного дела.

На заключительном этапе осмотра информационной среды мобильного устройства проводится поэтапная детальная фотосъемка экрана мобильного телефона с информацией, представляющей значение для уголовного дела. Для визуальной фиксации большого объема сведений, содержащихся в информационной среде, следует применять видеосъемку.

При этом, следователь в обязательном порядке комментирует с одновременной фиксацией в протоколе осмотра все действия, направленные на получение той или иной информации с помощью соответствующих манипуляций.

Тактика и технология обыска (в жилище, в ином помещении)

Наличие достаточных следственно-оперативных данных о том, что в каком-либо месте или у какого-либо лица могут находиться орудия

преступления, предметы, документы, которые могут иметь значение для уголовного дела, является основанием для проведения обыска (ст.252 УПК РК). В качестве разыскиваемых в ходе обыска орудий преступления, предметов, относящихся к интернет-мошенничеству, является средства мобильной связи, электронные носители информации и иные носители информации, содержащие следы события, подлежащего расследованию.

При производстве обыска следует иметь ввиду, что современные носители информации могут быть интегрированы в различные предметы (флэшки, наручные часы, кулон, телевизоры OLED и т.п.). Поэтому, обыск целесообразно проводить с применением соответствующих технических средств (приборов нелинейной локации), позволяющих обнаружить мобильные устройства и электронные накопители в помещениях, автотранспорте, в том числе при досмотре людей или личном обыске.

Индивидуальная тактика обыска избирается следователем в зависимости от характера и способа совершенного интернет - мошенничества, условий следственной ситуации. При этом, следователю рекомендуется обращать внимание на место нахождения и возможного сокрытия цифровых устройств и в особенности извлекаемых из них накопителей (например, флэш и SIM-карты), а также на поведение участников обысков, пытающихся противодействовать расследованию или уничтожить улики с помощью магнита и т.д. Если в ходе обыска были предприняты попытки уничтожить или утаить мобильные устройства (уничтожить информацию, хранящуюся в их карте памяти), то об этом в протоколе делается соответствующая запись, и указываются принятые меры.

Выемка предметов - электронных носителей информации, электронной почтовой корреспонденции.

Выемка производится в тех случаях, когда следователь располагает точной информацией о том, что нужные ему предметы, документы находятся в определенном месте (ст.253 УПК РК). Проведение выемки необходимо в целях изъятия цифровых носителей, содержащих файлы с искомым текстовым и графическим содержимым, а также программ, используемых для подготовки и совершения преступлений рассматриваемой категории. Такие носители информации чаще всего находятся в персональных компьютерах, гаджетах лиц, подозреваемых в совершении преступления (таблица 7).

Целенаправленное и полное изъятие «традиционных» документов на бумажном носителе осуществить достаточно сложно, поэтому следователь может лишь определить состав и объем изымаемых документов. На практике достаточно часто бывают случаи, когда в ходе выемки изымается большой объем документов. Однако, в дальнейшем, следователь понимает, что многие документы не содержат информацию, относящуюся к событию преступления.

Поэтому, перед выемкой очень важно получить консультацию специалистов, компетентных в финансовых операциях, осуществляемых с помощью электронных платежных систем, а также в современных компьютерных технологиях, чтобы определить, какие документы необходимо изъять. Такая консультация позволит существенно повысить эффективность данного следственного действия, исключить выемку ненужных документов и, в

то же время, изъять документы, действительно содержащие доказательственную информацию по уголовному делу.

Рекомендации по выемке электронной почтовой корреспонденции Email, Gmail, голосовой почты и т.д.		
во-первых	во-вторых	в-третьих
- необходимо указать, у какой почтовой службы производится выемка	- в ходе выемки изымаются файлы, не содержащие в явном виде тексты писем и вложения к ним	- выемке электронной корреспонденции всегда сопутствует последующий осмотр предметов (документов) с участием специалиста
- данные из каких ящиков электронной почты подлежат выемке	- выемка является лишь носителем информации с записанными на нем базами электронной корреспонденции	- применяются программные обеспечения для преобразования баз электронной корреспонденции
- какая именно электронная корреспонденция подлежит выемке (входящие, исходящие, иные электронные письма)		- преобразуются электронные письма и вложения в формат баз почтовой программы, позволяющий осмотреть непосредственно содержимое писем и вложений, задокументировать содержимое на бумаге, для предъявления участникам следственного действия

Таблица 7 Выемка цифровых носителей

Отметим, что бывают случаи, когда выемка подменяется истребованием необходимых документов, приводящие к тому, что заинтересованные лица получат возможность скрыть или частично уничтожить искомые документы, либо заменить их другими. Поэтому подмена выемки истребованием документов крайне нежелательна.

Если при производстве выемки в известном следователю месте необходимых документов не оказалось, то действия по их обнаружению в других местах на основании того же постановления будут незаконными, а собранные таким образом доказательства недопустимыми. В этом случае необходимо немедленно вынести постановление о производстве обыска и произвести его для обнаружения скрываемых документов, причем выемка не является частью обыска, а представляет собой самостоятельное следственное действие, по результатам которого составляется отдельный протокол, подробно отражающий ее ход и результаты.

При проведении выемки и обысков по делам об интернет-мошенничестве, существенные сложности возникают при изъятии персональных компьютеров в кредитной или иной организации. Поэтому, при подготовке к проведению выемки, в ходе которых следователь намерен изъять персональные компьютеры, необходимо предварительно установить помещение, в котором находится нужный персональный компьютер, а также получить сведения о его подключении к локальной сети или сети Интернет. Если персональный компьютер подключен к сети Интернет и в режиме онлайн, то следует учитывать возможность срабатывания аппаратных или программных средств

уничтожения информации на его носителях при отключении от сети Интернет (таблица 8).

Поэтому все действия по корректному отсоединению от сети и выключению средств компьютерного устройства должны осуществляться специалистами, участвующими в следственном действии.

Рекомендации по выемке электронных носителей информации	
- недопустимо выемки неопределенных предметов, т.е. нельзя выносить постановление о выемке «электронных носителей информации» без их конкретизации	- для изъятия цифровой информации в ходе выемки следователю необходимо вынести постановление о выемке конкретных электронных носителей информации или цифровых устройств
- недопустимо выносить постановление о выемке «файлов»: так как это понятие не является предметом с точки зрения закона	- при изъятии носителей цифровой информации (цифровых следов), необходимо упаковывать и опечатывать таким образом, чтобы обеспечить сохранность имеющейся в цифровой памяти информации
- не рекомендуется привлекать специалистов (самоучек) в области IT-технологии	- все порты, слоты, входы и выходы цифровых устройств опечатываются

Таблица 8 Выемка цифровых носителей в режиме онлайн

С современными возможностями онлайн доступа к памяти цифровых мобильных устройств и находящихся в них электронных накопителей с целью уничтожения собственниками устройств через операторов связи информации, рекомендуется сразу же при обнаружении такого устройства поместить его в специальный чехол (например, «Мешок Фарадея», поставляемый в комплекте с универсальным устройством извлечения судебной информации UFED - Universal Forensic Extraction Device) [69].

В протоколе выемки следователю необходимо указать, в каком месте и при каких обстоятельствах были обнаружены цифровые устройства, выданы они добровольно или изъяты принудительно. Все изымаемые цифровые устройства должны быть перечислены с точным указанием их количества, индивидуальных признаков, в том числе модели, серийных номеров, а в необходимых случаях стоимости. Также соответствующая запись делается в случаях, если по ходатайству законного владельца изымаемых электронных носителей информации с разрешения следователя осуществляется копирование цифровой информации.

***Тактика допроса** (обвиняемого, подозреваемого, потерпевшего, свидетеля, специалиста, эксперта).*

Допрос – это следственное действие, заключающееся в получении и фиксации в установленном законом порядке показаний свидетелей, потерпевших, подозреваемых, обвиняемых и экспертов об известных им фактах, значимых для расследуемого уголовного дела [70, С. 135] (ст.208 УПК РК) (таблица 9).

