Научная статья
Научная специальность
5.1.4 «Уголовно-правовые науки»

УДК 343.98
DOI https://doi.org/10.26516/2071-8136.2024.3.110

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В МЕХАНИЗМЕ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ

© Усачев С. И.[1], Усачева Е. А.[2], 2024
[1] Восточно-Сибирский институт МВД России, г. Иркутск, Россия
[2] Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, г. Иркутск, Россия

Представлены возможности информационно-коммуникационных технологий (ИКТ) и их влияние на общество, в том числе на трансформацию преступной деятельности, ввиду активного использования возможностей ИКТ физическими и юридическими лицами, а также преступниками в противоправных целях. Установлено, что распространение ИКТ в повседневной жизни имеет целый ряд неоспоримых преимуществ, однако наряду с этим такие технологии все чаще выступают инструментом преступной деятельности. Появление новаций в цифровой среде закономерно влечет появление новых способов совершения преступлений. Сделан вывод, что повышение уровня вовлеченности граждан в использование современных технологий и платформ зачастую продуцирует множество уязвимостей в цифровом пространстве, используемых преступниками. Установлено, что в этой связи противодействие преступлениям, совершаемым с использованием ИКТ, будет эффективным только в случае комплексного подхода: изучения механизма и способов преступной деятельности, повышения уровня «компьютерной грамотности» физических лиц – пользователей интернет-пространства, повышения уровня знаний сотрудников правоохранительных органов, совершенствования законодательства и т. д. Выявлено, что современные возможности ИКТ напрямую влияют на механизм преступной деятельности. Сделан вывод, что раскрытие, расследование и предупреждение преступлений, совершаемых с использованием ИКТ, требуют полноценного и всестороннего анализа, при этом деятельность правоохранительных органов будет существенно отличаться для разных направлений.

Ключевые слова: информационно-коммуникационные технологии, механизм преступления, сеть Интернет, конфиденциальность, анонимность, IP-адрес пользователя, TOR-браузер.

INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE MECHANISM OF CRIMINAL ACTIVITY

© Usachev S. I.[1], Usacheva E. A.[2], 2024
[1] East Siberian Institute of the Ministry of Internal Affairs of Russia, Irkutsk, Russian Federation
[2] Irkutsk Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation, Irkutsk, Russian Federation

The possibilities of information and communication technologies and their impact on society, including the transformation of criminal activity, due to the active use of ICT capabilities by individuals and legal entities, as well as criminals for illegal purposes, are presented. It has been established that the spread of ICTs into everyday life has a number of undeniable advantages, however, along with this, such technologies are increasingly becoming an instrument of criminal activity. The emergence of innovations in the digital environment naturally entails the emergence of new ways of committing crimes. It is concluded that increasing the level of citizen involvement in the use of modern technologies and platforms often produces many vulnerabilities in the digital space that are used by criminals. It has been established that in this regard, countering crimes committed using ICT will be effective only in the case of an integrated approach: studying the mechanism and methods of criminal activity, increasing the level of "computer literacy" of individuals - users of the Internet space, increasing the level of knowledge of law enforcement officers, improving legislation, etc. It has been revealed that modern ICT capabilities directly affect the mechanism of criminal activity. It is concluded that the disclosure, investigation and prevention of crimes committed using ICT requires a full and comprehensive analysis, while the activities of law enforcement agencies will differ significantly for different areas.

Keywords: information and communication technologies, mechanism of crime, Internet, confidentiality, anonymity, user IP address, TOR browser.

В настоящее время можно с уверенностью констатировать, что различные информационно-коммуникационные технологии (далее – ИКТ) достаточно прочно интегрированы практически во все сферы деятельности общества и государства в целом. Стремительная популярность и активное распространение ИКТ напрямую связаны с развитием технологий (рост вычислительных мощностей компьютерной техники и смартфонов, совершенствование стандартов мобильной связи: внедрение сетей пятого поколения 5G[1], использование волоконно-оптической связи провайдерами и т. д.); повышением уровня вовлеченности граждан в использование современных технологий и различных платформ (необходимость оплаты услуг посредством интернет-банкинга, использование федеральной государственной информационной системы «Единый портал государственных услуг Российской Федерации» (далее – «Госуслуги»), создание в крупных компаниях различных виртуальных помощников, голосовых ассистентов, чат-ботов, с которыми приходится взаимодействовать потребителям каких-либо услуг).

