Информационные технологии в уголовно-правовой сфере

Под редакцией
Заслуженного юриста Российской Федерации,
доктора юридических наук, профессора ***А.И. Бастрыкина,***
доктора юридических наук, профессора ***А.Н. Савенкова***

Рекомендовано к изданию Научно-исследовательским институтом образования и науки в качестве монографии. Научная специальность «Международное право; европейское право»

Рекомендовано к изданию Международным учебно-методическим центром «Профессиональный учебник» в качестве монографии. Научная специальность «Международное право; европейское право»

Электронные версии книг
Издательства «ЮНИТИ-ДАНА» на сайте
Международной электронной библиотеки
«Образование. Наука. Научные кадры»
www.niion.org

ЮНИТИ
UNITY
Москва • 2023

УДК [343.5:004](470+571)
ББК 67.408.135(2Рос)
И74

Рецензенты:
заслуженный деятель науки РФ, заслуженный юрист РФ,
доктор юридических наук, профессор *Б.Я. Гаврилов*
(профессор кафедры управления органами расследования преступлений
Академии управления МВД России);
доктор юридических наук, доцент, эксперт РАН *А.В. Минбалеев*
(заведующий кафедрой информационного права и цифровых технологий Московского
государственного юридического университета имени О.Е. Кутафина (МГЮА)

Главный редактор издательства *Н.Д. Эриашвили*,
кандидат юридических наук, доктор экономических наук,
профессор, почетный работник сферы образования РФ,
лауреат премии Правительства РФ в области науки и техники,
лауреат премии Правительства РФ в области образования

И74 **Информационные** технологии в уголовно-правовой сфере: монография / под ред. А.И. Бастрыкина, А.Н. Савенкова. — М.: ЮНИТИ-ДАНА, 2023. — 279 с.

ISBN 978-5-238-03749-3

Агентство CIP РГБ

Монография подготовлена профессорско-преподавательским составом Московской академии Следственного комитета Российской Федерации и Института государства и права Российской академии наук с учетом современных тенденций науки и следственной практики. На основе анализа современных проблем теории и практики рассмотрены актуальные вопросы правового регулирования информационных технологий, проблемы уголовно-правового противодействия использованию информационных технологий в преступных целях, специфика информационных технологий в уголовном судопроизводстве. Даны криминалистические рекомендации по расследованию преступлений, совершенных с использованием информационных технологий.

Законодательство приведено по состоянию на 1 апреля 2023 г.

Для научных и практических работников правоохранительных органов, преподавателей юридических вузов, аспирантов и других юристов.

ББК 67.408.135(2Рос)

ISBN 978-5-238-03749-3

Авторы

О.Ю. Антонов, доктор юридических наук, доцент, декан факультета подготовки криминалистов Московской академии СК России, — п. 4.1 гл. 4 (в соавт. с Т.А. Сааковым)

А.И. Бастрыкин, доктор юридических наук, профессор, Председатель Следственного комитета Российской Федерации, заслуженный юрист Российской Федерации, — введение, п. 4.4 гл. 4

А.А. Бессонов, доктор юридических наук, доцент, ректор Московской академии Следственного комитета Российской Федерации, — п. 3 гл. 4

Я.Н. Ермолович, доктор юридических наук, профессор кафедры уголовного права и криминологии Московской академии СК России, — п. 2.2, 2.3 гл. 2 (в соавт. с В.А. Перовым)

С.В. Маликов, доктор юридических наук, заместитель директора Института государства и права РАН по научной работе, — п. 1.1 гл. 1, п. 2.1 гл. 2

Н.В. Османова, кандидат юридических наук, доцент, декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии СК России, — пар. 3.1 гл. 3

В.А. Перов, профессор кафедры уголовного права и криминологии Московской академии СК России, — п. 2.2, 2.3 гл. 2 (в соавт. с Я.Н. Ермоловичем)

Т.А. Полякова, доктор юридических наук, профессор, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, главный научный сотрудник, заслуженный юрист Российской Федерации, — п. 1.2 гл. 1 (в соавт. с А.А. Смирновым, А.И. Химченко); п. 1.3 гл. 1 (в соавт. с А.А. Смирновым)

В.А. Прорвич, доктор юридических наук, доктор технических наук, профессор, профессор кафедры уголовного процесса Московской академии СК России, — п. 3.3 гл. 3

Т.А. Сааков, кандидат юридических наук, старший преподаватель кафедры судебно-экспертной и оперативно-розыскной деятельности Московской академии СК России, — п. 4.1 гл. 4 (в соавт. с О.Ю. Антоновым); п. 4.2 гл. 4 (в соавт. с С.Ю. Скобелиным)

С.Ю. Скобелин, кандидат юридических наук, доцент, доцент кафедры информационных технологий и организации расследования киберпреступлений Московской академии СК России, — п. 4.2 гл. 4 (в соавт. с Т.А. Сааковым)

А.А. Смирнов, доктор юридических наук, доцент, ведущий научный сотрудник 3-го отдела НИЦ № 4 ВНИИ МВД России, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, — п. 1.2 гл. 1 (в соавт. с Т.А. Поляковой, А.И. Химченко), п. 1.3 гл. 1 (в соавт. с Т.А. Поляковой)

А.И. Химченко, кандидат юридических наук, старший преподаватель кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), — п. 1.2 гл. 1 (в соавт. с Т.А. Поляковой, А.А. Смирновым)

Ю.А. Цветков, кандидат юридических наук, доцент, заведующий кафедрой уголовного процесса Московской академии СК России, — п. 3.2 гл. 3

ВВЕДЕНИЕ

В последние десятилетия планета находится на новом витке научно-технического прогресса, обусловленного глобальной цифровой трансформацией. Цифровые технологии глубоко проникли практически во все сферы деятельности современного человека, общества и государства, и их эффективное применение стало фактором ускорения экономического развития государства и совершенствования функционирования общественных и государственных институтов. Цифровая экономика формирует новую систему расчетов, приводит к появлению новых видов нематериальных активов и трансформации традиционных материальных. Например, возникла и активно развивается цифровая валюта. Мобильные системы и социальные сети порождают новые виды коммуникации между людьми, объектами виртуального и реального мира. Искусственный интеллект способствует разработке новых технологий и в какой-то степени заменяет человека.

Одновременно возникают негативные явления, обусловленные использованием таких технологий в противоправных целях. Количество преступных деяний возрастает параллельно с динамикой распространения технологий. Киберпространство используется для вовлечения молодежи в различные радикальные течения, нанесения вреда детям, финансирования терроризма. Подключение к сетям общего пользования расширяет географию лиц, вовлеченных в преступную деятельность, а применение свободно распространяемого программного обеспечения не требует от злоумышленников высокой квалификации.

Динамика и беспрецедентная глубина происходящих преобразований предопределяют необходимость научных исследований характера угроз охраняемым законом правоотношениям.

В связи с этим в настоящей работе выделены факторы, влияющие на состояние преступности в информационной сфере; определены наиболее значимые цифровые угрозы для современного общества и Российского государства; проанализированы криминогенные риски наиболее распространенных современных технологий: искусственный интеллект, большие данные, блокчейн, Интернет вещей. Проведено научное исследование правового режима ключевых информационных технологий на основе анализа российских нормативных правовых актов, выделены существующие направления государственного регулирования в рассматриваемой сфере, проанализировано состояние ключевых элементов, образующих такие технологии.

Серьезное внимание в данной монографии уделено изучению состояния преступности в сфере информационных технологий как угрозе национальной и международной информационной безопасности. В данном контексте немаловажным представляется тот факт, что процессы глобализации как на межгосударственном уровне, так и в интернет-пространстве обусловили необходимость формирования международных механизмов борьбы с киберпреступностью. Поэтому в работе изучены проблемы правового регулирования международного взаимодействия борьбы с преступностью в сфере информационных технологий, рассмотрены подходы к формированию единого понятийного аппарата и видов рассматриваемых преступлений.

Наиболее активно информационные технологии использует финансовая сфера, позволяющая осуществлять финансовые операции с цифровой валютой, за которой порой стоят и противозаконные финансовые операции, и запрещенные законом сделки криминального характера. В связи с этим авторами даны понятие и классификация цифровой валюты, описан ее правовой режим, выявлены сложности, возникающие в следственной практике.

Преступления с использованием информационных технологий совершаются, как правило, группой лиц различной степени организации. При этом наличие у одного из них специальных знаний в данной сфере позволяет использовать информационные технологии в преступных целях с максимальной для себя и ос-

тальных соучастников степенью анонимности. Поэтому один из параграфов работы посвящен проблемам соучастия и стадий в преступлениях, совершенных с использованием информационных технологий, а также путям их решения.

Использование информационных технологий при совершении преступлений обусловило потребность в разработке уголовно-процессуального инструментария, способствующего реализации назначения уголовного судопроизводства. Досудебное производство по данной категории уголовных дел приобретает выделенные характерные черты, например: типичные поводы возбуждения уголовного дела, уголовно-процессуальная специфика определения места совершения преступления и подследственности уголовных дел, специальная процедура изъятия электронных носителей информации и копирования с них информации, с учетом которых в настоящем исследовании предложены пути его оптимизации.

Особое внимание с учетом зарубежного опыта уделено цифровой трансформации уголовного судопроизводства, реализуемой в трех направлениях: применение дистанционных технологий производства следственных и судебных действий преимущественно путем расширения возможностей использования средств видео-конференц-связи, развитие электронного документооборота, аудио- и видеопротоколирование, внедрение искусственного интеллекта в правосудие и процессуальную деятельность следователя, прокурора и суда.

Предложены алгоритмы формирования доказательств и доказывания по уголовным делам о преступлениях, совершенных с использованием информационных технологий.

Изучение следственной практики демонстрирует, что при расследовании различных видов преступлений в качестве источника криминалистически значимой информации все чаще выступают следы преступной деятельности, образуемые при помощи использования информационных технологий. С учетом многообразия взглядов о сущности и наименовании таких следов в научной литературе предложены авторские понятие и классификация таких следов по двум основаниям — степени опосредованности воздействия пользователя на компьютерную систему и результату этого воздействия. Описана существующая практика расследования преступлений, совершенных с использованием информационных

технологий, следственными органами Следственного комитета Российской Федерации и направления ее совершенствования.

Настоящее монографическое исследование посвящено также разработке научно-практических рекомендаций, направленных на устранение имеющихся пробелов в криминалистике, связанных с собиранием следов преступной деятельности, оставленных на электронных носителях информации и удаленных серверах, а также разработке тактических подходов проведения отдельных следственных действий и использования специальных знаний при расследовании преступлений, совершенных при помощи информационных технологий.

Представляется, что описанные в работе теоретические положения, сформулированные выводы и практические рекомендации могут быть использованы в науке и практике борьбы с преступностью в сфере информационных технологий.

Александр Иванович Бастрыкин,
Председатель Следственного комитета
Российской Федерации,
заслуженный юрист Российской Федерации,
доктор юридических наук, профессор

Глава 1

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ: ПОНЯТИЕ, ПРАВОВОЙ РЕЖИМ, УГОЛОВНО-ПРАВОВЫЕ РИСКИ

1.1. Тенденции и риски развития информационных технологий

С.В. Маликов[1]

Цифровые технологии глубоко проникли в структуру повседневного существования современного человека, стали универсальным и рутинным посредником в самых разных сферах жизни (труд, быт, общение, образование, культура). Цифровизация как социотехнический процесс создает новые возможности и вызовы. Широкое внедрение цифровых технологий в повседневную жизнь облегчает выполнение многих рутинных операций и способствует решению ряда социальных проблем (например, расширяется доступ к образованию, появляются новые возможности для осуществления трудовой деятельности). Одновременно возникают негативные социальные и психологические явления, которые отрицательно влияют на качество жизни людей (например, такие явления, как цифровой разрыв, агрессия и мошенничество в Интернете)[2].

Внедрение цифровых технологий происходит быстрее, чем внедрение любых других инновационных разработок в истории человечества: всего за два десятилетия цифровыми технологиями

---

[1] Сергей Владимирович Маликов — заместитель директора Института государства и права РАН по научной работе, доктор юридических наук.

[2] См.: *Щекотин Е.В.* Концепция качества жизни в условиях цифровизации общества: социолого-управленческие аспекты: Автореф. дис. ... д-ра социол. наук. М., 2023. С. 2.

удалось охватить около 50% населения развивающихся стран и преобразовать с их помощью общества. Так, в секторе здравоохранения передовые технологии, основанные на использовании искусственного интеллекта, помогают спасать жизни людей, диагностировать заболевания и увеличивать продолжительность жизни.

В области образования обеспечение виртуальной учебной среды и дистанционного обучения позволило участвовать в программах тем учащимся, которые в противном случае не имели бы такой возможности. Кроме того, благодаря использованию систем на базе блокчейна государственные услуги становятся более доступными, предоставляющие их учреждения — более подотчетными, а в результате применения искусственного интеллекта процессы становятся менее бюрократизированными. Большие данные могут также способствовать развитию более гибких и точных политических стратегий и программ[1].

Сейчас планета находится в стадии глобальной цифровой трансформации, и недавняя пандемия только ускорила все процессы, связанные с технологиями. Согласно интегральному показателю Ростелекома за 2022 г.[2], который учитывает количество научных публикаций, патентов и объем инвестиций в технологию, искусственный интеллект занимает в последнее время лидирующую позицию в ежегодном мониторинге трендов цифровизации. Лидером по объему инвестиций стало направление цифровой медицины (e-Health). По патентной активности, которая говорит о близкой коммерциализации научных открытий, лидируют мобильные сети (142,2 тыс. патентов) и искусственный интеллект (140,6 тыс.).

В целом топ-10 трендов цифровизации выглядит следующим образом:

1) искусственный интеллект (Artificial Intelligence);
2) альтернативная энергетика (Alternative energy);
3) мобильные сети (Mobile networks);
4) цифровое здравоохранение (e-Health);

---

[1] См.: *Последствия* использования цифровых технологий. [Электронный ресурс]. Режим доступа: https://www.un.org/ru/un75/impact-digital-technologies (дата обращения: 23.03.2023).

[2] См.: *Мониторинг* глобальных трендов цифровизации [Электронный ресурс]. Режим доступа: https://www.company.rt.ru/upload/iblock/109/rostelekom_moni-toring_2022.pdf (дата обращения: 23.03.2023).

5) изучение рака (Cancer research);
6) вычислительная биология (Computational biology);
7) интеллектуальный анализ данных (Data mining);
8) социальные сети (Social Media);
9) информационная безопасность (Information security);
10) робототехника (Robotics).

Усиление данных процессов происходит во всем мире, в том числе России, постоянно увеличивающей расходы на развитие цифровой экономики (рис. 1.1)[1].

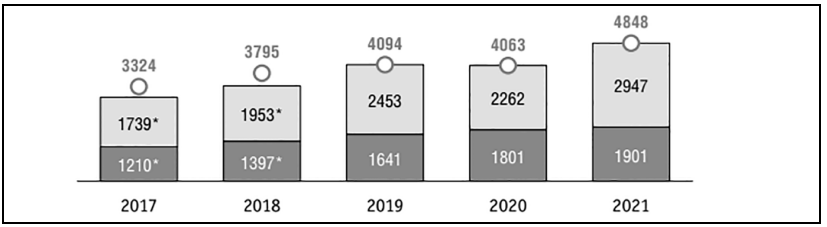

Рис. 1.1. **Затраты на развитие цифровой экономики в Российской Федерации в 2017—2021 гг.**

К наиболее значимым тенденциям в информационной сфере в краткосрочной перспективе специалисты относят следующие.

1. *Fintech: рост экосистем и доминирование крупных игроков.* Рынок финансовых технологий — один из самых быстрорастущих и динамичных среди всех направлений бизнеса. Изменения, происходящие на нем, по закону цепной реакции затрагивают и соседние сферы. Следует ожидать продолжения активной интеграции реального сектора и финансовых структур и следующее за этим укрупнение банковских экосистем. Скорее всего, в дальнейшем главные игроки рынка продолжат аккумулировать все больше и больше сфер нашей жизни в рамках своих сервисов, например доставку лекарств, продуктов и даже контента.

2. *Искусственный интеллект: рост спроса на ИИ-аналитиков и автоматизация целых профессий*. Глобальная автоматизация и цифровизация неизбежно ведут к отмиранию устаревших про-

[1] См.: *Цифровая* экономика 2022 (НИУ ВШЭ в партнерстве с Минцифры России и Росстатом) [Электронный ресурс]. Режим доступа: https://rosstat.gov.ru/folder/154885?print=1 (дата обращения: 23.03.2023).

фессий и появлению новых, отвечающих на вызовы современности. Вполне вероятно, что искусственный интеллект (далее — ИИ) сможет заменить некоторые профессии: чем более рутинной оказывается работа, тем проще ее автоматизировать. В частности, уже достигнут большой прогресс в массовой автоматизации бухгалтерского учета и кадрового документооборота. Это связано с тем, что государство постепенно берет на себя все больше и больше функций администрирования, вводятся новые законы, регулирующие работу с документами в электронном виде. Когда перевод межведомственного общения в цифровой формат полностью завершится, около 50—70% всех государственных решений сможет приниматься в автоматическом режиме по протоколам.

3. *Беспилотный транспорт и доставка.* За два года общество привыкло к ковидной реальности: перестроились привычные процессы, люди научились комфортно существовать в новом мире. Логично предположить, что тренд на развитие беспилотного транспорта просто неизбежен. Вслед за ретейлом эволюционировать в сторону бесконтактной доставки будет общественный транспорт — частные такси и городские автобусы призваны со временем занять место личных средств передвижения. Согласно данным аналитиков Canalys, в 2020 г. по всему миру было продано 11,2 млн машин, оснащенных автопилотом второго уровня (с частичной автоматизацией), что на 78% больше, чем в 2019 г. Очевидно, что этот тренд будет продолжать набирать обороты[1].

В среднесрочной перспективе будут стремительно развиваться и выделяться среди ведущих технологий квантовые вычисления, мобильность (в автомобильной отрасли) и цифровые двойники. Они станут определять основные направления развития[2].

Квантовые вычисления. Появятся экономичные и доступные способы передачи квантовых систем в руки исследователей из университетов, групп специалистов по обработке данных и ученых. Квантовые линии связи позволяют передавать большие мас-

[1] См.: *Как* изменится мир в 2022 году и куда приведет цифровая трансформация? [Электронный ресурс]. Режим доступа: https://www.banki.ru/news/columnists/?id=10960538 (дата обращения: 23.03.2023).

[2] См.: *2022* год и далее: технологии, которые изменят цифровое будущее. [Электронный ресурс]. Режим доступа: https://www.comnews.ru/content/218319/2022-01-20/2022-w03/2022-god-i-dalee-tekhnologii-kotorye-izmenyat-cifrovoe-buduschee (дата обращения: 23.03.2023).

сивы данных с высокой скоростью, причем они надежно зашифрованы, так как в основе лежит технология кодирования и передачи данных в квантовых состояниях фотонов.

Будущее мобильности. Автомобильная промышленность трансформируется на нескольких уровнях. Она быстро становится отраслью, управляемой данными, причем это касается буквально всего — от развлечений до обеспечения безопасности и таких крупных прорывных проектов, как автоматизированная доставка товаров и «автомобиль как сервис». В экосистеме автомобильной отрасли акценты будут быстро смещаться с механических систем на индустрию данных и вычислений. Отрасль продолжит свое развитие в направлении цифровой трансформации и более глубокого взаимодействия с ИТ-экосистемами.

Цифровые двойники. Цифровые двойники станут основной движущей силой цифровой трансформации 3.0. В них для создания симуляций, которые позволяют предсказать, как продукт или процесс будет функционировать, используются данные реального мира. Этот тип анализа данных изменит будущее бизнеса. С учетом всех возможных сценариев использования рынок цифровых двойников, по прогнозам, в ближайшие годы будет быстро расти.

В то же время информационные технологии подвергают организации и отдельных лиц целому ряду новых рисков, возникающих в результате атак с использованием цифровых интерфейсов. К ним относятся атаки типа «отказ в обслуживании» (DdoS), нарушения конфиденциальности и целостности данных на корпоративных и персональных устройствах, а также вирусы, способные нанести ущерб компьютерной инфраструктуре.

Специфика отклоняющегося поведения в цифровой среде связана с факторами масштаба, открытости технологических решений, появления новых цифровых сущностей и распределенного участия в преступном деянии.

С точки зрения *фактора масштаба* число преступников и количество посягательств фактически не ограничены и растут параллельно с ростом и динамикой распространения технологий. Подключение к сетям общего пользования расширяет географию вовлеченных в преступную деятельность, поскольку средства реализации преступления (специализированное программное обеспечение) может в любой точке планеты создавать гражданин, имеющий определенные навыки. Атака требует лишь подключе-

ния к Интернету. Из-за свободного распространения инструментария для совершения преступлений от злоумышленников уже не требуется высокой квалификации, а возможность использовать автоматизированные средства для проведения массовых атак ставит под угрозу огромное число пользователей и информационных систем. Вероятность проведения удаленных атак повышает сложность установления субъекта, осуществляющего преступные деяния, и снижает его чувство ответственности.

Фактор открытости заключается в том, что взрывной технологический рост обусловлен, в частности, тем, что многие компании и группы открывают доступ к своим разработкам и используют чужие на свободной основе. В результате множатся и технологические решения, и ошибки, а механизм распространения позволяет маскировать под полезные программные продукты зловредные программы и массово их сбывать. Кроме того, информация об уязвимостях информационных систем и программного обеспечения (ПО), способствующих совершению преступления, распространяется свободно, в том числе самими авторами ПО. Цель такого уведомления состоит в побуждении пользователей принять меры для ликвидации уязвимостей, однако зачастую эту информацию используют злоумышленники.

Значение *фактора новых цифровых сущностей* заключается в том, что в цифровом пространстве появляются сущности, у которых нет прямых аналогов в реальной жизни, но которые имеют финансовый эквивалент и влияние на объекты реального мира. Например, криптовалюта может быть конвертирована в валюту любой страны. Вычислительные мощности информационных систем — это сущности, обладающие стоимостным эквивалентом (как объект аренды), которые также могут быть задействованы в создании нематериальных сущностей, имеющих стоимостный эквивалент, игровую валюту или криптовалюту. Это делает информационную систему объектом атаки вне зависимости от ее предназначения.

Фактором распределенного участия является то, что существует несколько типов лиц с разными ролями, участвующих в совершении преступления. Их можно разделить на четыре группы:

1) лица, непосредственно совершающие преступление;

2) разработчики и распространители инструментов организации атак;

3) разработчики систем, имеющих уязвимости;

4) эксплуатанты, нарушающие правила эксплуатации.

Практически в каждом преступлении участвуют представители указанных групп, мера их ответственности определяется для каждого состава преступления. Проблема цифровой безопасности состоит, в частности, в том, что зоны ответственности если и установлены, то локализованы в рамках одной системы, на правовом уровне нет общего подхода к распределению ответственности за создание условий для преступления.

Применительно к отдельным гражданам эксперты обобщенно выделяют следующие наиболее значимые цифровые угрозы:

1) алгоритмическая обработка данных цифровыми платформами и государством может привести к нарушению права на неприкосновенность частной жизни;

2) цифровая дискриминация граждан государством и частными корпорациями на основе злоупотребления персональными данными и накопления больших данных о гражданах;

3) кибератаки и компьютерное мошенничество, направленные против человека, государства и бизнеса;

4) кибербуллинг, троллинг, иные акты агрессии в цифровой среде, направленные против граждан;

5) информационные войны в киберпространстве, рост числа «фейковых новостей» и спланированных кампаний по дезинформации в Интернете, в том числе с использованием современных технологий синтезирования медиаконтента (DeepFake);

6) усиливающиеся в условиях геополитической и корпоративной борьбы информационные войны за овладение массовым сознанием и контроль над цифровым пространством;

7) появление новых способов мониторинга и контроля со стороны государств (например, социальных рейтингов), основанных на сборе и анализе данных и влияющих на принятие решений, значимых для жизни граждан[1].

С учетом ограниченного объема приведем примеры криминогенных рисков наиболее распространенных современных технологий: ИИ, большие данные, блокчейн, Интернет вещей.

---

[1] См.: *Влияние* процессов цифровизации на права человека и развитие гражданского общества [Электронный ресурс]. Режим доступа: https://publications.hse.ru/articles/695233092 (дата обращения: 23.03.2023).

Искусственный интеллект

Искусственный интеллект — это область научных знаний и технологий создания интеллектуальных машин и интеллектуального программного обеспечения. Также ИИ называют свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека. Одной из ключевых особенностей интеллектуальных вычислительных систем является их способность приобретать знания посредством обучения (самомодификации) и применять эти знания для решения проблем. Угрозы безопасности систем ИИ могут реализовываться в разных сферах, приведем наиболее вероятные.

1. *В транспортной отрасли.* Злоумышленники могут нарушать штатную работу автономных транспортных средств посредством провокаций, приводящих к некорректной реакции транспорта на знаки ограничения проезда или скорости. К началу 2019 г. было опубликовано более 100 научных работ, в которых показаны разнообразные способы атак, имеющих целью вызвать ошибки системы распознавания изображений. Например: если маленький, трудноразличимый человеком стикер наклеить на дорожный знак, система ИИ будет воспринимать его как другой знак, что при специальном выборе места атаки может спровоцировать аварию. За счет выявления уязвимости алгоритма ИИ и несложного механизма ее реализации появляются угрозы не только для информационной системы, но и для жизни и здоровья людей.
2. *В системах контроля доступа.* Все более широкое распространение получают системы распознавания лиц в системах контроля физического доступа. Эти системы гораздо удобнее, чем RFID-карты, ключи или использование ПИН-кодов. Системы распознавания лиц снижают время, которое тратится на аутентификацию, и повышают долю эффективного рабочего времени сотрудников организаций. В настоящее время независимые исследования показывают, что многие системы распознавания образов можно обойти при помощи специальных очков, что позволит проникнуть на охраняемую территорию, украсть материальные ценности или обмануть банкомат или платежную систему.

3. *В системах обнаружения мошенничества с кредитными картами.* В некоторых системах обнаружения мошенничества специальный аналитический инструмент (классификатор логистической регрессии) применяется для выявления транзакций с признаками мошенничества, которые блокируются до детального выяснения их валидности. Однако он тоже может подвергнуться атаке, и мошеннические транзакции останутся незамеченными.
4. *В системах интеллектуальной идентификации человека.* Для усиления контроля выполнения «чувствительных» финансовых операций используются алгоритмы, определяющие по специфичности нажатия клавиш, что данные вводит человек, и идентифицирующие личность человека. Однако злоумышленники научились создавать состязательные выборки, которые обманывают весьма точный в нормальном режиме работы классификатор. После исследовательской атаки алгоритм начинал определять искусственно созданный клавиатурный ввод как принадлежащий конкретному пользователю — человеку.

Большие данные

Большие данные (Big Data) — это крайне большой объем структурированных и неструктурированных данных произвольного типа, обрабатываемый в горизонтально масштабируемых информационных системах. Назначение систем Big Data — помогать в принятии решений и инициировать действия на основе анализа цифровой информации. При помощи систем Big Data принимаются решения о необходимости профилактики эпидемий, об изменении полетного графика воздушных судов, о пригодности деталей автомобиля для эксплуатации, о необходимости провести внеплановый ремонт на строительных объектах и многие другие.

Взрывной рост использования и развития вызвал и проблему с обеспечением организационных мер безопасности. На этапе эксперимента и создания пилотных моделей системой больших данных управляют специалисты, ответственные за сбор, предоставление и анализ информации, т.е. специалисты в решении прикладных задач. Объем данных и общая ценность системы со вре-

менем растут, однако при переходе к промышленной эксплуатации ответственных за безопасность системы зачастую забывают назначить, вследствие чего система может оказаться не только изначально спроектирована без учета необходимости принятия мер безопасности, но и в процессе создания и эксплуатации не будет приведена к необходимому уровню защищенности.

Еще одна специфика безопасности больших данных — использование открытых технологических разработок. Например, поиск и обнаружение зависимостей в данных осуществляются при помощи специальных аналитических инструментов. Многие инструменты, используемые при обработке больших данных и в интеллектуальной аналитике, имеют открытый исходный код, т.е. представляют собой свободно распространяемый программный код и его описание. Это дает возможность на его основе создавать новые системы посредством копирования и доработки открытого кода. Зачастую использование осуществляется без детального изучения скопированного исходного программного кода и в случае, если код был получен не из доверенного источника, его использование может привести к появлению «черного хода» в новой системе.

Высокая динамика развития систем. Современная ситуация такова, что в коммерческих организациях постоянно создается управленческое давление, стимулирующее быстрое принятие решений при разработке ИТ-решений и построении ИТ-систем. В связи с тем что формирование требований к безопасности и применение мер безопасности замедляют скорость развития систем и их производительность, специалисты по безопасности зачастую отстраняются от участия в формировании архитектурных и бизнес-решений, поскольку рассматриваются как объективный фактор снижения скорости роста деловой активности компании. Риски, порождаемые слабой защитой данных, игнорируются, несмотря на то что они хорошо известны и у многих компаний есть собственный опыт получения финансового ущерба в результате реализации рисков безопасности.

Использование распределенных инфраструктур. Большая часть существующих систем больших данных управляет огромным количеством распределенных узлов обработки данных, обеспечивает взаимосвязь между значительным количеством интегрированных и смежных систем для обеспечения быстрого сбо-

ра и анализа информации. Сбор и обработка больших данных, основанная на использовании распределенных ресурсов, чаще всего осуществляются посредством интеграции с облачными ресурсами, что приводит к необходимости обеспечить системе доступ в Интернет. В результате тесная интеграция с сетями общего пользования негативно влияет на информационную безопасность распределенной системы.

Классические проблемы контроля доступа. Как и в случае с классическими корпоративными ИТ-системами, в системе больших данных очень важно обеспечить процедуры аутентификации и авторизации, которые определяют, что пользователь именно тот, за кого себя выдает, и устанавливают уровни доступа и полномочий в системе. Вероятный ущерб от несанкционированного доступа в системах больших данных существенно выше, чем в классических прикладных системах.

Сюда же можно отнести: проблему простых паролей; бесконтрольную передачу и тиражирование паролей; использование одинаковых паролей в нескольких системах; потерю аппаратных средств авторизации; использование устройств, не соответствующих корпоративной политике безопасности; некомпетентное управление привилегированным доступом; необоснованное повышение уровня доступа в системах. Еще одним фактором, уменьшающим защищенность информационных систем больших данных, является практика использования собственного оборудования сотрудников.

Отсутствие единых стандартов. В настоящее время при создании систем больших данных многие архитекторы и разработчики руководствуются весьма расплывчато сформулированными подходами или, наоборот, частными специализированными практиками отдельных отраслевых лидеров. Общепринятых стандартов в области больших данных в настоящее время нет.

Небезопасные веб-интерфейсы. Многие веб-интерфейсы устройств, являющиеся узкоспециальными веб-сайтами, имеют ряд уязвимостей безопасности, характерных именно для веб-решений. Реализация уязвимостей т.е. успешная атака на веб-интерфейс, позволяет киберпреступникам получить доступ к данным и/или возможность использовать ее функционал. Веб-интерфейсы обычно служат для просмотра и обработки данных независимо от их размера. Такие давно известные методы взлома сай-

тов, как SQL-инъекция, все еще эффективны против веб-интерфейсов, которые не проверяют вводимые данные.

Отсутствие базовых средств контроля безопасности. Эта системная и нередко встречающаяся уязвимость заключается в том, что принципы безопасности зачастую не рассматриваются как необходимые принципы проектирования. Компании не закладывают в продуктивную модель то, как они будут защищать свои хранилища больших данных в процессе эксплуатации, не конструируют механизмов проактивной и реактивной защиты (например, сканирование и анализ угроз, защита периметра), не обеспечивают фильтрацию потоков данных в режиме реального времени, чтобы выявить и нейтрализовать угрозы безопасности и аномалий. При этом зачастую недостатки подсистем безопасности, которые можно обнаружить в системах больших данных, связаны с применением примитивных, уязвимых механизмов аутентификации — это, например, идентификация по учетной записи и паролю. Еще одна распространенная уязвимость — отказ от создания безопасных каналов доступа к базам данных по сетям общего пользования.

Бессистемное использование средств маскировки и шифрования. Даже при наличии средств сетевой защиты применение безопасных механизмов надежной передачи данных от конечных точек к системам не всегда проводится должным образом. Необходимость часто перенаправлять потоки ведет к появлению каналов обмена данными, которые по тем или иным причинам обходят использование механизма шифрования. В такой ситуации возникают потоки незащищенных данных.