Прежде чем допрашивать подозреваемого, при расследовании интернет мошенничества следователю необходимо консультация специалиста в области IT-технологии (перед началом следственного действия), либо предусмотреть его непосредственное участие.

Цель привлечения специалиста в области IT – технологий при допросе (обвиняемого, подозреваемого, потерпевшего, свидетеля)	Цель допроса специалиста в области IT – технологий
- подготовка следователя к допросу включает подготовку опросного листа	- разъяснения следователю вопросов, связанных с техническими, организационными, правовыми аспектами IT-технологий, используемых при совершении интернет-мошенничества
- допрос обвиняемого, подозреваемого, потерпевшего, свидетеля сопровождается употреблением этими лицами большого количества терминов в области IT – технологий	- особенностей функционирования локальной сети при совершении интернет-мошенничества
- наличие специфичных в техническом аспекте способы интернет мошенничества, элементы которых с большой вероятностью могут обсуждаться в ходе допроса	- особенностей подключения к сети Интернет при совершении интернет-мошенничества

Таблица 9 Привлечение специалиста при допросе

Допрос эксперта производится, как правило, для разъяснения данного им заключения. В этом случае, функция допроса заключается не только в раскрытии существенных деталей, не отраженных в выводах эксперта или исследовательской части экспертного заключения, но и в транскрипции написанного понятным всем участникам уголовного процесса языком.

Одним из тактических приемов допроса, используемых при расследовании многоэпизодных интернет-мошенничеств, совершенных организованным преступным сообществом, является процессуальное соглашение.

Как следует из п.37 ст.3 УПК РК «процессуальное соглашение – соглашение, заключаемое между прокурором и подозреваемым, обвиняемым или подсудимым на любой стадии уголовного процесса или осужденным в порядке и по основаниям предусмотренным настоящим Кодексом».

Данное процессуальное действие как тактический прием применяется прокурором, для получения развернутых показаний от одного из соучастников организованной преступной группы, тем самым содействуя в досудебном расследовании интернет-мошенничества, в раскрытии и уголовном преследовании других участников преступления, розыске похищенных денежных средств.

Организация негласных следственных действий.

Негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации – это негласные следственные действия (далее - НСД), без предварительного информирования лиц, интересов которых оно касается, с последующим документированием уполномоченными подразделениями правоохранительных или специальных государственных органов. Проводится путём перехвата и снятия знаков, сигналов, голосовой информации, письменного текста, изображений, видеоизображений, звуков и другой информации, передающейся по проводной, радио, оптической и другим электромагнитным системам [71].

Порядок проведения данного следственного действия на сетях электросвязи, используемых для услуг передачи данных электрической (телекоммуникационной) связи, включая сети Интернет, регламентировано совместным приказом правоохранительных и специальных органов РК «Об утверждении Правил проведения негласных следственных действий» от 12 декабря 2014 года № 892 (далее - Правила НСД) [72, С. 46].

НСД осуществляется только на основании санкции следственного судьи с использованием оперативно-технических сил и средств уполномоченных подразделений правоохранительного или специального государственного органа [72, С. 49].

Согласно Правилам НСД в соответствии со ст.232 УПК РК, за исключением негласного контроля почтовых и иных отправлений, следователь направляет поручение на проведение НСД оперативным подразделениям для документирования с использованием форм и методов оперативно-розыскной деятельности [73].

Как правило, продуманное и полное документирование поручения на проведение НСД, увеличивает оперативность и шансы на установление и задержание интернет-мошенников. В данном случае, рекомендуется установить анкетные данные интернет-мошенника, использующего легкодоступные средства анонимизации в сети Интернет (например, VPN - виртуальная частная сеть).

Изучение работы IP-адреса является важным для следователя при составлении поручения на проведение НСД в расследование интернет-мошенничества, так как во многих мошеннических схемах используется Интернет.

IP-адрес – это уникальный идентификационный номер, который присваивается каждому компьютеру при подключении в сеть Интернета. Он представляет собой последовательность из 4 цифр в диапазоне от 0 до 255, чередующихся через точку. Например, 192.168.242.225 [74].

Интернет-провайдер выдает каждому персональному устройству IP-адрес в момент начала интернет сессии – открытия первой интернет-страницы, и заканчивается закрытием интернет-сессии – закрытием последней интернет-страницы [75].

Таким образом, на каждом сайте («OLX», «krisha.kz», «kolesa.kz» и т.д.) хранятся истории соединений с его пользователями, следовательно и их IP-адреса. При каждом выходе в Интернет - мошенник оставляет свой «цифровой след», по которому его можно вычислить.

Каждому интернет-провайдеру выделено определенное количество IP-адресов в конкретном диапазоне, со своими ресурсами нумерации. При помощи интернет ресурса https://2ip.ru/whois/#result-anchor, зная IP-адрес, можно легко определить провайдера.

При установлении IP-адреса и время его нахождения в сети Интернет, следователь может узнать, где находится персональный компьютер или гаджет, с которого работал интернет-мошенник (номер квартиры, дома и т.д.).

Тем, не менее, интернет-мошенники при совершении правонарушении используют средства анонимизации в сети Интернет - VPN (виртуальная частная

сеть). VPN виртуальная частная сеть - это сервер третьих лиц, локализующегося на территории зарубежного государства, где при использовании VPN, установить IP-адреса интернет мошенников практический невозможно.

Однако, способы установления лиц, совершающие интернет мошенничество с помощью виртуальной частной сети VPN, есть, например, Cookie-файлы. Cookie-файлы – это фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя [76].

Например, при поиске в веб-браузерах «Google» или «Яндекс» определенного типа товара (купить запчасти на автомобиль), веб-браузер начинает выдавать рекламу именно о нем. Причина в том, что многие Интернет сайты сохраняют информации о своих пользователях (логин, ключи, пароли для быстрого доступа к веб-сайтам).

Сбор и анализ этой информации происходит посредством Cookie-файлов. Cookie-файлы веб-браузеров передают информацию своего нового пользователя, чтобы «сохранить» его. При его повторном посещении сайт будет знать о подключившемся пользователе ряд информации.

Особенностью Cookie-файлов является его неизменность, где интернет-мошенник может менять свой IP-адрес через VPN, проходить регистрацию с разных абонентских номеров, но сайт все равно поймет, что все это время к нему подключается один и тот же пользователь, то есть используется веб-браузер одного и того же персонального компьютера.

Имея изначально информацию лишь по одному объявлению интернет-мошенника, с помощью анализа Cookie-файлов возможно, получить сведения по всем объявлениям, размещенным интернет - мошенником.

Целесообразно проанализировать все объявления интернет-мошенника для установления реальных объявлений, выложенных с данного персонального компьютера (гаджета), с указанием личных IP-адресов и личного абонентского номера.

Установив анкетные данные владельца персонального компьютера или гаджета подозреваемого, следователь выносит поручение на проведение одного или нескольких видов НСД:

1) о проведении негласного аудио- и (или) видеоконтроля лица или места;

2) о проведении негласного контроля, перехвата и снятия информации, передающейся по сетям электрической (телекоммуникационной) связи;

3) о негласном получении информации о соединениях между абонентами и (или) абонентскими устройствами;

4) о негласном снятии информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации;

5) о негласном проникновении и (или) обследовании места;

6) о негласном наблюдении за лицом или местом;

7) о проведении негласного контрольного закупа.

Все вышеуказанное дает возможность оперативному сотруднику в короткие сроки вынести постановление на проведение НСД и обосновать следственному судье о необходимости проведения НСД для санкционирования.