При этом в этой части стоит сделать уточнение: зачастую активное вовлечение граждан происходит от «безальтернативности». Так, в подавляющем большинстве случаев запись в отделения РЭО, МФЦ, УФМС просто невозможна традиционными способами (по телефону либо личный визит) – на сегодняшний день подобные действия зачастую доступны только через личные кабинеты либо через «Госуслуги».

Безусловно, распространение ИКТ в повседневной жизни имеет целый ряд неоспоримых преимуществ, однако наряду с этим такие технологии все чаще выступают инструментом преступной деятельности. Появление новаций в цифровой среде закономерно влечет появление новых способов совершения преступлений [6, с. 134]. Особенности информационных технологий позволяют, сохраняя анонимность, оплачивать криминальные услуги или запрещенные товары, финансировать организованную преступность, экстремистские и террористические структуры и т. д. [8, с. 6]. При этом расследование преступлений, совершаемых с использованием возможностей ИКТ, – это достаточно сложный процесс, так как требует от сотрудников правоохранительных органов не только традиционных знаний в области криминалистических методов, но и развитых навыков в области информационных технологий. Кроме того, роль правоохранительных органов заключается не только в расследовании преступлений, но и в предотвращении их совершения, создании механизмов защиты и сотрудничества с различными структурами и организациями. Эта проблема имеет множество аспектов, включая технические, юридические и этические.

Для исследования закономерностей возникновения и формирования криминалистически значимой информации о преступлениях, совершаемых с использованием ИКТ, обратимся к криминалистической дефиниции механизма преступления, который представляет собой сложную динамическую систему, определяющую содержание преступной деятельности [7, с. 15]. Элементами механизма преступления являются: субъекты преступления; отношение субъекта преступления к своим действиям, их последствиям, соучастникам; предмет посягательства; способ преступления; преступный результат; обстановка преступления (место, время и другие относящиеся к ней обстоятельства); поведение и действия лиц, оказавшихся случайными участниками события, и т. п. [5, с. 17]. Центральным звеном механизма преступления, в котором отражается факт использования информационных технологий, является способ совершения преступления, который, в свою очередь, обусловливает формирование иных специфичных элементов механизма, таких как механизм следообразования, средство совершения преступления и иные.

Нами предприняты попытки раскрыть наиболее часто встречающиеся способы использования ИТ-технологий в механизме преступной деятельности. Умение ориентироваться в разнообразии ИКТ, особенностях их работы, навык определения слабых, уязвимых сторон позволят в дальнейшем анализировать возникающие следственные ситуации, выдвигать актуальные версии и использовать весь потенциал правоохранительной системы для успешного выявления, раскрытия и предупреждения преступлений, совершаемых с использованием ИКТ.

Информационно-коммуникационные технологии в криминалистике и их значение в формировании механизма преступления

Не вдаваясь в подробную классификацию видов и классов различных ИТ-технологий, по-

[1] Правительственная комиссия одобрила дорожную карту развития 5G в России // ООО «МИЦ «Известия» : сайт. URL: https://iz.ru/1089281/2020-11-19/pravitelstvennaia-komissiia-odobrila-dorozhnuiu-kartu-razvitiia-5g-v-rossii (дата обращения: 07.01.2024).

пробуем разобрать данные технологии с точки зрения криминалистики и механизма преступления, возможности их использования в преступной деятельности – от самого простого способа до более сложного.