В настоящее время назрела необходимость разработки комплекса четкой и всеобъемлющей нормативной базы, регламентирующей поведение тех, кто оперирует большими данными. Нормы должны недвусмысленно определять права и ограничения на сбор, передачу и другие виды обработки, обеспечивать принципы обработки минимально необходимого состава и объема собираемых данных, прозрачности их использования и распространения (в том числе и продажи), пресечение использования, не соответствующего декларированным целям сбора, нарушения прав физических лиц и организаций. В настоящее время практически применимых норм нет ни в области уголовного права, ни в области административного права.

Блокчейн

Блокчейн — это тип электронного регистра для записи данных о транзакциях любого вида, которым нужно обеспечить постоянное хранение и защиту от несанкционированного доступа и изменений. Блокчейн функционирует как база данных, не имеющая центрального хранилища, которая управляется компьютерами, принадлежащими к сети блокчейн с равными полномочиями. Каждый из компьютеров в сети поддерживает копию регистра, чтобы предотвратить его потерю, все копии обновляются и проверяются одновременно. Иными словами, это регистр транзакций, хранящийся одновременно у всех его пользователей, защита которого обеспечивается шифрованием и технологиями электронной подписи. У данного регистра нет управляющего центра и администратора, который имел бы полномочия, превосходящие полномочия пользователей.

В большинстве случаев самыми легкими объектами атак являются пользователи блокчейна. В первую очередь из-за менталитета предприятий малого бизнеса, стартапов, в которых безопасность отодвигается на задний план. Еще одно направление атак — атаки на основе модификации широко распространенных блокчейн-систем, например, на базе Bitcoin и Ethereum, уязвимости которых широко известны.

Одна из слабых сторон технологии заключается в том, что она основана на предположении, что технологические операции блокчейна гарантированно распределены. В частности, ни одна организация или совместная группа не может представлять собой более чем 50% участников сети одновременно. Нарушение этого правила дает возможность проводить атаку большинства: если доля ресурсов злоумышленников более 50%, они могут обрабатывать блоки быстрее, чем все остальные участники, создавая свои собственные цепочки исключительно по своему пожеланию. Эта возможность помогает реализовывать такие операции, как осуществление двойных расходов, когда одну и ту же монету можно потратить несколько раз или исказить получателя криптомонеты, замкнув операцию перевода на себя.

Еще одна уязвимость заключается в том, что большая часть узлов участников блокчейна является доверенными. В ситуации, когда пользователь не способен соединиться ни с одним доверен-

ным узлом, повышается вероятность реализации атаки Sybil, при которой злоумышленник заставляет жертву общаться только с вредоносными узлами. Злоумышленник может контролировать то, к какой информации, включая сам реестр блокчейна, может получить доступ жертва, и полностью управлять записями жертвы в реестр. Для атаки Sybil особенно уязвимы небольшие корпоративные сети.

Другой уязвимостью является возможность появления коллизий (дублирования) значений хеш-функций. Значения хеш-функций используются для подтверждения прав на владение кошельком. Биткойн, например, использует 256-битную длину для идентификации владельца кошелька. Каждый ключ соответствует общему адресу, на который другие могут отправлять средства. До тех пор пока владелец имеет уникальный доступ к ключу, никто не может отправлять транзакции из этого кошелька. В случае коллизии значения хеш-функций право собственности на кошельки и фонды будет трудно доказать, потому что с точки зрения сети обе стороны будут иметь одинаковые права. Такие коллизии крайне редки.

Известны также *атаки по словарю,* как правило, они заключаются в подборе пароля жертвы. Когда пользователь создает пароль для сетевой учетной записи, поставщик услуг не должен хранить пароль в виде простого текста. Вместо этого он должен взять его видоизмененный криптографический хеш пароля и сохранить его значение. Например, если пользователь в качестве пароля возьмет само слово «пароль», сервер может сохранить запись 5baa61e4c9b93f3f068 2250b6cf8331b7ee68fd8, которая является хешем SHA-1 слова «пароль». Хотя в большинстве случаев трудно восстановить исходное слово, зная его хеш, но если злоумышленники увидят хеш-значение «пароль» и хеш-значение «пароль1», то «пароль1» они все-таки смогут преобразовать в исходный текст.

Для прямого взлома это преобразование должно быть повторено миллиарды раз в отношении каждого мыслимого пароля. Единственным ограничением является время, но злоумышленники могут сосредоточиться на общеупотребимых паролях. Коллекция хеш-значений в сочетании с открытым текстом пароля называется *радужной таблицей*. Преобразование криптографического хеша в пароль в виде открытого текста называется *атакой ра-*

дужной таблицы. Модифицированная атака радужной таблицы возможна против блокчейна, в частности биткойнов и связанных криптовалют. В биткойнах адрес представляет открытый интерфейс. Пользователи переводят монеты по этому адресу. Когда они платят кому-то монетами, транзакция происходит с этого адреса. Для того чтобы убедиться, что пользователи уполномочены инициировать транзакцию и тратить монеты с адреса, они должны применять свои закрытые ключи. Такой ключ должен быть известен только владельцу и должен использовать алгоритм цифровой подписи биткойна на основе ключа пользователя. Если пользователи задействуют вместо ключа цифровой подписи из 64 произвольных символов обычные пароли, такие транзакции позволят злоумышленнику перехватить полный контроль над кошельком.

Мошенничество с фишингом — самый известный тип атак на блокчейн-системы благодаря их успешности и массовости применения. Рассмотрим атаку на примере криптовалюты Iota. В результате фишинг-атаки жертвы потеряли 4 млн долл. Эта атака подготавливалась несколько месяцев: злоумышленник зарегистрировал интернет-адрес <iotaseed.Io> и запустил бесплатный сервис генерации надежных seed-фраз (кодовая фраза, при помощи которой пользователь может восстановить доступ к своему кошельку с криптовалютой) для кошелька Iota. Для повышенной безопасности фраза должна была быть сложной в подборе, поэтому такой генератор пользовался успехом. Сервис генерации активно рекламировался, служба стабильно работала, помогала жертвам успешно заводить и использовать свои криптокошельки, создавая ложное чувство безопасности и доверия. В течение длительного времени злоумышленник поддерживал сервис, собирал данные о жертвах и только через шесть месяцев провел атаку. Воспользовавшись ранее украденной информацией, злоумышленник перечислил все средства из кошельков жертв на свои полностью анонимные кошельки.

Cryptojacking. Это метод перехвата управления вычислительными ресурсами в целях выполнения криптографических функций майнинга криптовалют. До 2016 г. одним из основных способов майнинга криптовалюты были его недобросовестные методы. Однако взрывной рост скрытого майнинга пришелся на конец 2017 — начало 2018 г. Новые майнеры появились за счет измене-

ния апробированных вредоносных программ под задачи майнинга. Семейство вредоносного ПО фактически удвоилось за счет включения в него дополнительной функциональности. Так, вирус Black Ruby не только шифровал файлы пользователей и вымогал эквивалент 650 долл. в биткойнах, но и запускал майнинг на зараженном компьютере в пользу своего автора. Вредоносное ПО было модифицировано для осуществления перехвата управления программой XMRig Monero — популярным ПО для майнинга с открытым исходным кодом. Другая крупномасштабная майнинговая бот-сеть, обнаруженная в январе 2018 г., также использовала XMRig.

Атаки троянцами. В некоторых случаях атаки на вычислительные ресурсы являются целевыми, т.е. направленными на конкретные группы пользователей, что делает их более эффективными. Например, один майнер был нацелен на любителей компьютерных игр (геймеров), посещающих определенный российский форум. Его вредоносное ПО маскировалось под модификации популярных игр. В результате установки такой модификации на свои компьютеры геймеры загружали и вредоносные программы, и их компьютерные ресурсы служили для получения прибыли пресловутым майнером.

Чтобы скрыть использование чужих ресурсов и не вызвать подозрений, майнер настроил систему наблюдения за диспетчерами производительности. Если вирус определял, что открывается диспетчер, он останавливал майнинг. Более того, предполагаемый автор этого троянского ПО размещал свои вредоносные программы на нескольких российских форумах, не заботясь о сохранении анонимности.

Атаки на уязвимости реализации. Еще одним видом угроз являются атаки на реализацию самого блокчейна и его вспомогательные инструменты. Следует отметить: чем ближе к технологическому ядру блокчейна и чем глубже уровень реализации, на который направлена атака, тем сложнее добиться ее успеха. Как правило, атаки, в которых используются уязвимости реализации, осуществляются вредоносными программами, аналогичными эксплойтам традиционного ПО и веб-приложений.

Еще одна небезопасная ситуация с блокчейном сложилась в результате плохой подготовки команды разработчиков криптовалюты Verge. Они не сумели справиться с многочисленными уяз-

вимостями в ее реализации и были атакованы. Злоумышленники воспользовались недостатками, чтобы получать новые криптомонеты, не затрачивая ресурсов на их майнинг. Сделанная без должной осмотрительности разработчиков программная «заплатка» (patch) имела побочный эффект, давший возможность злоумышленникам провести «разветвление» монеты, создавая новую монету отдельно от оригинальной монеты. Ущерб, полученный от влияния на стоимость монет, оценили в 1,4 млн долл., а потеря репутации лишь чудом не лишила создателей их бизнеса.

Атаки на владельцев криптокошельков. С ростом стоимости криптовалют классические трояны, атакующие банковские счета, были изменены и нацелены на кошельки криптовалют. Как минимум два появились в 2016 г., когда в банковский троян Dridex добавили функцию кражи криптокошелька. Другой пример — ПО Trickbot, которое предназначалось для атак на финансовые учреждения и криптовалюты. Trickbot добавил в качестве одного из векторов атаки coinbase.com популярный обмен криптовалюты. После заражения системы вредоносное ПО внедряло поддельную страницу входа в систему всякий раз, когда жертва посещала обмен цифровой валюты, что позволяло киберпреступникам украсть данные входа в систему жертвы, а также целый ряд цифровых активов, включая биткойны, Ethereum и Litecoin.

Атаки на смарт-контракты. Особняком стоят атаки на смарт-контракты. По сути, смарт-контракт — это программа, использующая технологию блокчейн. Она может быть написана на любом языке, который понимает виртуальная машина блокчейна. Проблема в том, что уязвимость контракта зависит не от блокчейна, на котором он работает, а от квалификации его разработчиков. В качестве примера можно привести проект TheDAO — один из первых масштабных проектов на Эфириуме, который предлагал пользователям вкладывать валюту эфир в децентрализованную организацию и путем голосования выделять средства перспективным проектам. Средства также можно было возвращать. Взломщик нашел в смарт-контракте уязвимость, которая позволила закольцевать запрос на вывод средств, посылая новый запрос на вывод еще до того, как смарт-контракт успевал обновить баланс. Таким образом похититель вывел из общего фонда треть всего запаса валюты эфир эквивалентного 50 млн долл. Причиной была ошибка разработчика — он забыл включить в код проверку на рекурсию в одной

из частей кода. Эта ошибка привела к крупному финансовому ущербу, пострадало все сообщество сети.

Интернет вещей

Интернетом вещей (Internet of things, IoT) называют концепцию, согласно которой физические устройства подключаются к Интернету и взаимодействуют одно с другим без непосредственного участия человека. Большинство цифровых устройств (колонки, камеры, маршрутизаторы, накопители данных (устройства NAS)) обычно применяют в домашних условиях и в небольших офисах, и это означает, что хакеры могут с относительной легкостью использовать известные недостатки безопасности IoT для достижения своих целей.

Делает эту проблему особенно важной фактически непрерывный процесс написания глобальным сообществом хакеров нового вредоносного ПО, реализующего угрозы безопасности. Это ПО (эксплойты) наносит вред и потребителям и предприятиям, если они не осуществляют базовой проверки безопасности своих устройств IoT на регулярной основе.

Широко распространены сетевые атаки, когда злоумышленники перехватывают управление (компрометируют) сетевых устройств. Атака на «умный дом» или «умное здание» в целях перехвата удаленного управления и дальнейшей вредоносной эксплуатации начинается с компрометации маршрутизатора для того, чтобы сделать домашние устройства доступными через Интернет. Кроме перехвата управления злоумышленники могут отследить любую информацию, проходящую через эти устройства, что создает риск получения личных или конфиденциальных данных. К уязвимостям инфраструктуры и устройств Интернета вещей можно отнести следующие.

Слабые пароли. Эксперты по информационной безопасности установили, что наибольшее количество успешных атак на устройства IoT были рассчитаны на применение пользователями слабых паролей, паролей производителей, предустановленных в том числе на устройства, пароли для которых невозможно изменить, и на устройства которые имеют недекларированные или оставленные в результате ошибок разработчиков «черные ходы». На многих устройствах по умолчанию существует учетная запись

администратора, для которой установлен простой пароль, изначально заданный в программе или устройстве. Предустановленный пароль одинаков для всех устройств и систем этого типа. Владельцем оборудования он зачастую не меняется, а заводская учетная запись не отключается. Если злоумышленник сталкивается с устройством такого типа, ему достаточно просто найти пароль по умолчанию (который свободно доступен в Интернете на сайте производителя оборудования), войти в систему управления устройством и получить неограниченные права доступа.

Использование небезопасных сетевых сервисов. Во многих устройствах IoT, например в «умной» розетке или смарт-часах, предусмотрены сетевые сервисы, которые позволяют устройству обращаться к инфраструктуре IoT, а к ним — из IoT. Некоторые из этих сервисов небезопасны, не редки случаи, когда эти сервисы, в принципе, не нужны для функционирования устройства. Особую опасность представляют сетевые сервисы, которые доступны через Интернет. Такие сервисы ставят под угрозу конфиденциальность, целостность, подлинность и доступность данных на устройстве, а в некоторых случаях допускают перехват и несанкционированное удаленное управление самим устройством. Такой перехват используется для дальнейших атак на приватные сегменты сети IoT. Таким образом, злоумышленники используют уязвимые сетевые службы для атаки на само устройство или компрометируют его как промежуточную точку взлома.

Уязвимый веб-интерфейс. В IoT широко распространен подход, при котором для управления гаджетами и устройствами IoT в них встраивают специальный веб-сервер, на котором размещено веб-приложение. Как и у любого веб-сервера и веб-приложения, в исходном коде могут быть недостатки, которые делают интерфейс уязвимым для кибератак. Такого рода атаки могут исходить и от внешних и от внутренних пользователей сегмента сети IoT. Безопасность веб-интерфейса нарушается при отсутствии блокировки учетных записей, установленных производителем, слабых паролях, отсутствии защиты от подбора учетных данных и при наличии других уязвимостей. Одними из самых уязвимых являются веб-сервисы видеоустройств.

Ненадежный облачный интерфейс. Существенное количество устройств IoT для обмена данными и управляющими командами имеет возможность подключаться к облачным сервисам. Чаще

всего это облачный сервис, реализованный на ресурсах производителя IoT-устройства. Например, практически все «умные» браслеты и «умные» часы обмениваются данными через серверы их производителей на протяжении всего жизненного цикла своей работы. Эти механизмы передачи данных имеют характер массового использования, поскольку для использования не требуется дополнительной оплаты. При недостаточно квалифицированном или безответственном подходе облачный интерфейс управления становится еще одной потенциальной уязвимостью. Атаковать непосредственно устройство сложно, потому что, например, браслеты находятся в домашней сети, за домашним маршрутизатором или межсетевым экраном, удаленному злоумышленнику сложно получить доступ к интерфейсу управления на устройстве, тогда как облачные сервисы доступны всем владельцам устройств данного производителя через Интернет. В связи с этим атакующий выбирает следующие уязвимости для взлома облачного сервиса: недостаточно надежную аутентификацию, отсутствие шифрования при обмене данными и слабую защиту от подбора данных учетных записей. Посредством атаки происходит перехват доступа к данным и элементам управления через облачный вебсайт. Атака чаще всего осуществляется через Интернет. Небезопасные облачные интерфейсы легко обнаружить, проверив соединение с облачным интерфейсом и определив, используется специальный, защищенный посредством криптографии протокол SSL или шифрование не применяется. Запуская механизм восстановления паролей и давая ему на вход списки адресов электронной почты, можно определить, какие пользователи зарегистрированы в атакуемой системе, а впоследствии предпринять атаку подбором паролей.

Небезопасный облачный интерфейс приводит к компрометации пользовательских данных и перехвату управления устройством. В случае, например, браслетов это позволит злоумышленникам увидеть типовые маршруты и время перемещения детей, спрогнозировать отсутствие владельцев в квартире, на даче. Такая информация дает возможность усилить моральное давление на лиц с другой национальностью, верой, политическими взглядами, вести шантаж посредством угроз жизни, в частности детей, и выслеживание, чтобы нанести физический вред.

Ненадежный мобильный интерфейс. Устройства IoT также имеют мобильный интерфейс, в том числе с голосовым управлением. Наличие дополнительного интерфейса является для злоумышленника еще одной возможностью проникнуть в инфраструктуру IoT. Известны несколько векторов атак: слабая аутентификация в мобильном приложении; отсутствие шифрования при обмене данными посредством Wi-Fi, Blootooth, GPRS; подбор данных учетных записей и др. Небезопасные мобильные интерфейсы легко обнаружить при помощи программ-сканеров, позволяющих проверить надежность подключения к беспроводным сетям, установить, используются или нет безопасные механизмы регистрации в сети, например WEP2, или более надежные, определить, используется ли шифрование при обмене данными.

Повышает риски успешной атаки применение открытых небезопасных Wi-Fi-соединений в общественных местах. Возможна также атака посредством подделки доверенной точки доступа, когда злоумышленники выдают свою точку доступа, чтобы перехватить обмен данными, в ручном режиме определить надежность механизма восстановления или сброса пароля. При выявлении слабости злоумышленники определяют используемые учетные записи и, используя специальное ПО, подбирают к ним пароль. Возможные последствия перехвата управления мобильным устройством имеют разнообразные формы: несанкционированное списание денег посредством системы «клиент — банк»; кража конфиденциальной корпоративной информации, представляющей коммерческую тайну; похищение данных для авторизации на корпоративных ресурсах, благодаря которым можно временно вывести из строя ИТ-инфраструктуру организации и государственной службы, уничтожить критические данные пользователей, в том числе без возможности восстановления.

Незащищенные патчи и обновления. Написание ПО — сложный и трудоемкий процесс. В связи с этим практически любое ПО содержит ошибки. При разработке жизненного цикла программного продукта всегда закладывается механизм обновлений — изменений в программе, расширяющих или изменяющих ее функционал и механизм установки заплаток (патчей, patch), что устраняет выявленные недостатки текущего функционала, стабильности работы или безопасности. Если механизма обновлений нет

вообще, это само по себе является слабой стороной безопасности устройства.

Отсутствие шифрования при передаче данных. Если устройство IoT отправляет личные или другие критичные данные по небезопасному сетевому протоколу, они передаются в незашифрованном, незащищенном виде. В результате на любом участке передачи его можно перехватить, прочитать и исказить. В силу того что межкорпоративная стандартизация протоколов обмена в IoT все еще на этапе развития, а государственного регулирования практически нет, уязвимость представляет серьезную угрозу для пользователей IoT.

Отказ от функций безопасности. Одна из глобальных проблем IoT состоит в том, что, даже если разработчики инфраструктуры IoT корректно оценили риски и реализовали функции защиты, пользователи устройств, администраторы инфраструктур IoT не эксплуатируют их должным образом. Поскольку недостатки управления настройками безопасности являются относительно типовыми, это создает еще одно направление для массовых автоматизированных атак.

Недостатки стандартизации и регулирования. Уязвимости технологии порождают проблемы не только для частных лиц. Например, управляющие структуры «умных» городов сталкиваются с теми же угрозами, но в гораздо большем масштабе. Вероятный ущерб для муниципальных, государственных инфраструктур существенно выше, требования к безопасности должны быть более строгими. В условиях высоких рисков для имущества, жизни и здоровья людей, в целом для государственных и муниципальных систем очень востребованными становятся стандарты безопасности. Традиционно стандарты формируются естественным образом, и крупные компании создают альянсы в целях стандартизации. Однако в случае с IoT в силу многообразия устройств, подходов к реализации и производителей в ближайшее время ожидать стандартизации со стороны органов корпоративного регулирования не приходится. В таких случаях роль органа по стандартизации могут брать на себя службы государственного управления.

Небезопасные или устаревшие компоненты. Использование небезопасных или устаревших программных компонентов/библиотек может позволить скомпрометировать устройство. Это небезопасная настройка платформ операционной системы и сторон-

ние программные или аппаратные компоненты из скомпрометированных источников. Свободно распространяемые библиотеки для разработчиков ПО для устройств IoT зачастую содержат «черные ходы». При недостаточной осмотрительности можно интегрировать в свое ПО эти «черные ходы», если не было проявлено должное внимание при выборе источника, из которого разработчик скачивает библиотеки, или при выборе библиотеки, которая не прошла независимого аудита.

Недостаточная защита конфиденциальности. Производители устройств IoT предоставляют свои сервисы по управлению устройствами через облако условно бесплатно, однако при регистрации пользователей на этих сервисах производители собирают сведения о покупателе. Нередко это такая персональная информация пользователя, как имя, фамилия, состояние здоровья, место проживания, данные банковской карты. Устройство впоследствии передает данные геолокации, фотографии и прочую информацию с устройства в облачную экосистему. У пользователя нет гарантий того, что данные никуда не утекут, не будут переданы третьей стороне или проданы. Зачастую сам процесс такой передачи проходит небезопасно, ненадлежащим образом и без разрешения.

Завершая обзорный анализ уязвимостей отдельных информационных технологий, можно также сделать вывод, что в отечественном уголовном законодательстве в части обеспечения информационной безопасности практически не учитывается следующая специфика информационной сферы:

- информация об уязвимостях таких систем и программного обеспечения, которые дают возможность совершения преступления, распространяется свободно, в том числе самими их авторами;
- уязвимости создаются и выявляются непрерывно, запросы к требованиям по обеспечению безопасности, в том числе к юридическим мерам обеспечения, возникают постоянно, что требует перманентной актуализации законодательства;
- средства реализации преступления (специализированное программного обеспечение) может создавать человек в любой точке мира, имеющий определенные навыки;
- не существует средств, которые заведомо предназначены для совершения преступного деяния, практически любое

средство атаки может использоваться лишь как инструмент контроля защищенности;

- подключение к сетям общего пользования расширяет географию вовлеченных в преступную деятельность, а возможность удаленных атак повышает сложность установления субъекта, осуществляющего преступные деяния;
- распределение сфер ответственности осуществляется лишь в рамках одной информационной системы, не существует общего подхода к распределению ответственности за создание условий для преступления.

1.2. Правовой режим информационных технологий в Российской Федерации в условиях цифровой трансформации

Т.А. Полякова[1], *А.А. Смирнов*[2], *А.И. Химченко*[3]

Происходящие в современном обществе процессы цифровой трансформации, повсеместного внедрения новых технологий создали беспрецедентные предпосылки и условия их многофункционального применения во всех сферах социально-экономических отношений.

Информационные технологии стали неотъемлемой частью всех сфер деятельности личности, общества и государства, и их эффективное применение призвано стать фактором ускорения экономического развития государства и совершенствования функционирования общественных и государственных институтов. В то же время развитие технологий приводит к появлению

[1] Татьяна Анатольевна Полякова — главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, профессор, заслуженный юрист Российской Федерации.

[2] Александр Александрович Смирнов — ведущий научный сотрудник 3-го отдела НИЦ № 4 ВНИИ МВД России, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, доцент.

[3] Алексей Игоревич Химченко — старший преподаватель кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА), кандидат юридических наук.

новых видов нематериальных и трансформации традиционных материальных активов, формированию взаимосвязей между объектами виртуального и реального мира.

Сегодня информационные и коммуникационные технологии стали частью современных управленческих систем во всех отраслях экономики, сферах государственного управления, обороны страны, безопасности государства и обеспечения правопорядка.

Динамика и беспрецедентная глубина происходящих преобразований предопределяют необходимость научных исследований характера угроз собственности, жизни и здоровью человека, функционированию государственных и общественных институтов. Уголовно-правовые риски технологичной среды в настоящее время сосредоточены главным образом на компьютерных преступлениях и защите информации, что обусловлено существующей структурой уголовного законодательства, обособившего преступления в сфере компьютерной информации и включающего соответствующие квалифицирующие признаки в отдельные составы преступлений. При этом по мере цифровой трансформации и развития информационных технологий спектр их применения в преступных целях стал расширяться, пополнившись новыми подходами и методами.

Процессы цифровой трансформации и интенсивность развития инновационной активности зависят от сбалансированного использования как технологического потенциала, так и регуляторной среды. Общественные отношения, трансформируясь в соответствии с потребностями членов общества, инициируют неизбежные преобразования в теоретических и практических подходах в соответствующей законодательной деятельности. Динамика происходящих технологических изменений предопределяет вопрос развития правового регулирования, который в силу самой природы правотворчества и сложившейся практики нормотворческой деятельности не всегда может быть решен также стремительно либо хотя бы своевременно. Как справедливо отмечает А.В. Минбалеев, «в условиях развития цифровых технологий современная правовая система не способна быстро реагировать на изменение цифровых технологий, поскольку они совершенствуются значительно быстрее»[1].

[1] *Минбалеев А.В.* Трансформация регулирования цифровых отношений // Вестн. Ун-та им. О.Е. Кутафина (МГЮА). 2019. № 19. С. 32.

В связи с этим научное исследование правового режима ключевых информационных технологий представляется весьма актуальным и имеет существенное значение для развития всей правовой системы в современных условиях.

Прежде всего, следует обратить внимание на роль, отводимую вопросам создания и применения информационных и коммуникационных технологий в Стратегии развития информационного общества в Российской Федерации на 2017—2030 гг.[1] В данном документе выделены следующие приоритетные направления развития информационно-коммуникационных технологий:

- конвергенция сетей связи и создание сетей связи нового поколения;
- обработка больших объемов данных;
- искусственный интеллект;
- доверенные технологии электронной идентификации и аутентификации, в том числе в кредитно-финансовой сфере;
- облачные и туманные вычисления;
- Интернет вещей и индустриальный Интернет;
- робототехника и биотехнологии;
- радиотехника и электронная компонентная база;
- информационная безопасность.

В целях реализации указов Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21.07.2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в том числе для решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством РФ сформирована национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7[2].

---

[1] Утверждена Указом Президента Российской Федерации от 9 мая 2017 г. № 203. См.: *СЗ* РФ. 2017. № 20. Ст. 2901.

[2] См.: *Цифровая* экономика РФ // Минцифры России. https://digital.gov.ru/ru/activity/directions/858/?utm_referrer=https%3a%2f%2fyandex.ru%2f#section-description (дата обращения: 22.03.2023).

В состав национальной программы «Цифровая экономика Российской Федерации» входят следующие федеральные проекты:

- «Нормативное регулирование цифровой среды»
- «Кадры для цифровой экономики»
- «Информационная инфраструктура»
- «Информационная безопасность»
- «Цифровые технологии»
- «Цифровое государственное управление»
- «Искусственный интеллект»
- «Обеспечение доступа в Интернет за счет развития спутниковой связи»
- «Развитие кадрового потенциала ИТ-отрасли».

Изучение содержания Национальной программы показывает, что предусмотренная ею государственная политика в сфере развития информационных технологий строится на основе сочетания мер по созданию благоприятного правового поля для реализации в российской юрисдикции проектов цифровизации, с одной стороны, и построения эффективной системы защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности — с другой.

Исследование показывает, что в настоящее время в Российской Федерации законодательное регулирование информационных технологий носит фрагментарный характер, а вопросы их развития отражены преимущественно в концептуальных либо документах стратегического планирования.

Ключевое значение в рассматриваемой сфере имеет Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1]. Данный Закон определяет информационные технологии как «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» (ст. 2).

Законодательством в сфере информационных технологий установлены принципы правового регулирования в данной сфере, среди которых свобода поиска, получения, передачи, производства и распространения информации, ее достоверности, неприкос-

[1] См.: *СЗ* РФ. 2006. № 31. Ст. 3448.

новенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия[1].

При этом в отдельных случаях предусматривается ограничение доступа к информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Государственное регулирование в сфере применения информационных технологий предусматривает:

- регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий;
- развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;
- создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети Интернет и иных подобных информационно-телекоммуникационных сетей;
- обеспечение информационной безопасности детей[2].

Исходя из законодательного определения информационных технологий, а также подхода к их государственному регулированию, основной фокус в рамках настоящего исследования целесообразно сосредоточить на анализе ключевых элементов, образующих информационные технологии.

Вместе с тем среди требующих своего научного осмысления стоит отметить вопросы формирующейся в ходе процесса цифровой трансформации самой материи цифровой среды, правовой природы возникающих в ней правоотношений, а также применения современных норм права к составляющим ее цифровым технологиям.

---

[1] Статья 3 Федерального закона «Об информации, информационных технологиях и о защите информации».

[2] Статья 12 Федерального закона «Об информации, информационных технологиях и о защите информации».

В нормах действующего законодательства на текущий момент нет какого-либо легального определения цифровых технологий, при этом в отраслевых нормативных актах систематизируется подход к их развитию.

Преимущественный фокус внимания на цифровые технологии сосредоточен в Паспорте национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7), в соответствии с п. 4,5 которого определены задачи федерального проекта «Цифровые технологии»:

- создание «сквозных» цифровых технологий (реализация дорожных карт развития «сквозных» цифровых технологий, создание цифровых платформ исследований и разработок, создание и реализация программ и проектов по цифровой трансформации);
- создание комплексной системы финансирования проектов по разработке и (или) внедрению цифровых технологий и платформенных решений.

Направления разработки и развития перспективных «сквозных» цифровых технологий детализированы в Положении о проведении конкурсного отбора на предоставление государственной поддержки программ деятельности лидирующих исследовательских центров, реализуемых российскими организациями в целях обеспечения разработки и реализации дорожных карт развития перспективных «сквозных» цифровых технологий (утв. постановлением Правительства РФ от 3 мая 2019 г. № 551[1]):

- искусственный интеллект;
- системы распределенного реестра;
- квантовые технологии;
- новые производственные технологии;
- компоненты робототехники и сенсорика;
- технологии беспроводной связи;
- технологии виртуальной и дополненной реальностей.

Указанный перечень цифровых технологий применяется и в методике расчета показателей федерального проекта «Цифро-

[1] См.: *СЗ* РФ. 2019. № 19. Ст. 2307.

вые технологии» национальной программы «Цифровая экономика Российской Федерации» (утв. приказом Минкомсвязи России от 23.04.2020 № 195).

Кроме того, в положениях Указа Президента РФ от 30 сентября 2022 г. № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации»[1] отдельно выделяется категория «цифровые технологии идентификации и аутентификации», что расширяет перечень исследуемых технологий.

В конце вводной части следует отметить, что современных условиях, помимо традиционного правового регулирования, для нормативного воздействия на информационные отношения также широко задействуются методы технического регулирования и саморегулирования[2].

На сегодняшний день выделяются ключевые направления соприкосновения институтов саморегулирования и цифровых технологий, такие как внедрение технологий в работу уже существующих механизмов саморегулирования, а также стимулирование развития саморегулирования посредством инструментов цифровизации[3]. Так, отдельные установленные Федеральным законом от 1 декабря 2007 г. № 315-ФЗ «О саморегулируемых организациях»[4] функции саморегулируемых организаций могут быть реализованы посредством тех или иных цифровых технологий, в частности создание и ведение сайта в информационно-телекоммуникационной сети Интернет, ведение реестра членов саморегулируемых организаций, реализация мер дисциплинарного воздействия, осуществление взаимодействия и др.

Среди сфер с функционирующими механизмами саморегулируемых организаций, где интенсификация цифровизации может

---

[1] См.: *СЗ* РФ. 2022. № 40. Ст. 6791.

[2] См.: *Механизмы* и модели регулирования цифровых технологий: Монография / Под общ. ред. А.В. Минбалеева. М.: Проспект, 2023; *Правовое* регулирование цифровых технологий в России и за рубежом: Роль и место правового регулирования и саморегулирования в развитии цифровых технологий: Монография / Под общ. ред. А.В. Минбалеева. Саратов: Амирит, 2019.

[3] См.: *Правово*е регулирование цифровых технологий в России и за рубежом. Роль и место правового регулирования и саморегулирования в развитии цифровых технологий. С. 70—74.

[4] См.: *СЗ* РФ. 2007. № 49. Ст. 6076.

принести наибольший эффект, выделяются строительная, аудиторская и оценочная деятельности, поскольку на основе отдельных цифровых технологий могут быть реализованы процессы обработки жалоб, аудит и контроля соблюдения стандартов и правил.

Перспективным также является саморегулирование в отдельных сферах предпринимательской деятельности на основе использования цифровых технологий в случаях отраслевых объединений профессиональных участников, деятельность которых непосредственно связана с технологиями.