Таким образом, отмечается следующее:

1. Вопросы расследования и производства следственных действий по уголовным правонарушениям в сети Интернет требуют тщательного анализа первоначальной информации, индивидуального подхода к каждому факту и базовых знаний в сфере IT-технологии;

2. В целях повышения эффективности расследования в региональных подразделениях правоохранительных органов следует создать группы по делам данной категории, с обязательным участием специалиста-эксперта и использованием программных комплексов, позволяющих восстанавливать всю историю работы ПК;

3. В связи с появлением новых технологий и методов совершения уголовных правонарушений, повышение квалификации сотрудников правоохранительных органов необходимо проводить постоянно.

2.4 Особенности назначения и проведения судебных экспертиз при расследовании уголовных правонарушений, совершенных в сети Интернет

Раскрытие и расследование уголовных правонарушений, совершенных в сети Интернет, остается одной из сложных задач для большинства сотрудников органов уголовного преследования.

Как ранее отмечалось (раздел 1.4), в основном, это связано с отсутствием системных обобщений материалов следственной и судебной практики, небольшим опытом работы сотрудников правоохранительных органов со специфическими источниками доказательственной информации, находящейся в электронно-цифровом формате (электронные сообщения, страницы, сайты и др.), а также недостаточно высоким уровнем подготовки слушателей по соответствующей специализации в высших учебных заведениях.

В ходе расследования уголовных правонарушений данной категории, когда возникает потребность разрешения вопросов и получения новых доказательств с использованием научных знаний, назначается судебная экспертиза.

Таким образом, орган уголовного преследования, при невозможности проверки своих версии иными способами, имеет возможность существенно расширить объем доказательственной информации, используя знания специалистов и экспертов.

Поскольку рассматриваемые преступные деяния совершаются посредством передачи компьютерной информации, существенная доля доказательственной информации в виде цифровых следов остается на электронных носителях. Они возникают в результате активной деятельности человека в сети Интернет (общение в социальных сетях, выкладывание фотографий, просмотр того или иного контента, объявлений, оплата товаров, услуг, и др.).

По этой причине в ходе судебной экспертизы экспертами и специалистами, для поиска оставленной в сети Интернет информации интересующей правоохранительные органы, используются различные средства и ресурсы. Набор указанных средств и ресурсов достаточно велик и постоянно дополняется.

В качестве одного из них можно привести «никнейм» пользователя, который стал известен правоохранительным органам. Как правило, пользователи сети Интернет используют один и тот же «никнейм» в разных социальных профилях, что облегчает поиск.

Уголовно-процессуальным законодательством определены порядок сбора доказательств и их допустимость. Однако, доказательства в электронном виде и компьютерные данные легко можно изменить. Поэтому, при сборе и обращении с электронными доказательствами необходимо обеспечить целостность, подлинность и непрерывность доказательства в течение всего периода времени с момента его выемки до приговора суда или вынесения окончательного решения органом уголовного преследования.

Недостаток специальных, профессиональных знаний в области информационных технологий не позволяет следователю самостоятельно

правильно изъять копию жесткого диска компьютера на месте совершения преступления. Поэтому при расследовании уголовных правонарушений в сети Интернет целесообразно привлечение специалиста в области компьютерной информации и компьютерной техники.

Вопросы обеспечения целостности файлов и логов при осмотре места происшествия и последующей выемке для назначения судебной экспертизы можно назвать алгоритмом безопасного хеширования.

Хэш-функция обеспечивает шифрование с использованием алгоритма и без ключа. Они называются «односторонними хэш-функциями», потому что отменить шифрование невозможно. Открытый текст переменной длины «хешируется» в (обычно) хэш-значение фиксированной длины (часто называемое «дайджестом сообщения» или просто «хешем»). Хеш-функции в основном используются для обеспечения целостности: если хэш-код открытого текста изменяется, изменяется и сам открытый текст. Общие старые хэш-функции включают алгоритмы безопасного хеширования.

Например, при снятии специалистом образа диска на месте происшествия подсчитывается хэш-функция, значение которой заносится в протокол. Эксперт, получив на исследование копию, подсчитывает с нее хэш-функцию. Если ее значение совпадает со значением, внесенным в протокол, эксперт и иные лица получают уверенность, что исследуемая копия совпадает с оригиналом с точностью до бита.

Аналогично хэш-функция используется для контроля целостности отдельных файлов. Например, при изъятии логов. Подсчитывается хэш-функция от лог-файла, она заносится в протокол. Значение хэш-функции в протоколе обеспечивает неизменность файла при копировании и последующем хранении. Совпадение значений хэш-функции гарантирует полное совпадение файлов [77, С. 159].

В случаях, когда в ходе исследования представленных объектов установлено, что они претерпели существенные изменения (например, изменилось содержимое файлов), возникает необходимость получения дополнительных сведений от правообладателя. Такие сведения о значимых и неизменных свойствах программного продукта (например, областей кода в оперативной памяти) можно получить путем допроса с привлечением специалиста.

Данные меры позволят эксперту провести сравнительное исследование путем сопоставления программных продуктов между собой и вынести заключения в соответствии с типовой методикой исследования компьютерной информации.

Следует отметить, что при отсутствии технической возможности копирования информации на машинные носители (RAID-массив, большой объем и др.) осуществляется исследование компьютерной информации разрушающими методами.

К ним относятся: включение средства вычислительной техники (системного блока, ноутбука и др.) с использованием загрузочных машинных носителей (флеш-карт, CD- и DVD- дисков и др.) и использование собственной операционной системы.

Однако, исследование компьютерной информации такими методами крайне нежелательно и применяется лишь при отсутствии других технических возможностей. При использовании данных методов изменяется следовая картина деятельности пользователя на данном средстве компьютерной техники, что существенно ограничивает и лишает эксперта возможности по использованию специализированного программного обеспечения при исследовании компьютерной информации.

В лог-файлах (файлы расширения Log) содержится большой массив доказательственной информации. По сути, в ней в виде текстовой информации хранится вся история интернет-соединений, исходящие и входящие запросы с данного компьютера и IP-адреса, с которых производились запросы к серверу. Дальнейшая деятельность следователя будет направлена на проведение с оперативными сотрудниками совместных следственных действий по установлению владельцев IP-адреса.

Хостинг-провайдеры в соответствии с политикой безопасности при предоставлении IP-адреса и регистрации сервера требуют с владельцев предоставления анкетных данных (паспортные данные, номер телефона, адрес места жительства, почтовый адрес и др.), что в значительной мере упрощает процедуру идентификации преступника. После получения указанных сведений следователю остается только организовать оперативно-розыскные мероприятия по установлению местонахождения и задержанию предполагаемого преступника.

Таким образом, осмотр места происшествия и последующая выемка, проведенные с нарушением алгоритма безопасного хеширования, то есть, без соответствующего обеспечения целостности файлов и логов при назначении судебной экспертизы, могут способствовать утере важной доказательственной информации и цифровых следов на электронных носителях информации.

В этой связи, в качестве примера, можно привести опыт США, которые в августе 2015 года приняли на Федеральном уровне «Стандарты безопасного хеширования» (SHS) (FIPS PUB 180-4), разработанные Департаментом Коммерции США [78].

Этот стандарт определяет хэш-алгоритмы, которые могут использоваться для генерации дайджестов сообщений. Дайджесты используются с целью определения были ли сообщения изменены с момента создания дайджестов.

Для удостоверения целостности и неизменности данных электронных носителей информации с момента изъятия предлагается на примере опыта США определить «стандарты безопасного хеширования», которые могут использоваться для определения вопроса о том, были ли сообщения изменены с момента создания дайджестов.

Согласно главе 35 УПК РК судебная экспертиза является самостоятельным следственным действием.

Основания назначения и производства судебной экспертизы определяются УПК РК и Законом РК от 10 февраля 2017 года «О судебно-экспертной деятельности в РК» [79].

Подготовка материалов для назначения судебной экспертизы состоит из комплекса процессуальных, технических и тактических мероприятий направленных на собирание и оформление всех необходимых вещественных доказательств, документов, образцов и исходных сведений.

