СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ И ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Всероссийская научно-практическая конференция

(Москва, 10 декабря 2020 года)

Москва, 2021

УДК 343
ББК 67.408
П 83

П 83 Противодействие киберпреступлениям и преступлениям в сфере высоких технологий: материалы Всероссийской научно-практической конференции (Москва, 10 декабря 2020 года) / Под общ. ред. Д.Н. Кожухарика. М.: Московская академия Следственного комитета Российской Федерации, 2021. – 260 с.

Редакционная коллегия:

Кожухарик Д.Н., и.о. ректора Московской академии Следственного комитета Российской Федерации, полковник юстиции, кандидат юридических наук, доцент, почетный сотрудник Следственного комитета Российской Федерации.

Бычков В.В., декан факультета повышения квалификации Московской академии Следственного комитета Российской Федерации, полковник юстиции, кандидат юридических наук, доцент, почетный сотрудник Следственного комитета Российской Федерации.

Дмитриева Л.А., ученый секретарь Московской академии Следственного комитета Российской Федерации, полковник юстиции, кандидат психологических наук, доцент.

Саркисян А.Ж., руководитель редакционно-издательского отдела Московской академии Следственного комитета Российской Федерации, майор юстиции, кандидат юридических наук, доцент.

УДК 343
ББК 67.408

Сборник сформирован по материалам, представленным на Всероссийскую научно-практическую конференцию, проведенную заочно в Московской академии СК России 10 декабря 2020 года.

Конференция организована Московской академией СК России при участии ведущих вузов, ученых, специалистов, сотрудников правоохранительных органов России.

Сборник представляет интерес для юристов – учёных и практиков.

Редакционная коллегия обращает внимание на то, что научные подходы и идеи и взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

© Московская академия СК России, 2021

Всероссийская научно-практическая конференция
«Противодействие киберпреступлениям
и преступлениям в сфере высоких технологий»
(10 декабря 2020 года)

10 декабря 2020 года состоялась Всероссийская научно-практическая конференция «Противодействие киберпреступлениям и преступлениям в сфере высоких технологий», проведенная в формате видеоконференцсвязи с использованием программного обеспечения Zoom.

Конференция организована во взаимодействии Санкт-Петербургской и Московской академий СК России.

Регламент работы форума предусматривал пленарную часть, секционные заседания и круглый стол. Программа пленарного заседания и секций включала доклады научных работников и представителей профессорско-преподавательского состава ряда образовательных учреждений. Участниками форума стали 9 докторов наук и 30 кандидатов наук.

В работе круглого стола приняли участие 53 работника органов следствия, суда, прокуратуры, иных правоохранительных и государственных органов, экспертных и технических подразделений, представители ПАО «Мегафон», ПАО «Ростелеком» и др. Предметом обсуждения были определены прикладные проблемы профессиональной деятельности специалистов.

Сотрудники Московской академии СК России выступили на пленарном заседании, слушателями которого стали 46 участников. Значительный интерес вызвал доклад профессора кафедры предварительного расследования доктора юридических наук доцента Бертовского Льва Владимировича, представившего углубленный анализ проблем развития уголовного процесса и криминалистики в эпоху высокотехнологичного права. Заведующий кафедрой криминалистики кандидат юридических наук доцент Скобелин Сергей Юрьевич обозначил новые подходы в расследовании киберпреступлений.

Профессор кафедры уголовного права и криминологии Перов Валерий Александрович выступил сомодератором работы секции «Правовые и процессуальные аспекты противодействия киберпреступлениям и преступлениям в сфере высоких технологий», в рамках которой ведущий научный сотрудник научно-исследовательского отдела доктор юридических наук доцент Голоскоков Леонид Викторович выступил с докладом о модернизации парадигмы уголовного права в сфере противодействия преступлениям в сфере высоких и иных технологий.

В работе секционного заседания «Вопросы расследования киберпреступлений и преступлений в сфере высоких технологий» прозвучало содержательное выступление старшего научного сотрудника научно-исследовательского отдела кандидата юридических наук доцента Валова Сергея Владимировича об организационном обеспечении расследования уголовных дел о киберпреступлениях. Доцент кафедры криминалистики кандидат юридических наук Лебедева Анна Андреевна убедительно представила расследование киберпреступлений как новую функцию СК России.

Материалы работы форума будут опубликованы в сборнике научных статей, подготовленных участниками.

Организационный комитет конференции

А.Г. Апасова

Некоторые вопросы обеспечения корпоративной безопасности

Аннотация. В статье рассматривается некоторые аспекты защиты от рейдерских атак на современном этапе развития Российской Федерации. А также рассмотрено понятие «рейдерство», «корпоративная безопасность. Это позволило сформулировать ряд предложений по совершенствованию законодательства.

Ключевые слова: корпоративный захват, гринмейл, рейдер, рейдерство, корпоративная безопасность.

Согласно СМИ Россия к августу 2020 года потеряла 1 млн 95 тыс. 423 малых и средних предприятий, среди которых половину занимают, потерпевшие падение в связи с рейдерскими атаками. Так же в России еще за 2019 год количество уголовных дел о таком незаконном перехвате бизнеса за год выросло до 135%. При этом бизнес обычно начинает принимать меры, когда уже поздно. Коронокризис 2020 года привет к тому, что в Алтайском крае по данным Росстата РФ закрылись более 3 тысяч малых предприятий, конечно, добавилось новых 6500 самозанятых, но это уже другие объемы. Конечно, кризисами всегда пользуются банки, обогащаясь на залоговом имуществе, более рассудительные конкуренты, занимая освободившиеся рынки соседа рынки, выкупая за бесценок активы и переманивая работников.[1] Но это относительно законные методы работы бизнес-падальщиков. Сегодня же эксперты прямо говорят, что учащаются случаи «активных» рейдерских захватов. В крае за прошлые годы достаточно громко прозвучали процессы по ОАО «Соболь», гостинице «Александр-Хаус», ООО «Виктория-Агросервис» и многие другие, к ответственности виновные были привлечены, но это лишь капля в море.[2] Одним из «перспективных» направлений сегодня может выступать присвоение имущества реформируемых МУП и ГУП, которые начнут сокращать со следующего года. Поэтому в подобные кризисные периоды нужна не только поддержка органов власти, но и грамотное управление фирмой, санация возможных рисков ее деятельности. При этом мы понимаем, что профилактика всегда менее затратна и более эффективна.

Следует констатировать, что современное российское законодательство отстает от социально-экономических реалий и практически не содержит ответственности за «гринмейл», размывание доли в обществе миноритариев, захват рынка, агрессивное переманивание клиентской базы и сотрудников и прочие инструменты корпоративных войн. На жаргоне рейдеров отнимается скорее не имущество, а «ключевой актив», которым может быть ноу-хау, доля рынка, персонал, и даже модель бизнеса. И это происходит в рамках правовой базы!

Поэтому мы сформировали некоторые рекомендации для предпринимателей, направленные на повышение уровня экономической безопасности фирмы:

---

[1] Хужин А.М. Противодействие созданию «дружественных кредиторов» в процедурах банкротства // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 217-221.

[2] Сайт СУ Следственного комитета РФ по АК // https://altai-krai.sledcom.ru/news.

- постоянный мониторинг правового пространства (достаточно использования открытых баз данных судебной системы, ФНС РФ, ФССП РФ и других официальных источников);[1]

- разработка системы мер по тщательной проверке документов, поступающих на регистрационные действия в ФНС России, Росреестр, Минюст и проч.;

- подготовка квалифицированных кадров – в области экономико-правовой безопасности;

- принятие профилактических мер – проверка контрагентов, обременение в пользу собственников наиболее ликвидного имущества, что затруднит его изъятие, создание специального порядка смены генерального директора и проч.;

- тщательная проработка уставных документов организации;

- оказание органами местного самоуправление конкретных мер поддержки для кризисных отраслей, разработка рекомендаций по снижению рисков.

Делая вывод из всего вышесказанного, можно говорить о наличии существенной проблемы обеспечения безопасности от рейдерских атак в России, наличие которой представляет реальную угрозу экономической и национальной безопасности.

Для решения данной проблемы, следует ликвидировать недоработки в действующем законодательстве и исправить все недочеты, которые допускают собственники предприятий, так как именно эти моменты в основном дают рейдерам «зеленый свет» для захвата.

Требуется тщательная научная проработка и фиксация в законодательстве понятия «рейдерская атака» с использованием актуальной ситуации в экономике. Это можно сделать, например, путем заключения правовой нормы в уголовном законе, которая бы выделяла «рейдерство» как отдельно уголовно-наказуемое деяние. Оно может включать «корпоративный шантаж» или «гринмэйл», корпоративные атаки.

Для полной или частичной ликвидации рейдерства можно повысить число грамотных специалистов в сфере экономической безопасности, способных обеспечить как соответствующую профилактику, так и грамотную защиту.

Так же возможно проведение подробного анализа изучения иностранного законодательства в области регулирования рейдерских атак, с целью заимствования эффективных мер, а также сопоставление с действующим в России корпоративным законодательством и создание собственного комплекса правовых норм, направленных на защиту корпоративных отношений и противодействие незаконным захватам и давлению на имущественные комплексы юридических лиц.

---

[1] Чесноков А.А. Публичность имущественного реестра как гарантия безопасности добросовестного приобретателя // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 3 (47). С. 171-176.

Список использованных источников

1. Сайт СУ Следственного комитета РФ по АК // https://altai-krai.sledcom.ru/news.
2. Хужин А.М. Противодействие созданию «дружественных кредиторов» в процедурах банкротства // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 217-221.
3. Чесноков А.А. Публичность имущественного реестра как гарантия безопасности добросовестного приобретателя // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 3 (47). С. 171-176.

О.Р. Афанасьева

Состояние и тенденции развития преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий

Аннотация. Киберэкстремизм относится к одной из современных угроз национальной безопасности. В статье приводятся основные факторы, детерминирующие развитие киберэкстремизма. Кроме этого, анализируются статистические данные ФКУ «ГИАЦ МВД России», характеризующие состояния и тенденций развития как преступлений экстремистской направленности в целом, так и преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий.

Ключевые слова: экстремизм, киберэкстремизм, несовершеннолетние, социальная напряженность.

Экстремизм, представляет собой «одну из наиболее сложных проблем современного российского общества, в виду многообразия его проявлений и неоднородного состава экстремистских организаций, деятельность которых угрожает национальной безопасности Российской Федерации»[1]. В условиях перемещения ряда видов социальной деятельности (общение, обучение, дистанционная работа, банковские операции и т.д.) в виртуальное пространство особое внимание ученых и правоохранительных органов привлек киберэкстремизм, признаваемый новой формой экстремизма, и предполагающий использование для достижения своих целей компьютеры и электронные сети, новейшие коммуникационные технологии. На этом акцентируется внимание и в утвержденной Указом Президента РФ 29 мая 2020 года «Стратегии противодействия экстремизму в Российской Федерации до 2025 года» (далее по тексту- Стратиегия), в которой отмечается, что «основным средством для связи экстремистских организаций и вербовки их новых приспешников стали информационно-телекоммуникационные сети, в том числе интернет»[2].

[1] Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СЗ РФ. 2020. № 22. ст. 3475.
[2] Там же.

Предполагается, что развитие киберэкстремизма обусловлено[1]:

нарастанием социальной напряженности и протестной активности в обществе, особенно на фоне социально-экономических проблем, обострившихся в период развития пандемии коронавируса COVID-19;

развитием IT- технологий, ростом IT-грамотности населения, доступности IT-технологий, имеющих важное значение для развития киберэкстремизма, использующего «компьютерные сети для пропаганды своих взглядов, вербовки сообщников, размещения руководств по организации терактов, психологического терроризма, сбора информации о потенциальных объектах шантажа, подготовки террористов, пропаганды расовой, религиозной и других форм нетерпимости»[2];

особенностями молодежи как возрастной группы, склонной к протестным проявлениям, участию в несанкционированных митингах.

О негативной тенденции развития киберэкстремизма в Российской Федерации свидетельствуют результаты анализа официальных статистических данных, согласно которым в России отмечается тенденция их роста.

Таблица 1.

Динамика зарегистрированных преступлений экстремистской направленности в Российской Федерации в 2018–2020 годах

Преступления	2018	2019	2020
Публичные призывы к осуществлению экстремистской деятельности (Ст. 280 УК РФ)	269	278	367
Публичные призывы к осуществлению экстремистской деятельности (Ст. 280 УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	253	257	340
Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (Ст. 280.1 УК РФ)	13	9	17
Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (Ст. 280.1 УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	10	6	8
Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (Ст. 282 УК РФ)	780	18	63
Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (Ст. 282 УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	733	12	49
Всего преступлений экстремистской направленности	1265	585	833

[1] Саркисян А.Ж., Коимшиди Г.Ф. Факторы, определяющие состояние преступности в России // Расследование преступлений: проблемы и пути их решения. 2016. № 2 (12). С. 54-61.

[2] Гаврилова И.В. Молодежный киберэкстремизм и кибертерроризм как угроза безопасности электронной информационно-образовательной среды университета// В сб.: Новые информационные технологии в образовании. материалы VIII Международной научно-практической конференции. Российский государственный профессионально-педагогический университет. 2015. С. 296-298.

Так, в 2020 году посредством информационно-телекоммуникационных технологий, в том числе сеть Интернет, было совершено 92,64% факта публичных призывов к осуществлению экстремистской деятельности; 47,05 % - публичных призывов к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации и 77,7 % - возбуждения ненависти либо вражды, а равно унижение человеческого достоинства.

При этом, в 2020 году количество публичных призывов к осуществлению экстремистской деятельности (Ст. 280 УК РФ), совершенных с использованием ИТТ, увеличилось на 32,3%, публичных призывов к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (Ст. 280.1 УК РФ), совершенные с использованием ИТТ, - на 33,3%, фактов возбуждения ненависти либо вражды, а равно унижение человеческого достоинства (Ст. 282 УК РФ), совершенные с использованием ИТТ, - на 308,3%.

Таблица 2.

Состояние отдельных видов преступлений экстремистской направленности, совершенных с использование информационно-телекоммуникационных технологий в 2020 году

Преступления	2018	2019	2020	Динамика к 2019 г. +/- в %
Публичные призывы к осуществлению экстремистской деятельности (Ст. 280 УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	253	257	340	+32,30
Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (Ст. $280^{.1}$ УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	10	6	8	+33,3
Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (Ст. 282 УК РФ), совершенные с использованием информационно-телекоммуникационных технологий	733	12	49	+308,3

В структуре преступлений экстремистской направленности в 2020 году преобладали такие составы преступлений, как публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ) (44,06%), в том числе совершенные с использованием ИТТ (40,81%), и организация деятельности экстремистской организации (282^2 УК РФ) (26,17%) (рис.1).

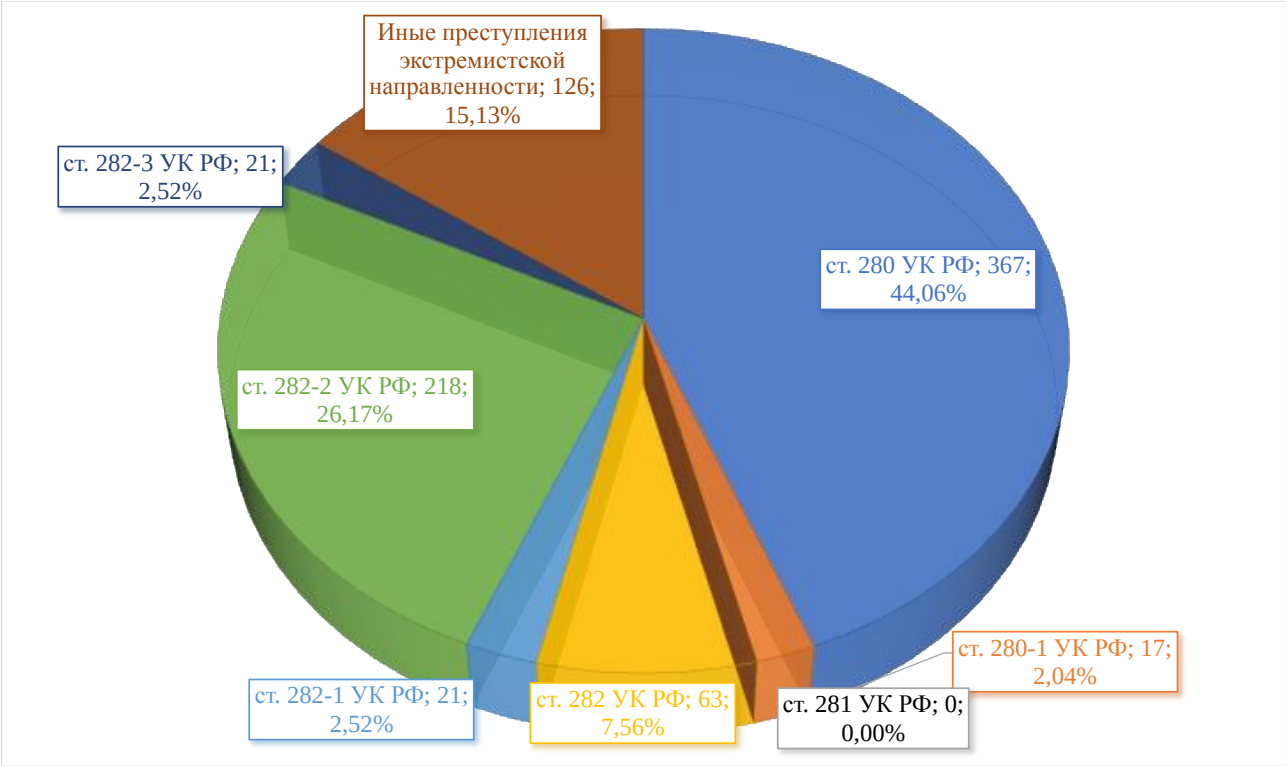


Рис. 1. Структура преступлений экстремистской направленности в Российской Федерации в 2020 году

Рост преступлений экстремистской направленности в 2020 году связывают с совокупностью социальных, экономических и политических факторов, предопределяющих рост экстремистских настроений в обществе. Эксперты полагают, что в современных условиях продолжится перемещение преступной деятельности в виртуальное пространство, что бесспорно способствует распространению идей радикализма, вовлечению в экстремистские сообщества новых членов, в том числе несовершеннолетних и молодежи.

Распространение преступлений экстремистской направленности в информационном пространстве предполагает модернизацию средств и методов противодействия данному виду преступности правоохранительными органами. Е.А. Антонян совершенно справедливо обратила внимание на возможности использования в качестве одного из средств противодействия - технологии блокчейн в различных ее разновидностях и сочетаниях[1]. Думается, что использование технологий блокчейн позволит достигнуть цели и выполнить задачи, определенные в вышеуказанной Стратегии.

В п. 29 Стратегии как документе стратегического планирования в качестве цели государственной политики в сфере противодействия экстремизму определяется «защита основ конституционного строя Российской Федерации, государственной и общественной безопасности, прав и свобод граждан от экстремистских угроз». Думается, что достижение поставленной цели возможно посредством использования блокчейн-технологий, возможности которых безграничны

[1] Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 167-177.

благодаря их уникальным свойствам, которые позволяют обеспечивает децентрализованную сеть для хранения информации, надежно защитить данные от взлома, а следовательно, исключают возможность утечки данных, защищают процесс обмена информацией, а службам безопасности и правоохранительным органам предоставляют дополнительное время для выявления источника опасности и устранения угрозы. Также блокчейн-технологии могут быть использованы при обработке больших массивов информации.

Таким образов, в условиях роста киберугроз, в том числе киберэкстремизма, перед государством встает проблема модернизации средств и методов противодействия преступности, в том числе посредством использования высокотехнологичных цифровых механизмов как блокчейн-технологий.

Список использованных источников

1. Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права. 2019. № 6 (103). С. 167-177.
2. Гаврилова И.В. Молодежный киберэкстремизм и кибертерроризм как угроза безопасности электронной информационно-образовательной среды университета// В сб.: Новые информационные технологии в образовании. материалы VIII Международной научно-практической конференции. Российский государственный профессионально-педагогический университет. 2015. С. 296-298.
3. Саркисян А.Ж., Коимшиди Г.Ф. Факторы, определяющие состояние преступности в России // Расследование преступлений: проблемы и пути их решения. 2016. № 2 (12). С. 54-61.
4. Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года»// СЗ РФ. 2020. № 22. ст. 3475.

Афанасьев П.Б.

Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Аннотация. Согласно Доктрине информационной безопасности Российской Федерации, информационные технологии признаются неотъемлемой частью всех сфер деятельности личности, общества и государства. К сожалению, они стали частью и криминальной деятельности. В статье представлен криминологический анализ официальных статистических данных ФКУ «ГИАЦ МВД России», выделены основные факторы, предопределяющие современные тенденции развития киберпреступности.

Ключевые слова: киберпреступность, информационные технологии, кибербуллинг, информационно-телекоммуникационные технологии.

Развитие информационных технологий породило как положительные тенденции, связанные с их успешным использованием в различных сферах жизнедеятельности общества, так и негативные, сопряженные с их применением как в качестве объекта (предмета) преступления, так и орудия, средства совершения преступления. Использование информационных технологий в преступных целях сопряжено с созданием для государства современных угроз, требующих соразмерного и эффективного ответа.

Стремительное развитие информационно-телекоммуникационных технологий приводят к расширению перечня преступлений, которые возможно совершать с применением IT-технологий. Так, в настоящий момент уже нет сомнений в возможности совершения насильственного преступления посредством IT-технологий. Так, например, кибербуллинг, понимаемый как моральный или физический террор, имеющий социальный и психологический характер, предполагает применение не только систематического и регулярного физического насилия, применяемого к жертве преступления, но и психологического, реализуемого посредством информационно-телекоммуникационных технологий, в том числе социальных сетей[1]. Подобное расширение использования современных информационных технологий в криминальных целях предопределяет возникновение целой совокупности проблем, возникающих у правоохранительных органов в сфере противодействия преступности[2].

Говоря о масштабах киберпреступности необходимо отметить следующее[3]. Так согласно официальным статистическим данным ФКУ «ГИАЦ МВД России» в 2018 г. каждое 11-12 (8,8 % 174 674 из 1 991 532) зарегистрированное преступление относилось к числу киберпреступлений, в 2019 это было каждое седьмое (14,5 % 294 409 из 21 024 337), а в 2020 г. –каждое четвертое (25,0 % 510 396 из 2 044 221). Таким образом, в 2020 году число преступлений в сфере информационных технологий увеличилось на 73,36% и составило 510396 преступлений. Отмечается увеличение количества зарегистрированных преступлений на 453,08% совершенных с использованием расчетных (пластиковых) карт (190 167); на 56,91% - с использованием компьютерной техники (28653); на 59,96% - с использованием программных средств (10050); на 39,63% - с применением фиктивных электронных платежей (1274); на 91,25% - с применением сети «Интернет» (300337); на 88,32% - с применением средств мобильной связи (218739) (табл.1).

---

[1] См.: Фомиченко А.С. Особенности проявления кибербуллинга в высшем образовании (по материалам зарубежных исследований) // Мир науки. 2018. Т. 6. № 5. С. 67; Усмонова Р.Н. Психологические особенности жертв кибербуллинга // Ученые записки Крымского инженерно-педагогического университета. Серия: Педагогика. Психология. 2017. № 1 (7). С. 162-165.

[2]См.: Афанасьева О.Р., Гончарова М.В., Шиян В.И. Криминология и предупреждение преступлений: Учебник и практикум / М., 2019; Афанасьева, О.Р., Афанасьев, П.Б. Жертвы насильственных преступлений // Вестник Московского финансово–юридического университета. – 2012. – № 4. – С. 110–119.

[3] Саркисян А.Ж. Состояние преступности в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. 2015. № 4 (10). С. 80-84.

Таблица 1.

Динамика количества зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Российской федерации в 2018-2020 гг.

Преступления	**2018**	**2019**	**2020**	**Динамика к 2019 г. +/- в %**
Всего	**174674**	**294409**	**510396**	**73,36**
Особо тяжкие	19370	25138	44798	78,21
Тяжкие	37949	117590	222815	89,48
Средней тяжести	75372	97827	160823	64,40
Небольшой тяжести	41983	53854	81960	52,19
Преступлений, совершенных с использованием или применением расчетных (пластиковых) карт	16427	34383	190167	453,08
Преступлений, совершенных с использованием или применением компьютерной техники	15027	18261	28653	56,91
Преступлений, совершенных с использованием или применением программных средств	4375	6283	10050	59,96
Преступлений, совершенных с использованием или применением фиктивных электронных платежей	489	984	1374	39,63
Преступлений, совершенных с использованием или применением сети «Интернет»	108016	157036	300337	91,25
Преступлений, совершенных с использованием или применением средств мобильной связи	61299	116154	218739	88,32

Уровень киберпреступности, т.е. количество преступлений на 100 тыс. населения, в 2020 году также увеличился на 73,4 % с 200,6 в 2019 г. до 347,8 в 2020 г. (рис. 1)

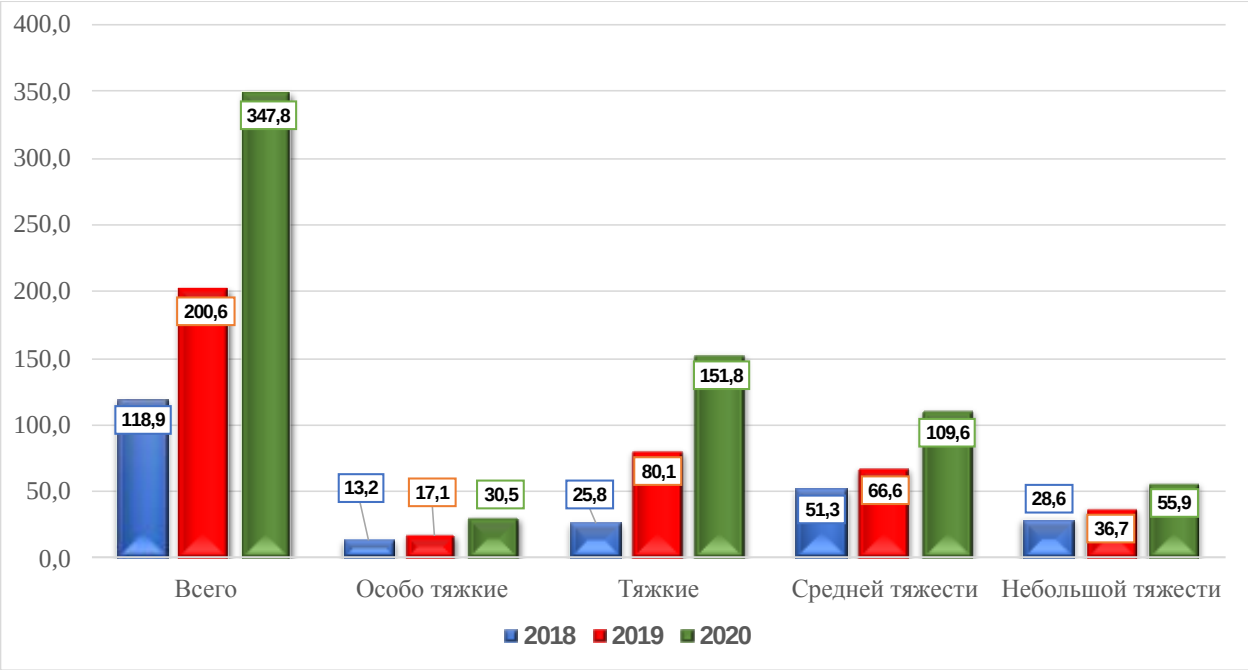


Рис. 1. Динамика уровня зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в Российской федерации в 2018-2020 гг.

Что касается структуры преступлений, совершаемых с применением информационно-телекоммуникационных технологий, то среди них преобладают мошенничества (41,24 %), кражи (34,0 %) и деяния в сфере незаконного оборота наркотиков (9,22 %).

Анализируя совокупность факторов, предопределяющих рост киберпреступности, необходимо отметить, что подобная тенденция развития преступности соответствует общемировой. В качестве же основных факторов выделяются[1]:

доступность информации о способах и средствах совершения киберпреступлений;

увеличение использования онлайн-коммуникаций как государственными органами, организациями, так и физическими лицами;

недостаточная цифровая грамотность населения, а также рост пользователей онлайн-сервисов из числа лиц пожилого возраста, которые также не обладают необходимыми знаниями по обеспечению информационной безопасности;

неподготовленность бизнес-процессов большинства организаций к переводу персонала на дистанционный режим работы[2];

рост числа сервисов и объемов онлайн-продаж;

---

[1] Гончарова М.В. Факторы, детерминирующие киберпреступность // В сборнике: Проблемы детерминации и предупреждения преступности. Под редакцией профессора А.И. Долговой. Москва, 2017. С. 84-88.

[2] URL: https://www.kaspersky.ru/about/press-releases/2020_laboratoriya-kasperskogo-79-rossiyan-ne-poluchali-rekomendatsii (дата обращения 1.12.2020).

безработица и желание трудоустроиться на работу с дистанционной занятостью способствуют росту криминальной активности в рассматриваемой сфере и др.

Развитие технологий, а также противодействие правоохранительных органов киберпреступности предопределяют необходимость киберпреступникам постоянно совершенствовать способы совершения преступлений. Представленный криминологический анализ состояния и тенденций развития киберпреступности мог бы свидетельствовать как о достаточно эффективной деятельности правоохранительных органов, способных выявлять и регистрировать киберпреступления, так и бурном росте киберпреступности. Между тем, цифры, характеризующие раскрываемость киберпреступлений, к сожалению, подтверждают второй довод, поскольку официальные статистические данные свидетельствуют о низкой раскрываемости регистрируемых киберпреступлений.

Таким образом, возможно заключить, что с учетом масштабов регистрируемой части киберпреступности, низкой ее раскрываемости, продолжающегося влияния как криминогенных, так и антикриминогенных факторов преступности очевидны как продолжающийся рост киберпреступности, так и потребность в адекватной превентивной деятельности со стороны не только государства, но и организаций, отдельных физических лиц.

Литература

1. Афанасьева О.Р., Гончарова М.В., Шиян В.И. Криминология и предупреждение преступлений: Учебник и практикум / М., 2019.
2. Афанасьева, О.Р., Афанасьев, П.Б. Жертвы насильственных преступлений // Вестник Московского финансово–юридического университета. – 2012. – № 4. – С. 110–119.
3. Гончарова М.В. Факторы, детерминирующие киберпреступность // В сборнике: Проблемы детерминации и предупреждения преступности. Под редакцией профессора А.И. Долговой. Москва, 2017. С. 84-88.
4. Саркисян А.Ж. Состояние преступности в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. 2015. № 4 (10). С. 80-84.
5. Усмонова Р.Н. Психологические особенности жертв кибербуллинга // Ученые записки Крымского инженерно-педагогического университета. Серия: Педагогика. Психология. 2017. № 1 (7). С. 162-165.
6. Фомиченко А.С. Особенности проявления кибербуллинга в высшем образовании (по материалам зарубежных исследований) // Мир науки. 2018. Т. 6. № 5. С. 67.

И.С. Бедеров

Проблемы и тенденции в расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Аннотация. В статье автор актуализирует тему, что низкая раскрываемость преступлений, совершаемых с использованием информационно телекоммуникационных технологий, ставят перед государством проблему модернизации в работе правоохранительных органов. Одной из причин стагнации этого процесса является дополнительное финансирование обучения «цифровых стражей порядка». Автор обосновывает, что эффективное противодействие киберпреступности возможно при активном участии коммерческих организаций и гражданских специалистов, а также с обязательным созданием системы криминалистической идентификации в киберпространстве.

Ключевые слова: киберпреступления, компьютерные преступления, компьютеры, преступления, идентификация.

За последние 7 лет число ежегодно регистрируемых преступлений, совершаемых при помощи информационно-телекоммуникационных технологий (далее – ИТП), выросло в 45 раз с 11 тыс. в 2013 году до 500 тыс. в 2020 году[1]. Раскрываемость этих преступлений постоянно падает и на текущий год не превышает 22%, а по отдельным видам ИТП, таким как кибермошенничество или виртуальный терроризм, не превышает 9%[2]. В 2020 году в 2 раза увеличились случаи телефонного мошенничества, в 3 раза чаще стала осуществляться регистрация мошеннических интернет-сайтов, в 4 раза увеличилось количество фишинговых сообщений[3]. ИТП также включают в себя наркопреступления и преступления экстремистской направленности[4]. Рост числа ИТП оказывает прямое влияние на такие негативные процессы, как:

- социальное приятие гражданами интернет-преступности в качестве допустимого поведения;
- вовлечение в совершение ИТП лиц, не имевших ранее опыта в информационно-телекоммуникационных технологиях;
- уменьшение возраста преступников (интернет-правонарушители начинают свою деятельность с 13-14 лет);
- обнажение существующих в стране проблем с защищенностью конфиденциальной информации, объектов критической инфраструктуры, а

[1] Основные статистические данные о деятельности органов прокуратуры [Электронный ресурс] Режим доступа : URL: https://genproc.gov.ru/stat/data/ (дата обращения 02.12.2020).

[2] Заседание коллегии Генпрокуратуры РФ [Электронный ресурс] Режим доступа : URL: http://kremlin.ru/events/president/news/62998 (дата обращения 02.12.2020).

[3] Банки прогнозируют рост телефонного и интернет-мошенничества [Электронный ресурс] Режим доступа : URL: https://1prime.ru/articles/20200902/831978061.html (дата обращения 01.12.2020).

[4] В России отметили рост экстремистских и наркотических преступлений [Электронный ресурс] Режим доступа : URL: https://lenta.ru/news/2020/11/25/rost/ (дата обращения 30.11.2020).

также неспособностью правоохранительных органов противостоять современной преступности.

Указанные проблемы неоднократно поднимались как на уровне Генерального прокурора РФ, так и Президента РФ. Президент РФ В.В. Путин на расширенном заседании коллегии Генеральной прокуратуры РФ в октябре 2020 года, поручил правоохранительным органам «разработать эффективную систему борьбы с киберпреступлениями»[1].

Отметим несколько ключевых направлений, которые могли бы оказать существенное влияние на повышение эффективности противодействия ИТП:

1. В правоохранительных органах существует недостаток специалистов, имеющих навыки по предупреждению и расследованию ИТП. Система образования в ведомственных образовательных организациях в целом еще не подстроилась к новым реалиям. Это приводит к недостатку подготовки преподавательского состава, программного и аппаратного обеспечения и, как следствие, к пробелам в обучении. Решить эту проблему предлагается за счет создания в ведомственных образовательных организациях специализированных лабораторий. В состав данных лабораторий предлагается включить, как научно-педагогический состав, так и представителей частных организаций, а также экспертов, накопивших наибольшую компетенцию в области расследования ИТП. Это позволит ознакомить обучающихся с современными методами и приемами работы киберкриминалистов, с программными и аппаратными комплексами, существующими на рынке.

Многие виды «цифрового сыска» (OSINT) являются эффективными аналогами существующих оперативно-розыскных мероприятий или отлично их дополняют. Сбор и обработка больших данных позволяет как успешно идентифицировать пользователей анонимных номеров телефонов, адресов электронной почты, владельцев защищенных мессенджеров, криптовалютных кошельков, а также отслеживать перемещения пользователей по всему миру при помощи рекламных модулей (технологии ADINT), так и вовсе деанонимизировать посетителя любого интернет-ресурса по идентификаторам, оставленным его электронным устройством. В связи с этим необходимо обучить сотрудников методам и приемам работы с открытыми данными при раскрытии и расследовании ИТП.

2. В стране практически отсутствует реальная возможность для внедрения в правоохранительную деятельность технологий, разработанных стартапами. Закупочная деятельность в государственных органах имеет большое число формальных требований и предлогов для того, чтобы отказать любому разработчику. Соответствие же требованиям государственного органа для любого стартапа является финансово неподъемным, что искусственно

[1] Генпрокурор РФ считает, что правоохранители не справляются с противодействием кибер-преступлениям [Электронный ресурс] Режим доступа : URL: https://www.advgazeta.ru/novosti/genprokuror-rf-schitaet-chto-pravookhraniteli-ne-spravlyayutsya-s-protivodeystviem-kiberprestupleniyam/ (дата обращения 30.11.2020).

ограничивает круг предпочитаемых «инноваторов» госкорпорациями или закрытыми НИИ.

Решить эту проблему предлагается за счет направления деятельности одного из государственных институтов развития в сферу работы со стартапами. Так, в июле 2019 г. на базе АО «Технопарк Санкт-Петербурга» был создан отдел специальных разработок (ОСР)[1]. За время своего существования ОСР более 300 раз привлекался для помощи правоохранительным органам в расследовании ИТП и собрал под своей крышей десятки стартапов, занимающихся неинструментальной детекцией лжи, расшифровкой интернет-трафика, идентификацией и отслеживанием мобильных устройств, обработкой и анализом больших данных, отслеживанием криптовалютных транзакций и идентификацией пользователей интернет по их электронно-цифровому следу.

3. Правоохранительные органы не сформировали в стране принципиально новой системы криминалистического учета и идентификации, предназначенной для использования в киберпространстве. В качестве объекта криминалистической регистрации следует использовать те идентификаторы электронных устройств пользователей, которые остаются при посещении ими любого интернет-ресурса (модель устройства, версия операционной системы и браузера, языковые и экранные параметры, ip-адрес и иные параметры соединения, авторизованные аккаунты электронной почты и социальных сетей, рекламные идентификаторы и иные). В своей совокупности эти идентификаторы позволяют установить и выделить уникальное устройство не менее чем из 40 млн. прочих. На базе ОСР Технопарка Санкт-Петербурга в начале 2020 года компанией «Интернет-Розыск» был создан прототип такой разработки[2].

Решить существующую проблему предлагается за счет создания в России государственного предприятия, занятого централизованным сбором и анализом электронно-цифровых следов (идентификаторов) пользователей сети Интернет в целях криминалистической идентификации. Данное предприятие может стать одним из основных поставщиков информации для всех субъектов оперативно-розыскной деятельности. Расследование ИТП с применением новой системы идентификации будет лишено таких существенных проблем, как затянутость сроков получения данных от операторов связи и владельцев интернет-ресурсов, урезанность предоставляемой ими информации, отсутствие возможности перекрестного анализа.

---

[1] Слежка самообслуживания. В «Технопарке Санкт-Петербурга» займутся разработками в сфере кибербезопасности [Электронный ресурс] Режим доступа : URL: https://www.dp.ru/a/2019/07/07/Slezhka_samoobsluzhivanija (дата обращения 29.11.2020).

[2] Тестирование пре-альфа версии IP-Розыск [Электронный ресурс] Режим доступа : URL: https://zen.yandex.ru/media/irozysk/testirovanie-prealfa-versii-iprozysk-5f154631a685c35c2a8960b1 (дата обращения 01.12.2020).

С.В. Беззатеев
С.Г. Фомичева

Перспективные подходы к решению проблем компрометации биометрических данных

Аннотация. В статье формулируются перспективные направления к решению проблем компрометации биометрических данных, по которым авторами ведутся фундаментальные и прикладные исследования. В частности, рассматриваются подходы по разработке методик беспарольного доступа, методы аутентификации и верификации в рамках архитектуры нулевого доверия к персоналу, а также системные архитектуры, снижающие/запрещающие возможность компрометации биометрических данных.

Ключевые слова: компрометация биометрических данных, непрерывная аутентификация, архитектура нулевого доверия к персоналу.

Введение

Современное общество повсеместно использует цифровые технологии, сталкиваясь, так или иначе, с проблемами противоправного использования биометрических данных, используемых для идентификации пользователей в цифровом пространстве. Среди глобальных проблем при обеспечении правозащитной деятельности стали фигурировать задачи по борьбе с такими преступлениями как неправомерный доступ к компьютерной информации [ст.272 УК РФ], неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре [ст.274.1 УК РФ] и т.п. Начиная с 2016 года, мобильные устройства стали занимать более 50% процентов доли устройств во всем мире [1]. В повседневной жизни, смартфон считывает показатели активности человека, его местоположения, биометрические характеристики, хранит информацию о банковских счетах и так далее. Заполучив доступ к данным, злоумышленник может не только незаконно обогатиться, но и скомпрометировать законопослушных граждан со всеми вытекающими последствиями. Актуальность решения проблем компрометации биометрических данных несомненна, и является одним из направлений фундаментальных и прикладных исследований сотрудников кафедры «Технологий защиты информации» СПбГУАП. Приведем в данной статье подходы, которые нами используются для решения, в частности, задач защиты биометрических данных.

1. Методы аутентификации и верификации в рамках архитектуры нулевого доверия к персоналу

Традиционные подходы к обеспечению безопасности были разработаны на принципах защиты периметра организации (демилитаризованной зоны - ДЗ). Чтобы попасть внутрь ДЗ, нужно было пройти проверку, но, оказавшись внутри ее никаких дополнительных сдержек и противовесов уже не требовалось. Среди новейших концепуальных подходов на первый план выходит архитектура нулевого доверия (Zero Trust) [1-,4]. Архитектура нулевого доверия основана на

принципе «проверять и никогда не доверять», что особо важно, когда рассматривается защита личности, где понятие демилитаризованной зоны отсутствует в принципе. Zero Trust опирается на такие технологии, как многофакторная аутентификация, IAM, оркестровка, аналитика, шифрование, оценка и разрешения файловой системы. Ключевым аспектом архитектуры нулевого доверия является то, что вся деятельность должна регистрироваться и отслеживаться, а любые аномалии, включая подозрительное боковое движение, немедленно фиксироваться. В Zero Trust системах современными исследователями (Bryan Embrey, 2016-2020) предлагается использовать аутентификацию с поддержкой контекста. Многими исследователями, например, M. Abdeljebar, M. Sadik, E.Sabir and M. Azmiy (2016), предлагается усилить многофакторную аутентификацию на основе мультимодальной биометрии (MFA-MB) с целью улучшения пользовательского опыта (UX). Ими определена функция измерения UX и предложен новый алгоритм, основанный на классификационном подходе под названием Class-Association Rules (CARs), который интегрирует классификационные и ассоциативные правила. Данный подход позволяет улучшить UX в процессе облачной аутентификации, учитывая переменные (время, место, устройство и т. д.), которые управляют аутентификацией пользователей. При таком подходе уязвимым остается возможность компрометации биологических данных субъекта. Авторами данной статьи (A. Ometov, Bezzateev S.V. (2015-2020)) для аутентификации с поддержкой контекста используется информация о местоположении субъекта в качестве механизма поддержки принятия решений для постоянной его аутентификации и/или для облегчения безопасного использования данных в распространяющихся вычислительных приложениях. Персонализированные характеристики поведения субъектов подразумевают регистрацию и последующий динамический анализ последовательностей многомерного наблюдения, которые генерируются окружением субъекта [5].

Среди активно исследуемых подходов в Zero Trust системах рассматривается непрерывная аутентификация (CA) (Bezzateev, S., Zhidanov, K., Afanasyeva, A, (2019), F. Hussain Al-Naji, R. Zagrouba (2020)). Блокчейн с его децентрализованными возможностями идентификации, а также его распределенной и неизменной способностью записывать транзакции, является одной из технологий, которые положили начало эпохе транзакций с нулевым доверием, наряду с другими моделями децентрализованной архитектуры идентификации [6]. В частности, при реализации CA используют методы потокового майнинга данных (DSM), применяемые к сенсорной информации. Среди ограничений применения CA следует отметить дополнительную потребность к накладным расходам с точки зрения потребления ресурсов [7], учитывая использования устройств окружения с ограниченным аккумулятором. Снизить остроту данного ограничения, в частности, при использовании специализированных протоколов обмена информацией предложено в 2019 авторами данной работы (Zhidanov, K., Bezzateev, S., Afanasyeva, A), при этом дальнейшие исследования авторами активно продолжаются.

2. Разработка методик беспарольного доступа

К снижению возможностей компрометации биометрических данных, частично, приводит использование методик беспарольного доступа (Passwordless Enterprise). Аутентификация без пароля устраняет необходимость использования паролей и обеспечивает множество бизнес-преимуществ, включая более удобное взаимодействие с пользователем, сокращение времени и затрат ИТ при более надежной системе безопасности. Ключевую роль для реализации беспарольного доступа играет использование многофакторной аутентификации на основе биометрических характеристик [6]. Многофакторная аутентификация без пароля (MFA) - это процесс проверки личности, который требует, чтобы пользователь предоставил несколько взаимно независимых подтверждений личности, не требуя пароля. В результате улучшается и удобство использования, и безопасность - нет паролей для восстановления и паролей для фишинга, взлома или взлома. Среди современных решений следует выделить стандарт FIDO2, протокол клиент-аутентификатор (CTAP) и спецификации W3C WebAuthn, которые позволяют обеспечить безопасную аутентификацию без пароля, конфиденциальность, защиту от фишинга через веб-браузеры ПК и мобильных устройств. FIDO2 обеспечивает подлинную аутентификацию без пароля, удаляя запомненные пользователем секреты для повышения безопасности и удобства использования. В основе МФА лежат криптографиические алгоритмы с разделением секрета.

Здесь следует отметить, что при компрометации биометрических данных злоумышленник получает доступ ко всем активам с биометрической верификацией. Поэтому при исследовании и разработке системных архитектур, снижающих/запрещающих возможность компрометации биометрических данных авторами данной работы предложен ряд методов многофакторной аутентификации на базе квантово-безопасных алгоритмов, основанных на методах помехоустойчивого кодирования и решетчатой криптографии [2, 3]. В отличии от существующих решений данные подходы помимо ограничения несанкционированного доступа позволяют обеспечить защиту от подмены информации, в том числе и биометрической.

3. Подходы к решению проблемы компрометации биометрических данных

В настоящее время общепризнанным фактом считается возможность восстановления синтетического образца, соответствующего оригиналу, по незащищенному биометрическому шаблону (паттерну) (Javier Galbally, Kevin Atighehchi, Loubna Ghammam, Morgan Barbier, Christophe Rosenberger, 2019). Этот процесс обратного проектирования, обычно называемый обратной биометрией (inverse biometrics), представляет серьезную угрозу для биометрических систем: во-первых, опасна сама возможность того, что биометрические данные могут быть получены из скомпрометированных незащищенных шаблонов. Во-вторых, на основе этих реконструированных образцов могут быть запущены мощные кибератаки. Отменяемая биометрия (Cancelable biometrics) - современный подход для решения проблем, связанных с защитой биометрических данных. Он

позволяет отменять и отзывать биометрические шаблоны, как пароли, бесчисленное количество раз. BioHash - это форма отменяемой биометрии, которая смешивает набор случайных векторов, специфичных для пользователя, с биометрическими характеристиками.

Среди современных направлений исследований актуальными являются такие, как разработка алгоритмов реконструкции для различных биометрических характеристик, предложение методологий для оценки уязвимости биометрических систем к вышеупомянутым алгоритмам, разработка мер противодействия для снижения возможных последствий атак. В качестве решений Harkeerat Kaur и Pritee Khanna в 2015 предложили отменяемый алгоритм генерации биометрических шаблонов с использованием гауссовских случайных векторов и одностороннего модульного хеширования, а в 2019 году «Метод случайного расстояния» для создания сохраняющих конфиденциальность, необратимых, отзываемых и уменьшенных по размеру псевдобиометрических идентификаторов [4, 5]. Множественные псевдоидентификаторы, сгенерированные из одной и той же биометрической информации, позволяют предотвратить перекрестное сопоставление и другие атаки на базу биометрических данных.

Кроме того, предлагается ряд подходов (Christian Rathgeb, Javier Galbally - 2016) на модификации схем, основанных на фильтрах Блума (Bloom filters). Многообещающей принято считать отменяемую биометрическую схему, называемую корреляционно-инвариантной случайной фильтрацией (CIRF). Эта схема преобразует биометрический объект, представленный в виде изображения, с помощью двумерного теоретического преобразования чисел (NTT) и случайной фильтрации (Takao Murakami, Tetsushi Ohki, Yosuke Kaga, Kenta Takahashi (2015-2019). Актуальными также являются комплексные техники, повышающие надежность хранения биометрии (например, blockchain-PSO-AES - A.H.Mohsin, A.A.Zaidan, B.B.Zaidan, O.S.Albahri, A.S.Albahri, M.A.Alsalem, K.I.Mohammed (2019)) при обработке биометрических данных.

Как уже отмечалось выше, авторами данной статьи разрабатываются новые методы отменяемой биометрии с использованием подходов, используемых в постквантовой криптографии. В частности, разрабатываются СВ-схемы на основе помехоустойчивых кодов.

Заключение

Развитие цифровых технологий, создавая новые возможности, порождает и новые проблемы, к числу которых относится компрометация биометрических данных. Решение данной проблемы носит комплексный характер и помимо организационных мероприятий должна базироваться на применении методов и алгоритмов с доказанной теоретической и вычислительной стойкостью. Разработка методов и методик таких. как непрерывная аутентификация в рамках архитектуры нулевого доверия к персоналу, блокчейн техника, а также методы пост квантовой криптографии на базе помехоустойчивого кодирована способна решить задачи компроментации биометрических данных.

Литература

1. Afanasyrva A., Bezzateev S., Zhidanov K., et al., An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends, , IEEE Access, 2020, 8, c.103994-104015, 9104713
2. Bezzateev S., et al., Challenges of multi-factor authentication for securing advanced IoT Applications, IEEE Network. 2019. Т. 33. № 2. С. 82-88].
3. Bezzateev, S., Fomicheva, S. Soft multi-factor authentication, Proceeding «Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020», 2020, 9131537
4. Bezzateev S.V., et al., The use of European internet communication properties for IP geolocation, Information Technology and Control. 2016. Т. 45. № 1. С. 77-85].
5. Davydov, V., Bezzateev, S. Accident detection in internet of vehicles using blockchain technology, International Conference on Information Networking, 2020, 2020-January, c.766-771, 9016602
6. Fomicheva S. Soft quantization of the productions knowledgebases for multi-agent systems, В сборнике: Conference of Open Innovation Association, FRUCT. Proceedings of the 20th Conference of Open Innovations Association, FRUCT 2017. 2017. С. 69-76].
7. Zhidanov, K., Bezzateev, S., Afanasyeva, A., et al., Blockchain Technology for Smartphones and Constrained IoT Devices: A Future Perspective and Implementation Proceedings - 21st IEEE Conference on Business Informatics, CBI 2019, 2019, 2, c.20-27, 8808043

Д.А. Бражников
Д.К. Воронкова

Цифровые технологии в криминалистике

Аннотация. В условиях всеобщей цифровизации общества и повсеместного применения цифровых технологий криминалистика должна «идти в ногу» со временем. В данной статье рассмотрены основные вопросы применения цифровых технологий в криминалистике.

Ключевые слова: криминалистика, цифровые технологии, компьютерные технологии, цифровизация.

Криминалистика, как наука по раскрытию и расследованию преступлений, претерпела несколько витков в развитии, связанных с достижениями антропологии, антропометрии, химии, физики, математики, психологии и ряда других наук. Такие витки развития именуются мутациями в науке [1].

На интегративном характере криминалистики настаивал и в своих последних работах профессор Р.С. Белкин, который отмечал, что «интеграция в криминалистику достижений естественных и технических наук, усложнение самих тех-

нических средств, совершенствование и развитие методик их применения нередко сопряжено со сложными технологическими операциями, поэтому необходимо говорить уже не только о криминалистической технике, но и о технологии. Особенно рельефно это видно при рассмотрении вопроса о связях техники, тактики и методики расследования отдельных видов преступлений» [2].

Криминалистику, в современных реалиях, сложно представить без применения различных компьютерных технологий и средств автоматизации. Это обусловлено несколькими причинами:

1. Сегодня большинство преступлений совершается с использованием информационных технологий. Преступники стараются найти все новые способы и приемы совершения самых разных преступлений с применением компьютерных средств.

2. Современные компьютерные технологии и средства автоматизации позволяют значительно упростить и ускорить процесс криминалистического исследования некоторых вещественных доказательств.

Говоря о криминалистической технике, как о разделе криминалистики, следует учесть то, что ни одно из ее направлений нельзя представить без использования средств и методов компьютерных технологий.

Так, криминалистическая фотография, звуко- и видеозапись сегодня стала полностью цифровой. При проведении различных следственных действий все чаще стали применяться различные компьютерные средства и средства автоматизации, которые позволяют фиксировать доказательственную информацию в цифровом виде. Так, комплекс «МСР-ТВ», состоящий из ноутбука и цифрового фотоаппарата, позволяет не только запечатлеть обстановку места происшествия, но и дополнить полученное фотоизображение текстовыми, графическими или звуковыми комментариями. Кроме того, данный продукт дает возможность извлечения из компьютера необходимого участка электронной карты местности и его вставки вместе с линиями разметки и другими необходимыми данными в фототаблицу, являющуюся приложением к протоколу осмотра. Перечисленные возможности комплекса «МСР-ТВ» не являются исчерпывающими.

Другим примером может служить фотокамера с GPS-модулем, предназначенным для геокодирования изображений и видеофайлов во время съемки на месте происшествия. Это обеспечивает получение компьютерной план-схемы с линейными размерами запечатленных объектов, указанием их положения и взаимного расположения, а также сведений о точном времени и месте производства каждого этапа следственного действия [3].

Говоря о фиксации доказательственной информации в цифровом виде, следует отметить лазерный сканер LEICA BLK360, с его помощью осуществляется фиксация, исследование и криминалистическая реконструкция места происшествия. В результате трехмерного сканирования, в отличие от традиционной фотосъемки, возможно получить координаты каждой отсканированной точки, которые позволяют проводить точные пространственные измерения.

Необходимость реконструкции при производстве осмотра места происшествия, обусловлена прежде всего изменениями, которые происходят в обста-

новке на месте происшествия. С этими задачами справляется 3D сканер. В комплексе со специализированным программным обеспечением данная система может быть использована для проведения ситуационных экспертиз.

Рассматривая дактилоскопию, как раздел криминалистической техники, нельзя не отметить, что с развитием информационных технологий исследование отпечатков пальцев рук вышло далеко за пределы традиционной криминалистики. Еще несколько десятков лет назад биометрическое сканирование отпечатков пальцев рук считалось недоступным способом, в то время как в настоящее время с развитием научно-технического прогресса биометрическое сканирование постепенно становится частью повседневной жизни. Широкое распространение получило повсеместное использование считывателей отпечатков пальцев (сканеров), а также различных терминалов идентификации отпечатков пальцев рук. Данные технологии активно применяются в сфере безопасности, получив особое распространение на объектах крупных государственных и коммерческих организаций в системах контроля и управления доступом.

Несмотря на всеобщую цифровизацию общества, в криминалистике все же сложилась довольно неоднозначная ситуация относительно применения компьютерных технологий. Так, использование различных автоматизированных информационных систем (АИС), основной задачей которых является поиск, сбор, накопление, хранение, передача, обработка информации с использованием вычислительной техники, компьютерных информационных сетей, средств и каналов связи, приводит к некоторым спорам, возникающим среди ученых и практиков.

Ряд ученых, считают, что применение таких АИС на практике приведет к ложным результатам исследования и, как следствие, к возможному вынесению ошибочных заключений экспертов. Как утверждает Л.Г Эджубов, даже самая совершенная автоматизированная дактилоскопическая информационная система (АДИС) способна допускать ошибки [4, с. 141]. При сравнении папиллярных узоров рук данные системы могут выдавать случайные совпадения, в связи с этим использование в качестве источника доказательства информации, выданной АДИС, без экспертной корректировки и оценки может повлечь за собой ошибочное уголовное преследование невиновного человека.

Однако, существует и другое мнение, на основании проведенных экспериментов В.А. Ивашков и С.С. Самищенко отмечают, что при идентификации человека по папиллярным узорам пальцев рук, при условии использования не менее 7 идентификационных признаков, ошибочное совпадение папиллярных узоров рук практически невозможно. Однако в редких случаях ошибки при дактилоскопической идентификации все же встречаются [5]. Но в таких ситуациях авторы указывают на, так называемый, «человеческий фактор» - ошибка эксперта, проявляющаяся в случае малой информативности следов.

Несмотря на столь противоречивые мнения, следует признать, что АИС все же способны повысить оперативность обработки и передачи информации, кроме того, такие системы служат повышению результативности расследования преступлений, в том числе раскрытию преступлений по горячим следам, а также расследованию преступлений прошлых лет.

Цифровые технологии и средства автоматизации позволяют не только значительно упростить и ускорить процесс криминалистического исследования некоторых вещественных доказательств, но и повышать результативность расследования и раскрытия преступлений.

Развитие информационно-телекоммуникационных технологий предоставило возможность совершения киберпреступлений практически безнаказанно, поскольку в настоящее время уголовное законодательство слабо адаптировано к новым видам преступлений в сфере информационных технологий, хотя онлайн – торговля, банковские операции, услуги скоростной передачи данных, современные форматы связи, электронное образование, игровые и развлекательные порталы вошли в жизнь довольно давно[6].

В настоящее время, преступники ищут новые способы совершения преступлений с использованием цифровых технологий. Для того чтобы расследовать подобные преступления, криминалистика должна «идти в ногу» с научно-техническим прогрессом. Поскольку это поспособствует своевременному раскрытию и расследованию таких преступлений.

Список используемых источников

1. Андреев А.С. Криминалистика в условиях развития цифровых технологий // Интеллектуальные ресурсы - региональному развитию. 2020. № 2. С. 456-461.
2. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: Учебник для вузов / под ред. заслуженного деятеля науки Российской Федерации, профессора Р.С. Белкина. – М.: Изд-во НОРМА, 2001. – 990 с.
3. Ищенко Е.П. О цифровых технологиях в криминалистике // В сборнике: Современные проблемы отечественной криминалистики и перспективы ее развития. Сборник научных статей по материалам Всероссийской научно-практической конференции (с международным участием), посвященной 20-летию кафедры криминалистики. Ответственный редактор Г.М. Меретуков. 2019. С. 5-11.
4. Эджубов Л.Г. Статистическая дактилоскопия. М.: Городец, 1999. С. 141.
5. Хайруллова Э.Т., Шадрина Е.С. Современное состояние дактилоскопической регистрации // Ученые записки Казанского юридического института МВД России. 2019. №2 (8). URL: https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-daktiloskopicheskoy-registratsii (дата обращения: 14.02.2021).
6. Антонян Ю.М., Бражников Д.А., Гончарова М.В., и др. Преступность в России: современные тенденции и прогноз развития. Монография. - М.: Изд-во ЮНИТИ-ДАНА, 2018. – С.71.

В.В. Бычков
С.В. Харченко

О понятии компьютерной преступности

Аннотация. В статье раскрываются понятия компьютерной преступности, преступлений, совершаемых с использованием телекоммуникационных, в частности, компьютерных технологий. Рассматриваются вопросы информационной безопасности. Приводятся официальные статистические данные по преступлениям данного вида.

Ключевые слова: компьютерная преступность, компьютерные преступления, телекоммуникационные технологии, информационная безопасность, статистика компьютерных преступлений.

Возможность использования сетевых технологий породила феномен компьютерной преступности. Этот высокоинтеллектуальный вид преступности требует адекватных мер борьбы с ней.

Компьютерные преступления могут причинить ущерб практически любым правоохраняемым интересам, начиная от частных неимущественных интересов отдельных граждан и заканчивая интересами государственной безопасности. На сегодняшний день практически все преступления могут быть совершены с использованием компьютерных и телекоммуникационных технологий.

В 2017 г., когда такие преступления вошли в официальную статистику, было зафиксировано 90 тыс. 587 таких преступлений[1]. В 2018 г. их количество увеличилось на 92.8% – до 174 тыс. 674. В 2019 г. еще на 68.5% – до 294.409, а в 2020 г. их количество «перевалило» за пол миллиона – 510 тыс. 396 (на 73.4% больше АППГ[2]). То есть в течение трех лет, с 2017 г. по 2020 г. количество преступлений данног вида увеличилось почти в 6 раз.

За этот же период отмечено и резкое увеличение количества их совершающих преступников. В 2018 г. таких лиц было вывлено 24 тыс. 2, в 2019 г. – 44 тыс. 158 (на 84% больше АППГ) и в 2020 г. – уже 65 тыс. 665 (на 48,7% больше АППГ).

В настоящее время информация определяет экономический, научный, культурный, образовательный и иные потенциалы общественного развития наравне с материальным производством, поэтому государство заинтересовано в обеспечении информационной безопасности как защите национальных интересов.

Интенсивное развитие информационного общества обязывает государство повышать уровень информационной безопасности общества и особое внимание обращать на борьбу с компьютерными преступлениями.

В июне 2012 года основатель одной из самых известных лабораторий по борьбе вирусами Евгений Касперский заявил о том, что человечество стоит на пороге кибервойны, которая может положить конец «миру, каким мы его знаем». Поводом для опасений стал вирус Flame («Пламя»), выявленный на 600

---

[1] Здесь и далее: Официльный сайт МВД России. Статистика и аналитика. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics.

[2] АППГ – аналогичный период прошлого года.

компьютерах на Ближнем и Среднем Востоке. В компании «Лаборатория Касперского» тогда заявили, что он является самым мощным и сложным из всех когда-либо существовавших[1].

По оценкам компании «Лаборатория Касперского» ущерб, который наносят компьютерные преступники мировой экономике, по самым предварительным подсчетам, составляет более 100 млн долларов в год. Вирусы на мобильных телефонах появляются значительно реже. По словам Касперского, их ежегодно регистрируется несколько тысяч[2].

В скором будущем масштабные хакерские атаки могут привести к тому, что отключенными от Сети окажутся целые страны. Создать абсолютную защиту от вирусов невозможно – ни для компьютеров, ни для мобильных платформ[3].

Проведенное нами исследование показало, что 42% организаций, которые подвергались кибератакам, считают информационную безопасность основной проблемой, превосходящей по важности природные катаклизмы, экстремизм, терроризм и традиционные преступления, вместе взятые[4].

В связи с этим 94% компаний и организаций разработали планы по внедрению в 2010 году нововведений в вопросах безопасности, а 48% из них намерены вносить в свою систему IT-безопасности кардинальные изменения[5].

Ограничившись сказанным в отношении понимания информационной безопасности, остановимся на содержании термина «компьютерная преступность». Данный термин возник в США в начале 70-х годов, когда в США правоохранительными органами было выявлено довольно большое количество преступлений, чаще экономического характера, совершенных в целях неправомерного обогащения путем использования компьютерных информационных систем.

Генеральным секретариатом Интерпола был разработан специальный кодификатор компьютерных преступлений, который включает следующие виды компьютерных преступлений: несанкционированный доступ и перехват компьютерной информации; изменение компьютерных данных (именно к ним относятся «вирусы», «троянские кони» и т.д.); компьютерное мошенничество (к данной группе преступлений отнесены, в том числе мошенничества с банкоматами); незаконное копирование; компьютерный саботаж; прочие компьютерные преступления, к которым относится хищение информации, составляющей коммерческую тайну[6].

---

[1] URL: http://news.rambler.ru/15981509/.

[2] URL: http://www.itsec.ru/newstext.php?news_id=58858#sthash.lqkGwOMP.dpuf.

[3] URL: http://hitech.newsru.com/article/14Apr2010/kasperskyonatt.

[4] Бычков В.В., Харченко С.В. Понятие и формы использования специальных знаний при выявлении противодействия расследованию преступлений экстремистской направленности // Раскрытие и расследование преступлений: наука, практика, опыт: сб. науч. трудов. Ч. 2. Тула, 2020. С. 9-14; Бычков В.В., Харченко С.В. К истории организационно-структурного обеспечения расследования преступлений экстремистской направленности // Создание и развитие модели органов предварительного расследования в Российской империи: мат-лы Всерос. науч.-практич. конф. (24.09.2020). М., 2020. С. 30-36.

[5] URL: http://hitech.newsru.com/article/25Feb2010/symsurvey.

[6] Степанов-Егиянц В.Г. Преступления против компьютерной информации: сравнительный анализ. М., 2010.

Опасность преступлений в сфере компьютерной информации состоит в том, что уничтожение, блокирование, модификация информации, важной для действий, связанных с управляющими датчиками сложных компьютерных систем оборонного, производственного, экономического, банковского и другого назначения, способны повлечь гибель людей, причинить вред их здоровью, уничтожить имущество, причинить экономический вред в больших размерах. Учитывая эти обстоятельства, законодатель отнес гл. 28 «Преступления в сфере компьютерной информации» к разд. IX УК «Преступления против общественной безопасности и общественного порядка».

Значение термина «компьютерная информация» сформулировано в примечании к ст. 272 УК РФ.

Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Особенность компьютерной информации – в ее относительно простых пересылке, преобразовании и размножении; при изъятии информации в отличии от изъятия вещей. Она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно практически неограниченное количество пользователей.

Еще в 1982 году в обзоре судебной практики Верховного Суда СССР были отражены условия использования компьютерной информации в уголовном судопроизводстве[1]. Чаще всего противоправный несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов, технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Не секрет, что эффективность выявления, предупреждения, пресечения и раскрытия любых преступлений находится в прямой зависимости от уровня владения оперативной и иной информацией[2].

Значение информации в организации работы по расследованию компьютерных преступлений обусловлено тем, что ее полнота и достоверность являются главным условием и средством реализации следственных действий, оперативно-розыскных и иных мероприятий[3].

Рассматривая понятие «информация», в начале обратимся к дефиниции, данной в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В этом Законе содержание информации понимается как «сведения (сообщения, данные) независимо от

---

[1] Бюллетень Верховного Суда СССР. 1982. № 6. С. 22.

[2] Овчинский А.С. Информация и оперативно-розыскная деятельность: монография. М., 2002. С. 44-51.

[3] Бычков В.В., Харченко С.В. О некоторых проблемах использования результатов оперативно-розыскной деятельности в раскрытии и расследовании преступлений экстремистской направленности // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования. Журнал. В двух томах. Том 1(2). Орёл, 2020. С. 49-57.

формы их представления». Развивая положения вышеназванного нормативно-правового акта, законодатель указывает, что, будучи представленными в форме электрических сигналов, сведения, сообщения и данные становятся компьютерной информацией.

Согласно теории информации и связи, разработанной Клодом Шенноном[1], сигнал – это материальный носитель информации, используемый для передачи сообщений в системе связи. Сигналы генерируются, и если они принимаются, то становятся сообщениями. Однако их прием вовсе не обязателен. Любую систему передачи информации можно считать состоящей из трех частей: источника сообщений, канала связи и приемного устройства. Между отправителем сообщения и каналом связи могут находиться устройства, преобразующие сообщение в форму, удобную для передачи по каналу связи. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, оптическими и т.д. Вся информация, которую обрабатывает компьютер, должна быть представлена двоичным кодом с помощью двух цифр 0 и 1. С их помощью можно закодировать любое сообщение. Это явилось причиной того, что в электронно-вычислительной машине обязательно должно быть организовано два важных процесса: кодирование (преобразование входной информации в форму, воспринимаемую компьютером, т.е. двоичный код) и декодирование (преобразование данных из двоичного кода в форму, понятную человеку). В вычислительных машинах коды нуля и единицы представляются электрическими сигналами. Наличие сигнала – это признак, который можно обозначить цифрой 1. Отсутствие сигнала обозначается цифрой 0 (также существуют системы, в которых 0 обозначает наличие сигнала, 1 – отсутствие). Вероятно, именно на такой подход ориентировался законодатель при включении термина «электрический сигнал» в рассматриваемое понятие. Теперь законодатель не привязывает компьютерную информацию лишь к машинному носителю, электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Таким образом, под защиту уголовного закона попала и та информация, которая еще не зафиксирована на каком-либо носителе или устройстве, а находится в процессе передачи. Это должно расширить сферу применения данной статьи. Однако информация, передаваемая по беспроводным и оптическим каналам связи, не будет являться объектом уголовно-правовой охраны, т.к. не подпадает под определение электрических сигналов при трактовке этого термина с точки зрения физики. В связи с этим использование такого термина, как «электрический сигнал», лишь вводит в заблуждение и поэтому нуждается в дальнейшем разъяснении или замене более подходящим термином. Сходной позиции придерживается и Верховный Суд Российской Федерации, который в официальном отзыве от 7.04.20 11 № 1/общ-1583. На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» отмечает, что предложенный в примечании к ст. 272 УК

[1] Шеннон К. Работы по теории информации и кибернетике. М., 1963.

РФ термин «электрический сигнал» не вносит достаточной ясности в определение понятия и требует дополнительного пояснения»[1]. В заключении Комитета Государственной Думы по информационной политике, информационным технологиям и св язи от 05.07.2011 «На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» (к первому чтению)» данная позиция получила развитие. Более того, там указывается, «что понятие компьютерной информации отсутствует в федеральных законах, а в предлагаемой дефиниции неясен смысл термина «электрические сигналы».

Таким образом, представляется необходимым уточнить данную формулировку.

Понятие компьютерной информации дается в п. «б» ст. 1 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1.06.2001 – это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи»[2]. Предложения о заимствовании понятия компьютерной информации из этого Соглашения высказывались и ранее[3]. Ввиду недостаточной ясности термина «электрический сигнал», который используется в настоящее время в определении компьютерной информации в примечании к ст. 272 УК РФ.

Таким обазом, ни в теории, ни в практике до сих пор не выработано единого определения «компьтерные преступления». Тем самым, «компьтерные преступления» продолжают оставаться не только предметом научной дискуссии, но и являются объектом научных исследований.

С.Б.Вепрев
С.А.Нестерович

Социальная инженерия - основная тенденций развития преступности в киберпространстве

Аннотация. В статье определяется понятия «социальная инженерия», приводятся основные приемы, использования социальной инженерии в сфере информационно-телекоммуникационных технологий. Предложены некоторые способы борьбы с ней.

Ключевые слова: социальная инженерия, обман пользователей, расследование преступлений, мошенничество в сфере информационно-телекоммуникационных технологий, киберпреступность.

Современное развитие информационно-телекоммуникационных технологий оказывает положительное влияние на все сферы деятельности человека. В то же

[1] URL: http://base.consultant.m/cons/cgi/online.cgi?req=doc;base=PRJ;n=87058
[2] URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=90718
[3] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: автореф. дис. ... канд. юрид. наук. М., 2005.

время оно порождает и комплекс негативных последствий, которые связанны с ростом криминала.

Так рост преступности с использование информационно-телекоммуникационных технологий оказывает существенное влияние на криминогенную ситуацию. В январе-октябре 2020 г. было зарегистрировано на 75,1% больше противоправных деяний, чем в прошлом году за этот же период[1].

В отчете компании Positive Technologies «Актуальные киберугрозы: за 2-ой квартал 2020 года», тема COVID-19 была затронута в 16% атак с использованием методов социальной инженерии, в 36% таких атак они не были привязаны к конкретной отрасли, в 32% атак были направлены против частных лиц[2]. Во время изоляции и удаленной работы появились факторы, которые нужно было службам безопасности банков учитывать: обработка документов клиентов осуществлялась преимущественно на домашних компьютерах; не всегда использовался хорошо защищенный домашний интернет и защита каналов связи (Skype, ZOOM). Директор дирекции мониторинга электронного бизнеса Альфа--Банка Алексей Голенищев утверждает: «очевидно, что при работе в удаленном режиме с конфиденциальными данными у недобросовестного работника больше возможностей для различных злоупотреблений, чем на рабочем месте в офисе, где есть и системы видеонаблюдения, и коллеги[3]».

В настоящее время одной из основных тенденций развития преступности в сфере информационно-телекоммуникационных технологий продолжают оставаться использование методов социальной инженерии, при совершении противоправных действий. Данные методы зачастую характеризуются применением определенных методов, направленных на введение человека в заблуждение. Количество попыток мошенничества с применением социальной инженерии в отношении россиян за прошлый год выросло на 40%, сообщил в интервью РИА Новости зампред правления Сбербанка[4].

Так, например, администрация Twitter летом 2020 года, рассказала, каким образом был взломан механизм аутентификации сервиса микроблогов. В своем официальном аккаунте компании специалисты заявили, что взлом произошел с помощью методов социальной инженерии, которая была направлена против некоторых сотрудников Twitter.

Атака злоумышленников на сервис микроблоков привела к захвату официальных аккаунтов американских политиков, бизнесменов, поп-звезд и некоторых

---

[1] Официальный сайт МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/21933965/ (дата обращения: 10.12.2020).

[2] COVID-19 как тема для социальной инженерии. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/#id5 (дата обращения: 12.12.2020).

[3] Пандемия и социальная инженерия. Что изменилось и как противодействовать? URL:https://plusworld.ru/journal/2020/plus-8-2020/pandemiya-i-sotsialnaya-inzheneriya-chto-izmenilos-i-kak-protivodejstvovat/ (дата обращения: 07.01.2021).

[4] Сбербанк отметил рост числа попыток использовать методы социнженерии URL: https://ria.ru/20200121/1563658583.html (дата обращения: 07.01.2021).

платежных систем[1]. Под термином социальная инженерия принято понимать комплекс используемых злоумышленниками психологических приемов, позволяющих обмануть пользователя или ввести его в заблуждение, чтобы заставить выполнить те или иные нужные киберпреступнику действия, например, передать пароли от аккаунта в социальных сетях, сообщить реквизиты банковской карты или запустить на компьютере вредоносную программу[2].

Само понятие социальной инженерии, по утверждениям ряда источников, ввел в обиход известный американский хакер Кевин Митник. Согласно рассказам его коллег и современников, сам Митник не обладал глубокими техническими познаниями в сфере информационных технологий, однако являлся при этом неплохим психологом. Он не брезговал покопаться в мусорных контейнерах на заднем дворе крупных офисных центров, куда сотрудники могли выбросить содержащие конфиденциальную переписку или важные пароли бумаги, распечатки внутренних документов и другие ценные источники информации. Он мог несколькими телефонными звонками выведать у работников различных фирм те или иные интересующие его сведения. Например, представившись новым руководителем одного из подразделений компании, Митник мог поинтересоваться по телефону у одного из сотрудников техподдержки, где найти системного администратора, чтобы подключить на его рабочем месте принтер, и заодно узнать, как его зовут. Затем, представившись тем самым системным администратором, он выведывал у ничего не подозревающей секретарши пароль от ее электронного почтового ящика.

Вот лишь малая часть простых приемов, которые применяются на практике в социальной инженерии, и используются современными злоумышленниками:

1. Фишинг (англ. password harvesting fi shing – ловля паролей) – наиболее распространенная и эффективная техника социальной инженерии, которая представляет собой массовую рассылку писем по электронной почте либо SMS. Зачастую злоумышленник отправляет письма с почтовых адресов, похожих на адреса известных компаний, банков, сервисов (например, ВКонтакте, mail.ru и др.), и просит выслать те или иные конфиденциальные данные. Поэтому многие жертвы не задумываясь сообщают преступникам свои персональные сведения. Признаками фишинга являются: массовость рассылки писем; искажение данных об отправителе; отсутствие информации о получателях при отправлении писем; использование психологических приемов, которые побуждают пользователей добровольно предоставлять злоумышленникам личную информацию (например, логин и пароль); наличие предложения перейти по указанной в письме ссылке.

2. Вишинг (англ. vishing – голосовая запись) – это вид телефонного мошенничества, который позволяет выманивать у клиентов банков конфиденциальную

---

[1] Взлом аккаунтов Twitter Маска, Гейтса, Безоса и др. был следствием успешного использования социальной инженерии – материалы расследования URL: https://d-russia.ru/vzlom-akkauntov-twitter-maska-gejtsa-bezosa-i-dr-byl-sledstviem-uspeshnogo-ispolzovanija-socialnoj-inzhenerii-materialy-rassledovanija.html (дата обращения: 07.01.2021).

[2] Холмогоров В. PRO ВИРУСЫ. Издание четвертое, переработанное и дополненное / Валентин Холмогоров. — СПб.: Страта, 2020. — 224 с.

информацию (PIN-коды, номера банковских карт и др.). Эта информация может использоваться злоумышленниками в преступных целях. Особенность Вишинга основывается в использовании системы предварительно записанных голосовых сообщений от якобы технического специалиста или представителя известной компании (например, сотрудника Сбербанка России).