В настоящий момент отсутствуют специализированные саморегулируемые организации в этой области, но уже существует ряд ассоциаций, объединяющих участников отдельных сфер цифрового рынка и имеющих достаточно высокий потенциал для приобретения статуса саморегулируемых организаций[1]. В то же время расширение механизмов саморегулирования применительно к цифровой среде формулирует определенные правовые вопросы, ключевым среди которых является отсутствие полноценного законодательства о цифровых технологиях.

Информационно-телекоммуникационная сеть Интернет

Информационно-телекоммуникационная сеть Интернет продолжает играть технологически ключевую роль в современной архитектуре организации оборота информации. Понятие «информационно-телекоммуникационная сеть» определено в Федеральном законе «Об информации, информационных технологиях и о защите информации» как «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» (ст. 2). Поскольку сеть Интернет является разновидностью сети связи, на нее распространяется действие Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[2] и основанных на нем подзаконных нормативных правовых актов.

---

[1] См.: *Минбалеев А.В.* Проблемы правового регулирования использования цифровых технологий в деятельности саморегулируемых организаций // Гражданское право. 2020. № 4. С. 31—34.

[2] См.: *СЗ* РФ. 2003. № 28. Ст. 2895.

Также в Федеральном законе «Об информации, информационных технологиях и о защите информации» содержится дефиниция сайта в сети Интернет: «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»»[1].

В зависимости от функционального предназначения законодателем были выделены основные субъекты правоотношений, связанных с использованием сети Интернет (организатор распространения информации в сети Интернет, социальная сеть, аудиовизуальный сервис, новостной агрегатор), и регламентирован их правовой статус.

Организатором распространения информации в сети Интернет является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет[2].

На организатора распространения информации в сети Интернет при осуществлении его деятельности возложена обязанность уведомить Роскомнадзор о начале осуществления деятельности, а также хранить на территории Российской Федерации и предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, следующую информацию:

- информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года;
- текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео, иные электронные сообщения пользователей до шести месяцев.

[1] Статья 2 Федерального закона «Об информации, информационных технологиях и о защите информации».

[2] Статья 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации».

Кроме того, установлена обязанность реализации установленных указанными органами требований к оборудованию и программно-техническим средствам, а также представления информации, необходимой для декодирования электронных сообщений в случае использования для приема, передачи, доставки и (или) обработки электронных сообщений дополнительного кодирования электронных сообщений либо при предоставлении такой возможности пользователям.

На организатора распространения информации при осуществлении деятельности по обеспечению функционирования информационных систем для обмена электронными сообщениями между пользователями также возложены следующие обязанности:

- осуществлять идентификацию пользователей сети Интернет;
- в течение суток с момента получения требования уполномоченного органа ограничить возможность осуществления пользователем передачи электронных сообщений;
- обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей;
- обеспечивать конфиденциальность передаваемых электронных сообщений;
- обеспечивать возможность передачи электронных сообщений по инициативе государственных органов;
- не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями в определенных Правительством РФ случаях.

Важно отметить, что сведения об идентификации абонентского номера пользователей подлежат хранению только на территории Российской Федерации, предоставление третьим лицам идентификационных сведений об абонентском номере может осуществляться только с согласия пользователя сервиса обмена мгновенными сообщениями, за исключением установленных случаев.

Следует признать, что одним из наиболее востребованных пользователями типов интернет-ресурсов являются *социальные сети*. Законодательно закреплено, что социальной сетью признаются сайт и (или) страница сайта в сети Интернет, и (или) информационной системы, и (или) программы для электронных вычис-

лительных машин, которые предназначены и (или) используются их пользователями для предоставления и (или) распространения посредством созданных ими персональных страниц информации на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более 500 тыс. пользователей сети Интернет, находящихся на территории Российской Федерации[1].

Социальные сети собирают и анализируют информацию об активности своих пользователей, их взглядах и убеждениях, других персонифицированных характеристиках, что порождает комплекс рисков, включая:

- преследование за указанные взгляды;
- накопление и анализ данных для прогнозирования потребительской активности пользователей;
- попытки войти в доверие (в том числе несовершеннолетним), а также выявление и отбор потенциальных жертв для совершения противоправных действий;
- фиксацию местоположения и активности владельцев для совершения противоправных действий против их имущества;
- использование социального капитала для совершения противоправных действий (формирование необходимого общественного мнения, неблагоприятного образа, клеветы и др.);
- использование социальных сетей для осуществления недобросовестной конкуренции и другие действия.

В целях минимизации рисков использования социальных сетей в противоправных целях для их владельцев законодательством установлены комплекс правовых запретов и обязанностей, включая следующие[2]:

- не допускать использование социальной сети в целях совершения уголовно наказуемых деяний, разглашения сведений,

[1] Статья 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации».
[2] Статья 10.6 Федерального закона «Об информации, информационных технологиях и о защите информации».

составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань;

- не допускать распространение информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями;
- соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;
- соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций;
- разместить в социальной сети адрес электронной почты для направления ему юридически значимых сообщений, свои фамилию и инициалы (для физического лица) или наименование (для юридического лица), а также электронную форму для направления обращений о распространяемой с нарушением закона информации;
- установить программу, предназначенную для определения количества пользователей информационным ресурсом;
- уведомлять пользователя социальной сети о принятых мерах по ограничению доступа к его информации в соответствии, а также об основаниях такого ограничения и др.

Кроме того, на владельца социальной сети возложена обязанность осуществлять мониторинг социальной сети в целях выявления:

- материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
- информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных ве-

ществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

- информации о способах совершения самоубийства, а также призывов к совершению самоубийства;
- информации, нарушающей требования о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи;
- информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;
- информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;
- информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации;
- информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов

энергетики, промышленности или связи, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации, сведений, позволяющих получить доступ к указанным информации или материалам;

- информации, пропагандирующей нетрадиционные сексуальные отношения и (или) предпочтения, педофилию, смену пола.

В случае выявления указанной информации при осуществлении мониторинга социальной сети или по результатам рассмотрения обращения владелец социальной сети обязан незамедлительно принять меры по ограничению доступа к ней.

На Роскомнадзор возложено ведение реестра социальных сетей. В целях обеспечения формирования реестра осуществляется мониторинг информационных ресурсов, в процессе которого данному органу предоставлено право запрашивать у владельца социальной сети и иных лиц информацию, необходимую для ведения такого реестра.

При соответствии критериям мониторинга владельцу социальной сети направляется уведомление о включении его в реестр социальных сетей с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

Кроме того, Федеральным законом «Об информации, информационных технологиях и о защите информации» регламентируется деятельность *поисковых систем, новостных агрегаторов, аудиовизуальных сервисов, сервисов обмена мгновенными сообщениями и иных цифровых платформ*. В интересах обеспечения безопасности на владельцев данных интернет-сервисов возложены следующие обязанности:

- не допускать использования сервиса в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также ма-

териалов, пропагандирующих порнографию, насилие и жестокость, и материалов, содержащих нецензурную брань;
- проверять достоверность распространяемых общественно значимых сведений до их распространения и незамедлительно прекратить их распространение в установленных случаях;
- не допускать использования сервиса в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения информации с нарушением законодательства Российской Федерации;
- не допускать распространения информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями;
- не допускать распространения новостной информации о частной жизни гражданина с нарушением гражданского законодательства;
- соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и выборах, о массовой информации;
- соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций и др.

Критическая информационная инфраструктура

Рассматривая правовой режим информационных технологий, необходимо отметить особое значение для национальной экономики и безопасности страны критической информационной инфраструктуры. Вопросам обеспечения ее надлежащего функционирования и защиты уделяется существенное внимание в документах стратегического планирования, определяющих цели и задачи в области национальной безопасности.

Так, обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь

критической информационной инфраструктуры Российской Федерации, Доктриной информационной безопасности[1] отнесено к национальным интересам в информационной сфере, а развитие информационной и коммуникационной инфраструктуры Российской Федерации в соответствии со Стратегией развития информационного общества в Российской Федерации признается одним из приоритетов при обеспечении национальных интересов при развитии информационного общества.

Вместе с тем в Доктрине информационной безопасности отмечаются постоянное повышение сложности, увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры[2].

В рамках данного исследования особенно важно отметить, что неправомерное воздействие на критическую инфраструктуру является уголовным преступлением. В случае если такое воздействие приводит к длительной приостановке или нарушению работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц и т.п. признаются квалифицирующим признаком тяжких последствий согласно разъяснению Пленума Верховного Суда РФ[3].

Отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак регулируются Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[4], положениями которого закрепляются принципы обеспечения безопасности критической информационной инфраструктуры, та-

---

[1] Утверждена Указом Президента РФ от 05.12.2016 № 646. См.: *СЗ* РФ. 2016. № 50. Ст. 7074.

[2] См.: ст. 16 Доктрины информационной безопасности Российской Федерации.

[3] См.: *Постановление* Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» // Российская газета. 2022. 28 декабря.

[4] См.: *СЗ* РФ. 2017. № 31. Ст. 4736.

кие как законность, непрерывность и комплексность обеспечения безопасности, приоритет предотвращения компьютерных атак.

В соответствии с нормами данного Закона создана и функционирует государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА). Координацию деятельности субъектов критической информационной инфраструктуры РФ по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты обеспечивает Национальный координационный центр по компьютерным инцидентам.

Категории значимости соответствующего объекта критической информационной инфраструктуры устанавливаются исходя из его социальной, политической, экономической, экологической значимости, а также значимости объекта для обеспечения обороны страны, безопасности государства и правопорядка. ФСТЭК России ведет реестр значимых объектов критической информационной инфраструктуры.

Следует иметь в виду, что на субъектов критической информационной инфраструктуры возложены следующие *обязанности*:

- незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации в установленном порядке;
- оказывать содействие должностным лицам указанного федерального органа в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;
- в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Кроме того, предусмотрены иные обязанности для субъектов критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, среди которых: соблюдать требования по обеспечению безопасности; выполнять предписания должностных лиц; реагировать на компьютерные инциденты; обеспечивать беспрепятственный доступ должностным лицам ФСТЭК России.

Персональные данные

Трудно переоценить значение правового обеспечения защиты персональных данных в условиях современной цифровой среды. В рамках настоящего исследования следует обратить особое внимание, что в Доктрине информационной безопасности отмечено увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий[1].

На обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, направлены нормы Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[2], которым регламентированы правила обработки персональных данных.

Нормами Закона установлено, что обработка персональных данных должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных, заранее определенных и законных целей, не допускать обработки, избыточной и несовместимой с целями сбора персональных данных.

Важно отметить, что не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой, устанавливается необходимость обеспечить точность и достаточность персональных данных, актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые

[1] Пункт 14 Доктрины информационной безопасности Российской Федерации.
[2] См.: *СЗ* РФ. 2006. № 31. Ст. 3451.

меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Федеральным законом «О персональных данных» установлена необходимость хранения персональных данных в форме, позволяющей определить субъекта персональных данных, и не дольше, чем этого требуют цели обработки персональных данных с последующим уничтожением либо обезличиванием по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

В отношении операторов и иных лиц, получивших доступ к персональным данным, предусмотрена обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Кроме того, субъекту персональных данных предоставлено право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

При этом в настоящем исследовании целесообразно акцентировать внимание на том, что право субъекта персональных данных на доступ к его персональным данным может быть ограничено, если:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
- обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации слу-

чаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;
- обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства[1].

В целях защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных на оператора возложена обязанность принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие.

Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных;
- применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий

[1] Часть 8 ст. 14 Федерального закона «О персональных данных».

компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных[1].

Оператор обязан в установленном порядке обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

Цифровые финансовые активы

Формирование новой технологической основы для развития экономики в соответствии со Стратегией развития информационного общества в Российской Федерации признано одним из приоритетов при обеспечении национальных интересов России.

По мере расширения технологических возможностей существенным образом менялся и весь спектр общественных отношений, в частности в современных экономических отношениях формируются новые модели и подходы, все более широкое применение находят цифровые финансовые активы.

Этап активного использования в гражданском обороте цифровых активов поставил перед цивилистами задачу их надлежащей правовой защиты, в то же время в силу своих технологических особенностей они стали активно использоваться вне правового

[1] Статья 19 Федерального закона «О персональных данных».

поля, в связи с чем и перед правом, в том числе его уголовно-правовой сферой, были поставлены новые задачи.

Отношения, возникающие при выпуске, учете и обращении цифровых финансовых активов, особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператора обмена цифровых финансовых активов, а также общественные отношения при обороте цифровой валюты в Российской Федерации регулируются нормами Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1].

В соответствии с указанным Законом *цифровыми финансовыми активами* признаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы»[2]. *Цифровая валюта* определена как «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении

[1] См.: *СЗ* РФ. 2020. № 31. Ст. 5018.

[2] Статья 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

действий по внесению (изменению) записей в такую информационную систему ее правилам» [1].

Цифровые финансовые активы и цифровая валюта подлежат учету, осуществляемому операторами информационной системы и операторами обмена. Так, оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, обязан обеспечить:

1) возможность восстановления доступа обладателя цифровых финансовых активов к записям информационной системы по требованию обладателя цифровых финансовых активов;

2) бесперебойность и непрерывность функционирования информационной системы;

3) целостность и достоверность информации о цифровых финансовых активах, содержащейся в записях информационной системы;

4) корректность реализации в информационной системе установленного оператором информационной системы алгоритма (алгоритмов) создания, хранения и обновления информации, содержащейся в распределенном реестре, и алгоритма (алгоритмов), обеспечивающего тождественность указанной информации во всех базах данных, составляющих распределенный реестр, а также невозможность внесения изменений в установленный оператором информационной системы алгоритм (алгоритмы) иными лицами — для информационных систем на основе распределенного реестра;

5) невозможность внести и (или) изменить запись о цифровых финансовых активах пользователем информационной системы.

На оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, возложена обязанность предоставлять содержащуюся в записях информационной системы информацию о цифровых финансовых активах, принадлежащих их обладателю:

- по требованию суда;
- по требованиям федерального органа исполнительной власти, принимающего меры по противодействию легализации

[1] Статья 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

(отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, Банка России, органов принудительного исполнения Российской Федерации, налоговых органов, других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности, а также на основании судебного решения в случаях, если такая информация необходима для осуществления ими своих функций, предусмотренных законодательством Российской Федерации;

- при наличии согласия руководителя следственного органа — по требованию органов предварительного следствия по делам, находящимся в их производстве;
- на основании судебного решения — по требованию должностных лица органов, уполномоченных осуществлять оперативно-розыскную деятельность, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела;
- по запросам, направляемым уполномоченными лицами в соответствии с законодательством Российской Федерации о противодействии коррупции;
- по требованию конкурсного управляющего в ходе конкурсного производства в отношении обладателя цифровых финансовых активов;
- по требованию регистратора (депозитария), в котором открыт лицевой счет (счет депо) цифровых финансовых активов[1].

Также оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, обязан обеспечить хранение информации о сделках с цифровыми финансовыми активами, выпущенными в информационной системе, оператором которой он является, а также об участниках таких сделок не менее пяти лет с даты совершения соответствующих сделок.

[1] Часть 3 ст. 1 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»

Цифровая медицина

Одной из сфер, где развитие информационных технологий имеет высокий потенциал влияния на качество жизни граждан и повышенную социальную значимость, является развитие цифровой медицины за счет развития технологий дистанционной диагностики, предсказательной аналитики, возможностей носимых устройств, телемедицины и вариативности выбора услуг на ее основе.

Под телемедицинскими услугами исследователями предложено понимать «медицинскую деятельность, осуществляемую медицинскими организациями при взаимодействии с другими субъектами информационной сферы, связанную с использованием информационно-коммуникационных технологий и направленную на повышение качества медицинской помощи, дистанционное оказание медицинских услуг, активизацию процессов изучения разработок в медицинской сфере, а также обеспечение охраны здоровья граждан, устойчивого информационного обмена медицинскими данными в удаленном режиме в условиях доверенной среды»[1].

Изменения технологий и способов оказания услуг открывают и новые возможности для совершения широкого спектра преступлений — от мошенничества и вымогательства у пациентов до подделки данных для страховых выплат и компенсаций. В условиях цифровой трансформации особенную актуальность приобретает вопрос об ответственности архитекторов и разработчиков медицинских информационных систем, лиц, осуществляющих их поддержку и эксплуатацию, и др.

Применение информационных технологий в медицинской деятельности способствует накоплению такого массива чувствительной информации, доступ к которому создает потенциальные риски со стороны всех субъектов процесса, в том числе медицинского персонала, подрядных и обслуживающих организаций, пациентов и потенциальных злоумышленников.

---

[1] *Буланова В.С.* Информационно-правовое обеспечение оказания телемедицинских услуг в условиях цифровой трансформации: Дис. … канд. юрид. наук. М., 2021. С. 9—10.

Искусственный интеллект

Традиционно наиболее существенные изменения происходили в периоды технологических преобразований, качественно менявших принципы общественного взаимодействия и производные экономические процессы. Активность цифровизации множества сфер деятельности и скорость изменения общественных отношений возрастают, механизмы информационных технологий становятся все сложнее, и мы становимся свидетелями того, как решения на основе ИИ превращаются из модного тренда в рабочий механизм, выполняющий многие производственные задачи, заменяя подчас все больший объем рутинной деятельности.

Ключевым вопросом в регулировании указанных технологий является выработка научно обоснованного подхода к определению правового статуса ИИ. Вместе с тем множественный состав участников этого процесса (разработчики, провайдеры, поставщики данных, эксплуатанты) осложняет вопрос распределения ответственности между задействованными субъектами, поиск решения которого при этом требует балансирования интересов всех участников. Указанные вопросы[1] все чаще становятся предметом внимания научного сообщества.

Однако следует обратить внимание также на то, что в настоящее время в Российской Федерации отсутствует специальное законодательное регулирование, учитывающее специфику применения технологий ИИ и робототехники и создаются лишь предпосылки для формирования основ правового регулирования новых общественных отношений, складывающихся в связи с разработкой и применением технологий ИИ и робототехники и систем на их основе.

Согласно Указу Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федера-

[1] См.: *Модели* правового регулирования создания, использования и распространения роботов и систем с искусственным интеллектом: Монография / Под общ. ред. к.ю.н. В.Б. Наумова. СПб.: ПН-Принт, 2019; *Батурин Ю.М., Полубинская С.В.* Искусственный интеллект: правовой статус или правовой режим? // Государство и право. 2022. № 10. С. 141—154; *Полякова Т.А., Камалова Г.Г.* Проблемы формирования правовой политики в сфере применения технологии искусственного интеллекта // Правовая политика и правовая жизнь. 2023. № 1. С. 28—37.

ции»[1], определены базовые термины и принципы использования технологий ИИ. Искусственный интеллект определен в данном Указе как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека»[2]. При этом отмечено, что указанный комплекс включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений[3].

Установлено, что использование технологий ИИ в отраслях экономики носит общий («сквозной») характер и способствует созданию условий для улучшения эффективности и формирования принципиально новых направлений деятельности хозяйствующих субъектов, в том числе за счет:

- повышения эффективности процессов планирования, прогнозирования и принятия управленческих решений (включая прогнозирование отказов оборудования и его превентивное техническое обслуживание, оптимизацию планирования поставок, производственных процессов и принятия финансовых решений);
- автоматизации рутинных (повторяющихся) производственных операций;
- использования автономного интеллектуального оборудования и робототехнических комплексов, интеллектуальных систем управления логистикой;
- повышения безопасности сотрудников при выполнении бизнес-процессов (включая прогнозирование рисков и неблагоприятных событий, снижение уровня непосредственного участия человека в процессах, связанных с повышенным риском для его жизни и здоровья);
- повышения лояльности и удовлетворенности потребителей (в том числе направление им персонализированных пред-

[1] См.: *СЗ* РФ. 2019. № 41. Ст. 5700.
[2] Пункт 5 Указа Президента РФ «О развитии искусственного интеллекта в Российской Федерации».
[3] Там же.

ложений и рекомендаций, содержащих существенную информацию);

- оптимизации процессов подбора и обучения кадров, составления оптимального графика работы сотрудников с учетом различных факторов[1].

Согласно положениям Указа Президента РФ «О развитии искусственного интеллекта в Российской Федерации», к 2024 г. должны быть созданы необходимые правовые условия для достижения целей, решения задач и реализации мер, предусмотренных Национальной стратегией развития искусственного интеллекта на период до 2030 г.[2], а к 2030 г. в Российской Федерации должна функционировать гибкая система нормативно-правового регулирования в области ИИ, в том числе гарантирующая безопасность населения и направленная на стимулирование развития технологий ИИ.

В Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г.[3] среди приоритетных целей предусмотрено стимулирование разработки, внедрения и использования таких технологий, создания систем ИИ и робототехники в доверенном и безопасном исполнении, которое будет способствовать достижению высоких темпов экономического роста, повышению благосостояния и качества жизни граждан. Кроме того, выделены вопросы регулирования оборота данных, ответственности и информационной безопасности, определены сферы применения.

Следует отметить и разработанный в 2021 г. Кодекс этики искусственного интеллекта, в котором, несмотря на рекомендательный характер, обозначены ключевые принципы, такие как ответственность, конфиденциальность, безопасность.

В целях соблюдения баланса между внедрением новых технологий и соблюдением прав граждан и интересов государства, поиска качественных правовых решений внедрения технологий, стимулирования инновационной деятельности предусмот-

---

[1] Пункт 21 Указа Президента РФ «О развитии искусственного интеллекта в Российской Федерации».

[2] Утверждена Указом Президента РФ от 10 октября 2019 г. № 490. См.: *СЗ* РФ. 2019. № 41. Ст. 5700.

[3] Утверждена распоряжением Правительства РФ от 19 августа 2020 г. № 2129-р. См.: *СЗ* РФ. 2020. № 35. Ст. 5593.

рено создание экспериментальных правовых условий применения отдельных новых инструментов (экспериментальные правовые режимы).

При этом ключевым законодательным в рассматриваемой сфере является Федеральный закон от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»[1] (далее — Закон), в соответствии с положениями которого с 1 июля 2020 г. в субъекте Российской Федерации — городе федерального значения Москве сроком на пять лет устанавливается эксперимент по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий ИИ, а также последующего возможного использования результатов применения ИИ.

В общих положениях Закона устанавливается невозможность ограничения конституционных прав и свобод граждан, введение для них дополнительных обязанностей, нарушение единства экономического пространства на территории Российской Федерации или иное умаление гарантий защиты прав граждан и юридических лиц, предусмотренных Конституцией РФ, федеральными конституционными законами, федеральными законами, указами Президента РФ, постановлениями Правительства РФ и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации по результатом установления экспериментального правового режима.

Однако, согласно Закону, обработка персональных данных в обезличенном виде может осуществляться без согласия субъекта персональных данных для целей проведения эксперимента в городе федерального значения Москве, а также для повышения эффективности государственного и муниципального управления.

Несмотря на то что, согласно ч. 1 ст. 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются, возникает

[1] См.: *СЗ* РФ. 2020. № 17. Ст. 2701.

ситуация, при которой фактически для жителей экспериментального субъекта Российской Федерации участие в эксперименте становится неизбежным.

В соответствии с Законом экспериментальным правовым режимом признается применение в течение предусмотренного срока проведения эксперимента в отношении участников экспериментального правового режима специального регулирования в целях создания необходимых условий для разработки и внедрения технологий ИИ в субъекте Российской Федерации — городе федерального значения Москве, а также последующего возможного использования результатов применения ИИ.

Указанным Законом закреплены понятийный аппарат в области ИИ, режимы общего и специального регулирования, участника экспериментального правового режима.

Целями установления экспериментального правового режима являются:

1) обеспечение повышения качества жизни населения;

2) повышение эффективности государственного или муниципального управления;

3) повышение эффективности деятельности хозяйствующих субъектов в ходе внедрения технологий ИИ;

4) формирование комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий ИИ, по результатам установления экспериментального правового режима[1].

К *задачам* установления экспериментального правового режима отнесены:

1) создание благоприятных правовых условий развития технологий ИИ;

2) апробация технологий ИИ и результатов его применения в субъекте Российской Федерации — городе федерального значения Москве;

[1] Статья 3 Федерального закона «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»».

3) оценка эффективности и результативности установления специального регулирования по результатам установления экспериментального правового режима[1].

Основными *принципами* установления экспериментального правового режима признаются:

1) прозрачность экспериментального правового режима;

2) защита прав и свобод человека и гражданина, обеспечение безопасности личности, общества и государства;

3) недискриминационный доступ к результатам применения ИИ[2].

Логика выделения тематики ИИ в отдельный предмет регулирования явно указывает на перспективу интеграции решений на основе ИИ во многие будущие технологические проекты.

В связи с этим проведение эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий ИИ является логичным и практическим шагом.

В целом в российском научном сообществе модель экспериментальных правовых режимов признается крайне востребованной для всех аспектов технологий ИИ[3].

При этом в попытках стимулирования инновационной деятельности при реализации так называемых «песочниц» перед всеми участниками процесса могут возникнуть в том числе и различные препятствия, к которым можно отнести и риски их реализации, связанные как с качеством осуществления регуляторных функций, так и вероятным причинением вреда потребителям и участникам правоотношений, злоупотреблением положением и нарушением конкуренции, совершения противоправных действий.

Поскольку одной из главных целей установления экспериментального правового режима является обеспечение повыше-

---

[1] Статья 3 Федерального закона «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных»».

[2] Там же.

[3] См.: *Незнамов А.В.* Правовые аспекты внедрения технологий искусственного интеллекта в финансовой сфере // Основные тренды развития цифровой экономики в финансовой сфере. Правовые аспекты регулирования и практического применения. М.: Изд. Государственной Думы, 2019. С. 46.

ния качества жизни населения и именно граждане становятся участниками проводимых экспериментов, возможность обеспечить соответствующий уровень защиты их прав приобретает особенное значение.

Важным является и обеспечение соблюдения баланса интересов участников рынка при использовании механизмов «регуляторных песочниц», исключение возможности их использования для недобросовестной конкуренции. В связи с этим особое значение приобретает разработка научно обоснованных эффективных инструментов контроля за всеми субъектами правоотношений при разработке и использовании технологий ИИ.

При этом особого внимания требуют вопросы юридической ответственности в сфере систем ИИ и роботехники[1], а также правового статуса соответствующих технологий[2], правосубъектности, информационной безопасности.

Квантовые коммуникации

В соответствии с определением, приведенным в преамбуле Дорожной карты развития «сквозной» цифровой технологии, «квантовые технологии, квантовые коммуникации — технология криптографической защиты информации, использующая для передачи ключей индивидуальные квантовые частицы. Главное преимущество квантовых коммуникаций — защищенность информации, гарантированная законами физики».

Квантовые коммуникации, как и все квантовые технологии, представляют собой следующее поколение информационных технологий, основанных на квантовой механике и открывающих новые возможности в сфере обеспечения безопасной передачи информации. Коммуникации на основе квантовых технологий имеют ряд преимуществ, в том числе:

- обеспечение более высокого уровня безопасности в процессе передачи данных, в том числе с использованием квантовой криптографии, позволяющей оперативно обнаружить факт вмешательства в передачу данных третьих лиц и предпринять необходимые меры по обеспечению безопас-

[1] См.: *Модели* правового регулирования создания, использования и распространения роботов и систем с искусственным интеллектом.
[2] См.: *Батурин Ю.М., Полубинская С.В.* Указ. соч. С. 141—154.

ности. Квантовые коммуникации не только открывают новые возможности в коммуникациях, но и создают угрозы безопасности коммуникациям, основанным на иных информационных технологиях. В связи с этим уже сейчас ведутся работы в области постквантовой криптографии;

- более высокая скорость передачи и обработки данных, создание «квантового» Интернета.

В настоящее время в Российской Федерации отсутствует специальное законодательное регулирование, учитывающее специфику применения технологий квантовых коммуникаций, а нормативную основу развития данной технологии в Российской Федерации обеспечивают два основных документа стратегического планирования:

- Дорожная карта развития «сквозной» цифровой технологии «квантовые технологии»[1];
- Паспорт «дорожной карты» развития высокотехнологичной области «квантовые коммуникации» на период до 2024 г.[2]

При этом формирование системы правового регулирования квантовых коммуникаций в Российской Федерации осуществляется в рамках преимущественно информационного законодательства, поскольку они являются разновидностью информационных технологий. Кроме того, квантовая, коммуникационная связь является разновидностью электросвязи. Соответственно на квантовые коммуникации полностью распространяются как общие нормы информационного законодательства, так и специальные нормы законодательства об информационных технологиях и нормы о связи, в том числе электросвязи.

Перспективные космические системы

В рамках настоящего исследования стоит отметить и перспективные космические системы, позволяющие реализовать широкий набор различных сервисов, широко востребованных во многих секторах экономики.

---

[1] См.: *Дорожная* карта развития «сквозной» цифровой технологии «Квантовые технологии» // СПС «КонсультантПлюс».

[2] См.: *Паспорт* «дорожной карты» развития высокотехнологичной области «квантовые коммуникации» на период до 2024 года, утвержден Минцифры России 27.08.2020 № 17 // СПС «КонсультантПлюс».

Цифровая трансформация придала значительный импульс развитию современных космических технологий, росту востребованности которых способствовало распространение новых видов цифровых услуг в труднодоступных регионах, рост экологических вызовов (мониторинг состояния опасных объектов, выбросов парниковых газов, развития чрезвычайных ситуаций).

Системы космической связи в ряде случаев являются резервными, а в районах, где отсутствует наземная инфраструктура связи, используются как основные. При этом цифровой формат реализации сервисов (медицинские, образовательные, досуговые и др.) требует устойчивой широкополосной связи на всей территории, в том числе в самых отдаленных районах, что особенно актуально в свете долгосрочных социально-экономических задач развития Арктического региона и Северного морского пути, где должны быть обеспечены все виды услуг связи, мониторинга и позиционирования, в том числе для наращивания грузопотока.

Решение задач по обеспечению современных продуктов и сервисов на основе космических технологий предусмотрено федеральным проектом «Комплексное развитие космических информационных технологий на 2022—2030 годы», реализация которого позволит охватить услугами спутниковой связи, цифрового вещания и высокоскоростного доступа в Интернет, а также спутникового Интернета вещей всю территорию Российской Федерации, а также обеспечит широкое внедрение сервисов на основе технологий дистанционного зондирования Земли в деятельность предприятий различных отраслей экономики, социальной сферы и государственного управления.

В настоящем исследовании отражена позиция авторов на состояние регулирования ключевых информационных технологий, отраженных в действующем законодательстве. При этом возникают вполне закономерные вопросы по существу рассмотренных норм.

Например, использование информационных технологий в сфере жилищно-коммунального хозяйства, что актуально для пресечения возможности собственников жилья или управляющих компаний искажать информацию, поступающую с датчиков или приборов, об использовании соответствующих ресурсов. Так, нормами ст. 9 Федерального закона от 21 июля 2014 г. № 209-ФЗ

«О государственной информационной системе жилищно-коммунального хозяйства» установлен правовой режим информации, размещенной в системе, и программ для электронных вычислительных машин системы. При этом применительно к данной ситуации можно отметить, что ответственность за причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием при отсутствии признаков хищения с использованием информационных технологий в целом не предусмотрена. Однако не предусмотрены нормы, устанавливающие правовой режим информационных технологий в медицинской деятельности, а также при использовании современных экосистем и цифровых платформ.

Таким образом, цифровая трансформация многих сфер жизнедеятельности и экономической активности наряду с ожидаемым эффектом имеет и определенные проблемы реализации, актуализирует вопросы, не получившие отражения в современном законодательстве Российской Федерации, в том числе с позиции уголовно-правовых рисков.

1.3. Преступность в сфере информационных технологий как угроза национальной и международной информационной безопасности

Т.А. Полякова[1], *А.А. Смирнов*[2]

Одной из ключевых угроз национальной безопасности и вызовов праву в настоящее время является преступность в сфере информационных технологий. Киберпространство, или ИКТ-сред, прочно утвердилось в качестве области деятельности преступных элементов. Опасность возрастающей угрозы, исходящей от преступлений в сфере информационных технологий, подчер-

[1] Татьяна Анатольевна Полякова — главный научный сотрудник, и.о. заведующего сектором информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, профессор, заслуженный юрист Российской Федерации.

[2] Александр Александрович Смирнов — ведущий научный сотрудник 3-го отдела НИЦ № 4 ВНИИ МВД России, старший научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН, доктор юридических наук, доцент.

кивается в базовых документах стратегического планирования в области национальной безопасности Российской Федерации. Так, в Доктрине информационной безопасности[1] в числе угроз информационной безопасности отмечалось увеличение масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом подчеркивалось, что методы, способы и средства совершения таких преступлений становятся все изощреннее (п. 14).