Подготовка включает в себя:

– принятие решения о необходимости назначить экспертизу;

– вынесение мотивированного постановления;

– подбор объектов, представляемых в распоряжение эксперта;

– выбор эксперта или экспертного учреждения;

– постановку вопросов, выносимых на разрешение;

– материалы уголовного дела [80, С. 17].

В ходе расследования уголовных правонарушений совершенных в сети Интернет могут быть назначены и проведены различные (почерковедческие, экономические, дактилоскопические, судебно-химические, и другие виды экспертиз), однако, с учетом того, что при совершении данного вида преступлений незаконные действия выполняются непосредственно с помощью компьютерной техники, актуальным является назначение и проведение компьютерно-технических экспертиз. Судебно-экспертные исследования средств компьютерной технологии назначаются с целью исследования компьютерных устройств, программных продуктов, машинных магнитных носителей информации.

Для организации данного исследования необходимо представить специалистам предметы и документы, имеющие значение для расследования уголовного дела, изъятые в соответствии с действующим законодательством в ходе осмотра, обыска, выемки, либо добровольно предоставленные участниками уголовного процесса.

Объектами судебно-экспертного исследования средств компьютерной технологии являются:

1) **аппаратные объекты:**

- различные виды персональных компьютеров *(настольные, портативные, карманные и т.д.)* с основными блоками *(системные блоки, мониторы)*, внутренними узлами, деталями, комплектующими и т.д. *(далее – ЭВМ)*;

- периферийные устройства различного вида и назначения;

- сетевые аппаратные средства *(серверы, рабочие станции, активное оборудование, сетевые кабели и т.д.)*;

- дисковые накопители данных *(жесткие диски HDD, флоппи-диски FDD, оптические компакт-диски CD-ROM, CD-RW, DWD-ROM, флэш-карты USB).*

2) **программные объекты:**

- системное программное обеспечение *(различные операционные системы для персональных компьютеров и локальных сетей MS-DOS, UNIX, Windows различных версий и т.д., вспомогательные программы – утилиты, средства разработки и отладки программ, служебная системная информация и т.д.)*;

- различные прикладные программные продукты *(приложения общего назначения: текстовые и графические редакторы, системы управления базами данных, электронные таблицы, редакторы презентаций; приложения специального назначения для решения задач в определенной области науки, техники, экономики и т.д.).*

3) **информационные объекты:**

- файлы, подготовленные с использованием указанных выше и других программных средств *(с расширениями текстовых форматов .txt, .doc, графических форматов .bmp, .jpg, .cdr, форматов баз данных .dbf, .mdb, электронных таблиц .xls, .cal и др.);*

- данные в форматах мультимедиа.

4) **объекты, содержащие информацию, необходимую для производства экспертных исследований:**

- различные документы *(договоры на покупку, создание (передачу) научно-технической продукции; акты сдачи-приема научно-технической продукции; калькуляции стоимости предпродажной подготовки компьютерной техники и периферийных устройств и пр.)*;

- сопроводительная документация к поставляемой на исследование компьютерной, вычислительной технике *(периферийным устройствам, магнитным носителям)*, различные справочные данные, инструкции пользователя, а также материалы дел.

Задачи, решаемые в рамках данной методики, относятся к задачам идентификационного, диагностического, классификационного, и ситуационного характера.

При назначении судебных экспертиз возможны определенные сложности с постановкой правильных вопросов эксперту, либо специалисту, проводящему компьютерно-техническую экспертизу. Как ранее нами отмечалось, это связано со сложностью технических терминов и отсутствием специальных знаний в этой области.

Полагаем, что решение указанной проблемы лежит в плоскости взаимодействия следователя при назначении экспертизы с экспертом или специалистом, которые могут проконсультировать назначающего экспертизу по всем вопросам научно-методического характера.

При производстве судебно-экспертного исследования средств компьютерной технологии решаются следующие вопросы:

1) **по аппаратным средствам:**

- каковы технические характеристики представленной компьютерной техники;

- возможно ли использование представленного технического комплекса для осуществления тех или иных функциональных задач *(например, выхода в Интернет, запись компакт-дисков)*;

- каковы ориентировочные даты создания вычислительного комплекса с заданными возможностями и даты изготовления его отдельных блоков.

2) **по программным продуктам:**

- какая операционная система установлена в представленном системном блоке;

- имеется ли в представленном системном блоке установленное программное обеспечение *(указывается название)*;

- находится ли данное программное обеспечение в работоспособном состоянии;

- каковы дата и время установки программного обеспечения *(указывается название);*

- имеются ли в предоставленных системных блоках программы, приводящие к неправомерному доступу к охраняемой законом компьютерной информации, внесению изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ;

- каковы основные функции представленного программного обеспечения;

- каково назначение представленных программ для ЭВМ;

- возможно ли осуществление заданного вида деятельности с использованием представленных технических средств и размещенного на нем информационного и специального программного обеспечения *(запись компакт-дисков, подготовка и изготовление поддельных денежных знаков).*

3) **по информационным объектам:**

- имеется ли на представленном магнитном диске или в составе технических средств вычислительной техники необходимое информационное обеспечение для решения какой-либо конкретной функциональной задачи;

- имеются ли на представленных магнитных носителях файлы с документами, относящимися к той или иной сфере деятельности *(файлы с изображениями денежных знаков, бланками юридических лиц и оттисками печатей);*

- имеются ли на представленных магнитных носителях ранее удаленные файлы *(указываются названия)*;

- имеются ли на магнитном носителе какая-либо информация, если да, то каков вид ее представления;

- каково дата и время создания файлов *(указываются названия)* [81].

Таким образом, тщательный осмотр места происшествия и последующая выемка с соблюдением алгоритма безопасного хеширования, обеспечение целостности файлов и логов при назначении судебной экспертизы, способствуют расширению объема исследуемых материалов.

Указанные меры позволят правоохранительным органам возможность получения дополнительной доказательственной информации, путем использования научных знаний специалистов и экспертов.

Заключение

В современном мире внедрение цифровых технологии происходит быстрее, чем внедрение любых других инновационных разработок в истории человечества. Всего за два десятилетия цифровыми технологиями удалось охватить около 50 процентов населения земли. Использование технологий, способствующих расширению коммуникационных возможностей и доступа к финансовым, государственным и коммерческим услугам значительно сократило цифровое неравенство граждан.

Сегодня во многих отраслях жизнедеятельности используются системы объединения данных и искусственный интеллект, которыми отслеживаются и диагностируются транспортно-логистические проблемы, окружающая среда, сельское хозяйство, здравоохранение, и множество других сфер.

При этом цифровые технологии используются как для защиты и осуществления прав человека, так и для грубого их нарушения. С их помощью отслеживаются и анализируются финансовые операции, перемещения, покупки, разговоры и поведение людей. Активно реализуемые в Казахстане проекты по цифровизации общества, вместе с прогрессом в социально-экономической сфере несут и негативные последствия. В цифровом пространстве появляются новые виды уголовных правонарушений, совершаемые с помощью высоких технологий.

Перешли в онлайн формат и совершаются в организованной форме такие преступления как сбыт синтетических наркотических средств, вредоносных программ, компьютерных вирусов, персональных и финансовых данных и др.

Указанные уголовные правонарушения имеют свою специфику и часто носят латентный характер, а недостаточный уровень подготовки сотрудников правоохранительных органов способствует формированию атмосферы вседозволенности и безнаказанности. Тем самым нарушаются основополагающие принципы, закрепленные в Конституции и уголовно-процессуальном законодательстве страны.

Интенсивный рост киберпреступлений требует постоянного повышения качества следственной практики по раскрытию и расследованию уголовных правонарушений в киберпространстве.

1 сентября 2021 года Глава государства в своем послании «Единство народа и системные реформы – прочная основа процветания страны», поручил правоохранительным органам поставить эффективный заслон на пути распространения наркотиков среди наших граждан, особенно среди молодежи, и отметил о необходимости разработки комплекса мер по противодействию мошенничеству [39].