Основные признаки Вишинга: получение конфиденциальной информации пользователя при помощи средств сотовой связи, а также заранее подготовленной записи официального разговора; использование техники для получения доступа к банковскому счету жертвы; стимулирование у пользователя желания совершить необходимые мошенникам действия с банковской картой; нагнетание психологической напряженности для достижения корыстных целей; отсутствие конкретных ответов на вопросы, задаваемые жертвой.

3. Претекстинг – это набор действий, проведенный по определенному, заранее подготовленному сценарию (претексту), в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Как правило, целью злоумышленников является пароль от какого-либо ресурса или иные секретные данные пользователя.

Признаками претекстинга являются: сбор информации о потенциальной жертве и ее окружении для создания доверительных отношений в ходе общения с ней; подготовка сценария диалога с жертвой на основании полученной информации.

4. «Троянский конь». Эта техника основывается на любопытстве, доверчивости и желании получить выгоду. Злоумышленник отправляет жертве сообщение с информацией, например, о выигрыше крупной суммы денег. Однако это письмо во вложении содержит вредоносную программу, и при переходе по ссылке или скачивании файла, как правило, происходит списание денежных средств с банковской карты либо заражение персонального компьютера вирусом, избавиться от которого можно, перечислив мошенникам определенную денежную сумму.

Характерными признаками техники «троянский конь» являются:

- использование в сообщении информации, которая вызывает большой интерес у любого человека;
- массовость рассылки писем от неизвестных отправителей;
- наличие вирусной программы в файле, прикрепленном к письму.

Например, очень часто рассылают пользователям с популярных онлайновых служб занятости выгодные приглашения на работу, при этом требуют оплатить какие-либо курсы переподготовки, или внести определенную сумму якобы за оформление необходимых документов.

Разновидностью социальной инженерии являются и классические «нигерийские письма»[1], получившие свое название благодаря тому, что этим видом мошенничества промышляли в основном жители Нигерии. «Нигерийский» письма

[1] Нигерийские» письма. URL: https://encyclopedia.kaspersky.ru/knowledge/nigerian-letters/ (дата обращения: 07.01.2021).

– это разновидность компьютерного мошенничества, попытка под неким вымышленным предлогом получить доступ к банковскому счету пользователя или иным путем получить с него деньги.

В качестве стандартного предлога в «нигерийских» письмах выступает необходимость обналичить крупную сумму денег. Автор письма обычно утверждает, что он располагает миллионами долларов, но они приобретены не совсем законным способом или же хранятся в обход закона. Например, это украденные иностранные инвестиции или гранты ООН. Далее автор письма объясняет, что по этой причине он не может разместить деньги на счету в банках своей страны, и что ему срочно требуется счет в зарубежном банке, куда можно перечислить «грязные» деньги. Еще одна типичная версия – деньги нажиты легитимным путем либо получены в наследство, однако в связи с политической нестабильностью в стране обналичить их невозможно.

Социальная инженерия активно используется и для взлома электронных почтовых ящиков. Например, в социальной сети потенциальной жертве может поступить сообщение от незнакомого человека, в котором он, крайне вежливо и обходительно извинившись за беспокойство, сообщает, что, возможно, учился в одном классе с матерью получателя. Чтобы убедиться в этом, он просит уточнить ее девичью фамилию. Нередко такие письма поступают пользователям и от отправителей, якобы озабоченных поиском дальних родственников. Отвечая на такие послания, самое время задуматься: а не является ли вопрос «девичья фамилия матери» ключевым для восстановления пароля в используемом жертвой почтовом сервисе? Если это так, злоумышленники очень быстро завладеют ее почтовым ящиком, а с помощью него – незамедлительно получат доступ к аккаунтам во всех социальных сетях и других подобных сервисах, допускающих восстановление пароля доступа при помощи электронной почты.

Защищаться от социальной инженерии достаточно сложно, так как сама жертва очень часто не догадываются о том, что его обманули и воспользовались его слабостью, чтобы заполучить конфиденциальную информацию. Решать эту проблему нужно комплексно:

1. Определить информацию, уязвимую к атаке

Сотрудники должны уметь классифицировать информацию по степени защищенности и понимать, раскрытие каких данных может причинить вред компании. Например, пользовательские учетные данные всегда принадлежат организации, их нельзя передавать третьим лицам или оставлять в открытом доступе. Необходимо сотрудникам распрощаться с наклейными стокерами в ящиках своих рабочих столов и т.п., где написаны логины/пароли. Воздерживаться от авторизации на корпоративных ресурсах через открытые Wi-Fi-сети. Блокировать персональные компьютеры или ноутбуки в свое отсутствие.

2. Повышать компетентность в вопросах информационной безопасности

Технологии социальной инженерии постоянно совершенствуются, и кибермошенники находят новые способы сыграть на человеческих слабостях. Сотрудникам компании необходимо знать, жертвами каких потенциальных атак они мо-

гут быть и как вести себя в подобных ситуациях. Например, куда следует написать/позвонить, если третьи лица запросили у них конфиденциальную информацию или данные для авторизации.

3. Ограничить права доступа к информационным системам

Доступ на скачивание, пересылку, копирование информации т.д. должны иметь только те сотрудники, для которых это необходимо должностными обязанностями. В ряде компаний необходимо запретить использование съемных носителей и на физическом уровне блокировать USB порты.

4. Создавать четкие инструкции по обмену информацией

В любом отделе и подразделении все – от рядового офисного сотрудника до руководителя – должны быть четкие инструкции о том, в каких условиях они могут раскрыть важную для компании информацию. В этих инструкциях необходимо указывать, какие сведения можно передавать службам техподдержки, или представителям контролирующих органов.

5. Систематически обновлять антивирусного программного обеспечения

В результате этого компьютеры сотрудников будут менее уязвимыми к массовым фишинговым атакам. Современное антивирусное программное обеспечение включает инструменты для защиты от шпионских и вредоносных программ, и предупреждает при переходе по подозрительным ссылкам.

А.Ф. Волынский
В.А. Прорвич

Интегрирующая роль компьютерной криминалистики в выявлении, раскрытии и расследовании преступлений в сфере цифровой экономики

Аннотация. Переход к информационному обществу и экономике знаний сопровождается быстрым ростом новых видов преступлений в сфере цифровой экономики и финансов, а также в системе цифровых прав экономических субъектов, связанных с определенными информационными системами. Показана роль нового инструментария компьютерной криминалистики в выявлении, раскрытии и расследавании преступлений данного вида. Предложены новые формы применения специальных знаний для получения необходимых доказательств.

Ключевые слова: цифровая экономика, компьютерная криминалистика, закодированные информационные следы, специальные знания, искусственный интеллект, интерактивные экспертные системы.

Быстрое изменение характера общественных отношений при переходе к информационному обществу и экономике знаний привело к появлению принципиально новых видов преступлений не только в сфере цифровой экономики и финансов, которые осуществляются в информационном пространстве компьютерных сетей. Появились не только новые способы совершения хорошо известных видов преступлений общеуголовного характера, но и новые виды преступлений в сети Интернет, связанные с экстремизмом, здоровьем населения, общественной нравственностью и многими другими видами криминала.

Что касается преступлений в сфере цифровой экономики и финансов, то необходимо учитывать ряд особенностей введенной год назад системы цифровых прав, связанных с информационными системами, через которые осуществляются потоки транзакций с помощью закодированной информации на многие миллиарды реальных рублей. Выявить следы таких преступлений в определенных совокупностях электронных документов и создать надежную систему уголовно-правовой защиты субъектов цифровой экономики, которыми постепенно становятся все граждане страны, в рамках «традиционных» подходов и инструментария криминалистики практически невозможно. Погоня за преступниками в виртуальном пространстве по оставленным им закодированным информационным следам имеет мало общего с богатейшим опытом работы «на земле».

В этой связи необходимо обратить внимание на ряд Указов Президента России, в соответствии с которыми[1] была принята национальная программа «Цифровая экономика Российской Федерации»[2], а Правительству РФ было поручено до 15 декабря 2019 г. обеспечить внесение изменений в национальную программу «Цифровая экономика Российской Федерации»[3], в том числе разработать и утвердить федеральный проект «Искусственный интеллект». Особо следует выделить запланированное создание к 2020 г. системы негосударственных экспертных организаций в области компьютерной криминалистики, ответственность за которое возложена на МВД России и Минюст России. И это при том, что в составе данных ведомств имеются государственные экспертные учреждения. Для прояснения сложившейся ситуации и поиска новых путей развития криминалистики XXI века, а также роли и места декларированной на высшем уровне «компьютерной криминалистики» [1,2] уместно напомнить ряд исторических уроков, оказавших существенное влияние на роль и место криминалистики в системе наук уголовно-правового блока.

Начало криминалистики, как науки о раскрытии и расследовании преступлений, было положено в нашей стране введением антропологической (1890 г.), а затем и дактилоскопической (1906 г.) регистрации. Однако, спустя почти два десятилетия стало понятно, что криминалистическая регистрация – это средство, прежде всего, раскрытия и расследования преступлений, розыска лиц, совершивших преступления. В результате криминалистическая регистрация была передана в ведение органов полиции (1908 г.), где для её осуществления была создана довольно широкая сеть территориальных регистрационных бюро, положивших начало развитию экспертно-криминалистической службы ЭКС МВД России.

Так, практически из одного источника возникли и, преодолевая организационные «заблуждения», стали развиваться в нашей стране экспертно-криминалистическая и судебно-экспертная виды деятельности (ЭКД и СЭД), обладающие существенными различиями по целям, задачам, организации и тактики их реше-

---

[1] Указ Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года».

[2] утверждена президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 24 декабря 2018 г. № 16.

[3] Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

ния. Так было положено начало формированию системы экспертно-криминалистических подразделений (ЭКП) полиции (органов внутренних дел) и судебно-экспертных учреждений (СЭУ) Минюста России. Вместе с тем, неоднозначность в определении предметов этих видов деятельности, их целей и задач, порядка их осуществления обусловило в дальнейшем длительные и бесплодные дискуссии, в частности, о праве производства экспертиз в ЭКП ОВД [3].

Отличительной особенностью этого периода становления и развития ЭКП ОВД и СЭУ было многообразие создававшихся в стране, созвучных по названиям, государственных, ведомственных, частных судебно-экспертных учреждений и экспертно-криминалистических подразделений. Это судебно-фотографическая лаборатория, созданная Е.Ф. Буринским (1889 г.), затем такая же по названию лаборатория при прокуроре Санкт-Петербургской судебной палаты (1892 г.) которая переименована в Кабинет научно- судебных экспертиз (1912 г.).

В советское время, кроме упомянутого Кабинета судебных экспертиз, затем НТО Центророзыска, создаются Кабинет судебной экспертизы (Харьков, 1923 г.); Институт криминалистики и судебной экспертизы (Минск, 1929 г.); Центральная криминалистическая лаборатория Наркомюста СССР (Москва, 1944 г.), на базе которой создан Центральный НИИ судебных экспертиз (ЦНИИСЭ, 1962 г.); Институт криминалистики МВД СССР (1945 г.); Центральная криминалистическая лаборатория (1969 г.) и т.д.

Такое разнообразие в названиях СЭУ и ЭКП однозначно свидетельствует об организационной неопределённости и нестабильности их развития, а в более глобальном масштабе дает основание для вывода об отсутствии в то время научно обоснованной государственной политики в области научно-технического обеспечения уголовного судопроизводства. При этом словами «судебной», а в некоторых случаях «научно-судебной» экспертизы в названиях подчёркивалась не только значимость судебной экспертизы как средства доказывания, как формы исследования доказательств в уголовном судопроизводстве, но и некое её превосходство перед «ненаучными» их исследованиями, проводимыми в НТО органов полиции. Так проявлялись первые признаки межведомственного противоречия по вопросам организации в нашей стране ЭКД и СЭД [3].

В этой связи заметим, что стремление правоприменительных ведомств и судебно-экспертного сообщества создать в нашей стране более масштабную и действенную систему СЭУ тогда были вполне объяснимы. Данная задача явно актуализировалась в условиях рыночной экономики и глобализации международных отношений, но нельзя признать оправданным её решение путём разрушительного воздействия на исторически сформировавшуюся систему ЭКП правоохранительных органов.

Анализ процесса возникновения и развития криминалистики, как науки о раскрытии и расследовании преступлений свидетельствует об исторически предопределенных существенных особенностях этого процесса в нашей стране. Например, в западноевропейских странах уже при зарождении криминалистики были обозначены два вида (направления) деятельности, определяющих её содержание: криминалистика для следователей – наука о «реалиях уголовного права», вышедшая из него и бази-

рующаяся на положениях всего блока уголовно-правовых наук [5] и криминалистика как наука о технике собирания, исследования и использования розыскной и доказательственной информации на основе достижений естественных и технических наук, в частности, в романской группе стран (А. Бертильон, Р.А. Рейсс). Это нашло свое отражение в организационном обособлении деятельности «технической полиции» (специалистов) и «научной полиции» (экспертов) [6].

Федеральным законном «О полиции» от 7 февраля 2011 г. №3-ФЗ (п. 12 ст. 2) фактически обозначена перспектива организации и в нашей стране, наряду с судебно-экспертной и экспертно-криминалистической деятельности, осуществление которой представляется в качестве одного из основных направлений деятельности полиции. Вместе с тем, из-за высокой загруженности государственных экспертных учреждений текущей работой, вполне понятно уже упоминавшееся выше решение руководства страны поручить создание компьютерной криминалистики под эгидой Минюста России и МВД России именно негосударственным экспертным организациям.

Сама по себе дифференциация научных знаний представляется как одна из закономерностей их развития, она объективно назревала и в криминалистике, но осуществлялась поспешно, стихийно под влиянием сформировавшегося к этому времени абсолюта судебной экспертизы, как единственной и незаменимой формы использования специальных знаний в уголовном процессе, результаты которого имеет доказательственное значение. В результате система криминалистических знаний, была явно обеднена и по содержанию, и по своим возможностям. Достаточно обратить внимание на определение ее предмета как науки «о закономерностях механизма преступления, возникновения информации о преступлении и его участниках, собирания, исследования, оценки и использования доказательств…» [6, с.6] и неизбежно возникает вопрос о его соответствии реалиям практики раскрытия и расследования преступлений без СЭД и ОРД.

Понятно, что после дифференциации криминалистических знаний непременно должен последовать процесс их интеграции, но на ином уровне и иной организационной основе, в форме взаимодействия наук, причём не только уголовно-правового блока, но и экономики, математики, информатики. Это становится все более очевидным в контексте проблем выявления, раскрытия и расследования преступлений в сфере традиционной и цифровой экономики и формирования в этой связи компьютерной криминалистики [1, 8]. При этом СЭД может быть одной из таких наук, но взять на себя роль интегратора криминалистических знаний, а тем более в форме компьютерной криминалистики, она не в состоянии из-за ограниченности предмета научно обеспечиваемой деятельности – производства судебных экспертиз [4].

В то же время, цифровизация населения и практически всех отраслей экономики привела к быстрому росту преступности с использованием компьютерных и информационно-телекоммуникационных технологий. Если в 2017 г. было отмечено 90587 преступлений данного вида, то в 2019 г. – 294409, то есть, за последние годы

произошел рост преступности данного вида более, чем в три раза. Растет и количество выявленных лиц, совершивших данные преступления: в 2018 г. – 24002 чел., а в 2019 г. – уже 44148 чел. (рост 84%)[1].

При этом криминал пока явно опережает правоохранительные органы в освоении современных информационных технологий. Особенно сложные для следствия проблемы возникают при использовании криминалом технологий блокчейн, криптовалют различного вида, в сочетании с самоисполняемыми контрактами. Само понятие рыночной стоимости любого объекта, который может стать предметом преступления, законодатель связал с вероятностью его отчуждения на открытом рынке по «договорной» цене. При этом признаки многих преступлений, связанных с рыночными операциями, неизбежно приобретают вероятностный характер, что с успехом используют преступники [7].

Таким образом, речь идёт о весьма специфичных, высокотехнологичных видах преступлений в сфере экономики, которые совершаются с помощью электронных документов, создающихся и хранящихся в определенных информационных системах, передающихся по компьютерным сетям в другие информационные системы, а соответствующие финансовые транзакции совершаются с помощью цифровых кодов в виртуальном информационно-сетевом пространстве, причем, в рамках недавно введенной в гражданское право системы цифровых прав экономических субъектов.

Соответственно, для выявления таких преступлений ряд оперативно-розыскных мероприятий и следственных действий приходится выполнять с учётом особенностей получения значимой для следствия информации из виртуального пространства по мере выявления и фиксации закодированных информационных следов. Эта задача осложняется ещё и тем, что такие преступления характеризуется длительностью сроков их приготовления, сложными формами соучастия, многоэпизодностью и выходом виртуального пространства за границы страны. Зачастую в поиске простых способов разрешения возникающих при этом проблем, они переводятся из правовой сферы в сугубо техническую либо информационно-технологическую, что неизбежно приводит к многочисленным ошибкам, характерным как для правотворчества, так и для правоприменения.

Результаты анализа особенностей «высокотехнологичных» преступлений в сфере экономики дают основание для вывода о необходимости кардинально менять подходы к методикам их выявления, раскрытия и расследования, к использованию при этом специальных знаний, причём не только и не столько в форме судебно-экономических и информационно-технических экспертиз, проводимых в СЭУ Минюста России и в ЭКП ОВД системы МВД России. Особого внимания заслуживают приобретаюшие приоритетное значение поисково-познавательные способы действий специалистов, представляющих различные правовые и естественно-технические науки и действующих в форме той самой экспертно-криминалистической деятельности, о которой говорилось ранее.

---

[1] Здесь и далее информация с официального сайта МВД России. URL: https://xn--b1aew.xn--p1ai/Deljatelnost/statistics.

Её преимущество перед судебной экспертизой заключается в том, что специалист действует в режиме текущего времени непосредственно и совместно со следователем или оперативным сотрудником, выявляемые им признаки преступления при этом документируются с соблюдением требований уголовно-процессуального законодательства, а соответствующая информация безотлагательно реализуется. При этом специалист оперативно использует необходимую компьютерную технику и информационные технологии.

Иначе говоря, в условиях нового информационного общества и становления различных отраслей цифровой экономики и финансов, необходимо, наконец, преодолеть межведомственные противоречия и, отказавшись от бесплодных дискуссий, сосредоточить усилия ЭКЦ МВД России и ФЦСЭ Минюста России на разработке и реализации программы государственного подхода к формированию системы научно-технического обеспечения уголовного судопроизводства, включая ЭКД и СЭД, как важнейших составляющих компьютерной криминалистики.

Вместе с тем, реализовать столь серьезное реформирование ЭКС в условиях ее высокой загрузки текущей деятельностью весьма проблематично. К тому же, научный потенциал этих организаций уже во многом утрачен и не позволяет рассчитывать на скорейшее практическое решение столь наукоемких задач государственной важности.

По результатам проведенного анализа можно сделать однозначный вывод о том, что для форсированной разработки научного фундамента современных разделов криминалистики, отвечающих актуальным государственным задачам борьбы с криминалом в условиях формирования новой системы общественных отношений необходимы новые подходы. Прежде всего, комплексный характер новых научно-практических задач требует организации коллективной разработки новых информационных технологий для борьбы с современной высокотехнологичной экономической преступностью силами ученых и специалистов различных отраслей наук уголовно-правового блока, экономики и информатики. Чтобы обеспечить целенаправленный характер таких коллективных исследований и разработок, интегрирующую роль должны сыграть ученые-криминалисты.

В этих целях следовало бы законодательно решить вопрос о создании единого государственного межведомственного научно-практического центра компьютерной криминалистики небольшой численности, обеспечивающего единство научно-методических подходов к разрабатываемым алгоритмам криминалистических и экспертных методик. Значительную часть научных разработок по созданию соответствующих частных экспертных и криминалистических методик целесообразно организовать в экспертно-криминалистических лабораториях (институтах) на базе ведущих профильных университетов и академий. Так будут созданы оптимальные, на наш взгляд, условия для реализации консолидированных усилий ведущих учёных – представителей не только экономических, но и юридических наук, а также математики, информатики, кибернетики. Соответствующий задел уже обозначен в наших предыдущих публикациях [1,2].

По мере создания и апробации в реальной практике новых криминалистических и экспертных методик, а также их реализации в виде интерактивных экспертных систем и создания соответствующих программных продуктов, они могут передаваться для практического использования не только в государственные экспертные учреждения, но и в следственные органы, прокуратуру, судебную систему. Кроме того, в базовых университетах могут проходить обучение и повышение квалификации сотрудники правоохранительных и следственных органов, экспертных учреждений, прокуратуры и судов. А лучшие выпускники данных университетов, прошедшие практику в экспертных лабораториях данных университетов и академий, и защитившие дипломы, магистрские и кандидатские диссертации, могут пополнить ряды сотрудников государственных правоохранительных и следственных органов.

Предварительные результаты проведенных исследований позволяют выделить на начальном этапе исследований и разработок два основных направления компьютерной криминалистики.

Первое из них сориентировано на обеспечение новым высокотехнологичным криминалистичесим инструментарием следователей и оперативных сотрудников, занимающихся выявлением, раскрытием и расследованием преступлений общеуголовного характера. Здесь уже имеется ряд серьезных заделов по технологиям обработки больших данных для распознавания и идентификации подозреваемых лиц по дактилоскопии, фотографиям, биологической и генетической информации. Для этого создаются и используются базы данных кримучетов, камер наблюдения, операторов мобильной связи и многие другие. Здесь на первый план исследований и разработок выходят не только проблемы чисто технического плана, но и вопросы обеспечения правового статуса тех сведений криминалистического характера, которые были получены с помощью элементов искусственного интеллекта различного вида.

Второе из направлений нацелено на решение криминалистических проблем обработки электронных документов экономических субъектов, которые имеют различный вид, информационный формат и правовой статус, чтобы найти эффективные способы выявления и фиксации закодированных информационных следов преступлений в сфере цифровой экономики и финансов. Сведения, имеющиеся в данной документации, а также в документации контрагентов фигурантов преступлений и правовых предписаниях, регламентирующих их деятельность, образуют сложно-структурированное информационно-правовое поле, работа в рамках которого требует применения новых криминалистических методик. При разработке соответствующих алгоритмов и информационных технологий, в том числе, с использованием элементов искусственного интеллекта, необходимо обеспечить применение средств контроля за сохранением правового статуса промежуточных и итоговых результатов индивидуальной и групповой обработки документированной информации.

Важно обратить внимание на ряд новых аспектов применения в системе компьютерной криминалистики элементов искусственного интеллекта, которые создаются для обработки информации без участия человека. По нашему мнению, такие результаты для уголовного судопроизводства в рамках действующего законодательства неприменимы, поскольку их невозможно проверить и оценить в рамках требований, предусмотренных ст. ст. 17, 87 и 88 УПК РФ. Поэтому речь идет о разработке новых

способов их применения в диалоговом режиме со следователем, в рамках соответствующих интерактивных экспертных систем, апробированных авторами в реальной практике более десяти лет назад.

Следует также учитывать, что взаимодействие субъектов преступлений в различных сферах цифровой экономики и финансов происходит в значительной, если не в большей части, их контактов не на привычном русском языке, на котором ведется вся финансово-экономическая документация, а на алгоритмических языках с помощью разнообразных компьютерных кодов. При этом использование переводчиков с алгоритмических языков, использованных фигурантами преступлений рассматриваемого вида, на русский язык, уголовно-процессуальным законодательством не предусматривается. Вполне очевидно, что назрела необходимость создания научных основ юридического алгоритмического языка, что может существенно повысить эффективность следственных действий по новым преступлениям, характерным для условий перехода к новому, информационному обществу и экономике знаний.

Имеющиеся заделы в данной сфере описаны в наших монографиях, ссылки на которые приведены в списке литературы по данной статье.

Список литературы

1. Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики : монография / М.: Экономика», 2020.
2. Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. / М.: Экономика, 2019.
3. Волынский А.Ф. К столетию экспертно-криминалистической службы МВД России: невыученные уроки истории // Труды Академии управления МВД России. 2019. №4.
4. Волынский А.Ф. Предмет криминалистики и «научный сепаратизм»: последствия и возможности их преодоления // Труды Академии управления МВД России. 2018. №1 (45).
5. Гросс Г. Руководство для судебных следователей как система криминалистики. М.: «ЛексЭст». 2020.
6. Криминалистика. Учебник. Под ред. А.Ф. Волынского, В.П. Лаврова. М.: ЮНИТИ-ДАНА. Закон и право. 2008.
7. Прорвич В.А. Актуальные проблемы расследования взаимосвязанных финансовых преступлений // Криминалистическое сопровождение расследования преступлений: проблемы и пути их решения. Материалы научно-практической конференции. (Москва, 19 февраля 2016 г.). М.: Московская Академия СК России. 2016.
8. Прорвич В.А. Об интегрированном подходе к организации расследования экономических преступлений // Вестник Московского университета МВД России имени В.Я. Кикотя. 2015. №10.

М.Р. Глушков

К вопросу о необходимости судебного решения для извлечения сведений о сообщениях из мобильных устройств

Аннотация. Доклад посвящен определению Конституционного Суда РФ от 25.01.2018 № 189-О по жалобе Прозоровского Д.А., которое многие юристы восприняли как правовую позицию, позволяющую получать доступ к переписке граждан без судебного решения – если такой доступ осуществляется в ходе осмотра мобильного устройства. Показано, что такой логики в решении Конституционного Суда не заложено. Все, о чем оно говорит – заявитель необоснованно посчитал, что его конституционные права нарушены положениями УПК РФ, не требующими судебного решения на осмотр предметов. По этой причине в приеме жалобы к рассмотрению было отказано. Также обозначена проблема с «осмотром и выемкой» сведений о сообщениях, которые введены в УПК РФ в 2016 году. Их возможность (тоже на основании судебного решения) заложена во вновь появившейся ч.7 ст.185 УПК РФ, однако процедура получения такого решения не определена. Как и возможность провести такие осмотр и выемку без судебного решения в случаях, не терпящих отлагательства.

Ключевые слова: тайна связи, судебное решение, Конституционный Суд РФ, определение по жалобе Прозоровского Д.А., сведения о сообщениях, случаи, не терпящие отлагательства, «пакет Яровой».

Значительное число преступлений в сфере высоких технологий, будь то мошенничества в сети Интернет, продажа там запрещенных предметов или махинации с банковскими картами, совершается с использованием средств мобильной связи.

По этой причине особый интерес для следствия представляют хранящиеся в них сведения и порядок их извлечения.

Это многоплановая проблема, только для обозначения различных ее сторон потребовалась бы целая статья, поэтому мы рассмотрим здесь лишь один из спорных моментов – извлечение сведений о сообщениях абонента (и самих сообщений).

Под такими сведениями (сообщениями) будем, в первую очередь, понимать: данные о соединениях абонентов сотовой связи, входящие/исходящие sms- и mms-сообщения, переписку в электронной почте, мессенджерах и социальных сетях[1].

Одним из дискуссионных вопросов, связанных с этими сведениями, является такой – требуется ли решение суда на их извлечение (или ознакомление с ними) в ходе осмотра мобильных устройств, которые были изъяты в законном порядке, но не на основании судебного решения?

[1] Другие средства коммуникации в данной работе не обозначаются, поскольку она посвящена правовым вопросам, а не техническим. Также не ставятся вопросы о том, подпадают ли под «сведения о сообщениях» - адрес электронной почты, номер абонента сотовой связи, IP-адрес, IMEI и данные о локации абонента. Они представляются частными случаями проблемы, которая должна быть решена сперва в целом.

На первый взгляд, никакой проблемы здесь нет – указанные сведения составляют охраняемую законом тайну связи и ее ограничение, т.е. правомерный доступ к сведениям, возможны только на основании судебного решения.

Об этом говорит ч.3 ст.63 (Тайна связи) Федерального закона от 07.07.2003 № 126-ФЗ «О связи» - «…ознакомление с информацией и документальной корреспонденцией, передаваемыми по сетям электросвязи и сетям почтовой связи, осуществляются только на основании решения суда».

Это же записано в Конституции РФ в явном виде – «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» (ч.2 ст.23).

Наконец, УПК РФ в ч.1 ст.13 предусматривает, что ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

Вместе с тем, в январе 2018 года Конституционный Суд РФ принимает по жалобе Прозоровского Д.А. определение[1], которое многими воспринято как правовая позиция, позволяющая осмотр мобильных устройств и сопутствующее ознакомление с хранящимися в них сообщениями без санкции суда.

Названия публикаций говорят сами за себя:

«КС разрешил следователям читать переписки с телефонов в ходе осмотра»[2],

«Конституционный суд разрешил следователям читать переписку с гаджетов без решения суда»[3],

«Изучение следователем содержимого телефона возможно без получения судебного решения»[4],

«КС назвал законным право следователей читать электронную переписку без решения суда»[5],

---

[1] Определение Конституционного Суда РФ от 25.01.2018 № 189-О "Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации".

[2] КС разрешил следователям читать переписки с телефонов в ходе осмотра // Право.ру [Электронный ресурс] URL: https://pravo.ru/news/200500/ (дата обращения 04.12.2020).

[3] Конституционный суд разрешил следователям читать переписку с гаджетов без решения суда // Роскомсвобода [Электронный ресурс] URL: https://roskomsvoboda.org/36348/ (дата обращения 04.12.2020).

[4] Изучение следователем содержимого телефона возможно без получения судебного решения // Коллегия адвокатов города Москвы «Отчерцова и партнеры» [Электронный ресурс] URL: https://advokat.msk.ru/izuchenie-sledstviem-soderzhimogo-telefona-vozmozhno-bez-polucheniya-sudebnogo-resheniya/ (дата обращения 04.12.2020).

[5] КС назвал законным право следователей читать электронную переписку без решения суда // Медиазона [Электронный ресурс] URL: https://zona.media/news/2018/02/14/taina-perepeski (дата обращения 04.12.2020).

«Следователи могут читать переписку с телефонов и планшетов без разрешения суда – КС»[1],

«КС: Для изучения содержимого телефона при его изъятии судебное решение не требуется»[2],

«Конституционный суд разрешил следователям читать переписки с телефонов, планшетов и компьютеров без разрешения суда»[3].

Перечисление можно было бы продолжать, но и эта выборка, в которую вошли известные правовые порталы, официальный источник адвокатского сообщества и один из ведущих уголовно-процессуальных журналов страны, видится вполне представительной.

Однако, насколько обоснованна такая точка зрения и вытекают ли из самого определения те лозунги, которые тиражируют СМИ? Для этого обратимся напрямую к тексту судебного решения[4].

Прозоровский Д.А., у которого на следствии изъяли электронные носители информации и обнаружили там сведения о текстах сообщений, просил суд признать протоколы этих осмотров недопустимыми доказательствами[5].

Суд в удовлетворении требований отказал, мотивируя отказ тем, что на такие осмотры и не требовалось судебных решений.

Прозоровский Д.А. обратился в Конституционный Суд, посчитав, что раз действующее законодательство[6] позволяет вскрыть переписку без судебного решения, то оно не соответствует Конституции РФ, в первую очередь – упомянутой ч.2 ст.23 о тайне связи[7].

Решение по жалобе, за вычетом установочной и резолютивной частей, изложено в двух абзацах. В первом КС сжато довел до правоприменителей положения ст.ст. 176 и 177 УПК РФ об осмотре предметов. Вся логика определения,

---

[1] Следователи могут читать переписку с телефонов и планшетов без разрешения суда – КС // Российское агентство правовой и судебной информации [Электронный ресурс] URL: http://rapsinews.ru/judicial_analyst/20180214/281936101.html (дата обращения 04.12.2020).

[2] КС: Для изучения содержимого телефона при его изъятии судебное решение не требуется // Адвокатская газета. Орган Федеральной палаты адвокатов [Электронный ресурс] URL: https://www.advgazeta.ru/novosti/ks-dlya-izucheniya-soderzhimogo-telefona-pri-ego-izyatii-sudebnoe-reshenie-ne-trebuetsya/ (дата обращения 04.12.2020).

[3] Конституционный суд разрешил следователям читать переписки с телефонов, планшетов и компьютеров без разрешения суда // Уголовный процесс [Электронный ресурс] URL: https://www.ugpr.ru/news/2035-sledovateli-mogut-chitat-perepisku-s-telefonov (дата обращения 04.12.2020).

[4] В этом всегда есть смысл, особенно когда речь идет о Конституционном Суде РФ.

[5] Очевидно, ссылаясь на тайну связи, ограничение которой произошло в отсутствие судебного контроля.

[6] Заявитель указал на ст.176 УПК РФ «Основания производства осмотра», ст.177 «Порядок осмотра» и ст.195 «Порядок назначения судебной экспертизы» (сведения из его мобильных устройств извлекались также экспертом).

[7] Имелись также ссылки на ч.1 ст.15 о прямом действии Основного закона, ч.1 ст.17. ст.18 о том, что права и свободы человека и гражданина в РФ признаются, гарантируются и действуют непосредственно. Также были приведены процедурные нормы ч.1 ст.45 о государственной защите прав и свобод, и ч.2 ст.50 о недопустимости доказательств, полученных с нарушением закона.

таким образом, сконцентрировалась во втором абзаце, который по этой причине необходимо процитировать полностью.

«Проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном статьей 125 УПК Российской Федерации».

Немного упрощая, но сохраняя при этом смысл написанного, можно сказать, что Конституционный Суд имел в виду следующее:

1) извлечение информации из абонентского устройства (посредством осмотра или экспертизы) не требует судебного решения;
2) тот, кто посчитает эти действия нарушением тайны связи, может обжаловать их в суд;
3) больше ничего.

Как представляется, в данном случае нет оснований полагать, что орган конституционного контроля хотел сказать больше, чем сказал. Увидеть в определении «разрешение» на доступ к переписке граждан вне судебного контроля можно лишь, сильно упрощая ситуацию – по логике «Если а) Прозоровский жаловался на то, что в отношении него действовали незаконно, и б) суд ему *отказал*, то в) с Прозоровским обошлись законно».

Решение, однако, построено на другой логике. Никаких правовых позиций (которые Конституционный Суд иногда приводит в своих решениях, подробно при этом мотивируя) здесь нет. Есть только отказ в принятии жалобы к рассмотрению. На том основании, что оспариваемые нормы, вопреки мнению заявителя, не нарушают его конституционных прав.

Нормы УПК РФ об осмотре предмета действительно не предусматривают санкции суда. Но осмотр *сам по себе* и не ограничивает тайну связи. Ходатайствовать перед судом о разрешении на это следственное действие лишь потому, что его объектом становится телефон - не нужно.

В телефоне может быть какая угодно информация, не составляющая тайну связи – фото-, видеофайлы, заметки, данные мобильных приложений[1].

Но как только заходит речь об охраняемой законом тайне – необходимо учитывать положения упомянутых уже Закона «О связи» и ч.2 ст.23 Конституции РФ.

Во-первых, Конституция РФ имеет прямое действие. Утверждать о возможности доступа к указанным выше сведениям в общем порядке (предусмотренном ст.176, 177 УПК РФ) значило бы игнорировать ее положения.

[1] Вопрос о доступе к сведениям о частной жизни гражданина выходит за рамки данной статьи.

Во-вторых, нормы, устанавливающие общий порядок осмотра (УПК РФ), и те, что требуют судебного решения для доступа к информации (Закон «О связи»), соотносятся как общие и частные – соответственно, в случае их конкуренции применяются вторые. Установленный в ч.2 ст.7 УПК РФ приоритет этого нормативного акта над остальными не является безусловным.

На это Конституционный Суд указывал неоднократно, например, в Определении от 8 ноября 2005 г. № 439-О "По жалобе граждан С.В. Бородина, В.Н. Буробина, А.В. Быковского и других на нарушение их конституционных прав статьями 7, 29, 182 и 183 Уголовно-процессуального кодекса Российской Федерации".

В данной ситуации адвокаты обжаловали обыски, проведенные в их кабинетах без судебного решения – ссылаясь при этом на ст.8 Закона «Об адвокатуре и адвокатской деятельности в РФ» (она предписывала проводить следственные действия в отношении адвоката, в т.ч. в его служебном помещении, только на основании судебного решения). Следствие и суды, отказавшие в удовлетворении жалоб, исходили из того, что уголовно-процессуальный закон требует обращаться в суд за разрешением лишь на обыск в жилище (ч.3 ст.182 УПК РФ).

Возникшую конкуренцию между этими нормами Конституционный Суд разрешил в пользу Закона «Об адвокатуре…», указав, во-первых, что

«…приоритет Уголовно-процессуального кодекса Российской Федерации перед другими федеральными законами не является безусловным: он может быть ограничен правилами о том, что в случае коллизии между различными законами равной юридической силы приоритетными признаются последующий закон и закон, который специально предназначен для регулирования соответствующих отношений», и, во-вторых, что

«разрешение в процессе правоприменения коллизий между различными правовыми актами должно осуществляться исходя из того, какой из этих актов предусматривает больший объем прав и свобод граждан и устанавливает более широкие их гарантии».

Эти недвусмысленные, казалось бы, положения были, однако, восприняты не везде.

Например, Фрунзенским районным судом г.Владивостока оставлено без удовлетворения ходатайство следователя о разрешении осмотра мобильного телефона обвиняемого В.

В апелляционном представлении прокурор Приморского края, цитируя положения ст.ст. 13, 29 и 165 УПК РФ, а также ст. 23 Конституции Российской Федерации, сослался на то, что ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений (к которым можно отнести и СМС-сообщения) допускается только на основании судебного решения.

Приморский краевой суд оставил решение суда первой инстанции в силе, указав, что осмотр сведений, находящихся на электронных носителях информации,

изъятых у обвиняемого, производится следователем в соответствии со ст. 176 УПК РФ и, для этого не требуется судебного решения[1].

Проблемы с реализацией конституционных положений о тайне связи связаны, вероятно, со сложностями процедурного характера.

Тайне связи в УПК РФ так или иначе посвящены лишь ст. 185 УПК РФ (арест, осмотр и выемка почтово-телеграфных отправлений), 186 (контроль и запись переговоров), 186[1] (получение информации о соединениях абонентов). Под эти три следственных действия был предусмотрен порядок обращения в суд (ст.165 УПК РФ). Который, в свою очередь, реализовывал соответствующие полномочия, предусмотренные в ч.2 ст.29 УПК РФ - п.8 (для ст.185), 11 (для ст.186) и 12 (для ст. 186[1] УПК РФ).

Других полномочий ни для следователя, ни для суда напрямую не предусмотрено. А в имеющийся правовой механизм просмотр содержимого мобильных устройств не укладывается.

В то же время с июля 2016 года отечественное уголовно-процессуальное законодательство в дополнение к упомянутым ст.ст. 185-186[1] УПК РФ содержит норму, действие которой, очевидно, распространяется на ознакомление с сообщениями, хранящимися в памяти мобильных устройств. Речь идет о ч.7 ст.185 УПК РФ, внесенной законом от 06.07.2016 № 375-ФЗ (одним из небезызвестного «пакета Яровой»).

Там сказано, что если «сведения, имеющие значение для уголовного дела, могут содержаться в электронных сообщениях или иных передаваемых по сетям электросвязи сообщениях, следователем по решению суда могут быть проведены их осмотр и выемка» (вероятно, все-таки не сведений, а носителей информации).

Однако и для этих действий была предусмотрена лишь возможность, но не порядок – ст.ст. 29 УПК РФ (о полномочиях суда) и 165 (о получении его разрешения на некоторые следственные действия) остались без изменений. Фактически «пакет Яровой» в этой своей части лишь продублировал уже имевшуюся и упомянутую ч.1 ст.13 УПК РФ о необходимости судебного решения на ограничение тайны связи.

Тем не менее, конституционные права граждан должны реализовываться вне зависимости от того, создан для этого механизм или нет. Показательно в этом смысле решение Омского областного суда № 22-2225/12 от 24 мая 2012 г. (кассационное определение). Им было отменено решение нижестоящего суда, отказавшего в удовлетворении жалобы защитника на действия следователя, который в ходе осмотра мобильного телефона ознакомился с перепиской фигуранта, не получил на это разрешения суда. В обоснование своей позиции кассационная инстанция, помимо прочего, указала:

---

[1] Апелляционное постановление Приморского краевого суда от 31.05.2016 по делу № 22-3453/2016 – приводится по: Васюков В.Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2 (10). С.10.

«Несмотря на то, что глава 25 УПК РФ прямо не закрепляет обязанность следователя получать судебное разрешение на осмотр СМС-переписки, эта обязанность вытекает из других норм как уголовно-процессуального закона и положений Конституции РФ, так и из международных норм, закрепленных в вышепоименованной Конвенции, подлежащих безусловному применению в РФ.

Очевидно, что приведенные выше положения предполагают защиту тайны личной жизни, требуя судебного разрешения на любые оперативно-розыскные мероприятия и следственные действия, которые могут ее нарушить».

В завершение отметим еще один недостаток упомянутого закона № 375-ФЗ от 06.07.2016. С одной стороны, он фактически поставил «осмотр и выемку» электронных сообщений в один ряд с другими следственными действиями, ограничивающими тайну связи (впрочем, не вполне удачно - не предусмотрев под них процедурные нормы, о чем только что говорилось).

С другой стороны, законом не были учтены особенности этих «осмотра и выемки». В отличие от упомянутых других следственных действий, которые сопряжены с техническими и организационными сложностями и потому всегда планируются заранее, эти два могут быть проведены гораздо оперативнее. Например, по «горячим следам», когда имеется фигурант, телефон которого, вероятно, содержит значимые для дела сведения.

Однако провести их без судебного решения по мотиву неотложности закон не позволяет – правила на этот счет (ч.5 ст.165 УПК РФ) остались прежними и позволяют «отсрочить» судебный контроль лишь для следственных действий, проводимых в жилище, для личного обыска, наложения ареста на имущество и выемки в ломбарде[1].

В этом видится явное упущение законодателя, который вместо продуманных и системных изменений в закон решает с его помощью частные задачи.

Характерно, что ч.5 ст.165 УПК РФ, изменения в которую напрашивались, «получила» их, но в другой части – вместе прежних 24 часов материалы следственных действий для подтверждения их законности должны быть представлены в суд в течение 3 суток.

Подводя итог, отметим:

1) ограничение тайны связи возможно лишь на основании судебного решения вне зависимости от способа такого ограничения;

2) Определение Конституционного Суда РФ от 25.01.2018 № 189-О по жалобе Прозоровского Д.А. не отменяет этого правила уже потому, что не было ему посвящено;

3) возможность ознакомления следователя со сведениями, составляющими тайну связи, путем изъятия и осмотра мобильных устройств – должно быть не

[1] … хотя на этот счет есть и другая точка зрения – «…в случае отказа лица - владельца мобильного телефона в даче согласия на его осмотр, но при необходимости производства осмотра в связи с его неотложностью, следователь может руководствоваться требованиями ч. 5 ст. 165 УПК РФ» - см. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2. С. 3. Эта позиция авторами, однако, никак не аргументируется.

только продекларировано в ч.7 ст.185 УПК РФ; на него должна быть распространена процедура ст.165 УПК РФ, в том числе – возможность неотложного производства без решения суда.

Список использованных источников

1. Васюков В.Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2 (10). С. 8-14.
2. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2. С. 2-4.
3. Изучение следователем содержимого телефона возможно без получения судебного решения // Коллегия адвокатов города Москвы «Отчерцова и партнеры» [Электронный ресурс] URL: https://advokat.msk.ru/izuchenie-sledstviem-soderzhimogo-telefona-vozmozhno-bez-polucheniya-sudebnogo-resheniya/ (дата обращения 04.12.2020).
4. КС: Для изучения содержимого телефона при его изъятии судебное решение не требуется // Адвокатская газета. Орган Федеральной палаты адвокатов [Электронный ресурс] URL: https://www.advgazeta.ru/novosti/ks-dlya-izucheniya-soderzhimogo-telefona-pri-ego-izyatii-sudebnoe-reshenie-ne-trebuetsya/ (дата обращения 04.12.2020).
5. Конституционный суд разрешил следователям читать переписки с телефонов, планшетов и компьютеров без разрешения суда // Уголовный процесс [Электронный ресурс] URL: https://www.ugpr.ru/news/2035-sledovateli-mogut-chitat-perepisku-s-telefonov (дата обращения 04.12.2020).
6. Конституционный суд разрешил следователям читать переписку с гаджетов без решения суда // Роскомсвобода [Электронный ресурс] URL: https://roskomsvoboda.org/36348/ (дата обращения 04.12.2020).
7. КС назвал законным право следователей читать электронную переписку без решения суда // Медиазона [Электронный ресурс] URL: https://zona.media/news/2018/02/14/taina-perepeski (дата обращения 04.12.2020).
8. КС разрешил следователям читать переписки с телефонов в ходе осмотра // Право.ру [Электронный ресурс] URL: https://pravo.ru/news/200500/ (дата обращения 04.12.2020).
9. Следователи могут читать переписку с телефонов и планшетов без разрешения суда — КС // Российское агентство правовой и судебной информации [Электронный ресурс] URL: http://rapsinews.ru/judicial_analyst/20180214/281936101.html (дата обращения 04.12.2020).

Л.В. Голоскоков

О модернизации парадигмы уголовного права в области противодействия преступлениям в сфере высоких и иных технологий

Аннотация. Рассмотрена существующая парадигма уголовного права – видеть преступления и преступность только через призму статей УК РФ. Это формально правильно, но не позволяет увидеть все причины и факторы роста преступности, понять в чём заключаются высокие технологий преступности. Модернизация парадигмы предложена путём расширения взгляда в смежные сферы и переходом только от одной борьбы к предупреждению преступности.

***Ключевые слова*:** парадигма, преступления, уголовное право, высокие технологии, Интернет.

Под научной парадигмой понимают принятую научным сообществом модель рациональной научной деятельности. В нашем исследовании под парадигмой уголовного права мы будем понимать совокупность устоявшихся воззрений, неписаных норм поведения, соблюдение которых происходит со строгостью большей, чем соблюдение писаных законов. Поэтому парадигму уголовного права можно вывести в точных формулировках и показать, что она есть вещь работающая, а не выдуманная, в отличие от многих писаных законов.

Когда говорят о преступлениях в сфере высоких технологий, обычно под ними подразумевают преступления в сфере компьютерной информации (гл. 28 УК РФ). Это естественно для УК РФ, в котором слово «технологии» есть лишь в нескольких статьях и не имеет значения «высоких технологий». УК РФ не видит других высоких технологий, кроме тех, что есть в главе 28.

УК РФ упоминает карты только в контексте «сбыт поддельных платёжных карт». Когда у гражданина выведывают по телефону необходимые данные для снятия с его банковских карт денег, и мы видим, как Банк России предупреждает об опасности исчезновения денег с карт, называет сумму 1,5 млрд рублей, похищенных за период пандемии, когда количество мошеннических звонков россиянам с марта по май выросло на 300 процентов по сравнению с такими же периодами прошлого года[1], можно ли считать, что эти технологии не высокие? Нет, это высокие технологии, и их критерием служит сумма похищенных средств и беспрерывный поток новых способов обмана, только вслед за которыми идут правоохранительные органы, но не успевают предотвращать и уменьшать этот поток. ЦБ РФ только предупреждает, а почему он ничего не сделал для предотвращения – потому что там высокие технологии, технологии постоянного опережения всех органов государства.

Ст. 186 УК РФ говорит об изготовлении поддельных денег или ценных бумаг – разве это не высокие технологии? Газета «Коммерсантъ», сообщает,

[1] ЦБ предупреждает: деньги могут исчезнуть с карт россиян. Замглавы департамента Банка России обратился к гражданам. 24 июля 2020, 04:00, https://primpress.ru/article/57460 (дата обращения 05.12.2020).

что «сотрудники полиции провели масштабную спецоперацию почти в десятке регионов, включая Москву и Санкт-Петербург, в результате которой был ликвидирован канал по изготовлению и сбыту поддельных денег. За два года существования преступная группа успела напечатать и запустить в оборот более полумиллиарда рублей … Реализация поддельных денег была налажена как через сеть сбытчиков в десятках регионов, так и через интернет-ресурс Hydra и его «зеркала», регулярно блокируемые Роскомнадзором … весной 2020 года сотрудники МВД ликвидировали другую крупную нелегальную типографию по производству фальшивых денег в Нижнем Новгороде, активно использовавшую в своей работе IT-технологии и успевшую отпечатать около 1 млрд руб.»[1]. Разве огромные полученные суммы с использованием для этого IT-технологии, Интернета, криптовалюты и сайта Hydra не являются доказательствами использования высоких технологий? И вот здесь возникает вопрос, где начинаются и где заканчиваются высокие технологии, измеряются ли они только степенью включения в преступный процесс новейших изобретений человечества?

Три грамма героина составляют в соответствии с п. 2 Примечания к ст. 228 УК РФ крупный размер[2], и хотя п.п. «б» п. 2 ст. 228.1 УК РФ говорит о сбыте наркотических средств, психотропных веществ или их аналогов, совершённых с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»), разве здесь речь о высоких технологиях? Нет, технологии в статье УК РФ упоминаются в качестве средства сбыта, отягощающего преступление. Высокие технологии здесь далеко не только в применении Интернета, сайта Hydra и других средств, включая сотовую связь, электронную почту, а в том, что организована глобальная сеть наркобизнеса.

Рассмотрим логику рассуждений: поймано лицо, сбывшее героин в крупном размере, например, 5 граммов. Использованы ли в его действиях высокие технологии? Если не считать в качестве таковых Интернет, тогда – нет. Увеличим ряд и положим, что имеет место сто таких случаев, затем сто тысяч, двести тысяч. Появились ли от увеличения количества высокие технологии в совершении преступления? Нет, в рамках нынешней парадигмы – это просто сумма рядовых случаев, все пойманы и отбывают наказание. Каждый

---

[1] Фальшивомонетчики заигрались. Раскрыта система производства денег в Дагестане для Москвы и Санкт-Петербурга // Газета «Коммерсантъ». № 215 от 24.11.2020, с. 4. https://www.kommersant.ru/doc/4584211 (дата обращения 05.12.2020).

[2] Постановление Правительства РФ от 01.10.2012 № 1002 (ред. от 29.07.2020) «Об утверждении значительного, крупного и особо крупного размеров наркотических средств и психотропных веществ, а также значительного, крупного и особо крупного размеров для растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса Российской Федерации» // «Собрание законодательства РФ», 08.10.2012, № 41, ст. 5624.

год осуждается известное количество лиц по таким статьям, система работает, отбывшие наказание выходят, их место занимают новые лица. Ничего не меняется, и в этом заключаются высокие технологии наркомафии.

Если теперь в этом процессе увеличить временной ряд и посмотреть, что произошло за 35-40 лет, то мы увидим произошедшую наркотизацию страны и появление наркомафии, которая построила сеть с высочайшими технологиями, и заключаются они в том, что этой сети совершенно безразлично, сколько людей в текущем году отправят отбывать наказание за хранение или сбыт наркотиков. Это для правоохранительных органов является достижением в текущем году большая цифра пойманных и осуждённых за преступления по статьям 228 и 228.1 УК РФ, а наркомафии все эти отчёты безразличны, потому что никакие аресты не разрушают её высокие технологии, состоящие в такой организации бизнеса, которая даёт устойчивые и только растущие доходы. Порядок цифр для России в 2014 году назвал директор ФСКН В. Иванов: 8 млн наркопотребителей, потребляющих в день на 4 млрд руб. или ежегодно на 1,5 трлн руб., общий рынок – 70 млрд долларов в год, а потери России – 200 млрд долларов в год[1].

Возглавляющий российскую секцию Международной полицейской ассоциации генерал-лейтенант Ю.Н. Жданов сообщил в интервью «Российской газете» о ситуации с наркотиками в условиях коронавирусной пандемии: «В России действительно выросло число преступлений, связанных со сбытом, производством и пересылкой наркотиков. Особенно заметный рост произошел в Липецкой, Новгородской, Тульской, Челябинской, Псковской, Курской областях, Чувашской республике, Республиках Марий Эл и Дагестан, Ставропольском крае. Но через месяц-другой это печальное «первенство» может перейти другим регионам»[2]. Это говорит о высоких технологиях организации бизнеса, ведь в условиях пандемии во всём мире и в России бизнес в целом падает, а наркобизнес, как мы видим, растёт.

Никто не говорит о высоких технологиях такого бизнеса, они никак не отражены в УК РФ, поскольку УК РФ видит единичное преступление, его обозначение в конкретных статьях, вскрытие, расследование и осуждение единичного преступника, а не работу против транснациональной сетевой структуры, сопряжённой с легальной банковской сетью, через которую проходят транзакции по оплате наркотиков валютой или криптовалютой; и электронные транзакции не являются чем-то новым, они действуют десятки лет. Вот эта устойчивость преступного бизнеса и является критерием наличия высоких технологий, под которыми нужно понимать сетевую организацию бизнеса, не убиваемую посадками рядовых или даже не рядовых членов преступной сети. Высокие технологии наркобизнеса ещё и в том, что ему всё равно, насколько эффективно действуют правоохранительные органы.

---

[1] *Иванов В.* Интервью на «Эхо Москвы» 06 октября 2014, 16:00, https://echo.msk.ru/programs/beseda/1413178-echo/ (дата обращения 06.12.2020)

[2] На острие иглы. Текст: Михаил Фалалеев. Российская газета - Федеральный выпуск № 139(8193), https://rg.ru/2020/06/28/kak-pandemiia-povliiala-na-oborot-narkotikov-v-rossii-i-v-mire.html (дата обращения 05.12.2020).

Действующая парадигма обращает внимание лишь на технологические новации (Интернет, Hydra, криптовалюта и др.) и уводит нас от анализа феноменов существования структур, которым не страшны никакие правоохранительные органы. Их высокая технологичность строится далеко не только на достижениях техники, но и на способах организации. Мы забываем, что борьба иерархических структур (правоохранительных органов) против сетевых структур (наркомафии) напоминает попытки уколом иглы разрушить единичный узел ткани (сети), которая вся состоит из узлов, и даже полная гибель любого узла не влияет на целостность всей сети.

Конечно, это не все сложности рассматриваемой проблемы.

Есть пример высоких технологий, которые право вообще не видит в качестве используемых в преступных целях. Это отток капитала из России. Легальный процесс. Экспертные оценки его таковы: О.О. Комолов полагает, что сумма чистого оттока капитала из российской экономики за последнее двадцатилетие составила более 1 трлн долларов США[1]. Цифры, приводимые другими экспертами, примерно такие же. После этого Россия ищет по всему миру инвестиции для развития. Вот где деяния с использованием высоких технологий уже подорвали национальную безопасность, но их применение не преступно: технологии обеспечивают легальный отток капитала, и правоохранительные органы не обязаны заниматься этими вопросами. Причиной стагнации экономики в первую очередь является отсутствие инвестиций. Национальная безопасность подорвана, а преступления нет. Высокие технологии спрятаны в организационной стороне: сделано так, что можно уничтожать экономику страны вывозом капитала десятки лет и не нести никакой ответственности. И это не какие-то новейшие, а старые правовые технологии.

Таким образом, парадигма уголовного права в области противодействия преступлениям в сфере высоких и иных технологий видит очень узкую сферу преступного через призму нескольких статей УК РФ, в то время как наступление на экономические интересы России множатся по всему фронту многомерных реалий, и как мы видим, существующие преступления при всём их масштабе не являются самими опасными. Опасность идёт от скрытых масштабов оттока капиталов и оборотов наркомафии, сопровождающихся ещё и ежегодной гибелью десятков тысяч российских граждан от передозировки наркотиков. Нынешняя парадигма права видит стык между уголовным и не уголовным явлением только в рамках УК РФ: есть статья или её нет. А пока её нет, на стыке отраслей права идёт процесс разрушения государства через отток капитала.

Пока будет произведена криминализация каких-то новых высокотехнологичных деяний, может пройти много времени, за период которого новое явление может набрать силу, которую будет неспособна остановить вся машина правоохранительных органов страны, и это случилось с наркотиками и с оттоком капитала. Поэтому нужно пересматривать парадигму уголовного права, которая,

---

[1] *Комолов О.О.* Отток капитала из России в контексте мир-системного анализа // Экономическое возрождение России. 2018. № 2 (56). С. 136.

не видя всю картину, слишком узко и поздно реагирует, и криминализирует деяние, когда оно становится неуправляемым. Нужно уходить от статичности в опережающую мир динамику, чтобы быть готовыми не только к борьбе с ними, но и к недопущению негативных разрушительных явлений. Это некий идеал. Сегодня он видится недостижимым, однако дело в том, что такая цель не ставится. Не было сто лет назад цели лететь в космос – и никто не летел. Поставили цель – полетели в космос. Так и в парадигме права и уголовного права – нужно поставить цель опережающего мышления и действия, а новые Королёв и Гагарин для полёта в невозможные дали появятся.

Список использованных источников

1. *Иванов В.* Интервью на «Эхо Москвы» 06 октября 2014, 16:00, https://echo.msk.ru/programs/beseda/1413178-echo/ (дата обращения 06.12.2020).
2. *Комолов О.О.* Отток капитала из России в контексте мир-системного анализа // Экономическое возрождение России. 2018. № 2 (56). С. 128-140.
3. На острие иглы. Текст: Михаил Фалалеев. Российская газета - Федеральный выпуск № 139(8193), https://rg.ru/2020/06/28/kak-pandemiia-povliiala-na-oborot-narkotikov-v-rossii-i-v-mire.html (дата обращения 05.12.2020).
4. Постановление Правительства РФ от 01.10.2012 № 1002 (ред. от 29.07.2020) «Об утверждении значительного, крупного и особо крупного размеров наркотических средств и психотропных веществ, а также значительного, крупного и особо крупного размеров для растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, для целей статей 228, 228.1, 229 и 229.1 Уголовного кодекса Российской Федерации» // «Собрание законодательства РФ», 08.10.2012, № 41, ст. 5624.
5. Фальшивомонетчики заигрались. Раскрыта система производства денег в Дагестане для Москвы и Санкт-Петербурга // Газета «Коммерсантъ». № 215 от 24.11.2020, с. 4. https://www.kommersant.ru/doc/4584211 (дата обращения 05.12.2020).
6. ЦБ предупреждает: деньги могут исчезнуть с карт россиян. Замглавы департамента Банка России обратился к гражданам. 24 июля 2020, 04:00, https://primpress.ru/article/57460 (дата обращения 05.12.2020).

Е.А. Емельянова

Проблемы взаимодействия Банка России с операторами связи при выявлении и расследовании преступлений, связанных с манипулированием рынком и неправомерным использованием инсайдерской информации

Аннотация. Статья посвящена проблеме получения Банком России информации от операторов связи при выявлении и проверке фактов манипулирования рынком и неправомерного использования инсайдерской информации. Автор исследует подходы судов к определению перечня информации, составляющей тайну связи. Анализируется изменение указанных подходов и его влияние на возможность оперативного выявления и расследования соответствующих правонарушений.

Ключевые слова: манипулирование рынком, инсайдерская информация, тайна связи, оператор связи, недобросовестные рыночные практики.

Уголовный кодекс РФ предусматривает ответственность за такие преступления, как манипулирование рынком[1] и неправомерное использование инсайдерской информации[2]. Между тем, выявление и расследование данных преступлений является, зачастую, крайне непростой задачей. Манипулирование рынком и неправомерное использование инсайдерской информации состоят в осуществлении одним или несколькими лицами, состоящими в сговоре, серии финансовых операций, охваченных единым умыслом и направленных на достижение преступного результата[3]. Как в случаях манипулирования рынком, так и в случаях неправомерного использования инсайдерской информации нарушителями применяются достаточно сложные схемы, в которые вовлечено множество субъектов, и доказать факт взаимодействия последних бывает весьма затруднительно.

Исследователи отмечают, что юридически грамотное решение вопроса о времени и месте совершения преступления как обстоятельств, подлежащих доказыванию по всем без исключения уголовным делам (п. 1 ч. 1 ст. 73 Уголовно-процессуального кодекса РФ), имеет не только научное, но и большое прикладное значение, являясь важнейшим фактором, влияющим на результативность расследования и судебного рассмотрения уголовного дела о любом преступлении, включая манипулирование рынком и неправомерное использование инсайдерской информации. Являясь элементами события преступления, время и место

[1] Ст. 185.3 Уголовного кодекса РФ.

[2] Ст. 185.6 Уголовного кодекса РФ.

[3] Арестова Е.Н., Борбат А.В. Проблемы доказывания времени и места совершения преступления по уголовным делам о манипулировании рынком и неправомерном использовании инсайдерской информации // Российский следователь. 2019. № 6. С. 17-20 // СПС КонсультантПлюс.

совершения уголовно наказуемого деяния являются первыми обстоятельствами, с которых, собственно, и начинается процесс доказывания[1].

Для установления факта манипулирования рынком или неправомерного использования инсайдерской информации, определения места и времени совершения данных противоправных деяний огромное значение имеет информация, которой могут располагать операторы сотовой связи. Более того, иногда данные операторов связи представляют собой единственные доказательства для обнаружения и доказывания существования инсайдерской или манипулятивной сделки.

Как отмечается в Регламенте № 596/2014 Европейского парламента и Совета Европейского Союза[2], подобные данные могут устанавливать личность лица, ответственного за распространение ложной или вводящей в заблуждение информации, или факт нахождения людей в контакте в определенное время и факт, что отношения существуют между двумя или более людьми. Именно поэтому важно, чтобы компетентные органы имели возможность требовать существующие записи телефонных разговоров, электронных сообщений и записи о передаче данных[3].

Между тем, на практике именно с получением информации от операторов сотовой связи, имеющей принципиальное значение для процесса доказывания по уголовному делу, возникает ряд проблем.

Соблюдение требований Федерального закона № 224-ФЗ «О противодействии манипулированию рынком и неправомерному использованию инсайдерской информации»[4] (далее – Федеральный закон № 224-ФЗ) с 01.09.2013 контролирует Банк России (ранее соответствующие функции выполняла Федеральная служба по финансовым рынкам, далее – ФСФР).

По получении информации о возможном нарушении требований Федерального закона № 224-ФЗ (например, после выявления нестандартной сделки организатором торгов) Банк России проводит проверку, в том числе запрашивает необходимую информацию у лиц, ею располагающих. Так, в силу ч. 1 ст. 16 Федерального закона № 224-ФЗ юридические лица, их должностные лица и работники обязаны по мотивированному письменному требованию (запросу) Банка России представлять в срок, указанный в данном требовании (запросе), имею-

---

[1] Арестова Е.Н., Борбат А.В. Проблемы доказывания времени и места совершения преступления по уголовным делам о манипулировании рынком и неправомерном использовании инсайдерской информации // Российский следователь. 2019. № 6. С. 17-20.// СПС КонсультантПлюс.

[2] REGULATION (EU) No 596/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC// Official Journal of the European Union N L 173. 12.06.2014. P. 1.

[3] См. п. 65 Преамбулы Регламента № 596/2014.

[4] Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства Российской Федерации. -2010. -№ 31. – Ст. 4193.

щиеся у них документы, объяснения, информацию (в том числе электронные документы и информацию в электронной форме), включая сведения, составляющие коммерческую, служебную, банковскую тайну, тайну связи (в части информации о почтовых переводах денежных средств) и иную охраняемую законом тайну (за исключением государственной и налоговой тайны), которые необходимы для осуществления проверки. В дальнейшем, по окончании проверки, уже может быть поставлен вопрос о привлечении виновных лиц к уголовной ответственности.

К сожалению, на практике во многих случаях получение запрашиваемой Банком России информации являлось проблематичным, что не позволяло оперативно провести проверку в полном объеме по «горячим следам». Еще на заре применения Федерального закона № 224-ФЗ, в 2012-2013 годах, ФСФР несколько раз, отследив нестандартные сделки и придя к предварительному выводу о неправомерном использовании инсайдерской информации, пыталась инициировать процесс сбора соответствующих доказательств для целей последующего привлечения виновных к ответственности - адресов электронной почты, с которых пользователями осуществлялась переписка, информации о том, какими абонентами использовался определенный телефонный номер, предоставлялись ли по данному номеру услуги связи в определенный период, детализации счетов абонента, какими еще номерами пользовался абонент и т.д. Оператор связи отказывался предоставлять запрашиваемые сведения со ссылкой на нежелание нарушать законодательство о персональных данных, тайне переписки, телефонных переговоров, и данная позиция поддерживалась судами[1].

Существует и более поздняя судебная практика подобного рода. Так, в одном из дел Банком России запрашивались информация о лице, использовавшем определенный IP-адрес в определенные даты и время, копии всех договоров о предоставлении услуг, заключенных оператором связи с этим лицом, справка, содержащая сведения обо всех способах оплаты услуг общества, оказываемых в рамках договоров, использованных за определенный период. По мнению суда, запрашиваемая регулятором информация не могла быть предоставлена, так как относилась к тайне связи[2]. Как отмечал суд в другом схожем деле, детализация счета конкретного абонента - физического лица, и сведения об идентификационных номерах абонентских устройств (IMEI) составляют тайну телефонных переговоров, так как составляют не только сведения, содержащиеся в телефонном соединении (разговоре), но и данные о таких соединениях между конкретными абонентами (дате, времени, продолжительности), а также любые иные сведения передаваемые, сохраняемые и устанавливаемые с помощью аппаратуры связи[3].

В настоящее время суды несколько изменили свой подход к трактовке того, какую именно информацию, запрашиваемую Банком России в целях проверки

---

[1] См., например, Постановление Девятого арбитражного апелляционного суда от 15.11.2013 № 09АП-28908/2013 по делу № А40-56142/13.

[2] Постановление Арбитражного суда Уральского округа от 31.05.2016 № Ф09-4708/16 по делу № А50-21341/2015.

[3] Постановление ФАС Московского округа от 12.03.2014 № Ф05-1622/2014 по делу № А40-56142/13-130-551.

соблюдения требования Федерального закона № 224-ФЗ, следует относить к тайне связи, что в определенной степени облегчает регулятору выявление фактов манипулирования рынком и неправомерного использования инсайдерской информации. В качестве примера можно рассмотреть Постановление Арбитражного суда Уральского округа от 22.01.2020 № Ф09-9457/19 по делу № А50-17377/2019.

Так, Банком России были запрошены у оператора связи следующие документы и сведения: сведения в отношении всех пользователей услуг связи, которым выделялись определенные абонентские номера, в том числе с указанием периода использования абонентских номеров каждым из пользователей услуг связи с приложением копий документов, подтверждающих изложенную информацию, договоров, соглашений, анкет клиентов, а также изменений и дополнений к данным документам; сведения о том, какие услуги связи предоставлялись по абонентским номерам в определенный период; информация об иных абонентских номерах пользователей; справка, содержащая сведения обо всех способах оплаты услуг оператора связи пользователями; справка, содержащая сведения о полных реквизитах всех счетов, открытых в кредитных организациях, с которых пользователями были проведены операции по оплате услуг оператора связи; списки сетевых адресов (диапазоны IP-адресов), которые выделялись пользователям услуг связи в определенный период.

Как отметил суд, исходя из правовой позиции Конституционного Суда Российской Федерации, отраженной в его определениях 02.10.2003 № 345-О, от 21.10.2008 № 528-О-О, к информации, составляющей тайну телефонных переговоров, относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям необходимо получение судебного решения. Информация о периоде использования абонентских номеров каждым из пользователей услуг связи с приложением копий документов, подтверждающих изложенную информацию, договоров, соглашений, анкет клиентов, а также изменений и дополнений к данным документам, сведения о предоставляемых услугах, об абонентских номерах, датах заключения и расторжения договоров с пользователями услуг, сведения о способах оплаты услуг заявителя, сведения о банковских счетах, с которых пользователями в конкретный временной интервал проведены операции по оплате услуг общества, несмотря на аргументы заявителя, непосредственно к тайне связи не относится. Следовательно, правовые основания для отказа в предоставлении подобной информации у оператора связи отсутствовали.

Аналогичные аргументы были приведены в Постановлении Семнадцатого арбитражного апелляционного суда от 15.10.2019 № 17АП-13165/2019-АК по делу № А50-17377/2019.

Вышеописанный подход судов к трактовке понятия «тайна связи» представляется более взвешенным, и изменение судебной практики в этой части следует приветствовать.

В заключение можно отметить, что информация, составляющая тайну связи, в части, не касающейся информации о почтовых переводах денежных средств, может быть запрошена Банком России в порядке, предусмотренном ч. 7 ст. 14 Закона № 224-ФЗ. Согласно указанной норме в случае, если для предотвращения, выявления и пресечения неправомерного использования инсайдерской информации и (или) манипулирования рынком требуется проведение оперативно-розыскных мероприятий, Банк России обращается в органы внутренних дел в установленном законодательством Российской Федерации порядке. Порядок взаимодействия Банка России и органов внутренних дел определяется совместным нормативным правовым актом Банка России и федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел.

Между тем, до настоящего времени соответствующий акт еще не принят, и это следует признать существенным упущением, препятствующим своевременному выявлению и расследованию фактов манипулирования рынком и инсайдерской торговли, на что справедливо обращается внимание исследователями[1]. Наличие разработанного порядка взаимодействия Банка России и органов внутренних дел позволило бы избежать или минимизировать проблемы, связанные с оперативным получением Банком России информации, относящейся к тайне связи.

Е.А. Загрядская

Проблемные вопросы квалификации преступного деяния, предусмотренного статьей 151-2 Уголовного кодекса Российской Федерации, совершенного в сети Интернет

Аннотация. Данная статья посвящена норме Уголовного кодекса Российской Федерации, предусматривающей ответственность за вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего. Автором предпринята попытка проанализировать содержание указанной нормы на предмет сложностей, которые могут возникнуть в судебно-следственной практике при ее применении. В статье обращено внимание на то, что круг противоправных и опасных для жизни деяний законодательно не определен, а также на то, что за полем правового регулирования остались вовлечение в опасные игры путем агитации и публичных призывов в сети Интернет.

Ключевые слова: несовершеннолетние, сеть Интернет, склонение или вовлечение, противоправность, опасность для жизни, публичные призывы, целенаправленность, уголовная ответственность, правоприменение.

---

[1] Методы противодействия неправомерному использованию инсайдерской информации и манипулированию рынком в системе обеспечения экономической безопасности государства : автореферат дис. ... кандидата экономических наук : 08.00.05 / Ахмедов Тимур Чингизович ; [Место защиты: С.-Петерб. ун-т МВД РФ]. - Санкт-Петербург, 2015. С. 19-20.

В настоящее время можно констатировать, что произошла криминализация деяний, ранее практически не встречавшихся в судебно-следственной практике, но ставших столь распространенными теперь в связи с возросшей и продолжающей возрастать информатизацией общества. Противодействие преступлениям в сфере компьютерной информации в отношении детей и подростков является одним из важнейших направлений уголовной политики государства, о чем свидетельствует появление в Уголовном кодексе Российской Федерации (далее – УК РФ) составов, таких как, например, статьи 110-1, 110-2, 242-1, 151-2, а также дополнение уже существующих квалифицирующим признаком – «совершенное с использованием информационно-телекоммуникационных сетей, включая сеть Интернет».

Одной из таких норм, направленных на охрану несовершеннолетних, является статья 151-2 УК РФ, предусматривающая ответственность за вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни. Эта статья стала реакцией законодателя на очередную интернет - игру «Беги или умри», которая завлекала детей по принципу «групп смерти». Несовершеннолетние, вступившие в нее, должны были перебежать дорогу на максимально близком расстоянии от приближающихся автомобилей. В связи с этим необходимо обратить внимание, что законодателем в часть 2 статьи 151-2 УК РФ совершенно правильно включен такой квалифицирующий признак, как сопряженность с публичным выступлением, использованием публично демонстрирующегося произведения, средств массовой информации или информационно-телекоммуникационных сетей.

Вместе с тем анализ содержания указанной нормы позволяет утверждать, что в судебно-следственной практике могут возникнуть сложности при квалификации рассматриваемого преступления.

Во-первых, законодательно не закреплен круг противоправных деяний, которые «представляют опасность для жизни». Так, в пояснительной записке к проекту закона, которым в уголовное законодательство введены составы, касающиеся защиты прав несовершеннолетних, указывалось: «примером опасной деятельности, запрещенной статьей 151-2 УК РФ, являются случаи вовлечения лицами, достигшими восемнадцатилетнего возраста, подростков в «трейн-серфинг» (проезд на крыше поезда) или иные виды смертельно опасного «зацепинга», «руфинг» (незаконное проникновение на крыши высоких зданий) либо иные занятия[1]. По мнению некоторых авторов в качестве противоправных действий, представляющих опасность для жизни несовершеннолетнего, можно назвать опасные формы «паркура» (городская акробатика)[2]. Безусловно, паркур

---

[1] О. В. Поликашина О некоторых аспектах квалификации склонения и вовлечения несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2 УК РФ) URL: https://cyberleninka.ru/article/n/o-nekotoryh-aspektah-kvalifikatsii-skloneniya-i-vovlecheniya-nesovershennoletnego-v-sovershenie-deystviy-predstavlyayuschih-opasnos

[2] Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. Разделы VII - VIII: В 4 т. (постатейный) / А.В. Бриллиантов, А.В. Галахова, В.А. Давыдов и др.; отв. ред. В.М. Лебедев. М.: Юрайт, 2017. Т. 2; СПС "КонсультантПлюс" (дата обращения: 18.12.2020)

в отдельных его проявлениях, может привести к травмам и повреждениям, которые могут повлечь за собой смерть, однако считать занятие им противоправными действиями, на наш взгляд, представляется неверным[1].

Если буквально толковать диспозицию статьи 151-2 УК РФ, к действиям, в совершение которых вовлекается несовершеннолетний, законодатель предъявляет следующие требования: во-первых, они должны быть противоправными, то есть нарушать установленные предписания и запреты, а, во-вторых, они должны представлять опасность для жизни несовершеннолетнего, который их совершает.

Говоря о противоправности, необходимо акцентировать внимание на уровне законодательных актов, в нарушение положений которых вовлекается несовершеннолетний. Например, законодательство об административных правонарушениях в Российской Федерации представлено как на федеральном, так и на региональном уровне. При этом законодательство об административных правонарушениях субъектов Российской Федерации, как правило, разнопланово и устанавливает запреты, не предусмотренные в качестве административных правонарушений в КоАП РФ. Так, например, в ч. 3 ст. 7.6 Кодекса Нижегородской области об административных правонарушениях установлена ответственность за нарушение правил пользования метрополитеном, а именно: проезд на подножках вагонов, сзади вагонов, на крыше вагонов, между вагонами и в иных не предназначенных для этого местах….[2]. Перечисленные противоправные действий, безусловно, могут создавать опасность для жизни, поэтому вовлечение несовершеннолетних в их совершение может рассматриваться как преступление, предусмотренное ст. 151-2 УК РФ. Однако в тех субъектах, где нет такого административного запрета, правоприменитель не сможет подобные действия квалифицировать как преступные. Действительно, в жизни немало не запрещенных законом действий, которые могут создавать реальную опасность для жизни человека, тем более детей и подростков, поэтому законодателю необходимо либо отказываться от признака противоправности при определении деяния, в которое вовлекается несовершеннолетний, либо устанавливать четкий перечень этих деяний, который будет пересматриваться «с изобретением новых видов таких деяний».