В действующем в настоящее время в России базовом документе стратегического планирования — Стратегии национальной безопасности Российской Федерации[2] обращено внимание на возрастающую угрозу криминальной активности в Интернете: «…в информационно-телекоммуникационной сети «Интернет» размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, осуществляется пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещается иная противоправная информация» (п. 52). Отдельно подчеркивается влияние фактора анонимности на преступную деятельность: «…анонимность, которая обеспечивается за счет использования информационно-коммуникационных технологий, облегчает совершение преступлений, расширяет возможности для легализации доходов, полученных преступным путем, и финансирования терроризма, распространения наркотических средств и психотропных веществ» (п. 54). Аналогичное положение о роли анонимности как криминогенного фактора отражено в недавно утвержденной Концепции

[1] Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. См.: *СЗ* РФ. 2016. № 50. Ст. 707.

[2] Утверждена Указом Президента РФ 2 июля 2021 г. № 400. См.: *СЗ* РФ. 2021. № 27. Ст. 5351.

информационной безопасности Союзного государства Республики Беларусь и России[1].

В Основах государственной политики Российской Федерации в области международной информационной безопасности[2] в числе основных угроз международной информационной безопасности выделены использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества в числе основных угроз международной информационной безопасности (подп. «г» п. 8).

В новой Концепции внешней политики[3] формирование и совершенствование международно-правовых основ противодействия использованию информационно-коммуникационных технологий в преступных целях названы одним из приоритетных направлений внешней политики России в области международной информационной безопасности (подп. 2 п. 30).

Хотя, согласно официальной статистике, темп роста преступлений, совершенных с использованием информационно-коммуникационных технологий (далее — ИКТ), в последние годы несколько замедлился, их число уже превышает полмиллиона. И это несмотря на общеизвестную латентность таких преступлений. Так, по данным ГИАЦ МВД России, в 2022 г. зарегистрировано 522,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. При этом доля таких преступлений в общей структуре преступности уже составляет более четверти (26,5%).

Кроме того, важно отметить то обстоятельство, что больше половины таких преступлений (52,1%) относится к категориям тяжких и особо тяжких (272,2 тыс.). А почти три четверти (73,0%) совершается с использованием сети Интернет (381,1 тыс.), и более трети от общего количества таких преступлений (40,8%) — с использованием средств мобильной связи (213,0 тыс.). Пример-

[1] Утверждена постановлением Высшего Государственного Совета Союзного государства от 22 февраля 2023 г. № 1. Официально не опубликована.

[2] Утверждены Указом Президента РФ от 12 апреля 2021 г. № 213. См.: *СЗ* РФ. 2021. № 16. Ст. 2746.

[3] Утверждены Указом Президента РФ от 31 марта 2023 г. № 229. См.: *Официальный* интернет-портал правовой информации. http://publi-cation.pravo.gov.ru/Document/View/0001202303310007 (дата обращения: 31.03.2023).

но три четверти таких преступлений (71,1%) совершается путем кражи или мошенничества (371,2 тыс.), а почти каждое восьмое преступление (11,9%) — в целях незаконного производства, сбыта или пересылки наркотических средств (62,2 тыс.)[1].

Наиболее массовыми видами преступлений с использованием ИКТ в Российской Федерации сегодня являются мошенничества и кражи денежных средств со счетов граждан и организаций. С попытками телефонного или компьютерного мошенничества сталкивался практически каждый гражданин нашей страны, пользующийся мобильным телефоном и компьютером.

При этом экономические потери от преступлений в сфере высоких технологий возрастают с каждым годом и исчисляются уже десятками миллиардов рублей. Как отметил министр внутренних дел Российской Федерации В.А. Колокольцев в ходе выступления на правительственном часе в Государственной Думе в октябре 2022 г., с начала года ущерб от преступлений в сфере IT увеличился на 20%, составив 65 млрд руб.[2] В мировом масштабе, по экспертным оценкам, доходы от киберпреступности уже превышают доходы наркоторговцев[3].

Также следует обратить внимание на постоянное совершенствование средств и методов, которые используются при совершении преступлений в сфере компьютерной информации. Кроме того, нельзя не отметить, что сегодня активно действует международный подпольный рынок в области киберпреступности, где предоставляются узкоспециализированные услуги криминального характера (DDoS-атаки, кража данных и финансовых средств, мошенничество, вымогательство, рассылка спама и др.)[4].

Одной из возрастающих угроз национальной безопасности следует признать также то, что информационно-телекоммуни-

---

[1] *Состояние* преступности в России за январь-декабрь 2022 г. ГИАЦ МВД России, 2023.

[2] См.: *Ущерб* от IT-преступлений в России с начала года вырос на 20% // Коммерсант. 19.10.2022. https://www.kommersant.ru/doc/5620873 (дата обращения: 12.02.2023).

[3] См.: *Международная* информационная безопасность: подходы России / Рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. М.: МГИМО МИД России, 2021. С. 8.

[4] См.: *Киберпреступность* как угроза международной информационной безопасности // Международная информационная безопасность: Теория и практика: В 3 т. Т. 1: Учебник для вузов / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект Пресс, 2021. С. 251.

кационные сети, включая сеть Интернет и пиринговые сети, активно используются преступниками для распространения порнографических материалов с участием несовершеннолетних, совращения детей и вовлечения их в сексуальную эксплуатацию. Через социальные сети, интернет-форумы и сеть Tor осуществляется торговля наркотическими средствами, психотропными веществами и их прекурсорами, новыми потенциально опасными психоактивными веществами, а также оружием, боеприпасами, взрывчатыми веществами и взрывными устройствами.

ИКТ все шире используются для совершения традиционных преступлений и административных правонарушений. Такое активное развитие информационной сферы приводит к постоянной адаптации противоправной деятельности к достижениям научно-технического прогресса в информационной сфере. Следует признать, что динамика развития сквозных технологий ИИ, виртуальной и дополненной реальности, квантовых технологий создает новые угрозы криминального характера для личности, общества и государства.

Проблема противодействия использованию информационных технологий в криминальных целях как одной из угроз международной информационной безопасности находится в фокусе внимания мирового сообщества. Следует обратить внимание, что в целой серии резолюций Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности», которые начиная с 1998 г. вносились в ООН по инициативе России, отмечается необходимость «предотвратить использование информационных ресурсов и технологий в преступных или террористических целях». Особо важно отметить, что борьбе с киберпреступностью посвящены такие специальные резолюции Генеральной Ассамблеи ООН, как A/55/63[1] и A/RES/56/121[2] «Борьба с преступным использованием

[1] См.: *Резолюция* Генеральной Ассамблеи ООН A/55/63 от 4 декабря 2000 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. URL: http://www.un.org/ru/documents/ods. asp?m= A/RES/ 55/63 (дата обращения: 23.04.2021).

[2] См.: *Резолюция* Генеральной Ассамблеи ООН A/56/121 от 19 декабря 2001 г. «Борьба с преступным использованием информационных технологий» // Организация Объединенных Наций. URL: http://www.un.org/ru/documents/ods.asp?m= A/RES/56/121 (дата обращения: 23.04.2021).

информационных технологий», A/73/187[1] и A/74/247[2] «Противодействие использованию информационно-коммуникационных технологий в преступных целях».

Вместе с тем до настоящего времени отсутствует универсальный международный договор, который регламентировал бы сферу борьбы с киберпреступностью. В 2017 г. Российская Федерация представила в ООН первый проект Конвенции о сотрудничестве в сфере противодействия информационной преступности[3]. В 2019 г. по инициативе нашей страны был учрежден специальный комитет ООН для разработки всеобъемлющей международной конвенции, и уже через два года Россия внесла в него проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях[4] (далее — проект Конвенции ООН о противодействию использованию ИКТ в преступных целях). В настоящее время работа в рамках специального межправительственного комитета ООН продолжается. Итоговый текст проекта указанной Конвенции Спецкомитет должен представить Генеральной Ассамблее ООН в ходе ее 78-й сессии (в 2024 г.)[5].

Необходимо также отметить и тот факт, что информационная преступность выделяется среди основных угроз международной

---

[1] См.: *Резолюция* Генеральной Ассамблеи ООН A/73/187 от 17 декабря 2018 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/73/187 (дата обращения: 23.04.2021).

[2] См.: *Резолюция* Генеральной Ассамблеи ООН A/74/247 от 27 декабря 2019 г. «Противодействие использованию информационно-коммуникационных технологий в преступных целях» // Организация Объединенных Наций. URL: https://undocs. org/pdf?symbol=ru/A/Res/74/247 (дата обращения: 23.04.2021).

[3] См.: *Проект* Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности A/C.3/72/12 от 17 октября 2021 г. // Организация Объединенных Наций. URL: https://undocs. org/ru/A/C.3/72/12 (дата обращения: 05.04.2021).

[4] См.: *О внесении* в Спецкомитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // МИД России. 28.07.2021. URL: https://archive.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения: 27.09.2021).

[5] См.: *О первой* сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности // МИД России. 12.03.2022. https://www.mid.ru/ru/foreign_policy/news/1803908/ (дата обращения: 23.02.2023).

информационной безопасности в Соглашении между правительствами государств — членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.[1], Соглашении о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г.[2], Соглашении о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г.[3], а также российской концепции Конвенции об обеспечении международной информационной безопасности 2021 г.[4]

Следует учитывать, что одним из первых региональных документов по противодействию преступности в сфере информационных технологий являлось Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г.[5] Данное Соглашение определяло терминологический аппарат и перечень уголовно наказуемых деяний, а также субъекты, формы и процессуальные аспекты сотрудничества государств Содружества в борьбе с преступлениями в сфере компьютерной информации.

Однако в 2018 г. в рамках СНГ было принято новое Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий[6]. Даже из наименования документа видно значительное расширение предмета его правового регулирования. Перечень уголовно наказуемых деяний включает уже не четыре, а восемь составов преступлений в сфере информационных технологий, включая хищения имущества с использованием

---

[1] См.: *Бюллетень* международных договоров. 2012. № 2.

[2] Официальный портал правовой информации. 06.04.2015. http://publication. pravo.gov.ru/Document/View/0001201506040007 (дата обращения: 12.01.2023).

[3] См.: *Официальный* портал правовой информации. 26.04.2019. http://publication. pravo.gov.ru/Document/View/0001201904260001?index=1&rangeSize=1 (дата обращения: 12.01.2023).

[4] Совета Безопасности РФ. См.: *Совет* Безопасности РФ. URL: http://www. scrf.gov.ru/security/information/document112/ (дата обращения: 09.01.2022).

[5] См.: *Бюллетень* международных договоров. 2009. № 6.

[6] См.: Там же. 2022. № 9.

ИКТ и распространение экстремистских материалов в информационно-телекоммуникационных сетях. Также в Соглашении регламентированы формы и процедура сотрудничества государств — участников СНГ в рассматриваемой сфере.

Кроме того, одним из наиболее известных региональных международных договоров в области борьбы с киберпреступностью является Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г.[1] (далее — Конвенция о киберпреступности), подписанная в г. Будапеште, которую нередко называют Будапештской конвенцией. По состоянию на март 2023 г. ее участниками являются 68 государств, причем среди них не только страны — члены Совета Европы, но и государства Азии, Африки, Северной и Латинской Америки[2]. Обращает внимание тот факт, что Россия не подписала и соответственно не ратифицировала данную Конвенцию из-за неприемлемости нормы п. «b» ст. 32 о трансграничном доступе к компьютерным данным без уведомления и согласия компетентных органов государства.

Однако следует отметить, что впоследствии были приняты Дополнительный протокол в отношении криминализации деяний расистского и ксенофобского характера, совершаемых при помощи компьютерных систем, от 28 января 2003 г.[3] (далее — Дополнительный протокол к Конвенции о киберпреступности) и Второй протокол, касающийся расширения сотрудничества и раскрытия электронных доказательств, от 17 ноября 2021 г.[4] Указанные акты определяют составы киберпреступлений, процессуальные аспекты борьбы с ними, регламентируют вопросы

---

[1] См.: *Convention* on Cybercrime. Budapest, 23.XI.2001 (ETS — № 185) // Council of Europe. URL: https://rm.coe.int/1680081561 (дата обращения: 06.02.2022).

[2] См.: *Chart* of signatures and ratifications of Treaty 185 // Council of Europe. Status as of 18/03/2023. URL: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (дата обращения: 06.02.2022).

[3] См.: *Additional* Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 28.I.2003 (ETS No. 189) // Council of Europe. URL: https://rm.coe.int/168008160f (дата обращения: 06.02.2022).

[4] См.: *Second* Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence Council of Europe. URL: https://rm.coe.int/1680a49dab (дата обращения: 06.02.2022).

юрисдикции и международного сотрудничества в борьбе с киберпреступностью.

В Основах государственной политики Российской Федерации в области международной информационной безопасности определены основные направления реализации государственной политики в области международной информационной безопасности по повышению эффективности международного сотрудничества, направленные на противодействие угрозе использования информационно-коммуникационных технологий в преступных целях, и по созданию необходимого для этого международно-правового режима (п. 15), к которым отнесены:

а) содействие разработке специальным межправительственным комитетом экспертов открытого состава всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также создание условий для последующего принятия государствами — членами ООН данной Конвенции;

б) развитие сотрудничества с государствами — участниками СНГ, объединения БРИКС, государствами — членами ОДКБ, ШОС, АСЕАН, «Группы двадцати», другими государствами и международными организациями по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях;

в) повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере компьютерной информации, а также случаев мошенничества с использованием информационно-коммуникационных технологий;

г) совершенствование механизма обмена информацией о методиках расследования преступлений в сфере компьютерной информации, случаев мошенничества с использованием информационно-коммуникационных технологий, а также о судебной практике рассмотрения уголовных дел о таких преступлениях;

д) организация международных конференций и семинаров по вопросам противодействия использованию информационно-коммуникационных технологий в преступных целях.

Проблемы понятийного аппарата, связанного с противодействием преступности в сфере информационных технологий

Следует признать, что до настоящего времени понятийный аппарат в области противодействия преступности в сфере информационных технологий в полной мере не сформирован. В международном сообществе сегодня также отсутствует единый подход к определению рассматриваемого вида преступности, хотя выработана определенная унификация в соответствии с региональными международными договорами в сфере борьбы с преступлениями в сфере информационных технологий.

Два определения киберпреступности были выработаны на 10-м Конгрессе ООН по предупреждению преступности и обращению с правонарушителями (2000 г., Вена) в рамках соответствующего тематического семинара. В узком смысле под киберпреступностью предлагалось понимать «любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных», а в широком — «любое противозаконное поведение, осуществляемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное владение, предложение или распространение информации посредством компьютерной системы или сети»[1]. Однако в Российской Федерации понятие «киберпреступность» не имеет своего легитимного закрепления.

Поскольку наиболее известным международным договором в данной области является, как уже отмечалось, Будапештская конвенция о киберпреступности, то в большинстве стран мира для обозначения преступлений в сфере ИКТ используется термин «*киберпреступность*».

Российской Федерацией, а также государствами — участниками СНГ, ШОС и ОДКБ в официальных документах применяется иной терминологических подход. Вместо «киберпреступности» используются термины «информационная преступность», «использование информационно-коммуникационных технологий в преступных целях», «преступность в сфере информационных технологий» и т.п. При этом следует обратить внимание, что устоявшийся и

[1] См.: *Овчинский В.С.* Криминология цифрового мира: Учебник для магистратуры. М.: Норма — Инфра-М, 2018. С. 68—69.

нормативно закрепленный термин «преступления в сфере компьютерной информации» по своему содержанию гораздо у́же по сравнению с «преступлениями в сфере информационных технологий» и является лишь одной из составных частей таких преступлений.

В региональных международных соглашениях по информационной безопасности ШОС и СНГ используется понятие «информационная преступность», которая трактуется как «использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях».

В российской научной доктрине и правоприменительный практике также наблюдается существенная дифференциация подходов к терминологическому и содержательному определению преступлений в сфере информационных технологий. Наибольшие различия наблюдаются в научных исследованиях, где употребляются понятия «компьютерная преступность»[1], «интернет-преступность»[2], «киберпреступность»[3], «цифровая преступность»[4], а также «преступления в сфере высоких технологий»[5], «преступления в сфере информационных технологий»[6], «преступления, со-

---

[1] См.: *Евдокимов К.Н.* Противодействие компьютерной преступности: теория, законодательство, практика: Дис. ... докт. юрид. наук. М., 2021; *Лопатина Т.М.* Криминологические и уголовно-правовые основы противодействия компьютерной преступности: Дис. ... докт. юрид. наук. М., 2007; *Добровольский Д. В.* Актуальные проблемы борьбы с компьютерной преступностью: Дис. … канд. юрид. наук. М., 2005.

[2] См.: *Дремлюга Р.И.* Интернет-преступность: Монография. Владивосток: Изд-во Дальневост. ун-та, 2008.

[3] См.: *Побегайло А.Э.* Киберпреступность: Учеб. пособие (для бакалавров). М.: Акад. Генеральной прокуратуры РФ, 2014; *Чекунов И.Г.* Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: Автореф. дис. … канд. юрид. наук. М., 2013; *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. … канд. юрид. наук. Владивосток, 2005.

[4] См.: *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения: Монография. 2-е изд., перераб. и доп. М.: Инфра-М, 2022; *Поляков И.В.* Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. 2020. № 4. С. 21—25.

[5] См.: *Противодействие* киберпреступлениям и преступлениям в сфере высоких технологий: Материалы Всерос. науч.-практ. конф. (Москва, 10 декабря 2020 г.) / Под общ. ред. Д.Н. Кожухарика. М.: Моск. акад.Следственного комитета РФ, 2021; *Никеров Д.М., Хохлова О.М.* Преступления в сфере высоких технологий в современной России // Вестн. Вост.-Сиб. ин-та МВД России. 2019. № 2. С. 89—93.

[6] См.: *Мысина А.И.* Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий: Дис. … канд. юрид. наук. М., 2021.

вершаемые в сфере информационных технологий»[1] и др. При этом ряд российских авторов настаивают на необходимости отхода от использования заимствованного с Запада термина «киберпреступность». В.Г. Степанов-Егиянц указывает по этому поводу следующее: «В целом представляется целесообразным, с точки зрения уголовно-правовой семантики отойти от «кибер»-терминологии и перейти к традиционно русской, к терминам, известным национальному уголовному и информационному праву, и все известные явления, реалии, процессы, описываемые с помощью приставки «кибер», трансформировать в аналогичные явления, описываемые с помощью понятия «информация», «компьютер». Иначе говоря, по нашему мнению, понятие «киберсфера» может быть без всяких потерь заменено понятием «информационная сфера», понятие «киберпреступность» — компьютерная преступность, киберсистема — информационная система и т.д.»[2].

Нам представляется наиболее целесообразным в настоящей работе использовать термин «преступления в сфере информационных технологий», который применяется в Соглашении СНГ 2018 года. Однако в тексте данного международного договора не содержится определение данного понятия.

Вместе с тем такие дефиниции выработаны научной доктриной. Например, А.И. Мысина в своей диссертации определила преступление в сфере информационных технологий как «противоправное общественно опасное виновно совершенное уголовно наказуемое деяние, причиняющее вред или создающие опасность причинения вреда личности, государству или международному сообществу, предметом посягательства которого являются информационные технологии и/или которое совершено с использованием информационных технологий»[3].

Что касается правоприменительной практики, то длительное время основным субъектом борьбы с преступлениями в сфере

---

[1] *Андреев А.В., Гончар В.В., Горач Н.Н.* и др. Противодействие преступлениям, совершаемым в сфере информационных технологий: Учебник / Под ред. И.А. Калиниченко. М.: Инфра-М, 2022.

[2] *Степанов-Егиянц В.Г.* Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): Дис. … докт. юрид. наук. М., 2016. С. 51—52.

[3] *Мысина А.И.* Международно-правовое регулирование сотрудничества государств по противодействию преступлениям в сфере информационных технологий: Автореф. дис. … канд. юрид. наук. М., 2021. С. 12.

информационных технологий выступало Управление «К» Бюро специальных технических мероприятий МВД России (далее — Управление «К»). К числу его основных направлений работы относились выявление, предупреждение, пресечение и раскрытие преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) и направленных против здоровья несовершеннолетних и общественной нравственности, включая изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних; использование несовершеннолетнего в целях изготовления порнографических материалов или предметов[1].

В 2022 г. в рамках реализации Указа Президента РФ от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» в структуре МВД России было создано новое Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России)[2]. В соответствии с Положением об УБК МВД России[3] на него возложены функции головного подразделения Министерства в области борьбы с преступлениями, совершенными с использованием (в сфере) информационно-коммуникационных технологий, а также противодействия распространению противоправной информации в информационно-телекоммуникационной сети Интернет (п. 2). Как видно из анализа норм Положения об УБК МВД России, в нем используются такие термины, как «преступления, совершенные с использованием (в сфере) информационно-коммуникационных технологий».

---

[1] См.: *Управление* «К» МВД России // МВД России. https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 28.06.2021).

[2] См.: *В структуре* МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий // МВД медиа. 30 сентября 2022 г. https://mvdmedia.ru/news/official/v-strukture-mvd-rossii-sozdano-upravlenie-po-organizatsii-borby-s-protivopravnym-ispol-zovaniem-infor/ (дата обращения: 09.01.2023).

[3] Приказ МВД России от 29 декабря 2022 г. № 1110 «Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации».

В Московском университете МВД России им. В.Я. Кикотя в июле 2022 г. создана кафедра противодействия преступлениям в сфере ИКТ[1].

Следует отметить, что Президент РФ В.В. Путин в ходе выступления на коллегии МВД России 20 марта 2023 г. назвал борьбу с преступлениями с использованием информационных технологий одним из безусловных приоритетов работы ведомства[2].

Для противодействия указанным преступлениям, составляющим угрозу национальной и международной информационной безопасности, представляется важным научное исследование таких значимых вопросов, как классификация и виды преступлений в сфере информационных технологий. Исследование показывает, что наблюдается существенная разница в применяемых правовых подходах.

Так, в тексте Будапештской конвенции о киберпреступности выделены четыре основные категории киберпреступлений:

1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;

2) преступления, связанные с использованием компьютерных средств;

3) преступления, связанные с содержанием данных;

4) преступления, связанные с нарушением авторского права и смежных прав.

Как уже отмечалось, Протокол к данной Конвенции предусматривает криминализацию в законодательстве государств деяний, связанных с распространением расистских и ксенофобских материалов посредством компьютерных систем, угрозами и оскорблениями расистского характера, одобрением или оправданием геноцида и иных преступлений против человечности.

Также составы преступлений, относимых к киберпреступности, закреплены в Факультативном протоколе к Конвенции о правах ребенка, касающемся торговли детьми, детской проституции

---

[1] См.: *Кафедра* противодействия преступлениям в сфере информационно-телекоммуникационных технологий // Московский университет МВД России имени В.Я. Кикотя. https://мосу.мвд.рф/Universitet/структ/кафедры/кафедра-противодействия-преступлениям-в- (дата обращения: 12.02.2023).

[2] См.: *Расширенное* заседание коллегии МВД России // Президент России. 20 марта 2023 г. http://www.kremlin.ru/events/president/news/70744 (дата обращения: 20.03.2023).

и детской порнографии, от 25 мая 2000 г.[1] (далее — Факультативный договор) и Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25 октября 2007 г.[2] (далее — Конвенция о защите детей).

В Европейском Союзе при выстраивании государственной политики по противодействию киберпреступности исходили из выделения четырех следующих категорий киберпреступлений[3]:

1) традиционные виды преступлений (мошенничество, подделка документов и т.п.), совершаемые с использованием электронных коммуникационных сетей и информационных систем;

2) размещение незаконного контента в электронных медиа;

3) атаки против информационных систем, блокирование программного обеспечения сайтов и хакерство;

4) преступления, связанные с нарушением авторского права и смежных прав.

В 2012—2013 гг. было проведено несколько крупных международных исследований по теме киберпреступности[4], в которых сделан вывод о наличии базового консенсуса в отношении криминализации 14 деяний. При этом отмечено, что для национальных подходов возможны изъятия из общего перечня, закрепление дополнительных квалифицирующих признаков (умысла и др.) или криминализация иных деяний (непристойных материалов, онлайн-казино, незаконных рынков наркотиков и оружия). Следует сделать оговорку, что сам термин «киберпреступность» при обозначении данных составов преступлений на момент проведения исследования (2013) использовался весьма редко, поэтому изложенный ниже перечень сформирован аналитическим путем.

---

[1] См.: *Организация* Объединенных Наций: официальный сайт. URL: http://www.un.org/ru/documents/decl_conv/conventions/rightschild_protocol2.shtml (дата обращения: 14 июня 2021 г.).

[2] См.: *Бюллетень* международных договоров. 2014. № 6.

[3] См.: *Communication* from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 «Towards a general policy on the fight against cyber crime». Brussels, 22.5.2007. COM(2007) 267 final.

[4] См.: *Герке М.* Понимание киберпреступности: явление, задачи и законодательный ответ / Международный союз электросвязи, 2012; *Всестороннее* исследование проблемы киберпреступности и ответных мер со стороны государст-членов, международного сообщества и частного сектора. УПН ООН, 2013 (Comprehensive Study on Cybercrime. UNODC, 2013).

Перечень 14 деяний, признанных киберпреступлениями, включает[1]:

1) незаконный доступ к компьютерной системе;

2) незаконный доступ, перехват или получение компьютерных данных;

3) незаконное вмешательство в данные или вмешательство в систему;

4) производство, распространение или хранение средств неправомерного использования компьютеров;

5) нарушение конфиденциальности или мер защиты данных;

6) компьютерное мошенничество или подлог;

7) компьютерные преступления, связанные с использованием персональных данных;

8) компьютерные преступления, касающиеся авторских прав или товарных знаков;

9) распространение спама;

10) компьютерные преступления, связанные с причинением личного вреда;

11) компьютерные преступления, связанные с расизмом или ксенофобией;

12) использование компьютеров в целях производства, распространения или хранения детской порнографии;

13) использование компьютера для завлечения детей (кибергруминг);

14) использование компьютера для содействия террористическим преступлениям.

В Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий 2018 г. определен конкретный перечень составов таких преступлений:

а) уничтожение, блокирование, модификация либо копирование информации, нарушение работы информационной (компьютерной) системы путем несанкционированного доступа к охраняемой законом компьютерной информации;

---

[1] См.: *Всестороннее* исследование проблемы киберпреступности и ответных мер со стороны государств — членов, международного сообщества и частного сектора. УПН ООН, 2013 (Comprehensive Study on Cybercrime. UNODC, 2013).

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации компьютерной системы лицом, имеющим к ней доступ, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, если это деяние причинило существенный вред или тяжкие последствия;

г) хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации, либо сопряженное с несанкционированным доступом к охраняемой законом компьютерной информации;

д) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи порнографических материалов или предметов порнографического характера с изображением несовершеннолетнего;

е) изготовление в целях сбыта либо сбыт специальных программных или аппаратных средств получения несанкционированного доступа к защищенной компьютерной системе или сети;

ж) незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, а равно присвоение авторства, если это деяние причинило существенный ущерб;

з) распространение с использованием информационно-телекоммуникационной сети Интернет или иных каналов электрической связи материалов, признанных в установленном порядке экстремистскими или содержащих призывы к осуществлению террористической деятельности или оправданию терроризма.

Наиболее широкий перечень преступлений в сфере информационных технологий предложен в российском проекте Конвенции ООН о противодействии использованию ИКТ в преступных целях 2021 г. Полагаем, что такой подход отражает опыт развития российского уголовного законодательства последнего десятилетия. Данный перечень включает в себя следующие составы преступлений (ст. 6—28 проекта Конвенции ООН о противодействии использованию ИКТ в преступных целях):

1) неправомерный доступ к цифровой информации;

2) неправомерный перехват;

3) неправомерное воздействие на цифровую информацию;

4) нарушение функционирования информационно-коммуникационных сетей;

5) создание, использование и распространение вредоносных программ;

6) неправомерное воздействие на критическую информационную инфраструктуру;

7) несанкционированный доступ к персональным данным;

8) незаконный оборот устройств;

9) хищение с использованием ИКТ;

10) преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ;

11) склонение к самоубийству или доведение до его совершения;

12) преступления, связанные с вовлечением несовершеннолетних к совершению противоправных действий, опасных для его жизни и здоровья;

13) создание и использование цифровой информации для введения пользователя в заблуждение;

14) подстрекательство к подрывной или вооруженной деятельности;

15) преступления, связанные с террористической деятельностью;

16) преступления, связанные с экстремистской деятельностью;

17) преступления, связанные с распространением наркотических средств и психотропных веществ;

18) преступления, связанные с незаконным оборотом оружия;

19) реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности;

20) незаконное распространение фальсифицированных лекарственных средств и медицинских изделий;

21) использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом;

22) нарушение авторских и смежных прав с использованием ИКТ;

23) соучастие в преступлении, приготовление к преступлению и покушение на преступление.

Кроме того, в проекте Конвенции ООН о противодействии использованию ИКТ в преступных целях содержится оговорка: «Настоящая Конвенция не является препятствием для признания государством-участником в качестве преступления любого другого противоправного деяния, совершенного умышленно с использованием ИКТ и повлекшего существенный ущерб» (ст. 29).

Наряду с этим следует признать, что в законодательстве Российской Федерации сегодня отсутствует как общепринятая терминология для обозначения преступлений в сфере информационных технологий, так и четкий перечень таких преступлений. В Уголовном кодексе Российской Федерации содержится отдельная глава 28 «Преступления в сфере компьютерной информации», тогда как другие составы преступлений в информационной сфере находятся в различных главах УК РФ.

В конце прошлого года было принято постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»»[1].

Следует признать, что систематизированное понимание перечня преступлений в сфере информационных технологий выработано правоприменительной практикой в области уголовной статистики. В официальной статистической отчетности о состоянии преступности, которую в соответствии со своими полномочиями ведет ГИАЦ МВД России, выделяется отдельная категория учета: преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. В соответствующем разделе такой отчетности за 2022 г. указано, что показатели сформированы в соответствии с перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 30 июня 2022 г. № 361/11/1.

[1] *Бюллетень* Верховного Суда РФ. 2023. № 3.

Однако данное указание было отменено в начале 2023 г. в связи с вступлением в силу нового аналогичного указания Генпрокуратуры России № 11/11, МВД России № 1 от 17 января 2023 г.[1] В нем также содержится перечень № 25 преступлений, совершенных с использованием (применением) ИКТ или в сфере компьютерной информации. В соответствии с перечнем № 25 к данной категории преступлений без дополнительных условий отнесены следующие преступления:

а) кража, совершенная с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ) (п. «г» ч. 3 ст. 158 УК РФ);

б) мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ);

в) мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ);

г) незаконные приобретение, передача, хранение, перевозка, пересылка или ношение огнестрельного оружия, его основных частей и боеприпасов к нему[2], совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 3 ст. 222 УК РФ);

д) незаконный сбыт огнестрельного оружия, его основных частей, боеприпасов к нему, совершенный с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 5 ст. 222 УК РФ);

е) незаконные приобретение, передача, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 3 ст. 222.1 УК РФ);

ж) незаконный сбыт взрывчатых веществ или взрывных устройств, совершенный с использованием информационно-теле-

[1] СПС «КонсультантПлюс».

[2] В данном пункте воспроизведена буквально законодательная конструкция состава преступления, предусмотренного п. «в» ч. 3 ст. 222 УК РФ. Однако очевидно, что с использованием информационно-телекоммуникационных сетей может совершаться лишь часть деяний, перечисленных в диспозиции указанной нормы. Данная оговорка также касается норм п. «в» ч. 3 ст. 222.1, п. «в» ч. 3 ст. 222.2 УК РФ

коммуникационных сетей, в том числе сети Интернет (п. «в» ч. 5 ст. 222.1 УК РФ);

з) незаконные приобретение, передача, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 3 ст. 222.2 УК РФ);

и) незаконный сбыт крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему, совершенный с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (п. «в» ч. 5 ст. 222.2 УК РФ);

к) склонение к потреблению наркотических средств, психотропных веществ или их аналогов (п. «д» ч. 2 ст. 230 УК РФ);

л) фото-, кино- или видеосъемка несовершеннолетнего в целях изготовления и (или) распространения порнографических материалов или предметов либо привлечение несовершеннолетнего в качестве исполнителя для участия в зрелищном мероприятии порнографического характера, совершенные лицом, достигшим 18-летнего возраста, совершенные с использованием информационно-телекоммуникационных сетей (включая сеть Интернет) (п. «г» ч. 2 ст. 242.2 УК РФ);

м) неправомерный доступ к компьютерной информации (ст. 272 УК РФ);

н) создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);

о) нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

п) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ);

р) нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования (ст. 274.2 УК РФ).