Мобильные телефоны, персональные компьютеры, ноутбуки, планшеты и другие компьютерные устройства, использующие электронную или информационно-телекоммуникационную сети, являются основными средствами совершения преступлений в сфере ИКТ. Следует отметить, что, в соответствии с Постановлением Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[1], понятия электронной и информационно-телекоммуникационной сетей не разграничиваются, и сеть Интернет является одним из их видов, представляя собой технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Использование указанных устройств и сетей позволяет реализовать более сложные схемы преступной деятельности, которые сложно повторить при личном общении, так как дистанционный (удаленный) формат общения является самым простым способом анонимизации личности и минимизирует риск быть идентифицированным. В последнее время становится популярным мошенничество с применением навыков «социальной инженерии» [4, с. 108], совершаемое в основном лицами, отбывающими наказание в местах лишения свободы. Так, осужденный, отбывающий наказание в ФКУ <…> ГУФСИН России, используя мобильный телефон, совершил 188 фактов мошенничества. Также есть данные о лицах, совершивших 173, 95 и 52 мошенничества [2, с. 67]. К сожалению, большинство таких преступлений остаются нераскрытыми.

Мобильные телефоны, компьютерные устройства, подключенные к информационно-телекоммуникационным сетям, дают возможность использовать разнообразные современные способы совершения преступлений. Назовем некоторые из них.

Самый простой и наиболее часто встречаемый способ – это изменение номера вызывающего абонента. Так, например, преступники присваивают официальные номера, используемые банками или другими государственными учреждениями, например номер «900».

Для изменения идентификационного номера вызывающего абонента используют возможности технологий VoIP (Voice over Internet Protocol) или IP-телефонии, позволяющих пользователям совершать звонки через сеть Интернет и изменять идентификатор вызывающего абонента на любой номер по своему выбору, а также аппаратных спуфинговых (spoofing) устройств.

Более того, в сети Интернет существуют организации, оказывающие услуги подделки идентификатора вызывающего абонента, позволяя пользователям вводить номер, который они хотят отобразить, и номер, на который они хотят позвонить.

В настоящее время на территории страны операторы сотовой связи активно подключаются к системе «Антифрод», которая позволяет проверить, действительно ли вызов совершается в данный момент с номера определившегося оператора, однако на сегодняшний день ее использование в полной мере осуществляется лишь половиной от общего количества операторов в России, что хоть и снизило количество преступлений, совершаемых с использованием подмены абонентского номера, но не исключило их вообще.

Также нередко преступники генерируют изображения и голос человека с помощью технологии искусственного интеллекта, так называемые дипфейки, позволяющие изменять лицо или его выражение, цвет кожи и прическу, синхронизировать движения губ на видео с аудиозаписью голоса и т. д. В настоящий момент российское законодательство не содержит такого понятия, как «дипфейк», однако это не означает, что использование данной технологии с нарушением чужих прав не повлечет за собой юридическую ответственность, например, в соответствии со ст. 152.1 ГК РФ использование изображения гражданина допускается только с его согласия, а после смерти с согласия родственников, УК РФ содержит ст. 159, предусматривающую ответственность за мошеннические действия.

Далее следует отметить, что нередко преступники используют технологии голосовых вызовов через сеть Интернет посредством популярных социальных сетей, мессенджеров,

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет : постановление Пленума Верховного Суда РФ от 15 дек. 2022 г. № 37 // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 17.01.2024).

например, таких как Viber, WhatsApp[1], ООО «ВКонтакте», Facebook Messenger[2], Wire и т. д. Для преступников есть ряд преимуществ в использовании данных мессенджеров для телефонных звонков и текстовых сообщений. При осуществлении звонка или отправке текстовых сообщений непосредственно через оператора связи последний, в соответствии с законодательством, обязан в течение трех лет хранить информацию о действиях абонента (звонки, смс и их дата, адресат и т. п.), а также до полугода хранить запись разговора, содержание сообщений или пересылаемые медиафайлы, т. е. исчерпывающую информацию о всех действиях, которые осуществлял абонент (ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[3]). Данные сведения предоставляются правоохранительным органам и могут использоваться в качестве доказательств преступной деятельности либо служить вспомогательной оперативной информацией. Указанные требования обязательны для исполнения зарегистрированными операторами связи, осуществляющими деятельность на территории Российской Федерации.