В соответствии со ст. 151.2 УК РФ, уголовная ответственность предусматривается за склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, путем уговоров, предложений, обещаний, обмана, угроз или иным способом, совершенное лицом, достигшим восемнадцати-

---

[1] Е.П. Коровин Некоторые теоретические и практические проблемы квалификации преступления, предусмотренного ст. 151.2 УК РФ URL: https://yandex.ru/turbo/wiselawyer.ru/s/poleznoe/94544-nekotorye-teoreticheskie-prakticheskie-problemy-kvalifikacii-prestupleniya-predusmotrennogo

[2] Кодекс Нижегородской области об административных правонарушениях (с изменениями и доп.) принят Законом Нижегородской области от 20 мая 2003 г. № 34-3. URL: http://docs.cntd.ru/document/944917687 (дата обращения: 18.12.2020)

летнего возраста, при отсутствии признаков склонения к совершению самоубийства, вовлечения несовершеннолетнего в совершение преступления или в совершение антиобщественных действий. Характерным признаком склонения или вовлечения является целенаправленность, то есть стремления вовлекающего должны быть направлены на конкретного несовершеннолетнего и на совершение им конкретного противоправного действия. Как упоминалось ранее в нашей статье, в глобальной информационной сети распространение получила интернет - игра «Беги или умри», в которой воздействие оказывалось на неопределенный круг лиц. В связи с этим, возникает вопрос: возможно ли привлечение к уголовной ответственности по ст. 151-2 УК РФ за призыв к совершению противоправных действий, представляющих опасность для жизни несовершеннолетнего, который был не персонифицирован или рассчитан на неопределенное количество потерпевших? На наш взгляд, вовлечение несовершеннолетнего в совершение противоправных действий, заведомо для виновного представляющих опасность для жизни несовершеннолетнего, следует отграничивать от публичных призывов и агитации. Вовлечение в совершение противоправных действий, опасных для жизни, должно быть направлено на одного или несколько, но конкретных несовершеннолетних, а публичные призывы не обращены персонально к кому-либо, охватывают, как правило, неопределенно широкий круг лиц и носят общий характер.

Поэтому организация деятельности, направленной на побуждение желания к совершению противоправных действий, представляющих опасность для жизни несовершеннолетнего, путем распространения информации о способах и видах вышеуказанных действий или призывов к совершению этих действий в сети Интернет, остались вне пределов правового регулирования данной нормы.

Кроме того, в информационно-телекоммуникационных сетях, включая сеть «Интернет», встречаются случаи склонения, а также распространения самими несовершеннолетними информации, тем или иным способом побуждающей несовершеннолетних к совершению противоправных действий, представляющих опасность для их жизни (например, селфи на краю крыши многоэтажного дома). Вместе с тем, учитывая, что детерминантами поведения несовершеннолетних являются отсутствие страха, участие «за компанию», бунтарство, можно с уверенностью сделать вывод о том, что данные опасные для жизни деяния привлекают детей, и пресечь их необходимо как можно скорее, иначе количество жертв только продолжит расти. Поэтому некоторыми учеными предлагается ввести уголовную ответственность за склонение лиц, не достигших совершеннолетия, к действиям, последствия которых несут опасность для них не с 18 , а с 16 лет[1].

В завершение отметим, что внесение в уголовный закон состава преступления, предусмотренного ст. 151-2, продиктовано стремлением законодателя выработать эффективный механизм противодействия сложившейся де-факто общественно опасной системе вовлечения несовершеннолетних лиц в различные

[1] Минюст предлагает уголовную ответственность с 16 лет за склонение детей к насилию через интернет URL: https://roskomsvoboda.org/42576/

формы самоповреждающего и опасного поведения. Вместе с тем обнаружившаяся рассогласованность положений уголовного закона не способствует его эффективному применению на практике и может создать дополнительные проблемы для правоприменителя. С учетом сказанного необходима дальнейшая работа над положениями уголовного закона, предусматривающими ответственность за склонение или иное вовлечение несовершеннолетнего в совершение противоправных действий, представляющих опасность для жизни несовершеннолетнего.

Список ичспользованных источников

1. Уголовный кодекс Российской Федерации, СПС "КонсультантПлюс" (дата обращения: 18.12.2020).
2. Кодекс Нижегородской области об административных правонарушениях (с изменениями и доп.) принят Законом Нижегородской области от 20 мая 2003 г. № 34-З. URL: http://docs.cntd.ru/document/944917687 (дата обращения: 18.12.2020).
3. Комментарий к Уголовному кодексу Российской Федерации. Особенная часть. Разделы VII - VIII: В 4 т. (постатейный) / А.В. Бриллиантов, А.В. Галахова, В.А. Давыдов и др.; отв. ред. В.М. Лебедев. М.: Юрайт, 2017. Т. 2; СПС "КонсультантПлюс" (дата обращения: 18.12.2020).
4. Коровин Е.П. Некоторые теоретические и практические проблемы квалификации преступления, предусмотренного ст. 151.2 УК РФ URL: https://yandex.ru/turbo/wiselawyer.ru/s/poleznoe/94544-nekotorye-teoreticheskie-prakticheskie-problemy-kvalifikacii-prestupleniya-predusmotrennogo.
5. Минюст предлагает уголовную ответственность с 16 лет за склонение детей к насилию через интернет URL: https://roskomsvoboda.org/42576/.
6. Поликашина О. В. О некоторых аспектах квалификации склонения и вовлечения несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2 УК РФ) URL: https://cyberleninka.ru/article/n/o-nekotoryh-aspektah-kvalifikatsii-skloneniya-i-vovlecheniya-nesovershennoletnego-v-sovershenie-deystviy-predstavlyayuschih-opasnos.

А.П. Киселев

Проблемы взаимодействия операторов сотовой связи, провайдеров, владельцев сайтов с правоохранительными органами при раскрытии и расследовании преступлений

Аннотация. В последние годы все большее распространение получают преступления, совершенные с использованием информационно-телекоммуникационных технологий. Однако их раскрываемость остается невысокой. Существуют определенные проблемы при расследовании данных преступлений.

Ключевые слова: преступления, информационно-телекоммуникационные технологии, мобильная связь, Интернет, провайдер.

С развитием науки и техники, средств мобильной связи, распространением коммуникации между людьми с использованием площадок различных социальных сетей, происходило «параллельное» использование вышеуказанных технических новшеств для совершения преступлений. Безусловно, в этой связи по своей распространенности, а порой и изощренности, лидирующее место занимают преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, куда входят общественно-опасные деяния с использованием или применением расчетных (пластиковых) карт, сети «Интернет», средств мобильной связи.

Чтобы увидеть положение указанной категории преступлений в общей структуре преступности, приведем некоторые статистические данные. За 10 месяцев 2020 года на территории России зарегистрировано 420,7 тыс. преступлений (рост 75,1 %). Говоря об общем числе зарегистрированных преступлений, их удельный вес увеличился с 14,0% в январе - октябре 2019 года до 24,2%, из них: 243,6 тыс. преступлений (рост 92,9%) с использованием сети «Интернет», 181,2 тыс. преступлений (рост 96,1 %) с использованием средств мобильной связи. Раскрываемость таких преступлений, из общего числа уголовных дел, находившихся в производстве, составила 22%, то есть более чем три из четырёх совершенных преступлений остались нераскрытыми. Стоит отметить, что из всех регионов России лидером по темпам прироста зарегистрированных преступлений является г. Санкт-Петербург – почти 582%, чтобы понять состояние картины по данному региону и величину так называемого «отрыва», следует отметить, что на втором месте по численности прироста находится Республика Ингушетия – чуть более 167 %, г. Москва находится на 8 месте по данному показателю с темпом прироста почти 112 %[1].

Безусловно, сведения, передаваемые, получаемые телефонными абонентами, владельцами аккаунтов, как собственно и их регистрационные данные, находятся под защитой и относятся к охраняемой законом тайне.

В соответствии с ч. 1 ст. 53 Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» сведения об абонентах и оказываемых им услугах связи, ставшие известными операторам связи в силу исполнения договора об оказании услуг связи, являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации. Предоставление третьим лицам сведений об абонентах-гражданах может осуществляться только с их согласия, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами[2].

Необходимость получения данных сведений при расследовании уголовного дела для раскрытия преступления, установления обстоятельств, подлежащих доказыванию, относится к таким исключительным случаям и требует судебного

[1] Официальный сайт Министерства внутренних дел Российской Федерации.
[2] Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

решения, возбуждаемого следователем, как правило, в порядке, предусмотренном ст. 186.1 УПК РФ (получение информации между абонентами и (или) абонентскими устройствами.

Ходатайства о получении решений на представление интересуемой следствие информации возбуждаются перед судом на первоначальной стадии расследования, если же речь идет о преступлении, совершенном непосредственно с использованием сети Интернет – то незамедлительно после возбуждения уголовного дела, поскольку исходные данные об абонентских устройствах могут иметься в распоряжении следователя еще со стадии доследственной проверки.

Как показывают исследования, самой популярной социальной сетью среди россиян по числу сообщений в месяц является «ВКонтакте»[1] что, несомненно, накладывает отпечаток на количество и характер преступлений с использованием указанной электронной платформы для обмена информацией.

Безусловно, порой чтобы отождествить личность, указанную в аккаунте и реально существующим человеком, установить его регистрационные данные, характер переписки и направляемых сообщений, которые могут быть использованы в процессе доказывания, необходимо затребовать данную информацию (в порядке, предусмотренном ст. 186.1 УПК РФ) у владельца (администратора) социальной сети, и наиболее часто – в ООО «ВКонтакте».

Анализ сложившейся следственной практики показывает, что взаимодействие с ООО «ВКонтакте» по истребованию интересуемой следствие информации, находится на крайне низком уровне, что связано с длительным процессом обработки указанным обществом запросов и подготовки на них ответов. Как правило, предоставление информации следует по прошествии 2-3 месяцев с момент направления запроса, при этом зачастую администратор социальной сети безосновательно просит уточнить отдельные параметры запрашиваемой информации, что фактически приводит к удвоению времени подготовки ответа на него. Свою медлительность администратор объясняет своей загруженностью, нехваткой кадров и т.п. Данное обстоятельство в лучшем случае приводит к затягиванию процесса расследования, в худшем – приводит к пополнению статистики низкой раскрываемости преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Для исправления сложившейся ситуации, видится необходимость совершенствования правового регулирования в рассматриваемой сфере, в том числе путем внесения изменений в нормативные правовые акты, касающихся сокращения сроков предоставления запрашиваемой информации.

Список использованных источников

1. Интернет-статья «Названы самые популярные соцсети среди россиян». Https://4pda.ru/2020/11/30/378841.

[1] Интернет-статья «Названы самые популярные соцсети среди россиян». Https://4pda.ru/2020/11/30/378841.

2. Официальный сайт Министерства внутренних дел Российской Федерации.
3. Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28 ст. 2895.

Н.Е. Краснова

Проблемы привлечения подростков к распространению экстремистских материалов через сеть Интернет

Аннотация. В статье рассмотрены проблемы привлечения подростков к распространению экстремистских материалов через сеть Интернет. Автор приходит к выводу, что необходимо принять меры по пресечению указанных выше действий, так как данные меры будут способствовать сокращению количества случаев вовлечения подростков в экстремистскую деятельность и позволят снизить уровень распространения ими в сети Интернет материалов экстремистского характера. Известно, что связь экстремизма и терроризма достаточно тесная, и пресечение действий в рамках распространения первого позволит сохранить множество жизней, которые могут оборваться в случае совершения каких-либо террористических актов.

Ключевые слова: подростки, распространение материалов экстремистского содержания, сеть Интернет.

В современном мире сеть Интернет представляет собой информационный ресурс, который предлагает пользователям огромный массив данных различного характера. Посредством социальных сетей и форумов люди разного возраста общаются между собой, ведут коммерческую деятельность и делятся друг с другом самой различной информацией.

В связи с высокой скоростью распространения информации в сети Интернет, а также с огромной потенциальной аудиторией, способной воспринимать различную информацию как посредством вирусных технологий, так и через непосредственные обращения, направляемые посредством электронных писем или завязывания диалогов, особую опасность вызывает расширение массивов информации экстремистского характера. Распространение данной информации преследуется по закону, однако, несмотря на возможные санкции как в разрезе административного, так и уголовного права, материалы экстремистского содержания все чаще и чаще появляются на различных сайтах и в социальных сетях[1].

Особую категорию пользователей электронных ресурсов составляют подростки, большая часть из которых достаточно длительное время проводит в сети Интернет. С учетом психологических и возрастных особенностей подростки, особенно в виртуальном пространстве, легко идут на диалог, особенно с теми людьми, которые располагают их к себе, обещают подросткам различные преференции (вознаграждение, продвижение страницы в соцсетях, повышение оценок фотографий подростков с личных страниц в соцсети и пр.).

[1] Рамазанова З.Г. Некоторые проблемы правового регулирования проявлений молодежного экстремизма в сети Интернет // Закон и право. 2019. № 3.

Часто через социальные сети подростков вовлекают в экстремистские группировки, руководство которыми обычно осуществляют совершеннолетние граждане. Подростки, которые привлекаются в подобные объединения, достаточно часто не интересуются идеологией такой группировки, фактором привлечения здесь служит различные лозунги такого объединения, а также привлекательная внешняя атрибутика. Кроме того, желание быть не таким как все, также выступает активным движущим фактором, способствующим обращению подростков к экстремистской деятельности. Также часто подростки недооценивают опасности подобных группировок, для несовершеннолетних это просто приятное времяпровождение в кругу сверстников[1].

Сетевой принцип объединения подростков в экстремистские группировки в сети Интернет позволяет их руководителям достаточно долго уходить от ответственности за свои деяния: обычно подростки, после соответствующей информационной обработки последних, объединяются в небольшие ячейки, которые действуют автономно. Проведение больших групповых акций экстремистской направленности в сети Интернет с участием подростков обычно не практикуется.

Наиболее уязвимыми для вербовщиков выступают подростки, которые находятся в ситуации возможного «попадания» в поле экстремистской активности. Соответственно, нужно учитывать жизненную ситуацию подростков, которая предполагает возможность привлечения их к распространению экстремистских материалов и привлечению к экстремистской деятельности средствами сети Интернет. Это могут быть:

– выходцы из неблагополучных, социально-дезориентированных семей, с низким социально-экономическим статусом, недостаточным интеллектуальным уровнем, имеющим склонность кповедению, которое нарушает социальные или культурные нормы, вызывая настороженное и враждебное отношение окружающих (алкоголизм, наркомания, физическое и морально-нравственное насилие);

– «золотая молодежь», склонная к безнаказанности и вседозволенности, экстремальному досугу и рассматривающая участие в экстремистской субкультуре как естественную форму времяпрепровождения;

– дети, подростки, молодежь, имеющие склонность к агрессии, силовому методу решения проблем и споров, с неразвитыми навыками рефлексии и саморегуляции; носители молодежных субкультур, участники неформальных объединений склонных к поведению, которое нарушает социальные или культурные нормы, вызывая настороженное и враждебное отношение окружающих уличных компаний[2].

---

[1] Мельникова Д. П. Правовое регулирование экстремистской деятельности в сети Интернет [Электронный ресурс]. URL: http://www.scienceforum.ru/2013/151/2191.

[2]Методические рекомендации по профилактике и противодействию экстремизму в молодежной среде (разработаны Минспорттуризмом России совместно с МВД России и ФСБ России) // Наша молодежь.- 2011.- № 6.

Именно указанные категории подростков наиболее восприимчивы к экстремистским настроениям и активно выполняют задания организаторов по распространению экстремистских материалов в среде Интернет. Это могут быть следующие действия:

– размещение по просьбе организаторов на своих страницах призывов к межнациональной розни, завуалированных под невинные картинки или фотографии, которые, как считает подросток, «просто должны набрать максимальное количество «лайков»;

– обращение к своим друзьям в социальных сетях с просьбой прокомментировать ту или иную информацию экстремистского содержания;

– рассылка в форумы информации экстремистского содержания в форме спама и другие виды деятельности.

Подобные виды заданий подростки не оценивают серьезно, они, как им кажется, просто увеличивают свою популярность в той или иной социальной сети. Однако недооценка серьезности таких поступков может повлечь за собой различные виды ответственности, минимальной из которых будет являться административная.

Однако нельзя не заметить, что согласно положениям КоАП РФ, за совершение противоправных действии экстремистского характера могут быть подвергнуты лица, достигшие шестнадцатилетнего возраста. Соответственно, организаторы и вдохновители процесса распространения экстремистских материалов и настроений в сети Интернет стараются, оставшись в тени, привлечь для выполнения своих заданий подростков, которые не достигли указанного возраста, и которых, соответственно, к административной ответственности привлечь нельзя. Данный фактор усложняет пресечение процесса распространения материалов экстремистского содержания в сети Интернет, так как подростки, не достигшие 16 летнего возраста, остаются безнаказанными, и данная безнаказанность становится причиной продолжения ими противоправных действий в данном направлении[1].

В данной ситуации необходимо адекватно оценивать действия несовершеннолетних, связанные с распространением в социальных сетях информации экстремистского содержания за тем, чтобы определить, носят ли они единичный характер или же выступают систематическими. В первом случае возможны случайные действия подростков, связанные с недооценкой последними экстремистского содержания распространяемых материалов и с желанием разместить на своей странице информацию, привлекающую внимание друзей и подписчиков.

Во втором случае, если информация экстремистского характера появляется на странице подростка регулярно, а характер такой информации становится все агрессивнее, то необходимо говорить о том, что действиями такого подростка руководит человек, который прямо заинтересован в распространении такой информации. Соответственно, в данной ситуации необходимо пресечь указанное

[1]Видова Б.Б. Экстремистское движение как тип девиантного поведения // Молодой ученый. 2014. № 21. С. 493.

распространение противозаконных материалов и выявить организатора, который стоит за действиями подростка.

В случае выявления лиц, которые руководят действиями подростка по распространению в сети Интернет материалов экстремистского характера, равно как и подростков, ведущих подобную деятельность и достигших 16 лет, такие лица должны быть привлечены к ответственности по ст.ст. 20.3, 20.3.1, 20.29 КоАП РФ. Согласно нормам данных статей, виновные должны нести ответственность за пропаганду либо публичное демонстрирование, изготовление, а также за сбыт в целях пропаганды нацистской атрибутики или символики, либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами, а также за массовое распространение экстремистских материалов, включенных в опубликованный федеральный список экстремистских материалов, а равно их производство либо хранение в целях массового распространения, за возбуждение ненависти либо вражды или унижение человеческого достоинства.

В качестве наказания данная статья предусматривает административный штраф от одной тысячи до двадцати тысяч рублей с конфискацией указанных материалов и оборудования, использованного для их производства.

Однако нельзя забывать о том, что такие правонарушения в подростковой среде, равно, как и привлечение подростков к распространению информации экстремистского характера, должны пресекаться до их совершения посредством применения профилактических мер. Среди мер профилактики, направленных на пресечение распространения подростками в сети Интернет информации экстремистского содержания, можно назвать следующие[1]:

– организация профилактической работы по месту работы или учебы подростков, в рамках которой подростки должны информироваться о том, какие материалы в сети Интернет могут носить экстремистский характер, и в чем заключена опасность их распространения;

– организация досуга подростков, входящих в «группы риска» с целью привлечения их к общественно-полезной или творческой деятельности;

– проведение бесед с родителями подростков, входящих в «группы риска» для оказания помощи в недопущении вовлечения их детей в деятельность по распространению материалов экстремистского содержания.

– своевременное выявление и пресечение экстремистских настроений в подростковой среде, проведение профилактических бесед с такими подростками.

Данные меры будут способствовать сокращению количества случаев вовлечения подростков в экстремистскую деятельность и позволят снизить уровень распространения ими в сети Интернет материалов экстремистского характера. Кроме того, это также позволит снизить динамику распространения указанных

[1] Методические рекомендации по профилактике и противодействию экстремизму в молодежной среде (разработаны Минспорттуризмом России совместно с МВД России и ФСБ России) // Наша молодежь.- 2011.- № 6. – С. 181.

материалов силами совершеннолетних граждан, поскольку подростки, по достижению ими совершеннолетия, не будут совершать противоправные поступки, связанные с распространением экстремистских материалов. Известно, что связь экстремизма и терроризма достаточно тесная, и пресечение действий в рамках распространения первого позволит сохранить множество жизней, которые могут оборваться в случае совершения каких-либо террористических актов.

Список использованных источников

1. Бидова Б.Б. Специально-криминологическое противодействие молодежному экстремизму //Актуальные вопросы юридических наук: Матер. Междунар. заоч. науч. конф. (г. Пермь, март 2012 г.). Челябинск: Два комсомольца, 2012. С. 76.
2. Видова Б.Б. Экстремистское движение как тип девиантного поведения // Молодой ученый. 2014. № 21. С. 493-495.
3. Методические рекомендации по профилактике и противодействию экстремизму в молодежной среде (разработаны Минспорттуризмом России совместно с МВД России и ФСБ России) // Наша молодежь.- 2011.- № 6.
4. Мельникова Д. П. Правовое регулирование экстремистской деятельности в сети Интернет [Электронный ресурс]. URL: http://www.scienceforum.ru/2013/151/2191
5. Рамазанова З.Г. Некоторые проблемы правового регулирования проявлений молодежного экстремизма в сети Интернет // Закон и право. 2019. № 3
6. Татаров ЛА. Молодежный экстремизм. Вопросы противодействия: отечественный и зарубежный опыт // Гос-во и право. 2016. № 4. С. 29-37.

А.В. Лаур
Д.В. Тимощенко

Вопросы контроля мессенджеров в целях пресечения террористической деятельности

Аннотация. В статье рассмотрен вопрос контроля мессенджеров для безопасности населения, которое нуждается в защите от противоправных действий со стороны преступников и как такой контроль поможет правоохранительным органам в предупреждении, раскрытии и пресечении преступлений террористической направленности

Ключевые слова: террористическая направленность, мессенджеры, социальные сети, бэкдор, оперативно-розыскные мероприятия, судебная информация (UFED).

Согласно статистическим данным, количество преступлений террористической направленности за январь-июль 2020 года возросло на 21,7% и составило

1183 преступлений[1]. Данный рост связан с пандемией COVID-19, так как в сложившихся условиях террористы еще активнее уходят в онлайн[2]. Террористическая деятельность создает внутреннюю угрозу национальной безопасности и общественного порядка, поэтому необходимо оперативно решать задачи, стоящие перед МВД России по содействию в борьбе с терроризмом[3].

Террористическая деятельность – это деятельность, включающая в себя:

а) организацию, планирование, подготовку, финансирование и реализацию террористического акта;

б) подстрекательство к террористическому акту;

в) организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации террористического акта, а равно участие в такой структуре;

г) вербовку, вооружение, обучение и использование террористов;

д) информационное или иное пособничество в планировании, подготовке или реализации террористического акта;

е) пропаганду идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности[4].

Из вышеприведенного определения можно сделать вывод о том, что большинство из действий, которые входят в понятие террористической деятельности можно реализовывать через мессенджеры. Например, вербовка граждан в террористические организации, как правило, осуществляется через социальные сети[5].

Отсюда вытекает необходимость осуществления контроля мессенджеров. В первую очередь это необходимо для безопасности населения, которое нуждается в защите от противоправных действий со стороны преступников. Во-вторых, данный контроль поможет правоохранительным органам в предупреждении, раскрытии и пресечении преступлений террористической направленности.

В настоящие время сотрудники правоохранительных органов могут получить доступ к перепискам в программах мгновенного обмена сообщениями – мессенджерах, разными способами:

1. изъятие материального носителя;
2. дистанционный перехват сообщений;
3. получение информации по запросу.

---

[1] Статистический сборник Генеральной прокуратуры Российской «Состояние преступности в России за январь – июнь 2020 года» - стр. 7

[2] Российская газета [Электронный ресурс] // В Совбезе РФ прогнозируют серьезную активизацию террористов. URL: https://rg.ru/2020/10/20/v-sovbeze-rf-prognoziruiut-sereznuiu-aktivizaciiu-terroristov.html (дата обращения 21.10.2020).

[3] Противодействие органов внутренних дел экстремизму и терроризму: учебное пособие / С.Н. Миронов и др.; под ред. Ф.К. Зиннурова. – М.: ДГСК МВД России, 2018. – с.13

[4] Федеральный закон "О противодействии терроризму" от 06.03.2006 № 35-ФЗ

[1] Новости в России и мире – ТАСС [Электронный ресурс] // Генпрокуратура: террористы вербуют граждан в основном через мессенджеры и соцсети. URL: https://tass.ru/obschestvo/5134521 (дата обращения 21.10.2020)

Изъятие материального носителя переписки осуществляется в соответствии с ч.1, ст.15 Федерального закона «Об оперативно-розыскной деятельности»[1] в рамках оперативно-розыскного мероприятия и заключается в открытом изъятии телефона, смартфона либо другого носителя, на котором содержится переписка. Для этого обязательно наличие у должностного лица постановления о проведении оперативно-розыскного мероприятия. Также необходимо составить протокол в соответствии с требованиями Уголовно-процессуального кодекса Российской Федерации.

Помимо этого, сотрудники правоохранительных органов могут изъять электронные носители при задержании человека, в ходе личного обыска, при осмотре места происшествия, при производстве выемки, либо в ходе допроса, допрашиваемое лицо, может добровольно выдать электронный носитель информации.

Извлечь информацию, которая содержится на компьютере, при условии его непосредственного изъятия можно в ходе такого оперативно-розыскного мероприятия как получение компьютерной информации.

В случаях, когда владелец электронного устройства отказывается предоставить его должностным лицам, то извлечение информации может осуществляться с помощью универсального устройства извлечения судебной информации (UFED).

Если сотрудники правоохранительных органов не имеют возможности изъять устройство, на котором содержится необходимая информация, тогда можно получить информацию с помощью дистанционного перехвата сообщений. Здесь сотрудники негласно устанавливают устройства аудио- и видеозаписи для наблюдения за лицом, которое представляет интерес для следствия. Еще можно установить контакт с человеком, который общается с данным лицом, в целях добровольного предоставления первым переписки.

В добавок существует еще множество способов с помощью, которых можно извлечь информацию в режиме онлайн в рамках оперативно-розыскного мероприятия – снятие информации с технических каналов связи.

Стоит отметить, что вышеуказанные способы довольно сложные с технической и организационной сторон.

Для того чтобы упростить процесс получения информации правоохранительным органам можно предложить использование бэкдоров. Суть бэкдоров заключается в том, что компании, владеющие мессенджерами, специально создают уязвимые места в шифровании. Благодаря этому, сотрудники правоохранительных органов зная «ключ» смогут беспрепятственно получить нужную им информацию.

Бывают случаи, когда нет возможности изъять материальный носитель или дистанционно перехватить сообщения, тогда правоохранительные органы имеют право направить запрос о содействии в компетентный орган, то есть в компанию, которая владеет мессенджером.

---

[1] Федеральный закон «Об оперативно-розыскной деятельности». – Москва : Проспект, 2019. – с.12.

При направлении запроса о содействии правоохранительные органы сталкиваются с проблемой, что информация в данных компаниях хранится определённый период, и как правило, этот период очень небольшой от 24 часов до 90 дней приблизительно.

Для решения данной проблемы можно обязать компании, которые владеют мессенджерами, хранить информацию более долгий срок, например, от 6 до 12 месяцев, так как необходимость в определенной информации может появиться в любой момент в ходе расследования уголовного дела.

Таким образом можно сделать вывод о том, что в деятельности правоохранительных органов существует много способов получения информации в мессенджерах, но все они трудоемкие, поэтому необходимо изобретать и создавать новые методы получения информации.

Список использованных источников

Учебная литература:

1. Противодействие органов внутренних дел экстремизму и терроризму: учебное пособие / С.Н. Миронов и др.; под ред. Ф.К. Зиннурова. – М.: ДГСК МВД России, 2018. - С.144

Нормативно – правовые акты:

1. Федеральный закон "О противодействии терроризму" от 06.03.2006 № 35-ФЗ
2. Федеральный закон «Об оперативно-розыскной деятельности». – Москва : Проспект, 2019. – С.16.

Интернет – источники:

1. URL: https://tass.ru/ Новости в России и мире – ТАСС (дата обращения 21.10. 2020)
2. URL: https://rg.ru/ Российская газета (дата обращения 21.10.2020)

Иные источники:

1. Статистический сборник Генеральной прокуратуры Российской «Состояние преступности в России за январь – июнь 2020 года». - С.52.

А.А. Лебедева

Некоторые аспекты деятельности Следственного комитета Российской Федерации при расследовании киберпреступлений

Аннотация. В статье рассмотрены некоторые аспекты деятельности СК России при расследовании киберпреступлений, проиллюстрированные примерами следственной практики. В последнее время объектами целенаправленных кибер атак становятся школьники. Лица, не достигшие возраста совершеннолетия, вовлекаются в преступную деятельность по средствам Сети Интернет. Учитывая темпы роста киберпреступлений, ориентированность их на подрастающее поколение, в Следственном комитете Российской Федерации создано подразделение по расследованию киберпреступлений и преступлений в сфере компьютерной информации.

***Ключевые слова*:** киберпреступления, расследование, следственные действия, следователи СК России.

В последние годы, с учетом тотальной цифровизации всех сфер жизнедеятельности общества, особенно в условиях так называемой «короновирусной пандемии» возросло число киберпреступлений.

Цифровизация и виртуализация общественной жизни не только отразились на современных тенденциях преступности, но и актуализировали вопросы использования информационных технологий при противодействии этому негативному социальному явлению. Причем существующие научные разработки давно вышли за рамки обеспечения расследования преступлений в сфере компьютерной информации. Активно разрабатываются методики собирания и исследования цифровой информации, сохраненной в различных информационных объектах.

В центральном аппарате СК РФ создано подразделение по расследованию киберпреступлений.

По мнению А.И. Бастрыкина, новый отдел «должен … стать неким связующим «элементом», объединяющим усилия государственных ведомств, научных учреждений и специалистов для эффективного и слаженного противодействия преступным явлениям в информационной сфере.[1]

Следует отметить, что так как отсутствует легальное определение киберпреступлений, то к данной категории, в соответствии с различными классификациями относят так же и общественно опасные деяния, запрещенные уголовным законодательством Российской Федерации, совершенные в том числе с применением компьютерных технологий. В указанных случаях способ реализации преступного умысла частично или целиком воплощается по средствам применения в том числе Сети Интернет, использования социальных сетей и различного рода мессенджеров.

Интернет ресурсы стали «площадкой», на которой в виртуальной реальности присутствуют и незащищенные слои населения- пенсионеры, люди преклонного возраста, несовершеннолетние, а также лица, не достигшие 16- ти летнего возраста, которые становятся объектами целенаправленных атак в Сети Интернет.

Представим лишь некоторые способы преступного воздействия на несовершеннолетних, а также лиц, не достигших 16-ти летнего возраста, представленные в СМИ[2].

---

[1] См.: Интервью А.И. Бастрыкина 10 июля. INTERFAX.RU//URL// https://www.interfax.ru/russia/716874 (дата обращения 25.01.21)

[2] См.: Данные официального сайта СК РФ//URL// https://sledcom.ru/(дата обращения 25.01.21).

Март-апрель 2020 г.	ГСУ СКР по Санкт-Петербургу возбуждено уголовное дело по ч. 1 ст. 272 УК РФ (неправомерный доступ к компьютерной информации). Следствием установлено, что к срыву уроков школьников причастен ведущий канал Russia Paver на платформе YouTube, который неоднократно (27.03.2020 и 06.04.20020) незаконно подключался к обучающему процессу в формате онлайн-трансляциям, во время подключений, представляясь сотрудником Министерства образования России, дискредитировал, вел себя «вызывающе», «хамил».
26 июня 2020 г.	Сервис Центральной избирательной комиссии РФ подвергся DDoS-атаке, направленной на срыв досрочного электронного Общероссийского голосования по внесению поправок в основной закон Российской Федерации.
Январь 2021 г.	Следственный комитет России возбудил уголовные дела по факту вовлечении несовершеннолетних в участие в несанкционированных акциях протеста по средствам Сети Интернет, именно через социальные сети «TikTok», «ВКонтакте», «Facebook», «Twitter», «Instagram», сервис «YouTube».

В указанных выше примерах так называемы «кибер атаки» осуществлялись на преимущественно «школьную аудиторию».

Несовершеннолетние лица- более уязвимы на просторах Сети Интернет, чем в обычной социальной действительности. Преступнику, пользующемуся преимуществами Интернет пространства (отсутствие физического контакта жертвы и преступника) – легче войти в доверие несовершеннолетнего, используя мнимый созданный профиль, обманом, хитростью и психологическими манипуляциями склонить к совершению вполне определенных, нужных преступнику действий.

В настоящее время следователи подразделений Следственного комитета России качественно расследуют и направляют в суд уголовные дела, условно отнесенные к категории киберпреступлений, и одновременно затрагивающие права и интересы в том числе несовершеннолетних граждан.

Так, Следственными органами Следственного комитета России по Чувашской Республике направлено в суд уголовное дело по обвинению лица в вовлечении несовершеннолетней в совершение преступления, а так покушении на незаконный сбыт наркотических веществ в крупном размере.

Следствием установлено, что осенью 2019 года обвиняемый через социальную сеть познакомился с несовершеннолетней К, которой предложил за денежное вознаграждение отправиться в лесной массив, где из указанного места забрать сверток, отвести по указанному адресу. Так, 13 декабря 2019 года девушка

и её знакомый приехали в лесной массив, где из тайника забрали сверток, содержащий наркотическое средство массой более 100 граммов. Их действиями при этом руководил обвиняемый, который давал им указания относительно места нахождения тайника и дальнейших действий путем переписки через интернет-мессенджер. Забрав сверток с наркотическим средством из тайника, молодые люди вернулись в город Чебоксары. Однако на остановке общественного транспорта обвиняемые были задержаны сотрудниками полиции[1].

Следует отметить, что при производстве в жилище обыска у обвиняемого одним из ключевых моментов было отыскание ПК и смартфона с помощью которых он подыскивал исполнителей, и вовлекал в преступную деятельность, по средствам которых осуществлял передачу указаний по поиску тайника с наркотическими веществами, транспортировке «запрещенного груза», реализации. Данные предметы и содержащаяся в них информация составили основу доказательной базы по уголовному делу.

Отдельно стоит упомянуть об использовании криминалистического комплекса UniversalForensicExtractionDevice (UFED). Данный аппаратный комплекс используется следователями-криминалистами СК России при извлечении так называемых цифровых следов преступлений из мобильных устройств.

Современная преступность бросает вызов правоохранительной системе в форме реализации преступного умысла в кибер пространстве, сотрудники СК России компетентны расследовать преступления с учетом последних тенденций.

Список использованных источников

1. Антонов О.Ю. Типичные следственные ситуации при расследовании сексуальных преступлений, совершаемых с использованием информационно-телекоммуникационных сетей: специфические особенности и пути разрешения // Российский следователь. 2018. № 2. С. 3 - 7.;
2. Интервью А.И. Бастрыкина 10 июля. INTERFAX.RU//URL// https://www.interfax.ru/russia/716874 (дата обращения 25.01.21);
3. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26 - 28.
4. Данные официального сайта СК РФ//URL// https://sledcom.ru/(дата обращения 25.01.21).

Е.А. Маркова

Тайное хищение денежных средств с банковского счета

Аннотация. Статья посвящена исследованию преступления, совершенного способом тайного хищения денежных средств с банковского счета. Отражены проблемы правового регулирования уголовной ответственности, противоречия в позициях рос-

[1] URL// https://chuvashia.sledcom.ru9 (дата обращения 21.12.20).

сийских судов при квалификации данного преступления. С целью решения актуальных проблем, для более четкого отграничения кражи, совершенной с банковского счета, от других преступлений, предложена авторская редакция новой статьи 158[2] УК РФ.

Ключевые слова: электронные средства платежа, сеть «Интернет», преступность, хищение, кража, уголовная ответственность.

В соответствии с действующим законодательством, хищение - противоправное посягательство на отношения собственности, совершенное в предусмотренных уголовным законом формах и видах (ст. 158–162, 164 УК РФ[1]), т. е. посредством кражи, мошенничества, грабежа, разбоя, присвоения, растраты[2]. При этом, кражу, включая кражу с банковского счета, как и в отношении электронных денежных средств (п. «г» ч. 3 ст.158 УК РФ) выделяет признак тайности изъятия, предусматривающий в т.ч. хищение имущества посредством воздействия на электронный банковский счет, компьютерную систему электронных платежных средств.

Особо квалифицированный признак состава кражи (п. «г» ч. 3 ст.158 УК РФ) введен в Уголовный кодекс РФ Федеральным законом от 23 апреля 2018 г. № 111-ФЗ[3], как тайное хищение чужого имущества, совершенное с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159[3] УК РФ). Подобные хищения характеризуются значительными угрозами и иными негативными особенностями - скрытность; трансграничный, дистанционный и интеллектуальный характер; невозможность предотвращения преступлений традиционными средствами профилактики преступности.[4] В большинстве случаев преступники не обладают информацией о потерпевших и совершают преступления посредством применения различных инновационных методов[5].

В целях противодействия преступлениям, совершенным в информационной системе в России, действует Концепция о долгосрочном социально-экономическом развитии на период до 2020 г.[6], разработанная по поручению Президента РФ В.В. Путина; Стратегия развития информационного общества на период

---

[1]Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 07.11.2020) // СЗ РФ. 1996. № 25. Ст. 2954.

[2]Зенин И. А. Гражданское право. Особенная часть: учебник. 18-е изд., пер. и доп. М.: Издательство Юрайт, 2018. С.85.

[3]Федеральный закон от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СЗ РФ. 2018. № 18.Ст. 2581.

[4]Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. №1. С. 104-106.

[5]Дмитренко А.П., Русскевич Е.А. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 5 (61). С. 18.

[6]Распоряжение Правительства Российской Федерации от 17 ноября 2008 года № 1662-р (ред. от 28.08.2019) «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // СЗ РФ. 2008. № 4. Ст. 5489.

2017–2030 г. г.[1], в которой отражено значение безопасной информационной среды, развивающейся на базе популяризации ресурсов, способствующих развитию традиционных духовно-нравственных ценностей.

Проблемы в сфере безналичных расчетов, однако, остаются. По сведениям Генеральной прокуратуры, более 50 процентов от всех зарегистрированных в России преступлений в 2020 г. (январь-июнь) составили хищения чужого имущества. При этом, каждый пятый факт совершенных деяний имел непосредственное отношение к тайному хищению денежных средств с банковского счета (74 241), каждый десятый подобный случай выявлен в г. Москве (7 848)[2]. Увеличение удельного веса данных хищений отмечается не только на российской территории - это мировая проблема и тенденция.

В настоящее время существует неопределенность в части соотношения указанного вида кражи и других хищений, посягающих на безналичные денежные средства и на наш взгляд, требует законодательного регулирования. Однако необходимо признать, что ряд актуальных проблем остается вне поля правового регулирования, что усугубляется отсутствием единства позиций судов. Особую актуальность приобрел вопрос о соотношении кражи (тайное хищение) по п. «г» ч. 3 ст.158 УК РФ и мошенничества (ст.159[3] УК РФ).

Причинами этого следует считать отсутствие четкой правовой формы уголовного закона и современных разъяснений Верховного Суда РФ. К сожалению, Постановление Пленума от 30 ноября 2017 г. № 48[3], раскрывающее положения о квалификации хищений, посягающих на безналичные денежные средства, после принятия Федерального закона от 23 апреля 2018 г. № 111-ФЗ, которым в УК РФ включен новый признак состава кражи - п. «г» ч.3 ст.158 УК РФ, устарело.

В указанной связи, следует признать необоснованность квалификации судами действий по ст. 159[3] УК РФ, как мошенничества с использованием электронных средств платежа, если совершена оплата чужой платежной картой путем умолчания о принадлежности карты другому титульному владельцу[4]. Данную позицию разделяют многие представителя научного сообщества, в частности, доктор

---

[1]Указ Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс] URL: http://www.pravo.gov.ru. (дата обращения 01.12.2020).

[2] Генеральная прокуратура. Состояние преступности в России. январь-июнь 2020 г. [Электронный ресурс] URL: https://genproc.gov.ru/smi/news/regionalnews/news-1774076/ (дата обращения 01.12.2020).

[3]Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации». 2018. № 2.

[4]Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Удмуртской Республики 26 марта 2019 года по делу № 22-52 (г. Ижевск) [Электронный ресурс] URL: https://vs--udm.sudrf.ru/modules.php?name. (дата обращения 01.12.2020).

Апелляционное Постановление Калининградского областного суда от 10 декабря 2018 года по делу № 22-1703/2018 (г. Калининград) [Электронный ресурс] URL: https://oblsud--kln.sudrf.ru/modules.php?name (дата обращения 01.12.2020).

юридическим наук, профессор С.В. Скляров, утверждающий также о необходимости внести в сложившуюся противоречивую ситуацию определенную ясность[1]. По мнению Е. В. Евстратова, при совершении кражи (п. «г» ч.3 ст.158 УК РФ) лицо, предоставляющее карту, умалчивает, а лицо, принимающее оплату, не осознает противоправность совершаемых действий[2].

Приведем позицию Верховного Суда РФ по данному вопросу. Так, Судебная коллегия по уголовным делам, рассмотрев в судебном заседании уголовное дело по кассационному представлению заместителя Генерального прокурора Российской Федерации В. Я. Гриня на определение Шестого кассационного суда общей юрисдикции от 13 мая 2020 г. по уголовному делу в отношении Ю.Ю. Кактана, указывает: принимая во внимание, что Ю.Ю. Кактан совершил хищение денежных средств путем оплаты покупки с чужой банковской карты, умышленно умалчивая о незаконности владения, резолюция суда кассационной инстанции о необходимости переквалификации действий лица с п. «г» ч.3 ст.158 УК РФ на ч. 3 ст. 30, ч. 1 ст. 159^3 УК РФ является сомнительной. По мнению суда, хищение денежных средств, совершенное с использованием электронного средства платежа, образует состав мошенничества (ст. 159^3 УК РФ) в случаях изъятия денег путем обмана или злоупотребления доверием либо владельца, либо иного лица. Ю.Ю. Кактан, осуществив оплату покупки бесконтактным способом, ложные сведения о владельце карты сотрудникам организаций не сообщал, в заблуждение не вводил, совершив хищение путем оплаты покупки с чужой банковской карты, умышленно умалчивая о незаконности владения картой. Верховный Суд РФ отметил: ссылка суда на разъяснения, указанные в п. 17 Постановления Пленума Верховного Суда РФ № 48 должна быть признана необоснованной, поскольку они приняты Верховным Судом РФ в 2017 г., т. е. до включения в Уголовный кодекс РФ п. «г» ч. 3 ст. 158 УК РФ.

Верховный Суд РФ резюмирует: поскольку Ю. Ю. Кактан, обнаружив чужую банковскую карту, осуществил оплату товаров бесконтактным способом, при этом, работники торговых организаций не принимали участия в операции по списанию денежных средств с банковского счета в результате осуществления оплаты, Ю. Ю. Кактаном сотрудники не были введены в заблуждение, им не сообщены ложные сведения о принадлежности банковской карты (т. е. имеет место умолчание – прим. автора). С учетом таких обстоятельств, обоснованность переквалификации судом кассационной инстанции действий Ю. Ю. Кактана с ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ на ч. 3 ст. 30, ч. 1 ст. 159^3 УК РФ у

---

[1]Скляров С.В. К вопросу о конкуренции норм, предусматривающих уголовную ответственность за кражу, совершенную с банковского счета, и мошенничество с использованием электронных средств платежа // Вестник Университета Генеральной прокуратуры Российской Федерации. 2019. № 4 (42). С. 20.

[2] Евстратенко Е. В. Хищение с банковского счета, а равно в отношении электронных денежных средств // Вестник Южно-Уральского государственного университета. Серия: Право. 2020. Т. 20, № 2.С. 20.

Верховного Суда РФ вызывает сомнение, в связи с чем, кассационное определение Шестого кассационного суда от 13 мая 2020 г. подлежит отмене с передачей уголовного дела на новое рассмотрение[1].

Принимая во внимание особенности объективной стороны кражи чужого имущества с банковского счета, а равно в отношении электронных денежных средств, направленность российской уголовной политики на гуманизацию уголовного законодательства, учитывая мнение Верховного Суда РФ, выраженное в Определении от 29 сентября 2020 г. № 12-удп20-5-к6 (в порядке главы 47.1 УПК РФ, а также сформировавшуюся судебную практику, свидетельствующую о проблемах в квалификации, необходимо:

- включение в Уголовный кодекс РФ (раздел VIII. Преступления в сфере экономики, глава 21. Преступления против собственности) новой статьи 158^2 УК РФ «Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств», дифференцировав уголовную ответственность, т. е. признавая дополнительно категорию преступления, как небольшой, так и средней тяжести.

Предлагается следующая редакция ст. 158^2 УК РФ «Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств» (путем исключения из Уголовного кодекса РФ п. «г» ч. 3 ст. 158 УК РФ):

«1. Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств, с использованием электронных средств платежа, путем несообщения сведений о незаконном владении платежной картой -

наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.

2. Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств, совершенная:

а) группой лиц по предварительному сговору;

б) с причинением значительного ущерба гражданину, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы, или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до одного года или без такового, либо лишением свободы на срок до пяти лет с ограничением свободы на срок до одного года или без такового.

---

[1] Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. n 12-удп20-5-к6 (в порядке главы 47.1 УПК РФ) [Электронный ресурс] URL: https://base.garant.ru/10108000/ (дата обращения 01.12.2020).

3. Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств, совершенная:

а) лицом, с использованием своего служебного положения;

б) в крупном размере,-

наказывается штрафом в размере от ста тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до полутора лет или без такового, либо лишением свободы на срок до шести лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.

4. Кража чужого имущества с банковского счета, а равно в отношении электронных денежных средств, совершенная:

а) организованной группой;

б) в особо крупном размере, -

наказывается лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до пяти лет, либо без такового и с ограничением свободы на срок до двух лет либо без такового».

Полагаем, что на современном этапе включение в Уголовный кодекс РФ ст.158^2 в изложенной редакции, с акцентом на умолчание, как обязательного условия для правильной квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, с исключением из Уголовного кодекса РФ действующей в настоящее время нормы п. «г» ч.3 ст.158 УК РФ, - единственно правильный путь в разрешении многолетних и многочисленных споров о соотношении п. «г» ч.3 ст. 158 УК РФ и специальных видов мошенничества..

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 07.11.2020) // СЗ РФ. 1996. № 25. Ст. 2954.
2. Федеральный закон от 23 апреля 2018 года № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СЗ РФ. 2018. № 18. Ст. 2581.
3. Указ Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс] URL: http://www.pravo.gov.ru. (дата обращения 01.12.2020).
4. Распоряжение Правительства Российской Федерации от 17 ноября 2008 года № 1662-р (ред. от 28.08.2019) «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // СЗ РФ. 2008. № 4. Ст. 5489.

5. Дмитренко А.П., Русскевич Е.А. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 5 (61). С. 18-22.
6. Евстратенко Е. В. Хищение с банковского счета, а равно в отношении электронных денежных средств // Вестник Южно-Уральского государственного университета. Серия: Право. 2020. Т. 20, № 2. С.19–23.
7. Занишевская А.А. Влияние сети интернет на формирование преступного и виктимного поведения личности // Развитие общественных наук российскими студентами. 2017. №3. С.93-96.
8. Зенин И. А. Гражданское право. Особенная часть: учебник. 18-е изд., пер. и доп. М.: Издательство Юрайт. 2018. 295 с.
9. Игнатьев, В.И., Степанова, А.Н. Виртуализация социального пространства и сетевое основание локализации мироцелостности // Вестник Московского Университета. Сер. 18. Социология и политология. 2008. № 2. С.63-70.
10. Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. №1. С. 104-106.
11. Скляров С.В. К вопросу о конкуренции норм, предусматривающих уголовную ответственность за кражу, совершенную с банковского счета, и мошенничество с использованием электронных средств платежа // Вестник Университета Генеральной прокуратуры Российской Федерации. 2019. № 4 (42). С. 17-22.
12. Слукина Е. В. Проблемы квалификации кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ) // Молодой ученый. 2019. № 52 (290). С. 179-181.
13. Определение Верховного Суда Российской Федерации от 29 сентября 2020 г. n 12-удп20-5-к6 (в порядке главы 47.1 УПК РФ) [Электронный ресурс] URL: https://base.garant.ru/10108000/ (дата обращения 01.12.2020).
14. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации». 2018. № 2.
15. Апелляционное определение Судебной коллегии по уголовным делам Верховного Суда Удмуртской Республики 26 марта 2019 года по делу № 22-52 (г. Ижевск) [Электронный ресурс] URL: https://vs--udm.sudrf.ru/modules.php?name. (дата обращения 01.12.2020).
16. Апелляционное Постановление Калининградского областного суда от 10 декабря 2018 года по делу № 22-1703/2018 (г. Калининград) [Электронный ресурс] URL: https://oblsud--kln.sudrf.ru/modules.php?name(дата обращения 01.12.2020).

17. Генеральная прокуратура. Состояние преступности в России. январь-июнь 2020 г. [Электронный ресурс] URL: https://genproc.gov.ru/smi/news/regionalnews/news-1774076/ (дата обращения 01.12.2020).

Е.Е. Михайлова

К вопросу о необходимости контроля и записи переговоров как следственного действия

Аннотация. В статье рассматривается вопрос о необходимости существования следственного действия «Контроль и запись переговоров». Приводится сравнительная характеристика указанного следственного действия и оперативно-розыскного мероприятия «Прослушивание телефонных переговоров». Высказываются предложения по совершенствованию нормативного регулирования механизма получения информации о содержании переговоров участников уголовного судопроизводства.

Ключевые слова: контроль и запись переговоров, прослушивание телефонных переговоров, следственные действия, оперативно-розыскные мероприятия, предварительное расследование.

Негласная фиксация переговоров лиц, располагающих информацией, представляющей интерес для следствия, бесспорно, является одним из эффективных способов получения доказательств по уголовному делу. Однако, отнесение данного мероприятия к числу предусмотренных уголовно-процессуальным законодательством следственных действий, повлекло не прекращающиеся до настоящего времени дискуссии. Кроме того, анализ судебной статистики за 2018, 2019 и 1 полугодие 2020 г. показывает, что количество рассмотренных и удовлетворенных судами ходатайств о производстве данного следственного действия на порядок меньше, чем о проведении аналогичного по содержанию оперативно-розыскного мероприятия (в 9, в 10 и в 15 раз соответственно)[1]. В связи с чем представляется актуальным проанализировать процедуру и необходимость проведения контроля и записи переговоров, высказать предложения по ее совершенствованию.

Все совершаемые преступления, с точки зрения их выявления и организации расследования, можно условно разделить на два типа:

- имеющие очевидные последствия и оставляющие явные следы преступления, выявляемые в короткие сроки уполномоченными органами в ходе первоначальных следственных действий и иных мероприятий, производство которых допустимо до возбуждения уголовного дела, на стадии его возбуждения (рассмотрения сообщения о преступлении);

[1] Отчеты о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции (Форма №1) за 12 месяцев 2018 г., за 12 месяцев 2019 г., за 6 месяцев 2020 г. [Электронный ресурс] // Официальный портал Судебного департамента при Верховном Суде Российской Федерации. Данные судебной статистики. URL: http://www.cdep.ru/index.php?id=79

- выявляемые в ходе тщательного анализа и сопоставления данных о действиях и решениях лиц, исследования документов, иной информации (в том числе компьютерной), главным образом осуществляемых в ходе проведения оперативно-розыскных мероприятий, с использованием информационных систем, технических и иных средств связи и фиксации полученных данных.

Ко второму типу, преимущественно, относятся и киберпреступления, и преступления в сфере высоких технологий.

Следы преступления, орудия и средства их совершения, иные вещественные доказательства, равно как и материальные носители информации, безусловно, имеют важнейшее доказательственное значение при расследовании любого преступления, в том числе и рассматриваемой категории. Однако во многих случаях этих объективных данных оказывается не достаточно для установления истинных обстоятельств произошедшего. Так как одни и те же последствия могут быть результатом как умышленных, так и неосторожных деяний лиц, достигших или не достигших установленного законом возраста уголовной ответственности, совершенных с различными мотивами, целями, в различных условиях, что в своей совокупности влияет на оценку и квалификацию произошедшего.

В арсенале лиц, осуществляющих расследование по уголовным делам, существует ряд следственных действий, позволяющих посредством составления протокола фиксировать показания – то есть сведения (информацию), официально сообщенные участниками уголовного судопроизводства в установленном уголовно-процессуальным законом порядке, в устной форме следователю (дознавателю, иному уполномоченному лицу, осуществляющему расследование) или суду. К таким следственным действиям относятся допрос, очная ставка, проверка показаний на месте.

В то же время, неоспоримым является и факт того, что не все показания, данные в ходе перечисленных следственных действий, отражают объективную картину произошедшего, являются полными, достоверными и достаточными. Право на отказ отдельных лиц от дачи показаний (в силу, например, родственных связей, занимаемого должностного положения или процессуального статуса) закреплен и в Конституции Российской Федерации (ст.51)[1], и в Уголовно-процессуальном кодексе Российской Федерации (далее – УПК РФ) (п.3 ч.2 ст.42, п.7 ч.4 ст.44, п.2 ч.4 ст.46, п.3 ч.4 ст.47, п.4 ч.2 ст.54, ч.3 и п.1 ч.4 ст.56)[2]. Кроме того, отдельные участники уголовного судопроизводства (подозреваемый, обвиняемый) не подлежат ответственности за дачу ложных показаний.

В связи с этим, важное значение в раскрытии и расследовании преступлений приобретает мероприятие, позволяющее уполномоченным органам и их должностным лицам, с использованием оперативно-технических сил и средств, с подключением к стационарной аппаратуре, посредством которой предоставляются услуги и средства связи, осуществить негласную фиксацию переговоров лиц,

---

[1] Конституция Российской Федерации: принята всенародным голосованием 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // Официальный интернет-портал правовой информации URL: www.pravo.gov.ru, 04.07.2020.

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) // СЗ РФ. 2001. №52 (ч.1). Ст.4921.

располагающих интересующей следствие информацией, вне их официального общения с представителями правоохранительных и иных органов, задействованных в расследовании преступлений, то есть в их бытовой, повседневной жизни или профессиональной сфере, и впоследствии использовать их в процессе доказывания.

Согласно действующему российскому законодательству, названное мероприятие может быть осуществлено в порядке, установленном УПК РФ (ст.186), в котором оно называется «Контроль и запись переговоров»[1], а также в порядке, предусмотренном Федеральным законом «Об оперативно-розыскной деятельности» (далее – ФЗ «Об ОРД») (п.10 ч.1 ст.6), где оно называется «Прослушивание телефонных переговоров»[2].

Казалось бы, два разных мероприятия (первое – следственное действие, второе – оперативно-розыскное мероприятие) должны преследовать разные цели и осуществляться в разном порядке. Однако между ними наблюдается больше сходства, чем различий.

Поскольку данные мероприятия ограничивают конституционные права граждан (на неприкосновенность частной жизни, тайну телефонных переговоров), их проведение допускается только на основании судебного решения.

После же получения такового, следственное действие «Контроль и запись переговоров» фактически выполняется негласно, с использованием оперативно-технических сил и средств теми же подразделениями специальных технических мероприятий (функционирующих в составе органов, осуществляющих оперативно-розыскную деятельность), при участии операторов связи, что и при проведении оперативно-розыскного мероприятия «Прослушивание телефонных переговоров».

Как подчеркнул Шаров В.И., именно гласность выступает гарантией достоверности всех процессуальных действий, предусмотренных уголовно-процессуальным законодательством[3]. Кроме того, по мнению Шейфер С. А., отсутствует такой определяющий признак следственного действия, как непосредственное извлечение информации лично следователем, путем непосредственного контакта со следами; следователь не может тайно прослушивать переговоры, ибо следственное действие – это всегда правоотношение между его участниками[4].

В то же время, как справедливо отмечено Калиновским К.Б., вплотную приближено к оперативно-розыскному мероприятию техническое осуществление контроля и записи переговоров, не урегулированное нормами уголовно-процессуального законодательства, в то время как процессуальные отношения имеют

---

[1] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) // СЗ РФ. 2001. №52 (ч.1). Ст.4921.

[2] Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 02.08.2019) «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. №33. Ст. 3349.

[3] Шаров В. И. Контроль и запись переговоров как следственное действие и как оперативно-разыскное мероприятие // Вестник Нижегородской академии МВД России. 2019. №3 (47). С.177-182.

[4] Шейфер С.А. Следственные действия – правомерны ли новые трактовки? // Lex Russia (Русский закон). 2015. №10. С. 115-127.

место при даче поручения на их проведение, а также при истребовании и оформлении их результатов[1].

Расследование преступления - в подавляющем большинстве случаев - деятельность, осуществляемая в целях установления уже прошедших (а не совершаемых в настоящее время) событий, разнесенная во времени с самим преступлением, т.е. осуществляемая по его следам. Соответственно, контроль и запись переговоров как следственное действие, осуществляемое в режиме «реального времени», может применяться, преимущественно, в целях установления соучастников преступления (членов организованных преступных групп), мест сбыта похищенного, места нахождения пропавшего без вести или похищенного лица, а также в целях фиксации переговоров, в которых может быть проявлена преступная или иная осведомленность определенных лиц об обстоятельствах расследуемого преступления.

То есть фактически обозначенные цели, которые преследуются в ходе выполнения следственного действия «Контроль и запись переговоров» полностью укладываются в задачи оперативно-розыскной деятельности, определенные ст.2 ФЗ «Об ОРД». А соответственно, могут быть реализованы в ходе выполнения оперативно-розыскного мероприятия «Прослушивание телефонных переговоров», производство которого, в отличие от мероприятия, регламентированного ст.186 УПК РФ, возможно как на стадии предварительного следствия, так и до возбуждения уголовного дела или после его передачи в суд, при наличии информации, установленной статьей 8 ФЗ «Об ОРД».

А поэтому возникает вопрос: Необходимо ли мероприятие «Контроль и запись переговоров» в арсенале следователя, в числе следственных действий, предусмотренных Уголовно-процессуальным кодексом Российской Федерации?

В качестве основного аргумента «за» можно выделить право следователя принять решение о его проведении. Ведь если исключить такое мероприятие из перечня следственных действий, для организации проведения соответствующего оперативно-розыскного мероприятия следователю необходимо будет составить и направить в орган, осуществляющий оперативно-розыскную деятельность, поручение о производстве оперативно-розыскных мероприятий. При этом, в соответствии с действующим законодательством, следователь будет лишен возможности указания конкретных оперативно-розыскных мероприятий, проведение которых, по его мнению, является необходимым для достижения обозначенной им в поручении задачи (например, установления круга общения подозреваемого /обвиняемого, или установления соучастников преступления, мест сокрытия похищенного имущества и т.д.). Решение данного вопроса будет полностью зависеть от начальника органа, осуществляющего оперативно-розыскную деятельность.

Второй аргумент «за»: «Контроль и запись переговоров» может проводиться по преступлениям, расследование по которым осуществляется в форме дозна-

[1] Уголовный процесс: учебник / А. В. Смирнов, К. Б. Калиновский; под общ. ред. А. В. Смирнова. – 7 изд., перераб. – М.: Норма: ИНФРА-М, 2018. С. 456-457.

ния, в то время как оперативно-розыскное мероприятие «Прослушивание телефонных переговоров», возможно лишь при наличии информации о признаках подготавливаемого, совершаемого или совершенного противоправного деяния (и лицах, его подготавливающих, совершающих или совершивших), по которому производство предварительного следствия обязательно (ст.8 ФЗ «Об ОРД» и ч.1 ст.186 УПК РФ).

Аргумент «против»: полученные по результатам следственного действия «Контроль и запись переговоров» материальные носители с фонограммой всех произведенных переговоров представляются следователю в полном объеме, и их осмотр и прослушивание производятся следователем, причем с участием лица, переговоры которого записывались (ч.7 ст.186 УПК РФ) – т.е. имеем место сразу же или вынужденное разглашение данных предварительного расследования до его завершения, что представляется тактически не обоснованным и в большинстве случаев повлечет за собой нецелесообразность его дальнейшего проведения; или отложение осмотра и прослушивания фонограммы до завершения производства «Контроля и записи переговоров», что повлечет за собой значительные объемы информации, на осмотр и прослушивание которых необходимо будет выделить большое количество времени.

По результатам же оперативно-розыскного мероприятия «Прослушивание телефонных переговоров» его результаты (записи) изначально принадлежат оперативным службам, прослушиваются сотрудниками органа, осуществляющего ОРД (в том числе и в целях планирования и организации проведения иных оперативно-розыскных мероприятий), и передаются следователю (фонограмма и бумажный носитель записи) в случае возбуждения уголовного дела в отношении лица, телефонные и иные переговоры которого прослушиваются, для приобщения к таковому в качестве вещественных доказательств.

В то же время, Инструкция о порядке предоставления результатов ОРД органу дознания, следователю или в суд, утвержденная совместным ведомственным приказом от 27.09.2013 №776/703/509/507/1820/42/535/398/68 (далее – Инструкция о порядке предоставления результатов ОРД) допускает (п.17) представление материалов, документов и иных объектов, полученных при проведении ОРМ, в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно указывается в сообщении (рапорте), и на бумажном носителе записи переговоров[1]. То есть по результатам осуществления «Прослушивания телефонных переговоров» (например, свидетелей, которые могут располагать сведениями о расследуемом преступлении) следователю могут быть предоставлены только те результаты, которые имеют значение для расследования уголовного дела. Необходимости незамедлительного осмотра представленных материалов, тем более с участием лиц, переговоры которых прослушивались, у следствия в данном случае нет.

[1] Приказ МВД России № 776, Минобороны России № 703, ФСБ России №509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (Зарегистрировано в Минюсте России 05.12.2013 № 30544) // Российская газета. 2013. № 282.

Проведение оперативно-розыскных мероприятий (в том числе «Прослушивания телефонных переговоров») – это всегда деятельность, осуществляемая и документируемая с соблюдением режима секретности.

Осуществление аналогичного по содержанию следственного действия «Контроль и запись переговоров» – производится в общем порядке, установленном УПК РФ, при этом практическая составляющая понятия «следственная тайна» не может обеспечить сохранение в тайне решения о его проведении и исключить распространение данной информации третьим лицам.

Так копии всех ходатайств перед судом о проведении следственных действий, в соответствии со ст.165 УПК РФ и ведомственными нормативными актами, направляются прокурору (принимающему участие в их рассмотрении в суде), а также руководителю следственного органа, согласовывающему данное постановление. Копии соответствующего ходатайства приобщаются в контрольное производство (в СК России) или в надзорное производство (в прокуратуре), формируемое, как правило, помощником руководителя (помощником прокурора, помощником следователя или инспектором), осуществляющим документационное обеспечение деятельности соответствующего органа. Материалы ходатайства в общем порядке направляются в суд и поступают на регистрацию в судебную канцелярию, лишь потом передаются для рассмотрения и назначения судебного заседания конкретному судье, и после вынесения судебного решения хранятся в архиве суда. В то время, как материалы, представленные с постановлением руководителя органа, осуществляющего оперативно-розыскную деятельность, о возбуждении ходатайства о разрешении проведения оперативно-розыскного мероприятия «прослушивание телефонных переговоров», возвращаются инициатору его проведения одновременно с выдачей вынесенного по результатам его рассмотрения судебного решения (ст.9 ФЗ «Об ОРД»).

Наконец, нельзя исключить и факта ошибки со стороны судебных и следственных работников.

Так, приведу пример из собственной практики: в один из районных судов г.Санкт-Петербурга поступили для рассмотрения три ходатайства (по одному уголовному делу) следователя следственной службы Управления ФСБ России по Санкт-Петербургу и Ленинградской области, о разрешении производства контроля и записи переговоров. Ходатайства были удовлетворены, копии вынесенных постановлений в день провозглашения были вручены участвующим в судебном заседании следователю и прокурору. Спустя 5 рабочих дней секретарь канцелярии суда, в обязанности которой входило оформление завершенных в производстве дел и исполнение постановлений суда, в том числе подготовка сопроводительных документов, изготовила сопроводительные письма не только в адреса следователя и прокурора (ранее уже фактически получивших под расписку постановления), но и в адреса лиц, в отношении которых данные постановления были вынесены (то есть чьи переговоры подлежали контролю и записи). Подготовленные сопроводительные письма вместе с иными документами по другим делам были представлены на подпись судье, который, полагаясь на длительный стаж работы секретаря суда, не изучив внимательно содержания каждого сопроводительного письма, подписал их (впрочем, при внимательном

прочтении тоже навряд ли смог выявить ошибку, т.к. в тексте унифицированного сопроводительного письма не приводилось содержание направляемого постановления, а указывались лишь дата его вынесения, адресат и разъяснение порядка обжалования), после чего секретарем были изготовлены копии постановлений суда, которые с сопроводительными письмами были направлены почтой России в адреса лиц, в отношении которых к тому времени было начато исполнение данных мероприятий. Известно о данном факте стало как раз из содержания прослушиваемых переговоров лиц, обсуждавших гуманность российского суда, а также необходимость обсуждения вопросов, интересующих следствие, «не по телефону», а при личной встрече, так как «их прослушивают»[1].

Таким образом, в результате допущенной работником суда ошибки вся негласность разрешенного судом следственного действия, да и дальнейшая целесообразность его проведения были утрачены.

Подводя итог изложенному, нам представляется, что необходимость существования следственного действия «Контроль и запись переговоров» отсутствует, и соответствующая норма может быть исключена из Уголовно-процессуального кодекса Российской Федерации. Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст.186.1 УПК РФ) – достаточное в арсенале следователя следственное действие, выполняемое следователем без привлечения органов, осуществляющих оперативно-розыскную деятельность, посредством которого возможно получение информации о произведенных контактах, их продолжительности, принадлежности абонентских номеров, местонахождении во время звонка (в зоне действия базовых станций). Получение такой информации целесообразно, когда необходимо получить соответствующие сведения за период времени, предшествующий возбуждению соответствующего ходатайства. Когда же речь идет о необходимости истребования сведений о соединениях абонентов (их переговоров) в реальном времени (т.е. в период, следующий после возбуждения соответствующего ходатайства), целесообразно инициировать прослушивание телефонных переговоров как вид оперативно-розыскного мероприятия, проведение которого будет организовываться и осуществляться с соблюдением режима секретности соответствующими оперативными подразделениями, а результаты предоставляться в строгом соответствии с Инструкцией о порядке предоставления результатов ОРД.

Решение же проблемы с нежеланием начальника органа, осуществляющего оперативно-розыскную деятельность, проводить данный вид оперативно-розыскных мероприятий по конкретному делу или в интересующее следствие время, можно решить или согласовывая данный вопрос в плане совместных оперативно-следственных мероприятий по нераскрытым делам, или посредством обращения к надзирающему прокурору в целях реализации им мер прокурорского надзора за оперативно-розыскной деятельностью.

Возможно также предложить проработку вопроса о внесении изменений в ФЗ «Об ОРД» и УПК РФ, разрешающие следователю в отдельных исключительных

---

[1] Материал проверки по сообщению о преступлении №3/3162 от 26.11.2002 // Архив прокуратуры Санкт-Петербурга

случаях (по отдельной категории дел или в определенных ситуациях – например, в случаях расследования дел в отношении организованных преступных групп, об экстремистской или террористической направленности, или расследования, например, дел о похищении человека, когда место нахождения потерпевшего не установлено) давать поручения о проведении конкретного вида оперативно-розыскных мероприятий.

Список использованных источников

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // Официальный интернет-портал правовой информации URL: www.pravo.gov.ru, 04.07.2020.
2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) // СЗ РФ. 2001. №52 (ч.1). Ст.4921.
3. Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 02.08.2019) «Об оперативно-розыскной деятельности» // СЗ РФ. 1995. №33. Ст.3349.
4. Приказ МВД России № 776, Минобороны России № 703, ФСБ России №509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» (Зарегистрировано в Минюсте России 05.12.2013 № 30544) // Российская газета. 2013. №282.
5. Уголовный процесс: учебник / А. В. Смирнов, К. Б. Калиновский; под общ.ред. А. В. Смирнова. – 7 изд., перераб. – М.: Норма: ИНФРА-М, 2018. – 752 с.
6. Шаров В. И. Контроль и запись переговоров как следственное действие и как оперативно-разыскное мероприятие // Вестник Нижегородской академии МВД России. 2019. №3 (47). С.177-182
7. Шейфер С.А. Следственные действия – правомерны ли новые трактовки? // Lex Russia (Русский закон). 2015. №10. С. 115-127
8. Отчеты о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции (Форма №1) за 12 месяцев 2018 г., за 12 месяцев 2019 г., за 6 месяцев 2020 г. [Электронный ресурс] // Официальный портал Судебного департамента при Верховном Суде Российской Федерации. Данные судебной статистики. URL: http://www.cdep.ru/index.php?id=79
9. Материал проверки по сообщению о преступлении №3/3162 от 26.11.2002 // Архив прокуратуры Санкт-Петербурга.

И.С. Мочалкина

К вопросу об особенностях правовой природы цифровых прав как предмета преступления

Аннотация. С учетом последних законодательных изменений в статье проанализирована имеющаяся правовая база новых объектов экономических отношений. Рассматривается правовая природа цифровых прав, их соотношение с цифровыми финансовыми активами и цифровой валютой. Акцентируется внимание на возможности признания цифровых прав предметом преступления, в частности хищения.

Ключевые слова. Цифровые права, предмет хищения, хищение, цифровые финансовые активы, предмет преступления, криптовалюта, цифровая валюта.

Согласно прим. 1 к ст. 158 Уголовного кодекса РФ (*далее УК РФ*), предметом хищения может выступать только чужое имущество[1]. Более того, предмет хищения должен характеризоваться набором определенных признаков. Поэтому для того, чтобы ответить на вопрос о возможности признания цифровых прав в качестве предмета хищения, необходимо доказать отнесение таковых к имуществу и наличествование вещного, экономического и юридического признаков.

УК РФ не содержит понятия имущества, в связи с чем, по сложившейся практике, правоприменители вынуждены обращаться к ст. 128 Гражданского кодекса РФ (*далее ГК РФ*)[2]. Так, среди объектов гражданских прав можно выделить вещи и иное имущество, а также некоторые примеры того, что же к ним относится. В целях осуществления регулирования рынка новых объектов экономических отношений, в ГК РФ в 2019 году был внесен ряд поправок, в частности появилась ст. 141.1 ГК РФ, которая закрепила правовой статус цифровых прав. Изменения коснулись и ст. 128 ГК РФ, в соответствии с которой цифровые права были отнесены к объектам гражданских прав. Исходя из законодательного определения, содержание цифровых прав определяется через категорию обязательственных или иных прав. Таким образом, **цифровые права**, будучи разновидностью имущественных прав, попадают в категорию **иное имущество**.

Дальнейшая тенденция нормативного регулирования объектов цифровой экономики находит свое отражение в Федеральном законе от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (*далее Федеральный закон «О цифровых активах»*), где раскрываются понятия цифровых финансовых активов и цифровой валюты[3].

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[2] Гражданский кодекс Российской Федерации от 30.11.1994 г. № 51-ФЗ // СЗ РФ. 1994 г. № 32. Ст. 3301.

[3] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2020. № 31 (часть I). Ст. 5018.

При анализе ч. 2 ст. 1 вышеуказанного закона, цифровые финансовые активы представляют собой одну из разновидностей цифровых прав. Так, при соотношении общего и частного, цифровые финансовые активы, являясь цифровыми правами, согласно гражданскому законодательству также относятся к иному имуществу.

Гораздо сложнее дело обстоит с цифровой валютой, правовой статус которой закреплен в ч. 3 ст. 1 Федерального закона «О цифровых активах». Законодатель отказался от закрепления понятия криптовлюты, подменяя ее весьма широким по своему значению термином – цифровой валютой. И если ранее выявлялись и расследовались преступления, в которых криптовалюта выступала в качестве средства платежа, а не предмета преступления[1], то сегодня, не смотря на все ожидания, эта проблема так и не была окончательно урегулирована.

Закон не относит цифровую валюту к такому объекту гражданских прав, как цифровые права, следовательно, и ее отнесение к имуществу ставится в зависимость от внутреннего убеждения правоприменителя. Однако интерес представляет тот факт, что в рамках, например, антикоррупционного, антиотмывочного законодательства, исполнительного производства, цифровая валюта признана имуществом[2]. Таким образом, весь парадокс заключается в том, что для определенных целей законодателя цифровая валюта определяется как имущество, а глобально, на уровне специально принятого закона «О цифровых активах» и ГК РФ – прямого указания на это нет. Представляется, что для разрешения такой юридической коллизии необходимо привести к единообразному пониманию сущность цифровой валюты. Как справедливо отметил Председатель Следственного комитета РФ А.И. Бастрыкин, для расследования уголовных дел, в которых цифровая валюта выступает предметом преступления, в частности хищения, ее необходимо признать имуществом[3].

Проанализировав правовую природу цифровых прав и некоторых новых объектов цифровой экономики, можно сделать вывод, что только цифровые финансовые активы определяются как цифровые права. Поскольку заявленная тема статьи предусматривает рассмотрение именно цифровых прав в качестве предмета хищения, далее представляется возможным рассмотреть на примере цифровых финансовых активов наличие вещного, экономического и юридического признаков.

Вещный признак – предметом хищения может быть только физически осязаемая вещь, очерченная в пространстве. Однако п. «г» ч. 3 ст. 158 УК РФ предусматривает исключение из этого общего правила. Так, например, электронные

---

[1] Перов В.А. Криминалистическая методика выявления лиц, совершающих преступления с использованием криптовалюты. Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 87-92.

[2] Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал Высшей школы экономики. 2020. № 4. С. 43–77.

[3] Бастрыкин А.И. призвал признать криптовалюту имуществом. URL: https://ria.ru/20201208/kriptovalyuta-1588242025.html (дата обращения: 12.12.2020).

денежные средства не являются осязаемой вещью, однако отнесены законодателем к предмету хищения. Более того, п. 5 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» указывает на возможность хищения безналичных денежных средств[1]. Таким образом, в связи со вступлением в цифровую эпоху, особой значимостью и ценностью компьютерной информации, традиционное понимание предмета хищения было скорректировано. Признание цифровых финансовых активов в качестве предмета хищения как нематериального объекта не будет являться чем-то новым, противоречащим как УК РФ, так и судебной практике.

Экономический признак – имущество должно иметь экономическую стоимость. Так, вступивший в силу 1 января 2021 года закон, регулирующий процедуру выпуска цифровых финансовых активов, в решении о выпуске последних предусматривает такое обязательное условие, как указание на цену или порядок определения этой цены. Таким образом, руководствуясь вышеизложенным законодательным требованием, цифровые финансовые активы подлежат денежной оценке.

Юридический признак – по отношению к виновному лицу, имущество должно являться заведомо чужим; оно не должно быть изъято из гражданского оборота. Действительно, цифровые финансовые активы являются чужим имуществом по отношению к виновному лицу, поскольку ч. 7 ст. 4 Федерального закона «О цифровых активах» устанавливает критерии для обладателя этих новых объектов цифровой экономики. Обладатель цифровых финансовых активов не просто имеет доступ к той информационной системе, где ведется учет этого его имущества, не просто владеет и пользуется принадлежащими ему цифровыми правами, а также может распоряжаться цифровыми финансовыми активами. Более того, цифровые финансовые активы не изъяты из гражданского оборота, подлежат свободному выпуску и обращению при соблюдении всех законодательных требований.

Таким образом, на законодательном уровне цифровые права отнесены к категории иного имущества; правовой статус цифровой валюты нуждается в корректировке – необходимо недвусмысленно отнести ее к имуществу; цифровые финансовые активы, как разновидность цифровых прав, могут выступать в качестве предмета хищения.

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.
2. Гражданский кодекс Российской Федерации от 30.11.1994 г. № 51-ФЗ // СЗ РФ. 1994 г. № 32. Ст. 3301.

[1] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2.

3. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СЗ РФ. 2020. № 31 (часть I). Ст. 5018.
4. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2.
5. Перов В.А. Криминалистическая методика выявления лиц, совершающих преступления с использованием криптовалюты. Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 87-92.
6. Янковский Р.М. Криптовалюты в российском праве: суррогаты, «иное имущество» и цифровые деньги // Право. Журнал Высшей школы экономики. 2020. № 4. С. 43–77.
7. Бастрыкин А.И. призвал признать криптовалюту имуществом. URL: https://ria.ru/20201208/kriptovalyuta-1588242025.html (дата обращения: 12.12.2020).