Далее приводится перечень преступлений, относящихся к рассматриваемой категории преступлений при наличии определенных условий. Так, к ним относятся преступления, которые в соответствии с Особенной частью УК РФ имеют альтернативный ква-

лифицирующий признак, предполагающий использование информационно-телекоммуникационных сетей, включая сеть Интернет, при наличии соответствующей отметки, предусмотренные п. «д» ч. 2 ст. 110, п. «д» ч. 3 и ч. 6 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.1, п. «б» ч. 3 ст. 133, ч. 3 ст. 137, п. «в» ч. 2 ст. 151.2, ст. 171.2, 185.3, ч. 2 ст. 205.2, п. «б» ч. 2 и ч. 3, 4, 5 ст. 228.1, ч. 3, 4 ст. 230, ч. 1.1, 2 и 3 ст. 238.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 245, ч. 1.1, п. «б» ч. 2, ч. 2.1, 3 и 3.1 ст. 258.1, ч. 2 ст. 280, ч. 2 ст. 280.1, п. «в» ч. 2 ст. 280.4, ст. 282, п. «в» ч. 2 и ч. 4 ст. 354.1 УК РФ.

В п. 2.2 Перечня № 25 также приводится список преступлений, предусмотренных ст. 119, 128.1, 133, 135, 137, 138, 138.1, 146, 150, 151, ч. 4 ст. 158, ст. 159, 159.1, 159.2, 163, 165, 174, 174.1, 183, 186, 187, 205.1, 207, 207.1, 207.2, 207.3, 210, 228, 228.2, 228.3, 228.4, 229, 234, 234.1, 238, 240, 280.3, 283, 283.1, 284.2, 288, 292, 296, 298.1, 311, 327, 327.1, 354 УК РФ, которые относятся к перечню при наличии в статистической карточке отметок о следующих способах совершения преступления:

- с использованием сети Интернет (ресурсов глобальной сети);
- с использованием сети Даркнет (Теневая сеть), под которой понимается скрытая сеть, соединения которой устанавливаются по типу р-2-р (peer-to-peer, децентрализованная сеть);
- использование фишингового (поддельного) сайта или ссылки;
- с использованием средств мобильной связи, под которыми понимаются технические и программные средства, служащие для передачи информации беспроводным способом, без использования сети Интернет;
- неправомерное списание денежных средств со счетов банковских карт;
- использование вредоносных компьютерных программ, создание и распространение вредоносных компьютерных программ либо иной компьютерной информации, под которыми понимаются программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

- с использованием «программ-шифровальщиков», представляющих собой разновидность вредоносных программ, которые с помощью различных алгоритмов шифрования блокируют доступ пользователей к файлам либо преобразуют их содержимое на компьютере до состояния, непригодного к использованию правообладателем;
- с использованием бот-сетей (ботнет), под которыми подразумевается компьютерная сеть, состоящая из узлов, зараженных вредоносным программным обеспечением с возможностью централизованного управления без ведома владельцев узлов;
- с использованием DDoS-атак, представляющих собой распределенную атаку типа «отказ в обслуживании» с одновременным использованием большого числа атакующих компьютеров, в том числе объединенных в бот-сеть, целью которой, как правило, является воспрепятствование доступу легитимных пользователей к атакуемому ресурсу, частичное нарушение штатного функционирования информационной инфраструктуры и т.д.;
- с использованием информационно-телекоммуникационных технологий (отметка проставляется при использовании различных технологий, не имеющих самостоятельных кодовых значений для отражения в статистической карточке (машинные носители, технические средства снятия информации);
- с использованием (применением) компьютерной техники, под которой понимается компьютер, а также отдельное оборудование, которое работает совместно с ним и обеспечивает его дополнительную функциональность;
- с использованием (применением) расчетных (пластиковых) карт, отметка о котором проставляется при непосредственном использовании карт (в том числе кредитных) при совершении преступления;
- с использованием (применением) программных средств, под которым понимается любое программное обеспечение, установленное на персональном компьютере, смартфоне или другой технике;
- с использованием (применением) фиктивных электронных платежей, под которыми понимаются поддельные элект-

ронные платежные документы, имеющие равную юридическую силу с платежными документами на бумажных носителях;

- с использованием социальных сетей, под которыми понимаются платформы, онлайн-сервисы или веб-сайты, предназначенные для построения, отражения и организации социальных взаимоотношений;
- с использованием средств мгновенного обмена сообщениями (интернет-мессенджеров), под которыми понимаются приложения или программы, установленные на смартфоне или компьютере;
- с использованием электронных платежных систем, под которыми понимаются системы расчета между финансовыми организациями и интернет-пользователями при покупке-продаже товаров и оплате услуг;
- операции с цифровой валютой, под которыми понимаются выпуск цифровой валюты и осуществление в отношении нее действий;
- с использованием SIP-телефонии, под которой понимается система звонков через сеть Интернет с использованием протокола IP на обычные телефонные сети передачи голосовой информации (подвижной или стационарной);
- неправомерный доступ к компьютерной информации, под которым понимается получение возможности ознакомиться и (или) воспользоваться компьютерной информацией лицом, не обладающим правами на получение и работу с данной информацией либо компьютерной системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ (при условии уничтожения, блокирования, модификации либо копирования компьютерной информации);
- операции с цифровыми финансовыми активами, под которыми понимаются их выпуск и осуществление в отношении них действий;
- с использованием технологий «Дипфэйк», под которыми подразумеваются методика синтеза аудио или визуальной информации, основанная на искусственном интеллекте, целью которой является создание сравнимой с оригиналом копии аудио- или видеоизображения;

- использование специальных средств и техники, предназначенной для компрометации банковских устройств самообслуживания (банкоматов, терминалов);
- с использованием информационной инфраструктуры иностранного государства (или придание такого вида), под которой в том числе понимаются зарубежные серверы (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д.;
- с использованием информационной инфраструктуры стран — участников СНГ (или придание такого вида), под которой в том числе понимаются серверы стран — участников СНГ (услуги хостинг-провайдеров, интернет-провайдеров, почтовых серверов), доменные зоны, телефонные сети и т.д.

Таким образом, исследование показывает значительное разнообразие терминологических, содержательных подходов к определению преступлений в сфере информационных технологий (включая составы преступлений, их классификации, типологизации и т.д.). В целях противодействия преступности в указанной сфере в условиях экспоненциального роста и трансграничного характера информационных технологий необходимо совершенствование правового регулирования в рассматриваемой сфере.

Список литературы

1. *Риски* цифровизации: виды, характеристика, уголовно-правовая оценка / Под ред. Ю.В. Грачевой. М.: Проспект, 2022.
2. *Беспилотники* на дорогах России: (уголовно-правовые проблемы) / Под ред. А.И. Чучаева. М.: Проспект, 2021.
3. *Цифровые* риски и правовое обеспечение управления ими / А.А. Арямов, Ю.В. Грачева, А.И. Чучаев, С.В. Маликов. М.: Юридическая фирма Контракт, 2020.
4. *Искусственный* интеллект и интеллектуальные системы управления: Монография / А.Б. Барский. М.: Ruscience, 2022.
5. *Большие* данные и машинное обучение / М.А. Ахановa, С.В. Овчинникова, О.М. Барбаков. Тюмень: ТИУ, 2022.
6. *Блокчейн* на службе государства / А.В. Варнавский, А.О. Бурякова, Е.В. Себеченко. М.: КноРус, 2020.

7. Интернет вещей / Под ред. А.М. Тюрликова. СПб., ГУАП, 2021.
8. *Цифровая* трансформация: вызовы праву и векторы научных исследований: Монография / Под общ. ред. А.Н. Савенкова; Отв. ред. Т.А. Полякова, А.В. Минбалеев. М.: РГ-Пресс, 2021.
9. *Международная* информационная безопасность: подходы России / Рук. авт. кол. А.В. Крутских, Е.С. Зиновьева. М.: МГИМО МИД России, 2022.
10. *Международная* информационная безопасность: теория и практика. В 3 т. Т. 1: Учебник для вузов / Под общ. ред. А.В. Крутских. 2-е изд., доп. М.: Аспект-Пресс, 2021.
11. *Противодействие* преступлениям, совершаемым в сфере информационных технологий: учебник / А.В. Андреев, В.В. Гончар, Н.Н. Горач [и др.]; под ред. И.А. Калиниченко. М.: Инфра-М, 2022.
12. *Механизмы* и модели регулирования цифровых технологий: Монография / Под общ. ред. А.В. Минбалеева. М.: Проспект, 2023.
13. *Модели* правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальном информационном обществе: Монография / Под общ. ред. Т.А. Поляковой. Саратов: Амирит, 2020.
14. *Модели* правового регулирования создания, использования и распространения роботов и систем с искусственным интеллектом: монография / Под общ. ред. канд. юрид. наук В.Б. Наумова. СПб.: ПН-Принт, 2019.

Глава 2

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОГО ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРЕСТУПНЫХ ЦЕЛЯХ

2.1. Информационные технологии как объект уголовно-правовой защиты

С.В. Маликов[1]

Осознание рисков, связанных с развитием информационных технологий, мировым сообществом произошло довольно давно[2], что выразилось в принятии ряда программных документов, к которым можно отнести Конвенцию от 28 января 1981 г. «О защите физических лиц при автоматизированной обработке персональных данных»; Конвенцию Совета Европы от 4 октября 2001 г. «Об информационном и правовом сотрудничестве, касающемся «Информационных общественных услуг»»; Соглашение от 1 июня 2001 г. о сотрудничестве государств — участников СНГ в борьбе с преступлениями в сфере компьютерной информации; Конвенцию Совета Европы от 30 мая 2002 г. «О киберпреступности».

В таких актах, как правило, отмечается обеспокоенность переходом преступности в цифровое пространство, т.е. увеличением фактов использования компьютерной техники и сети Интернет

---

[1] Сергей Владимирович Маликов — заместитель директора Института государства и права РАН по научной работе, доктор юридических наук.

[2] Об этом подробно см., например: *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения. М., 2019; *Козаев Н.Ш.* Противодействие злоупотреблениям современными технологиям. М., 2016; и др.

при совершении преступлений. Основное внимание международного сообщества концентрируется на вопросах налаживания совместного противодействия отдельным видам преступлений в цифровом пространстве (терроризму, детской порнографии, хищения данных и др.)[1].

Национальная безопасность Российской Федерации в информационной сфере признается ключевым аспектом безопасности государства и охватывает всю совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности[2]. Стоит отметить, что Россия присоединяется не ко всем международным актам, а ее инициативы в ООН приводят лишь к формулированию определенных дорожных карт в области кибербезопасности[3].

Количество зарегистрированных преступлений, связанных с использованием информационно-телекоммуникационных технологий, за последние годы стремительно увеличивалось: 2017 г. — 62 404; 2018 г. — 132 733 (+112,7%); 2019 г. — 240 144 (+80,9%); 2020 г. — 510 396 (+73,4%); 2021 г. — 517 722 (+1,4%); 2022 г. — 522 065 (+0,8%) (рис. 2.1).

---

[1] Обзор международных подходов к вопросам обеспечения кибербезопасности представлен в отчете Международного союза электросвязи. См.: *Понимание* киберпреступности: Явление, задачи и законодательный ответ [Электронный ресурс]. Режим доступа: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_ R.pdf (Дата обращения: 06.05.2020).

[2] См.: *Указ* Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «КонсультантПлюс».

[3] См. об этом подробно: *Henriksen A.* The end of the road for the UN GGE process: The future regulation of cyberspace // Journal of Cybersecurity. Vol. 5. Iss. 1. 2019. P. 1—9.

Вопрос информационной безопасности был внесен в повестку дня Организации Объединенных Наций, когда в 1998 г. Российская Федерация впервые представила проект резолюции на заседании Первого комитета Генеральной Ассамблеи. Проект был принят без голосования. Последняя резолюция Генеральной Ассамблеи на данную тему была принята без голосования 2 декабря 2014 г. Соответствующие материалы размещены на сайте ООН. Режим доступа: https://www.un.org/disarmament/ru.

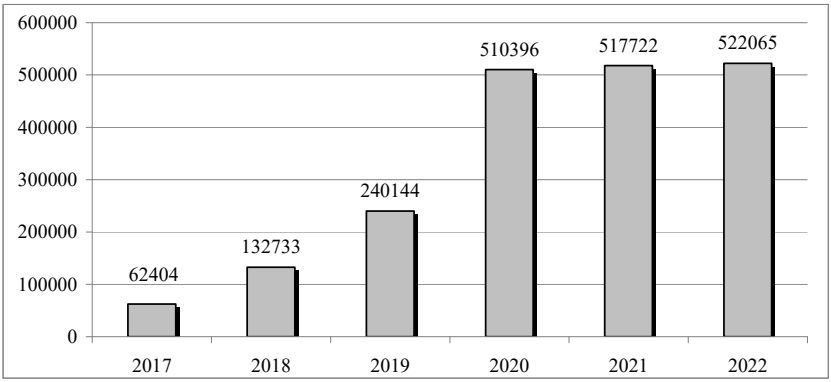

Рис. 2.1. **Количество зарегистрированных преступлений, связанных с использованием информационно-телекоммуникационных технологий в Российской Федерации с 2017 по 2022 гг.**

Две трети из регистрируемых общественно опасных деяний в цифровой среде являются преступлениями экстремистского характера, каждое девятое преступление — террористического характера. Значительно вырос уровень киберпреступности в сфере экономической деятельности. Киберпреступления приобрели организованный и транснациональный характер. Внимание экспертного и научного сообщества концентрируется на отдельных кибератаках, которые приобретают общественный и политический резонанс, являясь лишь видимой частью общей картины девиаций в цифровой среде, получающей освещение в средствах массовой информации.

Основной мишенью целевых кибератак остается государственный и финансовый сектор, а их мотивом — промышленный шпионаж или хищение, однако этим не исчерпывается девиантное поведение в цифровой среде, которое включает более широкий спектр общественно опасных деяний, до сих пор не изучавшихся системно:

а) деяния против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, получение, перехват, искажения);

б) деяния, связанные с контентом (порнографические материалы, экстремизм, терроризм, азартные игры, клевета, травля, спам, вымогательство);

в) деяния, связанные с правом собственности и товарными знаками;

г) деяния, связанные с применением компьютеров (мошенничество, подлог, присвоение идентифицирующей информации, неправомерное использование устройств, фишинг, кардинг, легализация денежных средств, склонение к суицидам и др.).

Таким образом, преступления, совершаемые с использованием информационных технологий, часто являются многообъектными. Основной объект указанных преступлений — общественные отношения, обеспечивающие безопасность в сфере компьютерной информации, предусмотренные главой 28 УК РФ. В качестве дополнительного объекта могут выступать охраняемые законом общественные отношения, предусмотренные другими главами УК РФ. Свойством каждого из объектов посягательства в преступлениях с использованием информационных технологий выступает самостоятельная уголовно-правовая охрана общественных отношений, на которые такое посягательство осуществляется, их разнородность, взаимосвязь с другими элементами состава преступления.

Отсутствие комплексного подхода к анализу преступности в цифровой среде приводит к тому, что уголовно-правовое противодействие указанным явлениям бессистемно, имеет запаздывающий характер, страдает дублированием норм или их «разбросанностью» по отдельным главам и разделам УК РФ. Практически не дается оценка криминогенным рискам и угрозам вследствие цифровизации общественных отношений: цифровое неравенство; увеличение безработицы вследствие автоматизации производства; уязвимость общества при повсеместном проникновении компьютерных технологий; агрессивная идентификация (религиозная, национальная, культурная), осуществляемая в том числе посредством сети Интернет; трудность государственного управления и контроля в условиях вовлечения огромного количества лиц в активную жизнь общества; многомерность и многосторонность конфликтов; увеличение влияния малых негосударственных групп.

Низким остается уровень раскрываемости преступлений в сфере информационных технологий — на протяжении последних пяти лет он не превышает среднего показателя в 27%. Таким образом, в Российской Федерации фактически раскрывается лишь

каждое четвертое преступление, связанное с использованием информационно-телекоммуникационных технологий, при кратном увеличении числа этих зарегистрированных преступлений.

Обобщение подходов, изложенных в многочисленных актах, в том числе международных, позволяет разделить криминальные угрозы информационной безопасности на три основных блока:

а) «оцифровка» традиционных видов преступлений при помощи информационных технологий (хищения, терроризм, оборот наркотиков, торговля людьми, порнография и т.д.);

б) воздействие собственно на компьютерную информацию (блокировка, модификация, удаление и др.);

в) воздействие на информационную инфраструктуру (критическую инфраструктуру).

Охрана информационных отношений осуществляется посредством конструирования соответствующих составов преступлений. Информационные отношения при этом являются дополнительным, а не основным непосредственным объектом преступлений в информационно-коммуникационном пространстве (за исключением преступлений в сфере компьютерной информации), их целесообразно классифицировать исходя из содержания основного непосредственного объекта. С данной позиции можно выделить группу преступлений, где использование информационных технологий является способом или средством совершения «традиционных» общественно опасных деяний, а также группу преступлений, посягающих на отношения в сфере компьютерной информации и критической инфраструктуры.

В рамках первой группы можно выделить самостоятельные преступления в зависимости от непосредственного объекта:

- против личности (п. «д» ч. 2 ст. 110, п. «д» ч. 3 ст. 110.1, ч. 2 ст. 110.2, ч. 2 ст. 128.2, п. «б» ч. 3 ст. 133 УК РФ);
- против конституционных прав и свобод человека и гражданина (ч. 3 ст. 137, ч. 3 ст. 141 УК РФ);
- против несовершеннолетних (п. «в» ч. 2 ст. 151.2 УК РФ);
- против собственности (п. «г» ч. 3 ст. 158, ст. 159.6 УК РФ);
- преступления в сфере экономической деятельности (ч. 2 ст. 170.1, 171.1, 183, 185.3, 187 УК РФ);
- против общественной безопасности (ч. 2 ст. 205.2, ст. 207.1, 207.2, 207.2 УК РФ);

- против здоровья населения и общественной нравственности (п. «б» ч. 2 ст. 228.1, ч. 1.1 ст. 238.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1, п. «г» ч. 2 ст. 242.2, п. «г» ч. 2 ст. 245 УК РФ);
- против основ конституционного строя и безопасности государства (ч. 2 ст. 280, ч. 2 ст. 280.1, ч. 2 ст. 280.4, ч. 2 ст. 281, ст. 282 УК РФ).

Указанную группу преступлений объединяет то, что они совершаются с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет. В настоящее время правоприменительная практика может опираться на разъяснения Пленума Верховного Суда РФ, снявшие наиболее сложные вопросы терминологического характера[1].

В частности, под информационно-телекоммуникационной сетью в соответствующих статьях Особенной части Уголовного кодекса Российской Федерации предлагается понимать технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. При этом следует иметь в виду, что сеть Интернет является одним из их видов.

Для признания наличия в действиях подсудимого признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики. Таковыми могут признаваться, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен

[1] См.: *Постановление* Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть Интернет» // СПС «КонсультантПлюс».

информацией (передачу сообщений) между компьютерными устройствами (п. 17).

Под сайтом в сети Интернет понимается совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты. Страница сайта в сети Интернет (далее — интернет-страница) — часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети Интернет (п. 18).

Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления (например, при публичных призывах к осуществлению экстремистской деятельности — территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого лица, или использовалось компьютерное устройство для размещения в сети Интернет информации, содержащей призывы к осуществлению экстремистской деятельности).

Доступ к электронным или информационно-телекоммуникационным сетям, в том числе сети Интернет, может осуществляться с различных компьютерных устройств, технологически предназначенных для этого, с использованием программ, имеющих разнообразные функции (браузеров, программ, предназначенных для обмена сообщениями, — мессенджеров, специальных приложений социальных сетей, онлайн-игр, других программ и приложений). При квалификации действий лиц как совершенных с использованием данных сетей необходимо установить, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

Применительно к отдельным преступлениям из обозначенной нами группы необходимо привести обоснования их принятия в УК РФ. Приведем некоторые примеры[1]. Так, Федеральным зако-

[1] См. об этом подробно: *Голованова Н.А., Гравина А.А.,. Зайцев О.А* и др. Уголовно-юрисдикционная деятельность в условиях цифровизации: Монография / М.: ИЗиСП, КОНТРАКТ, 2019; *Дьяконова М.О., Ефремов А.А., Зайцев О.А.* и др. Цифровая экономика: актуальные направления правового регулирования: Науч.-практ. пособие / Под ред. И.И. Кучерова, С.А. Синицына. М.: ИЗиСП: Норма, 2022.

ном от 7 июня 2017 г. № 120-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия в деятельности, направленной на побуждение детей к суицидальному поведению»[1] закреплены меры по предотвращению широкого распространения в сети Интернет негативной информации, побуждающей к совершению самоубийств или к иной деструктивной деятельности, самоубийств среди детей и подростков, по борьбе с разными формами содействия суицидам и вовлечения несовершеннолетних в совершение противоправных действий, заведомо для виновного представляющих опасность для их жизни.

Законом введены новые составы преступлений, направленные на противодействие таким общественно опасным деяниям. Так, ст. 110.1 УК РФ предусматривается ответственность за «склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства» (ч. 1) и за «содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению или обещанием скрыть средства или орудия совершения самоубийства» (ч. 2).

В ч. 1 ст. 110.2 УК РФ установлена ответственность за «организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства». В данном случае речь идет об установлении уголовной ответственности для «администраторов «групп смерти»» и иных неформальных сообществ, деятельность которых связана с побуждением несовершеннолетних к совершению самоубийства.

Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[2] ч. 3 ст. 158 УК РФ была дополнена п. «г», в котором определена ответственность за кражу, совершенную с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного ст. 159.3 УК РФ).

---

[1] См.: *СЗ* РФ. 2017. № 24. Ст. 3489.
[2] См.: *СЗ* РФ. 2018. № 18. Ст. 2581.

Расширение сферы применения информационных технологий в финансовом секторе привело не только к развитию электронных услуг и более широкому предоставлению клиентам банков удаленного доступа к их счетам для совершения платежей и переводов, но и к возникновению угроз криминального характера. Значительный рост хищений со счетов клиентов банков определяется относительной простотой их осуществления посредством методов социальной инженерии, для использования которых, как правило, не требуется специальных знаний и технических средств.

Отличительной чертой преступлений, совершаемых данными методами, является то, что многие граждане, попадая под влияние преступников, подтверждают правомерность совершения операций по их счетам даже в случаях, когда служба банка, осуществляющая мониторинг входящей и исходящей информации на предмет обнаружения мошеннических действий, определяет таковые как подозрительные. Потерпевшими от подобных посягательств, как правило, являются незащищенные слои населения.

Кроме того, методы социальной инженерии также активно используют хакеры, атакующие клиентов с помощью вирусного и вредоносного программного обеспечения, позволяющего получить удаленный доступ к их компьютеру. Для получения разовых паролей, приходящих на телефон клиента, они имитируют сбой в работе его автоматизированного рабочего места, а затем звонят от имени технической поддержки банка и просят сообщать пароли якобы для отмены ошибочных платежей.

Высокая степень общественной опасности указанных противоправных деяний подтверждается спецификой преступлений, совершить которые могут лишь лица, обладающие специальными знаниями и использующие технические средства, что приводит к нарушению не только права собственности, но и банковской тайны. Причинение существенного вреда очевидно при повсеместном применении безналичных расчетов, влекущем снижение наличных сбережений.

Изменение закона обосновывалось тем, что нередко совершению преступления предшествует длительная подготовительная стадия, включающая отдельные деяния, которые самостоятельно могут не образовывать состава преступления. Согласно действующим уголовным нормам, ответственность за приготовление к преступлению наступает только при совершении тяжких и особо

тяжких преступлений. Реализация предложения позволила в целях предупреждения и предотвращения преступлений использовать весь арсенал оперативно-розыскных мероприятий.

Процессы цифровизации общества обусловили появление новых форм террористической и экстремистской деятельности. Так, Федеральным законом от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»[1] ч. 2 ст. 205.2 УК РФ (Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма) дополнена указанием на публичные призывы к террористической деятельности, публичное оправдание терроризма или пропаганду терроризма, совершенные с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет. Аналогичный квалифицирующий признак введен Федеральным законом от 28 июня 2014 г. № 179-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [2] в ст. 280 и 282 УК РФ.

Федеральным законом от 21 июля 2014 г. № 274-ФЗ «О внесении изменений в статью 280.1 Уголовного кодекса Российской Федерации»[3] в ч. 2 ст. 280.1 УК РФ закреплена ответственность за публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, совершенные с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет). В связи с этим пробелом выглядит отсутствие этого признака в ч. 3 ст. 212 УК РФ, которой предусмотрена ответственность за призывы к массовым беспорядкам, а равно призывы к насилию над гражданами.

На противодействие распространению наркотиков в сети Интернет были направлены изменения, предусмотренные Федеральным законом от 1 марта 2012 г. № 18-ФЗ «О внесении изменений

[1] См.: *СЗ* РФ. 2016. № 28. Ст. 4559.
[2] См.: *СЗ* РФ. 2014. № 26 (ч. I). Ст. 3385.
[3] См.: *СЗ* РФ. 2014. № 30 (ч. I). Ст. 4275.

в отдельные законодательные акты Российской Федерации»[1]. В частности, в п. «б» ч. 2 ст. 228.1 УК РФ (Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества) была установлена ответственность за сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

Федеральным законом от 1 апреля 2020 г. № 100-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации»[2] УК РФ был дополнен новыми составами преступлений о публичном распространении заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан (ст. 207.1), и заведомо ложной общественно значимой информации, повлекшей тяжкие последствия (ст. 207.2).

Таким образом, проникновение информационных технологий в различные сферы жизнедеятельности общества сопровождается изменениями уголовного законодательства: устанавливается ответственность за совершение «традиционных» преступлений с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (квалифицированные составы преступления).

Применительно к группе преступлений, посягающих на отношения в сфере компьютерной информации и критической инфраструктуры, можно отметить следующие проблемные аспекты.

Объект охраны, предусмотренный гл. 28 УК РФ, в литературе имеет дискуссионный характер. Так, Л.А. Букалерова указывала на то, что оформляются преступления в сфере охраняемого государством официального информационного оборота и говорила об информационных преступлениях. Она также указывала, что информация может быть предметом или способом преступления[3].

---

[1] См.: *СЗ* РФ. 2012. № 10. Ст. 1166.

[2] См.: *СЗ* РФ. 2020. № 14 (ч. I). Ст. 2030.

[3] См.: *Букалерова Л.А.* Необходимо формулирование новой главы УК РФ «Информационные преступления» // Уголовное право: стратегия развития в XXI в. Материалы 5-й Междунар. науч.-практ. конф. М., 2008. С. 401—403.

М.В. Талан справедливо указывала, что ни в одном составе преступлений не предусмотрено признака с «использованием компьютерных технологий», поэтому термин «компьютерные преступления» должен использоваться лишь в криминалистике и криминологии[1].

И.А. Юрченко предложила несколько понятий в данной сфере:

1) преступления против безопасности информации — посягательства, связанные с преднамеренным воздействием на такие свойства информации, как ее доступность, целостность и конфиденциальность;

2) преступления против информационной безопасности — общественно опасные деяния, основным или дополнительным объектом которых является информационная безопасность в объективном и субъективном (психологическом) аспектах;

3) преступления информационной направленности — деяния, основным или дополнительным объектом направленности которых выступает информационная безопасность, либо предметом является информация, либо способ носит информационный характер, либо в качестве средства используются информационно-телекоммуникационные технологии[2].

Действительно, в предложении данного автора имеется рациональная основа: используется терминология Доктрины информационной безопасности РФ, корректно определяются объекты посягательства; происходит унификация криминологического подхода к преступности с выделением определенных сфер и статистических показателей. Однако упускается из вида и такая составляющая информационной безопасности, как программно-аппаратные и технические компоненты информационной сети, иными словами — техническая часть информационной инфраструктуры.

Таким образом, гл. 28 УК РФ содержит две группы преступлений: преступления против безопасности информации и преступления против безопасности информационной инфраструктуры

---

[1] См.: *Талан М.В.* Компьютерные преступления и преступления в сфере компьютерной информации // Уголовное право: стратегия развития в XXI в. Материалы 7-й Междунар. науч.-практ. конф.. М., 2010. С. 43—434.

[2] См.: *Юрченко И.А.* Преступления против безопасности информации, преступления против информационной безопасности, преступления информационной направленности: определение понятий // Уголовное право: стратегия развития в XXI в.: Материалы XIV Междунар. науч.-практ. конф. М., 2017. С. 477—484.

(средств хранения, обработки или передачи охраняемой компьютерной информации; информационно-телекоммуникационных сетей и оконечного оборудования).

Предмет преступлений против компьютерной информации. УК РФ в качестве предмета компьютерных преступлений понимает охраняемую законом информацию.

В примечании 1 к ст. 272 УК РФ информация определяется через физическую сущность ее представления — электрический сигнал, однако в настоящее время электрический сигнал является не единственным способом представления информации. Более того, применяя исключительно указанный способ передачи, невозможно построить ни одну информационную систему.

Так, самым надежным и обладающим наибольшей пропускной способностью является представление (передача) информации посредством оптического сигнала. Оптические сигналы применяется в магистральных каналах передачи данных, обеспечивающих связи стран и континентов. Широкое распространение имеет представление (передача) данных посредством радиосигнала.

Все это требует пересмотра существующей терминологии УК РФ в целях адекватного парирования существующих угроз в сфере компьютерной информации. В частности, понятие компьютерной информации может быть изъято из текста УК РФ либо устранено указание на электрический сигнал предоставления информации. Применительно к неправомерному доступу следует отказаться от указания на необходимость преодоления специальных средств защиты для доступа к компьютерной информации.

Общим для всех преступлений в сфере компьютерной информации является причинение вреда в виде наступления определенных последствий. Оценка характера и объема причиняемого вреда и круг объектов, которым причиняется такой ущерб от компьютерных преступлений, пожалуй, одна из самых сложных задач на текущем этапе. Некоторые наработки методического характера уже предлагаются в специальной зарубежной литературе[1].

Цифровая инфраструктура является социально-технической системой, и поэтому вовлеченные в них люди и их интересы так-

[1] См.: *Agrafiotis I., Nurse J., Goldsmith M., Creese S., Upton D.* A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate // Journal of Cybersecurity. Vol. 4. Iss. 1. 2018.

же выступают объектами атак. Полагаем, что можно выделить следующие виды вреда в результате кибератак (табл. 2.1).

Таблица 2.1. **Обобщенная модель вреда, причиняемого в результате совершения преступления в сфере информационной безопасности**

Вид вреда (ущерба)	*Конкретизация вреда (ущерба)*
Физический вред	*Применительно к личности:* 1) причинение вреда здоровью человека; 2) смерть человека; 3) хищение персональных данных. *Применительно к организации:* 1) повреждение или недоступность актива; 2) уничтожение актива; 3) хищение актива; 4) компрометация актива; 5) заражение актива; 6) снижение производительности актива
Психологический (моральный) вред Репутационный вред	*Применительно к организации:* 1) дезорганизация деятельности; 2) отрицательные изменения в восприятии окружающими (клиентами, поставщиками, СМИ, заказчиками, кредиторами и т.д.); 3) сокращение деловых возможностей; 4) неспособность набрать желаемый персонал и потеря персонала; 5) утрата или приостановление аккредитации или сертификации; 6) снижение кредитного рейтинга
Экономический вред	*Применительно к организации:* 1) нарушение операций; 2) срыв продаж или уменьшение оборота; 3) сокращение клиентов; 4) снижение прибыли; 5) снижение роста; 6) сокращение инвестиций; 7) падение цены акций; 8) потеря финансов или капитала; 9) расходы, которые организация должна была заплатить в качестве компенсации тем, кто пострадал в результате инцидента

Окончание табл. 2.1

Вид вреда (ущерба)	*Конкретизация вреда (ущерба)*
Социальный вред, т.е. вред, который может привести к последствиям в обществе (государстве) в целом	*Применительно к государственным и общественным интересам:* 1) воздействие на критическую инфраструктуру; 2) хищение сведений, составляющих государственную тайну; 3) публикация недостоверной социально значимой информации на веб-ресурсах организации, которая может привести к социальной напряженности, панике среди населения и т.п.; 4) нарушение работоспособности систем и сетей органов государственной власти, предприятий оборонно-промышленного комплекса; 5) нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонент или к техногенным авариям

Представленный перечень видов причиняемого вреда является примерным. Таким же абстрактным способом описываются угрозы в методических рекомендациях ФСТЭК России: к негативным последствиям от реализации угроз безопасности относятся событие или группа событий, наступление которых в результате успешной реализации угроз безопасности может привести к нарушению законодательства Российской Федерации и (или) социальному, экономическому (финансовому), политическому, технологическому, экологическому ущербу, ущербу в области обеспечения обороны страны, безопасности государства и правопорядка, ущербу репутации или иным негативным последствиям. Однако данный перечень может быть заложен в качестве ориентира для определения места уголовно-правовой нормы в системе Особенной части УК РФ.