На практике отмечены случаи использования мессенджеров, с помощью которых автоматизируются программные процессы Bot (виртуальный робот, робот-бот), не имеющие привязки к конкретному лицу, но в то же время предоставляющие возможность общения с потребителями. Телеграм-бот не требует постоянного нахождения человека за компьютером, автономно, по заданному алгоритму выполняет различные действия, что значительно снижает количество точек соприкосновения между участниками сообществ, а также затрудняет выявление их деятельности [1, с. 123].

Кроме того, преступники применяют возможности изменения IP-адреса, представляющего собой уникальный идентификатор, назначенный каждому устройству, подключенному к сети Интернет. IP-адрес может дать представление о местоположении устройства, связанного с сетью Интернет, однако многие интернет-провайдеры используют метод маскирования IP-адресов, так что местоположение устройства, определенное по IP-адресу, может быть неточным. Кроме того, IP-адрес не привязан к конкретному человеку, использующему это устройство, а также одно и то же устройство (общий компьютер в интернет-кафе и т. д.) могут использовать несколько человек.

Для возможности идентификации человека по IP-адресу необходима дополнительная информация, такая как имя пользователя и пароль для входа в систему, либо информация из браузера или других используемых преступником приложений.

Далее отметим использование технологии геолокации, позволяющей определить местоположение устройств в Интернете, их IP-адреса, подключенные сети Wi-Fi и применение сведений о метаданных. Это могут быть текстовые файлы, схемы, чертежи, фотографии, видео, какие-либо программы. Анализ метаданных позволяет получить ценную информацию о потенциальных потерпевших. Если это физическое лицо, в зависимости от типа файла можно узнать различную информацию. Для фотографий это модель устройства, с помощью которого сделано фото, и его технические характеристики; размер фотографии; дата и время съемки; геолокация, если у камеры есть доступ к ней; автор фотографии; расстояние от камеры в момент съемки; теги и ключевые слова, описывающие содержание фото (создаются автором). Для видеофайлов набор идентичный и может дополняться в зависимости от модели устройства. Из текстовых файлов можно получить следующую информацию: автор документа (если пользователь его указал), формат файла, название файла, даты создания и редактирования файла, размер файла. Важен и сам способ передачи файлов. Если файлы передаются через почтовые сервисы (Gmail, «Яндекс. Почта», Mail.ru, Protonmail), то они остаются неизменными, соответственно, метаданные сохраняются в полном объеме. Если мы используем мессенджеры, как правило, есть два варианта передачи: «отправить как фото» и «отправить как файл». При отправке фотографии как файла метаданные остаются. При отправке «как фото» большинство популярных мессенджеров удаляют метаданные с отправляемых изображений.

Если же деятельность преступников направлена на сайт или приложение какой-либо организации, изучая метаданные с этих источников, можно узнать адреса корпоративной электронной почты, операционную систему, которую используют сотрудники организации,

[1] Принадлежит экстремистской организации Meta, запрещен на территории Российской Федерации.

[2] Принадлежит экстремистской организации Meta, запрещен на территории Российской Федерации.

[3] О связи : федер. закон от 7 июля 2003 г. № 126-ФЗ (послед ред.) // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_43224/ (дата обращения: 11.01.2024).

и т. п. Собранная информация может помочь преступникам осуществить различные виды атак с использованием методов социальной инженерии (например, зная модель фотоаппарата, можно завести разговор с фотолюбителем или же сделать рассылку писем с вредоносным ПО на адреса электронной почты работников определенной организации).