С.А. Нестерович
С.Б. Вепрев

Мошенничество в интернет

Аннотация. Авторы говорят о необходимости создания специальной программы, с помощью которой провайдер, в автоматическом режиме мог бы осуществлять мониторинг сайтов на фишинг и проверять подлинность оригинальных логотипов, товарных знаков и других специальных атрибутов проверяемых сайтов, которые используются официальными – законными правообладателями этих логотипов и знаков.

Ключевые слова: фишинг; Роскомнадзор; провайдер; ответственность; киберпреступность; мошенничество.

В 2013 году в ООН, был подготовлен проект «Всестороннее исследование проблемы киберпреступности». В этом документе дано определение киберпреступности. Это определение можно считать наиболее официальным определением киберпреступности для целей разработки уголовного законодательства[1].

Киберпреступность — это совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.

[1] Всестороннее исследование проблемы киберпреступности // Управление Организации Объединенных Наций по наркотикам и преступности. / Проект, февраль 2013 года URL: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf (дата обращения: 01.12.2020).

Компьютерные преступления имеют характерные особенности:

- высокая степень незаметности, которая обеспечивается высокой распределенностью компьютерных сетей и их сложной архитектурой;
- важным аспектом компьютерных преступлений, является то, что злоумышленник и потерпевший часто находятся на очень удаленном расстоянии, а порой на территории разных стран;
- многие компьютерные злоумышленники могут иметь хорошую ИТ – подготовку;
- новое программное обеспечение, которым пользуются пользователи, зачастую до конца не отработано и имеет уязвимости;
- компьютерные преступления могут совершаться в автоматическом режиме из нескольких мест одновременно, когда в арсенале злоумышленника имеется несколько сот или тысячи зараженных компьютеров пользователей, которые и не подозревают об их заражении (так называемые ботнеты).

Согласно данным Генпрокуратуры РФ, киберпреступность является самым популярным видом преступления! Основным видом киберпреступности стало мошенничество.

Статья 159 УК РФ. Мошенничество

Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Так, за 2018 год зафиксировано 204 870 случаев нарушения статей 159 (мошенничество) и 159.6 (мошенничество в сфере компьютерной информации) УК РФ. При этом, объем мошенничества в сфере компьютерной информации превысил половину.

Следует отметить, что при общей раскрываемости в 54% раскрываемости дел о мошенничестве, раскрываемость мошенничество в сфере компьютерной информации составляет всего 25%.

В настоящее время в России количество компьютерных преступлений с использованием ИТ неуклонно растет и возрастает их удельный вес по размерам похищаемых сумм.

В настоящее время в мире насчитывается более 4 миллиардов пользователей. Наибольшее количество интернет-пользователей в Ките – около 800 млн. и США – около 300 млн. В Российской Федерации уже более – 100 млн интернет-пользователей. Лидер поисковых систем – Google. В России Google обрабатывает 49% всех запросов. На втором месте Яндекс, который 46%всех запросов.

Часто для проведения мошеннических действий используются поддельные сайты —сайты, которые внешне копируют какой-то популярный сайт. Цель таких сайтов — заставить вас ввести пароль. Чтобы распознать поддельный сайт, следует посмотрпть на его адрес в строке браузера — он будет отличаться от официального. Так, например, для сайта Бьюти Инструмент:

- https://beautyinstrument.ru -адрес официальный.
- https://beautyinstrement.ru -адрес поддельный.

Также часто для проведения мошеннических действий используются и фишинговые сайты. Фишинг – это вид мошенничества, посредством которого злоумышленники получают личную информацию пользователя (логины, пароли,

реквизиты платежных документов)[1]. Например, это письма от злоумышленников, которые представляются банками. Цель таких писем — заставить вас ввести пароль или данные карты в поддельную форму.

Фишинговые сайты очень часто используют вредоносные компьютерные программы. К вредоносным программам относят любое программное обеспечение, несанкционированно проникающее в компьютерную технику. Задача таких продуктов заключается в нарушении работы компьютера, хищении личных данных и т.д.

Вредители создаются для реализации различных целей. Самая распространенная цель, это получение выгоды от внедрения в компьютер жертвы. Например, злоумышленник добивается возможности управлять компьютером, крадет секретную информацию, осуществляет вымогательство.

Одной из мер противодействия противоправным действиямявляется блокировка сайтов - пресечение незаконной деятельности сайта.

Список уполномоченных органов, которые на основании ФЗ - № 149 имеют право блокировать сайты с запрещенным контентом.

Таблица 1.

КТО БЛОКИРУЕТ	ЗА ЧТО БЛОКИРУЕТ
Генеральная прокуратура	• призывы к массовым беспорядкам; • призывы к несогласованным митингам; • экстремистские высказывания; • распространение материалов нежелательных организаций; • распространение фейковых новостей; • неуважение к власти.
Службы и органы государственной власти: • Роспотребнадзор • ФНС • Роскомнадзор • Федеральная служба судебных приставов • Росмолодожь и др.	• детская порнография; • информация о методах самоубийства и призывы к суициду; • информация о способах изготовления нар котиков; • информация о детях-жертвах; • вовлечение несовершеннолетних в противоправную и опасную для их жизни и здоровья деятельность; • продажа алкоголя через интернет; • нарушение законодательства об азартных играх; • невыполнение судебных решений по искам о защите чести; достоинства и деловой репутации.
Суды	• информация, которая признается судебным решением запрещенной к распространению; • незаконное распространение персональных данных; • нарушения авторского права.

Однако нужно понимать, что временное пресечение в виде блокировки сайтов – это довольно неэффективная мера. Отметим, что чтобы запустить новый сайт

[1] Хачатурова С.С., Жихарева Ю.П. ОСТОРОЖНО, ФИШИНГ! // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 4-4. – С. 793-795

на новом домене и IP-адресе, программистам, которые создают сайты, потребуется всего несколько десятков минут. Поэтому мониторинг фишинг-сайтов должен осуществляться уже на уровне провайдера. Для этого требуется осуществить соответствующие действия.

Провайдер хостинга - лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети "Интернет".

Итак, главный вопрос: должен или не должен провайдер нести ответственность за все нарушения своих пользователей – тех, кто реализует через него свой интернет-ресурс. С одной стороны, именно провайдер отвечает за предоставление пользователю информационного пространства, с другой стороны, очевидно, что реальным нарушителем все-таки является именно сам пользователь сайта.

В законодательстве разных государств проблема ответственности провайдеров решается по-разному. Она колеблется от положения, когда за действия пользователей провайдер несет полную ответственность, до положения, когда за действия пользователей провайдер вообще не отвечает.

В Российской Федерации на сегодняшний день, фактически, у провайдера нет никакой ответственности. Если прочитать договор провайдера интернет-доступа, то можно увидеть, что Исполнитель не несет ответственности буквально ни за что: ни за перебои в работе, ни за упущенную выгоду Клиента, и даже не гарантирует качественной работы. В настоящее время сложилась ситуация, при которой ответственность за нарушение прав не несет ни провайдер, ни нарушитель.

Судебные органы в настоящее время, в основном, придерживаются позиции, при которой провайдер должен нести ответственность в случае, если он является **инициатором** передачи данных и **заведомо знает** о существовании на своем сервере вредоносных данных. Ответственность провайдера основывается на том, что он имеет соответствующие ресурсы, позволяющие в любой момент времени контролировать пользователя. Но если реально посмотреть на вещи, то выполнение последнего условия физически просто невозможно - для этого провайдер должен просматривать и оценивать каждый ресурс, то есть сменить свою исходную целевую задачу (между прочим – коммерческую) на другую (между прочим – не коммерческую).

Какая ответственность должна быть у провайдеров,

- Вопрос первый: а есть ли у него для проведения данных исследований достаточно компетенций, какими ресурсами он обладает для качественной реализации данной задачи?
- Вопрос второй: а не будет ли провайдер сознательно злоупотреблять своими полномочиями в том числе и в меркантильных целях?
- Вопрос третий: а обладает ли провайдер соответствующими ресурсами для проведения такой очень трудоемкой работы как предметный анализ контента?

Одним из способов борьбы с фишинговыми сайтами, может стать база данных знаков и логотипов, созданная Роскомнадзором. Специальная программа в автоматическом режиме должна осуществлять мониторинг всех сайтов на фишинг и

проверять подлинность оригинальные логотипы, товарные знаки и другие специальные атрибуты оригинальных сайтов, которые используются официальными – законными правообладателями этих логотипов и знаков.

Очевидно, что такие фильтры должны быть разработаны по техническому заданию, инициируемому Роскомнадзором. Состав перечня ограничений и порядок его использования и внедрения также должен формировать Роскомнадзор. Каждый провайдер должен быть своевременно обеспечен соответствующими материалами и программным средствами, настройку которых вообще желательно обеспечивать централизованно и дистанционно. Вот тогда, если провайдер осуществляет распространение вредоносной информации, значит он намеренно нарушает установленные ограничения.

Эта программа в обязательном порядке бесплатно должна быть предоставлена всем провайдерам интернета в России (аналогично установке системы «Ревизор»), с уведомлением о соответствующей ответственности провайдера в случае ее неустановки. В этом случае как административная, так и юридическая ответственность за функционирование фишинг-сайта будет возложена на провайдера со всеми вытекающими отсюда последствиями.

Таким образом, провайдер должен нести соответствующую ответственность в случае нарушения установленных правил распространения информации, то есть, если он не соблюдает установленных Роскомнадзором ограничений.

В связи с тем, что такие ограничения носят унифицированный характер, ответственность провайдера легко может быть определена.

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63 – ФЗ (ред. от 30.03.2016)
2. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обнспечение национальной безопасности» / [Рогозин и др.] – ЮНИТИ – ДАНА, 2016. – 287 с.

В.Н. Николаев

Использование результатов оценки РЭО при расследовании уголовных дел

Аннотация. В статье отражены вопросы осуществления оценки РЭО в районах, интересующих следствие, а также использование полученных данных при расследовании уголовных дел. Изложены предложения для повышения эффективности использования биллинговых данных, полученных с базовых станций, обслуживающих районы совершения преступлений.

Ключевые слова: цифровая криминалистика, биллинговые данные, базовые станции, компании операторов сотовой связи, оценка РЭО.

Основная задача цифровой криминалистики[1] - электронных следов и их использование в ходе расследования уголовных дел. В условиях высоких темпов информатизации общества, значимость цифровой криминалистики возрастает и уже в настоящее время позволяет получить объективные данные, недоступные при использовании традиционных криминалистических методов. Несомненно, возможности цифровой криминалистики будут постоянно возрастать.

Одним из наиболее информационно ёмких и значимых для следствия является информация, содержащаяся в телекоммуникационных сетях операторов сотовой связи. Данную информацию можно использовать по большинству расследуемых уголовных дел, прежде всего по преступлениям, совершенных в том числе в условиях неочевидности. В отдельных случаях только аналитическая обработка биллинговых данных, полученных с базовых станций, обслуживающих районы совершения преступлений, позволяет установить пользователей, причастных к совершенным преступлениям. Установление параметров базовых станций, обслуживающих интересующий следствие район, осуществляется методом оценки радиоэлектронной обстановки[2] (далее – РЭО). Оценка РЭО не предусматривает обращение к операторам в целях установления параметров базовых станций на основании частотно-территориального плана (далее – ЧТП), отображающего зоны покрытия базовых станций. Как правило, в условиях населенного пункта в одном месте присутствуют сигналы более двух десятков базовых станций по каждому оператору. При изменении местоположения (за зданиями или перед ними, на земле или на верхних этажах, в различных комнатах квартиры и т.д.) изменяются приоритетные базовые станции. Поэтому проведение измерений является обязательным требованием.

Способы оценки РЭО их особенности:

Контрольные звонки. Необходимо произвести так называемые «отзвоны» по каждому оператору в каждом стандарте связи. Позволяют установить параметры только одной базовой станции. Отсутствие данных об уровне сигнала и соотношении с уровнем сигнала соседних базовых станций. При изменении местоположения цикл измерений необходимо повторить. Это самый малоинформативный метод, который целесообразно использовать только вне населенных пунктов.

Привлечение специалистов радиочастотной службы (далее – РЧЦ). Измерения осуществляются с использованием не носимых, а мобильных технических средств, поэтому невозможно использовать в зданиях и иных труднодоступных местах. Невозможность привлечения специалистов РЧЦ на постоянной основе.

---

[1] См.: Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42 - 44.; Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26 - 28.

[2]Радиоэлектронная обстановка - совокупность радиоэлектронных средств в заданном районе пространства.

См.: Приказ Госкомсвязи РФ от 03.07.1998 № 48 "Об утверждении "Положения о порядке государственного надзора за использованием радиочастот, радиоэлектронных средств (РЭС) и высокочастотных устройств (ВЧ устройств)".

Использование инженерного меню или функции «NetMonitor» мобильного телефона. Возможность получения параметров соседних базовых станций и формирование списка по приоритету. Метод корректный, но требует множество измерений и их фиксацию на месте.

Использование мобильных приложений типа «NetMonitor», «G-NetTrack». Менее корректный, но более удобный в использовании, благодаря интерфейсу и возможности сохранения логов. Оптимален для установления приоритетных базовых станций на маршруте передвижения по длительности обслуживания мобильного телефона на базовых станциях.

Использование специализированных изделий типа «Датчик РЭО». Наиболее корректный метод, позволяющий получить параметры базовых станций по всем операторам и стандартам связи, а также экспортировать данные в формат «Excel». Целесообразно использование *«Датчика РЭО»,* основанного на использовании SIM-карт в целях формирования списка базовых станций по приоритетности. Данное требование критично для стандарта 2G, в котором приоритет зависит от параметра качества C2, а не от уровня сигнала. В противном случае из общего списка отбираются менее приоритетные базовые станции частотного диапазона 900 МГц, зона обслуживания которых многократно превышает зоны обслуживания других стандартов и частотных диапазонов. В результате аналитической обработки получаемых на основе оценки РЭО биллинговых данных, под стандартные условия отбора номеров попадает значительное количество пользователей, находившихся в интересующий период времени на значительном удалении от мест совершения преступлений.

Отбор необходимых базовых станций из общего списка должен осуществляться специалистом с учетом обстоятельств преступления и возможных моделей поведения преступника. Поэтому оценку РЭО целесообразно осуществлять специалисту, который будет впоследствии обрабатывать биллинговые данные. Причина в том, что аналитическая составляющая (модели поведения преступника и критерии отбора номеров) формируется в процессе оценки РЭО на местности. Обработка в большей мере представляет собой реализацию решений, формируемых в ходе оценки РЭО, математическим методом.

Эффективность использования биллинговых данных зависит, прежде всего, от уровня профессиональной подготовки специалиста на начальном этапе. Неквалифицированная оценка РЭО сводит к минимуму возможность получения положительного результата в ходе обработки биллинговых данных. В настоящее время в компаниях операторов запрашивается огромный объем биллинговых данных, значительная часть которых непригодна для аналитической обработки, так как не позволяет реализовать критерии отбора для установления необходимых номеров. При этом, формируется значительный объем бесполезной работы для сотрудников оперативных подразделений и следователей, связанный с проверкой пользователей абонентских номеров на причастность к совершенным преступлениям. Но самым критичным является факт, что метод считается отработанным, хотя в биллинговых центрах компаний операторов с высокой вероятностью содержатся данные, позволяющие получить положительный результат при квалифицированном подходе.

Актуальность данных, полученных в ходе оценки РЭО по преступлениям прошлых лет высокая. Азимуты антенн базовых станций практически не меняются. По базовым станциям, развернутым в период после совершения преступления, данные будут отсутствовать. Единственное требование – отбор из общего списка большего количества базовых станций, что связано с возможностью изменения их приоритетности. Наиболее оптимальным является требование о приобщении протокола оценки РЭО к протоколу осмотра мест совершения преступлений, прежде всего по тяжким и особо тяжким.

Решение вышеназванных проблем возможно только при системном подходе. Во-первых, специальная подготовка технических специалистов, обеспечивающих технико-криминалистическое сопровождение расследования уголовных дел. Во-вторых, формирование регламента взаимодействия с компаниями операторов сотовой связи с переходом на электронный документооборот. Доступ в систему электронного документооборота должен предоставляться по электронной цифровой подписи[1] (далее – ЭЦП) техническим специалистам и следователям-криминалистам, прошедшим курс обучения. Предоставление следователям возможности запрашивать биллинговые данные при отсутствии специальной подготовки и корректных результатов оценки РЭО будет способствовать увеличению объема запрашиваемых данных, что еще больше усугубит существующие проблемы.

Подводя итог вышеизложенному, следует отметить, что специфика материала, изложенного в настоящей статье может быть полезна при раскрытии и расследовании преступлений, совершенных в условиях неочевидности.

Список использованных источников

1. Приказ Госкомсвязи РФ от 03.07.1998 № 48 "Об утверждении "Положения о порядке государственного надзора за использованием радиочастот, радиоэлектронных средств (РЭС) и высокочастотных устройств (ВЧ устройств)"
2. Постановление Правления ПФ РФ от 26.01.2001 № 15 "О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи" (вместе с "Регламентом регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации").
3. Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42 - 44.;

[1] Электронная цифровая подпись (ЭЦП) - последовательность символов, полученная в результате криптографического преобразования исходной информации, которая позволяет подтверждать целостность и неизменность этой информации, а также ее авторство..." См.: Постановление Правления ПФ РФ от 26.01.2001 № 15 "О введении в системе Пенсионного фонда Российской Федерации криптографической защиты информации и электронной цифровой подписи" (вместе с "Регламентом регистрации и подключения юридических и физических лиц к системе электронного документооборота Пенсионного фонда Российской Федерации").

4. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26 - 28.

В.А. Перов

Электронный след: понятие, виды, способы обнаружения и фиксации

Аннотация. Рассматриваются различные криминалистические определения понятия «электронный след». Предлагается определенная классификация «электронных следов», способы его обнаружения и фиксации.

Ключевые слова: электронный след, цифровой след, следообразование, киберпреступность, блокчейн-технологии, кейлоггер, виртуальное пространство.

Конец XX и начало XXI столетия ознаменовали собой резкий скачок развития информационно-цифровых технологий и активное их внедрение в современную жизнь. К сожалению такое внедрение не всегда носит позитивный характер и все чаще сегодня мы сталкиваемся с фактами, когда электронные средства являются орудиями преступления, а сама информационная среда выступает в качестве обстоятельства способствующего совершению так называемых «киберпреступлений».

При всем этом единообразного понятия «киберпреступления» не существует.

Если в поисковой строке любой поисковой системы телекоммуникационной сети «Интернет» набрать термин «киберпреступления», то можно найти следующие их определения:

-преступления, которые совершаются в сфере информационных технологий, и включающие в себя создание и распространение вредоносных компьютерных программ, так называемых компьютерных вирусов, несанкционированный доступ к различным компьютерным программам, кражу безналичных денежных средств, посредством опять-таки несанкционированного доступа к банковским счета других лиц, распространение в сети противоправной информации, фишинг;

-преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства;

-преступная деятельность, в которой компьютер либо иное сетевое устройство используется в преступных целях.

Подобные определения понятия «киберпреступности» легко можно найти как в сети «Интернет», так и в научной криминалистической литературе.

Какое из них правильное каждый решает для себя сам.

Тем не менее все эти определения говорят нам о том, что такие преступления совершаются с помощью цифровой компьютерной техники. Таким образом можно говорить о том, что использование такого оборудования оставляет специфический «электронный» или как его еще называют в криминалистической литературе «цифровой» след.

Этим самым подчеркивается взаимосвязь таких сравнительно новых в криминалистике понятий как «киберпреступность» и «электронный» или «цифровой

след». Одно не может существовать без другого. Также как преступление, совершаемое в объективной реальности оставляет следы физического воздействия друг на друга предметов материального мира, также и в виртуальном пространстве остаются следы преступной деятельности.

При этом с одной стороны оставленный в виртуальном пространстве используемым цифровым устройством «электронный след» является следствием использования такого устройства, а с другой стороны, такого рода технические устройства служат средством обнаружения и документирования подобного вида следов.

Но при этом принятого все криминалистическим сообществом термина определяющего характер указанного следообразования не существует.

В научной литературе можно встретить понятия: «электронный», «цифровой», «электронно-цифровой», «виртуальный» след, а иногда и такое определение как «цифровой отпечаток» от англ. digital footprint.

Анализируя данные понятия можно прийти к выводам, что термины «электронный» и «цифровой» след все же имеют тождественные определения, под которыми понимают определенный набор действий на цифровом устройстве или в телекоммуникационной сети «Интрернет», в результате которых появляется некая если так можно выразится «остаточная» информация являющаяся результатом совершения подобный действий.

А вот такое понятие как «электронный след» по мнению автора является более широким чем понятия «цифровой» или «виртуальный» след, так как включает в себя не только цифровую, но и некую аналоговую информацию.

Видимо исходя из данного обстоятельства многие криминалисты используют такое понятие, как «электронно-цифровой след» как более конкретно и точно отражающее процесс такого следообразования в соответствии с криминалистической теорией отражения.

Данная теория предусматривает, что – следообразование является результатом взаимодействия между собой объектов физического мира. Каждый из указанных объектов отражается на физических свойствах другого в виде соответствующего следа.

Образовавшийся след имеет причинную связь с расследуемым событием преступления и возникает как уже было сказано в результате действий людей, животных, отдельных предметов либо природных воздействий.

Все вышеперечисленные обстоятельства полностью применимы к так называемому виртуальному миру. Различия будут лишь в том, что в мире виртуальном между собой взаимодействуют виртуальные объекты, а электронный след может возникать не только в результате действий людей, но и результате действий электронной системы, осуществляемой в отдельных случаях и без участия человека или с ограниченным его участием, как например это происходит в блокчейн-технологиях или так называемых смарт-контрактах.

Исходя из определения «электронного следа» как результата определенного набора действий на цифровом устройстве или в телекоммуникационной сети Интернет, по механизму следообразования «электронный след» можно условно разделить на две группы:

1. Статический «электронный след» (от греч. Στατός- неподвижный (пассивный).

2. Динамический «электронный след» (от греч. Δύναμις- сила, мощь (активный).

Такое деление полностью соответствует тем разделам механики и физики, в соответствии с которыми происходит сам процесс следообразования.

При статистическим следообразовании возникновение «электронного следа» происходит в результате функционирования электронного устройства (компьютера). К такому типу «электронного следа» могут относиться, например, сведения об IP-адресе используемого устройства и его перемещении в телекоммуникационной сети «Интернет».

Таким образом статические «электронные следы» фиксируются провайдером интернет –услуг (оператор связи), предоставляющим услуги по предоставлению каналов связи, передаче данных, голосовой информации, телематические услуги и могут им быть переданы следственному органу с соблюдение необходимых процессуальных требований.

К динамическому типу следообразования можно отнести «электронные следы» получаемые в результате определенных действий человека или определенной электронной системы в результате которых появляется виртуальный объект. В данном случае такой «электронный след» будет являться отображением подобного вида действий. В качестве примера такого «электронного следа» можно привести регистрацию пользователя телекоммуникационной сети «Интернет» на определенном сайте. При манипулировании компьютерным оборудованием (нажатие клавиш на клавиатуре, манипуляции с джойстиком) такие действия фиксируются в буфере обмена, то есть промежуточном хранилище данных, которое предоставляется программным обеспечением и имеет своей целью осуществление возможности переноса либо копирования информации между приложениями, а также одного приложения через совершение соответствующих операций.

Соответственно данная информация может быть извлечена и зафиксирована на данном электронном устройстве.

«Электронные следы» данного вида также могут сохранятся в так называемом кейлоггере (от англ. key - клавиша и logger - регистрирующее устройство), то есть определенном компоненте программного обеспечения либо являться специальным аппаратным устройством, которое запоминает и сохраняет все манипуляции (логги) пользователя с клавиатурой компьютера.

Чаще всего для этих целей применяется программный кейлоггер, который также является частью таких вредоносных программ как руткиты или трояны, вследствие чего в данном случае можно вести речь о технических средствах, предназначенных для негласного получения информации. Использование таких средств без получения соответствующего разрешения на проведение оперативно-розыскных мероприятий является незаконным.

При этом при наличии соответствующих оснований для проведения оперативно-розыскных мероприятий, предусмотренных статьей 7 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», одним

из которых является наличие в производстве следователя возбужденного уголовного дела с помощью кейлоггера может быть осуществлено оперативно-розыскное мероприятие, предусмотренное пунктом 11 статьи 6 указанного Закона-снятие информации с технических каналов связи. То есть в данном случае можно говорить о том, что с помощью контроля специальными техническими средствами, программным кейлоггером будет получена информация в виде «электронного следа» работы соответствующей интересующей следствие системы либо устройства определенного пользователя. Такой «электронный след» в дальнейшем будет иметь доказательственное значение по расследуемому уголовному делу.

Таким образом можно констатировать, что обнаружение и фиксация «электронных следов» является не только теоретической, но и практической составляющей современной криминалистики без которых невозможно эффективное расследование киберпреступлений.

Список использованных источников

1. Г.Л. Грановский. Основы трасологии. М.1965
2. Л.Я. Драпкин, В.Н. Карагодин. Криминалистика. Учебник. М. 2011
3. Р.С. Белкин. Курс криминалистики в 3-х томах. Р.С. Белкин М.; Юрист, 1997. Т. 1 Общая теория криминалистики.
4. С.М. Потапов. Введение в криминалистику. М.;1946
5. Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. Криминалистика. Учебник для вузов. Под ред. Заслуженного деятеля науки Российской Федерации, профессора Р. С. Белкина. Издательство НОРМА. М: 2000
6. А.И. Семикаленова. Цифровые следы: назначение и производство экспертиз. Вестник Университета имени О.Е. Кутафина (МГЮА) 5/2019. С. 115-120.
7. Е.Р. Россинская, И.А. Рядовский. Концепция цифровых следов в криминалистике. Аубакировские чтения: материалы Международной научно-практической конференции (19 февраля 2019 г.). — Алматы, 2019. С. 6—8.
8. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения 10.12.2020).

С.В. Петраков

Использование учетов при раскрытии и расследовании преступлений, совершаемых с использованием компьютерных и информационно-телекоммуникационных технологий

Аннотация. В статье автор рассматривает необходимость формирования новых видов учетов в связи с преступлениями, совершаемыми с использованием компьютерных и информационно-телекоммуникационных технологий. Анализируются положения приказа МВД России о вводе учета «Дистанционное мошенничество». Делается вывод, что необходимо учитывать большой массив данных

по преступлениям, совершаемым с использованием компьютерных и информационно-телекоммуникационных технологий.

Ключевые слова: компьютерные преступления, MAC-адрес, IP-адрес, IMEI, криминалистические учеты.

Статистические данные свидетельствуют о росте преступлений, совершаемых с использованием компьютерных и информационно-телекоммуникационных технологий и их низкой раскрываемости. При этом раскрываемость данных преступлений крайне низкая, что было отмечено на коллегии Генеральной прокуратуры РФ [1]. В настоящее время в статистической отчетности преступления относятся к «совершенным с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации» и кодируются соответствующим образом если:

1) деяние квалифицировано по какой-либо статье УК РФ: 138.1, 159.6, 272, 273, 274, 274.1;

2) деяние совершено одним из указанных способов: с использованием средств мобильной связи, с использованием вредоносных компьютерных программ, с использованием информационно-телекоммуникационных технологий, сети Интернет, создание вредоносных компьютерных программ либо иной компьютерной информации; распространение вредоносных компьютерных программ либо иной компьютерной информации; с использованием (применением) компьютерной техники, расчетных (пластиковых) карт, программных средств, фиктивных электронных средств;

3) преступление совершено с использованием или применением: поддельных кредитных, расчетных (пластиковых) карт; компьютерной техники, программных средств, машинных носителей; фиктивных электронных платежей, сети Интернет;

4) при совершении преступления использовались какие-либо специальные технические средства для негласного: получения и регистрации акустической информации, визуального наблюдения и документирования, прослушивания телефонных переговоров, перехвата и регистрации информации с технических каналов связи

Поскольку преступления совершаются удаленным способом, то одна из сложностей заключается в идентификации лица. Для совершения этих преступлений лица используют различные технические средства, которые характеризуются набором своих идентификационных признаков. В связи с наличием соответствующих преступлений целесообразно вводить новые виды криминалистических учетов. Поскольку субъекты соответствующих преступлений совершают не одно, а несколько различных преступных деяний, то высока вероятность того, что они будут использовать какое-либо одно техническое средство по ряду преступлений. В настоящее время часть этих преступлений раскрывается по причине ошибок, допускаемых преступниками.

---

[1] Заседание коллегии Генпрокуратуры РФ [Электронный ресурс] // URL: http://kremlin.ru/events/president/news/62998 (дата обращения 04.12.2020).

Поэтому выявив лицо по одному уголовному делу можно проверить его на причастность к другим преступлениям. Кроме того, в ряде уголовных дел по преступлениям, совершенным одним лицом могут быть какие-либо следы, анализ которых может позволить установить преступника. Именно для этого и нужны новые виды учетов по рассматриваемым видам преступлений.

Приказом МВД России от 22.04.2020 № 236 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф»»[1], с 30.04.2020 введена в эксплуатацию подсистема программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня. Несмотря на то, что в соответствии с данным приказом должны собираться, систематизироваться, обрабатываться и анализироваться сведения, собираемые в рамках расследования уголовных дел по преступлениям, совершаемым дистанционным способом с использованием информационно-телекоммуникационных технологий, в базу вносятся лишь сведения по мошенничеству на основании квалификации в правоприменительном документе. В практике это происходит исходя из названия подсистемы. Таким образом все остальные преступления, совершаемые дистанционным способом, не учитываются в данной базе. Исходя из этого данная система учета уже на начальном этапе ее функционирования малоэффективна.

В соответствии с данным приказом должен быть обеспечен доступ к данной системе подразделениям центрального аппарата МВД России, территориальным подразделениям МВД России, и иным организациям, и подразделениям, созданным для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел. Вместе с тем, соответствующие преступления могут расследоваться не только сотрудниками ОВД, но и следователями и дознавателями иных правоохранительных органов. В связи с этим, сотрудники иных органов предварительного расследования могут обращаться с соответствующими запросами в информационные центры МВД России по соответствующему субъекту России для предоставления сведений из указанного банка данных.

Исходя из того при наличии каких обстоятельств то или иное деяние может быть учтено как рассматриваемый вид преступления, в соответствующий банк данных должны вноситься следующие сведения: IP-адрес, который использовался для доступа; IMEI мобильного устройства с которого произошел доступ, MAC-адрес сетевой карты устройства, с которого произошел доступ; номер счета (карты), на который (ую) перечислены денежные средства. Помимо этого, соответствующий банк данных целесообразно систематически обновлять на предмет учитываемых сведений, которые позволят идентифицировать лицо, совершившее преступление удаленным способом. Так, можно рассмотреть вопрос о необходимости учета всех IP-адресов, IMEI и MAC-адрес, посредством

[1] Приказ МВД России от 22.04.2020 № 236 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 07.12.2020).

которых лицо подключилось к сети Tor, для последующей проверки оперативными сотрудниками этих данных по другим уголовным делам.

Еще раз необходимо отметить, что в соответствующий банк данных необходимо вносить идентификационные показатели не только по хищениям, совершаемым дистанционным способом, а в целом по всем рассматриваемым преступлениям. Конечно преступники будут менять и компьютеры, и телефоны, и счета, но не все и не по каждому новому деянию. Поэтому если использование новых видов учетов поможет раскрыть даже незначительное количество соответствующих преступлений, это в целом будет значимо, с учетом сложности раскрытия рассмотренных преступлений.

Списко использованных источников

1. Приказ МВД России от 22.04.2020 № 236 «О вводе в эксплуатацию подсистемы «Дистанционное мошенничество» ПТК «ИБД-Ф» [Электронный ресурс] // Доступ из справ.-правовой системы «КонсультантПлюс».
2. Заседание коллегии Генпрокуратуры РФ [Электронный ресурс] // URL: http://kremlin.ru/events/president/news/62998.

Е.П. Полянская

Роль социальной инженерии в преступлениях, совершаемых посредством использования информационно-телекоммуникационных устройств и методы борьбы с ней

Аннотация. В статье приведен анализ роли человеческого фактора в механизме совершения преступления дистанционным способом. Рассмотрены наиболее яркие примеры преступлений, совершенных посредством использования социальной инженерии и даны предложения по снижению уровня преступности.

Ключевые слова: мошенничество, преступления, совершенные посредством информационно-телекоммуникационных устройств, раскрытие, расследование, социальная инженерия, устройства, финансово-кредитные учреждения.

Хорошее программное обеспечение создается людьми. Так же, как и плохое.[1] Информация защищается людьми, и основные носители информации – тоже люди, со своим обычным набором комплексов, слабостей и предрассудков, на которых можно играть и на которых играют[2]. Данный инструмент мошенников имеет своё наименование -социальная инженерия, под которой понимается метод управления действиями человека без использования технических средств. Этот метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Важно данный метод рассматривать именно в

[1] Ларри Л. Константин Человеческий фактор в программировании. М., 2004. С. 1.

[2] Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры. СПб., 2007. С.2.

контексте информационной безопасности, где оно означает психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.[1]

Не секрет, что подавляющее количество мошеннических действий совершается посредством использования социальной инженерии. Даже если на минуточку представить, что доступ ко всем нашим девайсам и гаджетам защищен от атак, малвари[2] и прочего вмешательства, то с самим человеком, который будет являться жертвой социальной инженерии, мы ничего поделать не сможем. Никакие профилактические беседы, к сожалению, не помогут, поскольку всегда присутствует человеческий фактор.

Стоит ли говорить о неподготовленных гражданах, если сотрудники финансово-кредитных учреждений, обладающие информацией о видах преступлений, сопряженных с хищением денежных средств с банковских счетов, проходящие необходимые инструктажи, становятся жертвами классических схем мошенничества.

Так, в мае 2020 года, ведущий эксперт Центрального банка Российской Федерации гр. Д. перевела 250 тыс. рублей звонившему ей якобы сотруднику службы безопасности ПАО «Сбербанк России», сообщившему о подозрительной активности по счету и попросившему продиктовать данные карты для устранения проблемы.[3]

Аналогичная ситуация произошла с сотрудницей территориального управления Центрального банка Российской Федерации, лишившейся 1 млн. рублей, сообщив мошеннику данные своей банковской карты, а затем посредством банкомата дополнительно переведя на указанный им счет денежные средства.[4]

Таким же образом, в феврале 2020 года была обманута сотрудница Саратовского отделения банка, осведомленная о подобных случаях, но сообщившая мошеннику данные своей банковской карты и код, пришедший в sms-сообщении, тем самым лишившись 297 тыс. рублей.[5] Эти случае не единичны. В период самоизоляции 2020 года мошенники значительно активизировали свою деятельность. Особенно показателен пример, когда мошенник, представившись гинекологом клиники «Евромед», убедил в переписке приложения «Instagram» девушку в том, что он является высококвалифицированным специалистом и может оказать ей дистанционную помощь, а именно видеоконсультацию за 3000 руб-

---

[1] Википедия. -[Электрон. ресурс].-Режим доступа: https:// ru.wikipedia.org/wiki/ Социальная_ инженерия (дата обращения 10.12.2020).

[2] Малварь - общее название для всех видов кибер-угроз, таких как: вирусы, трояны, шпионские программы, кейлоггеры, adware и др.

[3] Новостной портал Oka.fm -[Электрон. ресурс].-Режим доступа: https://www.oka.fm/new/read/social/Vedushego-eksperta-TCentrobanka-oblaposhili-bankovskie/ (дата обращения 11.12.2020).

[4] Википедия. -[Электрон. ресурс].-Режим доступа: https:// ru.wikipedia.org/wiki/ Социальная_ инженерия (дата обращения 10.12.2020).

[5] Новостной портал Рамблер/Финансы -[Электрон. ресурс].-Режим доступа: https://finance.rambler.ru/other/43729248-sotrudnitsu-banka-obmanuli-lzhe-rabotniki-banka/?article_index=1(дата обращения 11.12.2020)

лей. Гинеколог попросил девушку продемонстрировать половые органы, записал видео и шантажируя рассылкой друзьям, потребовал перевести ему 200 тыс. рублей.[1]

От рода деятельности и должности жертвы, влияние на него социальной инженерии абсолютно не зависит, необходимо только найти его слабое место.

Так, в марте 2019 года мошенник позвонил заместителю одного из департаментов агропромышленного комплекса и представившись вице-губернатором попросил оказать материальную помощь в размере 50 тыс. рублей, необходимую на операцию больного ребенка. Поскольку, как показалось заместителю, голос звонившего был очень похож на голос реально действующего политика, денежные средства посредством мобильного банка были переведены.[2] Аналогичная по способу совершения преступления ситуация произошла в октябре 2020 г. с директором школы Ядринского района Чувашской Республики, которому позвонил мошенник, представившийся сотрудником правоохранительных органов и сообщивший о предстоящей проверке. В ходе разговора он попросил оплатить расходы на проверяющих в сумме 12 тыс. рублей, что и было сделано.[3]

Также следует обратить особое внимание на то, что подобные преступления совершаются не в 2001-2010 гг. когда только зарождалась подобная преступность, а в 2019 – 2020 гг., когда большинство граждан осведомлены из различных источников о преступных схемах, предупреждены о необходимости быть осмотрительными, перепроверять информацию, не доверять неизвестным лицам и не передавать персональную информацию, а особенно данные банковских карт. В настоящее время у нас имеется масса возможностей и ресурсов для проверки поступающей к нам информации.

С момента появления сотовых телефонов, возникли различные вариации мошеннических действий, но основным катализатором их совершения, послужили массовый переход на смартфоны с доступом в сеть Интернет и использование различных гаджетов и сервисов. Отдельную проблему представляет использование сотовой связи осужденными в пенитенциарных учреждениях.[4]

Роль социальной инженерии в совершении мошеннических действий колоссальна и примеров этому достаточно. Защититься от «социальных мошенников» можно только зная методы их работы, но следует помнить, что не зря ее называют неуловимым врагом в мире кибербезопасности.

---

[1] Новостной портал LIFE-[Электрон. ресурс].-Режим доступа: https://life.ru/p/1320124 (дата обращения 13.12.2020)

[2] Сайт информационного агентства Приморья-[Электрон. ресурс].-Режим доступа: https://primamedia.ru/news/798141/(дата обращения 13.12.2020)

[3] Сайт издания Аргументы и факты -[Электрон. ресурс].-Режим доступа: https://chv.aif.ru/incidents/details/eshche_odin_direktor_shkoly_perevela_dengi_telefonnym_moshennikam (дата обращения 13.12.2020)

[4] Полянская Е.П. О мерах борьбы с преступлениями, совершаемыми посредством информационно-телекоммуникационных устройств лицами, содержащимися в местах отбывания лишения свободы // Уголовно-исполнительная система на современном этапе и перспективы ее развития: сб. тез. выступлений и докладов участников Междунар. науч.-практ. конф. – Рязань: Академия ФСИН России. 2020. С. 119-122.

Социальной инженерии посвящено большое количество работ. В данном исследовании невозможно кратко охватить столь емкую тему, равно как и перечислить основные схемы, начиная от обмана продавца с интернет-сервиса «Avito» и заканчивая действиями преступников, связанными с подменой номеров при использовании IP-телефонии, модулятора голоса и т.д. Об этом говорится в многочисленных памятках в общественном транспорте, объявляется в метро, подробно детализируется в новостных передачах, на ведомственных сайтах и в средствах массовой информации.[1]

Почему социальная инженерия до сих пор остается эффективной? Преступники знают, что большинство граждан не осознают, что делают что-то не так; и / или не понимают ценности раскрываемой информации. Именно эта наивность создает идеальную атмосферу для совершения уголовно-наказуемого деяния. Вероятно, наиболее эффективным способом защиты от подобных атак может являться обучение граждан культуре грамотного использования информационно-телекоммуникационных устройств.

Касательно обучения, А.В. Кравченко в своем исследовании указывал, что достаточно быстрый и положительный результат может дать взаимодействие образовательных организаций с организациями, имеющими определенные достижения в области обеспечения собственной информационной безопасности (банками, лабораториями информационной безопасности). По его мнению, для совершенствования подготовки сотрудников правоохранительных органов, специализирующихся на раскрытии и расследовании преступлений в сфере информационных технологий целесообразно ввести курс по изучению социальной инженерии.[2] На наш взгляд, подобный подход, но только в виде небольшого экскурса необходим и в обучении школьников, студентов, что могло бы повысить уровень их грамотности в сфере информационной безопасности.

Не следует забывать, что наиболее уязвимой категорией населения являются люди пожилого возраста, которые не всегда могут и умеют проверить информацию. Однако, по изученным автором уголовным делам, возбужденным по рассматриваемой категории преступлений, потерпевшими являлись как правило лица 1959–1966 годов рождения. На наш взгляд, сотрудникам финансово-кредитных учреждений необходимо при выдаче пластиковых карт гражданам, информировать их о возможных мошеннических действиях со стороны иных лиц. Не лишним было бы подобное информирование и работниками социальных служб. Представляется эффективной мерой и профилактическая беседа, осуществляемая операторами банковских организаций при обзвоне клиентов, если бы помимо предлагаемого продукта или уведомления о проводимых акциях, будет напоминание о комплексе правомерных действий сотрудников банков по отношению к клиентам.

---

[1] Сайт Российской газеты -[Электрон. ресурс].-Режим доступа:https://rg.ru/2020/10/13/telefonnye-moshenniki-kogda-nado-srazu-brosat-trubku.html (дата обращения 13.12.2020)

[2] Кравченко А.В. Психологические механизмы социальной инженерии при совершении преступлений // Психология и педагогика служебной деятельности. 2019. № 1. С. 49.

Как показывает анализ уголовных дел, граждане знают только об определенных способах обмана и продолжают попадаться на уловки мошенников. Исходя из личного опыта автора, можно выделить случай, произошедший с обратившейся за консультацией гр. Л. В декабре 2020 г. ей позвонил неизвестный, сославшись на объявление из интернет-сервиса «Avito» о предоставлении услуг сиделки, перечислив задаток. Немного позже, ей на счет поступили денежные средства в сумме 930 тыс. рублей, после чего снова позвонил неизвестный и потребовал перевести указанную сумму ему на счет, ввиду ошибочно совершенного перевода. Никаких уведомлений гр. Л. при этом не поступало. Впоследствии, в банке выяснилось, что на ее имя был оформлен кредит, вследствие чего, одобренная банком сумма поступила на принадлежащий ей банковский счет. Не будь она осмотрительнее, лишилась бы денежных средств и приобрела кредитное обязательство.

Значимой мерой борьбы с дистанционным хищением денежных средств посредством использования социальной инженерии может послужить массовая цифровизация банковских карт. Сбербанк и ВТБ планируют к концу 2023 года эмитировать 40-50% выпускаемых карт исключительно в цифровом формате.[1]

Список использованных источников

1. Википедия.-[Электрон. ресурс].-Режим доступа: https://ru.wikipedia.org/wiki/ Социальная_ инженерия (дата обращения 10.12.2020).
2. Кравченко А.В. Психологические механизмы социальной инженерии при совершении преступлений // Психология и педагогика служебной деятельности. 2019. № 1. С. 49.
3. Кузнецов М.В., Симдянов И.В. Социальная инженерия и социальные хакеры. СПб., 2007. С.2.
4. Ларри Л. Константин Человеческий фактор в программировании. М., 2004. С. 1.
5. Новостной портал Oka.fm -[Электрон. ресурс].-Режим доступа: https://www.oka.fm/new/read/social/Vedushego-eksperta-TCentrobanka-oblaposhili-bankovskie/ (дата обращения 11.12.2020).
6. Новостной портал LIFE - [Электрон. ресурс]. - Режим доступа: https://life.ru/p/1320124 (дата обращения 13.12.2020).
7. Новостной портал Конкретно.ru -[Электрон. ресурс].-Режим доступа: https://konkretno.ru/kriminal/129600-sotrudnica-banka-rossii-dvazhdy-popalas-na-ulovki-moshennikov.html (дата обращения 11.12.2020)
8. Новостной портал Рамблер/Финансы -[Электрон. ресурс].-Режим доступа: https://finance.rambler.ru/other/43729248-sotrudnitsu-banka-obmanuli-lzhe-rabotniki-banka/?article_index=1(дата обращения 11.12.2020).

[1] Кравченко А.В. Психологические механизмы социальной инженерии при совершении преступлений // Психология и педагогика служебной деятельности. 2019. № 1. С. 49.

9. Полянская Е.П. О мерах борьбы с преступлениями, совершаемыми посредством информационно-телекоммуникационный устройств лицами, содержащимися в местах отбывания лишения свободы // Уголовно-исполнительная система на современном этапе и перспективы ее развития: сб. тез. выступлений и докладов участников Междунар. науч.-практ. конф. – Рязань: Академия ФСИН России. 2020. С. 119-122.
10. Сайт издания Аргументы и факты -[Электрон. ресурс].-Режим доступа: https://chv.aif.ru/incidents/details/eshche_odin_direktor_shkoly_perevela_dengi_telefonnym_moshennikam (дата обращения 13.12.2020).
11. Сайт информационного агентства Приморья-[Электрон. ресурс].-Режим доступа: https://primamedia.ru/news/798141/(дата обращения 13.12.2020).
12. Сайт издания РБК -[Электрон. ресурс].-Режим доступа: https://www.rbc.ru/finances /17/12/2020/5fda24649a79472a3b493276 (дата обращения 13.12.2020).
13. Сайт Российской газеты -[Электрон. ресурс].-Режим доступа: https://rg.ru/2020/10/13/telefonnye-moshenniki-kogda-nado-srazu-brosat-trubku.html (дата обращения 13.12.2020).

В.А. Прорвич
В.В. Бычков

Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета

Аннотация. В статье сформулирована необходимость создания алгоритмов взаимодействия следователей с искусственным интеллектом, на основе которых может быть создано информационное обеспечение раскрытия и расследования экстремистских преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

Ключевые слова: экстремизм, экстремистские преступления, расследование, следователь, алгоритм, информационное обеспечение, искусственный интеллект, интерактивные экспертные системы.

В Российской Федерации с начала 90-х годов прошлого века фиксируется рост преступлений экстремистского характера[1]. В последние годы отмечается качественное изменение характера, способов совершения и субъектов таких преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»[2]. Раскрытие и расследование которых

[1] См. подробно: Бычков В.В. Динамика российского терроризма и экстремизма в XXI веке // Расследование преступлений: проблемы и пути их решения. 2018. № 3(21). С. 60-71.
[2] Бычков В.В. Информационно-телекоммуникационные сети как средство совершения преступлений экстремистской направленности // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 3. С. 43-46.

усугубляется использованием при их совершении специфических технических средств – электронно-вычислительного оборудования и современных информационных технологий, адаптированных к Интернету. К сожалению, следует признать, что раскрытие и расследование таких преступлений вызывает определенные затруднения у следователей.

Решению данной проблемы, однозначно, будет способствовать использование следователями современных информационных технологий, включая элементы искусственного интеллекта[1]. Хотя при этом нельзя не учитывать появление новых задач. Прежде всего, необходимо акцентировать, что искусственный интеллект определяется в рамках науки информатики как сложная компьютерная программа, созданная для решения определенных задач без участия человека[2].

Но правоприменение по уголовным делам не может осуществляться в автоматизированном режиме без участия следователей. Поэтому возникает ряд принципиально новых задач организации их взаимодействия с искусственным интеллектом, а точнее такого построения алгоритмов компьютерных программ данного вида, которое полностью укладывается в рамки уголовного и уголовно-процессуального законодательства.

Анализ публикаций об особенностях применения современных информационных технологий, включая использование искусственного интеллекта правоохранительными органами, показывает, что чаще всего речь идет о применении уже готовых, «фирменных» программ, разработанных крупными компьютерными фирмами. При этом во многих случаях речь идет о целевых установках, связанных с обработкой больших данных, содержащихся в специализированных базах данных правоохранительных органов.

Вместе с тем, для раскрытия и расследования экстремистских преступлений, совершаемых с использованием Интернета, с широким применением электронных документов различного вида – графических, текстовых, причем на разных языках, табличных и иных, необходимо более широкое применение самых разнообразных информационных технологий[3].

До настоящего время следователям предлагаются компьютерные программы, созданные западными фирмами. Специалистами признается, что они не только сложны, но и пишутся программистами, то есть «технарями», а не юристами. При этом хотя они и создаются с учетом мнения юристов, но специализирующихся

---

[1] Бычков В.В. Искусственный интеллект: государственная политика и векторы применения // Расследование преступлений: проблемы и пути их решения. 2020. № 4. С. 45-50

[2] Бычков В.В., Прорвич В.А. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» // Вестник Московской академии Следственного комитета Российской Федерации. 2020. № 4. С. 47-52

[3] Волынский А.Ф., Прорвич В.А. Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: монография. М., 2020.

на англосаксонском праве[1]. А это создает высокий уровень рисков совершения юридических ошибок в отечественном уголовном судопроизводстве. Особенно опасны такие ошибки при раскрытии и расследовании экстремистских преступлений, совершаемых с использованием Интернета.

Поэтому назрела необходимость создания с участием отечественных юристов-правоприменителей алгоритмов взаимодействия следователей с искусственным интеллектом, которые могут быть положены в основу информационных технологий следственной деятельности. При этом при разработке проблемно-ориентированных алгоритмов, предназначенных для создания информационных технологий, нацеленных на повышение качества всего комплекса средств, используемых для борьбы с современными экстремистскими преступлениями, необходимо применение всего арсенала наук уголовно-правового блока.

Предлагается создание следующих групп алгоритмов:

Первая группа алгоритмов нацелена на создание научно обоснованного фундамента для всех следственных действий, нацеленных на раскрытие и расследование преступлений рассматриваемого вида, включая взаимодействие с оперативными сотрудниками, экспертами и специалистами.

С ее использованием создается возможность формирования развернутой уголовно-правовой характеристики конкретного преступления, установления и систематизации всех его обязательных и факультативных признаков. При этом приходится учитывать, что диспозиции уголовно-правовых норм о преступлениях экстремистского характера носят бланкетный характер, а при раскрытии их содержательных особенностей с применением положений гражданского и специального законодательства возникают риски выхода за рамки уголовного права. Поэтому необходимо включить в состав алгоритмов данной группы ряд процедур по контролю за данной деятельностью следователя, которые практически не отличаются от разработанных для других уголовно-правовых норм[2].

На этой основе могут быть сформированы проблемно-ориентированные базы данных, содержащие информационно полные перечни обязательных признаков «основных» и «дополнительных» составов «высокотехнологичных» преступлений экстремистского характера.

С помощью алгоритмов данной группы возможно также сформировать план соответствующих следственных действий – как на стадии проверки сообщения о преступлении, так и входе его расследования.

Одной из важнейших особенностей первой группы алгоритмов является необходимость дифференцирования признаков тех составов преступлений, которые связаны с высокотехнологичным экстремизмом. Нередко возникает ряд юридических ошибок, связанных с неверной идентификацией состава конкретного преступления рассматриваемого вида. Чаще всего это связано с тем, что совершение

---

[1] Волынский А.Ф., Прорвич В.А. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография. М., 2019

[2] Эриашвили Н.Д. Новый уровень разработки проблем электронного судопроизводства по преступлениям в сфере экономики (рецензия на монографию Волынского А.Ф., Прорвича В.А.) // Государственная служба и кадры. 2020. № 1. С. 181-184.

экстремистских преступлений с использованием сети Интернет сопряжено с незаконным проникновением в определенные информационные системы, взлому их систем защиты, в том числе с применением компьютерных вирусов и иных высокотехнологичных приемов. То есть, фактически в таких случаях речь идет о совершении определенных преступлений в сфере компьютерной информации, перечисленных в главе 26 УК РФ.

Вторая группа алгоритмов нацелена на информационную поддержку важнейшей стадии практической работы следователя по надлежащей квалификации конкретного высокотехнологичного экстремистского преступления.

Ее структура имеет ряд особенностей, обусловленных целевой функцией, связанной с установлением взаимного соответствия полученных первоначальных сведений о совершенном деянии, а затем полученных доказательств тем признакам конкретного состава преступления, которые были формализованы по его развернутой уголовно-правовой характеристике. Для этого в параллельно-последовательном режиме формируется система юридических тождеств.

Вторая группа алгоритмов тесно связана с первой группой, поскольку при формировании системы юридических тождеств необходимо использовать результаты применения алгоритмов формирования развернутой уголовно-правовой характеристики данного преступления и формализации его обязательных и факультативных признаков. При этом может быть использовано несколько вариантов тех результатов обработки информации, которые были получены с использованием алгоритмов первой группы.

Третья группа алгоритмов нацелена на информационное обеспечение для надлежащего применения важнейших положений криминалистической науки.

Четвертая группа алгоритмов – для информационного обеспечения взаимодействия с оперативными сотрудниками;

Пятая группа алгоритмов – для информационного обеспечения взаимодействия со специалистами и экспертами.

Шестая группа алгоритмов нацелена на надлежащее информационное обеспечение проверки и оценки каждого из собранных доказательств по расследуемому уголовному делу. Их содержание обусловлено необходимостью безусловного выполнения требований ст. 87 и 88 УПК РФ. При этом используется специальный инструментарий, позволяющий привести доказательства различного виде к единому информационному формату, обеспечивая при этом контроль за сохранением их правового статуса. Кроме этого, при взаимном сопоставлении доказательств при выполнении их проверки, а также при сопоставлении каждого из доказательств с критериями относимости, допустимости и достоверности, установленными ст. 88 УПК РФ для их оценки, используется интерактивный режим, позволяющий следователю принимать соответствующие решения самостоятельно.

Седьмая группа алгоритмов предназначена для надлежащего информационного обеспечения завершающего этапа расследования уголовного дела. Прежде всего, речь идет об установлении достаточности собранной совокупности доказательств, на что прямо указывается в требованиях ст. 88 УПК РФ. Правда, при

этом содержательные особенности данного критерия в данной статье не раскрываются. Поэтому первая часть данной группы алгоритмов нацелена на формирование итогового варианта системы юридических тождеств с использованием уже рассмотренных выше алгоритмов второй группы. После этого выполняется анализ информационной полноты полученной системы – как на количественном, так и на качественном уровне.

Если выявляются информационные пробелы, а также возникают сомнения в том, что какое-либо из доказательств при дальнейшем рассмотрении уголовного дела прокурором и судом может быть исключено, что не позволит доказать наличие в расследуемом деянии состава преступления, то приходится возвращаться к предыдущему этапу расследования и принимать меры для получения недостающих доказательств. Но в том случае, когда информационные пробелы в итоговом варианте системы юридических тождеств отсутствуют, следователь может сделать вывод о наличии в расследуемом деянии состава преступления и принять обоснованное решение о достаточности собранной им совокупности доказательств. При этом он также принимает обоснованное решение о завершении предварительного следствия и переходе к завершающей стадии следственных действий – подготовке и оформлению обвинительного заключения по данному уголовному делу.

Используемое для этого информационное обеспечение основано на применении не только соответствующей части алгоритмов седьмой группы. Эта часть алгоритмов сопряжена и с другими группами алгоритмов, чтобы обеспечить возможность использования в тексте обвинительного заключения той информации, которая была получена на различных этапах расследования уголовного дела. При этом речь идет отнюдь не об «автоматической генерации» текста обвинительного заключения с помощью искусственного интеллекта.

С использованием описанной системы алгоритмов в рамках интерактивной экспертной системы следователь получает возможность в режиме реального времени получать необходимое ему в определенный момент информационное обеспечение на всем протяжении своей работы, начиная с доследственной проверки, всех этапов предварительного следствия и заканчивая подготовкой обвинительного заключения. Следует подчеркнуть, что при возникновении необходимости сформировать и провести сопоставление нескольких вариантов плана расследования, следственных версий, а также ряда других видов нового информационного обеспечения, возникающего в ходе выполнения процессуально регламентированных действий, следователь может получить его также в режиме реального времени.

Но речь идет не только о новых возможностях существенного сокращения трудоемкости и сроков выполнения большей части следственных действий. Не менее важно обратить внимание на ряд новых возможностей для значительного повышения качества следственных действий, что достигается в результате обработки больших объемов информации, имеющей отношение к расследуемому высокотехнологичному экстремистскому преступлению, в том числе, с использованием элементов искусственного интеллекта. Такие объемы информации в настоящее время в ходе выявления преступлений данного вида и расследования

соответствующих уголовных дел ни один следователь обработать не в состоянии. Из-за этого фактически используется лишь малая часть сведений и фактах и обстоятельств, имеющих отношение к таким преступлениям. А возникающие пробелы и противоречия в собранной совокупности доказательств нередко приводят к развалу уголовного дела в суде, в результате чего преступники избегают заслуженного наказания.

Таким образом, для создания научных основ надлежащего информационного обеспечения деятельности следователя по раскрытию и расследованию преступлений экстремистского характера, совершенных с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», необходима консолидация усилий ученых и специалистов для разработки системы алгоритмов взаимодействия следователей с искусственным интеллектом. На их основе могут быть созданы интерактивные экспертные системы, позволяющие в режиме реального времени обеспечить следователя всей необходимой информацией, что, несомненно, будет способствовать более эффективному раскрытию и расследованию преступлений данной категории.

Е.А. Русскевич

Преступления, совершаемые в целях майнинга криптовалюты: вопросы квалификации

Аннотация. Процесс проникновения цифровых финансовых активов в повседневную жизнь граждан и деятельность хозяйствующих субъектов, а равно неуклонный рост преступлений, совершаемых с использованием, в отношении и по поводу криптовалют, актуализируют необходимость научного осмысления особенностей их квалификации. Цель исследования состоит в разработке теоретических рекомендаций по преодолению проблем, возникающих в связи с квалификацией преступлений, совершаемых в целях майнинга криптовалюты.

Ключевые слова: уголовное право; криптовалюта; преступления в сфере компьютерной информации.

Несмотря на наличие известного правового вакуума, следует согласиться с мнением специалистов, что расширение сферы обращения и повышенный криминальный интерес к использованию криптовалюты все чаще вынуждают правоприменителя признавать ее предметом или средством совершения преступления[1]. Изучение доктринальных источников и материалов отечественной судебно-следственной практики позволяет выделить группу преступлений, совершаемых в целях майнинга цифровых финансовых активов (криптовалют).

Анализ современной правоприменительной практики показывает, что к таковым относятся все посягательства, ответственность за которые предусмотрена главой 28 УК РФ «Преступления в сфере компьютерной информации». Прежде

[1] Ляскало А.Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. М., 2019. С. 89.

всего, здесь следует выделить неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ). Так, Б. признан виновным в неправомерном доступе к охраняемой законом компьютерной информации, содержащейся в административной части сайта «regionorel.ru» ГУП ОО «Орловский издательский дом», повлекшем ее модификацию путем внедрения кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование, а также уничтожение компьютерной информации, содержащей сведения обо всех посещениях сайта пользователями и изменениях компьютерной информации сайта (журналы истории посещений и истории команд) объемом 45 Гб, совершенных из корыстной заинтересованности.

Согласно решению суда Б. состоял в трудовых отношения с ГУП ОО «Орловский издательский дом», в должности ведущего специалиста разработал сайт, который к 2012 году обрел свой вид и был размещен на домене «epressa.su» на сервере, распложенном в редакции газета «Орловская правда». В 2014 году редакцией было принято решение о переименовании сайта и смены доменного имени, и вместо «epressa.su» был приобретен домен «regionorel.ru». В июне 2015 года Б. уволился, после чего никакого отношения к сайту «regionorel.ru» не имел.

Прекратив трудовые отношения с ГУП ОО «Орловский издательский дом» с 17 июня 2015 г., перестав иметь законные основания на доступ к серверу и к административной части сайта «regionorel.ru», Б. со своего рабочего компьютера осуществил неправомерный доступ к информации, содержащейся на административной части сайта «regionorel.ru», владельцем которого является ГУП ОО «Орловский издательский дом», путем создания новой учетной записи с правами администратора на любые изменения, регистрации нового пользователя сайта и введения кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование.

Сторона защиты, не согласившись с решением суда первой инстанции, в апелляции указывала на то, что файлы, в которые вносились изменения, являлись общедоступными, автором сайта «regionorel.ru» является Б., а ГУП ОО «Орловский издательский дом» принадлежит только адрес. Сторона защиты не согласилась также с вменением квалифицирующего признака «корыстная заинтересованность», поскольку доказательств возможности получения денежных средств из криптовалюты, их ценность и возможность конвертации обвинением не было представлено.

Несмотря на то что контент сайта не был приведен в непригодное состояние, суд апелляционной инстанции также признал, что это само по себе не влияет на квалификацию действий осужденного, поскольку приведенными выше доказательствами достоверно установлено, что скрипт, внедренный Б. в тело файлов «header.php» и «footer.php», модифицировал сайт «regionorel.ru» в целях получения криптовалюты «Monero» в его личное пользование путем использования вычислительных ресурсов неограниченного круга посетителей пользовательской части сайта «regionorel.ru».

Наличие в действиях Б. квалифицирующего признака «корыстная заинтересованность» суд подлежал установленным, сославшись на то, что в личном кабинете Б. на сайте «Coinhive» имеется информация о том, что сайт, используемый

для майнинга – «regionorel.ru», сумма «монет», заработанная за весь период, составила 0,03225 XMR. Доводы защиты о необходимости представления доказательств получения денежных средств из криптовалюты, суд посчитал также необоснованными, поскольку «сведения о криптовалютах, как о платежных средствах в сети «Интернет», являются общеизвестными и общедоступными, содержащимися в сети «Интернет», где также приводятся и их списки и курс»[1].

Использование вредоносных компьютерных программ (ст. 273 УК РФ), как правило, осуществляется лицами для обеспечения неправомерного доступа к вычислительным ресурсам потерпевших и последующего майнинга криптовалюты. Так, согласно приговору суда, у Ш. возник преступный умысел, направленный на использование из корыстных побуждений аппаратной мощности серверов различных организаций, расположенных на территории Российской Федерации, для генерации криптовалюты (майнинга) путем установки своего программного обеспечения и получения таким способом денежных средств. В период с 28 ноября 2017 г. по 9 января 2018 г. Ш., получив с помощью компьютерной программы IP-адрес сервера с открытым портом, принадлежащего местной муниципальной организации, с целью реализации своего преступного умысла, находясь по месту своего жительства, умышленно, из корыстной заинтересованности ввел IP-адрес организации во вредоносную компьютерную программу и с помощью своего персонального компьютера, подключенного к сети «Интернет», запустил ее, тем самым предпринял попытку получения удаленного доступа к интернет-ресурсам организации, размещенным на сервере, осуществляя повторяющиеся однотипные TCP-сессии с последующей передачей аутентификационной информации. Через некоторое время вредоносная компьютерная программа подобрала логин и пароль к серверу организации. После чего Ш. с помощью незаконно полученных логина и пароля осуществил доступ к серверу и установил на нем свое программное обеспечение (не являющееся вредоносным) для генерации криптовалюты (процесса майнинга)[2].

В приведенном примере квалификация содеянного только по ст. 273 УК РФ, на наш взгляд, является неверной. Исходя из фабулы дела, виновный не только подобрал сетевые идентификаторы к серверу, но и установил программное обеспечение для майнинга криптовалюты, что позволяет утверждать о модификации компьютерной информации. Таким образом, полная юридическая оценка содеянного должна была также включать квалификацию самого неправомерного доступа к серверу с последующей модификацией информации по ст. 272 УК РФ.

По ст. 274 УК РФ как преступное нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей следует оценивать действия работников организации, использовавших ее вычислительные мощности для вычисления

---

[1] Апелляционное постановление Орловского областного суда от 23.08.2019 г. по делу № 22-1120/2019.

[2] Приговор Курганского городского суда Курганской области от 29.11.2018 г. по делу № 1-1186/18.

(майнинга) криптовалюты. Подобный подход нашел свое отражение и в правоприменительной практике. Так, Б. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 274 УК РФ. Согласно приговору суда Б. совместно с другими лицами, находясь в Институте теоретической и математической физики (ИТМФ), действуя умышленно, из корыстной заинтересованности, обладая специальными познаниями в сфере компьютерной техники, заведомо зная о действующих в Федеральном государственном унитарном предприятии «Российский федеральный ядерный центр – Всероссийский научно-исследовательский институт экспериментальной физики» (ФГУП «РФЯЦ-ВНИИЭФ») правилах эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, в том числе о запретах на подключение служебной вычислительной сети к сети «Интернет», а также использование на автоматизированных рабочих местах программного обеспечения, не разрешенного к применению соответствующей комиссией Института, договорились об использовании вычислительных мощностей находящегося в Институте неиспользуемого компьютерного оборудования и возможностей служебной вычислительной сети, предназначенной для обработки конфиденциальной информации уровня конфиденциальности «для служебного пользования», «персональные данные» и «коммерческая тайна», для вычисления (майнинга) криптовалюты и ее последующего обращения в свою пользу, вопреки служебным интересам ФГУП «РФЯЦ-ВНИИЭФ». Реализуя совместный преступный умысел, Б. проследовал в комнату 104 здания ФГУП «РФЯЦ-ВНИИЭФ», где под непосредственным личным контролем со стороны других соучастников, действуя с ними группой лиц по предварительному сговору, путем соединения предоставленных вычислительных систем (серверов) посредством предоставленного коммутатора осуществил сборку вычислителя, необходимого для вычислений (майнинга) криптовалюты. Для обеспечения соединения собранного вычислителя с сетью «Интернет» подключил к нему GSM-модем, после чего загрузил программное обеспечение, предназначенное для майнинга криптовалюты, а также программное обеспечение «eth-proxy», предназначенное для получения через сеть «Интернет» задач на вычисление (майнинг) криптовалюты, сбора результатов вычислений и их отправки в сеть «Интернет» на «Pool» (сервер, который связан со всеми участниками майнинга криптовалют). После этого в период с 1 мая по 31 июля 2017 года Б., действуя умышленно, из корыстной заинтересованности в составе группы лиц по предварительному сговору, находясь в здании ИТМФ в течение нескольких недель преимущественно в ночное время, запускали процесс майнинга криптовалют на вышеназванной «ферме». Вышеуказанные действия привели к нарушению условий действия аттестата соответствия на объект информатизации, что повлекло необходимость проведения внеочередной повторной аттестации, стоимость которой составила 1 140 157 рублей 10 копеек. Таким образом, нарушение правил эксплуатации средств хранения, обработки и

передачи охраняемой компьютерной информации, совершенное Б., повлекло причинение ФГУП «РФЯЦ-ВНИИЭФ» крупного материального ущерба[1].

Литература

1. Ляскало А.Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. М., 2019. С. 87-92.
2. Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. – М. : ИНФРА-М, 2019. – 227 с.

А.Л. Санташов

Преступления экономической направленности, совершаемые в местах лишения свободы дистанционно

Аннотация. В статье рассматриваются проблемы совершения преступлений осужденными с использованием интернет-ресурсов. Проводится анализ виктимологических аспектов безопасности сотрудников уголовно-исполнительной системы и их взаимоотношений с представителями криминального мира. Делается вывод о необходимости более тщательного подбора кадров для исправительных учреждений.

Ключевые слова: киберпреступность; интернент; преступления, совершенные дистанционно; осужденные; уголовно-исполнительная система.

Проблема киберпреступности и ее предупреждения имеет сегодня приоритетное значение. В 2020 году каждое 4 преступление совершалось с использованием высоких технологий. Так, в указанном периоде число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%[2]. Сегодня уже далеко не секрет, что благодаря кибертехнологиям и сети интернет, совершается масса преступлений экономической направленности, в том числе и дистанционно. Зачастую, мошенниками выступают лица, отбывающие наказание в виде лишения свободы в исправительных учреждениях уголовно-исполнительной системы (далее – УИС).

Поскольку профессиональная деятельность сотрудников УИС каждодневно связана с лицами, осужденными за совершение уголовно наказуемых деяний, их виктимная предрасположенность не вызывает сомнений. Более того, рост

[1] Приговор Саровского городского суда Нижегородской области от 17.09.2019 г. по делу № 1-149/2019.

[2] См.: Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года // Официальный сайт МВД России. – URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 15.12.2021).

уровня виктимности сотрудника исправительного учреждения имеет прямую зависимость от количества непосредственных контактов со спецконтингентом и характера исполняемых жертвой служебных обязанностей.

Вступая в преступный сговор с осужденными, организующими совершение преступлений экономического характера, сотрудник не только подрывает имидж сотрудника, авторитет уголовно-исполнительной системы как субъекта государственной власти, причиняет экономический вред интересам общества и государства, но и создает ситуацию потенциальной угрозы для себя и своих близких.

Сотрудники исправительных учреждений зачастую становятся жертвами насильственных преступлений, совершаемых осужденными. По данным официальной статистики Федеральной службы исполнения наказаний наблюдается рост посягательств на сотрудников УИС. Так, в 2020 году зарегистрировано 175 фактов применения насилия в отношении сотрудников УИС (АППГ – 174)[1]. При этом одной из причин покушения на жизнь и здоровье сотрудников исправительных учреждений является преступное взаимодействие самих сотрудников с лицами, отбывающими наказание в местах лишения свободы, которые продолжают преступную деятельность в целях финансового обогащения, совершая преступления дистанционно.

Недочеты в правовом регулировании, кадровой, воспитательной работе соответствующих подразделений исправительных учреждений с сотрудниками усугубляют описанную ситуацию, и указывают на необходимость соответствующих правовых и организационных изменений в данной сфере, в том числе, усиление виктимологической профилактики пенитенциарной преступности экономической направленности.

Как справедливо отмечает в юридической литературе, любое нарушение безопасности в УИС свидетельствует о возможности наступления негативных последствий как для осужденных, так и для персонала пенитенциарных учреждений, для нормальной деятельности уголовно-исполнительной системы в целом и, в конечном счете, - общества и государства[2]. Более того, восстановить и укрепить безопасность после потрясений гораздо сложнее, чем удержать уже существующий порядок[3].

Однако если проблеме безопасности осужденных посвящены многие научные работы, то безопасности сотрудников УИС уделяется недостаточное внимание[4].

---

[1] См.: Основные показатели деятельности уголовно-исполнительной системы (январь – декабрь 2020 г.). Информационно-аналитический сборник. Тверь, 2021. С. 19, 31.

[2] См.: Казак Б.Б., Савихин А.М. Теоретические основы безопасности в уголовно-исполнительной системе: Лекция. – Псков: Псков. юрид. ин-т ФСИН России, 2006. С. 4-5.

[3] См.: Казак Б.Б. Уголовно-исполнительная система в механизме обеспечения внутренней безопасности общества (теоретические и организационно-правовые аспекты): Дис. … д-ра юрид. наук – М., 2000. – С. 24.

[4] См.: Санташов А.Л., Житков А.А. Современное состояние и перспективы развития уголовного законодательства о дезорганизации деятельности учреждений, обеспечивающих изоляцию от общества // Вестник Московской академии Следственного комитета. 2020. № 4. С. 58-64.

При этом ее актуальность не вызывает сомнений. Значимость данного вопроса объясняется особыми условиями деятельности сотрудников, состоящих в штатах учреждений, исполняющих наказание в виде лишения свободы, и подтверждается мнением самих сотрудников. Так, анализ результатов анкетирования показал, что преобладающее большинство опрошенных указывают на важность деятельности по обеспечению безопасности сотрудников учреждения.

Действительно, в связи с гуманизацией уголовной и уголовно-исполнительной политики, более широким применением мер наказаний, не связанных с лишением свободы, в исправительных колониях концентрируется наиболее криминальная часть осужденных, совершивших тяжкие и особо тяжкие преступления. Каждый шестой из них отбывает наказание за совершение убийства, каждый третий - за грабеж, разбойное нападение и бандитизм. 20% спецконтингента относятся к алкоголикам и наркоманам. В места лишения свободы поступает все больше лиц с повышенной агрессивностью и возбудимостью, очевидными психическими отклонениями. Попытки подкупа, шантажа и запугивания со стороны осужденных перерастают в угрозы и акты физического воздействия на сотрудников исправительных учреждений и членов их семей.

Особое внимание следует уделить характеристике пенитенциарной преступности, которая является отражением характеристики преступности в целом. По данным статистики за 2020 год в исправительных учреждениях совершено 1025 преступлений (АППГ – 974), из них преступления экономической направленности и корыстно-насильственные составляют более 60%. Например, дезорганизация деятельности учреждения – 192 (АППГ – 181) случая, незаконный оборот наркотических средств – 225 (АППГ – 201) случаев, убийства и умышленное причинение тяжкого вреда здоровью – 33 (АППГ – 37) случая[1].

Так, высокие показатели количества преступлений, серьезные негативные качественные изменения в ней, усиление криминализации общества, а, следовательно, и малая эффективность традиционных мер уголовно-правового принуждения выступают мощными факторами криминальной угрозы, в том числе в отношении сотрудников исправительных учреждений. Что заставляет активизировать как общее, так и виктимологическое предупреждение пенитенциарных преступлений.

Виктимологическая профилактика преступлений, совершаемых против сотрудников УИС, выступает важным элементом обеспечения их безопасности.

Криминологами установлено, что одним из факторов, приводящих к совершению преступлений в отношении личности, является ее контакт с представителями криминального мира. Это утверждение справедливо в отношении 70% изученных ими случаев, из чего получен вывод о повышении виктимизации личности при условии ее взаимодействия с преступниками[2]. Поскольку профессиональная деятельность сотрудников УИС каждодневно связана с лицами, осуж-

---

[1] См.: Основные показатели деятельности уголовно-исполнительной системы (январь – декабрь 2020 г.). Информационно-аналитический сборник. Тверь, 2021. С. 19, 31.

[2] См.: Криминопенология: Учебное пособие. Рязань, 2010. С. 56.

денными за совершение уголовно наказуемых деяний, их виктимная предрасположенность не вызывает сомнений. Более того, рост уровня виктимности сотрудника пенитенциарного учреждения имеет прямую зависимость от количества непосредственных контактов со спецконтингентом и характера исполняемых жертвой служебных обязанностей.

Кроме того, любой сотрудник УИС воспринимается представителями криминального мира враждебно, как представитель чуждого им социума, не разделяющего их ценности и правила. Это обстоятельство не только оправдывает, но и делает желаемым, поощряемым в преступной среде любое физическое или психическое насилие, оскорбление в отношении сотрудника учреждения.

Осужденный, совершающий подобные действия, автоматически повышает свой авторитет в преступной среде. Поэтому преступник часто реализует уголовно наказуемое деяние в отношении сотрудника УИС публично, стараясь привлечь внимание других осужденных к его преступным действиям.

Анализ пенитенциарной преступности показывает, что большое количество преступлений, совершаемых лицами, отбывающими наказание в местах лишения свободы – это преступления в сфере экономики, а именно против собственности. С учетом изоляции таких лиц от общества, практически единственным видом этих преступлений является мошенничество, то есть хищение чужого имущества путем обмана или злоупотребления доверием (ст. 159 УК РФ). Кроме того, для исправительных учреждений незаконный оборот наркотических средств не является исключением и имеет корыстный характер. Особенностью осуществления данных действий выступает также форма их совершения – дистанционно. Такие преступления позволяют осужденным, будучи изолированными от общества, продолжать преступную деятельность в целях финансового обогащения. При этом помощь в реализации преступного умысла оказывают должностные лица исправительных учреждений. Зачастую осужденные создают организованные группы и преступные сообщества, привлекая в число участников именно сотрудников. В свою очередь, сотрудники, используя свое служебное положение, осуществляют проносы запрещенных предметов, в том числе, средств мобильной связи, наркотических средств, попустительствуют при поддержании правил внутреннего распорядка исправительных учреждений, допуская пользование осужденными указанными запрещенными предметами.

Будучи вовлеченным в совершение преступлений сотрудник не только преступает закон, но и становится зависимыми от осужденных. А, следовательно, в случае отказа от дальнейшего преступного взаимодействия его жизнь и здоровье ставятся под угрозу. Что используется осужденным для планирования преступной деятельности при их ограниченных возможностях.