В УК РФ последствия сформулированы как уничтожение, блокирование, модификация и копирование информации. Поста-

новление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 дает следующие понятия:

- *уничтожение компьютерной информации* — приведение такой информации полностью или в части в непригодное для использования состояние в целях утраты возможности ее восстановления независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;
- *блокирование компьютерной информации* — воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);
- *модификация компьютерной информации* — внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;
- *копирование компьютерной информации* — перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т.п.);
- *нейтрализация средств защиты компьютерной информации* — воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например осуществляющие мониторинг работы антивирусных программ) в целях утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты (п. 4).

Одной из серьезных проблем в применения ст. 272 и 273 УК РФ является сам факт формулирования закрытого перечня последствий. Видов вредоносных последствий существенно больше, а с развитием технологий они будут изменяться и дополняться. Приведем несколько известных примеров опасных последствий, появляющихся при воздействии на компьютерную информацию.

1. *Снижение скорости предоставления доступа к данным.* Злоумышленники создают большое количество задач для вычислительной системы, имитирующих формально корректные обращения, что приводит снижению скорости корректных запросов на предоставление доступа к информации и повлечет, например:

- в коммерческих организациях — замедление доступа к каталогу товаров интернет-магазина, приводящее к оттоку покупателей и причинению финансового ущерба;
- в лечебных учреждениях, оказывающих помощь посредством систем телемедицины при проведении операций, связанных с хирургическим вмешательством в режиме удаленного подключения к труднодоступным местам (судна дальнего плавания, лес и пр.), а также при проведении удаленного оперативного консилиума в режиме реального времени — снижение скорости доступа к информации, которое может привести к причинению вреда здоровью и жизни человека.

2. *Снижение скорости обработки данных* — это создание условий, ограничивающих скорость доступа к данным, которые могут приводить к потере актуальности получаемой информации. Такого рода воздействие может заключаться в запуске конкурирующих за ресурс процессов или, например, намеренном применении неэффективных алгоритмов, связанных с обработкой больших объемов данных. Так, в коммерческих организациях выводы, сделанные на основании неактуальной информации, могут приводить к финансовому ущербу; в логистических компаниях в случае применения вычислительных систем для управления транспортными средствами снижение скорости обработки данных может приводить к авариям, нанесению вреда здоровью и жизни человека.

3. *Дополнение (внесение) информации.* Посредством дополнения базы данных ложными сведениями можно исказить смысл

всей базы данных. Например, дополняя информацию о росте продаж ложной информацией об эффективности определенного канала продаж, злоумышленник может получить личную выгоду и нанести ущерб организации за счет нерационального использования маркетингового бюджета, сформированного на основании искаженной аналитики.

4. *Нейтрализация средств защиты* — косвенный способ воздействия на информацию. Такое воздействие создает повышение рисков информационной безопасности, что, с точки зрения специалистов информационной безопасности, имеет криминальный характер. На практике это воздействие практически всегда является сопутствующим для большинства компьютерных преступлений. Нейтрализация средств защиты является распространенной целью несанкционированного доступа.

Близким к этому последствием является нейтрализация средств контроля эффективности защиты информации. Влияние на режим обработки информации, которое также создает риски информационной безопасности, является по характеру криминальным и на текущий момент не может быть квалифицировано по статьям гл. 28 УК РФ.

5. *Перехват информации* — неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов (ГОСТ Р 53114-2008). Не является копированием, поскольку злоумышленник сам информацию не копирует, но информацию получает. Является одним из самых распространенных видов компьютерных преступлений.

6. *Нарушение достоверности информации.* Достоверность — это строгая принадлежность информации субъекту, который является ее источником, либо тому субъекту, от которого она принята. В случае если получатель начнет принимать информацию из недостоверного источника, он может быть введен в заблуждение и выполнить действия, к которым его побуждает злоумышленник. Например, перевести денежные средства по полученным недостоверным реквизитам.

7. *Снижение доверия к информации* — это изменение, снижение ожиданий получателей результата обработки информации к достоверности получаемого результата. К получателям результата относятся как стороны информационного обмена, так и поль-

зователи информационных систем, имеющих непосредственный доступ к данным.

Снижение доверия может быть осуществлено:

- за счет предоставления ошибочной информации (этот способ реализуют посредством подмены доверенного источника информации на источник информации, контролируемый злоумышленником, и дальнейшей выдачи измененных данных);
- путем появления регулярных и (или) трудно определяемых ошибок, вызванных технологическими сбоями, что также снижает доверие к информации и вычислительной системе вне зависимости от причин сбоев;
- посредством внесения данных, изменяющих смысл информации, что приводит к ошибочным выводам и обесцениванию результата.

Несмотря на отсутствие формального понимания снижения доверия к информации, отсутствие ожиданий достоверного результата может привести к отказу от ее использования. Снижение доверия к таким службам, как удостоверяющий центр сертификатов электронной подписи, может привести к полному закрытию организации и крупному финансовому ущербу.

Сложные вопросы возникают применительно к определению деяния в виде неправомерного доступа. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 дает следующее понятие: *неправомерным доступом к компьютерной информации* является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа) (п. 5).

Более общее понятие — доступ к информации — введено Федеральным законом от 27 июля 2006 г. 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1]

[1] См.: *Федеральный* закон от 27.07.2006 № 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 20.03.2021) // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

и определяется как возможность получения информации и ее использования.

Под данным деянием понимается тот или иной способ проникновения в информацию с использованием интеллектуальных средств или технических ресурсов компьютера, что позволяет совершать с компьютерной информацией какие-либо действия[1]. В случае если у лица отсутствует право на доступ к компьютерной информации или лицо, обладающее таким правом, нарушает правила защиты информации и установленный порядок воздействия на информацию, то такое воздействие на компьютерную информацию будет считаться неправомерным. Неправомерный доступ к компьютерной информации − незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации[2]. Иногда выделяется дополнительный признак неправомерного доступа — *защищенность информации*, т.е. доступ к незащищенной и открытой информации не будет являться уголовно наказуемым[3].

Неправомерный доступ к информации представляет собой действия преступника, который, используя компьютер, получает возможность воздействовать на хранящуюся на машинных носителях информацию посредством определенных команд, соответствующих той операционной среде, которая предназначена для работы с информацией в конкретном устройстве. Часто компьютерная информация защищена от несанкционированного доступа различными средствами идентификации (пароли, считывание отпечатков пальцев, идентификация пользователя по радужной оболочке глаза и т.п.). В таком случае доступ может произойти, только если защита преодолена. После получения доступа к информации появляется возможность ознакомиться с нею. Само по себе ознакомление, даже если впоследствии виновный сможет воспроизвести полученную информацию в точном соответствии

---

[1] См.: *Уголовное* право России. Части Общая и Особенная: Учебник для бакалавров / Под ред. А.И. Рарога. М., 2018. С. 426.

[2] См.: *Методические* рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]. Режим доступа: https://genproc.gov.ru/documents/nauka/execution /document-104550 (дата обращения: 23.04.2021).

[3] См.: *Тропина Т.Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. ... канд. юрид. наук. Владивосток, 2005. С. 186.

с оригиналом на ином машинном носителе, не образует преступления, предусмотренного ст. 272 УК РФ.

Основные термины, используемые в этой области информационной безопасности:

а) *права доступа* — совокупность возможностей и ограничений на использование информации;

б) *управление доступом* — предотвращение несанкционированного использования какого-либо ресурса, включая предотвращение пользования ресурса неполномочным образом.

Права доступа определяют порядок и условия доступа субъекта к объектам информационной системы (информации, ее носителям, процессам и другим ресурсам), установленные нормативными документами или собственником, владельцем информации. Права доступа определяют набор действий (чтение, запись, выполнение и др.), разрешенных для выполнения субъектам (например, пользователям системы) над объектами данных.

Так, для использования информации, составляющей коммерческую тайну, некоторые сотрудники компании имеют возможность чтения информации, другие могут информацию редактировать и изменять, третья группа обладает полномочиями информацию удалять. Полномочия могут быть ограничены: по видам доступа (чтение, изменение, удаление, дополнение, выполнение); по времени доступа; по территориальным зонам, в которых должен находиться субъект, получающий доступ и другими существенными для владельца информации факторами.

Таким образом, с точки зрения информационной безопасности нарушением будет являться не сам факт доступа к информации, а ее использование, выходящее за рамки предоставленных полномочий — прав доступа. Данный подход продиктован одним из базовых положений в организации защиты данных — не предоставлять избыточных прав для исполнения функций пользователя. Следует также отметить, что вредоносное воздействие на информацию не всегда является следствием именно несанкционированного доступа.

1. *Отказ в обслуживании,* т.е. предотвращение или прерывание авторизованного доступа к ресурсу системы или задержка в действиях или функциях системы. В системах промышленной автоматики и контроля отказ в обслуживании может относиться

к прекращению функционирования процесса, а не только к прекращению передачи данных[1].

Атаки на отказ в обслуживании заключаются в следующем: сетевые ресурсы, такие как веб-серверы, имеют ограничения по количеству запросов, которые они могут обслуживать одновременно. Помимо допустимой нагрузки на сервер, существуют также ограничения пропускной способности канала, который соединяет сервер с Интернетом. Когда количество запросов со стороны злоумышленника превышает производительность любого компонента инфраструктуры, может произойти: а) существенное замедление время ответа на запросы; б) отказ в обслуживании всех запросов пользователей или части из них.

Для осуществления этой атаки получение неправомерного доступа не является необходимым. Ущерб, наносимый атакой, зависит от атакуемого ресурса и функций, исполняемых ресурсом.

2. *Передача ложной информации:* злоумышленник, передавая ложную информацию от имени доверенного контрагента, может ввести в заблуждение и вынудить перечислить денежные средства на свой счет, получить конфиденциальную информацию в ответ (в данном случае доступ является целью, а не условием преступных действий).

3. *Атака посредника, или атака «человек посередине»,* — кибератака, при которой злоумышленник тайно ретранслирует и в некоторых случаях изменяет данные обмена между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Одним из примеров атаки MITM является подслушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передает сообщения между ними, чтобы заставить их поверить, что они разговаривают непосредственно друг с другом по приватному каналу связи, когда на самом деле весь разговор контролируется злоумышленником. Злоумышленник должен уметь перехватывать все соответствующие сообщения, передаваемые между двумя жертвами, и вводить новые

[1] См.: *ГОСТ* Р 56205-2014. IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Ч. 1-1: Терминология, концептуальные положения и модели [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200114169 (дата обращения: 17.04.2021).

(в данном случае получение доступа к передаваемой информации является целью преступных действий, а не признаком).

4. *Веб-инжект* — технология, позволяющая изменить содержимое веб-страницы на стороне клиента (в браузере) и добавить в него своей контент через внедрение вредоносного кода в адресное пространство браузеров и перехват всех HTTP-запросов и ответов от сервера. Таким способом злоумышленник, не получая доступа, добивается исполнения нужных ему действий на стороне атакуемого ресурса.

5. *Физическое воздействие на информацию.* Вредоносное влияние на информацию посредством физического воздействия на каналы и носители информации не требует получения доступа к данным в установленном нами смысле. Например, гарантированное уничтожение данных с использованием программного обеспечения представляет собой управляемый физический процесс изменения электромагнитными волнами состояния физического носителя информации.

К вредоносным действиям в отношении информации посредством физического воздействия на информационную систему или ее элементы, имеющие целью уничтожить, блокировать, модифицировать информацию относятся:

- физическая порча носителей информации, т.е. приведение в негодность флеш-карт, накопителей на жестких магнитных дисках, систем хранения данных и пр.;
- физическая порча средств и каналов обмена с целью блокировать доступ к данным, например разрыв кабеля, оптики;
- радиочастотное навязывание, т.е. искажение электромагнитного поля с целью заблокировать обмен данных по беспроводным каналам, таким как Wi-Fi, Bluetooth;
- силовое электромагнитное воздействие на информацию — воздействие, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования их технических и программных средств.

Таким образом, использование в УК РФ ссылок на частные технологические решения, реализующие тот или иной процесс,

имеет риски оставить без оценки широкий спектр противоправных деяний в цифровой среде. Данный подход рискует описывать только существующие на определенный момент технологии, что, наблюдая динамику современного технологического развития, не выглядит предусмотрительным.

2.2. Проблемы соучастия и стадий в преступлениях, совершенных с использованием информационных технологий

Я.Н. Ермолович[1], *В.А. Перов*[2]

Преступления, совершаемые группой лиц, т.е. двумя и более лицами, как правило, обладают большей степенью общественной опасности, чем преступления, совершаемые единолично, так как объединение усилий группы для достижения преступного результата облегчает совершение действий, образующих объективную сторону преступления. Данное утверждение в полной мере относится к совершению преступлений с использованием информационных технологий, так как такие преступления совершаются, как правило, группой лиц по предварительному сговору, в которой участвуют лица, заранее договорившиеся о совместном совершении преступления, либо организованной группой, т.е. устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений с использованием информационных технологий. Наличие у лица специальных знаний в IT-сфере позволяет использовать информационные технологии в преступных целях с максимальной для себя и остальных соучастников степенью анонимности. И хотя различные виды информационных технологий достаточно распространены во всем мире, количество специалистов, имеющих специальные знания о принципах их работы, что позволяет использовать такие технологии с определенной степенью анонимности, довольно ограниченно. Большинство

[1] Ярослав Николаевич Ермолович — профессор кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.

[2] Валерий Александрович Перов — профессор кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации.

лиц осуществляют работу с высокотехнологичными устройствами на уровне пользователей, при этом либо вообще не имеют представления об информационной безопасности, либо их знания носят разрозненный характер и не позволяют противостоять потенциальным угрозам. Поэтому спрос на людей, которые обладают определенной профессиональной квалификацией в работе с информационными технологиями, неуклонно растет. Наличие таких знаний предоставляет им как возможность противостоять преступным посягательствам, так и возможность совершения преступлений с использованием вышеуказанных технологий. Востребованность таких специалистов возрастает также в криминальных кругах, так как позволяет совершать преступления с высоким уровнем латентности.

На территории Российской Федерации такие случаи фиксировались неоднократно.

Так, по приговору Шпаковского районного суда Ставропольского края от 09.02.2022 г. по уголовному делу № 1-467/2021 по обвинению N в совершении преступления, предусмотренного ч. 3 ст. 30, п. «г» ч. 4 ст. 228^1 УК РФ установлено следующее.

N в интернет-магазине Crise, расположенном на интернет-платформе, действуя умышленно, из корыстных побуждений, путем переписки вступил в предварительный преступный сговор с неустановленным лицом в целях незаконного сбыта неопределенному кругу лиц наркотического средства «масло каннабиса (гашишное масло)» в крупном размере с использованием сети Интернет, бесконтактным способом путем размещения вышеуказанного наркотического средства в тайниках — «закладках» на территории Ставропольского края.

Во исполнение общего преступного умысла N и неустановленное лицо распределили между собой преступные роли, согласно которым роль неустановленного лица заключалась в приобретении наркотического средства «масло каннабиса (гашишное масло)» в целях последующего незаконного сбыта неопределенному кругу лиц с использованием сети Интернет путем размещения оптовых тайников — «закладок» с указанным наркотическим средством и передачи через интернет-мессенджер сведений о точных местах их нахождения, поиске покупателей наркотического средства и предоставлении им через интернет-магазин Crise сведений о точных местах нахождения произведенных тайников — «закладок» с наркотическим

средством, а также в распределении в определенных долях полученных от продажи наркотиков денежных средств между собой.
Реализуя единый преступный умысел, действуя умышленно, из корыстных побуждений, группой лиц по предварительному сговору, в нарушение порядка деятельности, связанной с оборотом наркотических средств, вопреки требованиям Федерального закона от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах», совершили умышленные действия, непосредственно направленные на незаконный сбыт наркотического средства, с использованием сети Интернет, в крупном размере[1].

Данный пример показывает наличие в составе организованных преступных групп исполнителей, обладающих специальными знаниями. Такие лица не только непосредственно выполняют объективную сторону преступлений с использованием информационных технологий, но и предпринимают меры к сокрытию следов совершенного преступления.

При таких обстоятельствах для вменения квалифицирующего признака «организованная группа» необходимо наличие устойчивости группы и общность целей. Действия всех участников организованной группы вне зависимости от роли, ими выполняемой, следует квалифицировать как действия исполнителей преступлений, в совершении или подготовке которых они участвовали. Необходимо отметить, что часть объективной стороны преступлений с использованием информационных технологий выполняется в так называемой виртуальной среде лицами, имеющими специальные знания в области IT-технологий. Использование специальных знаний позволяет им игнорировать установленные Законом ограничения доступа к информации, а также совершать иные преступления в виртуальном пространстве. При этом другие участники организованной группы могут лишь оказывать содействие совершению указанных преступлений, предоставляя необходимое для совершения преступлений компьютерное оборудование, ин-

[1] *Приговор* Шпаковского районного суда Ставропольского края от 09.02.2022 г. по уголовному делу № 1-467/2021. Судебные и нормативные акты РФ. URL: https://sudact.ru/regular/doc/MLht2ESs1yrT/?regular-txt=%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=&regular-judge=&_=1679055547689 (дата обращения: 17.03.2023).

формацию о лицах, в отношений которых должно быть совершено преступление, а также устраняя препятствия к совершению преступления, например, путем оказания физического воздействия на потерпевшего в целях получения соответствующих электронных ключей, паролей, логинов.

Действия организатора таких групп следует квалифицировать как исполнительские в отношении всех преступлений, совершенных группой, при условии, что они охватывались его умыслом на момент создания группы, вне зависимости от того, принимали ли они непосредственное участие в совершении или подготовке того или иного конкретного преступления[1]. Организаторы групп, осуществляя общее руководство и планирование преступных действий, могут выполнять часть объективной стороны преступления, а могут и не принимать непосредственного участия в выполнении объективной стороны преступлений, совершаемых посредством использования информационных технологий. При этом они пользуются результатами преступной деятельности, в том числе денежными средствами, полученными в результате совершения таких преступлений. В том и другом случае их действия необходимо рассматривать как соисполнительство.

Характерной особенностью преступлений, совершаемых организованными преступными группами с использованием информационных технологий, является наличие в составе таких групп лиц, обладающих специальными знаниями в IT-сфере, которые позволяют совершать преступления с максимальной степенью анонимности. Несмотря на то что информационные технологии получают все большее распространение в мире, количество специалистов, имеющих углубленные знания о работе с ними, крайне ограничено. Участие в составе организованной преступной группы таких специалистов дает группе в целом возможность совершения преступлений с высоким уровнем латентности. Такие специалисты не только непосредственно выполняют объективную сторону преступлений с использованием информационных технологий, но и предпринимают меры к сокрытию так называемых виртуальных (цифровых, электронных, т.е. существующих в виртуальном пространстве) следов совершенного преступления. По

[1] См.: *Украинчик А.В.* Понятие и признаки исполнителя преступления // Гуманитарные, социально-экономические и общественные науки. 2020. № 9. С. 164.

сути, руководители организованных преступных групп используют для совершения преступлений специалистов в сфере IT-технологий, отводят им роль технических специалистов, выполняющих объективную сторону (полностью или в части) указанных преступлений в виртуальном пространстве, т.е. непосредственных исполнителей.

Характерными преступлениями, совершаемыми организованными группами с использованием информационных технологий, являются преступления с разновидностями цифровых валют, в том числе с криптовалютами различного вида.

Аналитический отчет компании Chainalysis «Криптопреступность 2021»[1] свидетельствует, что большая часть отправленных с криминальных криптокошельков средств попадает на депозитные кошельки крупных криптобирж, рискованных сервисов, т.е. бирж с высокой степенью риска. К таковым могут относиться биржи с неточными или несуществующими программами комплексной системы мер по осуществлению безопасности криптовалютных транзакций, построенной с учетом требований действующего национального законодательства, а также криптомиксеры, т.е. специальные сервисы анонимизации, усложняющие отслеживание криптовалютных транзакций в соответствующей блокчейн-сети. Такие сервисы используют технологию, позволяющую раздробить средства клиента на мелкие части, после чего смешивают их в случайном порядке с частями средств других клиентов. В результате указанных операций к конечному получателю приходит заданное количество криптовалюты, но разными транзакциями от разных случайно выбранных адресов из общего принадлежащего такому сервису пула. Часть таких кошельков-получателей контролируется членами организованной преступной группы, другая же часть принадлежит сторонним сервисам. Такие сервисы предоставляют преступникам услуги по отмыванию денег, полученных в результате совершения преступления. Аналогичные сервисы осуществляют свою деятельность на территории Российской Федерации. Возможность использования больших объемов цифровой валюты, которые вложенные сервисы могут через себя

[1] См.: *Chainalysis.* Криптопреступность 2021. Системы информационной безопасности. URL: https://is-systems.org/blog_article/11617368536 (дата обращения: 20.03.2023).

провести, позволяет говорить, что часть из них целенаправленно создается в целях содействия в совершении преступлений с цифровой валютой. Такой способ совершения преступлений используется в том числе крупными компаниями, для которых незаконная деятельность составляет лишь небольшую долю от общего объема сделок, что, в свою очередь, позволяет предположить, что нелегальные средства попадают в законный оборот. Таким образом, объемы хищений цифровой валюты позволяют говорить о наличии соответствующих компаний, которые оказывают услуги по отмыванию средств, полученных в результате совершения преступлений.

Из указанного аналитического отчета можно сделать вывод, что в данном случае имеет место организованная преступная группа со строгим распределением ролей. Имеется организатор, который планирует преступления с использованием криптовалюты и осуществляющий контроль за деятельностью остальных участников группы. Имеются исполнители, непосредственно осуществляющие действия в зависимости от ранее определенной им роли, и имеются пособники из числа лиц, обладающих специальными знаниями использования информационных технологий и осуществляющих соответствующую техническую и консультативную поддержку преступной деятельности. Часть членов такой группы могут не знать друг друга в лицо, взаимодействуя с помощью сети Интернет или так называемых даркнет-сетей, осуществляя свою деятельность для достижения общего преступного результата. При этом постоянное поддержание связей внутри группы может свидетельствовать о ее устойчивости, сплоченности и наличии общих целей. Как следует из представленного аналитического отчета, такие связи между членами группы могут иметь не только устойчивый характер, но и обладать определенной иерархичностью, что в случаях использования вышеуказанного преступного способа крупными компаниями позволяет говорить о наличии преступного сообщества (преступной организации), т.е. совершении преступления, предусмотренного ст. 210 УК РФ. Такое преступное сообщество будет обладать более сложной многоступенчатой внутренней структурой (иерархией), позволяющей совершать тяжкие и особо тяжкие преступления. К таковым можно отнести мошенничество, совершенное организованной группой либо в особо крупном размере с последующей

легализацией полученных от преступной деятельности денежных средств.

В зависимости от конкретной ситуации существует возможность объединения двух или более организованных групп с аналогичной целью в преступное сообщество. Можно резюмировать, что при совершении группой лиц преступления с использованием информационных технологий в такой группе, как правило, присутствует технический специалист. Целью таких преступлений зачастую является имущественная выгода, однако может быть также уничтожение, блокирование, модификация, копирование компьютерной информации. Такие преступления совершаются с использованием информационных технологий в виртуальном пространстве посредством использования компьютерного (сетевого) оборудования, предоставляющего лицу соответствующие возможности работы в сети Интернет или сетях Даркнета.

В литературе неоднозначно решается вопрос о квалификации действий лиц, использующих для связи между собой электронную почту и мессенджеры. Одни ученые предлагают квалифицировать такие действия как преступления, совершаемые с использованием информационных технологий. Сторонники второго подхода полагают более узкую трактовку понятия преступлений с использованием информационных технологий, исходя из того, что информационные технологии должны выступать в качестве средства совершения преступления или предмета преступления.

Видится, что, рассматривая данный вопрос, необходимо исходить из следующего. Если способ совершения преступления как часть объективной стороны предусматривает использование информационных технологий как средства преступления, то такое преступление должно относиться к преступлениям с использованием информационных технологий. В том случае, если информационные технологии выступают предметом преступления, такое преступление также можно отнести к указанной категории. Конечно, данная точка зрения хотя и является субъективной, но, по сути, отражает реалии сегодняшнего дня.

Можно представить следующий перечень преступлений с использованием информационных технологий, совершаемых в соучастии:

1) хищения (кража, мошенничество), совершенные посредством информационных технологий. В качестве примера можно

привести так называемый фишинг (англ. phishing) — разновидность интернет-мошенничества, используемого для получения путем обмана паролей, номеров карт, банковских счетов и другой конфиденциальной информации, позволяющей осуществить хищение принадлежащих пользователю денежных средств;

2) вымогательство с использованием информационных технологий. Так называемые атаки с использованием вредоносных программ, при которых на компьютер пользователя, помимо его воли, устанавливается вредоносное программное обеспечение, блокирующее его работу одновременно с требованием выплаты денежных средств за его деблокирование;

3) нарушение неприкосновенности частной жизни, т.е. незаконное собирание или распространение с помощью информационных технологий сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия;

4) создание, использование и распространение вредоносных компьютерных программ;

5) легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления, либо легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем.

В ряде случаев при квалификации преступлений, совершаемых с использованием цифровой валюты, не всегда правильно определяется роль, выполняемая каждым из лиц при совместном совершении таких преступлений. Так, использование вредоносных программ, которые позволяют осуществлять копирование данных клиентов криптобирж с последующим выдвижением требований о передаче имущества (криптомонет) под угрозой блокирования криптокошельков, квалифицируется по ст. 273 УК РФ. При такой квалификации не учитывается, что целью лица, такие действия совершающего, является совершение более тяжкого преступления, предусмотренного ст. 163 УК РФ, т.е. вымогательства. Такое вымогательство осуществляется под угрозой невозможности пользоваться своим имуществом (криптовалютой). Тем не менее правоприменительная практика идет по другому пути. Полагая, что угроза уничтожения компьютерных программ или компьютерной информации не является признаком состава преступления, предусмотренного ст. 163 УК РФ, а принадлежащая

потерпевшему криптовалюта не может быть уничтожена в силу технологических особенностей ее функционирования, такое преступление квалифицируется по ст. 273 УК РФ. Если же наряду с вышеуказанными действиями в адрес потерпевшего поступали угрозы применения к нему насилия, то действия всех участников такой группы необходимо квалифицировать по совокупности преступлений, предусмотренных ст. 163, 273 УК РФ, вне зависимости от того, от кого конкретно из членов преступной группы такие угрозы исходили. Соответственно можно говорить о множественности преступлений, совершаемых группой лиц ради достижения ранее обусловленной преступной цели. В зависимости от роли каждого члена такой группы в совершении указанных преступлений должен быть определен его вид соучастия.

От соучастия в деятельности таких преступных групп необходимо отличать эксцесс исполнителя, которым признается совершение исполнителем преступления, не охватывающегося умыслом других соучастников. В соответствии со ст. 36 УК РФ за эксцесс исполнителя, т.е. совершения преступления, которое не охватывалось умыслом других участником группы, остальные соучастники преступления уголовной ответственности не подлежат. Теория уголовного права предусматривает общую трактовку такого понятия, как «охват умыслом», вследствие чего разные ученые формулируют свое определение указанного понятия. Так, А.И. Рарог связывает эксцесс исполнителя с осознанием соучастником нового преступления[1]. А.П. Козлов полагает, что следует устанавливать характер и объем соглашения и определять отношение соучастников к различным элементам преступления[2]. А.А. Пионтковский полагал, что эксцесс — это совершение преступления, которое не охватывалось предвидением конкретного соучастника[3]. По сути, все вышеуказанные определения не противоречат, а, скорее, дополняют друг друга, не вступая при этом в противоречие со ст. 36 УК РФ, вследствие чего могут использоваться в правоприменительной деятельности при квалификации преступлений, совершенных с использованием информационных технологий.

---

[1] См.: *Рарог А.И.* Квалификация преступлений по субъективным признакам. СПб., 2003. С. 231.

[2] См.: *Козлов А.П.* Соучастие. Традиции и реальность. СПб., 2001. С. 329.

[3] См.: *Курс* советского уголовного права: В 6 т. Т. II. М., 1970. С. 484.

При эксцессе исполнитель может выйти за рамки согласованного преступного посягательства, совершив однородное с задуманным преступление. Так, после завладения паролем от электронного или криптокошелька один из участников группы по собственной инициативе, в целях сокрытия совершенного преступления осуществляет убийство потерпевшего, о чем остальные члены группы не были осведомлены заранее и их умыслом совершение данного преступления не охватывалось. Остальные члены преступной группы ответственности за данное преступление нести не могут.

При квалификации таких действий соучастника, которые включают в себя признаки подстрекателя и организатора, необходимо иметь в виду, что основное отличие организатора от подстрекателя заключается в том, что последний не планирует совершения преступления и не руководит подготовкой преступления или его совершением. Подстрекатель в совершении преступления может подать идею о завладении чужими криптомонетами в целях последующего материального обогащения, но при этом не заниматься разработкой плана совершения преступления, оставляя себе роль «технического консультанта» или соучаствуя в выполнении объективной стороны в виртуальной среде.

Если же при этом лицо не только склонило другое лицо к совершению преступления, но впоследствии выполнило и организационные действия, то такие действия соучастника следует оценивать только как организационные, поскольку по своей сути они являются более опасными, чем подстрекательские. Организация преступления включает в себя действия, направленные на склонение другого лица к совершению преступления, равно как и создание организованной группы или преступного сообщества (преступной организации), а также руководство ими.

При квалификации соучастия в преступлении с использованием такой разновидности цифровой валюты, как криптовалюта, необходимо в каждом конкретном случае устанавливать не только объективные, но и субъективные признаки преступления. И хотя соблюдение данного правила относится к процессу квалификации любого преступления, тем не менее стоит отметить, что его несоблюдение приводит к ошибкам квалификации.

В частности, следует помнить, что соучастие в преступлении с субъективной стороны характеризуется умышленной виной со-

участников. Данная форма психической деятельности соучастников проявляется в их отношении ко всем признакам состава преступления, в том числе и квалифицирующим. Квалифицирующие признаки состава преступления могут вменяться соучастникам только при условии установления у них умысла в отношении этих признаков. Так, совершение насильственных действий, образующих объективную сторону соответствующих преступлений и направленных на противоправное получение от собственника (владельца) криптокошелька соответствующего пароля, не могут вменяться лицу, не участвующему в их совершении совместно с другими лицами — членами преступной группы.

Под приисканием соучастников преступления необходимо понимать предложение лица другим лицом, хотя бы одному, совместно совершить преступление в качестве соисполнителя, исполнителя или пособника, приведшее к согласию на это предложение. Такое предложение не обязательно должно быть сделано вербальным способом. Для этого могут быть использованы электронная почта, мессенджеры, определенные сайты даркнет-сетей. Так, в даркнет-сети «Тор» можно найти сайты с объявлениями, предлагающими предоставить свои банковские счета для обналичивания денежных средств, приобретенных другими лицами преступным путем, за определенный процент от обналичиваемой суммы. Такие лица выполняют роль организатора преступления или подстрекателя к преступлению. Моментом окончания приискания соучастников следует признавать момент дачи согласия хотя бы одним соучастником на совершение преступления. Приискание соучастников отличается от покушения на преступление и от оконченного преступления тем, что лица, давшие согласие на совершение преступления, не выполняют ни полностью, ни частично действий или бездействия, описанных в диспозиции соответствующей статьи Особенной части УК РФ.

Аналогичным образом в даркнет-сетях может быть осуществлен сговор на совершение преступления, т.е. на взаимное, обоюдное соглашение двух или более лиц, при котором каждое из них изъявляет желание совместно совершить преступление. В данном случае заранее не выделяется организатор преступления или подстрекатель к преступлению, а роли соучастников распределяются в процессе сговора, который также осуществляется посредством даркнет-сетей. Оконченным сговор на совершение

преступления является с момента дачи обоюдного согласия и изъявления взаимного желания совместно совершить преступление. Отличие сговора на совершение преступления от покушения на преступление и от оконченного преступления состоит в том, что участники сговора не совершают ни полностью, ни частично действий или бездействия, описанных в диспозиции статьи Особенной части УК РФ, устанавливающей ответственность за преступление, о совместном совершении которого состоялся сговор.

Иное создание условий для совершения преступления представляет собой оценочный признак, который может выражаться, например, в устранении препятствий, могущих помешать совершению преступления, например «взлом» электронной почты потерпевшего в целях получения данных его банковского счета. Иное создание условий следует признавать оконченным с момента завершения такого создания. Иное создание условий для совершения преступления отличается от покушения на преступления и от оконченного преступления тем, что указанное создание не является ни полностью, ни частично действиями или бездействием, описанными в диспозиции статьи особенной части УК РФ.