Данное поручение обнажило имеющиеся проблемы правоохранительной системы ввиду перехода значительной части рассматриваемых уголовных правонарушений в Интернет и неготовности государства к системному противодействию этим угрозам в цифровом пространстве.

Отдельного внимания со стороны научного сообщества, практических работников требует вопрос унификации ряда понятий, используемых в

отдельных статьях УК РК и применяемых при расследовании дел данной категории.

В этой связи, авторским коллективом проведены теоретические и прикладные изыскания, изучено международное и национальное законодательство в сфере защиты прав граждан от преступных посягательств в сети Интернет.

В результате выработаны следующие предложения теоретического, нормативного, организационного и методологического характера, направленные на повышение эффективности расследования уголовных правонарушений, совершенных в сети Интернет.

Теоретические выводы и предложения:

1. Содержание криминалистической характеристики для каждого вида уголовного правонарушения, совершенного в сети Интернет, является индивидуальным;

2. Криминалистическая характеристика уголовного правонарушения в сети Интернет содержит в себе научно-обоснованный инструмент когнитивной деятельности, обусловленный необходимостью обеспечения всестороннего, полного и объективного исследования обстоятельств совершенного противоправного деяния и решения задач по его раскрытию, а также реализации принципа неотвратимости наказания для виновных лиц. Вследствие эволюции общественных отношений появились явления и предметы, нуждающиеся в нормативной конкретизации и закреплении. Данная работа требует от законодателя постоянного совершенствования и унификации имеющихся норм;

3. Вопросы расследования и производства следственных действий по уголовным правонарушениям в сети Интернет требуют тщательного анализа первоначальной информации, индивидуального подхода к каждому факту и базовых знаний в сфере IT-технологии.

Законодательные предложения:

1. В ст.ст.105, 132, 134 УК РК используется квалифицирующий признак **«совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет».**

При этом, **сеть Интернет** согласно ст.1 Закона РК «Об информатизации» представляет собой сеть телекоммуникаций**.**

В этой связи предлагаем исключить в данных статьях слова «в том числе сети Интернет» как оборот речи, не несущий смысловой нагрузки;

2. Используемый в ст.ст.105, 132, 134 УК РК квалифицирующий признак **«совершенное посредством использования сетей телекоммуникаций, в том числе сети Интернет»** ограничивает правоприменителя, сужая сферу применения данной нормы к подобным деяниям.

В связи с чем, в целях расширения сферы действия данной нормы предлагается в качестве квалифицирующего признака в пп.4 ч.2 ст.105, ч.2 132, пп.1-1 ч.3 134 УК РК использовать оборот **«с использованием средств массовой информации или сетей телекоммуникаций»**;

3. В целях единообразного применения терминов, их логического построения и изложения юридическим языком используемых в УК РК речевых оборотов, закрепить в ст.ст.131, 161, 174, 179, 180, 256, 274, 299-1, 373, 375, 376, 378 УК РК, применяемый термин **«с использованием»** и в ст.ст.147, 148, 188, 190, 223 УК РК термин **«путем»**, заменить на термин **«посредством»** как наиболее соответствующий требованиям юридической техники;

4. Ввиду отсутствия в действующем уголовном законодательстве ряда дефиниций, применяемых в нем терминов, предлагается дополнить ст.3 УК РК (Разъяснения некоторых понятий, содержащихся в настоящем Кодексе) следующими дефинициями:

а) **компью́тер** - устройство или система, способная выполнять заданную, чётко определённую, изменяемую последовательность операций.

б) **компьютерная программа** - представленная в объективной форме совокупность данных и команд, предназначенных для функционирования компьютера и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для компьютера, и порождаемые ею аудиовизуальные отображения.

в) **компьютерная система** - любое устройство или группа взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

г) **компьютерная сеть** - система, состоящая из компьютеров и компьютерных устройств (принт-серверов, серверных веб-камер и др.), которые взаимодействуют по единым правилам, определённым сетевыми протоколами;

5. Установлено, что понятие «информационно-коммуникационная сеть», закрепленное в ч.1 ст.212 УК РК, фактически является сетью телекоммуникаций.

В этой связи, в целях реализации принципа единообразия применяемых терминов в УК РК, предлагаем ч.1 ст.212 изложить в следующей редакции:

«- заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в **сетях телекоммуникаций,** для размещения интернет-ресурсов, преследующих противоправные цели»;

6. В целях создания эффективного механизма противодействия теневому обороту наркодоходов посредством «электронных кошельков» и пресечения распространения новых психоактивных веществ с использованием виртуальных платежных систем, предлагается поручить Национальному банку внести изменения в Закон РК «О платежах и платежных системах» в части отказа в оказании услуг неидентифицированным пользователям электронных платежных систем.

Процесс идентификации пользователей предлагается осуществлять по аналогии с процедурой прохождения регистрации в онлайн-режиме в банковских и сервисных мобильных приложениях («Каспи», «InDriver» и др.);

7. В целях совершенствования правоприменительной практики расследования уголовных правонарушений, совершаемых в сети Интернет, предлагается вернуться к рассмотрению вопроса о ратификации Конвенции Совета Европы «О компьютерных преступлениях».

Имплементация положений Конвенции и приведение национального законодательства в соответствие с международными нормами позволит расширить сферы взаимодействия правоохранительных органов Казахстана с зарубежными коллегами по раскрытию уголовных правонарушений, совершаемых в сети Интернет;

8. В целях создания единого алгоритма обнаружения и изъятия цифровых доказательств при расследовании уголовных правонарушений, совершенных в сети Интернет поручить ЦСЭ МЮ РК рассмотреть вопрос законодательного закрепления использования стандарта безопасного хеширования.

Указанные меры позволят удостоверить целостность и неизменность данных электронных носителей информации с момента их создания и последующего изъятия (на примере опыта США).

9. В целях определения общего количества правонарушений, совершенных в сети Интернет, предлагается в форму отчета №1-М «О зарегистрированных уголовных правонарушениях» в раздел «Всего правонарушений» внести строку «совершено посредством сети Интернет» (имеется акт внедрения в КПСиСУ ГП);

10. Для разграничения суммы ущерба от уголовных правонарушений, совершенных в сети Интернет, предлагается в графу «общая сумма ущерба всех преступлений» ЭИУД формы ЕРДР-2 отчета №1-М внести в реквизит №23 «ущерб», дополнительный показатель «посредством сети Интернет»;

11. В целях устранения пробелов понятийного аппарата, расширения определения персональных данных, создания безопасной среды для детей от киберпосягательств заинтересованным государственным органам предлагается рассмотреть вопрос о кодификации норм права в единый кодекс.

Указанные меры позволят систематизировать разрозненные и фрагментированные нормы закона, регулирующие важнейшие общественные отношения в сфере ИКТ, безопасность и защиту информации, связи, обработки данных, цифровых активов, искусственного интеллекта, защиты прав субъектов персональных данных в единый нормативный документ.

Организационные предложения:

1. В целях укомплектования компетентными и профессиональными сотрудниками следственных и оперативных подразделений в учебных заведениях правоохранительных органов предлагается создание центров и кафедр по подготовке специалистов по противодействию уголовным правонарушениям в сети Интернет;

2. В целях повышения эффективности противодействия уголовным правонарушениям в сети Интернет предлагается создать в МВД самостоятельное подразделение по борьбе с киберпреступностью.

Подразделению следует придать функции по реализации государственной политики в сфере борьбы с киберпреступностью, межведомственной

координации, исследований электронно-цифровых доказательств, взаимодействия с частным сектором (провайдеры, банковский сектор, ВУЗы, научное сообщество, правообладатели и др.) и международного взаимодействия.

3. В целях повышения эффективности расследования в региональных подразделениях правоохранительных органов следует создать отделы (группы) по делам данной категории, с обязательным участием специалиста-эксперта и использованием программных комплексов, позволяющих восстанавливать всю историю работы ПК.