Нередко преступники используют в противоправных целях информацию, полученную из открытых источников – социальных сетей. Многие пользователи добровольно размещают личную информацию: Ф. И. О., возраст, образование, религиозные убеждения, увлечения, статусы (краткие заметки) и т. д. С возрастом или трудоустройством в какую-либо организацию или с занятием ответственной должности пользователи часто корректируют либо вообще удаляют информацию о себе. Однако не все пользователи осведомлены о существовании так называемого Архива интернета (англ. Internet Archive) – некоммерческой организации, основанной в 1990-х гг. в США. Главной заявленной целью Архива является предоставление всеобщего доступа к накопленной в интернете информации. Коллекция Архива интернета состоит из множества подколлекций архивированных веб-сайтов, оцифрованных книг, аудио- и видеофайлов, игр, программного обеспечения. Один из проектов Архива интернета – это сервис Wayback Machine, расположенный по адресу http://web.archive.org/. Данный сервис периодически сохраняет страницы в сети Интернет. При изменении информации или даже удалении самой страницы она остается в архивах сервиса. Введя адрес сайта, можно посмотреть, на какие даты есть «снимки» сайта, и просмотреть их. Полученная таким образом информация также может быть использована для атак с использованием методов социальной инженерии, в том числе для шантажа лица распространением нежелательной информации о нем.

Некоторые наиболее сложные технологии, используемые в преступной деятельности

К наиболее сложным технологиям следует отнести перехват передаваемых сообщений в мессенджерах или трафика в сети. Один из способов – взлом аккаунта пользователя. Преступники могут пытаться получить доступ к аккаунту, используя уязвимости в программном обеспечении или социальные инженерные атаки, такие как подделка веб-сайтов или фишинговые электронные письма. В этом случае преступник создает фальшивую страницу входа на сайт или приложение, которая по визуальному оформлению похожа на официальную платформу, и просит пользователя ввести учетные данные для входа. Как только пользователь вводит свои учетные данные, преступник получает доступ к его учетной записи и может перехватить информацию, находящуюся на платформе (персональные данные, сообщения, номера банковских карт), а также воспользоваться личным кабинетом гражданина и осуществлять преступные действия от его имени.

Для защиты от фишинга важно всегда проверять адрес веб-сайта, прежде чем вводить учетные данные, и быть осторожным с электронными письмами или сообщениями, в которых запрашивается конфиденциальная информация. Кроме того, использование двухфакторной аутентификации и регулярная смена паролей также могут повысить безопасность пользователя.

Для перехвата трафика в сети могут также использоваться вредоносные программы или оборудование, такие как шпионские программы или промежуточные прокси-серверы, чтобы перехватывать и читать переписку. Например, атаки «человек посередине» (от англ. Man-in-the-middle, MITM) – распространенный метод, используемый преступниками для перехвата сообщений в платформах обмена мгновенными сообщениями. Этот тип атаки заключается в том, что злоумышленник перехватывает связь между двумя пользователями, обычно путем создания поддельной сети, которая кажется истинной сетью, и обманом заставляет пользователя подключиться к ней. Как только пользователь подключается к поддельной сети, преступник получает доступ к конфиденциальной информации, включая сообщения, отправленные через платформу обмена мгновенными сообщениями.

Для защиты от MITM-атак важно использовать безопасные сети, такие как виртуальные частные сети (VPN), которые шифруют данные, передаваемые через сеть Интернет. Кроме того, использование шифрования на платформах обмена мгновенными сообщениями также может помочь защититься от этих атак. Обнаружить данный тип атаки можно по следующим признакам: неожиданное или повторяющееся отклонение от доступа к странице, поскольку преступники принудительно отключают пользователей, чтобы перехватить имя пользовате-

ля и пароль при повторной попытке подключения; подозрительные адреса в строке браузера, например www.go0gle.com вместо www.google.com, что свидетельствует о перехвате DNS[1].

Кроме того, на практике не редки случаи использования вредоносного ПО – это тип программного обеспечения, предназначенный для причинения вреда компьютеру или устройству. Использование вредоносного ПО в преступных целях позволяет получить доступ к устройству пользователя и конфиденциальной информации, включая сообщения, отправляемые через платформы обмена мгновенными сообщениями.