Приготовление к преступлению имеется тогда, когда развитие преступной деятельности завершилось на данной стадии по обстоятельствам, не зависящим от виновного. Например, виновный не смог найти соответствующее орудие совершения преступления в виде компьютерной программы, позволяющей ему осуществить «взлом» электронной почты потерпевшего. Если такое приготовление к преступлению переросло в покушение на преступление, попытка «взлома» все же была осуществлена или оконченное преступление, то оно поглощается последними, и содеянное квалифицируется как покушение на преступление либо оконченное преступление.

Приискание средств или орудий совершения преступления как завершенный процесс (результат) — это их приобретение любым способом, в частности путем покупки, получения во временное пользование, хищения. Вышесказанное полностью относится к совершению преступлений с использованием информационных технологий. Компьютерную программу, используемую как орудие «взлома», необходимо либо создать, либо приобрести. Моментом окончания приискания является момент приобретения средств или орудий совершения преступления, т.е. момент, с ко-

торого лицо обладает реальной возможностью в данном случае пользоваться и распоряжаться такими программами. Приискание отличается от покушения на преступление и от оконченного преступления тем, что приобретенные средства и орудия не используются на последующих названных стадиях совершения преступления. Например, приобретенное для совершения преступления компьютерное оборудование и (или) соответствующее программное обеспечение не используется для совершения преступления, как ранее планировалось. Другой вариант предполагает использование такого оборудования и программного обеспечения для совершения преступления, однако такое преступление не доводится до его завершения в силу отсутствия или недостаточности знаний у лица, использующего компьютерное оборудование (программное обеспечение), т.е. по обстоятельствам, не зависящим от воли лица, совершающего преступление.

Таким образом, в целях правильной квалификации отдельных преступлений, совершенных с использованием информационных технологий, необходимо отграничить, во-первых, покушение от оконченного преступления, во-вторых, покушение — от приготовления к совершению преступления. Решение данной задачи имеет практическое значение, так как законодатель определил возможность смягчения наказания за неоконченное преступление. При совершении преступлений с использованием информационных технологий правильно разграничить приготовление к совершению преступления от покушения на преступление бывает довольно проблематично. Так, на протяжении последних нескольких лет среди определенной категории IT-специалистов, так называемых хакеров (от англ. hack, т.е. тип компьютерных специалистов, добывающих конфиденциальную информацию в обход систем защиты компьютерной системы), получил широкое распространение метод несанкционированного доступа («взлома») путем брутфорс-атаки. Брутфорс (анг. bruteforce) — это метод несанкционированного входа в защищенную компьютерную систему пользователя, при котором тестировщик (хакер) подбирает данные для входа путем перебора соответствующих символов. Во время такого «взлома» системы компьютерная программа за короткое время вводит в систему множество комбинаций паролей на случай, если одна из комбинаций окажется верной. Такой метод используется для «взлома» электронной почты, электронных ко-

шельков, криптокошельков, аккаунтов пользователей и других защищенных систем. Цель «взлома» — получение информации, составляющей охраняемую законом тайну, и последующее за этим хищение денежных средств или цифровой валюты.

Методы брутфорс-атаки могут быть различными, но всегда для начала такой атаки нужна предварительная подготовка, т.е., по сути, имеет место приготовление к совершению преступления. Такое приготовление будет заключаться в подборе соответствующей компьютерной брутфорс-программы, подборе и загрузке соответствующих словарей для последующего их использования. Если планируется осуществление атаки на электронную почту пользователя, может понадобиться база адресов (e-mail), никнеймов (псевдоним, которым пользуется пользователь в сети Интернет или сетях Даркнета), номеров телефонов. Осуществляя брутфорс-атаку, программа вводит большое количество комбинаций, которые могут оказаться паролями, и пытается авторизоваться. В зависимости от сложности задачи могут потребоваться мощности, превышающие мощность персонального компьютера (ПК). В этом случае будет использован соответствующий компьютерный пул (объединение мощностей отдельных ПК) либо сервер. В случае если попытки подбора пароля завершаются успехом, авторизация успешно завершается, и хакер получает доступ к защищенной системе (аккаунту пользователя). Подготовка к использованию соответствующего компьютерного оборудования также будет отнесена к стадии приготовления к совершению преступления, так как происходит приискание средств и орудий совершения преступления.

Необходимо учитывать, что приготовление, как и покушение на совершение преступления, — неоконченная преступная деятельность, совершаемая только с прямым умыслом. То есть не любое приготовление к брутфорс-атаке может быть рассмотрено как приготовление к совершению преступления. Если такая атака на систему происходит с согласия или по просьбе пользователя, например когда пользователь забыл пароль и не может его восстановить, вышеуказанные действия не могут являться приготовлением к совершению преступления, а сама атака — покушением на преступление.

2.3. Отдельные виды преступлений, совершаемых с использованием информационных технологий

Я.Н. Ермолович[1], *В.А. Перов*[2]

Учитывая, что с помощью информационных технологий осуществляются поиск, сбор, хранение, обработка и передача информации практически во всех сферах деятельности человека, включая сферу финансов, которая является основой любой экономической системы, совершение преступлений в указанной сфере может затрагивать права и законные интересы неопределенного круга лиц. Именно финансовая сфера сегодня активно использует информационные технологии, позволяющие осуществлять финансовые операции с цифровой валютой, распространение и использование которой получают все более широкое распространение в мире по причине удобства ее использования, быстроты производимых транзакций, отсутствия в определенных случаях административных барьеров.

За такого рода деятельностью стоят иногда противозаконные финансовые операции и запрещенные законом сделки криминального характера. Более того, цифровые валюты сами становятся предметом преступного посягательства. В соответствии со статистическими данными в Российской Федерации имеют место такие преступления, как вымогательство, убийства, совершенные из корыстных побуждений, целью которых является завладение цифровой валютой. Также цифровая валюта используется для финансирования экстремистских и террористических организаций, дачи и получения взяток, торговли оружием, наркотическими и сильнодействующими средствами, которые запрещены или ограничены в гражданском обороте. Таким образом, цифровые валюты могут выступать либо как предмет преступления, либо как средство совершения преступления, а в определенных случа-

[1] Ярослав Николаевич Ермолович — профессор кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент

[2] Валерий Александрович Перов — профессор кафедры уголовного права и криминологии Московской академии Следственного комитета Российской Федерации

ях используясь фактически как платежное средство. Например, разновидность цифровых валют — криптовалюта может являться предметом таких преступлений как: кража (ст. 158 УК РФ); мошенничество (ст. 159 УК РФ); присвоение или растрата (ст. 160 УК РФ); грабеж (ст. 161 УК РФ); разбой (ст. 162 УК РФ); вымогательство (ст. 163 УК РФ); легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ); легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1 УК РФ); приобретение или сбыт имущества, заведомо добытого преступным путем (ст. 175 УК РФ). Криптовалюта выступает в виде имущественных прав или средства совершения преступлений, предусмотренных главой 30 УК РФ (Преступления против государственной власти, интересов государственной службы и службы в органах местного самоуправления), а также в преступлениях, совершаемых по найму.

Все разновидности цифровой валюты включают в себя свойства и признаки, присущие традиционным валютам в виде монет или банкнот. В частности, они могут быть использованы для приобретения товаров, оплаты работ либо услуг, но также могут ограниченно применяться определенными сообществами для расчетов только между его членами. Они могут иметь централизованного эмитента, а могут быть децентрализованы, как, например, криптовалюта.

Квалификация и расследование таких преступлений осложняются тем, что ряд проблем относительно правового режима определенных видов цифровой валюты в Российской Федерации до настоящего времени фактически не разрешен, хотя такие попытки предпринимались неоднократно. Так, п. 3 ст. 1 Федерального закона от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» дает следующее определение понятия «цифровая валюта»: «совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющего-

ся денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам» (п. 3 ст. 1).

Исходя из указанного определения, можно провести следующую классификацию цифровых валют:

1) фиатные электронные деньги на базе сетей (network-based).

Электронные деньги работают на основе программной системы, представленной в виде программы либо сетевого ресурса. Такого рода системы использует шифрование данных и электронную цифровую подпись.

Применяются для оплаты товаров, приобретаемых через интернет-магазины, а также в онлайн-играх. К таковым можно отнести: WebMoney, «Яндекс.Деньги», RUpay, E-gold, E-port, PayCash, MoneyMail, CyberPlat, Rapida, QIWI, Деньги@Mail.Ru и им подобные;

2) фиатные электронные деньги на базе смарт-карт, т.е. многоцелевых пластиковых карт со встроенным микропроцессором (чипом).

Клиенты банков переводят деньги со своих счетов на смарт-карты, операции по которым производятся в пределах зачисленных на такие карты денежных средств. Режим ведения лицевого счета смарт-карты отличается от режима ведения лицевого счета традиционных карт. Обычная дебетовая банковская карта не содержит информации о состоянии счета клиента банка, она лишь является инструментом доступа к данному счету. В момент зачисления банком денежных средств на такой счет на саму карту зачисления как такового не производится. В момент пополнения средств смарт-карты остаток на лицевом счете уменьшается на сумму, на которую было произведено пополнение карты. На самой карте появляется электронная наличность;

3) частные электронные деньги на базе сетей — криптовалюта.

Оборот криптовалюты осуществляется с помощью аппаратно-программного комплекса, включающего в себя набор технических и программных средств, работающих совместно для выполнения определенных задач. Такими задачами в данном случае являются создание (майнинг) и оборот в соответствующей блокчейн-сети криптовалюты определенного вида. При этом сами по себе понятия «компьютерная сеть» и «блокчейн-сеть» имеют определенные отличия.

Компьютерная сеть представляет собой систему, которая обеспечивает обмен данными между вычислительными устройствами — компьютерами, серверами, маршрутизаторами или другим оборудованием. Блокчейн-сеть представляет собой распределенную базу данных, т.е. такую базу данных, в которой данные хранятся на разных компьютерных устройствах, физически находящихся в различных местах.

«Любая распределенная система является программной системой, построенной на базе сети. Эта программная система обеспечивает высокую степень связности и прозрачности элементов. Таким образом, различие между компьютерной сетью и распределенной системой заключается в программном обеспечении (особенно в операционной системе), а не в аппаратном комплексе.

Тем не менее эти два понятия имеют очень много общего. Например, как компьютерная сеть, так и распределенная система занимаются перемещением файлов. Разница заключается в том, кто вызывает эти перемещения — система или пользователь»[1].

Следует также отметить, что хотя криптовалюты можно отнести к разряду цифровых валют, так как, конечно, в данном случае мы говорим об использовании так называемых цифровых технологий, но все-таки термин «цифровая валюта» охватывает более широкое понятие. Данным определением охватываются все цифровые, а не только блокчейн-технологии, используемые для безналичного денежного оборота.

Правовой режим криптовалюты в Российской Федерации в различные временные периоды кардинальным образом изменял-

[1] *Таненбаум Э., Уэзеролл Д.* Компьютерные сети. 5-е изд. СПб.: Питер, 2012. С. 32

ся, что, в свою очередь, влияло непосредственно на квалификацию преступлений, совершаемых с использованием криптовалюты, так как фактически с изменением правового статуса криптовалюты изменялся непосредственно предмет преступления.

Вступивший в силу с 1 января 2021 г. Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» предусматривает такое понятие, как «цифровая валюта».

В соответствии с п. 3 ст. 1 данного Закона под *цифровой валютой* понимается «некая совокупность электронных данных в виде цифрового кода либо обозначения, содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам».

Данная формулировка более точно определяет правовой режим криптовалюты в системе национального права как одну из разновидностей цифровой валюты. Таким образом, криптовалюта становится законодательно определенным объектом гражданского права и в качестве такового может быть указана в соответствующих уголовно-процессуальных документах, в том числе в качестве предмета преступного посягательства.

Также необходимо отметить, что некоторые страны разработали определения цифровых валют, изложенные в законодательных актах. В Евросоюзе к таким можно отнести Директиву Совета Европейских сообществ 2009/110/ЕС от 16 сентября 2009 г. об учреждении и деятельности организаций, эмитирующих элек-

тронные деньги, о пруденциальном надзоре за их деятельностью, представляющем собой системный процесс, при помощи которого контролирующий орган следит за соблюдением правил регулирования[1], а также об изменении Директив 2005/60/ЕС («О предотвращении использования финансовой системы для отмывания денежных средств и финансирования терроризма») и 2006/48/ЕС («О реализации прав на интеллектуальную собственность») и об отмене Директивы 2000/46/ЕС.

В Евросоюзе под понятиями «цифровая валюта» (электронные, цифровые деньги) понимают денежные обязательства эмитента, выраженные в электронном виде и находящиеся в распоряжении пользователя на электронном носителе.

Такие денежные обязательства должны быть зафиксированы на определенном электронном носителе, являющемся одновременно и их хранилищем. Они могут приниматься как платежное средство иными, помимо их непосредственного эмитента, лицами и выпускаться при получении эмитентом от иных лиц денежных средств в объеме, не меньшем их эмитированной стоимости.

Какой-либо единой принятой во всем мире классификации криптовалют также не существует. Никто точно не знает, сколько разновидностей криптовалют существует в мире. Связано это с тем, что не все существующие криптовалюты используются для осуществления расчетов и включены в листинг мировых криптобирж. Более того, листинг и делистинг криптовалют происходит постоянно, что, в общем-то, нормальное явление для фондового рынка, к которому отчасти можно отнести и рынок криптовалют. Большинство созданных криптовалют являются производными (так называемым форком) от программы наиболее сейчас известной и популярной криптовалюты — биткойна. При этом создатели таких программ не всегда ставят цель использовать криптовалюту как средство платежа, а создают ее исходя из иных соображений (профессиональная гордость, тщеславие и.т.п.).

---

[1] См.: *Кондаков О.В., Шепелев О.М.* Организационно-правовые основы осуществления пруденциального надзора кредитных организаций // Социально-экономические явления и процессы. 2015. Т. 10, № 10. С. 65.

По способу добычи (эмиссии) и функционирования можно разделить криптовалюты, функционирующие на основании двух алгоритмов:

- Proof of Work — доказательство выполнения работы, представляющий собой определенный алгоритм достижения консенсуса в сети блокчейн. Такой алгоритм используется сетью для подтверждения криптовалютных транзакций и создания новых блоков. При этом майнеры конкурируют друг с другом за завершение транзакций в сети и получение вознаграждения;
- Proof of Stake (доказательство доли владения) — формирование участником очередного блока в блокчейне пропорционально доле, которую составляют принадлежащие этому участнику расчетные единицы данной криптовалюты от их общего количества. То есть вместо решения криптографической задачи транзакции валидируются путем оставления в качестве обеспечения определенного количества монет майнеров.

Необходимо также сказать о так называемом стейблкоине, который некоторые считают разновидностью криптовалюты, другие же полагают, что это токены. С технической точки зрения стейблкоин — обеспеченный фиатными деньгами цифровой актив, обеспеченный долларами США. Сумма в долларах США, равная общему количеству стейблкоинов.

При росте или падении цены доллара США стоимость стейблкоинов также изменяется. Стейблкоин может быть как децентрализованным, так и централизованным, т.е. иметь определенного эмитента.

Как правило, для работы с большинством централизованных стейблкоинов необходимо зарегистрироваться у эмитента данной цифровой валюты под собственными паспортными данными, получить пароль для работы с соответствующим приложением. Все сведения о владельцах стейблкоинов и проведенных с их использованием операциях могут быть получены у эмитента по соответствующему запросу следователя.

Следует отметить, что преступления с использованием криптовалют совершаются, как правило, с участием лиц, обладающих специальными знаниями в IT-сфере.

Следователи Следственного комитета Российской Федерации столкнулись со следующими проблемами при расследовании преступлений, совершаемых с использованием криптовалюты:

1) проблематичное определение стоимости различного вида цифровой валюты, являвшейся предметом преступного посягательства;

2) сложности, связанные с наложение ареста на цифровую валюту, в целях обеспечения исполнения приговора в части гражданского иска, взыскания штрафа либо иных имущественных взысканий, а также возможной конфискации имущества в соответствии с требованиями Уголовно-процессуального кодекса Российской Федерации;

3) сложности в определении характера и размера вреда, причиненного потерпевшему совершенным преступлением.

Их наличие приводит к тому, что преступления с использованием цифровой валюты совершаются во многих случаях безнаказанно. Так, в Даркнете на протяжении нескольких лет существуют интернет-магазины по торговле наркотиками. Оплата за товар осуществляется одной из разновидностей цифровой валюты — криптовалютой, а передача наркотиков — путем закладок для покупателя в различных городах России в зависимости от пожеланий покупателя. Более того, такого рода магазины регулярно публикуют объявления о принятии на работу соответствующего персонала, непосредственно осуществляющего закладки наркотических средств. Именно они время от времени и привлекаются к уголовной ответственности, в то время как организаторы преступной деятельности остаются анонимными и продолжают ее заниматься.

В преступлениях, совершаемых с применением насилия, криптовалюта может выступать как в качестве фактического средства платежа при совершении таких преступлений по найму, так и являться непосредственно предметом преступного посягательства, например при разбое в целях завладения криптомонетами потерпевшего. Физическое насилие при этом чаще всего выступает в качестве средства совершения преступления.

Осуществляя квалификацию преступлений, совершаемых с использованием цифровой валюты, необходимо учитывать ее

свойства и порядок ее обращения, который основан на определенных принципах, заложенных их создателями.

Другой разновидностью преступлений с использованием информационных технологий является использование вредоносных компьютерных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации. Согласно примечанию 1 к ст. 272 УК РФ, под компьютерной информацией следует понимать любые сведения (сообщения, данные), которые представлены в виде электрических сигналов, вне зависимости от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин, а также в других компьютерных устройствах или на любых внешних электронных носителях: дисках различного вида, в том числе жестких дисках — накопителях, флеш-картах и других аналогичных устройствах в форме, доступной восприятию компьютерного устройства, либо передаваться по каналам электрической связи.

В свою очередь, к числу компьютерных устройств можно отнести любые электронные устройства, которые способны выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов, такие как персональные компьютеры (ноутбуки, планшеты, мобильные телефоны, смартфоны). К иным электронным устройствам можно отнести физические объекты, которые оснащены встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека.

Таким образом, к вредоносной программе можно отнести любую компьютерную программу, созданную в целях несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. К таковым можно отнести так называемые компьютерные вирусы, имеющие следующие разновидности:

1) «компьютерный (сетевой) червь» — вредоносная компьютерная программа, способная воспроизводить себя на компьютер-

ных устройствах либо через компьютерные сети. Она распространяется следующими способами:

- в виде файла, отправленного во вложении в электронном письме;
- в виде ссылки на интернет-ресурс;
- через пиринговые сети обмена данными P2P;

2) «трояны», или «троянские программы», — предназначены для несанкционированного удаления, блокировки, изменения, копирования данных компьютерного устройства или нарушения работы компьютеров и компьютерных сетей. Специалисты по способу действия выделяют следующие разновидности «троянских программ»: «бэкдоры», «эксплойты», «трояны, выполняющие DDoS-атаки», «трояны-вымогатели», «трояны-шпионы», «трояны — сборщики адресов электронной почты». Данный перечень не является исчерпывающим. Кроме того, некоторые виды таких программ могут быть комбинированы и одновременно выполнять несколько действий;

3) «руткиты» — компьютерные программы, предназначенные для предотвращения обнаружения пользователем других вредоносных программ;

4) «кейлоггеры» — определяют и запоминают все манипуляции с клавиатурой компьютера пользователя.

Вышеуказанная классификация является достаточно условной, так как вредоносные компьютерные программы могут быть комбинированными и выполнять одновременно несколько функций.

Преступления, совершаемые с использованием вредоносных компьютерных программ, подпадают под действие ст. 273 УК РФ, так как такие программы несанкционированно устанавливаются на компьютерное оборудование пользователя, что влечет наступление общественно опасных последствий, предусмотренных диспозицией указанной нормы, в виде уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Объектом преступления являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Объективная сторона преступления предусматривает совершение следующих альтернативных действий:

1) создание вредоносных компьютерных программ, которые заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты;

2) распространение вредоносных компьютерных программ или машинных носителей с такими программами;

3) использование вредоносных компьютерных программ или машинных носителей с ними.

Субъект преступления общий — вменяемое лицо, достигшее 16 лет.

Субъективная сторона состава преступления характеризуется виной в виде прямого умысла. Виновный должен осознавать, что компьютерные программы, им создаваемые или используемые, заведомо приведут к указанным в диспозиции ст. 273 УК РФ общественно опасным последствиям. Мотив и цель в данном случае не будут влиять на квалификацию преступления. Однако в том случае, если целью использования вредоносных компьютерных программ будет являться передача чужого имущества или права на имущество либо совершение иных действий имущественного характера под угрозой повреждения чужого имущества — компьютерного оборудования пользователя, будет иметь место совокупность преступлений, предусмотренных ст. 273, 163 УК РФ. Примером идеальной совокупности указанных преступлений может служить использование одной из разновидностей вредоносной компьютерной «троянской» программы так называемого вируса-шифровальщика. Данная программа, устанавливаясь на компьютерные устройства, осуществляет шифрование наиболее ценных для пользователя файлов — личных документов, фото, видео и других файлов компьютера (компьютерного устройства) — таким образом, что их нельзя использовать. Одновременно выдвигаются требования о перечислении денежных средств за разблокирование указанных файлов и возможность продолжать использовать компьютерное оборудование. Такие вирусы бывают двух типов: непосредственно шифровальщики (крипторы — англ. cryptoransomware), осуществляющие шифрование файлов, и бло-

кировщики (блокеры — англ. blockers), осуществляющие блокировку работы компьютера. Зачастую заявляются требования о выплате выкупа за разблокирование компьютера или дешифровку файлов в криптовалюте, что значительно повышает уровень латентности таких преступлений. Использование в целях вымогательства «вирусов-шифровальщиков» зафиксировано во многих странах мира, в том числе и в Российской Федерации.

Согласно проведенному компанией Chainalysis аналитическому исследованию «Криптопреступность 2021», использование при совершении вымогательства вируса-шифровальщика составляет значительную долю среди общего количества преступлений, совершенных в мире с использованием криптовалюты[1]. При этом такое преступление, как мошенничество, лидирует среди указанных преступлений в мире. Доля таких преступлений составляет 54%. Общая сумма ущерба от их совершения составляет примерно 2,6 млрд долл. США. Далее идут криминальные сделки, совершаемые на рынках Даркнета. Ущерб от таких преступлений, исчисляется в 1,7 млрд долл. США. На третьем месте по количеству совершенных преступлений находятся преступления, совершенные с использованием так называемого вируса-шифровальщика. Сумма денежных средств, полученная вымогателями, использовавшими данный вирус, составляет порядка 350 млн долл. США. При этом имеется значительный общемировой рост таких преступлений (на 311%) по сравнению с 2019 г. Ни одна другая категория преступлений с использованием цифровой валюты не показала такого роста в 2020 г.[2]

Кроме непосредственного ущерба, причиненного потерпевшим в результате совершения вымогательств с использованием вируса-шифровальщика, необходимо отметить, что атаки на компьютерное оборудование пользователей являются достаточно опасными как для отдельных пользователей, так и для государственных (муниципальных) организаций. Использование вышеуказанной вредоносной компьютерной программы может привести к

[1] См.: *Chainalysis.* Криптопреступность 2021. Системы информационной безопасности.
[2] Там же.

невозможности осуществления деятельности крупных государственных (правительственных) организаций.

Chainalysis отмечает, что «нападениям подвергаются в том числе и учреждения сферы здравоохранения, и это в разгар пандемии»[1]. Соответственно при подсчете ущерба от подобного вида деятельности необходимо учитывать упущенную выгоду (общий экономический ущерб) предприятий, организаций не только от выплаты выкупа вымогателям, но и от остановки работы предприятий, государственных и муниципальных органов. Некоторые эксперты оценивают общий ущерб от использования в 2020 г. вируса-шифровальщика в 20 млрд долл. США[2].

Среди стран, чьи организации вошли в число жертв вымогателей, использующих вирус-шифровальщик, в тройку наиболее пострадавших от такой деятельности вошли: США (47% организаций), Канада (12%), Германия (8%)[3].

Согласно данным, представленным лабораторией компьютерной криминалистики и исследованиями вредоносного кода Group-IB, в 2021 г. количество атак вируса-шифровальщика с последующим вымогательством разновидности цифровой валюты, криптовалюты на российские организации увеличилось более чем на 200%[4]. Эти данные согласуются с данными аналитического исследования Chainalysis «Криптопреступность 2021»[5], показывающей общий объем криптовалют, которые были получены преступниками в результате использования вируса-шифровальщика в мире за период 2016—2022 гг. Учитывая, что представленные выше данные отражают количественные показатели совершения преступлений с использованием информационных технологий, сумма ущерба, причиненного в результате совершения таких преступлений, приведена в долларах США.

---

[1] См.: *Chainalysis.* Криптопреступность 2021

[2] Там же.

[3] Там же.

[4] См.: *Как* операторы и программы вымогатели атаковали российский бизнес в 2021 году. Group-IB. URL: https://www.group-ib.ru/whitepapers/ransomware-in-russia- (дата обращения 15.03.2023).

[5] См.: *Chainalysis.* Криптопреступность 2021. Системы информационной безопасности.

Необходимо отметить не только тенденцию к росту вымогательств с использованием вирусов-шифровальщиков, но и низкую раскрываемость таких преступлений, что в совокупности приводит к увеличению суммы выкупа за разблокирование компьютерного устройства пользователя. Совокупность указанных факторов отражает комплекс социальных явлений (детерминант преступности), влияющих на увеличение количества данных преступлений. К таким детерминантам можно отнести: высокий уровень латентности указанных преступлений, связанный как с постоянным совершенствованием вредоносных программ, позволяющим обходить тот уровень противовирусной защиты, который установлен пользователем; высокий уровень анонимности в виртуальной сети лиц, совершающих преступления с использованием различного вида вредоносных компьютерных программ; сложности квалификации таких преступлений, связанной как с неоднозначной трактовкой действующего законодательства, так и с невозможностью определения всех квалифицирующих признаков указанных преступлений. Изложенная тенденция имеет общемировое значение и затрагивает интересы всех стран, где подобного рода преступления совершаются, в том числе и Российской Федерации. Вредоносные компьютерные программы могут блокировать как работу отдельной программы, используемой пользователем, так и работу операционной системы в целом.

В мире появляются все новые, в том числе комбинированные, разновидности вирусов-шифровальщиков. Так, например, компания Group-IB зафиксировала разновидность вируса-шифровальщика, способного, помимо шифрования файлов, генерировать (осуществлять майнинг) криптовалюту[1].

Необходимо отметить, что некоторые факультативные признаки объективной стороны преступлений, предусмотренные ст. 272—274 УК РФ, при конструкции уголовно-правовых норм не всегда отражают сущность технологических процессов. Одно и то же явление с точки зрения права и информатики будет прин-

[1] См.: *Group-IB* нашла вирус-шифровальщик, который научился майнить криптовалюту. РИА Новости. 24.06.2019. URL: https://ria.ru/20190624/1555846747.html (дата обращения 14.03.2023).

ципиально различным. То есть закон не в полной мере отражает суть технологических процессов, что, в свою очередь, приводит к определенным проблемам квалификации указанных преступлений. Так, в примечании 1 к ст. 272 УК РФ указано, что под компьютерной информацией понимаются сведения (сообщения, данные), которые представлены в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» также указано, что к информации относятся любые сведения (сообщения, данные) вне зависимости от формы их представления. Таким образом, законодателем ставиться знак равенства между понятиями «информация» и «данные». Между тем, исходя из положений информатики, следует, что понятия «данные» и «информация» применительно именно к компьютерным данным и компьютерной информации имеют существенные различия. Данные — это набор символов, воспринимаемых ЭВМ в соответствии с соответствующим протоколом передачи данных (набор определенных правил логического уровня, который определяет обмен данными между различными программами ЭВМ), в то время как информация — это обработанные ЭВМ данные, которые приобрели смысловое значение для человека. Таким образом, данные не зависят от информации, но информация зависит от данных, так как без получения данных ЭВМ не может предоставить человеку информацию.

В п. 5 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» законодатель определяет, что обладателем информации является лицо, которое самостоятельно создало такую информацию либо получило ее на основании закона либо договора. Из данной трактовки однозначно следует, что получателем, обладателем, создателем информации является человек, в то время как получателем и создателем данных может являться ЭВМ, т.е. неодушевленная вещь, которая в соответствии со ст. 19 УК РФ не может являться субъектом преступления. Между тем диспозиция всех статей главы 28 УК РФ запрещает совершение деяний, связанных с различными видами посягательств именно на компью-

терную информацию, не запрещая при этом посягательство на компьютерные данные по той причине, что закон определяет их как тождественные понятия.

Исходя из положений закона, любые несанкционированные пользователем компьютерного устройства модификации или копирование имеющихся на его компьютере данных должны рассматривается как модификация и копирование компьютерной информации, вследствие чего такое деяние будет квалифицировано по ст. 273 УК РФ. Так, владельцы сайтов, использующих так называемые файлы-«куки» (англ. cookie), т.е. файлы с информацией, полученной при посещении пользователем веб-ресурса, должны привлекаться к уголовной ответственности за совершение преступления, предусмотренного ст. 273 УК РФ, так как указанная информация или, если быть более точным, данные хранятся на жестком диске компьютера, изменяя путем дополнения, т.е. модернизируя, уже имеющиеся на компьютере пользователя данные.

Между тем файлы-«куки» призваны обеспечить пользователю удобство при работе с сайтами, т.е. их использование (распространение), формально образуя состав преступления, предусмотренного ст. 273 УК РФ, при этом это не представляет общественной опасности, так как не осуществляется посягательство на общественные отношения, обеспечивающие безопасность в сфере компьютерной информации. Фактически отсутствует объект преступления и соответственно состав преступления. В данном случае можно говорить о наличии правовой коллизии, не дающей возможности однозначно правильной квалификации преступлений, предусмотренных главой 28 УК РФ и подлежащей устранению на законодательном уровне.

Для устранения указанной коллизии можно использовать опыт Евросоюза, принявшего Директиву Европейского парламента и Совета Европейского Союза 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах свя-

зи)[1]. Статья 6 указанной Директивы предусматривает обработку данных трафика только лишь с согласия пользователя, что исключает возможность их модификации или копирования на компьютерном устройстве пользователя без его согласия. При этом пользователям предоставляется возможность отзыва такого согласия в любое время по его усмотрению. Внесение соответствующих изменений в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» позволит, в свою очередь, изложить диспозицию статей главы 28 УК РФ в иной редакции, позволяющей квалифицировать как преступление действия лиц, модифицирующих или копирующих данные компьютерного устройства пользователя без его согласия.

Таким образом, рассматривая информационные технологии как объект уголовно-правовой охраны, необходимо отметить, что обязательным условием такой охраны является не только своевременное выявление подобных преступлений, но и их правильная квалификация. Последнее невозможно без установления фактических обстоятельств совершенного преступления, в том числе способа его совершения как элемента объективной стороны, уяснения и правильного истолкования всех квалифицирующих признаков такого преступления.

Список литературы

1. *Абдулвалиев А.Ф., Белоусов А.В., Вассалатий Ж.В.* и др. Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования. Тюмень: Тюмен. гос. ун-т, 2021.
2. *Бегишев И.Р., Бикеев И.И.* Преступления в сфере обращения цифровой информации. Казань: Познание, 2020.

[1] См.: *Директива* Европейского парламента и Совета Европейского Союза 2002/58/ЕС от 12 июля 2002 г. в отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) // СПС «Гарант». URL: https://base.garant.ru/2570354/ (дата обращения: 15.03.2023).

3. *Голованова Н.А., Гравина А.А., Зайцев О.А*. и др. Уголовно-юрисдикционная деятельность в условиях цифровизации / Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации. М.: Юридическая фирма «Контракт», 2019.
4. *Козаев Н.Ш.* Современные проблемы уголовного права, обусловленные научно-техническим прогрессом. М.: Юрлитинформ, 2019.
5. *Козлов А.П.* Соучастие. Традиции и реальность. СПб., 2001.
6. *Перов В.А*. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: Учеб.-метод. пособие. М.: Юрлитинформ, 2017. (Сер. «Библиотека криминалиста»).
7. *Поппер И.* Цифровое золото. Невероятная история Биткойна, или Как идеалисты и бизнесмены изобретают деньги заново. М.: ООО «И.Д. Вильямс», 2016.
8. *Рарог А.И.* Квалификация преступлений по субъективным признакам. СПб., 2003.
9. *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения. 2-е изд. М.: Инфра-М, 2022.
10. *Фильченко А.П., Жандров В.Ю.* Противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Монография. М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2018.