4. Для повышения уровня осведомленности граждан на системной основе в СМИ, на ведомственных информационных ресурсах МВД освещать факты и способы совершения уголовных правонарушений в сети Интернет.

5. В связи с появлением новых технологий и методов совершения уголовных правонарушений, повышение квалификации сотрудников правоохранительных органов проводить на непрерывной основе.

Методологические предложения:

1. Выработаны предложения по алгоритму осмотра места происшествия, изъятия, выемки и назначения НСД при расследовании уголовных правонарушений, совершенных в сети Интернет;

2. Подготовлены и изданы научные публикации, учебное пособие, которые внедрены в учебную и практическую деятельность.

Список использованных источников

1. Конституция Республики Казахстан от 30 августа 1995 года // Режим доступа: https://online.zakon.kz/Document/?doc_id=30004865/ (дата обращения: 21.01.2021).
2. Указ Президента Республики Казахстан «Об утверждении Национального плана развития Республики Казахстан до 2025 и признании утратившими силу некоторых указов Президента Республики Казахстан» от 15 февраля 2018 года № 636 // Режим доступа: https://adilet.zan.kz/rus/docs/U1800000636 (дата обращения: 21.01.2021).
3. Головин, А.Ю. Системные средства и методы в криминалистической науке: Учебное пособие. - Тула, 2013. – 72 с.
4. Яблоков, Н.П. Криминалистическая характеристика преступления и типичные следственные ситуации как важные факторы разработки расследования преступлений. Вопросы борьбы с преступностью, Москва, 1979. – 112 с.
5. Густов, Г.А. Понятие и виды криминалистической характеристики преступлений // Криминалистическая характеристика преступлений. Москва, 1984. - 44 с.
6. Аристархова, Т.А. Основы криминалистической характеристики преступлений против прав и законных интересов человека и гражданина, совершенных по экстремистским мотивам // Известия Тульского государственного университета. Экономические и юридические науки. 2014. - Вып. 3. (Ч. II.). - С. 47-54
7. Чурилов, С.Н. В чем смысл и значение термина «криминалистическая характеристика механизма преступления»? // Вестник Криминалистики. 2008. - Вып. 2 (26). - С.17.
8. Савельева, М.В., Степанов, В.В. О понятии криминалистической информации // Вестник криминалистики. 2009. – Вып. 4 (32). - С.45.
9. Белкин, Р. С. Криминалистическая энциклопедия. – Москва, 2000. - 334с.
10. Паршина, Е.Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании: Автореферат диссертации. канд. юрид. наук. - Ижевск, - 2004. – С. 28.
11. Криминалистика: Учебник. Под ред. Образцова, В.А. Москва, 1997 – 238 с.
12. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V // Режим доступа: https://adilet.zan.kz/rus/docs/K1400000231 (дата обращения: 21.01.2021).
13. Павликов, С.Г. К вопросу о значении теории криминалистической характеристики преступлений // Российский судья. - 2012. - № 10. - С. 45—47.
14. Мустафаев, М.Х. Гносеологическое значение криминалистической характеристики преступлений // Актуальные проблемы государственного и правового строительства в Азербайджанской Республике в переходный период. – 2005. - №11. - С. 323-344.

15. Белкин, Р.С. Курс криминалистики: Учебник. – Москва, 1997. - Т.3. - 538 с.

16. Исаков, А.В. Содержание криминалистической характеристики // Режим доступа: https://superinf.ru/view_helpstud.php?id=838 (дата обращения: 21.01.2021).

17. Сверчков, В.В. Уголовное право. Общая часть: учебное пособие для ВУЗОВ, 10-е изд. перераб. и доп.- Москва. 2017 – 251 с.

18. Бессонов, А.А. Обстановка преступления как элемент его криминалистической характеристики // Режим доступа: https://cyberleninka.ru/article/n/obstanovka-prestupleniya-kak-element-ego-kriminalisticheskoy-harakteristiki (дата обращения: 02.03.2021).

9. Исаков, А.В. Содержание криминалистической характеристики уголовного правонарушения // Режим доступа: https://superinf.ru/view_helpstud.php?id=838 (дата обращения: 02.03.2021).

20. Мещеряков, В.А. Основы методики расследования преступлений в сфере компьютерной информации : автореферат диссертации. д-ра юрид. наук. – Воронеж. - 2001. - С. 21.

21. Антонян, Ю.М., Эминов, В.Е. Личность преступника. Криминологопсихологическое исследование: Монография. – Москва, 2018. – 368 с.

22. Прогноз и цифры о кибербезопасности // Режим доступа: https://vc.ru/future/55680-top-5-faktov-prognozov-i-cifr-o-kiberbezopasnosti (дата обращения: 03.03.2021).

23. Глобальная сеть Интернет: история развития // Режим доступа: http://sbmtwiki.wikidot.com/wiki:globalnaa-set-internet:istoria-razvitia (дата обращения: 03.03.2021).

24, 25. Перов, В.А. Электронный след: понятие, виды, способы обнаружения и фиксации. Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: Материалы Всероссийской науч.-прак-кой конференции. – Москва, 2021. – 260 с.

26. Интернет-мошенничество [Электронный ресурс]: Википедия, Свободная энциклопедия // Режим доступа: https://ru.wikipedia.org/wiki/ (дата обращения: 03.03.2021).

27. В период пандемии в Казахстане активизировались интернет-мошенники // Режим доступа: https://allinsurance.kz/articles/upravlenie-riskami/16568-v-period-pandemii-v-kazakhstane-aktivizirovalis-internet-moshenniki (дата обращения: 03.03.2021).

28. «Президентскую премию» предлагал мошенник в Акмолинской области // Режим доступа: https://timeskz.kz/58872-prezidentskuyu-premiyu-predlagal-moshennik-v-akmolinskoy-oblasti.html (дата обращения: 03.03.2021).

29. Шульгина, И.В. Криминалистическая характеристика личности мошенника // Режим доступа: https:// cyberleninka.ru/article/n/ kriminalisticheskaya-harakteristika-lichnosti-moshennika (дата обращения: 03.03.2021).

30. Интернет-мошенничество фишинг: механизм, виды и способы противодействия // Режим доступа: https://www.exocur.ru/internet-moshennichestvo-fishing-mehanizm-vidyi-i-sposobyi-protivodeystviya/ (дата обращения: 03.03.2021).

31. Буллинг [Электронный ресурс]: Википедия, Свободная энциклопедия // Режим доступа: https://ru.wikipedia.org/wiki/%D0%A2%D1%80% D0%B0%D0% B2%D0%BB%D1%8F (дата обращения: 03.03.2021).

32. Авганов, С. Кибербуллинг или немного об интернет-травле // Режим доступа: https://online.zakon.kz/Document/? doc_id=37000746&pos=5;-90#pos=5;-90 (дата обращения: 03.03.2021).

33. Байнекеева, З. Задача на миллион // Режим доступа: https://azh.kz/ru/news/view/43826 (дата обращения: 03.03.2021).

34. Неприкосновенность частной жизни: Монография / Коллектив авторов. - Косшы, 2020. - 196 с.

35. Трапезников, В.И. Характеристика и значение международной характеристики и значение международной статистики киберпреступности // Информатика та математичні методи в моделюванні. - 2014. – Т. 4. – С. 363-369.

36. Статистические данные и факты о кибербезопасности на 2021 год // Режим доступа: htths://www.websitehostinqratinq.com/ (дата обращения 05.04.2021).

37. Расследование продолжается // Режим доступа: https://kursiv.kz/news/obschestvo/2021-04/mvd-soobschilo-o-roste-kiberprestupleniy-v-kazakhstane (дата обращения 05.04.2021).

38. Бегалиев, Е.Н. Современный толковый словарь криминалиста 2020 г., // Режим доступа: http://academy.gp.kz/185.174.154 (дата обращения 05.04.2021).

39. «Единство народа и системные реформы - прочная основа процветания страны». Послание Главы государства народу Казахстана от 1 сентября 2021 года // Режим доступа: https://adilet.zan.kz/rus/docs/U1800000889 (дата обращения: 21.05.2021).