Известны случаи использования программ для удаленного доступа к телефону. Данные программы позволяют получить физический контроль над устройством (при оказании помощи в настройке телефона, установке приложений и т. п.), а также возможность удаления учетной записи при обнаружении устройства правоохранительными органами. Данный способ используется при совершении телефонного мошенничества. Например, пользователю поступает телефонный звонок, в котором мошенник сообщает о том, что неизвестное лицо из другого региона пытается войти в его личный кабинет приложения банка ВТБ. Преступники, выясняя информацию об использовании приложения банка, сведения о его обновлении, отправляют СМС-сообщение с кодом и требуют подтверждения факта получения такого СМС и дальнейшего обновления используемого приложения.

Активное развитие информационно-коммуникационных технологий и внедрение их в повседневную жизнь общества [3, с. 85] значительно упрощают преступникам задачу по совершению противоправных деяний, так, например, при использовании в устройстве операционной системы Android клиенту предлагают войти в магазин приложений Google Play, найти и скачать приложение «Поддержка ВТБ».

В первую очередь предлагается скачать приложения для удаленного управления устройством, установление которых и их активация абонентом путем ввода кода дают преступнику возможность получить удаленный контроль над смартфоном и произвести любые доступные операции (хищение персональных данных, перевод денег с приложений банков, рассылка писем от имени и т. п.).

Кроме того, преступники могут взломать сеть Wi-Fi, т. е. осуществить доступ к ресурсам сети или произвести кражу конфиденциальной информации. Существует несколько стандартов сетей Wi-Fi – WEP, WPA/WPA2, WPA3, сменяющих друг друга для обеспечения безопасности пользователей и увеличения скорости, но не все компьютерные устройства поддерживают современные стандарты, обеспечивающие безопасное пользование. Кроме того, WEP – это устаревший протокол безопасности, который легко взламывается, а WPA и WPA2 – защищенный доступ Wi-Fi; являясь более безопасными протоколами, они все же могут быть уязвимы для атак, если сетевой пароль слаб или сеть настроена неправильно. WPA3 – это новый стандарт безопасности Wi-Fi-сетей, представленный Wi-Fi Alliance в 2018 г., который является наиболее защищенным. Кроме того, возможно создать и поддельную сеть Wi-Fi с именем, похожим на настоящую сеть Wi-Fi (атака «злой двойник» (Evil Twin Attack)), при подключении к которой предоставляется доступ к информации, хранящейся на компьютерном устройстве.

В завершении укажем на использование интернет-браузера TOR (The Onion Router) – бесплатного веб-браузера с открытым исходным кодом, который предназначен для защиты конфиденциальности и анонимности пользователей при просмотре веб-страниц, работающего путем маршрутизации интернет-трафика через сеть серверов, также известных как узлы. TOR базируется на принципе луковой маршрутизации, который позволяет передавать данные через сеть узлов (нод), чтобы путь нельзя было отследить. Каждый узел в сети TOR представляет собой промежуточный пункт для передачи данных, которые затем передаются далее до конечной цели. Это означает, что никто не может узнать источник или пункт назначения данных, так как каждый узел в сети видит только предыдущий и следующий узлы, а не источник и пункт назначения. Это затрудняет перехват и чтение интернет-трафика пользователя. В свою очередь, зашифрованный трафик маршрутизируется через ряд узлов в сети TOR. Каждый узел в сети удаляет один уровень шифрования, а затем передает трафик следующему узлу. Конечный узел в сети, известный как узел выхода, расшифровывает трафик и отправляет его на целевой веб-сайт. Узел выхода действует как прокси-сервер пользователя, поэтому при анализе информации о взаимодействии с ресурсом отображается трафик, поступающий с узла вы-

[1] Man-in-the-Middle: советы по обнаружению и предотвращению // Хабр : веб-сайт. URL: https://habr.com/ru/companies/varonis/articles/526632/ (дата обращения: 11.01.2024).

хода, а не с устройства пользователя. Поскольку интернет-трафик пользователя маршрутизируется через несколько узлов сети, веб-сайт может видеть только IP-адрес выходного узла, а не фактический IP-адрес пользователя. Это затрудняет отслеживание физического местоположения пользователя.