Среди причин гибели и ранений, полученных личным составом УИС, недостаточного обеспечения их личной безопасности называют низкий профессионализм и личную недисциплинированность отдельной категории сотрудников,

снижение требовательности руководителей к подчиненным, отсутствие надлежащего контроля за их поведением на службе и в быту[1]. В целях минимизации чрезвычайных происшествий, связанных с безопасностью сотрудников УИС, руководителям органов и учреждений УИС следует пристальное внимание уделять профилактическим мерам. Превентивная стратегия должна базироваться на планировании и практической реализации комплекса взаимосвязанных мероприятий правового, воспитательного, кадрового, медицинского и психологического сопровождения[2].

Также особенностью деятельности по обеспечению безопасности сотрудников, как отмечается в научной литературе, является то, что наравне с кадровыми, воспитательными аппаратами, руководителями различных уровней, отвечающих за безопасность своих подчиненных, субъектами ее реализации выступают службы безопасности исправительных учреждений. Последние являются специальными субъектами, которые наделены соответствующими функциями.

Список использованных источников

1. Основные показатели деятельности уголовно-исполнительной системы (январь – декабрь 2020 г.). Информационно-аналитический сборник. Тверь, 2021.
2. Казак Б.Б., Савихин А.М. Теоретические основы безопасности в уголовно-исполнительной системе: Лекция. – Псков: Псков. юрид. ин-т ФСИН России, 2006.
3. Казак Б.Б. Уголовно-исполнительная система в механизме обеспечения внутренней безопасности общества (теоретические и организационно-правовые аспекты): Дис. … д-ра юрид. наук – М., 2000.
4. Карькина Н.Н. Обеспечение безопасности осужденных – представителей этнических групп от криминальных угроз в местах лишения свободы. Дис. … канд. юрид. наук. Рязань, 2010.
5. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года // Официальный сайт МВД России. – URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 15.12.2021).
6. Криминопенология: Учебное пособие. Рязань, 2010.
7. Санташов А.Л., Житков А.А. Современное состояние и перспективы развития уголовного законодательства о дезорганизации деятельности учреждений, обеспечивающих изоляцию от общества // Вестник Московской академии Следственного комитета. 2020. № 4. С. 58-64.

[1] См.: Карькина Н.Н. Обеспечение безопасности осужденных – представителей этнических групп от криминальных угроз в местах лишения свободы: Дис. … канд. юрид. наук. Рязань, 2010. С. 3-4.

[2] См.: Штаненко В. Основные направления служебной деятельности по организации режима отбывания наказания осужденными и обеспечению безопасности в ИУ // Ведомости уголовно-исполнительной системы. – 2007. - № 12. – С.3-5.

8. Штаненко В. Основные направления служебной деятельности по организации режима отбывания наказания осужденными и обеспечению безопасности в ИУ // Ведомости уголовно-исполнительной системы. – 2007. - № 12. – С.3-5.

А.Г. Скуковский
П.О. Мироненкова

Некоторые проблемы, связанные с расследованием киберпреступлений

Аннотация. В данной статье рассматриваются проблемы, возникающие при расследовании преступлений в киберпространстве, а также приводятся особенности данного вида преступлений, оказывающие влияние на организацию и планирование хода расследования.

Ключевые слова: киберпреступления, следственные действия, привлечение специалиста, осмотр места происшествия, информационное пространство.

На сегодняшний день мы являемся свидетелями грандиозного явления, называемого техническим прогрессом. Компьютеризация практически всех сфер общественной жизни открывает новые возможности в развитии экономики, медицины, образования. Вместе с тем это стимулировало резкий всплеск преступлений, совершаемых при помощи компьютерных технологий. Исходя из данных статистики, за январь-ноябрь 2019 г. в Российской Федерации было зарегистрировано около 261 тыс. фактов совершения киберпреступлений (что на 70% больше, чем за аналогичный период 2018 года)[1]. Становится бессмысленным отрицать факт вхождения в нашу жизнь нового вида преступлений, что, в свою очередь, требует разработки новых подходов и методов расследования.

На сегодняшний день преступления в сфере компьютерной информации являются одним из самых латентных видов преступлений. Процент выявления данного вида преступлений невелик, в том числе по причине того, что зачастую потерпевшим об их совершении ничего не известно либо становится известно лишь со временем. Так, к примеру незаконное копирование информации очень часто остается незамеченным, а введение в компьютер вируса обычно объясняется непреднамеренной ошибкой пользователя[2]. Высокая степень латентности киберпреступлений связана также с тем, что сами пострадавшие (особенно если потерпевшими являются крупные коммерческие организации, банки) не спешат сообщать правоохранительным органам о факте совершения преступления, опасаясь подрыва деловой репутации. А в ситуациях, когда потерпевшей стороной выступает физическое лицо, а не организация, граждане иногда предпочитают не обращаться в правоохранительные органы, поскольку боятся разглашения в

[1] Долженко Н.И., Ярощук И.А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. №1. С. 151-157.
[2] Долженко Н.И., Ярощук И.А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. №1. С. 151-157.

ходе следствия информации, которая может содержать сведения личного, интимного характера[1].

Еще одной особенностью киберпреступлений является их трансграничность (иными словами, преступления в киберпространстве чаще всего не ограничены территорией одного государства). Ситуация, когда субъект преступления и потерпевший находятся в разных странах, требует международного сотрудничества. Некоторым препятствием к успешному взаимодействию правоохранительных органов будут особенности в системе внутреннего права разных государств, различная степень разработанности вопроса о киберпреступлениях на законодательном уровне. В настоящее время рядом государств уже были предприняты успешные попытки заключения международных соглашений о сотрудничестве при предупреждении и расследовании преступлений в киберпространстве. Но на сегодняшний момент отсутствует единый (хотя бы для большей части государств) глобальный нормативно-правовой акт, регламентирующий порядок борьбы с киберпреступностью.

Киберпреступность отличается также высокой степенью анонимности преступника. Существующие на сегодняшний день VPN/VPS-сервисы для анонимизации трафика, виртуальные номера мобильных телефонов, криптовалютные кошельки (создание которых не требует внесения паспортных данных) обеспечивают лицу возможность практически полностью скрыть свою личность. Даже если следствию удается идентифицировать то или иное электронное устройство в качестве орудия совершения преступления, установить причастность конкретного лица к совершению (посредством данного устройства) преступления часто становится затруднительно.

Одна из главных проблем расследования киберпреступлений связана с невозможностью точного применения к ним стандартного алгоритма расследования: следственные действия, закрепленные в уголовно-процессуальном законодательстве, при расследовании данного типа преступлений не будут обладать большой эффективностью. Например, осмотр места происшествия, которому обычно придается центральное значение, при расследовании преступлений в киберпространстве будет иметь ряд особенностей. Во-первых, возникает вопрос, что именно будет считаться местом преступления с процессуальной точки зрения (например, в случаях, когда преступником была совершена хакерская атака): место нахождения хакера во время атаки, место написания им вредоносной программы, адрес потерпевшего, место обналичивания денег (при совершении атак на финансовые организации), или какое-либо иное место? Учитывая, что киберпреступления совершаются в так называемом «виртуальном пространстве», некоторые исследователи предлагают считать местом происшествия определенный диапазон виртуального (информационного) пространства[2]. Даже если принять их точку зрения, то следствие сталкивается со следующей проблемой: как

---

[1] Егерева О.А., Коломинов В.В., Сизова М.С. Некоторые вопросы методики расследования киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. №4 (22). С. 24-32.

[2] Протасевич А.А., Зверянская Л.П. Особенности осмотра места происшествия по делам о киберпреступлениях // Baikal Research Journal. 2013. №2. С. 23.

вообще возможно проведение осмотра места происшествия, если на киберпространство не распространяются географические (а, следовательно, и юридические) законы? Сама процедура осмотра места происшествия также сопряжена с рядом особенностей: традиционные методики криминалистической техники здесь безрезультативны, поскольку работа идет не с привычными следами, а с электронными[1] (их также называют «цифровыми следами» и выделяют две их разновидности: активные и пассивные следы. К первой категории относится информация, которую пользователь вводит самостоятельно: к примеру, ФИО, дата рождения в социальных сетях, личных кабинетах иных сайтов. А к группе пассивных следов относят следы, оставленные лицом ненамеренно, вследствие работы программного обеспечения).

Примерно также дела обстоят и со следственным экспериментом (с целью выяснения обстановки совершения преступления). При расследовании киберпреступлений данное следственное действие само по себе практически теряет свой смысл, поскольку изменения во внешней обстановке никак не влияют на изменения в кибернетическом пространстве (что и составляет суть киберпреступлений).

Даже такое следственное действие как допрос подозреваемого или обвиняемого в совершении киберпреступления сопряжено с рядом трудностей. Главная проблема здесь заключается в том, что подозреваемый/обвиняемый в процессе допроса практически всегда изъясняется специфическими терминами, трудно воспринимаемыми для человека без соответствующего образования и знаний в сфере компьютерных технологий. Следователю необходимо (с помощью привлечения соответствующего специалиста) перевести данные термины и выражения на юридический язык, при этом сделав их понятными для участников судопроизводства. Присутствие специалиста во время допроса подозреваемого/обвиняемого может отрицательно сказаться на результатах допроса по ряду причин[2]: во-первых, присутствие специалиста (как и присутствие любого третьего лица) осложняет налаживание психологического контакта между следователем и допрашиваемым лицом, а во-вторых, у подозреваемого/обвиняемого возникает понимание того, что следователь (ведущий производство по его делу) не понимает суть совершенного противоправного деяния и механизм его совершения (вследствие чего у лица возникает мысль о потенциальной возможности ввести следствие в заблуждение). Определенные трудности связаны и с допросом свидетелей. Это обусловлено тем, что основная масса свидетелей не имеет четкого понимания произошедшего вследствие отсутствия специальных знаний.

Практически всегда в рамках расследования дела о киберпреступлениях производится выемка техники (компьютера и периферийного оборудования, иных носителей электронной информации) с целью назначения экспертизы по данным

---

[1] Под «электронно-цифровыми следами» понимается «любая криминалистически значимая компьютерная информация, т.е. сведения, находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов.

[2] Смирнова И.Г., Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Baikal Research Journal. 2015. №3. С. 27.

объектам. Следователю на данном этапе приходится прибегать к помощи специалиста, поскольку изъятие и транспортировка данных объектов имеет ряд особенностей. При производстве выемки обязательно присутствие понятых, но они имеют представление лишь об изъятии носителя информации, а не о наличии той или иной криминалистически значимой информации на данном носителе. Также следует отметить, что процесс изъятия осложняется постоянным риском потери информации. Также процедура выемки осложняется тем, что следователю совместно со специалистом приходится решать вопрос об изъятии каждого конкретного предмета, исходя из необходимости полного и всестороннего исследования с одной стороны, и руководствуясь принципом обоснованной необходимости изъятия с другой стороны (так как компьютеры, мобильные телефоны, являются важными рабочими инструментами представителей многих профессий, и их изъятие на длительный срок может нанести существенный вред интересам лица).

Важным этапом расследования уголовных дел о киберпреступлениях будет назначение компьютерно-технической экспертизы. Вследствие того, что данный вид преступлений появился относительно недавно, количество экспертных учреждений, в которых имеются специалисты данной отрасли, невелико. Из-за этого возникает проблема высокой загруженности данных экспертных учреждений, что влечет за собой увеличение времени выполнения экспертиз. Также немаловажным аспектом назначения компьютерно-технической экспертизы будет постановка следователем грамотных вопросов эксперту, с чем возникают определенные трудности вследствие отсутствия у следователей специальных знаний в области компьютерной техники и информационных технологий.

В связи с ростом числа киберпреступлений за последнее время, в декабре 2017 года было создано Управление «К» МВД РФ (подразделение, борющееся с преступлениями в сфере информационных технологий), а в декабре 2019 г. Председатель Следственного комитета Российской Федерации подписал приказ о создании в составе Главного следственного управления нового подразделения – отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий. Тем не менее, на сегодняшний день (из-за большого числа совершаемых преступлений данного вида и малого количества сотрудников вышеуказанных подразделений) – расследовать уголовные дела о киберпреступлениях нередко приходится обыкновенным следователям, не имеющим специальных знаний в данной отрасли. Для более успешной борьбы с киберпреступлениями следует повышать уровень компьютерной грамотности как сотрудников правоохранительных органов (в целях обеспечения более успешного противодействия преступлениям данного вида), так и населения в целом.

Список использованных источников

1. Долженко Н.И., Ярощук И.А. Киберпреступность как одна из ключевых проблем современности // Legal Concept. 2020. №1. С. 151-157.

2. Егерева О.А., Коломинов В.В., Сизова М.С. Некоторые вопросы методики расследования киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2018. №4 (22). С. 24-32.
3. Протасевич А.А., Зверянская Л.П. Особенности осмотра места происшествия по делам о киберпреступлениях // Baikal Research Journal. 2013. №2. С. 23.
4. Смирнова И.Г., Коломинов В.В. Тактические особенности производства допроса по делам о преступлениях в сфере компьютерной информации // Baikal Research Journal. 2015. №3. С. 27.

С.В. Смелова

Актуальные вопросы квалификации преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий

Аннотация. В статье рассматриваются проблемы практики применения норм глав 28 УК РФ. Отмечается дискуссионность вопросов толкования отдельных признаков преступлений, предусмотренных статьями 272, 273 УК РФ. Приводятся различные подходы правоприменителя к квалификации данных преступлений по совокупности с иными преступлениями.

Ключевые слова: компьютерная информация, неправомерный доступ к компьютерной информации, вредоносная компьютерная программа, тяжкие последствия, квалификация преступлений.

Следственно-судебная практика демонстрирует противоречивые подходы к правовой оценке противоправных деяний, совершаемых с использованием компьютерных и телекоммуникационных технологий, в том числе, посягающих на общественные отношения в сфере безопасности компьютерной информации (глава 28 УК РФ). Из этой группы преступлений наиболее распространены неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных компьютерных программ (ст. 273). Проблемы правоприменения связаны с толкованием отдельных признаков данных преступлений, их квалификацией по совокупности с другими преступлениями. В настоящее время отсутствует обобщение практики применения норм главы 28 УК РФ на уровне отдельного постановления Пленума Верховного Суда РФ и соответствующие разъяснения по актуальным вопросам квалификации преступлений в сфере компьютерной информации.

Определенные сложности возникают в толковании оценочного понятия, используемого для описания квалифицирующего признака деяний, – наступление тяжких последствий (ч. 4 ст. 272, ч. 3 ст. 273 УК РФ), о чем свидетельствует и

незначительная практика применения данных норм[1]. В Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации применительно к ст. 273 УК РФ отмечается необходимость учета всей совокупности обстоятельств дела при определении тяжести последствий и приводится их примерный перечень: причинение особо крупного материального ущерба, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности и др.[2].

Законодатель конкретизировал лишь размер крупного ущерба применительно к нормам главы 28 (примечание 2 к ст. 272 УК РФ). Анализ материалов практики показывает, что при квалификации действий виновного по совокупности преступлений, предусмотренных ст. 272, 273 и 158 (159.6) УК РФ, правоприменитель в отдельных случаях признает крупным ущербом, причиненным в результате неправомерного доступа к компьютерной информации и использования вредоносных компьютерных программ, сумму, соответствующую стоимости похищенного имущества (как правило, денежных средств), если она превышает один миллион рублей[3]. Вместе с тем единообразный подход в этой части отсутствует, кроме того, необходимо учитывать категории тяжести этих преступлений. К примеру, квалифицируя по ч.3 ст. 272, ч.2 ст. 273 и ч.4 ст. 159.6 УК РФ действия лиц, похитивших в составе организованной группы из банкоматов денежные средства в сумме, признанной применительно к ст. 159.6 УК РФ особо крупным размером, следственные органы не усмотрели признак причинения тяжких последствий деяний в сфере компьютерной информации[4].

Неправомерный доступ к компьютерной информации, использование и распространение вредоносных компьютерных программ зачастую совершаются с целью облегчить совершение другого преступления, как правило, корыстной направленности. Согласно вышеуказанным методическим рекомендациям Генеральной прокуратуры, если действие вредоносной программы было условием совершения другого преступления, содеянное квалифицируется по совокупности преступлений независимо от степени тяжести иного преступления. При этом следует учитывать, что в случае хищения чужого имущества на сумму менее 2500 рублей, состав кражи (мошенничества) отсутствует, действия виновного

---

[1]В 2019 г. осуждено по ч. 4 ст. 272 УК – 2 лица (в 2018 г. – 2), по ч. 3 ст. 273 УК в 2019 г. и 2018 г. – 0. См.: Отчеты о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2018, 2019 годов //Официальный сайт Судебного департамента при Верховном Суде РФ / URL: www. cdep.ru (дата обращения 04.12.2020).

[2]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013 // Единый портал прокуратуры РФ. URL: http://epp.genproc.gov.ru (дата обращения: 04.12.2020).

[3] Приговор Октябрьского районного суда г. Владимира от 04.06.2019 г. Дело № 1-95/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

[4] Приговор Якутского городского суда Республики Саха (Якутия) от 26.08.2019 г. Дело № 1-681/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

квалифицируются только по ст. 272 (273) УК РФ как совершенные из корыстной заинтересованности.

Различные подходы имеют место при квалификации действий лиц, которые по независящим от них причинам при использовании заведомо вредоносной программы не смогли получить неправомерной доступ к охраняемой законом информации, ее модифицировать (копировать). Так, по ч. 1 ст. 273 УК РФ квалифицированы действия Е., который использовал вредоносное программное обеспечение для воздействий на веб-сервер с IP-адресом, принадлежащим информационным ресурсам правительства Кировской области, но ввиду его высокой технической защищенности доступ к компьютерной информации предоставлен не был[1]. По ч. 3 ст. 30 ч. 2 ст. 272, ч. 2 ст. 273 УК РФ осужден Г., который, используя заведомо вредоносную программу, совершил незаконные действия, направленные на получение несанкционированного удаленного доступа к базе данных адресов электронных почтовых ящиков зарегистрированных пользователей официального сайта администрации Курской области и паролей к ним, содержащихся в закрытой части сайта, однако не смог нейтрализовать систему защиты информации[2].

Актуальными для правоприменителя и дискуссионными среди исследователей остаются вопросы квалификации хищений, совершенных посредством неправомерного доступа к компьютерной информации и посредством создания, использования и распространения вредоносных компьютерных программ[3]. В научной литературе справедливо обращается внимание и на нерешенность вопроса о квалификации хищения денежных средств из банкоматов, совершенном с помощью вредоносных компьютерных программ: по ст. 158 или 159.6 УК РФ[4]. Рассматривая компьютерную информацию операционной системы банкомата как объект посягательства, правоприменитель в регионах демонстрирует различные подходы при квалификации схожих по способу противоправных действий, направленных на хищение денежных средств из банкоматов. Так, Д. осужден по ч. 3 ст. 272, ч. 2 ст. 273, ч. 3 ст.30 п. б ч. 4 ст.158 УК РФ. Подключив к банкомату клавиатуру, флешкарту USB и DSB-разветвитель и установив в банкомат вредоносную компьютерную программу, Д. совершил неправомерный доступ к охраняемой законом компьютерной информации в операционной системе банкомата, вследствие чего произошло блокирование и нейтрализация средств защиты этой информации, выразившаяся в том, что вредоносные файлы

---

[1] Приговор Иловлинского районного суда Волгоградской области от 11.02.2019 г. Дело № 1-14/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

[2] Приговор Ленинского районного суда г. Владимира от 27.07.2018 г. Дело № 1-211/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

[3] См.: пункты 20 и 21 постановления Пленума Верховного Суда РФ от 20.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2.

[4] Евдокимов К.Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Российский судья. 2019. № 2. С. 12-16.

скрытно, незаконно подключились к управлению банкоматом и к механизму выдачи денежных купюр, дав через удаленный доступ сети Интернет возможность управлять действиями вредоносной программы через клавиатуру банкомата, предоставив в распоряжение технические каналы выдачи наличных денежных средств. В результате банкомат выдал Д. денежные средства, однако в этот момент Д. был задержан сотрудниками охраны банка[1]. По другому делу в подобной ситуации органы расследования не усмотрели в действиях лиц признаки неправомерного доступа к компьютерной информации[2]. Хищение денежных средств из банкоматов аналогичным вышеуказанному способом квалифицируется и по ст. ст. 159.6, 272 и 273 УК РФ[3].

Таким образом, остается актуальной выработка единых подходов правоприменителя к квалификации преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий.

Список использованных источников

1. Постановление Пленума Верховного Суда РФ от 20.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // БВС РФ. 2018. № 2.
2. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013 // Единый портал прокуратуры РФ. URL: http://epp.genproc.gov.ru (дата обращения: 04.12.2020).
3. Евдокимов К.Н. Актуальные вопросы совершенствования судебной практики по уголовным делам о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Российский судья. 2019. № 2. С. 12-16.
4. Отчеты о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам за 12 месяцев 2018, 2019 годов //Официальный сайт Судебного департамента при Верховном Суде РФ / URL:: www. cdep.ru (дата обращения 04.12.2020).
5. Приговор Первомайского районного суда г. Ижевска Удмуртской Республики от 14.06.2018 г. Дело № 1-272/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения:

[1] Приговор Первомайского районного суда г. Ижевска Удмуртской Республики от 14.06.2018 г. Дело № 1-272/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

[2] Приговор Прикубанского районного суда г. Краснодара от 19.12.2019 г. Дело № 1-76/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

[3] Приговор Октябрьского районного суда г. Владимира от 04.06.2019 г. Дело № 1-95/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

04.12.2020).
6. Приговор Ленинского районного суда г. Владимира от 27.07.2018 г. Дело № 1-211/2018 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).
7. Приговор Иловлинского районного суда Волгоградской области от 11.02.2019 г. Дело № 1-14/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).
8. Приговор Октябрьского районного суда г. Владимира от 04.06.2019 г. Дело № 1-95/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).
9. Приговор Якутского городского суда Республики Саха (Якутия) от 26.08.2019 г. Дело № 1-681/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).
10. Приговор Прикубанского районного суда г. Краснодара от 19.12.2019 г. Дело № 1-76/2019 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: Sudact.ru (дата обращения: 04.12.2020).

А.Б. Смушкин

Проблемы поиска электронных следов в системах распределенного хранения данных в процессе расследования

Аннотация. В статье рассматриваются основные проблемы, с которыми могут столкнуться правоохранительные органы при исследовании распределенной информации. Определяется, что к технологиям, с которыми может столкнуться в рассматриваемой сфере следствие, относятся пиринговые или замкнутые сети ограниченного числа пользователей (типа Friend-to-friend- сети), блокчейн, сети распределенных вычислений и отдельные элементы некоторых мессенджеров. Автор констатирует необходимость активизации криминалистического исследования систем распределенного хранения электронных данных, как элемента электронной цифровой криминалистики.

Ключевые слова: криминалистическое исследование систем распределенного хранения информации; одноранговые сети; блокчейн; файлообменные сети; электронные следы; криптовалюта.

Технологии распределенного хранения информации занимают в последнее время в деятельности физических и юридических лиц все большее место. Однако они продолжают оставаться достаточно новым правовым явлением.

На настоящий момент исчезающе мало отечественных криминалистических публикаций посвящено в общем и целом исследованию распределенной информации и обнаружению, фиксации и исследованию следов в системах, образованных с использованием технологий распределенного хранения данных, в частности. Между тем правоохранительные органы все чаще начинают сталкиваться с необходимостью изъятия и исследования подобной информации и следов.

С необходимостью исследования распределенной информации следствие может столкнуться при расследовании различных вариантов незаконного распро-

странения информации (распространения экстремистской информации, информации, распространяемой с нарушением авторских прав, нарушением коммерческой тайны, тайны личной жизни и т.д.), использовании браузера типа Tor для совершения преступлений, организации внутренней файлообменной сети юридического лица, попавшего в сферу изучения правоохранительными структурами или группы лиц, совершающих преступления. К этой же категории можно отнести и инструменты, предоставляемые технологиями блокчейна, используемые пользователями «теневого» Интернета, Даркнета в ходе совершения преступлений.

К системам распределенного хранения информации относятся, в первую очередь, пиринговые (от английского peer-to-peer, P2p- «равный к равному») сети, блокчейн, сети распределенных вычислений и отдельные элементы некоторых мессенджеров типа Skype, Tox и т.д.

Теневой интернет, Даркнет, так же во многом задействует технологии распределенного хранения информации в изолированных пиринговых сетях замкнутого типа.

Особенностью функционирования систем распределенного хранения информации является дробление любого информационного объекта на доли. Эти доли располагаются не на одном сервере, как это происходит в централизованных сетях, что ограничивает пропускную способность при одновременном скачивании большим количеством пользователей. Распределенные сети- это, как правило, одноранговые, децентрализованные сети. Любой пользователь может перекачивать информационные объекты долями у любых иных пользователей сети. Скорость перекачки при этом ограничена скоростью самого пользователя. Если определенная доля информационного объекта есть у нескольких пользователей, то и перекачка происходит одновременно у нескольких, в итоге- повышая скорость раздачи. При этом у разных пользователей могут быть разные доли информационного объекта, перекачиваемые взаимно непоследовательно друг у друга.

Следует отметить первую проблему практической криминалистической деятельности- сложность установления источника происхождения информации в пиринговой сети. Как мы уже отмечали ранее, «при использовании технологий распределенного хранения информации, информационный объект (файл или совокупность файлов) дробится на определенное количество частей. При этом, у каждого пользователя может не быть полного информационного объекта, который собирается только по запросу. ... В определенный период времени может вообще ни у кого из пользователей не быть полного объекта, если первоначальный владелец, убедившись, что в пиринговой сети у совокупности пользователей есть полная совокупность частей информационного объекта, удалил полный объект» [1]. При этом, использование анонимайзеров, Proxy-серверов и vpn-

[1] Смушкин А.Б. Криминалистическое исследование и использование технологий распределенного хранения данных в Кн.: Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : коллективная монография в 2 т. / под ред. Н.Н. Ковалёвой ; ФГБОУ ВО «Саратовская государственная юридическая академия». – Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2020. Т.1 С. 311

технологий, позволит ему замаскировать даже первоначальное свое присутствие в сети. Рядовые же пользователи одноранговой сети вполне могут и не иметь представления о незаконности информации (конечно, когда противозаконность связана не с содержанием самой информации). В определенный момент, может вообще не быть полного информационного объекта ни у кого из пользователей сети, а доли объекта не давать возможности распознать даже формат целого, не говоря о содержании. Между тем, расследование преступлений, связанных с незаконным распространением или использованием определенной информации требует установления и источника происхождения этой информации. К основным идентификаторам пользователя в пиринговых сетях при сетевых действиях относится IP-адрес и MAC-адрес. Аппарата, с которого производился выход в сеть, однако динамический IP и VPN-технологии вполне маскируют сетевой адрес выхода в сеть. MAC-адрес компьютерного устройства может меняться программными средствами

Возникает так же проблема ответственности пользователей, обладающих лишь частью, долей информационного объекта с ограниченной в распространении информацией, а также проведением следственных действий в отношении таких пользователей- ведь их могут насчитываться сотни и тысячи, находящихся в разных местах страны и за ее пределами. При этом, необходимо принимать во внимание, что пользователь, осуществляющий скачивание крупного составного информационного объекта, может не иметь представление о противозаконности его отдельной части, размещенной там злоумышленником или не иметь представление о истинном содержании информационного объекта, перекачиваемого им по понравившемуся названию, не соответствующему содержимому.

Еще одной проблемой является то, что не все одноранговые сети дают свободный доступ к информации, в некоторых случаях, кроме авторизации нужно специальное приглашение, так называемый инвайт, от авторизированного пользователя. В некоторых случаях вообще реализуется идея F2F (friend-to-friend- от «друга к другу») одноранговых закрытых сетей с ограниченным кругом пользователей, в основном, известных друг другу. Проникновение в подобную сеть без получения оперативным или иным путем связки логин-пароль (имя-пароль) либо приглашения, крайне затруднено в связи с новинками разработок криптостойкости сетей.

Во многих случаях используются частично централизованные сети, имеющий общий сервер, хаб, на которых обрабатываются запросы пользователя на поиск определенной информации, и соответственно оставляют электронные следы. Конечно, эти следы могут помочь идентифицировать пользователей, осуществляющих поиск «пиратской» (используемой с нарушением имущественных прав владельца авторских прав) экстремистской, террористической, порнографической (в первую очередь- детской порнографии) и иной, ограниченной в распространении информации. Однако эти серверы могут располагаться за пределами Российской Федерации, что осложнит оперативность получения информации по международным запросам, либо вообще сделает ее невозможным.

Отдельного рассмотрения заслуживает распределенное хранение информации в системе блокчейн. Как отмечал изобретатель биткоина Сатоши Накомото

относительно технологии блокчейн: «Система работает по следующим правилам:

1 Новые транзакции рассылаются всем узлам.

2 Каждый узел объединяет пришедшие транзакции в блок.

3 Каждый узел пытается подобрать хэш блока, удовлетворяющий текущей сложности.

4 Как только такой хэш найден, этот блок отправляется в сеть.

5 Узлы принимают этот блок, только если все транзакции в нем корректны и не используют уже потраченные средства.

6 Свое согласие с новыми данными узлы выражают, начиная работу над следующим блоком и используя хэш предыдущего в качестве новых исходных данных»[1].

Многими зарубежными учеными отмечалось, что «Киберпреступники и террористы активно используют блокчейн-технологии совместно с специализированным программным обеспечением The Onion Router (TOR), представляющим собой систему прокси-серверов, позволяющих тайно входить в Интернет, сохранять анонимность при посещении сайтов, обмене мгновенными сообщениями, работе с приложениями»[2]. С ними вполне можно согласиться. Использование технологии блокчейн делает практически невозможным взлом информации «извне», без внедрения в круг пользователей или использования помощи пользователя, поскольку криптостойкость блокчейна на настоящий момент практически неоспорима. Как отметил В.А. Петров: «видя весь блокчейн и ключи, любой пользователь может проверить корректность любых данных, в том числе: верна ли последовательность блоков, не пропущен ли блок, не вставлен ли в середину цепи новый блок, соответствие ключей блока хранимым в нем данным, то есть убедится в отсутствии ложных сведений»[3].

Существенный объем незаконного оборота финансовых средств в компьютерных сетях сейчас осуществляется с использованием криптовалют. Однако использование технологии блокчейн не дает возможность отслеживать трансакции. Конечно, как указывают некоторые авторы, можно попытаться «отследить, по какому IP-адресу инициируется транзакция и прочитать всю информацию о транзакции»[4]. Однако, нам представляется, что данный автор преувеличивает

---

[1] Накамото Сатоши. Биткоин: цифровая пиринговая наличность (2009) / перевод // Coinspot: сайт. 21 декабря2013 г. // URL: http://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/ (дата обращения 06.12.2020).

[2] Malik N. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It//URL:https://www.google. ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism (дата обращения:06.12.2020).

[3] Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учеб.-методич. пособие. —М.: Юрлитинформ, 2017 С 70.

[4] Кирков А.Н. Проблемы перед экспертизой электронных денежных средств и криптовалюты// Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019 С.72.

возможности перехвата и расшифровки указанной информации, да и идентифицировать конкретных пользователей, осуществивших транзакции, при этом вряд ли удастся. А ведь как отмечалось Е.И. Галяшиной «требуется пошаговое документирование идентификационных свойств файла с целью установления всей «цепочки законных владений»[1].

Таким образом, нам представляется необходимым определить криминалистическое исследование систем распределенного хранения электронных данных в качестве одного из актуальных, наиболее важных и перспективных направлений развития соответствующей части электронной цифровой криминалистики[2].

Список использованных источников

1. Malik N. How Criminals And Terrorists Use Cryptocurrency: And How To Stop It//URL:https://www.google. ru/search?ie=UTF-8&hl=ru&q=blockchain%20against%20cyberterrorism%20and%20cyber-extremism (дата обращения:06.12.2020)
2. Галяшина Е.И. Оценка достоверности цифровых фонограмм в уголовном процессе – доказывание и принятие решений в современном уголовном судопроизводстве // Материалы международной научно-практической конференции, посвященной памяти доктора юрид. наук, профессора П. А. Лупинской: сборник научных трудов.- М, 2011 С. 131-142.
3. Кирков А.Н. Проблемы перед экспертизой электронных денежных средств и криптовалюты// Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019 С.72
4. Накамото Сатоши. Биткоин: цифровая пиринговая наличность (2009) / перевод // Coinspot: сайт. 21 декабря2013 г. // URL: http://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/ (дата обращения 06.12.2020)
5. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учеб.-методич. пособие. —М.: Юрлитинформ, 2017. 197 с.

[1] Галяшина Е.И. Оценка достоверности цифровых фонограмм в уголовном процессе – доказывание и принятие решений в современном уголовном судопроизводстве // Материалы международной научно-практической конференции, посвященной памяти доктора юрид. наук, профессора П. А. Лупинской: сборник научных трудов.- М, 2011 С. 132.

[2] В предыдущих публикациях мы уже обосновывали наименование частной теории именно электронной цифровой криминалистикой См: Смушкин А.Б. К вопросу О наименовании теории «Электронная цифровая криминалистика»//Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 1 (13). С.15-21, а так же Смушкин А.Б. Объект и предмет электронной цифровой криминалистики//Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 года) / под ред.Д. В. Бахтеева. — Екатеринбург: Уральский государственный юридический университет. — 2020. С. 530-541.

6. Смушкин А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика»//Проблемы уголовного процесса, криминалистики и судебной экспертизы. 2019. № 1 (13). С.15-21,
7. Смушкин А.Б. Криминалистическое исследование и использование технологий распределенного хранения данных в Кн.: Проблемы и вызовы цифрового общества: тенденции развития правового регулирования цифровых трансформаций : коллективная монография в 2 т. / под ред. Н.Н. Ковалёвой ; ФГБОУ ВО «Саратовская государственная юридическая академия». – Саратов: Изд-во ФГБОУ ВО «Саратовская государственная юридическая академия», 2020. Т.1.- 2020. 456 с.
8. Смушкин А.Б. Объект и предмет электронной цифровой криминалистики//Технологии XXI века в юриспруденции: материалы Второй международной научно-практической конференции (Екатеринбург, 22 мая 2020 года) / под ред.Д. В. Бахтеева. — Екатеринбург: Уральский государственный юридический университет. — 2020. С. 530-541.;

М.Г. Терехов

Противодействие трансграничным схемам наркорасчетов и легализации наркодоходов с использованием современных платежных инструментов

Аннотация. В современных условия интеграции цифровых технологий в повседневную жизнедеятельность, наибольшую популярность для цифровой среды приобретает признак децентрализации. Наиболее ярким представителем цифровой среды с признаком децентрализации остается по настоящее время – криптовалюта[1]. Проблема децентрализации и безналичного расчета цифровыми активами в настоящее время является наиболее актуальной темой для научной дискуссии, а также практического апробирования методик предупреждения, пресечения и расследования преступлений совершаемых с использованием современных цифровых технологий.

Ключевые слова: криптовалюта, наркотические средства, легализация (отмывание), транзакция, трансграничность, цифровые активы, стейблкоин.

В настоящее время большой популярностью и спросом у граждан Центральной Европы пользуется цифровое пространство (сеть-интернет). Достоинствами цифровой среды являются: удаленный (дистанционный) способ рыночных отношений (простота удаленной оплаты товаров, услуг, а также их продажа), доступность, простота эксплуатации, возможность децентрализации данных взаимоотношений между пользователями интернета с помощью специализированных

[1] Криптовалюта - выступает средством безналичного расчета в большинстве интернет-сервисов закрытого интернет - браузера «TOR» именуемого среди пользователей как «Даркнет», характерным признаком которого являются сервисы VPN-соединение. Учитывая простоту, защищенность (анонимность) и практичность использования криптовалют, как финансового инструмента, криптовалюта часто является практичным, современным средством легализации (отмывания) денежных средств, полученных преступным путем, либо средством безналичного расчета при незаконном обороте наркотических средств.

сервисов[1]. Процессы криминализации интернета происходящие, как в открытом, так и в закрытом (Даркнет и иные сервисы с VPN соединением) интернете согласно ежегодного отчета Европола "Оценка угроз организованной преступности в интернете" (IOCTA 2019) набирают большую популярность, приобретают свойства стабильности по критерию использования цифровых активов (таких как криптовалюта) в преступных целях[2].

Из данного отчета, следует сделать вывод о том, что отчеты, связанные с аналитической работой правоохранительных подразделений Европейских стран отсылают на трансграничный характер преступлений совершаемых взаимосвязано также на территории стран Прибалтики, стран СНГ и на территории Российской Федерации, но при этом отсутствуют конкретные статистические показатели по данной проблематике. Следовательно, возникает необходимость анализа статистических данных в практических подразделениях МВД России, по лицам, привлекаемым к административной и уголовной ответственности за незаконный оборот наркотических средств на предмет интеграции с цифровым пространством, а также высокими технологиями, с помощью которых производится безналичный расчет криптовалютами на территории Российской Федерации и СНГ.

Анализ статистических данных указывает на беспрецедентное преобладание использования цифровых технологий при совершении преступлений. Преступления, связанные с незаконным оборотом наркотических средств в цифровой среде, показывают устойчивую тенденцию к развитию[3].

При комплексной научно-исследовательской работе построенной на общеруководящих принципах анализа экосистемы механизмов преступной деятельности с использованием цифровых активов и сервисов предоставляемых при работе с последними в рамках форума «WayAway» работающего на платформе закрытого интернет-браузера «Даркнета». Прослеживается, что с каждым годом процесс использования криптовалютных активов становиться более изощрённым.

Яркий пример таких процессов, это интернет-сервисы, являющиеся цифровыми финансовыми инструментами на примере «криптовалютных миксеров» под которыми понимается, что - это один из новых способов находящийся в открытом доступе с помощью которого представляется возможным цифровой актив, как криптовалюта и стейблкоины – скрыть (придать анонимность транзакциям). Происходит данный процесс путем смешивания с различными другими криптовалютными активами, поступающими на сервис от других пользователей, исходя чего криптовалюта смешивается путем множества транзакций и разбития определенной суммы вводимой в сервис криптовалюты на части, последствием чего является возврат «чистой криптовалюты» пользователю сервиса.

---

[1] Тумаков А.В., Терехов М.Г. Создание финансовых пирамид с использованием цифровых активов // Вестник экономической безопасности. 2020. №3. URL: https://cyberleninka.ru/article/n/sozdanie-finansovyh-piramid-s-ispolzovaniem-tsifrovyh-aktivov (дата обращения: 04.10.2020).

[2] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019., С.19-35.

[3] Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (Дата обращения: 04.10.2020).

Данные сервисы начинают использовать, перед преступными транзакциями, появляются способы удержания сомнительных криптовалютных активов в качестве сбережений длительный период времени на холодном хранении с помощью офлайн кошельков[1], в качестве инвестиционного вклада путем перевода в стейблкоины (такие как токен Tether).

Исходя из этого, следует сделать вывод о том, что криптовалюта является сложным финансовым инструментом с большим функционалом. Данный финансовый инструмент может быть преобразован при необходимости в цифровой финансовый актив используя в зависимости от умысла применения. Не теряя при этом функциональных возможностей интегрироваться с интернет-сервисами выступающими вспомогательным элементом для оборота цифровых активов, что представляет обширные возможности для его использования.

Сущность совершения противозаконных действий в цифровой среде в настоящее время ориентируется на основные свойства цифровых технологий, - это децентрализация, чему удовлетворяет криптовалюта и иные сопутствующие интернет-сервисы.

Свойства децентрализации в настоящее время представляются самыми проблемными с точки зрения установления принадлежности транзакции тому или иному элементу взаимоотношений в рамках сделки (транзакция из точки «А» в точку «Б»). Помимо этого, также создание теневой экономики в рамках легализации (отмывания) денежных средств полученных преступных путем в цифровом пространстве взаиморазвивается благодаря принципам децентрализации.

Безусловно, одним из действенных практических способов выявления преступных транзакций правоохранительными органами в рамках расследований и оперативно-розыскной деятельности по настоящий момент остается метод аналитики и кластеризации информации в рамках группировки транзакций. Для выявления схемы преступной транзакции в рамках любого противоправного действия с использованием криптовалют следует выделять два типа информации связанной с криптовалютными транзакциями:

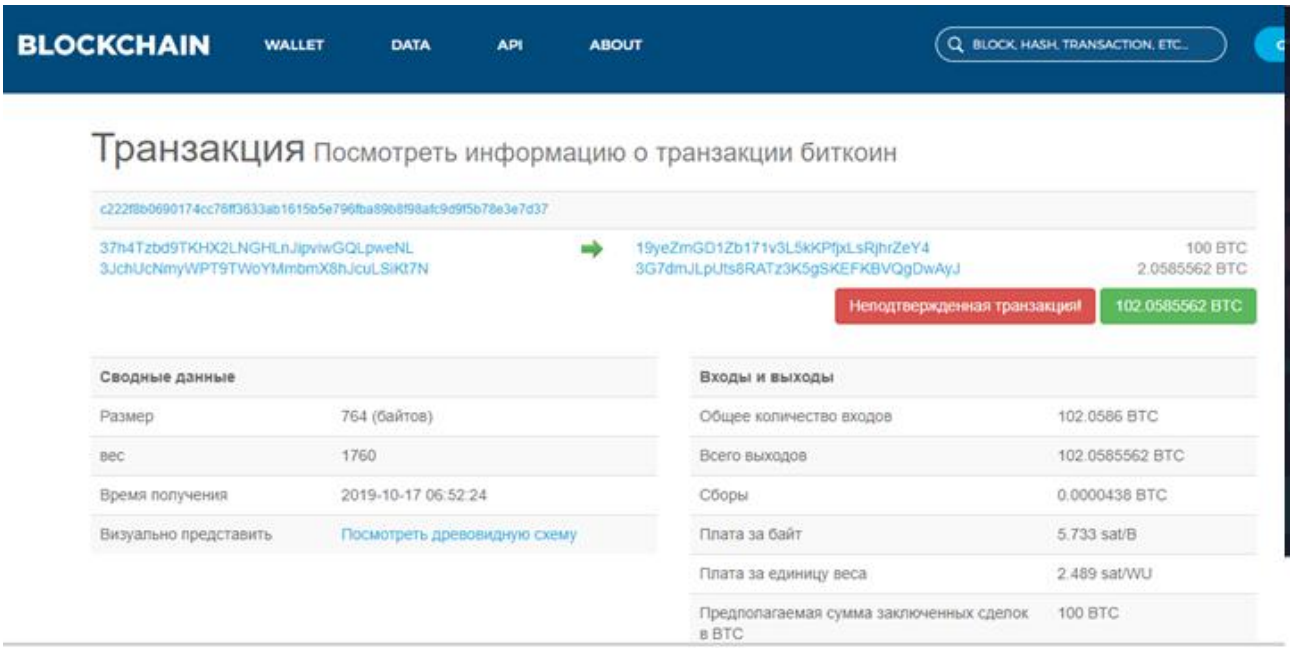
1. Общая информация находящаяся в общем доступе, где путем методики анализа представляется возможным выявить подозрительную транзакцию и придать сумме криптовалютного актива по данной транзакции статус подозрительной – проводить последующие оперативные проверочные мероприятия (схема № 1. Определение подозрительного статуса криптовалютных сделок по ряду запрашиваемых критериев в рамках методики анализа[2]).

---

[1] Сервисы, позволяющие в офлайн режиме (без доступа в интернет) хранить цифровые активы на персональных устройствах.

[2] Киптовалютная интернет – биржа с размещением URL: https://www.huobi.com/ru-ru/ (дата обращения 06.10.2020).

2. Конкретная информация по подозрительной транзакции имеющей признаки криминализированной, либо по транзакции которая является элементом преступной деятельности по возбужденному уголовному делу (Рисунок №1. Конкретная транзакция криптовалюты «Биткоин»).



Также в рамках анализа процессов связанных с криминальным использованием оборота цифровых активов в сети-интернет является, следует подвести итог, что в ходе проведения проверочных оперативных мероприятий правоохранительным органам следует проводить сложную систематизированную и индивидуальную аналитическую деятельность. Основные свойства данной работы заключаются в анализе путей следования криптовалюты от счета к счету, а также о сервисы (миксеры и т.д.) к которым потенциально может обращаться злоумышленник, чтобы ввести в заблуждение правоохранительные органы ведущие расследование, либо проверочные мероприятия по факту использования криптовалютного актива в преступных целях.

Во многом противодействие трансграничным схемам наркорасчетов и легализации наркодоходов должно начинаться со специализированной профессиональной подготовки сотрудников правоохранительных органов которые сталкиваются с противоправными действиями в которых присутствуют элементы цифровых технологий используемых через интернет.

Наиболее часто правоохранительные органы на территориальном уровне оказываются в затруднительном положении при работе с преступлениями, где объектом или орудием выступает криптовалюта, либо стейблкоин. Данные преступления требуют от сотрудника правоохранительных органов иметь соответствующий уровень квалификации в сфере цифровых преступлений, тщательную теоретическую подготовку понятийного аппарата элементов цифровых активов - криптовалют, иметь практическую составляющую с работой цифровых активов. Противоречие действительности и должного указывает на необходимость повышения квалификации сотрудников правоохранительных органов в сфере цифровых технологий использующихся в интернете злоумышленниками.

Список использованных источников

1. INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2019., С.19-35.
2. Киптовалютная интернет – биржа с размещением URL: https://www.huobi.com/ru-ru/ (дата обращения 06.10.2020).
3. Тумаков А.В., Терехов М.Г. Создание финансовых пирамид с использованием цифровых активов // Вестник экономической безопасности. 2020. №3. URL: https://cyberleninka.ru/article/n/sozdanie-finansovyh-piramid-s-ispolzovaniem-tsifrovyh-aktivov (дата обращения: 04.10.2020).
4. Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (Дата обращения: 04.10.2020).

А.Ю. Ушаков

Особенности производства обыска при расследовании преступлений, совершаемых с использованием современных электронных технологий

Аннотация. Рассмотрены отдельные положения, влияющие на производство обыска при расследовании преступлений, совершаемых с использованием современных электронных технологий. Пристальное внимание уделено подготовительному этапу производства обыска и объектам, подлежащим обнаружению и изъятию. Даны рекомендации по упаковке и транспортировке подлежащих изъятию объектов.

Ключевые слова: электронно-вычислительная техника, криптоконтейнер, облачное хранилище, энергонезависимые носители информации, Wi-Fi-роутер, протоколы работы (log-файлов).

Особой спецификой при расследовании преступлений, совершаемых с использованием современных электронных технологий обладает такое следственное действие как обыск. Именно от результата производства данного следственного действия в распоряжении правоохранительных органов появляются ключевые объекты и предметы, позволяющие в дальнейшем выстроить обвинительную или оправдательную линию в совершении преступлений, особенно совершаемых с использованием современных электронных технологий.

В современной практике очень мало внимания уделяется тактическим особенностям производства следственных действий и очень часто не обращается внимание на подготовительную сторону предстоящего действия.

Для производства обыска подготовительный этап является ключевым элементом, который влияет на итоговый результат.

При расследовании преступлений, совершаемых с использованием современных электронных технологий, на этапе подготовки к производству обыска необходимо:

– *запросить информацию о собственниках объекта недвижимости, где проживает лицо, причастность которого к совершению преступления установлена* органом дознания (сведения из подразделений по вопросам миграции, выписку из домовой книги, справку из домоуправляющей компании, справку от участкового уполномоченного, справку из БТИ или Росреестра, сведения от судебных приставов о возможных наложенных исполнительных мерах);

– *провести консультации со специалистами в области исследования компьютерной информации* и определить: целесообразность проведения предварительных оперативно-технических мероприятий по установлению местонахождения и функционального назначения электронно-вычислительной техники; способы изъятия компьютерной информации (копирование на собственные энергонезависимые носители информации, изъятие только электронно-вычислительной техники и пр.); перечень оборудования, необходимого для производства следственного действия; особенности тактики проведения следственного действия (последовательность осмотра помещений, необходимость осмотра электронно-вычислительной техники, особенности упаковки изъятого и пр.);

– *провести оперативное совещание с сотрудниками, которые будут принимать участие в проведении обыска*, в ходе которого довести тактику его проведения и в зависимости от конкретных обстоятельств разъяснить, что при производстве обыска рекомендуется установить все виды электронно-вычислительной техники, подлежащие изъятию; произвести изолирование всех участников обыска от доступа к электронно-вычислительной технике, подлежащей изъятию; составить схему расположения электронно-вычислительной техники в местах проведения обысков, провести фотографирование по правилам обзорной и узловой фотосъемки; осмотреть и скопировать информацию с включенной электронно-вычислительной техники в случаях, если установлено наличие на ней криптоконтейнеров и возможность доступа к облачным хранилищам; проверить соответствие текущей даты и времени с установленными датой и временем на подлежащей изъятию электронно-вычислительной технике; извлечь из электронно-вычислительной техники энергонезависимые носители информации

(флеш-накопители, карты памяти, оптические носители информации и т. п.). С целью исключения изъятия ненужных носителей информации осмотреть электронно-вычислительную технику неразрушающими методами, позволяющими блокировать запись информации на осматриваемом объекте и исключить непреднамеренное изменение следов картины обработки информации на осматриваемом объекте. При отсутствии возможности проводить на месте изъятия осмотр электронно-вычислительной техники лучше этого не делать во избежание признания полученных в ходе осмотра доказательств недопустимыми; при поступлении ходатайства собственников электронно-вычислительной техники или компьютерной информации и при наличии такой возможности создать посекторные копии или образы носителей информации, после чего скопировать их на предоставленный собственником энергонезависимый носитель информации и передать последнему[1];

– перед упаковкой и транспортировкой изъятая электронно-вычислительная техника должна быть выключена.

К производству данного следственного действия могут привлекаться сотрудники ЭКЦ, специализирующиеся на производстве компьютерных экспертиз или сотрудники Центра информационных технологий, связи и защиты информации (ЦИТС и ЗИ) ГУ МВД России по субъектам Российской Федерации. В исключительных случаях следует привлекать к участию в обысках иных лиц, имеющих основное или дополнительное образование в сфере информационных технологий. Таковыми могут являться:

– сотрудники оперативных подразделений (отдела «К» БСТМ субъекта Российской Федерации), но в этом случае необходимо будет исключить возможность их дальнейшего участия в производстве оперативно-разыскных мероприятий и отдельных следственных действий;

– сотрудники, которые по роду своей деятельности непосредственно связаны со сферой информационных технологий (например, сотрудники отделов, обеспечивающих образовательный процесс в образовательных организациях МВД России, и т. д.);

– специалисты сторонних организаций, которые также по роду своей деятельности непосредственно связаны со сферой информационных технологий[2].

Учитывая стрессовое состояние лиц, у которых проводится обыск, принять меры по добровольному получению от них паролей доступа к ресурсам электронно-вычислительной техники.

В ходе обыска обязательному изъятию, при необходимости либо по результатам консультации со специалистом, подлежат следующие предметы и документы: все виды электронно-вычислительной техники, позволяющей хранить

---

[1] Ушаков А. Ю. Практика расследования преступлений, совершенных с использованием криптовалюты: учебное пособие / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев. – Нижний Новгород: Нижегородская академия МВД России, 2020. – С. 42.

[2] Ушаков А. Ю. Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. Ю. Ушаков, А. М. Столповский. – Нижний Новгород : Нижегородская академия МВД России, 2019. – С. 24.

искомую информацию в цифровом виде на носителях, содержащихся в персональных компьютерах, ноутбуках, нетбуках, планшетных компьютерах, MP3-плеерах, диктофонах, цифровых фотоаппаратах, смартфонах, автомобильных регистраторах, системах видеорегистрации и т. д.

Обратить внимание на то, что устройства, оснащенные автономным питанием, для транспортировки и хранения целесообразно помещать в коробки, так как мягкая упаковка не защищает технику от несанкционированного включения.

При изъятии, упаковке и транспортировке избегать взаимодействия с магнитными полями, в том числе с магнитосодержащими средствами криминалистической техники (например, магнитных кисточек);

– все типы энергонезависимых носителей информации (накопители на жестких магнитных дисках (НЖМД), флеш-накопители);

– сетевые устройства различных видов (сетевые карты, концентраторы, коммутаторы, маршрутизаторы, беспроводные сетевые адаптеры, точки беспроводного доступа и пр.). Примечательно, что современные так называемые smart-телевизоры (от англ. *smart* – умный) оборудованы сетевой картой, позволяющей осуществлять доступ к сети «Интернет». Таким образом, при отсутствии целесообразности изъятия самого телевизора необходимо зафиксировать в протоколе следственного действия mac-адрес данного сетевого оборудования. Кроме того, в обязательном порядке с целью избежать повторного проведения обыска следует установить наличие и изъять сетевое оборудование беспроводного доступа (Wi-Fi-роутер), так как при последующем исследовании протоколов работы (log-файлов) в сети будет указан MAC-адрес беспроводного сетевого оборудования;

– средства мобильной связи, сим-карты, базы от сим-карт (пластиковая рамка, из которой извлекается сим-карта перед установкой), договоры на подключение услуг подвижной и стационарной радиочастотной связи. Примечательно, что, как правило, при производстве обысков базы от сим-карт не изымаются, хотя на них содержится ICCID – уникальный серийный номер сим-карты, по которому можно идентифицировать абонентский номер сим-карты. При имеющейся возможности средства мобильной связи перевести в авиарежим для исключения возможности их удаленного блокирования;

– документы, содержащие сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с использованием информационно-коммуникационных технологий;

– документы на приобретение движимого и недвижимого имущества (необходимы для последующего наложения ареста на данное имущество в порядке, предусмотренном статьей 115 УПК РФ, с целью обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий);

– свободные образцы почерка и подписи, содержащиеся в письмах, личных дневниках, рукописных договорах, записных книжках, и т. д.;

– похищенные денежные средства, приобретенные с их помощью товары, документы и предметы, свидетельствующие о месте хранения похищенных денежных средств и товаров (пластиковые карты, товарные и кассовые чеки, выписки

движения денежных средств по счетам, сберкнижки, ключи от камер хранения и банковских ячеек, квитанции о денежных переводах);

– фотографии, видеозаписи (особенно важно их изъятие при расследовании преступлений, совершенных организованными группами в целях доказывания наличия устойчивых межличностных связей между их участниками);

– средства криптографической защиты информации (аппаратные, программные, программно-аппаратные);

– иные предметы и документы, имеющие значение для доказывания.

Литература

1. Ушаков, А. Ю. Расследование преступлений, совершенных с использованием информационно-коммуникационных технологий / А. Ю. Ушаков, А. М. Столповский. – Нижний Новгород : Нижегородская академия МВД России, 2019. – 59 с. – Текст : непосредственный.
2. Ушаков, А. Ю. Практика расследования преступлений, совершенных с использованием криптовалюты: учебное пособие / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев. – Нижний Новгород: Нижегородская академия МВД России, 2020. – 54 с. – Текст : непосредственный.

В.Н. Цимбал

Особенности борьбы с преступлениями в сфере компьютерной информации: виды преступлений, способы совершения и методы противодействия

Аннотация. В статье рассматриваются некоторые особенности преступлений в сфере компьютерной информации, приводятся статистические данные, свидетельствующие о постоянном росте подобной разновидности противоправных деяний. Автором кратко анализируются способы их совершения и методы борьбы с компьютерными преступлениями на современном этапе.

Ключевые слова: преступление, компьютерная информация, киберпреступность, компьютерные преступления, информационные технологии.

Согласно статистическим данным Главного информационно-аналитического центра МВД России за 10 месяцев 2020 года зарегистрировано более 420 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 75,1 % больше, чем аналогичный период прошлого года.

Больше половины подобных преступлений относится к тяжким и особо тяжким – свыше 216 тысяч. Средства, при помощи которых они совершаются с ис-

пользованием и/или применением: сети Интернет (243,6 тыс.), средств мобильной связи (118 тыс.), компьютерной техники (23,8 тыс.), программных средств (8,2 тыс.), фиктивных электронных платежей (1 тыс.)[1].

Действующее уголовное законодательство Российской Федерации определяет преступления в сфере компьютерной информации в главе 28, а именно ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», а также помимо выше обозначенной главы к такого рода преступлениям относится ст. 159.6 «Мошенничество в сфере компьютерной информации».

Конвенция о преступности в сфере компьютерной информации ETS № 185 от 23.11.2001 г. предлагает государствам, подписавшим ее, рассматривать несколько групп таких преступлений: против конфиденциальности, целостности и доступности компьютерных данных и систем; связанные с использованием компьютерных средств; связанные с содержанием данных; связанные с нарушением авторского права и смежных прав[2].

Преступлений в сфере компьютерной информации, согласно указанным статистическим сведениям, за отчетный период всего зарегистрировано 4326. По отдельным статьям данные, следующие:

– ст. 159.6 УК РФ, зарегистрировано 615 преступлений (+4,2% по сравнению с АППГ), раскрыто всего 94;
– ст. 272 УК РФ, зарегистрировано 3369 преступлений (+71% АППГ), раскрыто всего 533;
– ст. 273 УК РФ, зарегистрировано 319 преступлений (-20,1% АППГ), раскрыто больше половины, а именно 172;
– ст. 274 УК РФ – сведения найти не удалось, подследственность ФСБ России.

Рассмотрим более подробно обозначенную категорию преступлений, основной отличительной чертой таких противоправных деяний является компьютерная информация, под которой в примечании к ст. 272 УК РФ понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[3].

Достаточно большое количество ученых (Т. Н. Богданова, В. М. Быков, В. Н. Черкасов, К. Е. Дёмин, Р. И. Дремлюга, А. А. Нагорный, В. А. Самсонов, А. И. Халиулин и др.[4]) изучало данное понятие. Глубокий анализ понятия «компьютерная информация» провел М. В. Старичков, который пришел к следующему

---

[1] Официальный сайт МВД России. Режим доступа: URL: https://мвд.рф/reports/item/21933965/Sb_2010.pdf (дата обращения: 01.12.2020).

[2] Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные проблемы права и отраслевых наук. – № 1 (3), 2017. – С. 13-14.

[3] Уголовный Кодекс РФ: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из СПС «Гарант».

[4] Богданова Т. Н. К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. – № 37 (291), 2012. –

выводу, что это «…зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначены для использования в таких устройствах»[1]. С данным мнением согласимся, так как обязательным условием совершения таких противоправных деяний и неотъемлемой его частью являются информационные технологии (компьютеры, средства связи и иное оборудование) и конечно же информация, обращаемая в них.

Способы совершения компьютерных преступлений, следующие:

а) кража носителя с компьютерной информацией или самого компьютера;

б) создание программ (компьютерные вирусы, сетевые черви, троянские программы), которые выполняют функции, причиняющие вред компьютерной информации (устройству и/или сети), например, хищение (удаление, модификация) данных, блокирование доступа, удаленное управление операционной системой или сетью, создание бот-сетей, распространение различной информации через зараженный компьютер, шифрование данных, их использование и распространение, и т. п.;

в) мошеннические действия;

г) перехват информации;

д) удаленный несанкционированный доступ;

е) удаленные (сетевые) атаки: DoS-атаки, анализ трафика, человек «по середине», IP-спуфинг, атаки на уровне приложений и т. д.

ж) комбинированные противоправные действия, в данном случае незаконные действия совершаются комплексно, например, осуществляется анализ трафика в сети, перехватываются логины/пароли и выполняется удаленный несанкционированный доступ.

Как видно из представленного, способов совершения преступлений большое количество, также не мало и орудий их реализации. Важными являются методы и применяемые при этом средства, для противодействия этим преступным деяниям, проведем некоторые параллели с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». Методы борьбы с компьютерными преступлениями можем определить, как технические, организационные (в

С. 64-67; Быков В. М., Черкасов В. Н. Понятие компьютерной информации как объекта преступления // Законность. – № 12 (950), 2013. – С. 37-40; Дёмин К. Е. О понятии «компьютерная информация» применительно к процессу доказывания // Вестник Московского университета МВД России. – № 1, 2019. – С. 44-47; Дремлюга Р. И. Понятие «компьютерная информация»: спорные вопросы в теории и законе // Библиотека уголовного права и криминологии. – № 1 (25), 2018. – С. 108-115; Нагорный А. А. Содержания понятия компьютерной информации как предмета компьютерных преступлений // Актуальные проблемы российского права. – № 8, 2014. – С. 1694-1698; Самсонов В. А. Понятие компьютерной информации и преступлений в сфере компьютерной информации // Деятельность правоохранительных органов в современных условиях. Материалы XVIII Международной научно-практической конференции, посвященной 20-летию образования Восточно-Сибирского институт МВД России. – Иркутск, 2013. – С. 107-109; Халиуллин А. И. Подходы к определению компьютерной преступности // Контуры глобальных трансформаций: политика, экономика, право. – Ч. 4. – № 6, 2011. – С. 16-23.

[1] Старичков М.В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. – № 1 (68), 2014. – С. 20.

ГОСТе это физический метод защиты), правовые и криптографические. На последнем пункте сильный акцент мы делать не будем, так как шифрование, как известно, является одним из самых эффективных способов защиты информации, при этом необходимо использовать соответствующее программное обеспечение (например, КриптоПРО, BitLocker, CryptoExpert 8, VeraCrypt и др.) и аппаратные устройства. Применение пользователем криптографической защиты информации, не позволит злоумышленнику использовать ее в собственных корыстных и иных целях. Рассмотрим остальные методы подробнее:

1. Технические, то есть обеспечение защищенности и безопасности компьютера или системы от возможного негативного воздействия при помощи различных программных и программно-технических средств, а также мер, направленных на обеспечение бесперебойной их работоспособности. Например, использование легального и актуального антивирусного программного обеспечения, шифрование защищаемой информации, применение межсетевых экранов, обновление операционных систем (программного обеспечения) и т. п.
2. Организационные, то есть обеспечение физической защищенности информации от получения ее злоумышленниками. Например, постоянное (своевременное, систематическое) обучение обычных пользователей, персонала предприятий (организаций) на предмет информационной безопасности, недопущение пренебрежения способами аутентификации/идентификации: логины, сложные пароли, иные методы аутентификации, сохранение их в тайне; информирование о новых видах угроз и способах их реализации; помещение защищаемой информации в надежные хранилища и т. д.
3. Правовые меры, то есть разработка норм, правил, инструкций, определяющих различные методы защиты информации, способы контроля эффективности ее защиты; определение ответственности за правонарушения. Обозначенная группа относительно эффективна: и действующее уголовное законодательство РФ, и международные документы, и участие РФ в деятельности международных организаций, которые в свою очередь уделяют большое внимание преступлениям в сфере компьютерной информации, киберпреступности и сотрудничеству государств в данной области.

Российской Федерацией признаются существующие проблемы в этой области и ведется следующая работа: в органах исполнительной власти созданы специальные подразделения (к примеру, Управление «К» МВД России[1]; Национальный координационный центр по компьютерным инцидентам, созданный ФСБ России[2]; отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий Следственного комитета России[3]) ведущие борьбу с компьютерными преступлениями; актуализируется законодательство РФ (к примеру,

---

[1] Официальный сайт МВД России. Режим доступа: URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 02.12.2020).

[2] Сайт СПС «Консультант Плюс». Режим доступа: URL: https://www.consultant.ru/law/hotdocs/54965.html/ (дата обращения: 02.12.2020).

[3] Официальный сайт Следственного комитета Российской Федерации. Режим доступа: URL: https://sledcom.ru/press/events/item/1481184/ (дата обращения: 02.12.2020).

в главу 28 УК РФ в 2017 году были внесены изменения, в Доктрине информационной безопасности РФ (указ Президента РФ от 05.12.2016 № 646) в разделе III, компьютерные преступления обозначены как один из видов угроз безопасности страны)); подготавливаются кадры для работы в данном направлении, в учебных заведениях вводятся специализированные дисциплины касающиеся рассматриваемой проблематики; на постоянной основе производится дополнительное обучение, переподготовка и повышение квалификации в области информационной безопасности сотрудников различных органов и организаций, а также иная деятельность.

Подводя итог рассмотренному, отметим, что количество совершенных преступлений в сфере компьютерной информации растет, о чем нам говорят приведенные статистические данные. Происходит это, как представляется, из-за бурного развития информационных технологий, их доступности как для обычного пользователя, так и для преступного элемента. Комплексность подходов по противодействию и борьбе с компьютерными преступлениями, актуализация законодательных норм, своевременный обмен опытом (информацией) на международном уровне, применение современных программных (технических, программно-технических) решений правоохранительными органами, а также минимизация возможного ущерба от противоправных действий залог успеха данной работы.

Список использованных источников

1. Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные проблемы права и отраслевых наук. – № 1 (3), 2017. – С. 11-16.
2. Официальный сайт МВД России. Режим доступа: URL: https://мвд.рф.
3. Официальный сайт Следственного комитета Российской Федерации. Режим доступа: URL: https://sledcom.ru.
4. Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. – № 1 (68), 2014. – С. 16-20.
5. Уголовный Кодекс РФ: федер. закон от 13.06.1996 № 63-ФЗ. Доступ из СПС «Гарант».

А.А. Чернопёров

Выявление и блокирование сайтов или страниц в социальных сетях как способ профилактики преступлений, совершаемых в сети Интернет

Аннотация. В статье на примере преступлений в отношении несовершеннолетних анализируется возможность использования технического блокирования пересылки информации о личной жизни несовершеннолетних, а также информации, способной причинить вред их психическому здоровью, как способа профилактики совершения преступлений против жизни, здоровья, половой свободы и половой неприкосновенности

несовершеннолетних. Вносятся предложения по недопущению распространения в сети Интернет запрещённой информации, в частности порнографических изображений несовершеннолетних, информации о способах совершения суицида, другой подобной информации.

Ключевые слова: Интернет, большие данные, искусственный интеллект, преступление, профилактика, блокировка, несовершеннолетние, дети, опасная информация.

Информационная среда занимает всё более значительное место в жизни современного человека. В последние годы вместе с развитием телекоммуникационных технологий, увеличения скорости обмена данных, повышения доступности сети Интернет всё больше активностей человека переходит в так называемый «виртуальный» формат. Пандемия KOVID-2019 способствовала ускорению обозначенного процесса.

Преступность, как неотъемлемая составляющая любого социума, активно внедряется и в дистанционные отношения между людьми.

Наибольшую опасность для общества представляют преступления, совершаемые в отношении несовершеннолетних, как наиболее ценной и, одновременно наименее защищённой группы населения.

Только недавно, благодаря скоординированным усилиям правоохранительных органов удалось пресечь хорошо организованную деятельность так называемых «групп смерти», создававшихся с целью побуждения несовершеннолетних к совершению суицидов (например, «Синий кит»). Не менее опасным, ломающим психику и судьбы детей является склонение их к совершению действий сексуального характера, их вовлечение в изготовление порнографической продукции.

На фоне некоторого снижения общего количества совершаемых преступлений растёт доля преступлений, совершаемых в отношении несовершеннолетних с использованием сети Интернет. Обоснованность данного утверждения наглядно доказывают практика работы следственного управления Следственного комитета Российской Федерации по Хабаровскому краю и Еврейской автономной области и статистика МВД Российской Федерации за прошедшие три года. Так, если в 2017 году на территории Еврейской автономной области и Хабаровского края совершено 3 таких преступления, в 2018 году было зарегистрировано 5 преступлений в отношении несовершеннолетних, то за 12 месяцев 2019 года их уже было 28. Как видим, прирост преступлений происходит в геометрической прогрессии, что явно указывает на необходимость принятия срочных мер по противодействию таким преступлениям. Анализ ситуации содержится в статье сотрудника Центра цивилизационных и региональных исследований РАН Кобзевой С.В[1]. На основе проведённого анализа автор пришла к выводу, что «… эпидемия, вызванная педофилией, коммерческой эксплуатацией детей и распространением детской порнографии в России, приобрела угрожающий характер и требует незамедлительного принятия комплексных мер, направленных на за-

[1] Кобзева С.В. Законодательные меры по борьбе с детской порнографией в Интернете: мировой опыт и российские реалии // Информационное право", 2009, № 2, С. 22-24.

щиту прав несовершеннолетних, которые должны быть направлены на усовершенствование законодательных норм и правоприменительной практики по борьбе с детской порнографией и другими формами сексуальной эксплуатации несовершеннолетних». С таким выводом сложно не согласиться. Российский законодатель также отреагировал на возникшую угрозу. С целью защиты несовершеннолетних от информации, которая может нанести вред их здоровью в декабре 2010 года был принят федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»[1]. В законе даны определения основных понятий, в частности, дано определение информации, причиняющей вред здоровью и развитию детей. За время действия указанного закона заинтересованными организациями разработаны механизмы выявления такой информации, проведения экспертизы информационной продукции, обладающей признаками вредной для детей. Но для противодействия такой информации мало возможности её выявлять и классифицировать, необходимы механизмы борьбы с её распространением.

Профилактика является одной из самых действенных мер. Кобзева С.В. верно определила распространение детской порнографии в сети Интернет как эпидемию. Соответственно, возможно применять медицинскую терминологию. Как говорил Гиппократ: «Facilius est morbos evitare, quam eos curare» - любую болезнь проще предотвратить, чем лечить. Одним из отличий преступлений, совершаемых в сети Интернет является то, что с момента размещения контента на общедоступном ресурсе происходит его немедленное непрерывное распространение. Спустя сутки информация устаревает и перестаёт интересовать пользователей. Таким образом, существующие сегодня пути блокировки доступа к данным, распространение которых незаконно, являются неэффективными. Федеральный закон «Об информации, информационных технологиях и о защите информации[2]» описывает механизм блокировки ресурсов, содержащих незаконный контент. Блокировка производится путём включения в Единый реестр доменных имён, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено, по решению суда или решению уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти. С момента выявления противоправного контента до момента принятия судом решения о блокировании соответствующего ресурса проходят, в лучшем случае, дни. За это время данные копируются многими пользователями, могут быть размещены на других страницах или сайтах.

В ходе осуществления своей деятельности следственные органы и органы полиции могут получать информацию, в том числе, и о распространении в сети Интернет запрещённой информации.

---

[1] Федеральный закон от 29.12.2010 436-ФЗ (ред. от 31.07.2020) «О защите детей от информации, причиняющей вред их здоровью и развитию» //СЗ РФ. 2011. № 1.Ст. 48.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации» //СЗ РФ. 2006. № 31.Ч. 1. С. 3448.

Источниками получения таких сведений являются:

-потерпевшие или законные представители потерпевших;

-представители средств массовой информации, общественных организаций;

-должностные лица системы образования;

-иные органы и физические лица.

Также подобного рода информация может быть получена в ходе производства следственных действий и оперативно-разыскных мероприятий по фактам совершения других преступлений, в ходе осуществления уполномоченными лицами мониторинга сети Интернет.

Для выявления запрещённого контента могут быть применены разработанные и эффективно применяемые в маркетинге технологии на основе нейронных сетей и искусственного интеллекта. Алгоритмы нейронных сетей, используемые искусственным интеллектом для определения профилей потребителей, выработки персонализированных рекомендаций, могут быть адаптированы для работы в социальных сетях.

Видится два направления анализа трафика: со стороны преступника и со стороны жертв. Как известно из практики расследования преступлений указанной категории, лица, совершающие противоправные действия в отношении несовершеннолетних, как правило, действуют стереотипно. Они создают множество фиктивных «фейковых» аккаунтов, в том числе, от имени несовершеннолетних, чтобы упростить процесс установления доверительных отношений с детьми. Запросы и предложения об обмене фотографиями и виде интимного плана рассылаемые с таких аккаунтов многим несовершеннолетним носят типовой характер, соответственно, могут быть отслежены (при этом не требуется вторгаться в содержание переписок, так как достаточно проанализировать размеры и исходящие IP). При выявлении подозрительной активности может быть сформирован «цифровой портрет» отправителя в виде всего объёма активности в глобальной сети, выявлены связанные профили социальных сетей, номера телефонов, адреса электронной почты, сетевые адреса и места подключения к беспроводной сети.

Со стороны потерпевших также может быть проанализирован трафик, в котором выявлены «нетипичные» для ребёнка контакты (из других регионов, с лицами, значительно старше и не имеющих общих связей).

На следующем этапе аномалии со стороны потерпевших могут быть сопоставлены в автоматическом режиме с аномалиями со стороны агрессоров, совпадения с высоким процентом вероятности противоправной активности могут быть проанализированы оператором, после чего приняты меры к блокированию опасной активности.

Для эффективной профилактической работы должен быть создан механизм, позволяющий уполномоченным лицам сразу после фиксации факта противоправной активности, размещения в общем доступе вредной информации, производить её блокирование, а также блокирование пользователей, занимающихся противоправной деятельностью.

Необходимы механизмы, позволяющие:

1. предотвратить факт пересылки незаконного контента, с использованием программных средств;
2. незамедлительно блокировать доступ к незаконному контенту, путём блокировки отдельных разделов или целых сайтов в сети Интернет, страниц пользователей в социальных сетях;
3. выявлять и документировать факты систематического распространения такой информации путём автоматизированного анализа по ключевым кадрам.

От владельцев операторов мобильной связи, Интернет-провайдеров, администраторов социальных сетей требуется принятие мер по внедрению программных средств, которые в автоматическом режиме распознавали бы запрещённую информацию (в частности – изображения, содержащие обнажённое тело малолетних) и не допускали бы их распространение. Также необходим работающий механизм оперативного реагирования на запросы и решения органов государства о блокировании конкретных пользователей, сайтов, страниц в социальных сетях с целью недопущения распространения запрещённых данных.

Предлагается рассмотреть вопрос о наделении следователей и сотрудников соответствующих оперативных подразделений системы МВД Российской Федерации правом принимать решения о блокировании конкретных ресурсов в сети Интернет, на которых в ходе проведения оперативно-разыскных мероприятий или следственных действий было обнаружено незаконное содержимое. Постановление следователя или начальника органа, осуществляющего оперативно-разыскную деятельность, должно направляться непосредственно оператору автоматизированной системы «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». Оператор безотлагательно исполняет содержащееся в постановлении решение. Законность таких решений, безусловно, должна проверяться судом, но уже после блокировки, по аналогии с проверкой решения следователя о проведении обыска в жилище в случаях, не терпящих отлагательства. В случае, признания решения о блокировке необоснованным, оператор реестра исключит соответствующий ресурс из списка запрещённых.

Вновь возвращаясь к аналогии с лечением инфекции, остановить лавинообразный рост числа преступлений указанной категории возможно только предотвратив размещение запрещённого контента в сети Интернет. Если ребёнок не сможет отправить свои фотографии и видеозаписи, содержащие изображение обнажённого тела, у преступника не будет мотивации вступать с ним в контакт, развращать или запугивать. Блокировка ресурсов, содержащих детскую порнографию хотя бы на территории Российской Федерации, лишит их владельцев возможности зарабатывать, что также сократит объём распространяемой информации.

А.А. Чугунов
Е.Р. Власенко

Использование кибертехнологий как способ совершения посягательств на интересы личности, охраняемые уголовным законом

Аннотация. В статье рассматриваются понятие киберпреступлений и их виды. Авторами осуществлен анализ действующего уголовного законодательства в части, относящейся к посягательствам в изучаемой сфере. На основании исследования сделан вывод о необходимости дополнения отдельных составов преступлений седьмого раздела УК РФ квалифицирующим признаком совершения преступного деяния с использованием современных технологий.

Ключевые слова: киберпреступления, киберпространство, кибертехнологии, способ совершения преступления, преступления против личности.

Современное общество невозможно представить без использования цифровых и сетевых технологий. Посредством информационного пространства совершается все больше операций во всех сферах жизнедеятельности: социальной, экономической, политической и духовной. Особую актуальность приобрело использование электронных средств коммуникации. Киберпространство помогает злоумышленникам самоорганизоваться, так как выступает удобным средством связи для ведения их «дел», а также служит условием трансформации традиционных и появления новых посягательств. Изучение киберпространства представляет определенный научный интерес, ведь преступления, совершаемые с использованием информационно-телекоммуникационных сетей, имеют высокий уровень общественной опасности из-за своего глобального характера и требуют тщательного изучения для разработки моделей противодействия им.