40. Алексеев, С.С. Общая теория права: Монография Москва, - 2002. Т 2. – 272 с.

41. Большой юридический словарь / Под ред. А.Я. Сухарева, В.Д. Зорькина и др. Москва, - 1998. – 782 с.

42. Пиголкин, А.С. Язык закона // Режим доступа: miepl.ru/pigolkin.html (дата обращения: 21.05.2021).

43. Онлайн словарь компьютерных терминов // Режим доступа: https://m.seonews.ru/glossary/internet-site/ (дата обращения: 21.05.2021).

44. Толковый словарь русского языка Ожегова, С.И. // Режим доступа: https://www.myfilology.ru/media/user_uploads/Tutorials/Tolkovy_slovar_Ozhegova.pdf (дата обращения: 21.05.2021).

45. Петров, Е.П. Юридическая терминология в процессе правотворчества и систематизации нормативных правовых актов, Science time // Режим доступа: https://cyberleninka.ru/article/n/yuridicheskaya-terminologiya-v-protsesse-pravotvorchestva-i-sistematizatsii-normativnyh-pravovyh-aktov (дата обращения: 05.06.2021).

46. Доклад Генерального секретаря ООН Гуттериша А. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Режим доступа: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 05.06.2021).

47. Ганиева, Т.И., Урматова, А.Д., Рыспаева, Г.С. Юридическая терминология и терминотворчество в процессе подготовки нормативных правовых актов в Киргизской Республике // Бюллетень науки и практики, - Т.5. - №10. – 2019. - С. 176-186,

48. Толковый словарь по вычислительным системам = Dictionary of Computing / Под ред. Иллингуорта, В. и др.: пер. с англ. Белоцкого, А.К. и др.; Под ред. Масловского, Е.К. — Москва, 1990. — 560 с.

49. Научно-технический энциклопедический словарь // Режим доступа: https://dic.academic.ru/dic.nsf/ntes/2134/ (дата обращения: 05.06.2021).

50. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 №230-ФЗ // Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_64629/ce1359ed5b9bd99896d7a496c7887e7c223a2cbc/ (дата обращения: 05.06.2021).

51. Борчашвили, И.Ш. Комментарий к Уголовному кодексу Республики Казахстан особенная часть (том 2). Алматы, 2015. - 1120 с.

52. Конвенции о компьютерных преступлениях (принята Советом Европы, в г. Будапешт 23.11.2001 года) // Режим доступа: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/ (дата обращения: 05.06.2021).

53. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы // Режим доступа: http://encarta.msn.com (дата обращения: 05.06.2021).

54. Давид, Р. Основные правовые системы современности // Режим доступа: http://lib.ru/PRAWO/rene.txt (дата обращения: 05.06.2021).

55. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: Учебное пособие / Коллектив авторов. Часть 1 Москва: Академия управления МВД РФ, 2019. – 208 с.

56. Архив Комитета информации Министерства информации и общественного развития РК, 2021 год.

57. Мещеряков, В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Вестник Воронежского государственного университета. - 2001. – С.74 – 76.

58. Терминологически «сведения о прохождении информации» в рассматриваемом контексте означают информацию, генерированную ЭВМ, записанную при помощи сетевого оборудования и касающуюся определенного сообщения или нескольких сообщений.

59. Информации Департамента криминальной полиции МВД РК. Архив МВД РК 2021г.

60. Шымкентцам предлагают 300 тысяч // Режим доступа: https://tengrinews.kz/kazakhstan_news/eto-chudovischno-shyimkenttsan- redlagayut-300-tyisyach-449409/24.09.21г. (дата обращения: 10.06.2021).

61. Иксанов, Р.А. Защита прав граждан от посягательств в сети Даркнет // Международный журнал гуманитарных и естественных наук. – 2018. – №4. – С. 271-273.

62. Доклад Генерального секретаря ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Режим доступа: https://www.unodc.org/documents/ Cybercrimer/SG_report/ V1908184_R (дата обращения: 15.06.2021).

63. Методические рекомендации по расследованию уголовных правонарушений, связанных с незаконным оборотом наркотических средств посредством интернет ресурсов. / Коллектив авторов. - Караганда: Карагандинская академии МВД РК, 2020г. 83 с.

64. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года №94-V // Режим доступа: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 15.06.2021).

65. Волчецкая, Т.С. Криминалистическая ситуалогия: Монография – Москва, 1997. – 248 с.

66. Толковый словарь Ушакова // Режим доступа: https://ushakovdictionary.ru/ (дата обращения: 21.06.2021).

67. Тактика осмотра места происшествия по делам о незаконном обороте наркотиков // Режим доступа: https://dspace.susu.ru/xmlui/bitstream/handle/ 0001.74/13523/2016_662_smarchkov.pdf?sequence=1&isAllowed=y (дата обращения: 21.06.2021).

68. Belkasoft X - Надёжное решение для комплексной цифровой криминалистической экспертизы и расследования корпоративных инцидентов // Режим доступа: https://belkasoft.com/ru (дата обращения: 21.06.2021).

69. Выемка электронных носителей информации // Режим доступа: https://si-center.ru/info/vyemka-jelektronnyh-nositelej-informacii/ (дата обращения: 21.06.2021).

70. Ищенко, Е.П., Филиппов, А.Г. Криминалистика. Учебник. — Москва, 2007. —1274 с.

71. Приказ Министра внутренних дел Республики Казахстан «Об утверждении Правил проведения негласных следственных действий» от 12 декабря 2014 года №892 // Режим доступа: https://adilet.zan.kz/rus/docs/V14C0010027 (дата обращения: 21.06.2021).

72. Медиев, Р.А., Сулейманова, Г.Ж. Негласные следственные действия в теории и практике органов уголовного преследования Республики Казахстан: Монография. - Актобе, 2017. — 200 с.

73. Закон Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года №154-XIII // Режим доступа: https://adilet.zan.kz/rus/docs/Z940004000_(дата обращения: 21.06.2021).

74. Словарь терминов интернет-рекламы и SEO // Режим доступа: https://www.russianpromo.ru/wiki/ip-adres/ (дата обращения: 21.06.2021).

75. IP-адрес // Режим доступа: https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80 %D0%B5%D1%81 (дата обращения 21.06.2021).
76. Cookie // Режим доступа: https://ru.wikipedia.org/wiki/Cookie (дата обращения 21.06.2021).
77. Күнғожинов, К.Ә. Проблемы расследования преступлений в Интернете. Сборник материалов научного мероприятия. Круглый стол, приуроченный к 30-летию Независимости Республики Казахстан. «Расследование уголовных правонарушений в сети Интернет: проблемы и пути решения». 28.05.2021г. Қосшы, 2021. ISSN 2709-4421, 180 с.
78. Криптографическая_хеш-функция // Режим доступа: https://ru.wikipedia.org/wiki/ (дата обращения: 25.06.2021).
79. Закон Республики Казахстан «О судебно-экспертной деятельности в РК» от 10 февраля 2017 года №44-VI // Режим доступа: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 25.06.2021).
80. Методические рекомендации по расследованию уголовных правонарушений, связанных с незаконным оборотом наркотических средств посредством Интернет ресурсов / Коллектив авторов. Караганды: Карагандинская Академия МВД РК имени Б.Бейсенова, 2020. – 36 с.
81. Справочник для правоохранительных органов и судов по вопросам назначения судебных экспертиз в Центре судебной экспертизы Министерства юстиции Республики Казахстан // Режим доступа: https://online.zakon.kz/Document/?doc_id=31098967#pos=1;-16 (дата обращения: 25.06.2021).

Приложение А

Анкета (опросный лист)

Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан проводит опрос населения об интернет-преступлениях с целью выработки эффективных мер по противодействию и расследованию.

Просим Вас ответить на вопросы анкеты. Отметьте, пожалуйста, мнение (при необходимости можно выбрать несколько вариантов), с которыми Вы согласны, а также по необходимости дополните пояснения в графе «иное».