С точки зрения конфиденциальности и анонимности браузер TOR обеспечивает высокую степень защиты, но он не является надежным. Например, если пользователь посещает вебсайт, который требует от него ввода личной информации, такой как его имя и адрес, эта информация все равно может быть отслежена и связана с пользователем.

Подводя определенный итог, можно констатировать, что в современный мир уже прочно внедрены различные информационно-коммуникационные технологии, которые внесли свои коррективы в развитие преступного мира. Раскрытие, расследование и предупреждение преступлений, совершаемых с использованием ИКТ, требуют полноценного и всестороннего анализа, при этом следует учитывать, что деятельность правоохранительных органов в рамках проверки сообщения о преступлении и осуществления предварительного расследовании для каждого конкретного способа совершения противоправного деяния будет сильно отличаться для разных направлений. Однако некоторые тактические приемы и программные продукты, в том числе находящиеся в открытом доступе, будут идентичны на первоначальном этапе расследования для всех преступлений, совершаемых в информационно-телекоммуникационном пространстве.

СПИСОК ЛИТЕРАТУРЫ

1. Гаврилин Ю. В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4 (56). С. 122–129.

2. Литвинов Н. Д., Федоров А. Н. Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. № 12 (32). С. 63–72.

3. Милюс А. И. Значимые аспекты получения видеозаписи с точки зрения источника криминалистически значимой информации при расследовании краж нефти и нефтепродуктов при их хранении и транспортировке на объектах топливно-энергетического комплекса // Актуальные проблемы криминалистики и судебной экспертизы : сб. материалов Междунар. науч.-практ. конф. Иркутск, 16–17 марта 2023 г. Иркутск : Вост.-Сиб. ин-т МВД России, 2023. С. 85–87.

4. Панфилова О. А. Некоторые вопросы обеспечения безопасности на объектах уголовно-исполнительной системы и организации борьбы с телефонными мошенничествами // Вестник Воронежского института ФСИН России. 2022. № 3. С. 107–115.

5. Россинская Е. Р. Криминалистика : учеб. для вузов. М. : Норма-ИНФРА-М, 2016. 464 с.

6. Рудых А. А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий : дис. … канд. юрид. наук. Ростов-на-Дону, 2020. 239 с.

7. Теория информационно-компьютерного обеспечения криминалистической деятельности / Е. Р. Россинская, А. И. Семикаленова, И. А. Рядовский, Т. А. Сааков. М. : Проспект, 2022. 254 с.

8. Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений / О. П. Грибунов [и др.]. Иркутск : Иркут. юрид. ин-т (филиал) Ун-та прокуратуры РФ, 2023. 170 с.

REFERENCES

1. Gavrilin Yu.V. Protivodejstvie cifrovoj transformacii narkoprestupnosti (po itogam Vserossijskogo onlajn-seminara) [Countering the digital transformation of drug crime (based on the results of the All-Russian online seminar)]. *Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia*, 2020, no. 4 (56), pp. 122-129. (in Russian)

2. Litvinov N.D., Fedorov A.N. *Osobennosti, prichiny i tendencii razvitiya distancionnogo moshennichestva licami, otbyvayushchimi nakazanie v mestah lisheniya svobody* [Features, causes and trends in the development of remote fraud by persons serving sentences in prison]. *Scientific research publications*, 2015, no. 12 (32), pp. 63-72. (in Russian)

3. Milyus A.I. Znachimye aspekty polucheniya videozapisi s tochki zreniya istochnika kriminalisticheski znachimoj informacii pri rassledovanii krazh nefti i nefteproduktov pri ih hranenii i transportirovke na ob"ektah toplivno-energeticheskogo kompleksa [Significant aspects of obtaining video recordings from the point of view of a source of forensically significant information when investigating thefts of oil and petroleum products during their storage and transportation at the facilities of the fuel and energy complex]. *Aktualnye problemy kriminalistiki i sudebnoj ekspertizy* [Current problems of forensic science and forensic examination]. Collection of materials of the international scientific and practical conference, Irkutsk, March 16–17, 2023. Irkutsk, East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2023, pp. 85-87. (in Russian)