Правовая борьба с киберпреступностью может осуществляться путем применения существующих законов, охватывающих правонарушения, совершаемые и без новых технологий, внесения в них соответствующих поправок, а также создания специальных нормативно-правовых актов, регулирующих отношения в данной сфере.

Однако действующие законы могут быть неприменимы к киберпреступлениям ввиду того, что были созданы до изобретения Интернета и цифровых технологий или без учета их влияния на охраняемые общественные отношения.

Большинство стран предпочли внесение поправок в национальное, в том числе уголовное, законодательство принятию специальных нормативных документов в рассматриваемой сфере, дополнив существующие законы положениями, касающимися преступных деяний в сфере компьютерных технологий. К числу таких государств относится и Российская Федерация.

Под *киберпреступлениями* в России понимают группу общественно опасных деяний в сфере компьютерной информации, предусмотренных главой 28 УК РФ. Однако такой подход не в полной мере отражает содержание данного понятия. В переводе с английского “*cyber*” означает «виртуальный, связанный с инфор-

мационными технологиями»[1]. Фактически, характер киберпреступления зависит от уровня задействованных цифровых и сетевых технологий, образа действий преступников. По нашему мнению, киберпреступления – понятие более широкое. Оно включает в себя как посягательства на установленный порядок обращения и защиты компьютерной информации и информационных ресурсов, так и преступления, посягающие на другие объекты уголовно-правовой охраны с использованием возможностей киберпространства и его технологий. Схожей позиции придерживаются и сотрудники Управления Организации Объединенных Наций по наркотикам и преступности, которые в части определения киберпреступлений делят их на кибернезависимые (те, которые существовали и без киберпространства) и резко контрастирующие с ними киберзависимые (те, совершение которых невозможно в отсутствие соответствующих технологий)[2]. Последние представляют собой деяния, совершение которых отечественный законодатель запрещает под угрозой наказания в упомянутой главе Уголовного кодекса.

Отсутствие универсального понятия киберпреступлений, а также общепринятых определений видов и категорий киберпреступлений затрудняет правоприменение.

Специалисты указанного управления выделяют три группы компьютерных преступлений: «преступления против машины», «преступления с использованием машины» и «преступления в машине»[3]. Первая включает преступления против конфиденциальности, целостности и доступности компьютерных данных или систем, например, неправомерное использование компьютеров хакерами. Ответственность именно за эти преступления отечественный законодатель закрепил в главе «Преступления в сфере компьютерной информации». Вторая группа включает традиционные виды преступлений, таких как мошенничество или незаконные азартные игры, которые благодаря использованию цифровых и сетевых технологий приобретают глобальный охват, а в отсутствие сети «Интернет» имеют локальный характер. Преступления, включенные в третью группу, связаны с незаконным контентом. В части данных преступных деяний в зарубежной практике нет согласия об общем подходе к их криминализации. Где-то подобные действия признаются законными, где-то – уголовно наказуемыми. В различных странах в эту категорию входит размещение в сети материалов сексуального, ненавистнического, террористического характера, обнародование ложной информации и пр.

---

[1] Кембриджский англо-русский словарь // Cambridge University Press – URL: https://dictionary.cambridge.org/ru/словарь/англо-русский/cyber?q=cyber- (дата обращения: 15.12.2020).

[2] Серия университетских модулей Управления ООН по наркотикам и преступности //E4J University module series: Cybercrime / Module 13: Cyber organised crime / Cyber organised crime: What is it? – URL: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html (дата обращения: 15.12.2020).

[3] Проект доклада Управления ООН по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности». Объединенные нации. Февраль 2013 г. с. 16.

Ответственность за преступления из второй и третьей групп указанной классификации в УК РФ закреплена в виде квалифицированных составов существующих преступлений или в специальных нормах. В основном, это преступления, вызывающие повышенный общественный резонанс – преступления экономического характера (предусмотренные ч. 1 ст. 171.2, ст. 185.3, ч. 1 ст. 187 УК РФ), в т. ч. различные виды хищений в киберпространстве (п. «г» ч. 3 ст. 158, ст. 159.3, ст. 159.6 УК РФ), деяния экстремистской направленности (ч. 2 ст. 205.2, ч. 2 ст. 280, ч. 2 ст. 280.1, ч.ч. 1, 2 ст. 282 УК РФ), преступления, связанные со здоровьем населения (п. «б» ч. 2 ст. 228.1, ч. 1.1 ст. 238.1 УК РФ), детской порнографией (п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2 УК РФ).

В настоящее время практически каждое преступление может быть совершено с использованием информационно-телекоммуникационных сетей из-за обширных возможностей современных технологий. Вследствие этого возникает вопрос, почему данный признак состава преступления, несомненно влияющий на уровень общественной опасности совершенного деяния, по нашему мнению, учтен законодателем далеко не везде, где необходимо. Например, в седьмом разделе УК РФ, посвященном преступлениям против личности, всего в 7 % составов предусмотрен анализируемый метод (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ст. 138.1, п. «в» ч. 2 ст. 151.2 УК РФ). Столь незначительное внимание, уделенное законодателем подобному способу совершения преступления, с нашей точки зрения, является пробелом в законодательстве и требует скорейшего устранения. Представляется, что использование возможностей современных технологий позволяет виновному совершать посягательства на жизнь и здоровье человека, а также причинять вред его чести и достоинству, конституционным правам и свободам.

Приведем актуальный в настоящее время пример использования сетевых технологий как способа убийства. Больной, находящийся на лечении в больнице, подключен к аппарату искусственной вентиляции легких. Жизнь этого человека зависит от стабильности работы упомянутого медицинского оборудования, так как работа легких не может обеспечить организм достаточным количеством кислорода, и аппарат ИВЛ выполняет эту функцию. Виновный посредством удаленного доступа блокирует подачу электроэнергии для конкретных приборов ИВЛ, вследствие чего циркуляция кислорода в организме больного прекращается и создается угроза наступления смерти человека. Принятие мер по спасению жизни врачами при этом не гарантирует отсутствие причинения определенного вреда здоровью потерпевшего. Внесение соответствующих изменений в ст.ст. 105, 111, 112, 115 УК РФ, включающих квалифицирующий признак, совершение преступления с использованием кибертехнологий, будет способствовать более эффективной защите охраняемых уголовным законом общественных отношений.

Активное распространение сейчас приобретает внедрение системы «умный дом». Автоматическое управление системами жизнеобеспечения облегчает быт и делает жилье более комфортным, но одновременно предоставляет преступникам шанс на совершение противоправных деяний, посягающих на права человека. В частности, неправомерное подключение к системе «умный дом» может

нарушать права на неприкосновенность частной жизни или жилища. Например, подключение к защитной системе видеонаблюдения, призванной обеспечивать безопасность в отсутствие владельца, может служить отличным способом слежки за хозяином в период его нахождения дома. А внесение изменений в интеллектуальную программу распознавания лиц, которая сама открывает двери в дом, когда узнает владельца, – легкий способ проникновения в жилище помимо воли проживающего там лица. Считаем необходимым дополнить ст. 137 и ст. 139 УК РФ указанным признаком, как квалифицирующим.

Подсчет голосов избирателей на выборах в большинстве субъектов РФ – процесс автоматический. Считаем возможным включение способа воздействия на автоматизированную систему подсчета голосов в целях искажения итогов голосования в диспозицию ст. 142.1 УК РФ для более эффективной защиты политических прав человека.

Следует отметить, что в ряде зарубежных стран (Австралия, Новая Зеландия, США, Австрия, Германия, Ямайка, Кения, ряд Африканских стран и др.), предусмотрена уголовная ответственность за деяния, предполагающие использование компьютера в целях причинения личного вреда человеку – домогательства, преследования, запугивания, угроз[1]. Изложенное свидетельствует о том, что иностранный законодатель учитывает подобный признак при конструировании составов преступлений, где основным непосредственным объектом является личность.

Киберпреступность включает в себя как «новые» общественно опасные деяния, выделенные российским законодателем в отдельную главу Уголовного кодекса, совершение которых возможно только в связи с существованием информационно-телекоммуникационных технологий, так и «традиционные» преступления, совершение которых облегчает использование таких технологий. Киберпространство является неотъемлемой частью современного мира, делающей существование человека более комфортным, но в то же время дающей виновным широкие возможности для совершения различных преступлений.

Для систематизации отечественного уголовного законодательства и дифференциации ответственности за преступления, совершенные с использованием информационно-коммуникационных технологий, считаем необходимым включить анализируемый признак в квалифицированные составы преступлений против личности.

Список использованных источников

1. Кембриджский англо-русский словарь // Cambridge University Press – URL: https://dictionary.cambridge.org/ru/словарь/англо-русский/cyber?q=cyber- (дата обращения: 15.12.2020).

[1] Серия университетсикх модулей Управления ООН по наркотикам и преступности // E4J University module series: Cybercrime / Module 2: General types of cybercrime / Computer-related offences – URL: https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html (дата обращения: 15.12.2020).

2. Проект доклада Управления ООН по наркотикам и преступности «Всестороннее исследование проблемы киберпреступности». Объединенные нации. Февраль 2013 г. с. 16.
3. Серия университетских модулей Управления ООН по наркотикам и преступности // E4J University module series: Cybercrime / Module 2: General types of cybercrime / Computer-related offences – URL: https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html (дата обращения: 15.12.2020).
4. Серия университетских модулей Управления ООН по наркотикам и преступности //E4J University module series: Cybercrime / Module 13: Cyber organised crime / Cyber organised crime: What is it? – URL: https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html (дата обращения: 15.12.2020).

А.В. Шахматов
А.А. Пальцев

К вопросу противодействия коррупционным преступлениям, совершаемым с использованием современных электронных технологий

Аннотация. В статье рассматриваются отдельные вопросы, возникающие в ходе осуществления правоохранительными органами Российской Федерации деятельности по противодействию коррупционным преступлениям, в том числе взяточничеству, совершаемым с использованием электронных технологий и возможностей информационно-телекоммуникационных сетей. Отдельное внимание уделяется используемым технологиям, а также проблемам межрегиональности и транснациональности преступной деятельности, в ходе которой используются современные электронные технологии.

Ключевые слова: противодействие коррупционным преступлениям, совершаемым с использованием электронных технологий, взяточничество, информационно-телекоммуникационная сеть, компьютерные средства, межрегиональная и транснациональная преступная деятельность.

Вопросы противодействия преступлениям, совершаемым с использованием электронных технологий и возможностей информационно-телекоммуникационных сетей, в современных условиях, когда происходит цифровизация практически всех аспектов жизни людей, приобретают всё большее значение.

Несмотря на то, что в Уголовном кодексе Российской Федерации[1], содержится определенное количество статей, предусматривающих ответственность за совершение преступлений в сфере компьютерной информации, нужно сказать, что возможность совершения преступных действий с той или иной степенью

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.10.2020) // СПС КонсультантПлюс.

использования информационно-телекоммуникационных сетей и электронных технологий, в настоящее время практически не ограничена.

Яркими примерами такого рода противоправных деяний являются преступления, совершаемые в сфере незаконного оборота наркотических средств, когда в информационно-телекоммуникационных сетях создаются интернет-магазины, с использованием которых осуществляется незаконная деятельность по распространению наркотиков[1].

Помимо этого, с помощью компьютерных и иных электронных технических средств совершаются многочисленные виды мошенничеств, взяточничество, а также торговля предметами, изъятыми из гражданского оборота и другие противоправные действия.

В 2020 году повсеместное осложнение санитарно-эпидемиологической обстановки, связанное с распространением новой коронавирусной инфекции, обусловило повышение активности в сфере использования дистанционных услуг и новейших технологий, в том числе применяемых для бесконтактного совершения тех или иных действий.

Данное обстоятельство, а также всё более активное вовлечение граждан в процессы использования бесконтактных электронных технологий, компьютерных и иных технических средств и возможностей информационно-телекоммуникационных сетей, в частности сети «Интернет», обусловило существенный рост количества преступлений в указанной сфере.

Так, в 2017 году количество преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий составило 90 587.

В 2018 году количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составило уже 174 674 (+ 92,8 %).

В 2019 году количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации составило 294 409 (+ 68,5 %), из них 142 728 тяжких и особо тяжких (+ 149 %), в том числе 157 636 преступлений (+ 45,4 %), совершенных с использованием информационно-телекоммуникационной сети «Интернет».

За 10 месяцев 2020 года зарегистрировано 420 662 преступления, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, из них 216 366 тяжких и особо тяжких (+ 84,9 %), в том числе 243 642 преступления (+ 92,9%), совершенных с использованием информационно-телекоммуникационной сети «Интернет»[2].

---

[1] Бесконтактный сбыт наркотических средств с использованием интернет-магазинов: актуальные вопросы / С.И. Земцова // Наркоконтроль. 2019. № 3. С. 17-22; Федоров А.В. Наркопреступность периода пандемии / А.В. Федоров // Наркоконтроль. 2020. № 3. С. 6 – 9; Халиуллина Л.Г. Криминальные киберуслуги участникам незаконного оборота наркотических средств и психотропных веществ / Л.Г. Халиуллина // Наркоконтроль. 2019. № 4. С. 23-25.

[2] МВД Российской Федерации [Электронный ресурс] URL: http://мвд.рф/folder/101762 (дата обращения 30.11.2020).

Наиболее опасным среди коррупционных преступлений по праву считается взяточничество, в ходе которого могут использоваться различные современные электронные технологии и противоправные схемы.

Например, осуществление взяткодателем бесконтактного перевода денег на счет в банке или кошелек какой-либо из разнообразных платежных систем и предоставление, с соблюдением мер конспирации, взяткополучателю информации необходимой для получения доступа к счету, передача взятки с использованием одного из многочисленных видов криптовалюты и так далее[1].

Так, в соответствии с приговором Люберецкого городского суда Московской области от 10.06.2020 по ч. 2 ст. 290, ч. 2 ст. 290, ч. 2 ст. 290 УК РФ осужден заместитель начальника управления транспорта, дорог и связи администрации городского округа, получивший взятки за общее покровительство деятельности коммерческой организации, в том числе в виде безналичного перечисления денег на счет используемой им банковской карты[2].

Следует отметить, что отдельные вопросы, связанные с бесконтактной передачей денег, в том числе зачисление с согласия должностного лица на указанный им счет или электронный кошелёк, как момент окончания преступления - взяточничества, нашли своё отражение в постановлении Пленума Верховного Суда Российской Федерации от 24.12.2019 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» и от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий»[3].

При этом, в современных условиях даже передача взятки в виде наличных денег, иного имущества в редких случаях обойдется без использования средств связи, а также имеющихся в информационно-телекоммуникационной сети «Интернет» мессенджеров, таких как «WatsApp», «Viber», «Signal», «Telegram», «Imo», «Wire», «Line», «WeChat» и других подобных программ.

Так, в соответствии с приговором Советского районного суда г. Брянска от 15.06.2020 по ч.6 ст.290 УК РФ осужден сотрудник органов внутренних дел, использовавший в ходе совершения преступления мессенджер «Telegram», посредством которого были достигнуты договоренности о получении им взятки

---

[1] Типичные способы дачи взятки с использованием средств сотовой связи и сети Интернет / Е.А. Пидусов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1 (5). С. 75-81.

[2] Судебные решения.рф [Электронный ресурс] URL: http://судебныерешения.рф/50899244/extended (дата обращения 04.12.2020).

[3] Постановление Пленума Верховного Суда Российской Федерации от 24.12.2019 № 59 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» и от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // СПС КонсультантПлюс.

за совершение незаконных действий, а именно: за незаконное прекращение уголовного преследования по уголовному делу[1].

Таким образом, вопросы эффективности противодействия преступлениям коррупционной направленности, совершаемым с использованием современных электронных технологий, в настоящее время выходят на первый план борьбы с преступностью.

Вместе с тем, в ходе осуществления деятельности по противодействию преступлениям, совершаемым с использованием возможностей информационно-телекоммуникационных сетей, в частности сети «Интернет», правоохранительные органы Российской Федерации сталкиваются с различными трудностями.

Наряду с иными, к таковым следует отнести использование в ходе осуществления противоправной деятельности различных современных технологий, например, TOR (многослойный маршрутизатор), VPN (виртуальная частная сеть), функции автоматического экстренного отключения от информационно-телекоммуникационной сети «Интернет» и других, а также криптовалют, характеризующихся отсутствием контроля за их оборотом со стороны государственных органов.

Применение в ходе совершения преступлений вышеуказанных технологий позволяет осуществить многоступенчатое шифрование передаваемых данных, выполнение соединений «поверх» информационно-телекоммуникационной сети «Интернет», обеспечить высокую степень анонимности пользователей и тем самым осложнить работу правоохранительных органов по установлению лиц причастных к их совершению.

К числу второй группы трудностей, возникающих в ходе осуществления правоохранительными органами Российской Федерации деятельности по противодействию коррупционным преступлениям, совершаемым с использованием возможностей информационно-телекоммуникационных сетей, необходимо отнести осложнения связанные с их межрегиональностью, а зачастую и транснациональностью.

Так, лица, осуществляющие администрирование тех или иных ресурсов, например, страницы в социальной сети, с использованием которой в г. Санкт-Петербурге совершается то или иное противоправное деяние, могут находиться на территории любого субъекта Российской Федерации.

Принимая во внимание ограниченные требованиями Уголовно-процессуального кодекса Российской Федерации [2] сроки проведения процессуальных проверок, своевременное выполнение необходимого комплекса проверочных мероприятий, включающего опрос лица, осуществляющего администрирование интернет - ресурса не всегда представляется возможным.

---

[1] Судебные решения.рф [Электронный ресурс] URL: http://судебныерешения.рф/51308377/extended (дата обращения 04.12.2020).

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.10.2020) // СПС КонсультантПлюс.

Помимо результативности процессуальных проверок, изложенное негативным образом влияет на сроки следствия по уголовным делам, производство по которым, безусловно, должно осуществляться в разумный срок.

Кроме того, в достаточной степени распространены случаи нахождения за пределами Российской Федерации лиц, использующих для совершения тех или иных преступлений возможности информационно-телекоммуникационных сетей.

В таких случаях, даже при условии преодоления в необходимой степени анонимности таких лиц, создаваемой с применением вышеуказанных технологий, получение необходимых для уголовного судопроизводства материалов возможно только в рамках процедур международно-правовой помощи, оказание которой, зачастую, занимает длительный срок.

Таким образом, вышеуказанные вопросы, возникающие в ходе осуществления правоохранительными органами Российской Федерации деятельности, направленной на противодействие преступлениям коррупционной направленности, совершаемым с использованием современных электронных технологий, требуют дальнейшей проработки и формулирования отвечающим современным условиям жизни ответов на них.

Представляется, что эффективным способом противодействия вышеуказанной преступной деятельности, осуществляемой с использованием такого рода технологий, является создание действенной возможности блокирования доступа пользователей к соответствующим интернет-ресурсам.

Принятие мер по ограничению доступа к ресурсам в информационно-телекоммуникационных сетях, в том числе в информационно-телекоммуникационной сети «Интернет» в Российской Федерации возложено на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)[1].

Однако, блокирование, осуществляемое в настоящее время Роскомнадзором, не позволяет в достаточной мере противостоять таким технологиям.

Данное обстоятельство обуславливает необходимость выработки новых подходов к техническим способам решения этого вопроса, в том числе с учетом опыта других государств, например, фильтрации содержимого в информационно-телекоммуникационной сети «Интернет», проводимой в Китайской Народной Республике, позволяющей прекращать доступ к интернет-ресурсам, с использованием которых совершаются преступления.

В части касающейся, вопросов межрегиональности преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, представляется, что необходимым условием противодействия им является следующее.

Дополнительно проработать и закрепить на законодательном уровне, в том числе процедуру документального оформления, а также возможность органов

---

[1] Постановление Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» // СПС КонсультантПлюс.

предварительного расследования осуществлять проверочные мероприятия и процессуальные действия с использованием информационно-телекоммуникационной сети «Интернет».

Например, по аналогии с проводимыми в судах действиями с участниками судебного производства, в частности, допросами свидетелей и иных лиц, законодательно закрепить соответствующие процедуры на стадии досудебного производства (в противном случае, то есть без законодательного закрепления, проводимые органами предварительного следствия процессуальные действия, могут быть результативно оспорены стороной защиты).

При этом, эффективное практическое применение таких возможностей требует адекватного складывающейся обстановке уровня технической и кадровой оснащенности следственных подразделений.

Одновременно с этим, транснациональный уровень использования возможностей информационно-телекоммуникационных сетей и электронных технологий, в ходе осуществления преступной деятельности, на сегодняшний день в очередной раз подчеркивает важность совместной работы правоохранительных органов различных государств по противодействию ей.

В связи с этим, инструменты в виде оперативного обмена информацией, в частности между органами, осуществляющими предварительное расследование, требуют дальнейшего совершенствования и выработки механизмов и решений, позволяющих дать адекватный ответ коррупционной преступности.

Список использованных источников

1. Земцова С.И. Бесконтактный сбыт наркотических средств с использованием интернет-магазинов: актуальные вопросы / С.И. Земцова // Наркоконтроль. 2019. № 3. С. 17-22.
2. Пидусов Е.А. Типичные способы дачи взятки с использованием средств сотовой связи и сети Интернет / Е.А. Пидусов // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1 (5). С. 75-81.
3. Постановление Пленума Верховного Суда Российской Федерации от 24.12.2019 № 59 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» и от 16.10.2009 № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» // СПС КонсультантПлюс.
4. Постановление Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 27.10.2020) // СПС КонсультантПлюс.

6. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 27.10.2020) // СПС КонсультантПлюс.
7. Федоров А.В. Наркопреступность периода пандемии / А.В. Федоров // Наркоконтроль. 2020. № 3. С. 6 – 9.
8. Халиуллина Л.Г. Криминальные киберуслуги участникам незаконного оборота наркотических средств и психотропных веществ / Л.Г. Халиуллина // Наркоконтроль. 2019. № 4. С. 23-25.

В.И. Шиян

Криминологические аспекты противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий

Аннотация. В статье представлены криминологические аспекты противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. Уделено внимание противоправному применению достижений технического прогресса в сфере экономики, общественной безопасности и общественного порядка, незаконного оборота наркотиков, общественной нравственности. Обозначены основные задачи и формы сотрудничества правоохранительных органов в борьбе с киберпреступностью.

Ключевые слова: противодействие, борьба, киберпреступления, киберпреступность, информационно-телекоммуникационные технологии, медиапространство.

Развитие науки и техники привело к масштабному использованию информационно-телекоммуникационных технологий (далее – ИТТ) во всех сферах жизнедеятельности общества, в том числе и криминальной.

Согласно официальным статистическим данным ФКУ «ГИАЦ МВД России» в последние годы отмечается последовательный рост абсолютных и относительных показателей преступлений, совершенных с использованием ИТТ (киберпреступлений). Так, если в 2018 году их доля в структуре всей преступности составляла 8,8%, то по итогам 2020 года – 25,0%. Как видим прирост к 2018 году составил 184,1%. Думается, что в немалой степени тенденция роста исследуемого вида преступлений обусловлена применением ограничительных мер, направленных на противодействие распространению коронавирусной инфекции COVID-19. Причем число зарегистрированных преступлений, совершенных в общественных местах и на улицах за этот период сократилось на 11,6%.

По справедливому замечанию А.Ж. Саркисян, в настоящее время неправомерные действия с использованием ИТТ возможны не только в сфере компьютерной информации[1]. В частности, посредством ИТТ совершаются преступления в сфере экономики: хищения денежных средств путем доступа к идентификаци-

[1] Саркисян А.Ж. Преступления в сфере информационно-коммуникационных технологий: понятия и особенности // Уголовное судопроизводство: проблемы теории и практики. 2020. № 1. С. 69-74.

онным данным сотрудников кредитных организаций; хищения и вымогательства денежных средств с помощью «банковских» вирусов; мошенничество с использованием электронных средств платежа; мошенничество в сфере компьютерной информации; легализация (отмывание) денежных средств и др.

Глобализация информационных процессов обусловила появление новых форм терроризма и экстремизма – кибертерроризма и киберэкстремизма[1].

Лица, участвующие в террористической деятельности, перешли на общение друг с другом под прикрытием игроков сетевых компьютерных игр. Многообразие сценариев данных игр позволяет осуществлять координацию действий, устанавливать контакты и репетировать возможные атаки на виртуальных моделях[2].

Широко применяются достижения технического прогресса и в сфере незаконного оборота наркотиков. Особенно популярным становится сбыт наркотиков бесконтактным способом с использованием сети Интернет, а также электронных платежных систем, что позволяет обеспечить анонимность соединений с серверов и создавать скрытые ресурсы на псевдодоменах. Согласно данным проведенного исследования, в ходе которого было изучено более 800 приговоров судов, наиболее активно используются такие электронные системы оплаты, как: «ЮMoney», «QIWI Кошелёк», «LegaIRC», «WebMoney»[3].

В целях противодействия использованию преступниками возможностей современных телекоммуникационных технологий и электронных систем оплаты субъектами предупреждения преступности на регулярной основе проводится мониторинг медиапространства. В результате, только по итогам 2019 года принято свыше 22,7 тыс. экспертных решений о пресечении работы тех веб-сайтов, приватных групп в социальных сетях и мессенджерах, посредством которых осуществляется пропаганда наркопотребления и распространение наркотиков.

Противоправное использование современных ИТТ способствует распространению нетрадиционных форм сексуальной эксплуатации: теле-секс, виртуальный секс и порнография на экране компьютера. Самый распространённый и наказуемый практически во всех государствах вид киберпреступлений – преступления, связанные с детской порнографией.

По данным экспертов, в настоящее время практически от 70 до 100% порнографических изображений несовершеннолетних распространяется с помощью сети Интернет. Причем в сети спрос на детскую порнографию в 3–5 раз превышает предложения. Порнографические материалы с изображениями несовершеннолетних, изготавливаемые на территории России, с огромной прибылью

---

[1] Саркисян А.Ж. Преступления в сфере информационно-коммуникационных технологий: понятия и особенности // Уголовное судопроизводство: проблемы теории и практики. 2020. № 1. С. 69-74.

[2] Бражников Д.А., Шиян В.И. Основные криминальные угрозы государственной и общественной безопасности // Расследование преступлений: проблемы и пути их решения. 2016. № 4 (14). С 41-45.

[3] См.: Афанасьева О.Р., Шиян В.И. Современные тенденции незаконного оборота наркотиков на объектах транспорта // Транспортное право и безопасность. 2020. № 4 (36). С. 45 – 53.

распространяются через Интернет к конечным пользователям – жителям стран Европы и США, а также «домашним» потребителям[1].

Киберпреступления представляют угрозу транспортной безопасности, о чем неоднократно в своих исследованиях упоминал А.В. Борисов[2].

Лица, совершающие преступления с использованием ИТТ, постоянно совершенствуют средства и методы, применяемые в преступной деятельности.

Исследуемый вид преступлений имеет транснациональный характер и создает угрозу национальной безопасности не только России, но и других государств.

Учитывая изложенное, эффективное противодействие преступлениям, совершаемым с использованием ИТТ может быть обеспечено на основе тесного взаимодействия всех правоохранительных органов России, а также с правоохранительными органами других государств.

Задачами такого сотрудничества должны стать: 1) выработка, внедрение и использование понятий и категорий, используемых в процессе противодействия преступлениям, совершаемыми с использованием ИТТ, создание условий для эффективного сотрудничества с иностранными государствами в правовом регулировании взаимодействия в данной сфере; 2) разработка и реализация согласованных мер, направленных на противодействие преступлениям, совершаемым с использованием ИТТ; 3) результативная координация этой деятельности; 4) повышение эффективности сотрудничества правоохранительных органов России и зарубежных государств в предупреждении, выявлении, пресечении и расследовании преступлений, выявлении и установлении лиц, их подготавливающих, совершающих или совершивших, а также розыске лиц, скрывающихся от уголовного преследования, в целях привлечения их к уголовной ответственности.

В качестве основных форм сотрудничества следует назвать, прежде всего:

обмен оперативной, статистической, научно-методической и иной информацией о состоянии преступности в сфере ИТТ, информацией для пополнения единого банка данных о транснациональных преступных группах и преступных организациях, совершающих преступления с использованием ИТТ;

проведение согласованных следственных действий, комплексных совместных и/или согласованных профилактических оперативно-розыскных мероприятий и специальных операций, создание и укрепление специализированных подразделений по противодействию преступлениям, совершаемым с использованием ИТТ, оснащение их современными аппаратно-программными научно-техническими средствами;

---

[1] Польшиков А.В., Серов Ю.В. Преступления, связанные с изготовлением и оборотом детской порнографии в сети Интернет: проблемы детерминации и предупреждения // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж: Воронежский ин-т МВД России, 2017. № 1. С. 42–50.

[2] Борисов А.В. Угрозы транспортной безопасности // Вестник Академии Следственного комитета Российской Федерации. 2020. № 2 (24) С. 76 – 79; Борисов А.В. Криминогенное влияние пандемии коронавирусной инфекции на состояние транспортной безопасности // Расследование преступлений: проблемы и пути их решения. 2020. № 2 (28) С. 32 – 35.

выработку рекомендаций и предложений по совершенствованию правового обеспечения, форм и методов совместной деятельности специализированных подразделений по противодействию преступлениям, совершаемым с использованием ИТТ;

разработку и внедрение технологий, рекомендаций и согласованных мер, препятствующих совершению преступлений с использованием ИТТ.

Противодействие преступлениям, совершаемым с использованием ИТТ должно иметь комплексный, регулярный и наступательный характер.

Литература

1. Афанасьева О.Р., Шиян В.И. Современные тенденции незаконного оборота наркотиков на объектах транспорта // Транспортное право и безопасность. 2020. № 4 (36). С. 45 – 53.
2. Борисов А.В. Криминогенное влияние пандемии коронавирусной инфекции на состояние транспортной безопасности // Расследование преступлений: проблемы и пути их решения. 2020. № 2 (28) С. 32 – 35.
3. Борисов А.В. Угрозы транспортной безопасности // Вестник Академии Следственного комитета Российской Федерации. 2020. № 2 (24) С. 76 – 79
4. Бражников Д.А., Шиян В.И. Основные криминальные угрозы государственной и общественной безопасности // Расследование преступлений: проблемы и пути их решения. 2016. № 4 (14). С 41-45.
5. Польшиков А.В., Серов Ю.В. Преступления, связанные с изготовлением и оборотом детской порнографии в сети Интернет: проблемы детерминации и предупреждения // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. Воронеж: Воронежский ин-т МВД России, 2017. № 1. С. 42–50.
6. Саркисян А.Ж. Преступления в сфере информационно-коммуникационных технологий: понятия и особенности // Уголовное судопроизводство: проблемы теории и практики. 2020. № 1. С. 69-74.

А.Д. Юницкая

Необходимость разработки регламента по идентификации электронной судебной документации

Аннотация. Статья представляет собой пример разрешения проблемы возникновения конфликта, который заключается в противоречии принципов гласности и профессиональной тайны при судебном делопроизводстве. Данный конфликт присущ практически всем уровням судебной власти и на настоящее время не разрешен нормативно и технически. В качестве подхода к разрешению данного конфликта, предлагается способ использования цифрового водяного знака (далее – ЦВЗ) с целью обнаружения источника утечки информации в ходе судебной деятельности.

Ключевые слова: гласность, информационная безопасность, судебное делопроизводство, цифровой водяной знак, регламент.

XXI век характеризуется стремительным развитием информационных технологий, которые затрагивают все сферы жизни общества, в том числе судебную власть. При этом, любая информация, представленная в цифровом виде, нуждается в соответствующего рода защите. Особенно, когда вероятность ее нелегитимного распространения может составлять угрозу репутационного, экономического характера, а также достигать масштабов угрозы государственной безопасности. Условно назовем вышеуказанные сведения «судебной тайной». Данное понятие внесено в кавычки, так как в Российской Федерации законодательно закреплен принцип гласности судебного разбирательства – одно из основных условий деятельности современной судебной системы [1]. В данном случае будут рассматриваться сведения, попадающие под ограничения указанного принципа и выступающие поводом для рассмотрения уголовных дел в закрытом порядке.

При этом, соблюдая принцип гласности, упомянутый выше и закрепленный в «Постановлении Пленума Верховного Суда РФ от 13.12.2012 г. № 35», данные, его ограничивающие и обозначенные Регламентом организации сведений о находящихся в суде делах и текстов судебных актов в информационно-телекоммуникационной сети Интернет на официальном сайте суда общей юрисдикции, маркируются и ретушируются. Их мы так же вносим в понятие "судебной тайны".

Соблюдая принцип гласности, возникает явное противостояние открытости и необходимости введения мер по организации информационной безопасности (рисунок 1), которая необходима судам как обладателям критической информации, получаемой в ходе реализации своей основной функции – осуществления правосудия. При этом, необходимо обеспечить информационную безопасность, не умаляя значимости принципа открытости.

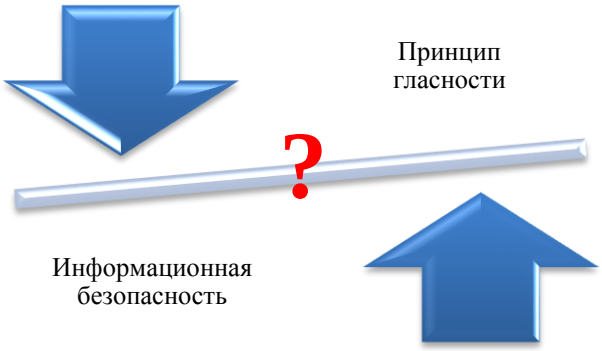


Рисунок 1 — Демонстрация противостояния

Чтобы грамотного внедрить и использовать цифровой водяной знак (далее– ЦВЗ) в судебной практике, необходимо разработать регламент. Для этого был проведен системный анализ процессов обработки информации в ходе судебного делопроизводства, основные результаты которого, с акцентом на функционал ЦВЗ, приведены ниже.

Под мерами обеспечения информационной безопасности подразумевается организация защищенного документооборота с выполнением условия обнаружения источника потенциальной утечки посредством внедрения в предварительно оцифрованную документацию ЦВЗ. Следует обратить внимание на тот факт, что используется именно цифровой водяной знак, а не цифровой отпечаток, так как последний, скорее, предназначен для идентификации объекта защиты. Следует отметить, что цифровой подписи также недостаточно для решения поставленной задачи. поскольку требуется установить не только факт искажения документа, но и зафиксировать источник несанкционированной модификации документа, Специальным образом сформированные исходные данные (далее – метаданные) устанавливаемого на документ ЦВЗ в ряде случаев предоставляет возможность идентификации нарушителя. В качестве метаданных используются IP/MAC адрес потенциального нарушителя, его геолокация (при возможности ее корректного фиксирования) и дата-время открытия документа. Потенциально, можно для этих целей использовать технологию, подобную "Fingerprint".

В качестве базового алгоритма внедрения ЦВЗ в объекты защиты в данной работе был взят метод встраивания цифрового знака Коха-Жао, так как он позволяет сделать стеганосистему более робастной [6] к таким часто выполняемым в ходе делопроизводства преобразованиям, как сжатие с потерями. Суть алгоритма состоит в том, чтобы встроить скрываемое сообщение, а именно специальным образом сформированные метаданные, в документ судебного делопроизводства, цифровая версия которого представлена в форматах изображений или видеопотоков (.pdf, .png, .jpeg, mpeg и др.). При этом изображение квантуется целиком и встраиваемый в него ЦВЗ распределится по всему изображению. Сначала производится дискретно-косинусное преобразование, после чего изображение делится на блоки размерностью 8x8 пикселей с последующим квантованием.

$$\Omega(u,\upsilon)=\frac{\zeta(u)\zeta(\upsilon)}{\sqrt{2N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cos\left[\frac{\pi u(2x+1)}{2N}\right]\cos\left[\frac{\pi\upsilon(2y+1)}{2N}\right];$$

$$S(x,y)=\frac{1}{\sqrt{2N}}\sum_{u=0}^{N-1}\sum_{\upsilon=0}^{N-1}\zeta(u)\zeta(\upsilon)\Omega(u,\upsilon)\cos\left[\frac{\pi u(2x+1)}{2N}\right]\times\cos\left[\frac{\pi\upsilon(2y+1)}{2N}\right],$$

где:

$C(x,y)$ и $S(x,y)$ — элементы оригинального u восстановленного по коэффициентам ДКП изображения соответственно размерностью $N \times N$;

x, y — пространственные координаты пикселей изображения;

$\Omega(u, v)$ — матрица коэффициентов ДКП;

u, v — координаты в частотной области;

$\zeta(u) = 1/\sqrt{2}$ если $u = 0$, и $\zeta(v) = 1$, если $v > 0$.[3, с.130]

В полученные блоки встраивается сообщение, содержащее исходные метаданные. На этом процедура сжатия завершается. На выходе мы получаем документ с встроенным цифровым знаком, при открытии которого злоумышленником, в данный цифровой знак фиксируется информация о его геолокации, MAC- и IP-адресе.

В рамках концепции данной работы, по сути, подразумевается организация защищенного документооборота с выполнением условий поставленной ранее задачи, а именно обнаружением источника потенциальной утечки посредством внедрения в предварительно оцифрованную документацию цифрового водяного знака (рисунок 2).

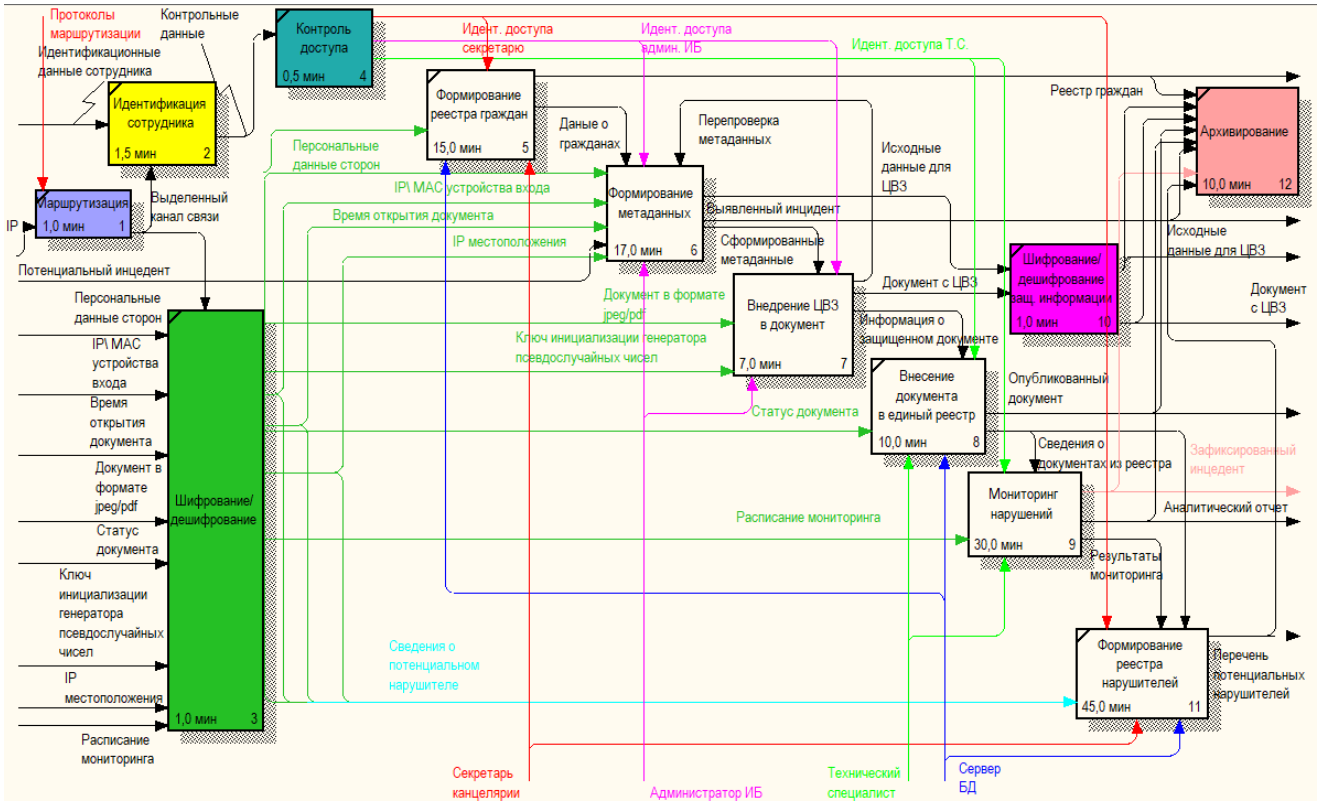


Рисунок 2 – Модель разрабатываемой системы

В данном отображении продемонстрированы основные функции, выполняемые сотрудниками аппарата суда, задействованными в рассматриваемом процессе.

Все данные, необходимые для последующего функционирования, должны пройти процесс шифрования для криптозащиты и обеспечения защищенного документооборота. Маршрутизация на канальном уровне необходима для выделения сегмента пользователей, не допущенных к сети Интернет для работы с информацией ограниченного доступа. Идентификация пользователей выделенного сегмента происходит на основе входных данных (пароль, логин) с последующим предоставлением доступа, согласно правам. В зависимости от полномочий, сотрудник выполняет работу в соответствии со своими должностными обязанностями. Сформированные метаданные внедряются в документ, подлежащий защите. После завершения процедуры внедрения ЦВЗ, документ вносится в единый реестр защищенных документов для возможности проведения дальнейшего мониторинга нарушений.

Мониторинг потенциальных нарушений осуществляется посредством фиксации на сервере приложений, бизнес-аналитика которого реализует выявление

инцидентов несанкционированного доступа к документам. Производится в соответствии с заранее установленной периодичностью, обозначенной в "расписании мониторингов", предположительно, дважды в месяц. По итогу мониторинга формируется реестр нарушителей. Итогом проделанной работы является сформированный аналитический отчет, который отправляется Судебному Департаменту раз в месяц.

Внедрение рассматриваемой регламентируемой системы в рамках организации защищенного документооборота позволит правоохранительным структурам своевременно реагировать на современные вызовы и угрозы.

В рамках реализации "Концепции информационной политики судебной системы на 2020 - 2030 годы", в краткосрочной перспективе, возможен переход к единой информационной платформе, позволяющий в реальном масштабе времени обеспечить исключительно санкционированный доступ ограниченного круга лиц к закрытым материалам судебного разбирательства [4]. Таким образом, будет практически пресечена потенциальная возможность утечки информации "изнутри" – инсайдерская угроза.

Список использованных источников

1. "Гражданский процессуальный кодекс Российской Федерации" от 14.11.2002 № 138-ФЗ (ред. от 08.12.2020) // СПС "КонсультантПлюс".
2. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации 09.09.2000 № Пр-1895) // Российская газета. 2000. 28 сентября.
3. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика.— К.: "МКПресс", 2006 . — 288 с, ил.
4. "Концепция информационной политики судебной системы на 2020 - 2030 годы" (одобрена Советом судей РФ 05.12.2019) // СПС "КонсультантПлюс".
5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 г. № 149-ФЗ // СПС "КонсультантПлюс".
6. Фомичева С.Г. Моделирование мобильных агентов в киберфизических системах В сборнике: Волновая электроника и инфокоммуникационные системы. Сборник статей XXIII международной научной конференции. Санкт-Петербург, 2020. С. 368-374.

К.С. Ярославский

Криминалистические аспекты расследования незаконной игорной деятельности, осуществляемой посредством сети Интернет

Аннотация. В статье автор рассматривает изменение криминалистического подхода к расследованию незаконной игорной деятельности, осуществляемой посредством сети Интернет, на примере такого понятия как место совершения преступления, а также делает краткий обзор проблемных вопросов, с которыми сталкиваются правоохранительные органы при расследовании такого рода преступлений.

Ключевые слова: незаконные организация и проведение азартных игр, незаконная игорная деятельность, интернет-казино, онлайн-казино, место совершения преступления.

В современном обществе высокие технологии прочно вошли в повседневную жизнь людей и играют в ней все большую роль. Еще не так давно для большинства были не понятны такие термины как «облачное хранилище», «VPN», «вэбмани» и т.д., сеть Интернет не имела повсеместной доступности, а платежи осуществлялись посредством наличных денежных средств. В настоящий момент ситуация в указанной сфере изменилась кардинально, и уже достаточно сложно найти людей, которые так или иначе не используют высокие технологии. Столь серьезные изменения, произошедшие в достаточно короткий срок, позволяют прогнозировать и дальнейшее развитие высоких технологий в геометрической прогрессии, что означает, что совсем скоро подобные новшества окажутся обыденной частью жизни практически каждого человека. К сожалению, развитие высоких технологий затрагивает не только конструктивные области социума, но и находит свое отражение в ряде негативных сфер, в том числе активно применяется при совершении уголовно наказуемых деяний. Такой вызов требует своевременной и эффективной реакции со стороны правоохранительной системы путем исследования данной тематики и выработки приемов борьбы, в том числе криминалистического характера.

Вместе с тем, криминалистические аспекты расследования преступлений, совершенных при помощи высоких технологий, обладают существенной спецификой и отличаются рядом проблемных вопросов.

Принципы организации расследования любых преступлений включают в себя в качестве обязательного к установлению обстоятельства – определение места совершения преступления, а обязательного к проведению следственного действия – осмотр места происшествия. Об этом же свидетельствует анализ классической криминалистической характеристики любого из составов преступлений. При расследовании целого ряда уголовно-наказуемых деяний правильное определение места совершения преступления и его осмотр занимают центральную роль и являются одним из основных источников доказательств по делу в целом и главным – на первоначальном этапе расследования, когда следователь вынужден действовать в условиях недостаточности информации как о совершенном преступном деянии, так и о лицах его совершивших.

Таковым является и место совершения преступления при расследовании незаконной игорной деятельности. Большинство используемых правоприменителями алгоритмов расследования указанного вида преступления[1] предлагают следователю начинать процесс расследования именно с осмотра места происшествия или проведения обыска на месте совершения преступления – территории незаконного игорного заведения.

[1] Вывод сделан на основе анализа материалов более 200 уголовных дел, расследованных следователями СК России в период с 2016 по 2019 год по ст. 171.2 УК РФ.

Практика свидетельствует, что именно благодаря месту преступления и связанным с ним следственным действиям следователь получает неопровержимые доказательства как самого факта организации и проведения азартных игр, так и доказательства причастности к этому конкретных лиц. Однако, следователи привыкли, что местом совершения данного преступления является некое помещение, обладающее конкретным географическим расположением, где находится нелегальное игорное заведение. Вокруг этого принципа строится тактика проведения осмотра места происшествия или обыска, включающая в себя решение таких важных задач как определение времени проведения тактической операции; способа обеспечения внезапности тактической операции, в том числе вариантах быстрого проникновения в помещение игрового зала; сил и средств, необходимых для осмотра, изъятия и транспортировки игрового оборудования, а также места его хранения; мер по нейтрализации возможного противодействия в форме уничтожения или повреждения игрового оборудования.

Вместе с тем, в последние годы нелегальная игорная деятельность постепенно перемещается в виртуальное пространство. Процесс этот является объективным и связан в основном с двумя факторами: во-первых, создание и функционирование нелегального интернет-казино экономически менее затратно, во-вторых, такая форма обеспечивает высокую степень анонимности организатора и сложность его привлечения к уголовной ответственности.

Отсутствие привычного места преступления в виде помещения игрового зала делает невозможным применение зарекомендовавшей себя схемы расследования данного преступления и требует адаптации существующей методики расследования незаконной игорной деятельности путем разработки и применения новых криминалистических приемов и рекомендаций.

В этой связи требуется сформулировать основные задачи, стоящие перед следователем при проведении осмотра места происшествия (обыска) в незаконном игорном заведении и определить тот результат, к которому стремятся правоохранительные органы по итогам производства данных следственных действий, а затем предложить равноценную замену в целях формирования достаточной совокупности доказательств с учетом специфики функционирования интернет-казино.

Итак, основными задачами, связанными с получением доказательств при исследовании места совершения преступления, являются – установление самого факта проведения азартной игры и доказывание причастности к совершению преступления конкретных лиц. В обычном игорном заведении это достигается путем:

- описания помещения игрового зала с акцентом на характерную для игорного заведения обстановку;
- описания и фиксации процесса проведения азартной игры при помощи имеющегося в зале игрового оборудования, его изъятие;
- фиксации наличия персонала игорного заведения и игроков;
- описания и изъятия средств управления (администрирования) игровым залом;
- обнаружения и изъятия денежной кассы зала, бухгалтерских записей;

- обнаружения и изъятия средств связи администраторов зала с лицами, организовавшими данную деятельность;

- изъятия данных видеозаписывающих систем;

- обнаружения и изъятия документации, связанной с закупкой, и обслуживанием оборудования, обслуживанием помещения игорного зала (коммунальные платежи, оплата услуг связи, договоры аренды помещения и т.д.).

Из сказанного очевидно, что решение одной из задач в случае с интернет-казино для следователя упрощается, а второй – значительно усложняется.

Перенос места совершения преступления – игорного заведения в виртуальную среду делает возможным доступ к нему любого лица, в любое время без своей фактической идентификации, что относится и к следователю. Таким образом, следователь получает возможность беспрепятственно фиксировать факт проведения азартной игры путем проведения следственных действий, например путем осмотра интернет-ресурса, представляющего услуги нелегального игорного заведения, или проведения следственного эксперимента.

Однако, одновременно значительно усложняется установление личности иных игроков, участвующих в азартных играх, определение суммы дохода нелегального интернет-казино, а самое главное – идентификация организатора такого заведения. Установление перечисленных аспектов возможно при получении сотрудниками правоохранительных органов доступа к учетной записи организатора казино, где хранятся подобные сведения, в свою очередь для этого требуется получение логина и пароля такой учетной записи.

Установление организатора незаконной игорной деятельности и доказывание его вины в совершенном преступлении возможно по двум основным направлениям:

- посредством анализа электронных следов, оставляемых при регистрации и функционировании интернет-казино, в том числе сведений о персональных данных организатора (IP-адреса, MAC-адреса компьютеров, IMEI планшетов и мобильных телефонов, использованных при входе в личный кабинет; сведения, указываемые при регистрации и обслуживании казино; функционирование службы поддержки казино и т.д.);

- посредством анализа движения денежных средств, получаемых организаторами в качестве прибыли интернет-казино, вплоть до их вывода в пользу бенефициара.

Однако, проведение указанных мероприятий связано со значительными трудностями, в том числе с необходимостью привлечения для участия в расследовании специалистов в области высоких технологий, с международным взаимодействием в области осуществления уголовного преследования, с преодолением принципа неразглашения персональных данных рядом государств, с борьбой против использования средств программ-анонимайзеров в целях обезличивания преступника при совершении противоправных деяний посредством сети Интернет.

Решение указанных проблемных вопросов в рамках разработки криминалистической методики расследования незаконной организации и проведения

азартных игр видится крайне актуальным и позволит выйти правоохранительным органам на новый уровень противодействия киберпреступлениям.

Литература

1. Лимарь А.С. Противодействие незаконной игорной деятельности, совершенной с помощью интернет-технологий // Криминологический журнал. 2019. № 2. С. 58 – 61.

2. Нестерович С.А. Проблемы расследования киберпреступлений, которые стоят перед сотрудниками следственных органов // Вестник науки и образования. № 8 (44). 2018. Том 2. С. 46 – 49.

3. Халиуллин А.И. Место совершения преступления как признак состава преступления в сфере компьютерной информации // Актуальные проблемы экономики и права. 2012. № 1. С. 291 – 294.

4. Щукин В.И., Скоморохов О.Н. Организационные и тактические аспекты осмотра мест происшествий при расследовании преступлений, связанных с незаконными организацией и (или) проведением азартных игр с использованием игрового оборудования // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2017. № 1 (29). С. 39–42.

ОБУЧАЮЩИЕСЯ

А.Д. Балабаева
Научный руководитель:
С.Ю. Скобелин

Получение и анализ биллинговой информации при расследовании преступлений, связанных с безвестным исчезновением несовершеннолетних

Аннотация. В статье исследуются возможности получения информации о соединениях между абонентами и (или) абонентскими устройствами для расследования преступлений по фактам безвестного исчезновения несовершеннолетних. Рассматривается порядок действий следователя для получения и анализа биллинговой информации. Предлагается вариант использования данных детализации для определения максимально точного местоположения пропавшего ребенка.

Ключевые слова: биллинговая информация, абонент, абонентское устройство, несовершеннолетний, безвестное исчезновение.

Безвестное исчезновение несовершеннолетних вызывает большой общественный резонанс и требует особого контроля со стороны правоохранительных органов. Именно поэтому, как отмечает Председатель СК РФ А.И. Бастрыкин, так важно своевременно и четко организовать розыск пропавшего[1]. Следственная практика свидетельствует о том, что для расследования преступлений по факту безвестного исчезновения детей широко применяется биллинговая информация. Получение биллинговой информации реализуется в порядке производства следственного действия в виде получения информации о соединениях между абонентами и (или) абонентскими устройствами, предусмотренного ст. 186.1 УПК РФ[2].

При подготовке данного следственного действия следует учитывать, что биллинг – это информация о соединениях между абонентами и (или) абонентскими устройствами, содержащаяся в базах данных компаний-операторов. Ее срок хранения у оператора составляет 3 года[3].

Получение информации о соединениях между абонентами и (или) абонентскими устройствами допускается только по возбужденному уголовному делу, которое согласно совместной инструкции МВД, Генеральной прокуратуры и

---

[1]Бастрыкин А.И. О деятельности следственных подразделений Следственного комитета Российской Федерации по поиску без вести пропавших несовершеннолетних // Раскрытие и расследование преступлений, связанных с безвестным исчезновением граждан. М.: Московская академия Следственного комитета Российской Федерации, 2018. С. 8. – 7-9 с.

[2] Антонов О.Ю. Тактика получения и использования криминалистически значимой информации от операторов связи // Российский следователь. 2020. №4. С.3-7.

[3]Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 // URL: https://rg.ru/2005/09/02/pravila-dok.html. Дата обращения: 25.01.2020.

Следственного комитета Российской Федерации[1], возбуждается незамедлительно при наличии данных о том, что безвестное исчезновение несовершеннолетнего связано с совершением в отношении его преступления. Практика идет по тому пути, что уголовное дело в связи с безвестным исчезновением несовершеннолетнего возбуждается по ст. 105 УК РФ.

Кроме того, для производства данного следственного действия необходимо получить решение суда в порядке ст. 165 УПК РФ. Для этого следователь направляет в суд ходатайство. Такое ходатайство должно быть мотивированным, процессуальные требования к его содержанию указаны в ч. 2 ст. 186.1 УПК РФ[2].

Однако для повышения эффективности производства данного следственного действия следует уточнять ту информацию, которую необходимо получить от оператора сотовой связи, в частности, необходимо запросить не только сведения о дате, времени, продолжительности, типе соединения, номерах абонентов и местах расположения базовых станций, но также и данные номеров этих базовых станций (параметры LAC и CID), их азимутов действия и временной задержки «TA», а также GPRS-сессий (для получение информации о соединениях через популярные приложения-мессенджеры, такие как WhatsApp, Viber и пр.

GPRS-сессия представляет собой интернет-соединение, когда телефон произвольно осуществляет выход в сеть, другими словами, абонент зачастую не контролирует этот процесс, в то время как его абонентское устройство принимает сигнал, который проходит через определенную базовую станцию и может быть отражен в детализации. Этот факт неоспоримо важен для целей расследования и поиска как жертвы, так и преступника.

Такие же данные следует отразить в запросе оператору сотовой связи.

Анализ полученной от оператора сотовой связи информации играет ключевую роль и осуществляется за счет проведения осмотра предмета (полученного от оператора – CD-диска) или документа (распечатанной детализации). Следует обратить внимание на то, что осмотр должен содержать не только данные, перечисленные в документе, бумажном или электронном, но и анализ этой информации[3]. На наш взгляд, целесообразно производить осмотр с участием родственников без вести пропавших несовершеннолетних либо тщательно сопоставлять показания, содержащиеся в их допросах, с полученными данными. Также на сегодняшний день, когда необходимо анализировать большой объем данных о со-

---

[1]Приказ Министерства внутренних дел Российской Федерации, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации от 16 января 2015 г. № 38/14/5 // URL: https://rg.ru/2015/03/30/bezvesti-dok.html. Дата обращения: 25.01.2020.

[2] Курченко В.Н. Особенности рассмотрения судами ходатайств о получении информации о соединениях между абонентами // Уголовный процесс.2015. №8. С.58-67.

[3] Скобелин С.Ю. Осмотр детализации соединений абонентов (тактические аспекты) // Уголовное судопроизводство: проблемы теории и практики.2020. № 1. С.60-63.

единениях, к осмотру целесообразно привлекать специалиста, актуальность приобретает компьютерно-аналитическая экспертиза[1]. Так же рекомендуется составление планов, схем, отображающих перемещение абонентского устройства на карте местности.

Именно полнота запрашиваемой и предоставленной биллинговой информации позволит наиболее точно установить маршрут передвижения и определить возможное местонахождение несовершеннолетнего.

Маршрут передвижения без вести пропавшего позволяет использовать так называемый массовый биллинг – детализация соединений всех пользователей, находящихся в интересующем районе в определенное время[2]. Он нужен для поиска возможных преступников, которые передвигались с несовершеннолетним по одному маршруту. Необходимо выехать к базовым станциям, отраженным в детализации без вести пропавшего, и с помощью датчика РЭО или мобильного приложения типа Netmonitor установить номера базовых станций в конкретных местах. Использование датчика РЭО в данному случае допускается, однако он слишком чувствительный и может ловить сигналы в том числе и не интересующих следствие базовых станций, поэтому оптимально использовать приложение Netmonitor, установленное на телефон. Следует помнить, что мы не знаем, СИМ-картами какого оператора пользовались преступники, а также тип сети пользователя (2G, 3G или LTE), приложение отражает только базовые станции того оператора, СИМ-карта которого установлена в телефоне, поэтому при использовании мобильного приложения для определения базовых станций нужно менять в телефоне СИМ-карты, а также предпочтительный тип сети. Все эти действия необходимо оформить в виде следственного эксперимента, а с полученными номерами базовых станций направить в суд ходатайство на получение массового биллинга уже по конкретным базовым станциям (например, по ходу движения пропавшего ребенка из показаний свидетелей).

Целесообразно также выявить место последнего соединения абонентского устройства, которым пользовался без вести пропавший несовершеннолетний, и произвести осмотр данного участка местности. Для этого следует на основании информации, содержащейся в детализации, определить ту базовую станцию, через которую передавался сигнал последнего соединения, и отметить ее на карте. Каждая базовая станция обслуживает угол в 60 градусов, при этом значение азимута является биссектрисой этого угла. Значение азимута из детализации нужно перенести на карту, отложив данный угол от линии севера, а затем отмерить от значения азимута углы по 30 градусов в обе стороны (так как азимут является биссектрисой). Далее для определения удаленности места соединения от басо-

---

[1] Себякин А.Г. Анализ информации о соединениях между абонентами, использование его результатов в раскрытии и расследовании преступлений // Полицейская и следственная деятельность. 2018. № 4. С. 29-38.

[2] Скобелин С.Ю. Использование биллинговой и иной цифровой информации для установления местонахождения пропавшего без вести // Раскрытие и расследование преступлений, связанных с безвестным исчезновением граждан. М.: Московская академия Следственного комитета Российской Федерации, 2018. С. 209. – 208-210 с.

вой станции необходимо обратиться к параметру временной задержки «ТА». Известно, что сигнал проходит расстояние от базовой станции до устройства за определенное время – это значение и называется временной задержкой. Значение ТА (timing advance) представляет собой число от 0 до 63, которое увеличивается на 1 при росте удаленности от базовой станции на каждые 550 метров. Так, при значении данного показателя «0» удаленность конкретного сектора, где находилось абонентское устройство, составляет от 0 до 550 метров, при значении «1» - от 550 метров до 1100 метров, «3» - от 1100 метров до 1650 метров и так далее. Определив на карте конкретное место соединения, следует выехать к нему и произвести осмотр в целях возможного обнаружения следов преступления или самого пропавшего (его трупа).

Тот же результат можно получить на местности, отложив угол азимута от нулевого показателя компаса и измерив удаленность места соединения от базовой станции.

Таким образом, получение биллинговой информации способствует эффективному расследованию преступлений по фактам безвестных исчезновений несовершеннолетних, однако для ее использования следователь должен быть осведомлен о порядке работы с такого рода данными. Кроме того, важно обращать внимание на полноту запрашиваемых и получаемых от оператора сотовой связи сведений.

Список использованных источников

1. Антонов О.Ю. Тактика получения и использования криминалистически значимой информации от операторов связи // Российский следователь. 2020. №4. С.3-7.
2. Бастрыкин А.И. О деятельности следственных подразделений Следственного комитета Российской Федерации по поиску без вести пропавших несовершеннолетних // Раскрытие и расследование преступлений, связанных с безвестным исчезновением граждан. М.: МАСК РФ, 2018. – 7-9 с.
3. Курченко В.Н. Особенности рассмотрения судами ходатайств о получении информации о соединениях между абонентами // Уголовный процесс.2015. №8. С.58-67.
4. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538. URL: https://rg.ru/2005/09/02/pravila-dok.html. Дата обращения: 25.01.2020.
5. Приказ Министерства внутренних дел Российской Федерации, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации от 16 января 2015 г. № 38/14/5. URL: https://rg.ru/2015/03/30/bezvesti-dok.html. Дата обращения: 25.01.2020.
6. Себякин А.Г. Анализ информации о соединениях между абонентами, использование его результатов в раскрытии и расследовании преступлений // Полицейская и следственная деятельность. 2018. № 4. С. 29-38.
7. Скобелин С.Ю. Использование биллинговой и иной цифровой информации для установления местонахождения пропавшего без вести // Раскрытие и

расследование преступлений, связанных с безвестным исчезновением граждан. М.: МАСК РФ, 2018. – 208-210 с.
8. Скобелин С.Ю. Осмотр детализации соединений абонентов (тактические аспекты) // Уголовное судопроизводство: проблемы теории и практики.2020. № 1. С.60-63.

Е.П. Васильева
Научный руководитель: **А.Г. Скуковский**

Криминалистическая характеристика киберпреступлений

Аннотация. В данной статье рассмотрены криминалистические характеристики само содержание киберпреступлений, особенности раскрытия и расследования киберпеступлений и через какие средства проникают «вирусы».

***Ключевые слова*:** киберпреступления, криминалистическая характеристика, вредоносная программа.

Киберпреступление - это общественно опасное деяние, совершаемое в сети Интернет, посягающее на информационную безопасность, собственность, права человека, другие охраняемые законом отношения, связанные с информацией и сведениями, хранящиеся в сети Интернет. Основным элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления[1].

Под криминалистической характеристикой, понимают совокупность значимой информации, которая содержит свойства и признаки преступления, который служат для выдвижения версий. Они позволяют оценить ситуацию, которая возникает в процессе расследования компьютерных преступлений. Характеристику кибепреступлений составляют элементы, такие как: способы совершения преступления и механизмы противоправного деяния; способы сокрытия преступлений в сфере компьютерной информации; орудии (средства) совершения противоправного деяния; обстановка и место совершения преступления; следы преступления; предметы преступного посягательства; лица, совершающие данные преступления.[2]

Способ совершения преступления - это совокупность приёмов и методов, с помощью которых совершается преступления. Из содержания статьи 273 УК РФ, можно определить способы совершения преступления, которые заключаются в постановке задач, целей, выборе средств и приемов создания вредоносных программ. В соответствии с ГОСТ Р 50922-2006, вредоносная программа-это программа, предназначенная для осуществления незаконного доступа к информации и (или) иные воздействия на информацию и ресурсы информацион-

[1] Шевченко, Е.С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39).
[2] Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014

ной системы. Другими словами, вредоносная программа предназначена для модификации, блокировки и уничтожения информации. В отдельных случаях, информацию, полученную незаконным способом, киберпреступники используют для вымогательства, например, взлом и хищение информации, в которой содержатся сведения о личной или интимной жизни потерпевшего, для создания условий, в которых преступник требует деньги дабы не отправить похищенные сведения в свободных доступ. Основными средствами незаконного доступа «вируса» является: хищение электронных паролей и ключей, использование оптических и акустических средств наблюдения за ЭВМ (электронно-вычислительная машина).

На сегодняшний день в криминалистике нет единой классификации способов совершения преступлений в сфере компьютерной информации[1]. Можно рассмотреть классификацию, предложенную А.Н. Родионовым и А.В. Кузнецовым, согласно которой, способы совершения компьютерных преступлений можно разделить на основных четыре элемента. Первый элемент- это совокупность элементов, направленных на изъятие средств компьютерной техники, для получения средств совершения преступления. Второй элемент подразумевает неправомерный доступ к компьютерной информации, с последующими незаконными действиями, например, взлом личной информации в корыстных целях или взлом паролей к доступам карт и кошельков. В третий элемент входят приемы, направленные на изготовление и распространение вредоносных программ (например, вирусы, программы-взломщики). Четвертый элемент носит характер нарушения прав человека и гражданина, например, нарушение авторских прав. Четвертый элемент включает в себя изъятие и использование полученной информации в корыстных или иных целях, например, компьютерное пиратство, мошенники и вымогатели.

Киберпреступники используют сеть Интернет как средство и место совершения преступлений. Сеть можно применять для разных целей, например, таких как: взлом сайтов и индивидуальных страниц, поиск ключей к электронных картам и кошелькам. Также, сеть может быть применена для получения информации, которая позволит совершить преступление, например, информация или практическое пособие о том, как создать взрывное устройство или изготовить наркотик в домашних условиях. С другой стороны, сеть Интернет можно использовать для распространения незаконных или компрометирующих материалов, или информации. В данном случае, оно используется для нахождения покупателей, для пересылки информации и денежных средств, тем самым, используется для совершения преступления. Использование киберпространства позволяет создавать всемирную сеть сбыта и способствует наступлению преступных последствий, а также позволяет оставить эту деятельность вне поля зрения, а в некоторых случаях и вне досягаемости, правоохранительных органов. В вышеуказанных возможных способах использования сети выступает в качестве средства совершения преступления. Не надо забывать, что киберпространство для преступников – это не только средство совершения преступления, но и главным

[1] Парфенов А.Ф. Общее учение об объективной стороне преступления: СПб., 2006. 169 с.

местом для их совершения. Такое специфическое место достаточно сильно осложняет процесс расследования преступления. Для того, чтобы раскрыть преступления в сети Интернет, потребуется помощь соответствующего специалиста[1]. Киберпространство сложно изучать со стороны юриспруденции, но в современном мире разрабатываются новые приемы в криминалистике, для расследования подобных преступлений. Традиционные способы осмотра места происшествия, применяемые в материальном пространстве, не подходят для осмотра мета происшествия киберпреступлений. Для этого, необходимы специальные методики расследования и раскрытия киберперступлений в соответствии с характерными особенности интернет пространства. Особенным считается и место совершения преступления, поскольку само общественно опасное деяние происходит в цифровом (виртуальном) мире (пространстве), но свое отражение оставляет в реальном мире.[2]

Киберпреступления в современном мире все чаще заставляют обращать особое внимание на безопасность персональных данных в сети. Они имеют специфический характер по своему содержанию и расследованию преступлений в виртуальном мире.

Литература

1. Атальянц М. А. Способ совершения преступления и его уголовно-правовое значение : дис. канд. юрид. наук. М., 2010.
2. Вехов В. Б. Компьютерные преступления. — М.: Право и Закон, 1996.
3. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014.
4. Парфенов А.Ф. Общее учение об объективной стороне преступления: СПб., 2006. 169 с.
5. Шевченко, Е.С. О криминалистической трактовке понятия «киберпреступность» // Информационное право. 2014. № 3 (39). С. 29 - 32.

[1] Вехов В. Б. Компьютерные преступления. — М.: Право и Закон, 1996.

[2] Атальянц М. А. Способ совершения преступления и его уголовно-правовое значение : дис. канд. юрид. наук. М., 2010.

В.И. Воронова
Научный руководитель:**В.А. Перов**

Уголовно-правовой аспект противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей

Аннотация. На сегодняшний день информатизация общества развивается высокими темпами. На этом фоне огромных масштабов достигла преступность в сфере информационно-телекоммуникационной сети «Интернет». Расследование преступлений в сети «Интернет», в частности мошенничества с использованием информационно-комуникационных технологий требует от сотрудников правоохранительных органов владения теорией и практикой расследований данной категории преступлений.

Ключевые слова: киберпреступность, киберполиция, преступления в сфере информационно-коммуникационных технологий, международное сотрудничество, международное законодательство в сфере противодействия киберпреступности.

Развитие научно-технического прогресса и широкое использование современных информационных технологий в обществе поднимает перед государством и международным сообществом проблемы информационной безопасности. В современных условиях развития общества государственные границы размываются, а правоохранительные органы до сих пор не могут адекватно отвечать на эти новые вызовы.

По разным экспертным оценкам во всем мире ущерб от киберпреступности составляет ежегодно от 300 до 800 млрд евро[1].

Функции по противодействию киберпреступности возлагают на правоохранительные органы (в том числе, органы внутренних дел и государственной безопасности).

Главными задачами правоохранительных органов в сфере противодействия киберпреступности являются:

- мониторинг киберпространства с целью выявления соответствующих преступлений, вирусов либо вредоносного программного обеспечения;
- осуществление оперативно-розыскных мероприятий, расследование киберпреступлений в порядке, предусмотренном Уголовно-процессуальным законом;
- накопление, обобщение и анализ информации о киберпреступности, подготовка методологии выявления и расследования соответствующих преступлений;
- профилактику киберпреступлений с активным привлечением гражданского общества, средств массовой информации.

По данным форума страховых технологий InnoIns-2018, в России в 2018 году ежедневно 16 предприятий подвергались кибератакам. Для защиты от кибератак различные коммерческие компании во всем мире выделяют около 122, 5 млрд. долларов в год.

---

[1] Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. URL: https://cyberleninka.ru/article/n/istoriya-i-zarubezhnyy-opyt-pravovoy-reglamentatsii-kompyuternoy-prestupnosti.

По данным ПАО «Сбербанк России», объем мировых капиталовложений в сферу кибербезопасности до 2021 года вырастет в 14 раз и достигает около одного триллиона долларов США. На практике участились случае нападения на информационную инфраструктуру. Так, например, во время Чемпионата мира по футболу в России (2018) было зафиксировано более 25 млн. вредоносных атак.

Несмотря на значительную распространённость киберпреступлений в России и мире следственно-судебная практика свидетельствует буквально о единичных случаях привлечения к уголовной ответственности по статье 159[3] УК РФ (мошенничество с использованием электронных средств).

Согласно официальной статистики, в 2017 году за совершение таких деяний было привлечено к уголовной ответственности всего лишь 47 человек.

На сегодняшний день значительную распространённость получило интернет мошенничество с использованием социальных сетей и мессенджеров (в частности, ВКонтакте», «WhatsApp» «Telegram» «Инстаграм»).

Как отмечают представители Банка России, интернет - мошенничество в нашей стране обуславливается, в первую очередь, недостаточным уровнем финансовой грамотности населения[1].

Уголовным законом европейских государств мошенничество в интернет-пространстве выделяется в качестве самостоятельного состава преступления, предусматривающие, как правило, более строгие санкции по сравнению с общими нормами о хищении. Так, в Федеративной Республике Германии имеет место отдельный состав преступления объективной стороной которого является мошенничество с использованием вредоносных программ (статья 263 Уголовного кодекса ФРГ)[2].

В некоторых государствах использование информационно-телекоммуникационных сетей признаётся особым способом совершения мошенничества (УК Швеции)[3].

Также необходимо проведение модернизации положений Уголовного закона. Так, например, действующая редакция Уголовного кодекса РФ не даёт однозначного ответа как квалифицировать кибертерроризм.

Ряд учёных предлагают часть 2 статьи 205 УК РФ дополнить пунктом "совершённый с использованием информационно-коммуникационных сетей".

---

[1] Якимова Екатерина Михайловна, Нарутто Светлана Васильевна. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. №2. URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu.

[2] Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. №4 (46). URL: https://cyberleninka.ru/article/n/mezhdunarodnyy-i-zarubezhnyy-opyt-ugolovno-pravovogo-protivodeystviya-hischeniyam-sovershaemym-s-ispolzovaniem-kompyuternoy.

[3] Немов Максим Владимирович. Киберпреступность как новая криминальная угроза // Эпоха науки. 2017. №9. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza-1.

Ряд учёных (Протасевич А.А., Р. Е. Джансараева) предложили следующие изменения в статьи Уголовного кодекса с целью установления уголовной ответственности за киберпреступления. В частности было предложено в статье 205.1 УК РФ установить, что использование сети «Интернет» является орудием для вовлечения в совершение преступлений террористической направленности; в статье 207 УК РФ указать сообщения полученные органами государственной власти с помощью информационно-коммуникационных технологий средством заведомо ложного сообщения об акте терроризма[1].

Таким образом, для эффективного противодействия киберпреступлениям необходимо усовершенствование деятельности правоохранительных органов в сфере выявления, расследования и противодействия преступлений в сфере информационно-коммуникационных технологий.

Также выглядит целесообразным усовершенствование положений Уголовного закона в части законодательного определения понятия кибертерроризма и выделения использования информационно-телекоммуникационных сетей как особого способа совершения преступлений.

Литература

1. Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. URL: https://cyberleninka.ru/article/n/istoriya-i-zarubezhnyy-opyt-pravovoy-reglamentatsii-kompyuternoy-prestupnosti
2. Журавленко Н.И., Шведова Л.Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. №3 (53). URL: https://cyberleninka.ru/article/n/problemy-borby-s-kiberprestupnostyu-i-perspektivnye-napravleniya-mezhdunarodnogo-sotrudnichestva-v-etoy-sfere
3. Немов М.В. Киберпреступность как новая криминальная угроза // Эпоха науки. 2017. №9. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza-1
4. Пучков Д.В. К вопросу взаимосвязи кибернетических технологий и уголовного права // Социально-политические науки. 2017. №6. URL: https://cyberleninka.ru/article/n/k-voprosu-vzaimosvyazi-kiberneticheskih-tehnologiy-i-ugolovnogo-prava
5. Романов И.В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. №5 (13). URL: https://cyberleninka.ru/article/n/ponyatie-kiberprestupleniy-i-ego-znachenie-dlya-rassledovaniya

[1]Романов Иван Викторович. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. №5 (13). URL: https://cyberleninka.ru/article/n/ponyatie-kiberprestupleniy-i-ego-znachenie-dlya-rassledovaniya.

6. Чернякова А.В. Международный и зарубежный опыт уголовно-правового противодействия хищениям, совершаемым с использованием компьютерной информации // Юридическая наука и правоохранительная практика. 2018. №4 (46). URL: https://cyberleninka.ru/article/n/mezhdunarodnyy-i-zarubezhnyy-opyt-ugolovno-pravovogo-protivodeystviya-hischeniyam-sovershaemym-s-ispolzovaniem-kompyuternoy
7. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. №2. URL: https://cyberleninka.ru/article/n/mezhdunarodnoe-sotrudnichestvo-v-borbe-s-kiberprestupnostyu

В.О. Гаврилова
Научный руководитель: **В.А. Мишенин**

Криминологические аспекты совершения преступлений против собственности с использованием информационно-телекоммуникационных сетей

Аннотация. В настоящей статье анализируется криминологическая составляющая совершения преступлений против собственности с использованием информационно-телекоммуникационных сетей, способы решения и повышения эффективности мер предупреждения преступлений в данной сфере.

Ключевые слова: мошенничество, предупреждение преступлений, противодействие преступности, виктимологические факторы.

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[1] в качестве приоритетного направления внутренней политики определяет развитие информационных и коммуникационных технологий, формирование информационного пространства и соответствующей инфраструктуры.

Информационные технологии все глубже проникают в повседневную жизнь граждан. Все большее количество персональных данных пользователи размещают в информационных системах: посредством электронной почты пересылаются копии документов, удостоверяющих личность, на сервисы платежных систем направляются реквизиты банковских карт, в социальных сетях размещается информация о личной жизни, посредством мессенджеров передается иная конфиденциальная информация.