Настоящая анкета носит **анонимный характер,** полученные данные будут использованы в обобщенном виде для научных целей.

Заранее благодарим Вас за искренние ответы и оказанную помощь в исследовании!

1. Что Вы предпочитаете делать в Интернете?

1. читать новости;
2. использую электронные платежные системы (Webmoney, Яндекс.Деньги, PayPal, онлайн покупки и др.);
3. скачиваю файлы (музыку, видео, книги, фотографии и т.д.);
4. пользуюсь системой файлообменов BitTorrent (Rutracker.ru, Torrent.ru и т.д.);
5. пользуюсь мессенджерами (WhatsApp, *Facebook*, ВКонтакте, *Instagram, Twitter* и др. соц.сети);
6. пользуюсь видеопорталами (YouTube, **TikTok, Likee** и т.д.);
7. иное_____.

2. Осведомлены ли Вы об угрозах информационной безопасности?

1. да;
2. нет;
3. впервые слышу об этом;
4. не знаю, что это такое
5. иное_____.

3. Подвергались ли Вы преступлениям, совершаемым посредством использования сетей телекоммуникаций, в том числе сети Интернет?

1. да;
2. нет;
3. впервые слышу об этом;
4. не знаю, что это такое;
5. иное_____.

4. Каким из указанных видов преступлений в сети Интернет Вы подвергались?

1. неправомерный доступ к информации;
2. неправомерное уничтожение или модификация информации;
3. неправомерное завладение информацией;
4. принуждение к передаче информации;

5. создание, использование или распространение вредоносных программ;
6. интернет-мошенничество;
7. бесконтактная торговля наркотиками;
8. распространение порнографической продукции;
9. иное_____.

5. Как устанавливает мошенник контакт с жертвой?
1. обращается лично, но не представляется (свое или имя жертвы);
2. обращается лично, называя имя (свое или жертвы);
3. иное _____.

6. Когда Вы столкнулись с интернет – преступлением, как вы повели себя:
1. доверился и оказался жертвой интернет-преступлений;
2. я вовремя понял, что это действия злоумышленников, и не среагировал;
3. мне не приходилось сталкиваться с интернет-преступлениями;

7. Какими методами и способами чаще всего пользуются преступники, чтобы привлечь потенциальных жертв:
1. взлом социальных сетей и мессенджеров (угроза распространения личных данных, блокировка компьютеров и т.д.);
2. приглашает на сайты с тематикой, которые могут заинтересовать потенциальную жертву (работа, наркотики, порно, розыгрыши, акции);
3. звонки и сообщения на телефон;
4. атака компьютерными вирусами (в том числе вредоносные спам и отсылочные файлы);
5. иное_____;

8. Вы или Ваши близкие и знакомые стали жертвой интернет-преступников, потому что к вам обратились:
1. с просьбой;
2. с угрозами;
3. с требованиями;
4. с предложениями;
5. иное _____
6. затрудняюсь ответить;

9. С какими техниками мошенничества Вы знакомы или встречались, о каких знаете, но не встречались.

№№	Техники мошенничества	Знаю и встречался	Знаю, но не встречался	Не знаю
1	спам			
2	SMS-оплата			
3	фальшивые извещения о выигрыше в лотерею			
4	фишинг мошенничеством в виде рекламы товаров и услуг			
5	попрошайничество			
6	тайпсквоттинг			
7	имитаторы вирусов и антивирусов			
8	взлом сайтов			
9	кража пароля от учетной записи пользователя			
10	мошенничество с платежными системами			
11	иное			

10. Кто чаще подвергается интернет-мошенничеству?
1. доверчивые люди;
2. корыстный человек;
3. азартные;
4. невнимательные;
5. желающие получить легкие деньги;
6. люди, у которых нет средств к существованию;
7. неопытный пользователь Интернета;
8. не знающие об интернет-мошенничествах;
9. иное _____
10. затрудняюсь ответить;

11. Сталкивались ли Вы или Ваши близкие, знакомые с предложениями в сети работы по распространению запрещенных наркотических препаратов и психотропных веществ?
1. да, но не придал значения;
2. нет, не сталкивался;
3. показалось подозрительным, испугался;
4. подумал, что розыгрыш;
5. иное_____;

12. Обращались ли Вы в правоохранительные или уполномоченные органы, при попытке интернет-преступления?

1. нет;
2. да, обращались в полицию;
3. не знаю куда обращаться;
4. решал проблемы самостоятельно;
5. обращение в уполномоченный орган в сфере обеспечения информационной безопасности;
6. обращался к IT-специалистам на платной основе;
7. бесполезно обращаться, все равно ничего не решится;
8. не хочется иметь дело с формальностями в правоохранительных органах;
9. нет, из–за угрозы мошенников;
10. иное _____;

13. Укажите какие потери, Вы понесли в результате интернет-преступления *(деньги, личные данные, покушение на жизнь, здоровье и др.)?*
1. морально – психологические;
2. финансовые: деньги в сумме: _____;
3. другие материальные ценности (какие?) _____;
4. никакие;
5. иное _____;
6. затрудняюсь ответить;

14. Какое было принято решение правоохранительным или уполномоченным органом по Вашему обращению?
1. были даны рекомендации по дальнейшему безопасному использованию сети Интернет;
2. принято заявление;
3. даже не приняли заявление;
4. предложили пройти обучающие курсы;
5. иное _____;

15. Как Вы считаете, в чем заключается проблема роста интернет-преступлений?
1. все больше мошенников владеют IT- технологиями;
2. виноват сам пользователь;
3. правоохранительные органы не противодействуют интернет-преступлениям;
4. иное _____;
5. затрудняюсь ответить;

16. Известны ли Вам факты привлечения к ответственности интернет-преступников?
1. да;
2. нет;
3. иное_____;
4. затрудняюсь ответить;

17. По Вашему мнению, какие действия правоохранительных органов были бы более эффективными?

1. фиксация всех значимых, по мнению жертвы, обстоятельств преступления;
2. оперативное реагирование (сбор и фиксация) по заявлению;
3. повысить эффективность сотрудничества с другими органами;
4. привлечение специалистов и экспертов в области IT-технологии на начальных этапах работы сотрудников;
5. иное_____;

18. По Вашему мнению, какие действия государства были бы более эффективными для предупреждения интернет-преступности?

1. подготовка и повсеместное распространение социально-ознакомительных роликов;
2. распространение брошюр и информационных листов;
3. информация в всплывающие окна в сети Интернет;
4. посвящение рубрики в программе новостей;
5. иное_____;

19. Доверяете ли Вы государственным органам, в базах данных которых хранятся Ваши персональные данные?

1. да, полностью доверяю;
2. нет, сомневаюсь в честности сотрудников государственных органов;
3. думаю, что в госорганах недостаточна надежная система информационной безопасности;
4. не знаю, не думал об этом;
5. иное _____;

В заключении сообщите, пожалуйста, общие сведения о себе:
(отметьте галочкой, выбранный Вами ответ)

20. Ваш пол:

1. мужской**;**
2. женский**.**

21. Пожалуйста, укажите Ваш возраст:

1. 10 - 17 лет;
2. 18 - 26 лет**;**
3. 27 - 36 лет**;**
4. 37 - 46 лет**;**
5. 47 - 56 лет**;**
6. 57 – 68 лет**.**

22. Ваше образование?

1. высшее;

2. неполное высшее;
3. средне-специальное**;**
4. среднее;
5. без образования**.**

23. В каком регионе Вы проживаете
1. в столице;
2. в областном центре;
3. в районном центре;
4. в небольшом городе;
5. в поселке городского типа;
6. в селе.

24. Укажите, пожалуйста, Ваш социальный статус?
1. государственный служащий;
2. предприниматель;
3. само занятый;
4. не работающий;
5. учащийся (студент/ученик средней школы).

Благодарим за участие в опросе!