4. Panfilova O.A. Nekotorye voprosy obespecheniya bezopasnosti na ob"ektah ugolovno-ispolnitelnoj sistemy i organizacii borby s telefonnymi moshennichestvami [Some issues of ensuring security at the facilities of the penal system and organizing the fight against telephone fraud]. Vestnik Voronezhskogo instituta FSIN Rossii [Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia], 2022, no. 3, pp. 107-115. (in Russian)

5. Rossinskaya E. R. *Kriminalistika* [Forensics]. Textbook for universities. Moscow, Norma-INFRA-M, 2016, 464 p. (in Russian)

6. Rudykh A.A. *Informacionno-tekhnologicheskoe obespechenie kriminalisticheskoj deyatel'nosti po rassledovaniyu prestuplenij v sfere informacionnyh tekhnologij* [Information and technological support of forensic activities in the investigation of crimes in the field of information technology]. Cand. sci. diss. Rostov-on-Don, 2020, 239 p. (in Russian)

7. Rossinskaya E.R., Semikalenova A.I., Ryadovsky I.A., Saakov T.A. *Teoriya informacionno-kompyuternogo obespecheniya kriminalisticheskoj deyatelnosti* [Theory of information and computer support for criminalistic activities]. Moscow, Prospekt, 2022, 254 p. (in Russian)

8. Gribunov O.P. et al. *Cifrovaya valyuta i cifrovye finansovye prava kak predmet i sredstvo soversheniya prestuplenij* [Digital currency and digital financial rights as a subject and means of committing crimes]. Irkutsk, Irkutsk Law Institute (branch) of the University of the Prosecutor's Office of the Russian Federation Publ., 2023, 170 p. (in Russian)

Статья поступила в редакцию 11.03.2024; одобрена после рецензирования 11.05.2024; принята к публикации 04.09.2024.

Received on 11.03.2024; approved on 11.05.2024; accepted for publication on 04.09.2024.

Усачев Сергей Игоревич – кандидат юридических наук, доцент кафедры криминалистики, Восточно-Сибирский институт МВД России (Россия, 664071, г. Иркутск, ул. Лермонтова, 110), ORCID: 0000-0002-4306-0535, РИНЦ AuthorID: 994377, e-mail: ysachef@list

Usachev Sergey Igorevich – Candidate of Juridical Sciences, Associate Professor of the Department of Criminalistics, East-Siberian Institute of the MIA of Russia (110, Lermontov st., Irkutsk, 664071, Russian Federation), ORCID: 0000-0002-4306-0535, RSCI AuthorID: 994377, e-mail: ysachef@list

Усачева Екатерина Анатольевна – кандидат юридических наук, доцент кафедры организации и методики уголовного преследования, Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации (Россия, 664035, г. Иркутск, ул. Шевцова, 1), ORCID: 0000-0002-4770-1133, РИНЦ AuthorID: 874860, e-mail: malykhina_ek@mail.ru

Usacheva Ekaterina Anatolievna – Candidate of Juridical Sciences, Associate Professor of the Department of Organization and Methods of Criminal Prosecution, Irkutsk Law Institute (Branch) of the University of the Prosecutor's Office of the Russian Federation (1, Shevtsova st., Irkutsk, 664035, Russian Federation), ORCID: 0000-0002-4770-1133, RSCI AuthorID: 874860, e-mail: malykhina_ek@mail.ru

Вклад авторов

Усачев Сергей Игоревич – концепция исследования (формирование идеи, формулировка ключевых целей и задач), редактирование статьи (внесение замечаний), написание текста (обсуждение результатов и выводы), утверждение окончательного варианта статьи.

Усачева Екатерина Анатольевна – сбор и обработка материала, статистическая обработка данных, работа с нормативными актами и методическими материалами, написание текста (материалы и методы исследования, результаты исследования).