Такие глобальные изменения в сфере информационных технологий сильно отразились на состоянии преступности в целом. Так, по данным ГИАЦ МВД России, которые содержатся в Отчетах о преступлениях, совершенных в сфере телекоммуникационной и компьютерной информации, в 2017 г. в производстве

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

правоохранительных органов находились уголовные дела о 105 645 преступлениях, совершенных с использованием информационно-коммуникационных технологий, что на 24,5 % превышает аналогичный показатель предыдущего года – 79 704. Следует отметить, что данная тенденция сохраняется и на протяжении последних лет.

Приведенные статистические показатели отражают составы преступлений, предусмотренных ст. ст. 158, 159, 159.3, 159.6, 183, 272–274 УК РФ.

Официальная статистика показывает динамику роста количества зарегистрированных и расследованных преступлений, совершенных в финансовой сфере, с использованием информационно-телекоммуникационных технологий.

Так, в 2010 г. было выявлено 1 819 случаев совершения мошенничества указанным способом, в 2011 г. – 2 049, 2012 г. – 2 748, 2013 г. – 2 196, 2014 г. – 2 187, 2015 г. – 13 483. При этом в 2014 г. расследовано и направлено в суд только 457 уголовных дел, 1 396 приостановлено в связи с неустановлением лица, совершившего преступление, а в 2015 г. направлено в суд только 1 352 уголовных дела, приостановлено – 9 488. Аналогичная картина наблюдается и с кражей, совершенной с использованием информационно-телекоммуникационных технологий: только каждое 5 преступление расследуется и передается в суд.

В системе противодействия преступлениям, совершаемым с использованием высоких технологий, целесообразно сосредоточить внимание на разработке нижеперечисленных мер.

1. Повышение эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий.

2. Совершенствование системы правоприменения и разработка новых форм и методов борьбы с преступлениями, совершаемыми с использованием высоких технологий (методическое обеспечение).

3. Принятие организационно-управленческих мер предупреждения преступлений, совершаемых с использованием высоких технологий.

4. Проведение комплекса целенаправленных мероприятий по устранению причин и условий, способствующих совершению компьютерных преступлений в отношении государственных и иных учреждений, предприятий и организаций.

Отдельно следует остановиться на виктимологическом аспекте противодействия преступлениям, совершаемым с использованием высоких технологий. Поведение жертвы является составным элементом механизма преступления, поэтому одним из необходимых условий повышения эффективности предупреждения экономических преступлений в рассматриваемой сфере являются меры виктимологической профилактики.

В качестве субъектов осуществления виктимологической профилактики высокотехнологичных преступлений выступают как государство в лице правоохранительных органов, так и общественные формирования и иные негосударственные структуры.

Подводя итоги, следует сказать, что на данный момент количество преступлений в экономической сфере, совершенных с использованием информационно-

коммуникационных сетей, растет в связи с увеличением количества пользователей данными технологиями и переходом к хранению информации в сети «Интернет».

Эффективное противодействие данному виду преступлений возможно только при условии воздействия на все факторы, способствующие совершению преступления. К ним относится виктимологическая составляющая. Необходимо соблюдать меры предосторожности в информационно-телекоммуникационном пространстве.

Список использованных источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в редакции от 27 декабря 2019 года) // СПС КонсультантПлюс (дата обращения 28.11.2020).
2. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.
3. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС КонсультантПлюс (дата обращения 28.11.2020).
4. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.
5. Грибунов О. П. Расследование преступлений в сфере компьютерной информации и высоких технологий : учеб. пособие / О. П. Грибунов, М. В. Старчиков. – М. : ДГСК МВД России, 2017. – 159 с.
6. Климов Д. В. Расследование хищений, связанных с использованием сети «Интернет» : учеб. пособие / Д. В. Климов. – Н. Новгород : Нижегородская академия МВД России, 2017. – 24 с.
7. Организация данных в системах обработки данных. Термины и определения [Электронный ресурс]: ГОСТ 20886-85. – Взамен ГОСТ 20886-75; введ. 1986-07-01 / Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200015708.

К.О. Даценко
Научный руководитель: **В.А. Мишенин**

Использование специальных знаний в области компьютерной техники в целях предупреждения киберпреступлений

Аннотация. В настоящей статье анализируются возможности использования специальных знаний в области компьютерной техники в целях повышения эффективности мер предупреждения киберпреступлений.

Ключевые слова: компьютерная техника, киберпреступление, предупреждение преступлений, противодействие преступности, специальные знания.

В эпоху цифровизации, когда современные компьютерные технологии пронизывают каждый аспект жизни современного человека, преступность глобально видоизменилась, получив новый вид под названием «киберпреступность».

В современном мире в сетях Интернет совершается огромное количество преступлений, которые угрожают обществу и всем государствам.

Уголовное законодательство разных стран не адаптировано к киберпреступлениям, именно поэтому киберпреступники почти безнаказанно совершают преступления в компьютерной сфере, несмотря на то, что различные сферы общественной жизни адаптировались в информационной сфере, например такие, как наука, образование, финансовые операции, банковские услуги, торговая деятельность и иные.

Современные тенденции киберпреступности заключаются в следующем:

1) усложнение преступных схем, усиление организационной структуры;
2) совершение совместно с иными общественно опасными деяниями;
3) приобретение данным видом преступности транснационального характера.

Компьютерные Интернет-технологии на сегодняшний день представляют собой удобное для преступников средство и орудие для совершения общественно опасных деяний. Отмечается, что каждый день растут возможности Интернет-технологий, что привлекает внимание таких субъектов, как преступные, террористические и экстремистские организации, так как киберпространство на сегодняшний день представляет собой сложную систему, для пользования которой необходимо наличие специальных знаний.

Связано это с тем, что киберпространство обеспечивает анонимность, делает сложной идентификацию правонарушителей и их оборудования. В пример можно привести мессенджер «Telegram», которым активно пользуются преступники, так как указанный мессенджер с помощью шифрования полностью защищает данные пользователя.

Согласно статистическим данным, около 80% компьютерных преступлений совершаются при помощи вредоносного программного обеспечения компьютеров, вирусных программ, бот–сетей, хищения пользовательских данных в целях их дальнейшей продажи.

Определить точное число преступлений, совершаемых в Интернет-пространстве, не представляется возможным, так как потерпевшими от преступлений являются миллионы человек. Согласно статистическим данным, только в 2019 году пользователей Интернета насчитывалось 4,1 млрд человек, что составляет 53,6% населения мира.[1]

По статистическим данным МВД России за 2019 год совершено около 300 000 IT-преступлений, а самым распространенным видом преступлений в сети Интернет является мошенничество.

Исходя из обобщенных данных, киберпреступления совершают мужчины в возрасте до 35 лет, многие из них являются студентами ВУЗов либо уже имеют высшее образование, а также широкие познания в компьютерной технике. Данные лица имеют хорошие организаторские и технические способности, для совершения технически сложных мошенничеств они могут объединяться в группы.

Потерпевшими, как правило, становятся лица, обладающие теми материальными ценностями, на завладение которыми направлен умысел преступника. Кроме того, их допреступное поведение также может спровоцировать криминальные действия. Так, потерпевшие при мошенничестве, как правило, излишне доверчивы, простодушны. Иногда их поступки противоречат нормам морали — потерпевшие проявляют алчность, жадность, стремление нечестным путем обойти существующие порядки.

Пол, возраст и социальный статус значения при этом не имеют. Жертвой Интернет–мошенничества может стать любой пользователь глобальной сети.

Как отмечает Р.С. Атаманов, в независимости от того, о каком виде мошенничества в Интернете идёт речь, характеристика круга потерпевших лиц, во многом, похожа. Большинство жертв Интернет-мошенников являются людьми, слабо знакомыми с техникой безопасности при работе в Сети.[1]

В зависимости от того, в какой области действовал мошенник, его жертвам могут быть присущи такие характеристики как: склонность к азартным играм, опрометчивость, самонадеянность, желание лёгкой наживы (мошенничества с инвестиционными схемами и платёжными системами), желание сэкономить (фальшивые интернет – магазины) и т.д.

Помимо физических лиц потерпевшими могут быть: операторы связи и провайдеры; банки и иные кредитные организации; Интернет-магазины; а также иные организации.

Активное использование глобальной сети Интернет, привело к тому, что мошенничество в отношении личного имущества граждан часто стало совершать именно в сети Интернет и достаточно специфическими способами.

Высокая степень анонимности, бесконтрольность и неподчиненность глобальной сети, низкие затраты на организацию деятельности очень привлекают мошенников, которые все чаще используют ее возможности для реализации преступных замыслов.

---

[1] Сайт информационного агентства «ТАСС» https://tass.ru/obschestvo/7080150 (Дата обращения 03.12.2020).

К основным способам мошенничества в глобальной сети можно отнести:

1) Организация мошенниками фиктивных «банков» и «инвестиционных фондов»;

2) Организация фиктивных Интернет–магазинов, аукционов, торговых площадок;

3) Предложение помощи в отмывании крупных сумм;

4) Организация Интернет-казино и лотерей;

5) Интернет–благотворительность. Спам рассылки и сайты с просьбой о материальной помощи под трогательную историю, просьбами внести денег в фиктивный благотворительный фонд и т д;

6) Фишинг - вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям путем обмана или злоупотребления доверием[1];

7) Подделка платежных систем и взлом аккаунтов – т.е. записей, содержащих сведения, которые пользователь сообщает о себе некоторой компьютерной системе;

8) Кардинг - вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

В связи с вышеуказанным, представляется возможным выделить уровни предупреждения киберпреступности: общесоциальный, специально-криминологический и индивидуальный.[1]

Общесоциальные меры предупреждения киберпреступлений направлены на решение социальных проблем, они оказывают благоприятное воздействие на детерминанты киберпреступности. Здесь мы можем также выделить внешнеэкономические, социальные, научно-технические, общекультурные меры.

К внешнеэкономическим мерам относят: проведение политики, направленной на увеличение показателей экономики, повышения уровня конкурентоспособности национальной экономики, развитие инноваций, снижение уровня коррупции, внедрение научных разработок и технологий в производство и другие.

К социальным мерам предупреждения относят: уменьшение социального расслоения общества, эффективную социальную политику, установление достойного уровня оплаты труда и другие.

К научно-техническим мерам предупреждения киберпреступности относят: эффективную государственную поддержку научных исследований, увеличение количества образовательных и научных учреждений, высококвалифицированную подготовку специалистов, конкурентоспособную разработку научных продуктов и другие.

К общекультурным мерам предупреждения киберпреступности относят: увеличения уровня юридической грамотности граждан, организацию патриотического и духовного воспитания подрастающего поколения, увеличение показателя культурного имиджа Российской Федерации и другие.

---

[1] Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия. № 1 - 2018 С. 120-127.

На законодательном уровне в целях предупреждения киберпреступности следует обратить внимание на повышение качества принимаемых законов, на уменьшение количества коллизий и пробелов в национальном законодательстве, увеличение взаимодействия с международным сообществом в законодательной сфере и т.д.[1]

К числу приоритетных задач в Стратегии развития информационного общества в Российской Федерации до 2030 года отнесены задачи по обеспечению комплексной защиты информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры. [2]

Киберпреступления совершаются также с использованием криптовалюты, при совершении сделок с ней. Это происходит потому, что отношения, связанные с криптовалютой, не урегулированы на законодательном уровне.

Законодатели считают, что операции с криптовалютой несут в себе риски, а граждане и физические лица могут быть вовлечены, например, в финансирование терроризма, так как операции с криптовалютой носят анонимный характер.

Специалисты отмечают, что криптовалюта является перспективным средством для развития финансовой системы Российской Федерации, но вместо того, чтобы создать механизм ее реализации, продумать способы регулирования отношений с криптовалютой, законодатель вводит одни лишь запретительные меры. Примером тому может служить безуспешное блокирование мессенджера Telegram.[3]

Кроме того, правоохранительными структурами предпринимались попытки блокировки различных Интернет-ресурсов, например, Linkedln, доступ к которому можно получить посредством использования информационно-телекоммуникационных сетей, информационных ресурсов (сайт в сети "Интернет" или страница сайта в сети "Интернет", информационная система, программа для электронных вычислительных машин), посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с Федеральным законом от 29.07.2017 №276-ФЗ «Об информации».

Под специально-криминологическими мерами понимается деятельность, направленная напрямую на искоренение причин и условий совершения преступлений.

К мерам по противодействию киберпреступлениям относят:

---

[1] Агапов П. В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности, монография. 2014. С. 135

[2] Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СПС КонсультантПлюс (дата обращения 03.12.2020)

[3] Решение Таганского районного суда г. Москвы от 13.04.2018 №2-1779-2018 // https://agora.legal/fs/a_delo2doc/80_file_Telegram_Taganskiy_Nemedlenno.pdf (Дата обращения 03.12.2020)

1. Повышение эффективности научного обеспечения деятельности по борьбе с киберпреступностью.

2. Разработка новых методов борьбы с киберпреступлениями.

Работа в данном направлении представляет собой усовершенствование нормативных актов, инструкций, которые способны оказать воздействие на ситуацию в случае проблем их законодательного разрешения.

Также следует прийти к гармонизации нормативной правовой базы, так как ее разнородность порождает проблемы в процессах правоприменения, что неэффективно сказывается на противодействии киберпреступности и порождает новые преступные деяния.

Как представляется, в целях предупреждения киберпреступлений, следует законодательно закрепить обязанность производителей компьютерной техники внедрять в программное обеспечение своих продуктов антивирусные программы. В качестве примера можно привести операционную систему Windows 10, в которой уже содержится программа защиты от вирусных программ – «брандмауэр» - инструмент, призванный обеспечить безопасность операционной системы благодаря функции сканирования входящих и исходящих пакетов данных, а также, в случае необходимости, их блокирования.

Реализация данной инициативы упирается в то, что почти все антивирусные программы являются платными и их установка производителями компьютерной техники на свои продукты не отменит периодические платежи для активации антивирусных программ. Иными словами, существует вероятность того, что пользователи после бесплатного периода использования установленной антивирусной программы не будут активировать ее продление, что, в свою очередь, не будет способствовать профилактике киберпреступлений.

К мерам предупреждения киберпреступлений также относится разработка новых методик противодействия им. На сегодняшний день предпринимаемые меры направлены, в основном, на усиления мониторинга социальных сетей в целях поиска материалов противоправного характера.

3. Организационно-управленческие меры предупреждения преступлений представляют собой комплекс мер, направленных на совершенствование деятельности субъектов, которые предупреждают данный вид преступлений.

К ним относят:

1) создание системы подготовки сотрудников в области информационных систем в образовательных учреждениях правоохранительных органов, таких, как МВД, Следственный комитет и так далее. Это обеспечит правоохранительную систему квалифицированными кадрами. В гражданской сфере следует учредить курсы для обучения данных специалистов по информационной безопасности.

2) совершенствование информационного обеспечения деятельности по противодействию киберпреступлениям. Данная работа решает ряд задач, включающих в себя сбор и систематизацию криминологически значимой информации, ее анализ и классификацию, определение состояния дел и перспективное прогнозирование развития ситуации.

Реализация перечисленных мер будет способствовать предупреждению киберпреступности.

Список использованных источников

1. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» // СПС КонсультантПлюс (дата обращения 03.12.2020)
2. Решение Таганского районного суда г. Москвы от 13.04.2018 №2-1779-2018 // https://agora.legal/fs/a_delo2doc/80_file_Telegram_Taganskiy_Nemedlenno.pdf (Дата обращения 03.12.2020)
3. Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия. Социально-политические науки. № 1 - 2018 С. 135-137
4. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / [П. В. Агапов и др.] ; Акад. Генеральной прокуратуры Российской Федерации. - Москва: Акад. Генеральной прокуратуры Российской Федерации, 2014. - 135 с.
5. Сайт информационного агентства «ТАСС» https://tass.ru/obschestvo/7080150 (Дата обращения 03.12.2020)

М.А. Забелина
Научный руководитель: **В.В. Бычков**

Особенности проведения обыска в ходе расследования публичных призывов к осуществлению террористической деятельности, оправдания или пропаганды терроризма

Аннотация. В статье рассмотрены особенности проведения обыска в ходе расследования преступлений террористической направленности, совершенных в информационно-телекоммуникационной сети Интернет. Проведен анализ следственной и судебной практики по уголовным делам данной категории.

Ключевые слова: преступления террористической направленности, расследование, следственные действия, обыск, информационно-телекоммуникационные сети, Интернет.

Преступления террористической направленности являются социальной проблемой, оказывающей негативное влияние на важные аспекты развития и функционирования государства. При этом в подавляющем большинстве публичный призыв к осуществлению террористической деятельности, публичное оправдание или пропаганда терроризма совершаются с использованием информационно-телекоммуникационных сетей в том числе сети Интернет, поскольку развитие компьютерных технологий привело к возможности создания виртуальной реальности, которая может рассматриваться как пространство поиска виртуальных единомышленников, без раскрытия реальной личности. Всеобщая компьютеризация является процессом внедрения электронно-вычислительной техники

во все сферы жизнедеятельности человека, что приводит к расширению преступной деятельности в информационно-телекоммуникационном пространстве.

В целях расследования преступлений данной направленности важное значение имеет проведение обыска, который всегда носит выраженный принудительный характер в отношении лиц, у которых он проводится. По уголовным делам данной направленности, обыск является одним из неотложных следственных действий. Исходя из специфики, совершения данного преступления в сети Интернет, замедление в производстве обыска приводит к уничтожению следов преступления, а также объектов по средствам, которых оно совершалось или сокрытию данных объектов, уничтожению электронных цифровых следов. Электронные цифровые следы – это изменения, возникающие в памяти электронных цифровых устройств в результате их использования в преступной деятельности[1]. Иначе говоря, это следы совершения любых действий (включения, создания, активации, внесения изменений, удаления) в информационном пространстве компьютерных и иных цифровых устройств, их систем и сетей.

Объектами поиска по данной категории дел являются различные носители информации, а именно флеш-накопители, сотовые телефоны, смартфоны всех видов и типов, системные блоки, компьютерные блоки (моноблоки), ноутбуки (нетбуки, ультрабуки), планшеты, цифровые часы, компакт-диски; копировальная и множительная техника; различные инструкции по вербовке людей, по сокрытию следов преступной деятельности; сведения о членах и структуре террористической организации и ее финансировании; клятвы и другие атрибуты деятельности; документы, свидетельствующие о поступлении денежных и материальных средств[2]. В ходе проведения следственного действия необходимо определить наличие у компьютера внешних устройств, накопителей информации на жестких магнитных дисках и картах памяти, виртуального диска[3]. Кроме того, объектами поиска в связи со спецификой преступления являются оружие, боеприпасы, взрывные устройства и взрывчатые вещества, в том числе самодельные. Необходимо при обыске сосредоточить в том числе внимание на материалах, из которых может быть изготовлено взрывное устройство, предметы, которые могут быть использованы для конструирования взрывных устройств (детонаторы, электросхемы и т.п.), инструменты и механизмы, которые могут быть использованы при изготовлении взрывных устройств (слесарный инструмент, станки, оборудование, специальные приспособления) с микрочастицами взрывчатых веществ[4].

---

[1] Лушин Е.А. Современные возможности раскрытия и расследования преступлений по электронным следам: лекция. СПб.: Санкт-Петербургская академия СК России, 2020. С. 7.

[2] Бычков В.В., Сабитов Р.А., Сабитов Т.Р. Противодействие преступлениям экстремистской и террористической направленности: криминологические, уголовно-правовые и криминалистические аспекты: монография. М., 2013. С. 225.

[3] Баранов В.В., Алескеров В. И. Телекоммуникация и киберпространство как средство преступления экстремистской и террористической направленности // Труды Академии управления МВД России. 2020. № 1 (53). С. 110.

[4] Багмет А.М., Бычков В.В., Зеленков М.Ю. Расследование преступлений, связанных с экстремистской и террористической деятельностью: учебник. М., 2019. С. 444.

Например, Магомедов осуществил поиск, скопировал с тематических интернет-ресурсов и сохранил на жесткий диск принадлежащего ему портативного компьютера и флеш-карту видеофайлы под названием «470328.mp4», «470329.mp4», «Бел Пор», «Детонатор», «приготовление Триперекись ацетона (ТА) – КИСА.avi», представляющие собой видеоинструкцию по изготовлению инициирующего взрывчатого вещества – перекиси ацетона, бризантного взрывчатого вещества на основе аммиачной селитры и взрывного устройства, где описываются средства, способы и методы изготовления вышеуказанных взрывчатых веществ и взрывных устройств в кустарных условиях, после чего Магомедов обучил лиц средствам, способам и методам их изготовления, взрывчатых веществ – перекиси ацетона и бризантного взрывчатого вещества на основе аммиачной селитры и снаряженного ими в качестве зарядов взрывного устройства[1].

В том числе поиску подлежат схемы, рисунки, чертежи поджигающих и взрывных устройств, блокноты, ежедневники, календари с пометками. Например, согласно заключению взрывотехнической экспертизы, в записной книжке, изъятой у подсудимого Назарова, имеется рукописный текст, на листах 59 и 60 содержащий сведения, позволяющие изготовить в домашних условиях инициирующее взрывчатое вещество – перекись ацетона[2].

Подготовка к проведению обыска включает в себя следующие действия: получение сведений о лице, лицах, в помещениях которых будет проведен обыск; определение времени и места производства обыска; при необходимости получение постановления суда о производстве обыска в жилище; подготовка необходимых технических средств; определение круга участников следственного действия.

При производстве обыска ключевыми вопросами помимо отыскания, обнаружения предметов, имеющих значение для расследования уголовного дела, является фиксация, изъятие и исследованием информации, содержащейся в памяти устройств. Электронные носители информации высокотехнологичны и для работы с ними необходимо участие специалиста, так как внешнего осмотра и получение той или иной информации недостаточно, такая информация может быть тщательно завуалирована, либо удалена. Основным условием допущения специалиста к участию в следственных действиях является наличие у него соответствующих знаний, сложившаяся практика идет по пути подтверждения наличия у специалиста специальных знаний при помощи его диплома о профильном высшем образовании. Поскольку электронные носители информации являются технически сложными объектами, следователь обязан обращать внимание не

---

[1] Приговор коллегия по уголовным делам Московского областного суда по обвинению Магомедова в совершении преступлений, предусмотренных ст. 208 ч.1, 222 ч.3, 282.1 ч.1, 205.2 ч.1, 280 ч.1, 30 ч.1 – 223 ч.3, 30 ч.1 – 205 ч.2 п. «а», 228 ч.2, 222 ч.1 УК РФ. URL: https://rospravjmnxyxlu3.darknet.to/ (Дата обращения 11.01.2021).

[2] Приговор коллегит по уголовным делам Московского областного суда по обвинению Назарова в совершении преступлений, предусмотренных ст. 282.1 ч. 2, 30 ч. 1 - 223 ч. 3, 30 ч. 1 – 205 ч. 2 п. «а», 228 ч. 2 УК РФ. URL: https://rospravjmnxyxlu3.darknet.to/ (Дата обращения 18.01.2021).

только на формальное наличие у специалиста высшего образования, но также и наличие у него практического опыта работы с аналогичными объектами[1]. В связи с постоянными и непрерывными изменениями в сфере информационных технологий специалисту необходимо отслеживал все современные тенденции развития техники, поскольку постоянно появляются новые программные и аппаратные средства удаления информации.

Таким образом, обыск по делам данной категории является неотъемлемой частью достижения истины, по средствам него надлежащим процессуально образом добываются и соответствующе закрепляются доказательства. В связи с быстро выраженным развитием технических средств, возможностью дистанционного воздействия на последние, появлению новых технологий и устройств хранения данных, следователю необходимо: повышать техническую грамотность работы с информационными носителями и информационными следами, следующим образом периодическое посещение курсов повышения квалификации в данной сфере, самоподготовка с помощью методических рекомендаций по тактике проведения отдельных следственных действий и методике расследования различных категорий преступлений. В зависимости от складывающейся следственной ситуации для проведения обыска должны быть привлечены следователь-криминалист СК России, эксперт ЭКЦ МВД России и сотрудники организаций, которые работают в сфере компьютерной информации и восстановления электронных данных.

Из чего следует, что результативность производства обыска по делам данной категории в значительной мере зависит от качественного проведения подготовительного этапа, с учетом которого определяется состав группы и необходимое техническое обеспечение.

Литература

1. Багмет А.М., Бычков В.В., Зеленков М.Ю. Расследование преступлений, связанных с экстремистской и террористической деятельностью: учебник. М.: ЮНИТИ-ДАНА, 2019.
2. Баранов В.В., Алескеров В.И. Телекоммуникация и киберпространство как средство преступления экстремистской и террористической направленности // Труды Академии управления МВД России. 2020. № 1 (53). С. 104–113.
3. Бутенко О.С., Расчетов В.А. Актуальные вопросы изъятия электронных носителей информации // Наука, образование и культура. 2017. № 8 (23). С. 44-46.
4. Бычков В.В., Сабитов Р.А., Сабитов Т.Р. Противодействие преступлениям экстремистской и террористической направленности: криминологические, уголовно-правовые и криминалистические аспекты: монография. М.: Юрлитинформ, 2013.

[1] Бутенко О.С., Расчетов В.А. Актуальные вопросы изъятия электронных носителей информации// Наука, образование и культура. 2017. № 8 (23). С. 44.

5. Лушин Е.А. Современные возможности раскрытия и расследования преступлений по электронным следам: лекция. СПб.: Санкт-Петербургская академия СК России, 2020.

А.Д. Капралова
Л.А. Нечаева
Научный руководитель: **В.А. Перов**

Проблемы, встречающиеся на пути расследования киберпреступлений

Аннотация. В данной статье рассмотрены особенности при расследовании киберпреступлений, их виды и способы защиты от них. Эта тема в наше время очень актуальна, потому что данный вид преступлений появился не так давно, но он развивается с огромной скоростью и совершенствуется ежедневно, изобретая все новые способы мошенничества, атаки, либо угрозы личной информации пользователей. Также это преступление обладает определенной спецификой, о которой и пойдет речь в данной статье.

Ключевые слова: киберпреступление, уголовный процесс, информационно-телекоммуникационные сети, криминологическая характеристика.

Несмотря на то, что мы обучаемся на 1 курсе, нас заинтересовала эта тема, ведь именно наше поколение наиболее свободно владеет новейшим техническим оборудованием. В современном мире свое распространения получают высокие технологии. Сейчас информационно-телекоммуникационные сети внедрены во все сферы нашей жизни, именно поэтому меняется характер преступности. Растет число преступлений, которые совершаются с помощью компьютерных технологий. Преступность в данной сфере выступает одной из угроз национальной безопасности РФ. Расследование киберпреступлений обладает рядом особенностей. Поэтому для их успешного раскрытия необходимо разобраться с теоретической частью данного вопроса и рассмотреть проблемы, которые могут встретиться в процессе расследования. Киберпреступление – это преступление в виртуальном пространстве. Итак, в соответствии со статьей 14 УК РФ, преступление – это виновно совершенное общественно опасное деяние, запрещенное настоящим Кодексом под угрозой наказания. Значит киберпреступление – это виновно совершенное общественно опасное деяние, совершаемое в виртуальном пространстве и необходимым элементом механизма подготовки, совершения, сокрытия и отражения которого является компьютерная информация, выступающая в роли предмета или средства преступления. Также преступления, совершенные в виртуальном пространстве, обладают рядом особенностей. Например, высокая степень скрытности, отсутствие необходимости прямого контакта преступника с жертвой, сложностью сбора доказательств и процесса доказывания, а также отсутствие единой стратегии и программы по расследованию и борьбе с киберпреступлениями. В современном мире существует большое многообразие киберпреступлений. Для каждого отдельного вида вырабатыва-

ется своя методика расследования. Совет Европы выпустил конвенцию[1], которая содержит положения о киберпреступности, на основе которых можно классифицировать киберпреступления на 5 групп: преступления, посягающие на конфиденциальность, целостность и недоступность компьютерных данных и систем; преступления, связанные с использованием компьютера как средства совершения противозаконных действий; преступления, связанные с размещением данных в сети «Интернет»; преступления, связанные с нарушением авторских и смежных прав; преступления, связанные с распространением в сети «Интернет» расистских и ксенофобских материалов. На данный момент законодательство РФ не располагает понятием киберпреступление. Можно сказать, что термин «киберпреступление» пока является лишь криминологическим, но в скором времени станет уголовно-правовым и будет закреплен в соответствующих НПА. Однако в Уголовном кодексе РФ[2] в главе 28 «Преступления в сфере компьютерной информации» указаны общественно опасные деяния в виртуальном пространстве. Статья 272. Неправомерный доступ к компьютерной информации, Статья 273. Создание, использование и распространение вредоносных компьютерных программ, Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Анализируя состав данных преступлений становится понятно, что предметом и средством общественно опасных деяний такого рода является компьютерная информация. Итак, к источникам компьютерной информации можно отнести данные на различных электронных носителях, пластиковых банковских картах, смартфонах, файлы, флеш-карты. Успешное расследование преступлений, совершенных в киберпростраcтве требует базовых теоретических и технических знаний. При расследовании киберпреступлений могут возникать определенные трудности, такие как осмотр места происшествия, так как места преступления как такового не имеется. Так же для расследования данного вида преступлений нет определенных методических рекомендаций ввиду того, что киберпреступления постоянно совершенствуются, изобретая новые способы мошенничества, кражи информации и т.д. Расследование данного вида преступления имеет определенную специфику, которая обусловлена тем, что действия, совершаемые в ходе расследования, должны быть максимально засекречены, чтобы преступник через свое техническое устройство не мог помешать расследованию и удалить имеющиеся сведения. Последовательность действий по расследованию преступления должна быть выстроена так, чтобы подозреваемые не догадывались о проведении расследования. Само же устройство должно быть отсоединено от локальной сети организации, если таковая имеется, потому что локальная сеть предполагает наличие доступа других пользователей к данному компьютеру.

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // Официальный интернет-портал правовой информации. URL: www.base.garant.ru

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.12.2020) //Официальный интернет-портал правовой информации. URL: www.consultant.ru.

Также следователь должен привлечь специалистов, которые оценят состояние технического устройства, подверженного атаке, проанализируют его возможности, установят, есть ли на нем механические повреждения, либо угрозы для информации, которая входит в доказательную базу преступления. Вся следовая информация хранится в памяти устройства, поэтому исследование должно проводиться в рамках компьютерной технической экспертизы, что также является определенной проблемой, которая препятствует расследованию данного вида преступлений, потому что такие экспертизы занимают длительный процесс. Компьютерно-техническая экспертиза выявит всю активность компьютера, что даст возможность узнать несанкционированное получение доступа к имеющимся файлам, время этого доступа и местонахождение человека, который совершил незаконное проникновение в техническое устройство. Но не всегда удается сразу узнать личность злоумышленника, потому что IP-адрес чаще всего динамичен, то есть он может принадлежать сразу нескольким людям, что усложняет процесс расследования преступления. При проведении обыска (выемки) следователь подбирает специалиста, работающего в сфере киберпреступлений, понятых, которые также должны иметь навыки работы с компьютерной техникой. Большое значение при проведении обыска также имеет проведение опроса потерпевшего, чтобы установить время обнаружения атаки, а также всех лиц, которые имели доступ к данному устройству, либо были осведомлены об информации, находящейся в нем. Следователь должен узнать, как можно больше информации о потерпевшем и о целях совершения данного преступления, так как это может значительно облегчить ход расследования. Существует множество способов, благодаря которым можно обезопасить себя и свои устройства от киберпреступлений. В первую очередь важно иметь хотя бы базовую осведомленность о принципах работы того или иного устройства. На любые устройства следует устанавливать проверенные антивирусы, которые будут информировать о всевозможных угрозах, атаках и вирусах, которым подвергается устройство, и антивирус будет устранять их, но его следует часто обновлять, потому что программное обеспечение антивируса постоянно совершенствуется. Также не мало важную роль играет установление сложных паролей, либо установление двухфакторной проверки доступа, чтобы получение доступа было невозможным. Находясь в сети интернет важно следить за тем, на какие ссылки следует переходить, потому что часто вредоносные ссылки скрываются под ссылками, которые на первый взгляд нам известны, но на самом деле они несут угрозу. Также не следует размещать личную информацию на сайтах, к которым нет определенного доверия.

Правовое воспитание граждан играет немаловажную роль в профилактике подобных преступлений, это означает, что еще в школе подростков должны ознакомить с тем, какие бывают киберпреступления, как обезопасить себя от них и какие последствия могут повлечь за собой действия подобного характера. Подводя итог вышесказанному можно сделать вывод, что данный вид преступления довольно сложен в расследовании в связи с нестандартными методами проведения следствия, соответственно уровень квалификации специалистов в сфере информационных технологий для расследования данного преступления должен

быть высок. Это значит, что следует обратить особо внимание на подготовку следователей, специалистов. Зачастую при расследовании киберпреступлений сотрудники обращаются к особому аппаратному обеспечению, следовательно, необходимость материально-технического обеспечения возрастает. На сложность расследования также влияет уникальность каждого преступления и отсутствие определенной методики.

Список использованных источников

1. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ (ред. от 30.12.2020) //Официальный интернет-портал правовой информации. URL: www.consultant.ru.
2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // Официальный интернет-портал правовой информации. URL: www.base.garant.ru
3. Илюшин Д. А., Особенности расследования преступлений, совершаемых в сфере предоставления услуг интернет, 2008, 32 с.
4. Мещеряков В.А., Преступления в сфере компьютерной информации: основы теории и практики расследования, 2002, изд-во Воронеж. гос. ун-та, 407 с.
5. Тропина Т.Л., Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы, 2005, 26 с.

А.С. Кондрашова
Научный руководитель: **А.А. Лебедева**

Особенности изъятия электронных следов преступлений и работы с ними

Аннотация. Основной целью данной статьи является углубленный процесс изучения особенностей изъятия электронных следов преступлений и работы с ними. Актуальность данной проблемы вызвана стремительным развитием информационных технологий, которые находят свое отражение в деятельности, связанной с раскрытием преступлений. Следует применять исключительно проверенные на практике криминалистические приёмы при расследовании преступлений в сфере информационных технологий. В своей научной работе я попытаюсь выяснить условия работы и особенности электронных следов преступлений.

Ключевые слова: преступления, информационные технологии, криминалистическая деятельность, электронные следы, закон, уголовный кодекс, следственная деятельность, специалист, статья.

Целью настоящей работы является изучение компьютерной информации, которая включает в себя электронные следы, рассмотрение их особенностей, а также способов поиска необходимых электронных сведений для расследования компьютерных преступлений на разных этапах следствия.

Преступления в сфере компьютерной информации регулируются Уголовным кодексом Российской Федерации от 13 июня 1996 Федеральный Закон №163 под редакцией от 30 декабря 2020, главой 28, касающейся преступлений в сфере компьютерной информации, включающая в себя статьи 272, 273, 274, 274.1.

В Предметом данного вида преступлений принято считать саму компьютерную информацию, ограниченного доступа. В качестве объекта преступлений в сфере компьютерной информации, обращаясь к Уголовному кодексу Российской Федерации, понимаются общественные отношения, которые обеспечивают правомерный доступ, создание, обработку и использование, охраняемой законом, компьютерной информации, самим создателем, а также потребление ее иными пользователями.

В качестве примера рассмотрим одно из крупных преступлений в сфере компьютерной информации, которое произошло в марте 2011 года. Известная американская компания RSA по обеспечению компьютерной и сетевой безопасности, специализирующаяся на стандартах шифрования и шифрования заявила, что за её сотрудниками следили хакеры с помощью шифинговых писем, которые способны были взять под управление компьютеры. Хакеры смогли получить доступ ко всем сетям компании и скомпрометировали полностью систему защиты компании, которая использовала жетоны SecureID[1] для защиты своих клиентов. Компания RSA понесла убытки в размере 66 миллионов долларов и замену пользовательских жетонов на новые.

В Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 30.12.2020) "Об информации, информационных технологиях и о защите информации"// "Российская газета", № 165, 29.07.2006, касающимся защиты информации, информационных технологий и защиту информации, упоминается, что компьютерная информация представляет собой сведения, определенные данные, независимо от формы их представления, обладателя информации, как лица, которое самостоятельно создало информацию, либо получило на основании закона или договора право разрешать или ограничивать доступ к информации, по каким-либо признакам.

Стоит заметить, что не вся компьютерная информация находится под защитой закона, а именно, если она не относится к типу государственной тайны или же конфиденциальной информации, то в этом случае информация будет считаться не защищенной законом.[2] Компьютерные сведения могут быть подвергнуты таким неправомерным действиям, например, как копирование, блокирование, модифицирование, распространение и уничтожение данной информации.[3] (статьи 273, 274 УК РФ)

---

[1] SecurID - технология, разработанная компанией RSA, для предоставления двухфакторной аутентификации между пользователем и сетевыми устройствами.

[2] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2т. /А.В.Бриллиантов, Г.Д. Долженкова, Э.Н. Жевлаков [и др.]; под ред. А. В. Бриллиантова. – 2-е изд. – Москва : Проспект, 2016. - С.701 С. 324-329.

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2т. /А.В.Бриллиантов, Г.Д.// Там же – С.326.

Электронные следы являются некой значимой компьютерной информацией, по-другому можно сказать, данные, которые принимают электронно-цифровую форму, они могут быть зафиксированы на электронном носителе или же переходить по электромагнитным сигналам. Данное понятие может иметь и другие название, такие как, цифровые, компьютерные, информационные, но все они подразумевают одно – фиксирование криминалистически-значимой информации.[1]

На данный момент не смогли еще разработать единый подход к выделению классификации электронных следов в связи с молниеносным прогрессом в области информационных технологий.

Следует обратить пристальное внимание на особенности изъятия электронных следов преступлений. Согласно Уголовно-процессуальному кодексу Российской Федерации от 18 декабря 2001 Федеральный закон№174 в редакции от 08 декабря 2020 с изменениями и дополнениями, вступивший в силу с 19 декабря 2020, Статья 164.1. В которой говорится об особенностях изъятия электронных носителей информации и копирования информации с них при производстве следственных действий. Изъятие электронных следов не разрешается, за исключением трех случаев, которые предусмотрены уголовно-процессуальным законом:

1) если имеется постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие производится исключительно при наличии судебного решения, на его основании;

3) если на электронных носителях информации содержится та информация, которой владелец электронного носителя информации не может хранить и пользоваться ей, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

Изъятие электронных следов преступлений в процессе следственных действий производится только в присутствии специалиста. При наличии ходатайства законного владельца, который изымает электронные носители информации или обладателя содержащейся на них информации специалистом, который участвует в следственном деле, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации. Копирование информации производится также на другие электронные носители информации, которые предоставлены законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации. Копирование информации не реализовывается при наличии обстоятельств, прописанных в пункте 3 части первой статьи 164.1 УК РФ. Электронные носители ин-

[1] Сайт справочно-правовой системы Консультант Плюс URL:http://www.consultant.ru, Федеральный закон от 07.12.2011 № 420-ФЗ (ред. от 03.07.2016) " О внесение изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации Сайт справочно-правовой системы Консультант Плюс.

формации, которые содержат скопированную информацию, передаются законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, которые содержат скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается запись.[1]

Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации, согласно уголовно-процессуальному кодексу РФ. В протоколе следственного дела обязательно должны быть указаны технические средства, которые были применены при совершении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и обязательно полученные результаты. Также должны быть приложены электронные носители информации, которые содержат информацию, скопированную с других электронных устройств, содержащих информацию в процессе производства следственного действия.

Интерпол, приказ МВД России от 31.03.2012 № 305 (ред. от 14.02.2020) "Об утверждении Положения о Национальном центральном бюро Интерпола Министерства внутренних дел Российской Федерации", подразделяет все преступления в компьютерной практике на шесть основных групп: компьютерное мошенничество, компьютерный саботаж, незаконное копирование, изменение компьютерных данных, несанкционированный доступ и перехват, прочие компьютерные преступления.

Структура видов преступлений в сфере компьютерной информации, которая выделяется Европейской конвенцией.

Европейская конвенция, не ратифицированная Российской Федерацией, обозначает же иные виды таких преступлений: противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств, подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторского права и смежных прав, покушение, соучастие или подстрекательство к совершению преступления.

Сбор доказательств по преступлениям, которые совершаются с использованием современных коммуникационных приборов, устройств, таких как смартфон, планшет, ноутбук всё это входит в классификацию персональных компьютеров, а информация, снятая с данных устройств будет являться компьютерной информацией.

---

[1] Сайт справочно-правовой системы Консультант Плюс URL:http://www.consultant.ru, "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 19.12.2020); См.: Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26 - 28.

Для того, чтобы избежать наказание за совершенное преступление злоумышленники пытаются всевозможными способами избавиться от этой информации, например, стереть ее или же скрыть1. Чаще всего они применяют такие приёмы скрытия информации:

получение информации через локальную или глобальную сеть с помощью удаленного доступа (данный приём позволяет преступникам изменить или же скрыть данные на другом устройстве удаленно с помощью интернета);

пользование услугами сотовых операторов связи (в данном случае злоумышленники используют определенные сервера голосовой связи, которые способны защитить их разговоры и сделать доступными только для узкого круга лиц);

шифрование данных на электронном носителе информации (этот способ помогает защитить конфиденциальную информацию от несанкционированного доступа, например, прочтения, подмены или же искажения);

использование VPN2 (VPN представляет собой сервис, который помогает скрыть и зашифровать личные данные при использовании интернета, информацию о том, какие сайты были посещены в то или иное время);

использование анонимайзеров (анонимайзеры применяются для обеспечения конфиденциальности информации, а также с их помощью можно посещать заблокированные сайты в стране).

Изъятие электронных следов информации на любой стадии уголовного судопроизводства, а также в процессе оперативно-розыскных мероприятий запрещено сотрудниками правоохранительных органов, за исключением тех случаев, когда у правоохранительных органов есть основания полагать, что информация, содержащаяся на электронных носителях может подтолкнуть на совершение новых преступлений в сфере компьютерной информации, а также по решению суда. При это должны быть обеспечены все условия, для того, чтобы фиксация электронных следов, которые находятся в киберпространстве, производилась своевременно и правильно, так как злоумышленники могут суметь изменить или вовсе уничтожить их. Особенности изъятия электронных следов преступлений помогают сотрудникам правоохранительных органов предпринять эффективные следственные действия для разрешения дела. Следует постоянно совершенствоваться в методах работы с электронными следами, более подробно изучать их особенности, а также проводить исследовательские работы для того, чтобы избежать возникновения новых преступлений в сфере компьютерной информации.

Список используемых источников

1. Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2т. /А.В. Бриллиантов, Г.Д.// Там же – С.326

[1] Лебедева А.А. Компьютерные преступления и трудности формирования следственной и судебной практики// Журнал «Судья», №10.2020, октябрь С.36-40;

[2] VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет).

2. Лебедева А.А. Компьютерные преступления и трудности формирования следственной и судебной практики// Журнал «Судья», №10.2020, октябрь С.36-40;
3. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26 - 28.
4. Сайт справочно-правовой системы Консультант Плюс URL:http://www.consultant.ru, Федеральный закон от 07.12.2011 № 420-ФЗ (ред. от 03.07.2016) " О внесение изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации Сайт справочно-правовой системы Консультант Плюс

Д.Т. Кудайбергенова
Научный руководитель: **В.А. Мишенин**

Криминологические аспекты борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей

Аннотация. В данной статье рассматривается глобальная проблема преступности, совершаемой с использованием информационно-телекоммуникационных сетей. На основе анализа статистики преступлений, наиболее распространенных схем совершения преступлений в данной сфере и составления портрета киберпреступника предлагаются некоторые меры по предотвращению и профилактике преступлений в информационном пространстве.

Ключевые слова: киберпреступность; киберпреступление; высокие технологии, информационно-телекоммуникационная сеть; виртуальное пространство, портрет киберпреступника.

XXI век – это эпоха информационного общества, где компьютерные технологии охватывают все сферы жизни человека. Безусловно, компьютеризация значительно упростила жизнь, но вместе с тем породила и новые проблемы. Так, преступность переместилась в виртуальное пространство и в последние годы активно набирает обороты.

Киберпреступления обладают повышенной общественной опасностью, поскольку нарушают не только порядок правомерного использования сетевого пространства, но и затрагивают интересы и права человека, а также подрывают национальную безопасность Российской Федерации. Также данные преступления не имеют географических границ, совершаются с меньшими усилиями и большой скоростью, в отличии от традиционного преступления.

Киберпреступление – это действие, нарушающее закон, совершаемое с использованием информационно-коммуникационных технологий и либо нацеленное на веб-сайты, сети, системы, данные и/или технологии, либо способствующее совершению преступления.[1]

[1] Киберпреступность. Модуль 1. Введение киберпреступность. Организация Объединенных Наций, Вена, 2019. https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf

По статистике МВД России за январь-октябрь 2020 г. зарегистрировано 420,7 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий, что на 75,1% больше, чем за аналогичный период 2019 г.[1] Причем удельный вес от общего числа зарегистрированных преступлений составил 24,2% (в 2019 г. – 14%). Среди них более половины, а именно 51,4% относятся к категории тяжких и особо тяжких преступлений.

Данные преступления чаще всего совершаются в сети «Интернет» (57,9%), остальные (42,1%) с помощью мобильной связи.

Стоит отметить резкий рост указанных категорий преступлений, т.к. по сравнению с аналогичным периодом прошлого года количество тяжких и особо тяжких преступлений с использованием информационно-телекоммуникационных технологий увеличился на 84,9%,

По данным МВД за январь-октябрь 2020 г. наибольший прирост преступности в сфере компьютерной информации наблюдается в Санкт-Петербурге (581,8%), при этом наибольший удельный вес в структуре преступности отмечается в таких регионах, как Ямало-Ненецкий автономный округ (38,8%), Ханты-Мансийский автономный округ (38,7%) и Чувашская республика (36,6%).

Появление преступлений в сфере компьютерной информации связывают с появлением «хакеров». Хакеры – это люди, которые занимаются поиском незаконных способов получения несанкционированного доступа к средствам компьютерной техники и данным в совокупности с их несанкционированным использованием в корыстных целях.[2] Хакеры делятся на «хороших» (белых), которые ищут и устраняют уязвимости в информационных сетях, и «плохих» (черных), которые используют уязвимые места системы в корыстных целях.

Представляется возможным составить портрет хакера – это люди в возрасте от 14 до 45 лет (подчас школьники и студенты), которые увлекаются компьютерной техникой и могут проводить за компьютером по 12-16 часов в день. Как правило, это творческие люди, знающие языки программирования и особенности операционных систем. Большое количество представителей молодого поколения среди киберпреступников объясняется тем, что навык владения компьютером они получают еще в раннем возрасте.

Также отмечается, что данный вид преступлений совершается мужчинами в 5 раз чаще, чем представителями женского пола.

Большинство из этих людей имеет высшее или неоконченное высшее образование. В трудовой деятельности они отличаются работоспособностью, первыми приходят на работу и последними уходят, часто задерживаются на рабочем месте, почти не используют отпуск.

---

[1] Состояние преступности в России за январь – октябрь 2020 года // Министерство Внутренних Дел Российской Федерации ФКУ «Главный Информационно – аналитический центр», Москва. 2020 г.

[2] Волчинская Е.К. Защита персональных данных: Опыт правового регулирования. М.: Галерея, 2001. 236 с.

Основным криминогенным фактором психологического характера является возможность полной анонимности при совершении преступлений. В виртуальном пространстве он живет еще одной жизнью, что позволяет создавать новый образ.

Эксперты-бихевиористы отмечают, что у данной категории людей часто встречаются психические отклонения такие, как психоз, расстройства личности, интернет-зависимость.

Среди мотивов преобладает корыстный; меньше преступлений совершаются из-за фанатизма, изобретательности или психического заболевания, мании.

На ежегодном саммите по кибербезопасности Всемирного экономического форума (ВЭФ) Annual Meeting on Cybersecurity 2020 спикеры отметили, что киберпреступность во время кризисной ситуации увеличилась во всем мире. По оценкам Сбера, ущерб российской экономике от киберпреступности в 2020 г. составит $44 млрд. (3,5 трлн рублей), а в 2021 г. эта сумма может удвоиться.

Анализ статистики преступности, совершаемой с использованием информационно-коммуникационных сетей, составление портрета киберпреступника и изучение практики позволяют разработать необходимые меры по профилактике преступлений в сфере компьютерных технологий.

Для обычных интернет-пользователей могут быть предложены следующие рекомендации:

- Использовать сложные пароли и периодически менять их;
- Не использовать одинаковые пароли;
- Не сохранять пароли в браузерах, особенно если заходить в аккаунт через чужой компьютер;
- Не регистрироваться на подозрительных сайтах;
- Использовать антивирусное программное обеспечение и обновлять его;
- Не заходить на подозрительные сайты, устанавливать приложения только из проверенных источников.

Держателям банковских карт необходимо:

- Не передавать банковскую карту и ее реквизиты третьим лицам, в том числе в Интернет-переписках и по телефону;
- Использовать отдельную банковскую карту для Интернет-покупок и не хранить на ней деньги;
- Не хранить ПИН-код рядом с банковской картой;
- Перезванивать лично в свой банк в случае поступления звонка сотрудников банка с сообщением о несанкционированных операциях (обычно звонок является бесплатным);
- Установить СМС-оповещение на телефон в целях отслеживания всех операций с банковской карты и возможности её своевременного блокирования в случае поступления информации о подозрительных действиях;
- Не доверять сайтам, где нужно вносить предоплату для получения товара или услуги.

На национальном уровне:

- На регулярной основе проводить образовательные курсы по повышению киберграмотности населения, особенно пожилых людей;
- Осуществить переподготовку сотрудников правоохранительных органов с целью обучения и формирования квалифицированных кадров в борьбе с преступностью в сфере высоких технологий;
- Разработать и внедрить новые средства для борьбы с преступлениями в информационном пространстве;
- В кредитно-финансовых организациях регулярно обновлять защитную систему.

Таким образом, нужно сделать еще многое, чтобы защитить общество от преступлений в виртуальном пространстве.

Вместе с тем, нужно отметить, что первые шаги по достижению данной цели уже делаются. Так, в июле 2020 года Председателем Следственного комитета России А.И. Бастрыкиным было проведено оперативное совещании, посвященное киберпреступности. Учитывая тенденции роста киберпреступности в стране в Следственном комитете был создан специализированный отдел по расследованию преступлений, совершенных с использованием высоких технологий. По мнению А.И. Бастрыкина, это подразделение должно "стать площадкой, объединяющей усилия различных государственных ведомств, научных учреждений и специалистов для эффективного и слаженного противодействия преступным явлениям в информационной сфере"[1].

Среди мер, направленных на повышение эффективности борьбы в информационном пространстве также была отмечена и качественная корректировка уголовного и уголовно-процессуального законодательства государства.

Список использованных источников

1. Волчинская Е.К. Защита персональных данных: Опыт правового регулирования/Е.К. Волчинская. - Москва: Галерея, 2001. 236 с.
2. Киберпреступность. Модуль 1. Введение киберпреступность. Организация Объединенных Наций, Вена, 2019. https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf
3. Козлова Н. По ту сторону монитора. Александр Бастрыкин: за год уровень киберпреступности вырос более, чем вдвое // Российская газета, 10 июля 2020 года.
4. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений/А.А. Протасевич, Л.П. Зверянская// Российский следователь. - 2013. -№11. -С. 45-47.
5. Состояние преступности в России за январь – октябрь 2020 года // Министерство Внутренних Дел Российской Федерации ФКУ «Главный Информационно–аналитический центр», Москва. 2020 г.

[1] Козлова Н. По ту сторону монитора. Александр Бастрыкин: за год уровень киберпреступности вырос более, чем вдвое // Российская газета, 10 июля 2020 года

С.О. Ламыкина
П.В. Сочка
Научный руководитель: **В.А. Мишенин**

Противодействие киберпреступлениям в банковской сфере РФ с применением специальных знаний в области компьютерной техники

Аннотация. В данной статье рассматривается понятие «киберпреступность» и его нормативное закрепление. Авторы приводят международную типологию компьютерных преступлений. Основная часть данной статьи посвящена рассмотрению наиболее распространенных типов кибератак, и мерам их предупреждения, которые содержат специальные знания в области компьютерной техники и информатики.

Ключевые слова: кибератака, киберпреступление, кибербезопасность, кредитно-финансовые организации, специальные знания компьютерной техники, меры предупреждения, информационная система.

Период пандемии 2020 года был ознаменовал резким ростом киберпреступности. В первую очередь способами совершения таких преступлений являлись: «социальная инженерия» (получение нужной информации при помощи манипуляции или обмана), вредоносные рассылки, выбор новых участников преступных сообществ.

Проблема роста киберпреступности является международной. Ее обсуждают на уровне таких международных организаций как: ООН, Совет Европы, Интерпол, Европол, правоохранительные органы государств (в рамках международного сотрудничества). Опасность данных видов преступлений состоит в том, что за максимально короткий промежуток времени удается совершить незаконный перевод крупной суммы денег, размер которых, подчас, может составлять миллиарды долларов. Ежегодные убытки мировой экономики от кибератак составляют 1 триллион долларов, а ущерб Российской Федерации достигает более 600 миллиардов рублей (0,64% ВВП РФ).[1]

В официальном ежегодном отчете о киберпреступности за 2019 год, опубликованном главным исследователем «Cybersecurity Ventures», сообщается, что атаки хакеров во всём мире происходят каждые 14 секунд, а к 2021 году их частота возрастёт до каждой 11 секунды. Киберпреступления в будущем десятилетии станут одной из самых острых проблем. «Cybersecurity Ventures» приводит данные о том, что к 2021 году ущерб от киберпреступности будет стоить миру 6 триллионов долларов в год (больше, чем от глобальных катастроф). [2]

Понятие «киберпреступность» нормативно не закреплено, однако, на десятом конгрессе ООН, посвященном вопросам по предупреждению преступности и об-

---

[1] Семеко Г.В. Информационная безопасность в финансовом секторе: Киберпреступность и стратегия противодействия// Социальные новации и социальные науки.- Москва: ИНИОН РАН, 2020.- №1 – С.77-96.

[2] [Электронный ресурс]URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (Дата обращения 09.12.2020)

ращению с правонарушителями, киберпреступность была определена как совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных.[1]

В Конвенции о преступности в сфере компьютерной информации 2001 года (ст. ст. 2-5) закреплены четыре основных типа компьютерных преступлений. К ним относятся:

1) противозаконный умышленный доступ к компьютерной системе либо ее части;

2) противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах;

3) противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных;

4) серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных.[2]

Наиболее подверженной кибератакам является банковская сфера, так как в ней осуществляется огромное количество транзакций и оборот денежных средств.

Для противодействия и профилактики данных преступлений необходимо принятие общих мер и применение специальных знаний.

По данным Генеральной прокуратуры РФ, один из пяти случаев кражи в России связан с банковскими счетами - прежде всего, звонки от фальшивой службы безопасности. По итогам января – августа 2020 года было выявлено 107200 хищений. Это вдвое больше прошлогодних показателей. Раскрывается лишь 8% таких преступлений.[3]

В 2019 г. объем всех операций, совершенных без согласия клиентов с использованием интернет-банкинга, составил 6426,5 млн рублей. Количество таких операций – 576 566 единиц. Средняя сумма одной такой операции по счетам физических лиц составила 10 тыс. руб., юридических лиц – 152 тыс. рублей.[4]

69% всех операций без согласия клиентов было совершено в результате побуждения клиентов к самостоятельному проведению операции путем обмана

---

[1] Доклад десятого конгресса ООН по предупреждению преступности и обращению с правонарушителями 2000г// URL: https://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (дата обращения 28.11.2020)

[2] Сомик К.В., Насибов М.З. Организация противодействия киберпреступлениям в банковской сфере. // Юридическая наука: история и современность. - 2018, № 8. С. 160-164.

[3] [Электронный ресурс] URL: http://crimestat.ru/ (Дата обращения 09.12.2020)

[4] [Электронный ресурс] URL: https://cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (Дата обращения 09.12.2020)

или злоупотребления доверием (методами так называемой социальной инженерии).

Применение конкретных специальных знаний напрямую связано с типом атаки. К основным атакам можно отнести: целевые, на клиентов кредитных организаций, на устройства самообслуживания.[1]

1. Под целевой атакой понимают проникновение в информационную систему с помощью дистанционного управления зараженными компьютерами с целью сбора информации об организации (пароли, документы и т.д.). В начале на электронную почту приходит письмо, содержащее в себе ссылку на вредоносную программу, проходя по ней, она автоматически устанавливается на компьютер. После этого «атакующий» получает удаленный доступ к компьютеру. В процессе изучения данных, имеющихся на зараженном компьютере, «атакующий» стремится найти и получить доступ к серверу, с помощью которого осуществляется централизованное управление. Как только он получит доступ к такому «контролеру», то следующим его шагом становится нахождение подсети банкоматов. Если «атакующий» получает доступ к подсети банкоматов, он устанавливает программу, обеспечивающую выдачу денежных средств по заданной команде. В это время привлекаются соучастники, которые должны находиться в конкретное время рядом с банкоматом для получения денежных средств.

Примером подобной атаки может служить преступление, произошедшее в июле 2016 года в Тайване. К банкомату First Bank пришел мужчина в маске. Затем он совершил звонок неизвестному лицу и банкомат в следующие несколько секунд выдал ему все наличные деньги. Тоже самое происходило у четырех десятков других банкоматов First Bank - преступники выпотрошили их почти на $2,2 млн и скрылись.[2]

Организационными мерами предупреждения целевой атаки являются систематическое повышение знаний сотрудников в области информационной безопасности, проведение их тренинга, например, с применением «ложной» рассылки писем с вредоносными программами.

Техническими мерами предупреждения являются обновление антивирусной базы, установка на банкомат программного обеспечения, предотвращающего несанкционированный запуск вредоносных программ.

2. Под атакой клиентов кредитных организаций понимаются действия, состоящие в подмене платежных поручений на стадии их передачи из бухгалтерской системы в систему дистанционного банковского обслуживания. Главным предметом такой атаки является файл «экспорта-импорта», который первоначально формируется клиентом, именно он заполняет все необходимые реквизиты платежного поручения. После произведения указанных действий клиент направляет этот файл в систему дистанционного банковского обслуживания (ДБО).

---

[1] Основные типы атак в кредитно-финансовой сфере в 2017 году. Банк России Финцентр.// URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (дата обращения 28.11.2020)

[2] [Электронный ресурс] URL: https://www.group-ib.ru/blog/polygon (Дата обращения 09.12.2020)

Вредоносная программа при данном типе атаки, обнаруживая такой файл, вносит в него изменения, а именно: подменяет банковский идентификационный код (БИК), номер счета и ИНН получателя. Суммы платежных переводов в большинстве случаев не менялись. Так, в системе ДБО клиент получал уже измененные платежные поручения и, не просматривая их содержание, отправлял на обработку.

В большинстве случаев такая вредоносная программа могла быть установлена либо при посещении взломанных бухгалтерских и финансовых сайтов, на которых размещались коды, инициирующие загрузку вредоносной программы, либо при помощи спам-рассылок по электронной почте.

Так, в феврале 2016 хакеры попытались похитить из Центрального банка Бангладеш $951 млн через систему международных межбанковских переводов SWIFT. Из-за ошибки в платежном документе им удалось украсть только $81 млн.[1]

При данном типе атаке меры предупреждения должны быть предприняты как со стороны клиента, так и со стороны организации.

Клиент должен иметь на своем техническом устройстве антивирусную программу, которая требует постоянного обновления; при помощи данной программы необходимо проводить проверку системы не реже одного раза в неделю. Клиенту рекомендуется не открывать файлы, если нет уверенности в надежности отправителя; проверять реквизиты платежных поручений; периодически менять наименование файла с платежным поручением.

Организации необходимо настроить систему мониторинга - антифрод, которая предупреждает клиента о проведении сомнительных операций, а также оповещать своих клиентов о данном типе атаки.

3. Атаки на устройства самообслуживания. Данный тип атак включает в себя как физическое подключение к внутреннему устройству банкомата, так и удаленное управление. Для такой атаки характерно участие двух лиц: организатора и исполнителя. Организатор снабжает исполнителя необходимым «переходником» и осуществляет дистанционное управление банкоматом, а исполнитель выбирает конкретный банкомат, подключает к нему компьютер с вредоносными программами, обеспечивающими выполнение команды на выдачу имеющихся купюр.

В 2015 году у компании «The Ubiquiti Networks» украли 40 миллионов долларов. При этом не были взломаны операционные системы. В похищении денег виноваты сами сотрудники. Мошенники прислали электронное письмо от имени топ-менеджера компании. Они попросили, чтобы финансисты перевели определенную сумму денег на специальный банковский счёт. И без проверки имени отправителя деньги были переведены.[2]

Мерами предупреждения совершения подобной атаки являются:

---

[1] [Электронный ресурс]URL: https://www.group-ib.ru/blog/polygon (Дата обращения 09.12.2020)

[2] [Электронный ресурс]URL: https://www.group-ib.ru/blog/polygon (Дата обращения 09.12.2020)

- создание «белого» списка программ и приложений;
- установка средств физической защиты от внешнего подключения к USB-портам;
- установка запрета в системе банкомата на подключение сторонних устройств к USB- портам;
- перевод устройства для выдачи денежных купюр в защищенный режим работы.

Лучшее противодействие кибератаке - это выявление и пресечение попытки взлома системы безопасности организации и клиента.

Несмотря на видовое разнообразие и постоянно появление новых атак, можно выделить наиболее общие меры предупреждения, которые обеспечат безопасность различных технических устройств банковского сектора:

1. Установка и своевременное обновление антивирусного обеспечения.
2. Установка программного обеспечения, предотвращающего несанкционированный запуск сторонних программ.
3. Проверка на индикаторы компрометации, то есть для обнаружения вредоносной активности.
4. Не допускать запуск файла, вызывающий сомнения в источнике происхождения.

Говоря об обеспечении глобальной кибербезопасности, необходимо:

1. Взаимодействие государств и международных организаций, целью деятельности которых является противодействие киберпреступности.
2. Сотрудничество банковских организаций и производителей антивирусного ПО.
3. Учреждение в каждой банковской организации специализированных отделов по обеспечению кибербезопасности.
4. Повышение финансовой грамотности населения, распространение среди граждан индивидуальных методов и способов защиты персональной информации. [1]

Перечисленные меры позволят значительно сократить количество совершаемых киберпреступлений.

[1] Дементьева М.А., Лихачева В.В., Козырев Т.Г. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия // Экономические отношения. – 2019. – Том 9. – № 2. – С. 1009-1020.

Список использованных источников

1. Доклад десятого конгресса ООН по предупреждению преступности и обращению с правонарушителями 2000 г. - URL: https://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml (дата обращения 28.11.2020).
2. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.). – URL: https://base.garant.ru/4089723/ (дата обращения: 28.11.2020).
3. Дементьева М.А., Козырев Т.Г., Лихачева В.В. Киберпреступления в банковской сфере российской федерации: способы выявления и противодействия. Экономические отношения, 2019, № 2 (9). С. 1009 – 1020 – URL: https://elibrary.ru/item.asp?id=39191641 (дата обращения: 28.11.2020).
4. Киберпреступность. 1. Введение в киберпреступность. ООН. Вена, 2019 – URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_1_Introduction_to_Cybercrime_RU.pdf (дата обращения: 28.11.2020).
5. Основные типы атак в кредитно-финансовой сфере в 2017 году. Банк России Финцентр. - URL: https://cbr.ru/Content/Document/File/72724/DIB_2018_20190704.pdf (дата обращения 28.11.2020).
6. Семеко Г.В. Информационная безопасность в финансовом секторе: Киберпреступность и стратегия противодействия. Социальные новации и социальные науки. Москва: ИНИОН РАН, 2020, №1. С.77-96. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-finansovom-sektore-kiberprestupnost-i-strategiya-protivodeystviya (дата обращения: 28.11.2020).
7. Сомик К.В., Насибов М.З. Организация противодействия киберпреступлениям в банковской сфере. Юридическая наука: история и современность, 2018, № 8. С. 160-164. – URL: https://elibrary.ru/item.asp?id=37242884 (дата обращения: 28.11.2020).

И.Ю. Лупандина
Научный руководитель: **Савин П.Т.**

Криптовалюта как средство совершения преступлений

Аннотация. В данной статье анализируется правовой статус криптовалют в России, рассматривается уголовно-правовой аспект данного явления. Автор приходит к выводу, что законодателю необходимо предусмотреть использование криптовалюты в качестве квалифицирующего признака для ряда статей УК РФ.

Ключевые слова: информационно-телекоммуникационные сети, криптовалюта; преступность; киберпреступления.

В настоящее время в Российской Федерации актуальной проблемой является противодействие преступлениям, совершаемым с использованием информаци-

онно-коммуникационных технологий, к которым согласно позиции Е.А. Русскевича следует относить все общественно опасные деяния, совершаемые полностью или частично в виртуальном пространстве посредством использования информационно-коммуникационных технологий[1]. Согласно статистическим данным представленным МВД фиксируется резкое увеличение количества IT-преступлений в 2020 году. Нарушений закона с использованием интернета стало больше на 91%, а при помощи мобильных телефонов — на 88%. Число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети Интернет – на 91,3%, при помощи средств мобильной связи – на 88,3%[2]. При этом необходимо в данном случае обратить внимание, что в целом с 2013 года уровень преступности в сфере информационных технологий возрос более чем в 20 раз и продолжает увеличиваться. Сегодня каждое седьмое преступление в России совершается с помощью информационных технологий или в киберпространстве[3]. Кроме того, согласно позиции руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России К.П. Комарды по делам о заказных убийствах было установлено использование одной из криптовалют в качестве средства платежа. Когда речь идет о конвертации криптовалюты в реальные денежные средства, преступниками используются сотни электронных кошельков, оформленных на посторонних лиц[4]. Таким образом, актуальным в правоприменительной практике является использование криптовалюты, как средства совершения преступления.

В соответствии с Конвенцией против транснациональной организованной преступности под имуществом понимаются «любые активы, будь то материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них»[5].

В настоящее время в уголовно-правовой науке отсутствует единое мнение о понимании содержания термина «иное имущество». При этом, согласно Постановлению Пленума Верховного суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных

---

[1] Русскевич Е.А. Преступления, совершаемые с использованием информационно-коммуникационных технологий: результат интерпретации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1(4). С. 101–106.

[2] МВД: увеличение числа киберпреступлений повлияло на рост тяжких преступлений в 2020 году. URL: https://tass.ru/obschestvo/10505371.

[3] Интервью руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России Константина Комарды ИА «ТАСС». URL: https://sledcom.ru/press/interview/item/1529946.

[4] Там же.

[5] Конвенция против транснациональной организованной преступности // СЗ РФ. 2004. № 40. Ст. 3882.

средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»[1] под имуществом предлагает понимать движимое и недвижимое имущество, имущественные права, документарные и бездокументарные ценные бумаги. Анализ данной формулировки позволяет сделать вывод, что она является общей и не раскрывает признаки и состав иного имущества. По нашему мнению, вопрос, связанный с правовым регулированием гражданско-правового оборота криптовалют и вопрос о ней как о средстве совершения преступлений должен решаться автономно, не подменяя друг друга и не ставя во взаимную зависимость. В данном случае необходимо обратить внимание на позицию В.В. Хилюты, который считает, что уголовное право охраняет фактически сложившиеся общественные отношения независимо от того, успели ли цивилисты придумать для них соответствующие конструкции[2].

Проводя изучение криптовалюты как средства совершения преступления, необходимо обратить внимание, что владение и распоряжение криптовалютой является анонимным процессом, который исключает идентификацию личности, в результате чего она используется для приобретения запрещенных или ограниченных в обороте предметов, таких как оружие, боеприпасы, наркотические и психотропные вещества. Необходимо отметить, что указанные виртуальные «магазины» уже неоднократно становились предметом исследования как российских, так и зарубежных криминологов. В качестве примера, необходимо обратить внимание на приговор Петропавловско-Камчатского городского суда Камчатского края по уголовному делу № 11901300001001393 по обвинению Хисматовой А.А. в совершении преступлений, предусмотренных ч. 3 ст. 30, п.п. «а», «г» ч. 4 ст. 228.1, п. «а» ч. 4 ст. 174.1 УК РФ. Согласно разработанной схеме незаконный сбыт наркотических средств должен был происходить посредством переписки с покупателями в сети «Интернет», а также с использованием различных Интернет-мессенджеров, в том числе «Телеграм», перевода покупателями денежных средств в счет приобретения наркотических средств с использованием обменных сервисов и криптовалютных бирж для перечисления виртуальных активов (криптовалюты – Биткоин) на открытые участниками организованной группы биткоин-кошельки и электронной платежной системы Виза Киви Валлет на используемые членами преступной группы счета[3].

Вместе с тем, необходимо отметить, что криптовалюта также может стать средством совершения преступлений террористической направленности, в частности преступления, предусмотренного ст. 205.1 УК РФ, преступлений против

---

[1] Постановлению Пленума Верховного суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Доступ из СПС КонсультантПлюс.

[2] Хилюта В.В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) / В.В. Хилюта // Библиотека уголовного права и криминологии. 2018. № 2 (26). С. 58–68.

[3] Приговор Петропавловско-Камчатского городского суда Камчатского края по уголовному делу № 11901300001001393. URL: https://sudact.ru/regular/doc/usNB6aTcmgHQ.

здоровья населения и общественной нравственности и иных. Было бы неразумным отрицать такой подход, основываясь только на том, что правовой статус криптовалют не определен. В данном случае, по нашему мнению не должна иметь значение характеристика инструмента, которым лицо финансировало совершение преступлений террористической направленности, за счет которого приобретало наркотические средства и т.д., важен результат, который закреплен в конкретном составе преступления.

Таким образом, в каждом из перечисленных случаев криптовалюта используется либо для непосредственного достижения преступного результата (например, при приобретении запрещенных предметов), либо для облегчения совершения преступления. Зачастую имеет место так называемая трансформация: за счет денежных средств, полученных преступным путем, приобретается криптовалюта, которая в дальнейшем вполне легально на обменных биржах меняется на чистые деньги. Вместе с тем, считаем, что в связи с развитием общественных отношений и появлением новых средств платежа, которые усложняют раскрытие и расследование преступных деяний, законодателю необходимо внести соответствующие изменения в УК РФ, в части квалифицирующего признака ряду статей, как посредством использования криптовалюты, что позволит создать правовую регламентацию противодействия в цифровой среде.

Список использованных источников

1. Интервью руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России Константина Комарды ИА "ТАСС". URL: https://sledcom.ru/press/interview/item/1529946.
2. Конвенция против транснациональной организованной преступности // СЗ РФ. 2004. № 40. Ст. 3882.
3. МВД: увеличение числа киберпреступлений повлияло на рост тяжких преступлений в 2020 году. URL: https://tass.ru/obschestvo/10505371.
4. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Доступ из СПС КонсультантПлюс.
5. Приговор Петропавловско-Камчатского городского суда Камчатского края по уголовному делу № 11901300001001393. URL: https://sudact.ru/regular/doc/usNB6aTcmgHQ.
6. Русскевич Е.А. Преступления, совершаемые с использованием информационно-коммуникационных технологий: результат интерпретации // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2018. № 1(4). С. 101–106.
7. Хилюта В.В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) / В.В. Хилюта // Библиотека уголовного права и криминологии. 2018. № 2 (26). С. 58–68.

Э.Г. Мартынюк
Научный руководитель: **В.А. Перов**

К вопросу об использовании знаний в области криптовалюты и технологии блокчейн в целях выявления, раскрытия, расследования и предупреждения киберпреступлений

Аннотация. Криптовалюта не так давно стала важным элементом общественного развития и заручилась повышенным вниманием со стороны не только честной части общества, но и со стороны контингента, старающегося обойти закон. Это обусловлено отсутствием крепкой и проверенной временем системы нормативно-правовой базы ввиду новшества киберденег. В данной статье освещены базовые знания, которыми должен обладать современный следователь для выявления, раскрытия, расследования и предупреждения киберпреступлений, связанный с использованием криптовалюты.

Ключевые слова: криптовалюта, блокчейн, киберпреступления, финансы, следователь, знания, общество, деньги, цифровая валюта, правоохранительные органы.

Криптовалюта – неотъемлемая часть общества, важная составляющая на пути общественного прогресса, неразрывно связанная с технологией блокчейн. На данном этапе нормативно не закреплены определения вышеназванных категорий, но взгляды специалистов на определения в сфере электронных финансов схожи[1].

Под криптовалютой понимаются: 1) виртуальные деньги, генерирующиеся в сети и не имеющие физического выражения; 2) цифровая валюта, операции с которой осуществляет децентрализованная платёжная система. В свою очередь, под технологией блокчейн понимается непрерывная последовательная цепочка блоков, каждый блок которого содержит информацию (ключ, хеш-сумму, нонс) из предыдущего блока.

Не согласиться с вышеописанными категориями сложно, в связи с отсутствием их нормативно-правового закрепления. Опираясь на определения, можно только сформулировать более точные характеристики этих понятий. Криптовалюта – это математический код, генерирущийся посредством майнеров в сети Интернет в виде последовательной цепочки блоков (блокчейн) и выраженный в определённой последовательности цифр, а также обеспеченный, как и физические деньги, доверием людей к нему. Нет доверия людей – нет поддержки и развития криптовалюты, как и бумажных денег в целом. Блокчейн же – это непрерывная последовательная цепочка блоков, каждый блок которого содержит информацию (ключ, хеш-сумму, нонс и др.) из предыдущего блока, что затрудняет подделку математического кода.

Казалось бы, зачем знания в области криптовалюты и технологии блокчейн нужны следователю? Как известно, половина ответа на вопрос содержится в са-

[1] Перов В.А. Научная работа [Электронный ресурс] // Криптовалюта как объект гражданского права: [elibrary.ru]. 2017. URL: https://elibrary.ru/item.asp?id=29911537. (Дата обращения: 03.02.2021).

мом вопросе. Общество развивается, совершенствуется, движется по восходящей, поэтому *современный* следователь обязан вникать во все нововведения, начиная с аграрной промышленности, заканчивая космическими исследованиями. В среде криптовалюты и технологии блокчейн предостаточно возможных преступных схем и махинаций.

Обусловлено это, повторюсь, отсутствием нормативно-правовой базы, а также новшеством киберденег[1]. Всё новое не может быть идеально с самого начала, для закалки требуется долгий процесс проб и ошибок, что и используют в преступных целях злоумышленники.

Говоря о знаниях, необходимых в области криптовалюты и технологии блокчейн, можно выделить следующие аспекты, которыми должен обладать современный следователь для успешного расследования киберпреступлений:

Базовые аспекты:

1) Владение специальным терминологическим аппаратом: сюда входят такие понятия как блокчейн, криптовалюта, майнинг, P2P торговля, фиат, маржинальная торговля, кредитное плечо, дериативы, фьючерсы, ордера, стоп-лимит и др. производные и непроизводные, но смежные, категории;

2) Знание простейших базовых операций, пути их осуществления: покупка/продажа криптовалюты/фиатных активов, регистрация профиля на бирже, виды бирж, стратегии майнинга[2];

3) Опыт в расследовании киберпреступлений.

Специальные (продвинутые) аспекты:

1) Изучение поведения рынка при разных обстоятельствах: покупка/продажа криптоактивов, падение/повышение спроса, рост «свечей» и др.;

2) Изучение функционирования обменников криптовалюты: BetaTransfers, AllWMCash, Шахта и др.;

3) Знания о функционировании различных биржевых видов торговли: конвертация, классическая, продвинутая, маржа, P2P;

4) Владение специальными инструментами в цифровой торговле: Аллигатор Билла Вильямса, Индекс массы, объём, глубина, VWAP, RSI Коннора и др.;

5) Знания о работе способов торговли: Лимит, Маркет, Стоп-Лимит.

6) Мониторинг криптоактивов в данный момент времени;

7) Опыт в расследовании киберпреступлений и экономических преступлений.

От обладания базовыми/продвинутыми аспектами будет зависеть частота и качество раскрытия киберпреступлений. Следователь, обладающий базовыми знаниями, не сможет выявить те преступные схемы, которые сможет выявить следователь, обладающий продвинутыми знаниями в области криптовалюты и технологии блокчейн.

---

[1] Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. №10. С. 109-115.

[2] Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь. 2018. №2. С. 8-11.

Касаемо киберпреступлений, которые могут возникнуть на почве цифровой валюты и которые квалифицируются по Особенной части УК РФ, можно выделить следующие – регулируемые и не регулируемые УК РФ:

Регулируемые УК РФ:

- В связи с тем, что любой желающий может стать добытчиком (майнером) криптовалюты, может возникнуть неконтролируемая инфляция, что, в свою очередь, приведёт к махинациям с обесцененной валютой (взяточничество – ст. 290, ст. 291 УК РФ; перевод средств посредством подложных документов – ст. 193.1 УК РФ; невозврат из-за рубежа денег в иностранной валюте – ст. 193 УК РФ), как это произошло в 1990-ых годах, и, как итог, новые долларовые миллионеры по всему миру[1];
- Кражи криптовалюты, фиатных активов – ст. 158 УК РФ[2];
- Частые хакерские атаки (неправомерный доступ к компьютерной информации – ст. 272 УК РФ)[3];
- Легализация (отмывание) денежных средств – ст. 174 УК РФ[4];
- Спонсирование радикально настроенных слоёв населения: террористические организации, преступные сообщества и др. – ст. 33 УК РФ, ст. 205.1 УК РФ[5];
- Подделка криптовалюты (денег) – ст. 186 УК РФ[6];
- Манипулирование рынком – ст. 185.3 УК РФ[7].

Не регулируемые УК РФ:

- Гиперконцентрация денежных средств в преступных целях;
- Неконтролируемая эмиссия со стороны лица/компании в преступных целях;
- Сведения о владельце кошелька отсутствуют, есть только номер кошелька. Другими словами, непонятно кто может совершать преступления, оставаясь безнаказанным.

Резюмируя всё вышесказанное, стоит отметить тот факт, что криптовалюта и технология блокчейн – потенциальное финансовое будущее планеты, но стоит подходить к рассмотрению и применению категорий с умом, ведь пока не существует нормативно-правовой базы, регулирующей криптовалюту и технологию блокчейн. Современному следователю следует серьёзно заняться рассмотрением вопроса об изучении вышеописанных категорий, ведь преступная среда развивается прямо пропорционально правовому полю как в количественных, так и в качественных величинах.

---

[1] Уголовный кодекс Российской Федерации. – Москва: Проспект, 2020. – С. 147-148, 253-255.
[2] Там же. С. 104.
[3] Там же. С. 236.
[4] Там же. С. 128.
[5] Там же. С. 16, 167.
[6] Там же. С. 143.
[7] Там же. С. 139.

Список использованных источников

1. Уголовный кодекс Российской Федерации. – Москва: Проспект, 2020. – 320 с.;
2. Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь. 2018. №2. С. 8-11;
3. Перов В.А. Научная работа [Электронный ресурс] // Криптовалюта как объект гражданского права: [elibrary.ru]. 2017. URL: https://elibrary.ru/item.asp?id=29911537;
4. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. №10. С. 109-115.

Е. И. Некипелова
Научный руководитель: **А. А. Лебедева**

Электронные следы и способы их изъятия

Аннотация. Статья посвящена анализу проблем изъятия электронных следов преступлений. Вследствие трансформации современного общества, развития информационных технологий, всё чаще совершаются киберпреступления, это вызывает необходимость реформирования уголовно-процессуальной деятельности для эффективного предупреждения и расследования новых видов преступлений. В данной статье подробно раскрыто понятие электронных следов преступления, проанализированы способы их изъятия (наиболее известные аналитические комплексы). Исследование данной проблематики произведено на основе анализа судебной практики и изучения научной литературы. Предложенная информация и выводы могут быть использованы в качестве основы для дальнейших научных исследований.

Ключевые слова: электронные следы, киберпреступления, доказательства, электронные носители, криминалистика, изъятие, расследование.

В современном мире происходит стремительное развитие информационных технологий. За последние 7 лет уровень киберпреступности увеличился в 20 раз и продолжает расти.[1] Анализ статистических данных показал, что только за 2020 год преступления с использованием IT-технологий выросли на 94,6%.[2] Вследствие пандемии COVID-19 общий уровень преступности в стране остаётся неизменным, однако статистика киберпреступлений растет.

---

[1] См.: интервью начальника отдела по расследованию киберпреступлений СК России п/п юстиции К.П. Комарды // URL//https://sledcom.ru/press/interview/item/1529946. (Дата обращения 25.01.2021г.); Лебедева А. А. Борьба с киберпреступлениями – новая функция Следственного комитета России Противодействие киберпреступности: современное состояние и пути повышения эффективности: сборник статей / Следств. ком. Респ. Беларусь; редкол.: С. Я. Аземша (гл. ред.) [и др.]. – Минск: ЮрСпектр, 2020. – 322с., с. 179-183.

[2] См.: Информационно-аналитический журнал «Рубеж» // URL//https://rubezh.ru/gossektor/news/20/12/02/chislo-kiberprestuplenij-v-rossii-vyiroslo-na-946-proczentov-za. (Дата обращения: 25.01.2021г.)

Научный прогресс не стоит на месте, и правоохранительным органам приходится подстраиваться под сложную систему развития современного общества. Именно из-за такой тенденции в Следственном комитете Российской Федерации было создано новое специализированное подразделение по борьбе с киберпреступностью. Свою деятельность оно стало осуществлять с 19 декабря 2019 года. Данное нововведение было вызвано тем, что злоумышленники всё чаще прибегают к использованию узконаправленных знаний и навыков, вредоносных программ и шифровке данных в целях получения несанкционированного доступа к банковским счетам, вымогательства денежных средств, мошенничества и т. п. Следует с особой осторожностью осуществлять сбор электронных следов, чтобы избежать потери необходимой информации.

Электронно-цифровые следы по мнению В.Б. Вехова представляют собой любую криминалистически значимую компьютерную информацию, т. е. сведения (сообщения, данные), находящиеся в электронно-цифровой форме, зафиксированные на материальном носителе с помощью электромагнитных взаимодействий либо передающиеся по каналам связи посредством электромагнитных сигналов.[1] На данный момент в научной литературе нет единой трактовки понятия «электронные следы», а также отсутствует единое название этого следа. Ряд ученых оперирует понятием «информационный след» (В. В. Борисов, Г. М. Шаповалова), другие придерживаются названия «электронно-цифровой след» (В.Б. Вехов, В. В. Поляков), дискуссионным остается такое понятие, как «виртуальный след» (В. А. Мещеряков, А. Б. Смушкин).[2] К информационным следам можно отнести: коды, подобранные пароли, лог-файлы отчетов и журналов операционной системы, специальные программы. Однако идентифицировать владельца электронной техники по цифровым следам практически невозможно.

Электронные следы включают в себя 2 элемента: информацию – сведения об объективной реальности, которые передаются по беспроводным каналам, не имеющим конкретной формы, и материальный носитель данных сведений.[3] Содержание компьютерной информации представлено в цифровой форме, ее материальным носителем выступает электромагнитное поле, которое может существовать в конкретном техническом устройстве (компьютере, мобильном телефоне, планшете, многофункциональных электронных часах и т. д.). Оно рассматривается как вторичный материальный носитель информации.[4]

---

[1] См.: Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. Волгоград: ВА МВД России, 2008. С. 401.; Багмет А.М., Бычков В. В., Скобелин С.Ю., Ильин Н. Н. Цифровые следы преступлений: монография. - Москва: Проспект 2021.- 168 с.

[2] См.: Иванов В. Ю., О теоретических аспектах использования в криминалистике понятия электронно-цифрового следа // Юридические исследования. 2020. № 7. С. 75 - 80.

[3] Криминалистическое исследование электронных и цифровых следов // URL//https://studme.org/347975/pravo/kriminalisticheskoe_issledovanie_elektronnyh_tsifrovyh_sledov. (Дата обращения: 26.01.2021).

[4] Криминалистическое исследование электронных и цифровых следов // URL//https://studme.org/347975/pravo/kriminalisticheskoe_issledovanie_elektronnyh_tsifrovyh_sledov. (Дата обращения: 26.01.2021).

Для сбора доказательственной информации, необходимо учитывать следующие факторы:

1) Не допускать посторонним лицам, а также не специалистам в данной области прикасаться к оборудованию;

2) Следует провести тщательный осмотр интересующего оборудования;

3) Необходимо определить программы, которые запущены на данном оборудовании, для этого нужно детально изучить и описать изображение на экране дисплея. Закрыть обнаруженные программы, если отсутствует риск потери информации.

4) Следует произвести копирование имеющейся информации на электронный носитель и обесточить оборудование;

5) При таких осмотрах необходимо наличие специалиста, который сможет оперативно среагировать на перемещение информации в сети;

А. В. Касаткин предложил при изъятии информации в качестве понятых приглашать квалифицированных пользователей компьютерной техники.[1] Данное предложение позволит увеличить доказательственное значение изъятых электронных следов.

6) Провести осмотр всех документов и записей, которые могут находиться поблизости с оборудованием. Ведь программисты часто делают заметки паролей, особенностей построения информационной базы компьютера. Поэтому следователю необходимо проявить внимание, для своевременного обнаружения и изъятия любых информационных носителей.

Соблюдение данных условий способствует сохранению электронных следов и дальнейшее их применение в расследовании преступлений.

Для качественного и оперативного получения информация применяются различные специализированные комплексы, например, «Мобильный криминалист»[2]. Это программа для судебно-технической экспертизы мобильных устройств. С помощью нее можно определить общую детальную информацию об устройстве, маршрут передвижения владельца, фотографии, видео, аудиозаписи и т. д.

Широко применяется аналитический комплекс - Universal Forensic Extraction Device - UFED, который позволяет восстанавливать из любых мобильных устройств удаленные данные. Следственное управление также приобрело нелинейный локатор, принцип работы которого заключается в обнаружении элек-

---

[1] См.: Мусаева У. А., Специфика проведения следственного осмотра по делам о преступлениях в сфере компьютерной информации // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 295-302

[2] См.: Бессонов А. А., О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник университета имени О. Е. Кутафина (МГЮА). 2019. С. 7.; Лебедева А. А. Компьютерные преступления и трудности формирования следственной и судебной практики// Журнал «Судья», №10.2020, октябрь С.36-40

тронных устройств, даже если они находятся в выключенном состоянии. Широкое распространение получили такие программы, как: XRY, MOBILedit, Тарантула и др.[1]

Если для производства осмотра требуется продолжительное время либо осмотр на месте затруднен, то подлежащие осмотру электронные носители изымаются, в последующем упаковываются и опечатываются, завершается всё подписью следователя и понятых. Изъятию подлежат только те предметы, которые могут иметь отношение к уголовному делу. Данный процесс регулируется ст.164.1 УПК РФ.[2]

Таким образом, на основе проведенного исследования можно сделать вывод о том, что существует необходимость постоянного совершенствования криминалистического оборудования, для качественного и оперативного расследования преступлений, повышения квалификации следователей, работающих в области IT-технологий. Это позволит существенно повысить уровень раскрытия киберпреступлений.

Библиографический список

Нормативно-правовые акты:

1. "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 19.12.2020)//URL//http://www.consultant.ru/document/cons_doc_LAW_34481/a181248bd35e283bbf253a905940bfb32dd9923e/. (Дата обращения: 26.01.2021)

Научная литература:

1. Багмет А.М., Бычков В.В., Скобелин С.Ю., Ильин Н.Н. Цифровые следы преступлений: монография. - Москва: Проспект 2021.- 168 с.
2. Бессонов А. А., О некоторых возможностях современной криминалистики в работе с электронными следами // Вестник университета имени О. Е. Кутафина (МГЮА). 2019. С. 7.
3. Вехов В.Б. Основы криминалистического учения об исследовании и использовании компьютерной информации и средств ее обработки: монография. // Волгоград: ВА МВД России, 2008. С. 401.
4. Иванов В. Ю., О теоретических аспектах использования в криминалистике понятия электронно-цифрового следа // Юридические исследования. 2020. № 7. С. 75 - 80.

[1] См.: Яковлев Н. А., Специфика применения специальной криминалистической техники в процессе расследования преступлений // Моя профессиональная карьера. 2020. № 2. С. 161-164

[2] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 08.12.2020) (с изм. и доп., вступ. в силу с 19.12.2020 //URL//http://www.consultant.ru/document/cons_doc_LAW_34481/a181248bd35e283bbf253a905940bfb32dd9923e/. (Дата обращения: 26.01.2021)

5. Кирсанова С. О., Калинина А.А., Виртуальные следы: понятие, сущность, проблемы // Скиф. Вопросы студенческой науки. 2018. С. 4.
6. Лебедева А.А. Компьютерные преступления и трудности формирования следственной и судебной практики// Журнал «Судья», №10.2020, октябрь С.36-40;
7. Лебедева А.А. Борьба с киберпреступлениями – новая функция Следственного комитета России Противодействие киберпреступности: современное состояние и пути повышения эффективности: сборник статей / Следств. ком. Респ. Беларусь; редкол.: С. Я. Аземша (гл. ред.) [и др.]. – Минск: Юр-Спектр, 2020. – 322с., с. 179-183.
8. Мещеряков В. А., «Виртуальные следы» под «Скальпелем Оккама» Информационная безопасность. 2009. № 1(4) С. 28-33.
9. Мусаева У. А., Специфика проведения следственного осмотра по делам о преступлениях в сфере компьютерной информации // Известия Тульского государственного университета. Экономические и юридические науки. 2013. № 4-2. С. 295-302
10. Яковлев Н. А., Специфика применения специальной криминалистической техники в процессе расследования преступлений // Моя профессиональная карьера. 2020. № 2. С. 161-164

Интернет ресурсы:

1. Криминалистическое исследование электронных и цифровых следов//URL//https://studme.org/347975/pravo/kriminalisticheskoe_issledovanie_elektronnyh_tsifrovyh_sledov. (Дата обращения: 26.01.2021)
2. Интервью начальника отдела по расследованию киберпреступлений СК России п/п юстиции К.П. Комарды // URL//https://sledcom.ru/press/interview/item/1529946. (Дата обращения 25.01.2021г.);
3. Информационно-аналитический журнал «Рубеж» // URL//https://rubezh.ru/gossektor/news/20/12/02/chislo-kiberprestuplenij-v-rossii-vyiroslo-na-946-proczentov-za. (Дата обращения: 25.01.2021г.)

А.Д. Одегова
Д.В. Цуканова
Научный руководитель: **В.А. Мишенин**

Личность потерпевшего и его индивидуальная виктимность в механизме преступлений, совершаемых с использованием информационно-телекоммуникационной сети Интернет

Аннотация. В статье рассматривается взаимосвязь компонентов личности с его индивидуальной виктимностью. Приведена статистика преступлений в сфере IT-технологий в 2019-2020 годах. Анализируется современное состояние киберпреступности и ее доля в сети Интернет. Как одна из ключевых проблем рассматривается подростковая виктимность и виды преступлений, которые совершаются в отношении несовершеннолетних в сети Интернет. В статье рассмотрены механизмы совершения

отдельных видов преступлений, а также описаны тенденции развития киберпреступности.

Ключевые слова: виктимность, личность потерпевшего, несовершеннолетние, особенности психики, интернет, киберпреступность.

В современности тема исследования виктимного поведения людей достаточно актуальна в связи с увеличением занимаемого сетью Интернет места в жизни человека, а также с наличием достаточно большого количества возможностей его негативного использования.

Но, прежде чем разобраться в этом, нужно определить, что же такое виктимность и чем обусловлено такое поведение потерпевших.

Науке такое понятие как виктимность известно достаточно давно. Первый учёный, который работал в этом направлении и являющийся его основателем, был Ганц фон Гентинг. Он в своей научной монографии обосновал положения, относящиеся к разграничению типов поведения жертв преступлений, отношения между потерпевшим и преступником, а также дал определения терминам, связанных с виктимологией.

В советский период такое явление как виктимность изучали многие учёные-криминологи. Так, термин виктимность, по мнению Л.В. Франка, есть «повышенная способность человека» в силу его социальной роли и ряда физических и духовных качеств при определённых обстоятельствах «становиться потерпевшим»[1].

При данном определении виктимности, решающий критерий – это особенность личности потерпевшего. Но индивид может стать жертвой преступления также в силу внешних факторов, которые способствовали бы этому. Ведь вероятность человека стать пострадавшим от преступных посягательств зависит не только он него самого, но и других внешних критериев. В условиях сети Интернет данные факторы ограничены только воздействием на индивида, так как только от него зависит, будет ли он продолжать общение с незнакомыми людьми, продолжит ли он изучать информацию, которая может привести к негативным последствиям.

В теории криминологии виктимность можно разделить на несколько видов, где самыми значимыми будут общая и специальная. Общий вид виктимности зависит от возраста, пола, социального статуса, различных увлечений. Специальный вид направлен на изучение психологической неустойчивости при воздействии внешних факторов, особенности воли индивида и его эмоционального состояния.

Наиболее уязвимой социальной группой являются подростки, потому что они, в силу особенностей своей неокрепшей психики и гиперэмоционального состояния, могут стать жертвами преступников, которые осуществляют свои преступные умыслы с помощью сети Интернет.

Виктимное поведение проявляется не только во внешнем мире при непосредственном взаимодействии людей, но и в сети Интернет. Данное явление можно

[1] Есберген Алауханов. Криминология. Учебник. – Алматы. 2008. - 429 с.

охарактеризовать как динамичное свойство личности человека, выражающееся в форме психологического, социального, морального деформационного поведения, которое проявляется через импульсивные и провоцирующие формы поведения[1]. В данном случае они не соответствуют нормам, обеспечивающим безопасность личности, а наоборот способствуют потенциальной или реальной предрасположенности субъекта стать жертвой преступления в Интернете.

На сегодняшний день, Интернет – самая динамично развивающаяся структура, которая не просто подстраивается под мировые тренды, а чаще всего задаёт их. Ни одно глобальное событие, происходящее в мире, не может обойтись без всеобщей огласки в Интернете. И порой такие события становятся благоприятной средой для деятельности преступников.

Рост преступлений в сфере IT-технологий является наиболее актуальной проблемой современности. По данным МВД за январь 2020 года правоохранительными органами РФ зарегистрировано 28,14 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[2]. Это на 75,2% больше, чем за аналогичный период 2019 года

По информации МВД, в 2019 году было зарегистрировано 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Причем значительно выросло количество преступлений, совершенных через Интернет – 44% от общего числа, что составляет почти 130 тысяч преступлений.[3]

Проблема подростковой виктимности напрямую вытекает из особенностей их психического состояния. Для подростков характерна полярность психики, которая может выражаться в чрезмерной импульсивности и целеустремленности, сменяемыми апатией; напускной уверенностью в себе на фоне тайной закомплексованности; желанием быть в центре внимания и периодами одиночества и т.д. В этом состоянии подросток стремится доказать окружающим, что он взрослый и самостоятельный, чем часто пользуются преступники в сети.

Используя уязвимое состояние психики подростка, преступники совершают преступления различной направленности. Отдельно стоят преступления против половой свободы несовершеннолетних. Механизм совершения таких преступлений очень прост: преступник завладевает доверием несовершеннолетнего в ходе общения в социальной сети, ведет разговоры на темы сексуального характера, присылает свои фотографии интимного характера и требует того же от своего несовершеннолетнего собеседника. К сожалению, не все подростки в состоянии выдержать эмоциональное давление более взрослого человека и выполняют тре-

---

[1] Биктагирова Г.Ф., Валеева Р.А., Дроздикова-Зарипова А.Р., Калацкая Н.Н., Костюнина Н.Ю. Профилактика и коррекция виктимного поведения студенческой молодежи в Глобальной сети Интернет: теория, практика. - Казань: Издательство «Отечество», 2019. -С. 320

[2] Портал правовой статистики Генеральной прокуратуры РФ http://crimestat.ru.

[3] Российская газета: федеральный выпуск. №17 // https://rg.ru/2020/01/28/rezko-vyroslo-chislo-prestuplenij-sovershaemyh-s-pomoshchiu-it-tehnologij.html.

бования, что по своей сути является преступлением и квалифицируется как развратные действия[1]. Чаще всего жертвами данных преступлений выступают девочки, но не всегда.

Также возможны случаи посредственного исполнительства при помощи сети Интернет. Мошенники просят несовершеннолетнего сообщить определенные данные своих родителей. Несовершеннолетний в данном случае выполняет просьбы под действием обмана, злоупотребления доверием или же угроз.

В последние годы в сети Интернет активно начали действовать так называемые «группы смерти», деятельность которых также основана на особенностях психики подростков. Механизм совершения данных преступлений схож с механизмом половых преступлений, однако здесь вместо обнаженных фото куратор требует выполнение определенных заданий, последнее из которых – совершить самоубийство. И несмотря на то, что процент самоубийств, совершаемых под влиянием таких групп, от общего число самоубийств невелик, такая преступная активность в сети Интернет обратила внимание на необходимость регулирования данной сферы отношений, в результате чего была принята стать 110.2 УК РФ «Организация деятельности, направленной на побуждение к совершению самоубийства»[2].

Давление на неокрепшую психику подростка может выражаться и в иной форме. Это «буллинг» в Интернете, когда любой пользователь может высказаться в сторону несовершеннолетнего, и не всегда это будет в положительном ключе: в большинстве случаев это негативные комментарии. Также создаются различные сайты, основная идея которых – причинение вреда не только себе, но и окружающим людям посредством выполнения различных заданий.

Рост преступлений в отношении несовершеннолетних обусловлен действием ряда факторов, в числе которых:

- отсутствие четкого законодательного запрета (ограничений) на доступ детей и подростков к информационным порталам и ресурсам в сети Интернет;
- недостаточный контроль со стороны взрослых за виртуальной жизнью несовершеннолетнего в социальных сетях;
- активизация различных категорий преступников, в том числе педофилов в Интернет-пространстве и социальных сетях, использующих дистанционные технические возможности применения вербовки и иных анонимных манипуляций сознанием и поведением подростков в сети;
- изменение социальных норм поведения, в том числе у самих несовершеннолетних.

Необходимость работы в сфере снижения уровня индивидуальной виктимности несовершеннолетних является актуальной для правоохранительных органов, а для Следственного комитета России в большей степени, так как преступления, совершенные в отношении лиц, не достигших восемнадцатилетнего возраста, относятся к подследственности Следственного комитета РФ. В этой связи стоит

---

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 23.04.2019),// Доступ из справочно-правовой системы «Консультант Плюс».
[2] Там же.

отметить, что преступления, совершенные с помощью сети Интернет, обладают определенной спецификой их расследования, в связи с чем не всегда получается достоверно установить личность преступника, что ведет к безнаказанному совершению преступлений.

Всё больше людей становятся потерпевшими от преступлений в Интернете, так как уровень современной компьютеризации даёт возможность каждому иметь доступ к данным технологиям. В Интернете сейчас можно создавать различные Интернет-ресурсы: сайты, блоги, чаты, не обладая при этом какими-либо специальными знаниями в области программирования. Поэтому доступное и бесконтрольное использование ресурсов Интернета в преступных целях является серьёзной угрозой не только для несовершеннолетних, но и для людей более старшего возраста.

В отношении людей старшего возраста совершение преступлений в сети Интернет осуществляется достаточно много. Данные виды преступлений имеют не конкретную личностную направленность, а ориентированы на совершение мошенничества в отношении их данных. Однако преступники не останавливаются на кибермошенничестве: совершаются попытки присвоения и сбора персональных данных человека, информацию о его кредитных картах или банковских счетах.

В последнее время данные преступления имеют всё больший вес в связи с распространением заболевания «COVID-19». Большинство людей находится на самоизоляции, поэтому все действия, которые раньше могли быть выполнены в реальной жизни, теперь происходят в виртуальной. Поход в магазин, просмотр кино – всё это сейчас заменяет Интернет, чем злоупотребляют преступники, создавая сайты, используемые в преступных целях.

Также способами мошенничества в условиях новой коронавирусной инфекции стали действия по реализации товаров, якобы спасающих от заражения коронавирусом, и вакцины от него, реклама которых была размещена в сети Интернет. Кроме того, через сеть Интернет реализовывались амулеты, обереги, предметы религиозного культа, которые также должны были защитить от заболевания.

Во всех преступлениях можно проследить закономерность проявления виктимного поведения в киберпространстве. Причинами данного поведения в Интернете служат определенные психологические качества личности, которые проявляются именно в сети. Ими являются большая доверчивость и наивность пользователей, на которых могут повлиять киберпреступники, чтобы в отношении них совершить преступление, или же путем психологического воздействия заставить человека самого совершить преступление, порой даже не подозревая этого. Также одной из причин является низкая осведомлённость о преступлениях в Интернете, способах их предотвращения и недопущения, так как большинство пользователей сети обычные люди, имеющие самые начальные знания о возможностях использования современных технологий в данной области.

Список использованных источников

1. Бастрыкин А.И. Преступления против несовершеннолетних в интернет-пространстве: к вопросу о виктимологической профилактике и уголовно-правовой оценке // Всероссийский криминологический журнал. 2017. №1.
2. Биктагирова Г.Ф., Валеева Р.А., Дроздикова-Зарипова А.Р., Калацкая Н.Н., Костюнина Н.Ю. Профилактика и коррекция виктимного поведения студенческой молодежи в Глобальной сети Интернет: теория, практика. - Казань: Издательство «Отечество», 2019.
3. Есберген Алауханов. Криминология. Учебник. – Алматы. 2008.
4. Портал правовой статистики Генеральной прокуратуры РФ http://crimestat.ru.
5. Российская газета https://rg.ru/.
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 23.04.2019) // Доступ из справочно-правовой системы «Консультант Плюс».

Е.Н. Оленкова
Научный руководитель**: В.А. Мишенин**

Предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации

Аннотация. Использование современных информационных технологий в промышленной, торговой, банковской, научной, культурной, образовательной и других сферах общественной жизни детерминировало динамический рост и качественное обновление компьютерной преступности в России, что создает новые угрозы для развития общества и государства. В статье приведены меры, непосредственно направленные на предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации.

Ключевые слова: информационно-коммуникационные технологии, компьютерная информация, безопасность, пользователи, высокие технологии.

Внедрение передовых информационных технологий в различных сферах социальной жизни стало причиной возрастания и качественного обновления преступлений в сфере компьютерной информации, совершаемых на территории Российской Федерации. При этом своевременное предупреждение преступлений в сфере информационно-телекоммуникационных технологий для правоохранительных органов является вопросом, решение которого зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов специального предупреждения данного вида преступлений.

Стремительное развитие информационно-телекоммуникационных технологий способствует тому, что совершенные преступления в данной сфере остаются безнаказанными. Причиной этого является то, что уголовное законодательство

слабо адаптировано к новым видам преступлений в сфере информационных технологий.

В криминологии выделяют три уровня предупреждения преступности в сфере информационно-телекоммуникационных технологий: общесоциальный, специально-криминологический и индивидуальный.[1]

В структуру общесоциального уровня входят меры, направленные, прежде всего, на решение комплексных социальных проблем, но оказывающие положительный эффект на процессы детерминации преступности. Их отличает от двух других уровней предупреждения преступности то, что при их осуществлении отсутствует непосредственная цель воздействия на криминогенные процессы, протекающие в обществе, однако решение общесоциальных проблем оказывает косвенное воздействие и на условия (иногда и на причины) совершения конкретных видов преступлений.

Применительно к системе предупреждения высокотехнологичной преступности можно выделить несколько направлений общесоциального воздействия.

Так, к общеэкономическим предупредительным мерам можно отнести создание условий для экономического роста и повышения конкурентоспособности национальной экономики, ликвидации бюрократических барьеров и снижения уровня коррупции, повышения производительности труда и т. д.

Социальные меры предусматривают противодействие процессам социального и имущественного расслоения в обществе, устойчивую социальную политику, направленную на своевременное и качественное решение социальных вопросов; функционирование системы личной безопасности граждан, а также решение отдельных остросоциальных вопросов, таких как достойная оплата активной трудовой деятельности, наличие безопасных и высококачественных товаров и услуг и др.

Научно-технические меры общесоциального предупреждения преступлений включают государственную поддержку системы целевых фундаментальных и прикладных исследований как необходимого элемента научного обеспечения национальной безопасности государства; расширение сети научно-исследовательских и образовательных учреждений, обеспечивающих разработку научных исследований в сфере высоких технологий и подготовку соответствующих специалистов; разработку современных цифровых технологий и перспективных образцов наукоемкой продукции; модернизацию производственного цикла и др.

К общекультурным мерам можно отнести укрепление духовного единства многонационального народа Российской Федерации и повышение международного культурного имиджа России; повышение роли культуры для возрождения и сохранения культурно-нравственных ценностей, организацию патриотического и духовного воспитания граждан России.

---

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

Отдельно следует остановиться на законодательных мерах общесоциального предупреждения преступлений в сфере высоких технологий.

К ним относятся: повышение качества принимаемых законов как на федеральном, так и региональном уровнях; устранение правовых коллизий, препятствующих деятельности правоприменителей в борьбе с преступностью; функционирование системы анализа применения действующего законодательства и своевременного реагирования на процессы, происходящие в обществе; создание механизма криминологической экспертизы законопроектов; координация законотворчества и правоприменения на международном уровне в рамках соответствия международным стандартам борьбы с преступностью, а также двусторонним и многосторонним межгосударственным соглашениям и договорам.

Так, утвержденная в 2017 г. Президентом Российской Федерации Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы к числу приоритетных задач относит обеспечение комплексной защиты информационной инфраструктуры Российской Федерации, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры.

Содержанием мер специально-криминологического предупреждения является деятельность, направленная непосредственно на причины и условия совершения преступлений. Здесь важно обратить внимание на вопросы повышения эффективности научного обеспечения деятельности по противодействию преступности в сфере высоких технологий. В настоящее время анализ основных направлений научных исследований проблем высокотехнологичной преступности показывает, что вопросам информационной безопасности, защиты компьютерной информации, предупреждения компьютерной преступности в Российской Федерации уделяется пристальное внимание как стороны государства, так и со стороны научного сообщества.

В качестве конечной цели предупреждения рассматриваемых преступлений следует считать создание системы международных и государственных гарантий информационной безопасности, обеспечивающих должный уровень защищенности личности, общества и государства в сфере создания, передачи, хранения, обработки и использования информации, а также функционирования соответствующих электронных средств и информационно-телекоммуникационных систем.

Эффективной мерой повышения компьютерной безопасности является возложение на руководителей или иных уполномоченных лиц персональной обязанности осуществлять контроль за установкой и постоянным обновлением антивирусного программного обеспечения, а также иных систем комплексной защиты с целью совершенствования систем безопасности компьютерной информации в государственных и муниципальных организациях. В свою очередь, в трудовых договорах (контрактах) лиц, работающих в корпоративной компьютерной сети или имеющих доступ к информационным ресурсам, необходимо предусмотреть положение об их персональной ответственности за разглашение

или передачу посторонним лицам конфиденциальных сведений, касающихся системы защиты информации, служебных паролей или иных средств идентификации.[1]

Говоря о содержании третьего – индивидуального уровня предупреждения преступности в сфере информационно-телекоммуникационных технологий, то здесь значение приобретает ряд профилактических рекомендаций. В целях профилактики целесообразно рекомендовать пользователям использовать наиболее подходящий, защищенный и правильно настроенный веб-браузер, который незамедлительно предупреждает пользователя о возможной опасности. Это касается не только браузеров, но и других используемых программ, например, электронных кошельков WebMoney. Кроме того, антивирусные пакеты многих производителей этого программного обеспечения пополнились модулями, защищающими пользователя. Однако, как показывает практика, основная проблема связана с небрежностью в вопросах защиты персональной информации самими пользователями. Поэтому важной задачей правоохранительных органов по-прежнему является информационно-просветительская деятельность среди населения по предотвращению высокотехнологичной преступности.

Таким образом, профилактика преступлений, совершаемых с использованием высоких технологий, должна быть организована с учетом виктимности различных групп населения. Необходимо учитывать различные аспекты обеспечения данного вида деятельности, иметь конкретную направленность на осознание необходимости соблюдения мер предосторожности в информационно-телекоммуникационном пространстве, основываться на доступных для населения или работников – неспециалистов рекомендациях по совершенствованию своей защищенности от киберугроз.

Список использованных источников

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы".
3. Электронные носители информации в криминалистике : монография / под ред. О. С. Кучина. – М. : Юрлитинформ, 2017. – 304 с.
4. Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.

[1] Гаврилин Ю. В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю. В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.

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

А.О. Пантелеева
А.П. Семенов
Научный руководитель: **В.А. Мишенин**

Криминологические аспекты предупреждения преступлений, совершаемых с использованием средств сотовой связи

Аннотация. В условиях расширения и усовершенствования современных технических средств возникает пространство для совершения противоправных действий в этой сфере. Растущие показатели количества преступлений, совершаемых с использованием средств сотовой связи, вызывают необходимость создания эффективных мер по их предупреждению. На основе изучения способов совершения преступлений с использование средств сотовой связи и их основных характеристик определяются основные направления мер по предупреждению.

Ключевые слова: преступления, совершаемые с использованием средств сотовой связи, сотовая связь, предупреждение, способы и методы воздействия на жертву.

Возможности современных технических средств постоянно увеличиваются, что не только способствует удовлетворению возрастающих потребностей пользователей, но и создает огромное пространство для совершения противоправных действий.

Сотовая связь является подвижной связью, в основе которой лежит сотовая сеть. Распространение действия сотовой связи ограничивается только зоной покрытия отдельных базовых станций, поэтому ее использование является транстерриториальным.

Согласно статистическим данным МВД РФ, за январь – октябрь 2020 года зарегистрировано 1 739 743 преступления, из них с помощью средств мобильной связи совершено 181 197 преступлений. За аналогичный период 2019 года с помощью средств мобильной связи было совершено 294 409 преступлений. Таким образом, прирост за один год составил 42,8 %[1].

В связи с этим ставится под сомнение эффективность существующих мер по предупреждению данного вида преступлений, что обуславливает необходимость определения основных направлений деятельности по их предупреждению.

Что касается раскрываемости данных преступлений на сегодняшний день из 181 197 преступлений, совершенных с использованием средств мобильной связи, не раскрыто 129 455 преступлений, что составляет 71,4%.

[1] «Состояние преступности в России за январь – октябрь 2020 года» // Министерство Внутренних Дел Российской Федерации ФКУ «Главный Информационно – аналитический центр», Москва. 2020 г.

Представленные статистические данные следует подвергать критической оценке, так как данный вид преступлений относится к категории преступлений с высокой латентностью и обуславливается практическими трудностями в их выявлении, раскрытии и расследовании.

Преступления, совершаемых с использованием средств сотовой связи – это активные, умышленные и целенаправленные действия лица с использованием средств сотовой или мобильной связи, заключающиеся во введении в заблуждение другого лица или предоставлении ему ложной информации, то есть путем обмана, с целью противоправного завладения денежными средствами или получения необходимой информации для этого.

Данный вид преступлений имеет следующие характерные признаки: умышленные и целенаправленные действия; средство совершения преступления - телефон сотовой связи, имеющий свои идентификационные признаки (IMEI, IP, сим-карта); дистанционный характер; использование электронных платежных систем; неограниченный круг потенциальных жертв; использование методов воздействия на жертву.

Способы и методы совершения преступлений с использованием средств сотовой связи представлены в следующей классификации. По предмету осуществления преступлений подразделяют на виды:

1. SMS – сообщения на номера абонентов;
2. Входящие звонки на номера абонентов от «Службы поддержки мобильного оператора»;
3. Входящие звонки на номера абонентов от «Службы поддержки банка»;
4. SMS – сообщения, использующие сеть «Интернет» для получения услуг и приобретения товара.

По мнению Г.В. Семенова, мошенничество по способу совершения преступления с использованием средств сотовой связи можно подразделить на следующие виды:

- техническое мошенничество (при получении доступа к телефону и банковской карте);
- процедурное мошенничество (неправомочное использование роуминга);
- мошеннический доступ (перепрограммирование идентификационных номеров сотовых телефонов);
- мошенничество с украденным телефоном;
- хакерское мошенничество (получение конфиденциальной информации)[1].

Приведем примеры из судебной практики, иллюстрирующие способы и методы совершения данного вида преступления. Так, согласно приговору № 1–166/2020 от 29 мая 2020 г. по делу № 1–166/2020 Иванов, находясь в жилом помещении своего знакомого Петрова, дождался времени, когда хозяин квартиры ляжет спать, похитил сотовой телефон, номер которого был привязан к банковской

[1] Семенов Г.В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи. // Центр исследования проблем компьютерной преступности. 2016. URL: http://www.crime-research.ru/library/Semenov.htm.

карте, а также саму банковскую карту ПАО «Сбербанк». После содеянного Иванов отправился к ближайшему банкомату и снял с банковской карты, воспользовавшись данными содержащимися в приложении телефона, в общей сложности 54 755 рублей[1].

Согласно приговору № 1-125/2012 от 05.07.2012 г. по делу № 1–125/ 2012 Сычев Д.Е., находясь в местах лишения свободы, с помощью средств сотовой связи, по раннее разработанному преступному плану, звонил на неизвестные ему номера телефонов абонентам, представляясь близким родственником, который попал в беду и которому срочно нужны денежные средства[2]. Также Сычев Д.Е. менял тактику хищения денежных средств, представляясь сотрудником правоохранительных органов, что дало ему возможность угрожать и шантажировать абонентов по факту возможности реализации уголовного наказания в виде лишения свободы их близких родственников, если потерпевшие не переведут определенную сумму денежных средств.

В ходе анализа способов совершения данного вида преступлений и соответствующей судебной практики можно сделать вывод о том, что успешность осуществления злоумышленником задуманного зависит от личностных качеств потенциальной жертвы, её устойчивости к психологическому воздействию. Злоумышленники применяют способы и методы психологического воздействия на потенциальную жертву, учитывая особенности ее поведения: запугивание, убеждение, использование доверительных отношений, возбуждение желания получения материальной выгоды.

Все методы воздействия на жертву сводятся к таким виктимологическим особенностям поведения личности: невнимательность; неосведомленность; доверчивость; корыстные мотивы жертвы (желание получения материальной выгоды); подверженность к запугиванию.

Преодоление вышеуказанных факторов видится возможным в осуществлении комплекса направлений предупредительных мер.

Первое направление - это работа с населением с целью повышения грамотности в области информационной безопасности, а также финансовой и правовой грамотности. Учитывая, что потенциальными жертвами является незащищенная часть населения - лица, подверженные социально- психологическому воздействию, необходимо уделить особое внимание этой категории населения.

Второе направление заключается в осуществлении постоянного мониторинга сферы предоставления услуг сотовой связи на предмет совершения противоправных действий или невыполнения предусмотренных законом требований, что позволит сократить распространение используемых злоумышленниками «серых» (с ложными данными о владельцах) и «пустых» (без официальной регистрации данных владельца) сим-карт.

---

[1] Приговор № 1–166/ 2020 от 29 мая 2020 г. по делу № 1–166/2020. URL: https://sudact.ru/regular/doc/Fr68WLr3aRHu//.

[2] Приговор № 1-125/2012 от 05.07.2012 г. по делу № 1–125/ 2012 URL: https://sudact.ru/regular/doc/XTTgzlaAaQle/.

Также в проводимой работе по мониторингу следует учитывать тот факт, что злоумышленники научились подменять подлинные телефонные номера кредитных организаций, государственных служб, и выдавать себя за работников данных организаций.

Следующее направление предупреждения данного вида преступлений видится в усовершенствовании существующих систем безопасности и защиты конфиденциальной информации о клиентах в банках и электронных системах платежа. На основе предоставляемых правоохранительными органами данных о новых способах совершения преступлений необходимо на их основе осуществлять разработку программных продуктов по обеспечению безопасности.

Важным направлением предупреждения преступлений, совершаемых с использованием средств сотовой связи, является разработка научно-методических рекомендаций по раскрытию, расследованию и предотвращению преступлений с использованием коммуникативных технологий для правоохранительных органов. Данные методические рекомендации должны также предлагать решения нестандартных проблем, связанных с процедурой получения необходимой информации, установления места нахождения личности, доказывания обстоятельств по делу. Кроме вышеуказанного, необходимо усовершенствовать криминалистические средства получения необходимой информации, позволяющей установить место совершения преступления, личность преступника и противоправность совершаемых им действий.

Значительную роль в деятельности по предупреждению данной категории преступлений играет следственная профилактика, реализующаяся в вынесении представлений об устранении причин и условий, способствовавших совершению преступлений (ст.158 УПК РФ). По мнению группы ученых, координатором профилактической деятельности по преступлениям должен выступать следователь[1], но такая мера должна носить целесообразный и обоснованный характер.

Таким образом, решение проблем профилактики рассмотренного вида преступлений видится в комплексной работе субъектов профилактики по выработке и реализации мер по предупреждению преступлений, совершаемых с использованием средств сотовой связи по вышеуказанным направлениям

В заключении необходимо отметить, что именно правоохранительные органы призваны стать инициатором и «координатором» профилактической деятельности в отношении данного вида преступлений.

Список использованных источников

1. Макаров Р.А., Кузнецов А.А. Следственная профилактика хищений с банковских карт, совершаемых дистанционно с использованием средств сотовой связи // Алтайский юридический вестник. 2020. 4 (32). – С. 144-150 URL: https://elibrary.ru/item.asp?id=44248280.

[1] Макаров Р.А., Кузнецов А.А. Следственная профилактика хищений с банковских карт, совершаемых дистанционно с использованием средств сотовой связи // Алтайский юридический вестник. 2020. 4 (32). – С. 144-150. URL: https://elibrary.ru/item.asp?id=44248280

2. Приговор № 1-125/2012 от 05.07.2012 г. по делу № 1 – 125/ 2012 Приговор № 1 – 166/ 2020 от 29 мая 2020 г. по делу № 1 – 166/2020. URL: https://sudact.ru/regular/doc/Fr68WLr3aRHu//.
3. Семенов Г.В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи. // Центр исследования проблем компьютерной преступности. 2016. URL: http://www.crime-research.ru/library/Semenov.htm.
4. Состояние преступности в России за январь – октябрь 2020 года // Министерство Внутренних Дел Российской Федерации ФКУ «Главный Информационно – аналитический центр», Москва. 2020 г.

Д.О. Соловьёва
Научный руководитель: **В.А. Мишенин**

Причины и условия роста количества преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет»

Аннотация. Данная статья посвящена рассмотрению причин и условий роста количества преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет» в Российской Федерации. В статье приводится классификация и анализ наиболее актуальных причин совершения преступлений в сети Интернет или с его помощью. Для подтверждения приведённых положений рассмотрены статистические данные, а также примеры из судебной практики.
Ключевые слова: интернет; интернет-преступность; киберпреступность; преступление в сети Интернет; социальные сети; информационные технологии; интернет-ресурс; компьютерные преступления.

Указом Президента Российской Федерации от 9 мая 2017 года была утверждена Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы. В ней были названы следующие приоритетные направления внутренней политики: развитие информационных и коммуникационных технологий, формирование информационного пространства с учетом потребностей граждан и общества.[1]

Разумеется, осуществление активной работы в данных направлениях, создание новых устройств и гаджетов, активизация научно-технической сферы – всё это приносит пользу экономике государства, выводит страну на новый уровень информационного общества. Однако, к сожалению, данная деятельность влечёт за собой и негативные последствия. По сравнению с 2018 годом в 2019 году число пользователей Интернет в России выросло на 6 миллионов человек. По данным, представленным в глобальном отчёте Digital 2020 от международного

[1] Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // // Доступ из справочно - правовой системы «КонсультантПлюс»

агентства «We are social», в 2020 году в России количество интернет-пользователей составило 118 миллионов человек. Это говорит о том, что интернетом пользуются 81% россиян.

Тот факт, что около 100 дней в году граждане России проводят в так называемом «киберпространстве» вместо того, чтобы находиться в «реальном» мире, объективно воспринимать окружающую действительность и контактировать с людьми с помощью «живого» общения, не является самым негативным последствием использования интернет-технологий. Наиболее опасным следствием развития и использования интернет-ресурсов, компьютерных технологий является стремительный рост интернет–преступности.

Вопросу определения понятия «интернет-преступность» учёными-правоведами практически не уделялось внимание. Простым, но в то же время раскрывающим в себе суть явления, представляется определение интернет-преступности, как совокупности противоправных общественно опасных деяний, совершенных с использованием информационно-телекоммуникационной сети «Интернет», как правило, характеризующихся высокой латентностью, неперсонифицированностью и стремительным ростом.

Интернет-преступность составляет часть от компьютерной преступности. Важно понимать, что любое интернет-преступление будет являться компьютерным, но никак не наоборот. Кроме того, если такие традиционные преступления, как мошенничество, кража, вымогательство и другие совершены с помощью Интернета, то они так же относятся к интернет-преступлениям.

Необходимо отметить, что к интернет-преступлениям могут быть отнесены не только преступления в сфере компьютерной информации (Глава 28 Уголовного кодекса Российской Федерации), но и некоторые составы преступлений, не относящихся к киберпреступлениям, однако совершаемые в интернет-пространстве или с помощью сети Интернет.

К таким преступлениям можно отнести: незаконные изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ), доведение до самоубийства (ст. 110 УК РФ), вовлечение несовершеннолетних в совершение преступлений и антиобщественных действий (ст. 150-151 УК РФ), содействие в террористической деятельности (ст. 205.1 УК РФ), организация деятельности террористической организации и участие в такой деятельности (ст. 205.5 УК РФ), склонение к употреблению наркотических средств, психотропных веществ или их аналогов (ст. 230 УК РФ) и другие.

Только с января по октябрь 2020 года в России было совершено 421 тыс. IT-преступлений. При этом более половины из них относятся к категории тяжких и особо тяжких. Сеть «Интернет» преступники использовали 244 тысячи раз. Это на 90 % чаще, чем в 2019 году за аналогичный период.

На основании статистики, предоставленной Министерством внутренних дел России, за 2019 год зарегистрировано более 294 тысяч преступлений, совершенных с использованием информационно-телекоммуникационных технологий.[1] К сожалению, это практически на 70 % больше, чем за аналогичный период прошлого года. Стоит отметить, что 50 % таких преступлений были совершены с использованием сети «Интернет».

Это ещё раз подчеркивает важность и актуальность изучения проблем предупреждения киберпреступлений, проведения исследований причин и условий их порождающих.

Очевидно, что научно-технический прогресс, усовершенствование имеющихся у граждан устройств и современных девайсов, создание новых – это не единственные факторы, способствующие увеличению количества преступлений, совершаемых как в сети «Интернет», так и с его помощью.

Для того, чтобы раскрыть причины и условия роста количества таких преступлений, необходимо определить, что обозначают данные показатели.

Итак, причины преступности – это детерминанты, которые непосредственно порождают, воспроизводят преступность как свое закономерное следствие. Условия преступности - такие явления, которые непосредственно не порождают преступность, но способствуют её проявлению, облегчают её формирование и развития.

Стоит отметить, что причины и условия – это два взаимосвязанных элемента, часто пересекающихся друг с другом, объединяемые понятием «криминогенные детерминанты». Именно их взаимодействие вызывает такое явление как преступность. Поэтому, зачастую, при анализе причин и условий преступности данные категории не разделяют на две самостоятельные группы.

Для более систематизированного подхода к анализу причин и условий роста количества преступлений сфере компьютерной информации, а также преступлений, не относящихся к данной группе, но совершаемых в сети «Интернет» или с его помощью, стоит их объединить в несколько групп.

По своему характеру причины и условия в рассматриваемом контексте могут быть экономическими, социальными, политическими, правовыми и организационно-техническими.

К экономическим причинам относятся:

1. Высокая конкуренция в сфере новейших технологий. Стремительное развитие компьютерных технологий стимулирует «изобретательность» преступников, Производители различных устройств (мобильных телефонов, персональных компьютеров и т.д.) находятся в постоянной гонке друг с другом, наполняя технически устройства усовершенствованными показателями: «разблокировка телефона в одно касание», «сканер объёмно-пространственной формы лица человека вместо пароля» (Face ID) и другими поражающими воображение характеристиками. Безусловно, создание подобных функций пользуется большим

[1] Официальный сайт Министерства Внутренних дел Российской Федерации // URL: https://мвд.рф.

спросом в современном обществе. Однако, очевидно, что производитель руководствуется материальной выгодой и не задумывается о негативных последствиях использования таких опций, особенно, связанных с упрощением процесса доступа к содержимому устройства.

2. Быстрое и достаточно безопасное для преступников обогащение. Субъекту преступления физически значительно проще совершить кражу с банковской карты в сети «Интернет», чем совершить такое преступное деяние в реальной действительности, где могут быть свидетели, камеры видеонаблюдения и другие факторы, способные препятствовать реализации преступной цели.

К социальным причинам относятся:

1. Всеобщая компьютеризация российского общества (о которой говорилось ранее), создающая благоприятную среду для совершения киберпреступниками противоправных действий. Виртуальный мир и компьютерные технологии настолько поглотили современной российское общество, что в среднем гражданин России проводит в сети в сутки не менее 7 часов, что по времени составляет протяжённость почти полного рабочего дня.

2. Достаточно высокий уровень цифровой (компьютерной) грамотности пользователей сетей. Многие люди становятся настолько увлеченными интернет-возможностями, что на определённом этапе решают монетизировать свои навыки, использовать свои умения в корыстных целях. К сожалению, в некоторых случаях такие «хакеры» злоупотребляют своими способностями и начинают их использовать в преступных целях.

3. Низкий уровень дохода, а также неудовлетворённость уровнем и качеством собственной жизни.

В качестве примера можно привести приговор Мурашинского районного суда Кировской области от 25.04.2012 года, согласно которому 18.12. 2011 гражданин П. в помещении железнодорожной торговой компании за денежное вознаграждение (4000 рублей) незаконно установил на жёсткий компьютера программы: «Microsoft Windows XP Professional SP 3 RUS» стоимостью 9276 рублей и «Microsoft Office 2007 Professional Rus» стоимостью 14233 рубля, правообладателем которых на территории Российской Федерации является корпорация «Майкрософт», а также программы «1С:Предприятие 7.70.027 SQL (Конфигурация: Бухгалтерский учет; Оперативный учет; Расчет Управление распределенными ИБ)» 171000 рублей, правообладателем которой является компания ООО «1С»; «CorelDRAW Graphics Suite X3» 11405 рублей, правообладателем которой на территории Российской Федерации является корпорация «Corel». Таким образом, гражданин П. причинил материальный ущерб вышеперечисленным правообладателям в размере 205915 рублей. За совершение преступлений, предусмотренных ч. 2 ст. 146, ч. 2 ст. 272, ч.2 ст. 273 УК РФ, суд назначил гражданину П. наказание в виде ограничения свободы на срок 1 год.[1]

В данном случае, гражданин П., руководствуясь корыстными интересами, с целью получения материальной выгоды с помощью сети «Интернет» скачивал

[1] Приговор Мурашинского районного суда Кировской области от 25.04.2012 года // Судебные и нормативные акты РФ. URL: http://sudact.ru/.

вышеперечисленные программы, и, благодаря имеющимся у него навыкам и знаниям, загружал и устанавливал их на устройства других пользователей за денежное вознаграждение.

4. Увеличение количества социальных сетей, их активное рекламирование по различным каналам связи, а, следственно, увеличение количества пользователей. По данным, приведённым в глобальном отчёте Digital 2020 от международного агентства «We are social», среднестатистический россиянин проводит в социальных сетях 2 часа 26 минут в день. В январе 2020 года у 87% российских граждан на мобильных устройствах были установлены мессенджеры, а приложения социальных сетей - у 92% мобильных пользователей. Самое популярное мобильное приложение в России по количеству пользователей - WhatsApp. За ним следует Viber, и замыкает тройку лидеров приложение ВКонтакте. При этом интересным является тот факт, что именно в мобильном приложении ВКонтакте россияне тратят больше всего денежных средств.

Большую часть преступлений, совершённых в социальных сетях, составляют общественно опасные деяния, связанные с незаконным оборотом наркотических средств и психотропных веществ. В основном это незаконные приобретение и сбыт наркотиков, совершенные при помощи социальных сетей. Также встречаются приговоры, в которых фигурирует пересылка и контрабанда наркотических средств.

Вторую по величине группу общественно опасных деяний, совершаемых при помощи социальных сетей, составляют преступления, посягающие на имущественные отношения.

Совершение вымогательства при помощи социальных сетей зачастую сопровождаются неправомерным доступом к компьютерной информации, нарушением тайны переписки и подлежит дополнительной квалификации по ст. 272 и 138 УК РФ. Получив необходимые сведения или файлы, преступник в социальных сетях угрожает потерпевшему распространением позорящих его сведений, если тот не предоставит ему определённую сумму денежных средств, пароль от банковских карт или не совершит любое другое действие, интересующее злоумышленника.[1]

5. Рост количества несовершеннолетних пользователей социальных сетей. По данным социального исследования, проведённого Институтом развития стратегических инициатив города Ярославль, наибольшей популярностью среди подростков пользуется социальная сеть «ВКонтакте», на втором месте – Instagram, далее Facebook, Одноклассники и Twitter.

Правовые причины и условия интернет-преступности включают в себя:

1. Несовершенство российского уголовного законодательства в сфере борьбы как с компьютерной преступностью в целом, так и с интернет-преступностью в

[1] Соловьёв В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. №1. С. 60-72

частности. В первую очередь, это отсутствие нормативного правового закрепления многих понятий, связанных с информационно-компьютерной сферой (компьютерная программа, электрический сигнал и другие).

Многие правоведы говорят о том, что отдельные деяния, совершаемые хакерами с помощью интернет-ресурсов и приносящие вред человеку и обществу, не отражены в Уголовном кодексе, а соответственно не могут быть квалифицированы как уголовно наказуемые. Специалисты в компьютерных технологиях пользуются этим и продолжают осуществлять свою неправомерную деятельность.

Некоторые исследователи предлагают ввести уголовную ответственность за умышленное приобретение вредоносных программ с целью несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Это объясняется тем, что большая часть компьютерных преступников не обладают достаточными навыками по созданию компьютерных вирусов и вредоносных программ, поэтому, чтобы совершить преступление им приходится приобретать вредоносное ПО (программное обеспечение) на хакерских форумах и сайтах. Таким образом, они приобретают в сети Интернет уже готовый продукт и используют его.

2. Несовершенство судебной практики.

Отсутствие разъяснений Пленума Верховного суда Российской Федерации по вопросам квалификации и определения наказаний за совершение компьютерных преступлений (в том числе интернет-преступлений) оказывает негативное влияние на эффективность судебной практики, а также выработку единообразного подхода к толкованию и реализации уголовно-правовых норм в сфере компьютерных преступлений.

К кадровой причине относится:

1. Некачественная, порой безответственная работа руководителей организаций и отдела кадров при выборе персонала, профессиональная деятельность которого непосредственно связана с использованием персональных компьютеров, сети Интернет и других современных технологий. Работодатели часто не реагируют на небрежность пользователей ЭВМ на работе, что часто приводит к утечке информации.

Политическими причинами и условиями роста интернет-преступности являются:

1. Стремление государства занять передовые позиции в рейтинге стран мира по уровню развития информационно-коммуникационных технологий. Как следствие, направление ресурсов, в первую очередь финансовых, на развитие компьютерных технологий, усовершенствование показателей качества и скорости Интернета в стране, увеличение количества точек доступа к сети Интернет. Это создаёт новые возможности для совершения преступлений в сети Интернет или с его помощью самыми изощрёнными способами.

2. Отсутствие эффективного государственного контроля над киберпространством и средствами массовой информации. СМИ не только не призывает обще-

ство соблюдать меры по противодействию киберпреступности, но и нередко стараются оправдать преступников в этой сфере, акцентируя внимание на их уникальных навыках в области информационных технологий. Большинство хакерских сайтов находятся в свободном доступе для любого интересующегося пользователя, который желает начать «карьеру» в этом деле. Государству в лице правоохранительных органов необходимо усилить контроль за интернет-ресурсами и информацией, которая распространяется в сети Интернет. Многими исследователями предлагается дополнить п. 1 ч. 5 ст.15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» включением в реестр сайтов, распространяющих вредоносные компьютерные программы; информацию о способах совершения и сокрытия компьютерных преступлений, а также иную вредоносную компьютерную информацию. Введение данного положения представляется целесообразным, способным привести к снижению количество подобных сайтов и ограничить приобретение вредоносных компьютерных программ.

К техническим причинам и условиям преступности в Интернете можно отнести следующие положения: недостаточная защита доступа к электронной почте; отступление от технологических режимов обработки информации; недостаточный уровень защиты программного обеспечения; нарушение технологического цикла проектирования, разработки, испытаний и сдачи в промышленную эксплуатацию компьютерных систем; совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения; нарушение сроков изменения паролей пользователей; нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда и полное их отсутствие.[1]

Таким образом, проанализировав причины и условия роста количества преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет», можно утверждать, что они связаны со всеми основными сферами жизни общества (экономической, политической, социальной и другими). Необходимо понимать, что с развитием информационных технологий, количество причин интернет-преступности в России будет только увеличиваться. Это означает, что предупреждение и пресечение данного вида преступлений в современной России должно носить постоянный, всеохватывающий и комплексный характер. Законодателям и правоохранительным органам необходимо идти в ногу со временем, владеть информацией о новейших изобретениях в этой сфере, их технических характеристиках и возможностях, а также предполагать возможные последствия от их использования.

[1] Егорышев А.С. Обзор обстоятельств, способствующих неправомерному доступу к компьютерной информации // Вестник Калининградского института МВД России: Научно-теоретический журнал. Калининград: Калининградский ЮИ МВД России. 2002. № 2. С. 185.

Список использованных источников

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) "Об информации, информационных технологиях и о защите информации" // Доступ из Справочно-правовой системы «КонсультантПлюс»
2. Указ Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // Доступ из Справочно-правовой системы «КонсультантПлюс»
3. Егорышев А.С. Обзор обстоятельств, способствующих неправомерному доступу к компьютерной информации // Вестник Калининградского института МВД России: Научно-теоретический журнал. Калининград: Калининградский ЮИ МВД России. 2002. № 2. С. 185
4. Информационно-аналитический отчет по результатам социологического исследования «Роль и степень влияния социальных сетей в жизни подростков» // МКУ «Институт развития стратегических инициатив». Ярославль. 2018. С. 16
5. Соловьёв В.С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2016. №1. С. 60-723.
7. Официальный сайт международного агентства «We are social» // URL: https://datareportal.com/reports/digital-2020-july-global-statshot
8. Официальный сайт Министерства Внутренних дел Российской Федерации // URL: https://мвд.рф
9. Приговор Мурашинского районного суда Кировской области от 25.04.2012 года // Судебные и нормативные акты РФ. URL: http://sudact.ru/
10. Статистика по интернет-пользователям из глобального отчета Digital 2020, предоставленного международным агентством «We are social» // URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/

Сведения об авторах

Апасова Анастасия Геннадьевна – студентка 3 курса Алтайского филиала Российской академии народного хозяйства и государственной службы при Президенте российской Федерации.

Афанасьева Ольга Романовна – профессор кафедры «Уголовное право, уголовный процесс и криминалистика» Юридического института Российского университета транспорта, доктор юридически наук, доцент.

Афанасьев Павел Борисович – старший «Уголовное право, уголовный процесс и криминалистика» Юридического института Российского университета транспорта.

Бедеров Игорь Сергеевич – советник генерального директора АО «Национальная Инжиниринговая Корпорация», руководитель отдела специальных разработок АО «Технопарк Санкт-Петербурга», генеральный директор ООО «Интернет-Розыск».

Беззатеев Сергей Валентинович – заведующий кафедрой «Технологии защиты информации» Санкт-Петербургского государственного университета аэрокосмического приборостроения, доктор технических наук, доцент.

Бражников Дмитрий Анатольевич – доцент кафедры уголовно-правовых дисциплин ГКОУ ВО «Российская таможенная академия», кандидат юридических наук, доцент.

Бычков Василий Васильевич – декан факультета повышения квалификации Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент.

Вепрев Сергей Борисович – заведующий кафедрой информационных технологий Московской академии Следственного комитета Российской Федерации, доктор технических наук, старший научный сотрудник, полковник юстиции.

Власенко Екатерина Романовна, курсант 2 курса института судебной экспертизы Московского университета МВД России имени В.Я. Кикотя, рядовой полиции.

Волынский Александр Фомич – профессор кафедры криминалистики Московского университета МВД России им. В.Я. Кикотя, Заслуженный деятель науки РФ, Заслуженный юрист РФ, Почетный профессор Московской академии Следственного комитета РФ, доктор юридических наук, профессор.

Воронкова Дарья Константиновна – аспирант кафедры уголовно-правовых дисциплин Юридического факультета ГКОУ ВО «Российская таможенная академия».

Глушков Максим Рудольфович – заведующий лабораторией по исследованию проблем процессуальной деятельности следственных органов научно-исследовательского института ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», полковник юстиции.

Голоскоков Леонид Викторович – ведущий научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент, майор юстиции.

Емельянова Елена Александровна – старший преподаватель кафедры гражданского права и процесса Юридического факультета НИУ «Высшая школа экономики» (Санкт-Петербург), кандидат юридических наук.

Загрядская Екатерина Александровна – старший преподаватель кафедры уголовного права и криминологии Нижегородского филиала ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации», полковник юстиции.

Киселев Александр Петрович – руководитель Ижемского межрайонного следственного отдела следственного управления Следственного комитета Российской Федерации по Республике Коми, подполковник юстиции.

Краснова Наталья Евгеньевна – помощник судьи в Ленинском районном суде г. Санкт-Петербурга.

Лаур Александр Владимирович – преподаватель кафедры криминалистики Санкт-Петербургского университета МВД России, майор полиции.

Лебедева Анна Андреевна – доцент кафедры криминалистики ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации» кандидат юридических наук, подполковник юстиции

Маркова Елена Алексеевна – адъюнкт кафедры уголовного права Санкт-Петербургского университета МВД России.

Мироненкова Полина Олеговна – студент 2 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Михайлова Екатерина Евгеньевна – старший преподаватель кафедры уголовного процесса факультета подготовки следователей Санкт-Петербургской академии Следственного комитета, полковник юстиции, аспирант Санкт-Петербургской академии Следственного комитета.

Мочалкина Ирина Сергеевна – аспирант кафедры уголовного права и криминологии Юридического факультета МГУ им. М.В. Ломоносова.

Нестерович Сергей Александрович – доцент кафедры информационных технологий Московской академии Следственного комитета Российской Федерации, кандидат технических наук, полковник юстиции.

Николаев Вячеслав Николаевич – инженер, факультет комплексной безопасности ТЭК РГУ нефти и газа (НИУ) им. Губкина.

Пальцев Александр Анатольевич – руководитель отделения по расследованию преступлений, совершенных должностными лицами правоохранительных органов, 2 СУ (с дислокацией в городе Санкт-Петербург) ГСУ СК России, аспирант Санкт-Петербургской Академии СК России.

Перов Валерий Александрович – профессор кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации.

Петраков Сергей Викторович – заведующий кафедрой предварительного расследования факультета повышения квалификацией Санкт-Петербургской академии Следственного комитета, кандидат юридических наук, доцент.

Полянская Елена Петровна – преподаватель кафедры уголовного процесса Московского областного филиала Московского университета МВД России имени В.Я. Кикотя, майор полиции.

Прорвич Владимир Антонович – профессор кафедры уголовного процесса Московской академии Следственного комитета РФ, Почетный профессор Московской академии Следственного комитета РФ, доктор юридических наук, доктор технических наук, профессор.

Русскевич Евгений Александрович – доцент кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, подполковник полиции.

Санташов Андрей Леонидович – главный научный сотрудник научно-исследовательского отдела Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.

Скуковский Анатолий Геннадьевич - старший преподаватель кафедры криминалистики, судебно-экспертной и оперативно-розыскной деятельности Санкт-Петербургской академии Следственного комитета Российской Федерации, полковник юстиции.

Смелова Светлана Владимировна – преподаватель кафедры предварительного расследования Санкт-Петербургского университета МВД России, кандидат юридических наук.

Смушкин Александр Борисович – доцент кафедра криминалистики ФГБОУ ВО «Саратовская государственная юридическая академия».

Терехов Максим Геннадьевич – соискатель кафедры гражданского и трудового права, гражданского процесса Московского университета МВД России имени В.Я. Кикотя, инспектор отдела международного сотрудничества Московского университета МВД России имени В.Я. Кикотя.

Тимощенко Дарья Васильевна – курсант 4 курса факультета подготовки сотрудников для подразделений по работе с личным составом Санкт-Петербургского университета МВД России, рядовой полиции.

Ушаков Андрей Юрьевич – заведующий кафедрой уголовного процесса Нижегородского филиала ФГКОУ ВО «Санкт–Петербургской академии Следственного комитета Российской Федерации», кандидат юридических наук, доцент, полковник юстиции.

Фомичева Светлана Григорьевна – профессор кафедры «Технологии защиты информации» Санкт-Петербургского государственного университета аэрокосмического приборостроения, кандидат технических наук, профессор, Почетный работник ВПО

Харченко Сергей Владмирович – профессор кафедры криминалистики Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.

Цимбал Виталий Николаевич – доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, подполковник полиции.

Чернопёров Алексей Александрович – заместитель руководителя отдела криминалистики следственного управления Следственного комитета Российской Федерации по Хабаровскому краю и Еврейской автономной области, аспирант первого курса аспирантуры Санкт-Петербургской академии Следственного комитета Российской подполковник юстиции.

Чугунов Александр Александрович, заместитель начальника кафедры уголовного права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент, полковник полиции.

Шахматов Александр Владимирович – профессор кафедры оперативно-разыскной деятельности в ОВД Санкт-Петербургского университета МВД России, доктор юридических наук, профессор.

Шиян Валентина Ивановна – доцент кафедры «Уголовное право, уголовный процесс и криминалистика» Юридического института, Российского университета транспорта, кандидат юридических наук, доцент.

Юницкая Анастасия Дмитриевна – старший специалист 1 разряда Октябрьского районного суда города Санкт-Петербурга.

Ярославский Константин Сергеевич – старший преподаватель кафедры предварительного расследования факультета повышения квалификации Санкт-Петербургской академии Следственного комитета Российской Федерации, полковник юстиции.

ОБУЧАЮЩИЕСЯ

Балабаева Александра Дмитриевна – обучающаяся 5 курса ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Васильева Екатерина Павловна – студент 2 курса Санкт-Петербургской академии Следственного комитета Российской Федерации.

Воронова Валерия Игоревна – обучающаяся 3 курса Московской Академии Следственного комитета Российской Федерации (г.Москва).

Гаврилова Валерия Олеговна – студент 4 курса ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Даценко Кристина Олеговна – студент курса ФКГОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Забелина Мария Александровна – обучающаяся Московской академии Следственного комитета Российской Федерации, факультет подготовки криминалистов.

Капралова Алена Денисовна – обучающаяся 1 курса Московской академии СК РФ.

Кондрашова Александра Сергеевна – студент 1-го курса Московской академии Следственного комитета Российской Федерации группа Ю-1.3.

Кудайбергенова Диана Турлыбековна – студент 4 курса ФКГОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Ламыкина Софья Олеговна – студент 4 курса ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Лупандина Ирина Юрьевна – обучающаяся 2 курса направления подготовки 40.05.01 «Правовое обеспечение национальной безопасности», ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Мартынюк Эдуард Геннадьевич – обучающийся 2 курса ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации».

Некипелова Елена Ивановна – студент 2 курса, Московской академии Следственного комитета РФ.

Нечаева Лада Александровна – обучающаяся 1 курса Московской академии СК РФ.

Одегова Алёна Дмитриевна – студент 4 курса 171 учебной группы ФГКОУ «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Оленкова Евгения Николаевна – студент 4 курса ФКГОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Пантелеева Анастасия Олеговна – студент 4 курса ФКГОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Семенов Андрей Павлович – студент 4 курса ФКГОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Соловьёва Дарья Олеговна – студент 4 курса ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Сочка Полина Владимировна – студент 4 курса ФГКОУ ВО «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Цуканова Дарья Вадимовна – студент 4 курса 171 учебной группы ФГКОУ «Санкт-Петербургская академия Следственного комитета Российской Федерации».

Содержание

Стр.

Всероссийская научно-практическая конференция **«Противодействие киберпреступлениям и преступлениям в сфере высоких технологий»** (10 декабря 2020 г.) 3

Апасова А.Г. Некоторые вопросы обеспечения корпоративной безопасности 4

Афанасьева О.Р. Состояние и тенденции развития преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных технологий 6

Афанасьев П.Б. Состояние и тенденции развития преступлений, совершаемых с использованием информационно-телекоммуникационных технологий 10

Бедеров И.С. Проблемы и тенденции в расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий 15

Беззатеев С.В., Фомичева С.Г. Перспективные подходы к решению проблем компрометации биометрических данных 18

Бражников Д.А., Воронкова Д.К. Цифровые технологии в криминалистике 22

Бычков В.В., Харченко С.В. О понятии компьютерной преступности 26

Вепрев С.Б., Нестерович С.А. Социальная инженерия - основная тенденций развития преступности в киберпространстве 30

Волынский А.Ф., Прорвич В.А. Интегрирующая роль компьютерной криминалистики в выявлении, раскрытии и расследовании преступлений в сфере цифровой экономики 35

Глушков М.Р. К вопросу о необходимости судебного решения для извлечения сведений о сообщениях из мобильных устройств 43

Голоскоков Л.В. О модернизации парадигмы уголовного права в области противодействия преступлениям в сфере высоких и иных технологий 51

Емельянова Е.А. Проблемы взаимодействия Банка России с операторами связи при выявлении и расследовании преступлений, связанных с манипулированием рынком и неправомерным использованием инсайдерской информации 55

Загрядская Е.А. Проблемные вопросы квалификации преступного деяния, предусмотренного статьей 151-2 Уголовного кодекса Российской Федерации, совершенного в сети Интернет 60

Киселев А.П. Проблемы взаимодействия операторов сотовой связи, провайдеров, владельцев сайтов с правоохранительными органами при раскрытии и расследовании преступлений 64

Краснова Н.Е. Проблемы привлечения подростков к распространению экстремистских материалов через сеть Интернет 67

Лаур А.В., Тимощенко Д.В. Вопросы контроля мессенджеров в целях пресечения террористической деятельности 71

Лебедева А.А. Некоторые аспекты деятельности Следственного комитета Российской Федерации при расследовании киберпреступлений 74
Маркова Е.А. Тайное хищение денежных средств с банковского счета 77
Михайлова Е.Е. К вопросу о необходимости контроля и записи переговоров как следственного действия 84
Мочалкина И.С. К вопросу об особенностях правовой природы цифровых прав как предмета преступления 92
Нестерович С.А., Вепрев С.Б. Мошенничество в интернет 95
Николаев В.Н. Использование результатов оценки РЭО при расследовании уголовных дел 99
Перов В.А. Электронный след: понятие, виды, способы обнаружения и фиксации 103
Петраков С.В. Использование учетов при раскрытии и расследовании преступлений, совершаемых с использованием компьютерных и информационно-телекоммуникационных технологий 106
Полянская Е.П. Роль социальной инженерии в преступлениях, совершаемых посредством использования информационно-телекоммуникационных устройств и методы борьбы с ней 109
Прорвич В.А., Бычков В.В. Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершенных с использованием Интернета 114
Русскевич Е.А. Преступления, совершаемые в целях майнинга криптовалюты: вопросы квалификации 119
Санташов А.Л. Преступления экономической направленности, совершаемые в местах лишения свободы дистанционно 123
Скуковский А.Г., Мироненкова П.О. Некоторые проблемы, связанные с расследованием киберпреступлений 127
Смелова С.В. Актуальные вопросы квалификации преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий 132
Смушкин А.Б. Проблемы поиска электронных следов в системах распределенного хранения данных в процессе расследования 136
Терехов М.Г. Противодействие трансграничным схемам наркорасчетов и легализации наркодоходов с использованием современных платежных инструментов 141
Ушаков А.Ю. Особенности производства обыска при расследовании преступлений, совершаемых с использованием современных электронных технологий 145
Цимбал В.Н. Особенности борьбы с преступлениями в сфере компьютерной информации: виды преступлений, способы совершения и методы противодействия 149
Чернопёров А.А. Выявление и блокирование сайтов или страниц в социальных сетях как способ профилактики преступлений, совершаемых в сети Интернет 153

Чугунов А.А., Власенко Е.Р. Использование кибертехнологий как способ совершения посягательств на интересы личности, охраняемые уголовным законом 158
Шахматов А.В., Пальцев А.А. К вопросу противодействия коррупционным преступлениям, совершаемым с использованием современных электронных технологий 162
Шиян В.И. Криминологические аспекты противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий 168
Юницкая А.Д. Необходимость разработки регламента по идентификации электронной судебной документации 171
Ярославский К.С. Криминалистические аспекты расследования незаконной игорной деятельности, осуществляемой посредством сети Интернет 175

ОБУЧАЮЩИЕСЯ

Балабаева А.Д. Получение и анализ биллинговой информации при расследовании преступлений, связанных с безвестным исчезновением несовершеннолетних 180
Васильева Е.П. Криминалистическая характеристика киберпреступлений 184
Воронова В.И. Уголовно-правовой аспект противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей 187
Гаврилова В.О. Криминологические аспекты совершения преступлений против собственности с использованием информационно-телекоммуникационных сетей 190
Даценко К.О. Использование специальных знаний в области компьютерной техники в целях предупреждения киберпреступлений 193
Забелина М.А. Особенности проведения обыска в ходе расследования публичных призывов к осуществлению террористической деятельности, оправдания или пропаганды терроризма 198
Капралова А.Д., Нечаева Л.А. Проблемы, встречающиеся на пути расследования киберпреступлений 202
Кондрашова А.С. Особенности изъятия электронных следов преступлений и работы с ними 205
Кудайбергенова Д.Т. Криминологические аспекты борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей 210
Ламыкина С.О., Сочка П.В. Противодействие киберпреступлениям в банковской сфере РФ с применением специальных знаний в области компьютерной техники 214
Лупандина И.Ю. Криптовалюта как средство совершения преступлений 219
Мартынюк Э.Г. К вопросу об использовании знаний в области криптовалюты и технологии блокчейн в целях выявления, раскрытия, расследования и предупреждения киберпреступлений 223

Некипелова Е. И. Электронные следы и способы их изъятия 226
Одегова А.Д., Цуканова Д.В. Личность потерпевшего и его индивидуальная виктимность в механизме преступлений, совершаемых с использованием информационно-телекоммуникационной сети Интернет 230
Оленкова Е.Н. Предупреждение преступлений, совершаемых с использованием информационно-коммуникационных технологий и в сфере компьютерной информации 235
Пантелеева А.О., Семенов А.П. Криминологические аспекты предупреждения преступлений, совершаемых с использованием средств сотовой связи 239
Соловьёва Д.О. Причины и условия роста количества преступлений, совершаемых с использованием информационно-телекоммуникационной сети «Интернет» 243
Сведения об авторах 251

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПЛЕНИЯМ И ПРЕСТУПЛЕНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Всероссийская научно-практическая конференция

(Москва, 10 декабря 2020 года)

Редакционная коллегия обращает внимание, что статьи представлены в авторской редакции. Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законов об интеллектуальной собственности несут авторы публикуемых материалов

Подписано в печать 30.03.2021

Формат 60x90 1/16
Усл. печ. л. 16,25
Тираж 100 экз.
Печать офсетная
Заказ № 287

Отпечатано в типографии Московской академии
Следственного комитета Российской Федерации,
ул. Врубеля, д. 12