Глава 3

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И УГОЛОВНОЕ СУДОПРОИЗВОДСТВО

3.1. Уголовно-процессуальные основы досудебного производства по уголовным делам о преступлениях, совершенных с использованием информационных технологий

Н.В. Османова[1]

Использование информационных и телекоммуникационных технологий при совершении преступлений обусловило потребность в обеспечении государственной защиты интересов граждан в информационной сфере[2] и разработке уголовно-процессуального инструментария, способствующего реализации назначения уголовного судопроизводства (ст. 6 УПК РФ).

Раскрытие, расследование и последующее рассмотрение по существу в суде уголовных дел, сопряженных с использованием информационных и телекоммуникационных технологий, коррелирует с пониманием происходящих в информационно-телекоммуникационной области процессов, в том числе противоправных явлений, и с умением их распознавать, облекать в процессуальную форму и использовать в доказывании в целях установления обстоятельств, предусмотренных ст. 73 УПК РФ.

---

[1] Надежда Валерьевна Османова — декан факультета подготовки научно-педагогических кадров и организации научно-исследовательской работы Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент.

[2] См.: *Стратегия* развития информационного общества в Российской Федерации на 2017—2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203 // Президент России: официальный сайт. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 13.03.2023).

Познавательная деятельность при этом лежит в основе принятия процессуальных решений и производства по уголовному делу и способна нивелировать возможные сложности при обнаружении, фиксации и изъятии информации в целях ее дальнейшего использования в качестве доказательств по уголовному делу.

С момента поступления сообщения о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, досудебное производство по уголовному делу приобретает следующие характерные черты:

- начало досудебного производства по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий, выражающееся в типичных поводах возбуждения уголовного дела и особенностями проведения проверки;
- уголовно-процессуальная специфика определения места совершения преступления и подследственности уголовных дел;
- особый предмет доказывания по уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий;
- специальная процедура изъятия электронных носителей информации и копирования с них информации;
- установление информации о соединениях между абонентами и (или) абонентскими устройствами, используемыми в целях совершения преступления;
- обязательное взаимодействие следователя с органами дознания, администрацией социальных сетей, мессенджеров и др.

Рассмотрим указанные особенности.

Преступления, совершенные с использованием информационных и телекоммуникационных технологий, о совершении которых становится известно правоохранительным органам посредством подачи лицом заявления, обладают высокой латентностью.

Ситуация осложняется тем, что факт совершения преступления ввиду его специального способа не всегда рассматривается пострадавшим как таковое. Дополнительным негативным фактором выступает неспособность лица объяснить, от каких именно действий и в какой момент в отношении него было совершено преступление.

Преступления о неправомерном доступе к компьютерной информации с использованием информационно-телекоммуникационных сетей (ст. 272 УК РФ), совершенные в отношении коммерческих предприятий (банков), являются особо латентными в связи с нежеланием предавать гласности сведения о похищении у них информации (а возможно, и денежных средств) путем взломов систем их защиты. Латентность указанных преступлений обусловлена репутацией соответствующих учреждений и заинтересованностью сохранения тайны утечки информации. Этим же обусловлено и сокрытие информации о фактах использования вредоносных компьютерных программ, повлекших блокирование, модификацию, копирование компьютерной информации (ст. 273 УК РФ).

Начало досудебного производства по сообщению о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий. Проведенное нами исследование позволяет сформулировать типичные поводы возбуждения уголовного дела о преступлении, совершенном с использованием современных информационных и телекоммуникационных технологий:

- заявление лица о том, что в отношении него совершено преступление, например: мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ); вымогательство, совершенное с использованием сети Интернет (ст. 163 УК РФ); нарушены его авторские права (ст. 146 УК РФ);
- заявление матери, отца, усыновителя, опекуна или попечителя (законного представителя) о том, что, например, совершена видеосъемка несовершеннолетнего в целях изготовления и распространения порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей (п. «г» ч. 2 ст. 242.2 УК РФ);
- рапорт об обнаружении признаков преступления, например, о незаконном сбыте наркотических средств, психотропных веществ или их аналогов, совершенном с использованием электронных или информационно-телекоммуникационных сетей (п. «б» ч. 2 ст. 228.1 УК РФ). Сеть Интернет может быть использована также для коммуникации с потенциальным покупателем, получения сведений об оплате и инфор-

мирования о месте нахождения наркотических средств[1]. Такие сведения в последующем (после их установления и анализа) становятся основанием для составления рапорта об обнаружении признаков преступления;

- постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании п. 4 ч. 1 ст. 140 УПК РФ. Такие материалы, как правило, формируются в ходе надзорного производства, а также по жалобам граждан.

Преступления, совершенные с использованием информационных и телекоммуникационных технологий, о совершении которых становится известно правоохранительным органам посредством подачи лицом заявления, обладают высокой латентностью. Особый способ совершения рассматриваемых преступлений позволяет скрыть или намеренно исказить идентификационные данные, что обусловливает достаточно редкую встречаемость в правоприменительной практике добровольного сообщения лица о совершенном им преступлении в соответствии с п. 2 ч. 1 ст. 140 УПК РФ (явка с повинной).

Основанием возбуждения уголовного дела о преступлении, совершенном с использованием информационных и телекоммуникационных технологий, является наличие достаточных данных, указывающих на объективные признаки преступления. Достаточность полученной информации об объекте и объективной стороне конкретного преступления определяется в каждом случае следователем по его усмотрению в зависимости от обстоятельств произошедшего, обосновывается в постановлении о возбуждении уголовного дела.

По преступлениям, совершенным с использованием информационных и телекоммуникационных технологий, важное значение имеет установление способа совершения преступления, доказывание которого на стадии возбуждения уголовного дела зачастую представляется затруднительным. Поэтому при получении в ходе проверки сообщения о преступлении сведений о невозможности установления специального способа совершения противоправно-

[1] См.: *Торговченков В.И., Иванов С.А.* Особенности предупреждения бесконтактных способов сбыта наркотических веществ в Российской Федерации // Законы России: опыт, анализ, практика. 2016. № 12. С. 84.

го уголовно наказуемого деяния с использованием сети Интернет и отсутствии обстоятельств, исключающих производство по уголовному делу, принимается решение о возбуждении уголовного дела по основному составу преступления.

Поскольку правовая конструкция квалифицированных или особо квалифицированных составов ряда преступлений содержит в себе указание на использование в преступных целях сети Интернет[1], возбуждение уголовного дела по признакам таких преступлений допускается только в случае наличия достоверной и достаточной информации о специальном способе совершения преступления. Вместе с тем категория достаточности данных либо доказательств всегда была и остается одной из самых дискуссионных как среди ученых-процессуалистов[2], так и в правоприменительной практике.

Так, по уголовному делу в отношении С., возбужденному по п. «б» ч. 4 ст. 132 УК РФ[3], между позициями следователя и прокурора возникли противоречия относительно достаточности данных, подтверждающих «специальный» способ преступления. Итогом конфронтации стали следующие друг за другом процессуальные решения: возбуждение уголовного дела следователем, отмена прокурором решения о начале уголовного преследования, далее — реализация следователем права на обжалование решения прокурора в порядке, предусмотренном п. 5 ч. 2 ст. 38, ч. 4 ст. 221 УПК РФ, и завершающая спор отмена вышестоящим прокурором необоснованного постановления нижестоящего прокурора об отмене постановления о возбуждении уголовного дела в соответствии с п. 6 ч. 2 ст. 37 УПК РФ. Предметом разногласий стала обязательность проведения в стадии возбуждения уголовного дела лингвистической экспертизы пере-

[1] См.: п. «д» ч. 2 ст. 110; п. «д» ч. 3 ст. 110.1; ч.2 ст. 110.2; п. «в» ч. 2 ст. 151.2; ч. 2 ст. 205.2; п. «б» ч. 2 ст. 228.1; п. «б» ч. 3 ст. 242; п. «г» ч. 2 ст. 242.1; п. «г» ст. 242.2; ч. 2 ст. 280; ч. 2 ст. 280.1 УК РФ и др.

[2] См.: *Барабаш А.С., Скоблик К.В.* Основание принятия решений в российском уголовном процессе: Монография. М., 2020; *Кочкина М.А.* Оценка достаточности доказательств на этапе окончания предварительного расследования по уголовному делу: Дис. ... канд. юрид. наук. М., 2015; *Профатилова Н.В.* Оценка следователем достаточности доказательств при принятии основных процессуальных решений по уголовным делам: Дис. … канд. юрид. наук. М., 2009; и др.

[3] См.: *Материалы* уголовного дела № 11702030006000041 // Архив следственного управления Следственного комитета Российской Федерации по Краснодарскому краю.

писки между подозреваемым С. и потерпевшим Б., полученной при осмотре компьютера потерпевшего. Следователь обжаловал его, указав в обоснование своей позиции, что наличие объяснения Б. и переписки между С. и Б. является достаточными для возбуждения уголовного дела, а отсутствие лингвистической экспертизы не препятствует принятию законного решения.

Таким образом, если в диспозиции статьи уголовного закона указан специальный способ «с использованием сети Интернет» или «информационно-телекоммуникационных технологий» (ст. 171.2, 272, 273, 274 УК РФ), возбуждение уголовного дела допускается только в случае наличия достоверной и достаточной информации об указанном в соответствующей норме способе совершения преступления. Достаточность при этом определяется следователем самостоятельно.

В случае отсутствия в диспозиции статьи указанного способа совершения преступления установление на этапе проверки сообщения о преступлении способа его совершения не является обязательным для принятия решения о возбуждении уголовного дела — достаточным может быть наличие иных данных о преступном деянии.

Следует также учитывать, что в настоящее время в целях установления оснований для принятия процессуального решения по сообщению о преступлении, связанном с использованием информационно-телекоммуникационных технологий, может использоваться практически весь спектр следственных и процессуальных действий, в том числе и производство судебной экспертизы в отношении изъятых предметов.

При проведении проверки сообщения о преступлении могут быть изъяты пользовательское оборудование, сетевые аппаратные средства, компьютерная информация, материалы сертификации информационных систем, запоминающие устройства и носители данных, системное программное обеспечение.

На первоначальном этапе процессуальной проверки сообщения о преступлении необходимо оперативно изъять указанные предметы, так как объективные обстоятельства совершения рассматриваемых преступлений могут быть установлены по результатам проведения судебных экспертиз, в основе которых лежит исследование изъятых предметов. В случае обнаружения и изъя-

тия указанных предметов и информации следующим шагом является их осмотр, в рамках которого следует обращать внимание на номера телефонов провайдера, имена и пароли пользователя, даты создания и другие идентификационные сведения, позволяющие установить обстоятельства совершения преступления. Если в ходе следственного действия был изъят электронный носитель информации, то следующим этапом досудебного производства будет производство осмотра предмета с соблюдением особенностей, указанных в ст. 164.1 УПК РФ.

Необходимость изъятия носителей информации и возможность проведения экспертных исследований на стадии возбуждения уголовного дела, в свою очередь, обусловила еще одну особенность производства. Сроки проведения проверок сообщений о таких преступлениях зачастую продлеваются по ходатайству следователя руководителем следственного органа в соответствии с ч. 3 ст. 144 УПК РФ для истребования документов и предметов (компьютеров, иных средств коммуникации), назначения и производства судебной компьютерно-технической экспертизы (аппаратно-компьютерной, программно-компьютерной, информационно-компьютерной, компьютерно-сетевой экспертиз, компьютерно-технической экспертизы мобильных телефонов сотовой связи), а также проведения оперативно-розыскных мероприятий (при необходимости установления лица, совершившего преступление, его соучастников и др.).

Производство судебной экспертизы может выйти за рамки установленных уголовно-процессуальными нормами сроков. Поэтому в зависимости от обстоятельств совершенного преступного деяния, а также в целях исключения дублирования процессуальных действий назначение судебной экспертизы может быть перенесено на стадию предварительного расследования.

Следует отметить, что в отличие от назначения судебной экспертизы изъятие предметов (электронных носителей информации) и документов, содержащих информацию о совершении преступления с использованием информационных и телекоммуникационных технологий, откладывать недопустимо.

Проведение осмотра и экспертизы в целях получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий *в установленном законом поряд-*

ке (выделено мной. — *Авт.*), не предполагает вынесения об этом специального судебного решения[1].

Срок проверки сообщения о преступлении, как и срок предварительного расследования, обусловлен спецификой совершения преступления: широкой географией совершения преступлений; возможностью совершения преступлений из любого места с помощью практически любого электронного устройства; наличием средств совершения преступления (например, мобильных устройств с доступом к сети Интернет) у широкой категории лиц, в том числе у школьников. Указанное определило еще одну особенность проведения проверки по сообщению о преступлении — установление места совершения преступления и определение подследственности.

Определение места совершения преступления и подследственности уголовных дел. В досудебном производстве по уголовным делам о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, нередко возникают вопросы, связанные с определением места производства предварительного расследования. При поступлении сообщения о преступлении необходимо решить вопрос о территориальной подследственности. В соответствии со ст. 152 УПК РФ предварительное расследование производится по месту совершения деяния, содержащего признаки преступления. При необходимости производства следственных действий в другом месте следователь вправе произвести их лично либо поручить производство этих действий органу дознания.

При совершении преступлений с использованием информационных и телекоммуникационных технологий определяющим является фактический момент окончания преступления: если преступление было начато в одном месте, а окончено в другом, то уголовное дело расследуется по месту окончания преступления.

---

[1] См.: *Об отказе* в принятии к рассмотрению жалобы гражданина Прозоровского Д.А. на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ: Определение Конституционного Суда Российской Федерации от 25.01.2018 № 189-О // СПС «КонсультантПлюс» (дата обращения: 15.03.2023); *Об отказе* в принятии к рассмотрению жалобы гражданина Тимофеева В.В. на нарушение его конституционных прав частью шестой статьи 164 УПК РФ: Определение Конституционного Суда РФ от 31.05.2022 № 1366-О // СПС «КонсультантПлюс» (дата обращения: 15.03.2023)

Вне зависимости от места и времени совершения преступного деяния и полноты сообщаемых сведений в соответствии с приказом Следственного комитета Российской Федерации от 11 октября 2012 г. № 72 «Об организации приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации» сообщение о преступлении подлежит обязательному приему во всех следственных органах Следственного комитета Российской Федерации. В большинстве случаев уголовное дело возбуждается тем следственным органом, в который обратился заявитель и, как правило, расположенный по месту его жительства.

В ходе расследования уголовного дела устанавливается точное место совершения преступления, и при наличии условий, указанных в ст. 152 УПК РФ, дело может быть передано по территориальной подследственности в другой следственный орган.

С учетом сложившейся следственной и судебной практики правоприменители преимущественно ориентируются на место нахождения IP-адреса, с которого осуществлялись противоправные действия. Если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них.

Следует учитывать, что субъекты, совершившие преступление с использованием информационно-телекоммуникационных систем, применяют различные программные средства в целях подмены реальных IP-адресов на вымышленные, а также динамические IP-адреса. Указанные особенности обусловили специфику доказывания причастности к совершенным преступлениям конкретного лица, а также сложности в установлении места совершения каждого конкретного преступления. Решение данной проблемы возможно только посредством анализа всех использованных преступником IP-адресов.

Если преступление совершено вне пределов Российской Федерации, то место производства по уголовному делу определяется с учетом правил привлечения к уголовной ответственности (ст. 12 УК РФ) и требований ст. 459 УПК РФ по месту жительства или месту пребывания потерпевшего в Российской Федерации, либо по месту нахождения большинства свидетелей, либо по месту

жительства или месту пребывания обвиняемого в Российской Федерации, если потерпевший проживает или пребывает вне пределов Российской Федерации.

При расследовании уголовных дел о преступлениях, объективная сторона которых выражается в размещении в информационно-телекоммуникационной сети запрещенной информации, могут быть выявлены обстоятельства, являющиеся основаниями для изменения территориальной подследственности.

По мнению А.А. Казакова, необходимость применения ч. 4 ст. 152 УПК РФ может быть обусловлена случаями, когда место выхода в сеть не совпадет с местом жительства подозреваемого (обвиняемого). В ситуациях, когда размещенные в сети сведения носили строго адресный характер в зависимости от установленных обстоятельств, а также при необходимости собирания доказательств по месту жительства потерпевшего (демонстрировавшего переписку родственникам и знакомым, делившегося с ними переживаниями и т.д.) предварительное расследование может производиться по месту нахождения потерпевшего[1].

При определении места производства расследования следует учитывать положения ч. 4.1 ст. 152 УПК РФ, согласно которым: «если преступление совершено вне пределов Российской Федерации, уголовное дело расследуется… по месту, определенному Председателем Следственного комитета Российской Федерации, при условии, что преступление совершено иностранным гражданином или лицом без гражданства, не проживающими постоянно в Российской Федерации, и направлено против интересов Российской Федерации».

В любом случае решение об определении либо изменении подследственности должно быть мотивированным с конкретным указанием конкретных фактических данных, предусмотренных уголовно-процессуальным законодательством.

При совершении преступлений с использованием информационно-телекоммуникационных технологий с разных IP-адресов (территориально удаленных друг от друга), направленных на

[1] См.: *Казаков А.А.* Об определении территориальной подследственности по уголовным делам о преступлениях экстремистской направленности // Расследование преступлений: проблемы и пути их решения. 2018. № 2(20). С. 159.

причинение вреда сразу нескольким потерпевшим, целесообразно рассмотреть вопрос о производстве предварительного следствия следственной группой (ст. 163 УПК РФ), о чем выносится отдельное постановление или указывается в постановлении о возбуждении уголовного дела. К работе следственной группы также могут быть привлечены сотрудники органа дознания, осуществляющего оперативно-розыскную деятельность и, как правило, специализирующегося на раскрытии преступлений, совершенных с использованием информационных и телекоммуникационных технологий. Особенностью формируемых для расследования таких преступлений следственно-оперативных групп является применение для обеспечения их скоординированных действий территориально обособленных подгрупп, которым поручено расследование преступлений, совершенных на определенной территории.

Доказательства и доказывание по уголовному делу о преступлении, совершенном с использованием информационных и телекоммуникационных технологий. При производстве по уголовному делу о преступлении, совершенном с использованием информационных и телекоммуникационных технологий, как и любом другом преступлении, доказыванию по общему правилу подлежат обстоятельства, указанные в ст. 73 УПК РФ.

Выявлению подлежат также обстоятельства, способствовавшие совершению преступления (ч. 2 ст. 73 УПК РФ). Поскольку на основании этих обстоятельств принимаются меры процессуального реагирования (вынесение представления о принятии мер по устранению указанных обстоятельств в адрес тех, кто их допустил), такие обстоятельства подлежат «выявлению» только путем уголовно-процессуального доказывания.

Установление обстоятельств, входящих в предмет доказывания, возможно только на основе доказательств, полученных в установленной законом процессуальной форме. В том случае, если при собирании и закреплении доказательств были нарушены гарантированные Конституцией Российской Федерации права человека и гражданина или установленный уголовно-процессуальным законодательством порядок их собирания и закрепления, а также если собирание и закрепление доказательств осуществлено ненадлежащим лицом или органом либо в результате действий, не предусмотренных процессуальными нормами, они будут призна-

ваться полученными с нарушением закона с соответствующими последствиями[1].

Наряду с доказательствами, определенными в ч. 2 ст. 74 УПК РФ, учеными-процессуалистами выделяются «электронные доказательства»[2], предпринимаются попытки соотнесения их с другими видами доказательств, выделения оснований их классификации[3], исследуются особенности их получения и использования в доказывании[4].

Термин «электронное доказательство» отсутствует в уголовно-процессуальном законодательстве и используется в научной литературе.

В целях подготовки высококвалифицированных кадров, готовых к новым вызовам и угрозам в условиях всеобщей цифровиза-

---

[1] См.: *О некоторых* вопросах применения судами Конституции Российской Федерации при осуществлении правосудия: постановление Пленума Верховного Суда Российской Федерации от 31.10.1995 № 8 // СПС «КонсультантПлюс» (дата обращения: 17.03.2023).

[2] См., например: *Палоян С.А., Дегтярева О.В.* Электронные доказательства по уголовным делам // Матрица научного познания. 2023. № 1-1. С. 288—292; *Рябова О.В.* Проблемы совершенствования положений УПК РФ в части регламентации электронных доказательств // Юрид. техника. 2023. № 17. С. 656—659.

[3] См., например: *Яковлева К.Ю.* Соотношение электронной информации с некоторыми видами доказательств в уголовном процессе // Теория и практика общественного развития. 2023. № 2(180). С. 153—156; *Количенко А.А.* Отличительные признаки и основания для классификации электронных доказательств в уголовном процессе // Вестн. Урал. юрид. ин-та МВД России. 2022. № 1(33). С. 19—23; *Хмельнова О.С.* Электронная переписка, электронные документы и другие электронные доказательства в системе средств доказывания в условиях цифрофизации // Трибуна ученого. 2022. № 3. С. 109—113.

[4] См., например: *Бердникова О.П.* Порядок получения электронных доказательств при проведении отдельных следственных действий // Право и государство: теория и практика. 2022. № 1(205). С. 366—368; *Долгаев В.В., Соколова А.В.* Вопросы регламентации использования в качестве доказательств информации, содержащейся на электронных носителях // Вестн. Волгоград. акад. МВД России. 2022. № 1(60). С. 79—84; *Муравейко А.С.* Особенности использования электронной информации в качестве доказательств в уголовном судопроизводстве России // Инновации. Наука. Образование. 2022. № 50. С. 1289—1297; *Прокопенко А.Н., Страхов А.А.* Правовые основания получения электронных доказательств посредством осмотра и изъятия электронных носителей // Вестн. Белгород. юрид. ин-та МВД России им. И.Д. Путилина. 2023. № 1. С. 50—56; *Собирание* электронных доказательств по уголовным делам на территории России и зарубежных стран: Монография / Под общ. ред. С.П. Щербы. М.: Проспект, 2022.

ции, разрабатывается учебная литература[1], изучение которой направлено на получение специальных знаний о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий.

На доктринальном уровне предлагаются изменения существующей системы следственных действий. Так, профессором А.С. Александровым в случаях, когда цифровая информация может выступать в качестве доказательств, подвергается сомнению целесообразность сохранения таких следственных действиях, как осмотр, выемка, обыск. На их смену должно прийти универсальное следственное действие — получение цифровой информации. При этом информация в рамках уголовного процесса будет передаваться на электронных носителях, по телекоммуникационным, информационным каналам связи[2].

По нашему мнению, в современных условиях на так называемые электронные доказательства, под которыми зачастую понимается электронная информация, может распространяться классификация традиционных доказательств с учетом их внедрения в действующую правовую регламентацию[3].

Определение термина «доказательства по уголовному делу о преступлении, совершенном с использованием информационных и телекоммуникационных технологий» необходимо формулировать в соответствии с положениями ч. 1 ст. 74 УПК РФ.

Такими доказательствами являются любые сведения, на основе которых суд, прокурор, следователь, дознаватель устанавли-

---

[1] См., например: *Способы* получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: Учеб. пособие / Под общ. ред. Б.Я. Гаврилова. М.: Проспект, 2017; *Электронные* доказательства в уголовном судопроизводстве: Учеб. пособие / Под общ. ред. С.В. Зуева. М.: Юрайт, 2023.

[2] См.: *Александров А.С.* Проблемы теории уголовно-процессуального доказывания, которые надо решать в связи с переходом в эпоху цифровых технологий // Судебная власть и уголовный процесс. 2018. № 2. С. 133—134.

[3] О способах внедрения в действующую правовую регламентацию так называемых «электронных доказательств» см., например: *Сергеев М.С.* Правовые регулирование применения электронной информации и электронных носителей информации в уголовном судопроизводстве: Дис. ... канд. юрид. наук. Екатеринбург, 2018; *Кувычков С.И.* Использование в доказывании по уголовным делам информации, представленной в электронном виде: Дис. ... канд. юрид. наук. Н. Новгород, 2016.

вают наличие или отсутствие обстоятельств, подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела о преступлении, совершенном с использованием информационных технологий.

Доказательства по уголовным делам о рассматриваемых преступлениях могут иметь признаки как вещественных доказательств (ст. 81 УПК РФ), так и иных документов (ст. 84 УПК РФ).

Выявление, раскрытие и расследование преступлений, совершенных с использованием информационных и телекоммуникационных технологий, характеризуются наличием вещественных доказательств в виде предметов и документов, которые служили средствами для обнаружения преступления и установления обстоятельств уголовного дела (п. 3 ч. 1 ст. 81 УПК РФ).

К таким доказательствам могут быть отнесены:

- пользовательское оборудование (оконечное оборудование): персональный компьютер, мейнфрейм, устройство сбора данных, приемник сигналов глобальной навигационной системы или любое другое оборудование, способное передавать или принимать данные;
- сетевые аппаратные средства: серверы, рабочие станции, активное оборудование, сетевые кабели и т.п.;
- компьютерная информация — сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (примечание 1 к ст. 272 УК РФ);
- документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами;
- материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов;
- запоминающие устройства и носители данных: микросхемы памяти, магнитные и лазерные диски, флэш-карты и т.п.;
- системное программное обеспечение (операционные системы) и другие доказательства.

Иные документы как доказательства по уголовному делу могут содержать сведения, зафиксированные как в письменном, так

и в ином виде. К ним могут быть отнесены материалы фото- и киносъемки, аудио- и видеозаписи и иные носители информации.

Изъятие электронных носителей информации и копирование с них информации при производстве следственных действий. Собирание доказательств представляет собой их выявление, изъятие и фиксацию в полном соответствии с требованиями уголовно-процессуального закона. Установление обстоятельств совершения преступлений с использованием информационных и телекоммуникационных технологий осуществляется посредством производства следственных и иных процессуальных действий.

Особое внимание следует уделить процессуальному порядку выполнения следственных действий, связанных с изъятием электронных носителей информации (ст. 164.1 УПК). Обязательным условием изъятия электронных носителей информации и копирования с них информации при производстве следственных действий является участие специалиста.

Профессор А.С. Шаталов отмечает в одной из своих работ одну из главных особенностей преступлений, совершенных с использованием современных информационных технологий: их предотвращение, выявление, раскрытие и расследование невозможно без современных информационных технологий. В связи с этим возникла необходимость подготовки специалистов для борьбы с такими преступлениями, переподготовке действующих кадров, с тем чтобы разоблачать преступников посредством обнаружения, фиксации, изъятия и использования разного рода «электронных доказательств»[1].

Следует учитывать, что информация (сведения) о совершении преступления, связанного с использованием информационных и телекоммуникационных технологий, даже после ее удаления может быть восстановлена и изъята в установленном законом порядке. Поэтому в обязательном порядке следует привлекать специалиста к производству следственных действий, направленных на поиск информации и предметов, изъятие предметов и их осмотр.

Участие специалиста является обязательным и в силу положений ч. 2 ст. 164.1 УПК РФ.

---

[1] См.: *Шаталов А.С.* Феноменология преступлений, совершенных с использованием современных информационных технологий // Право: Журнал Высшей школы экономики. 2018. № 2. С. 68—83.

Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации на другие электронные носители, предоставленные законным владельцем изымаемых электронных носителей информации или обладателем содержащейся на них информации.

Копирование информации не осуществляется при наличии обстоятельств, указанных в п. 3 ч. 1 ст. 164.1 УПК РФ: на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, 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 носителей информации не допускается при производстве следственных действий по уголовным делам о преступлениях, указанных в ч. 4.1 ст. 164 УПК РФ, совершенных индивидуальным предпринимателем в связи с осуществлением им соответствующей деятельности. Исключением из правила являются случаи, когда:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, 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 носителей информации и копирование с них информации могут быть произведены как по общим правилам производства следственных действий, так и по судебному решению в порядке, предусмотренном ст. 165 УПК РФ. Следователь в тех случаях, когда следственные действия могут быть произведены с разрешения суда, возбуждает с согласия руководителя следственного органа перед судом ходатайство о производстве следственного действия, о чем выносится постановление. Ходатайство о производстве следственного действия подлежит рассмотрению единолично судьей районного суда по месту производства предварительного следствия или производства следственного действия не позднее 24 часов с момента поступления указанного ходатайства.

На основании судебного решения изъятие электронных носителей информации и копирование с них информации может быть произведено в ходе производства следующих следственных действий:

- осмотра жилища при отсутствии согласия проживающих в нем лиц (п. 4 ч. 2 ст. 29 УПК РФ). С учетом положений ч. 5 ст. 177 УПК РФ на производство осмотра жилища требуется разрешение суда, если хотя бы одно из проживающих в нем лиц возражает против осмотра;
- обыска и (или) выемки в жилище (п. 5 ч. 2 ст. 29 УПК РФ);
- выемки заложенной или сданной на хранение в ломбард вещи (п. 5.1 ч. 2 ст. 29 УПК РФ);
- обыска, осмотра и выемки в отношении адвоката в соответствии со ст. 450.1 УПК (п. 5.2 ч. 2 ст. 29 УПК РФ);
- личного обыска, за исключением случаев, когда подозреваемый может быть подвергнут личному обыску без соответствующего постановления: при его задержании, а также при наличии достаточных оснований полагать, что лицо, находящееся в помещении или ином месте, в котором производится обыск, скрывает при себе предметы или документы, которые могут иметь значение для уголовного дела (п. 6 ч. 2 ст. 29 УПК РФ);

- выемки предметов, содержащих государственную или иную охраняемую федеральным законом тайну, а также предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях (п. 7 ч. 2 ст. 29 УПК РФ).

Электронный носитель информации, признанный вещественным доказательством по уголовному делу:

а) хранится в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на нем информацией и обеспечивающих его сохранность и сохранность указанной информации;

б) возвращается их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания.

К специальным процессуальным средствам, позволяющим установить обстоятельства, подлежащие доказыванию, также относятся получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) и производство контроля и записи переговоров (ст. 186 УПК РФ).

Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) допускается на основании судебного решения.

Пленум Верховного Суда Российской Федерации, разъясняя применение норм, регламентирующих получение информации о соединениях между абонентами и (или) абонентскими устройствами в соответствии со ст. 186.1 УПК РФ, указал, что судьей может быть дано разрешение на получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций. К другим данным, позволяющим идентифицировать абонентов, могут относиться, в частности, сведения о IMEI-коде абонентского устройства или о местоположении телефонного аппарата относительно базовой станции[1].

[1] См.: *О практике* рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): постановление Пленума Верховного Суда Российской Федерации от 01.06.2017 № 19 // СПС «КонсультантПлюс» (дата обращения: 17.03.2023).

Следует учитывать, что рассматриваемое следственное действие не может быть использовано для доступа к информации о содержании переговоров, ведущихся как голосовыми, так и не- голосовыми средствами, в том числе посредством электронной почты, SMS- и MMS-сообщений и т.д. Данное следственное действие может производиться по уголовным делам о преступлениях любой степени тяжести для получения информации о соединениях между любыми абонентами и вне зависимости от того, кому принадлежат абонентские устройства.

Информация предоставляется следователю в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств. Получив представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, следователь осматривает их, привлекая для этого при необходимости специалиста.

Представленные документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, признаются вещественными доказательствами[1], приобщаются на основании постановления следователя к материалам уголовного дела в полном объеме и хранятся в опечатанном виде в условиях, обеспечивающих их сохранность и исключающих возможность ознакомления с ними посторонних лиц.

Контроль телефонных и иных переговоров — это прослушивание и запись переговоров путем использования любых средств коммуникации, осмотр и прослушивание фонограмм, осуществляемое подразделением по проведению специальных технических мероприятий.

Следователь в течение всего срока производства контроля и записи телефонных и иных переговоров вправе в любое время истребовать от органа, их осуществляющего, фонограмму для осмотра и прослушивания[2]. Фонограмма передается следователю

[1] На основании п. 3 ч. 1 ст. 81, ч. 6 ст. 186.1 УПК РФ документы, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, относятся к иным предметам и документам, которые могут служить средствами для обнаружения преступления и установления обстоятельств уголовного дела.

[2] При производстве осмотра и прослушивания фонограммы целесообразно участие специалиста. К осмотру и прослушиванию фонограммы по решению следователя могут привлекаться лица, переговоры которых были записаны.

в опечатанном виде с сопроводительным письмом, в котором должны быть указаны дата и время начала и окончания записи указанных переговоров и краткие характеристики использованных при этом технических средств.

Об осмотре и прослушивании фонограммы составляется протокол. В данном протоколе дословно должна быть изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к делу.

Согласно ч. 8 ст. 186 УПК РФ, на основании постановления следователя фонограмма в полном объеме приобщается к материалам уголовного дела как вещественное доказательство и хранится в опечатанном виде в условиях, обеспечивающих ее сохранность и возможность повторного прослушивания.

Взаимодействие следователя с органами дознания, администрацией социальных сетей, мессенджеров. Собирание доказательств по уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий, может осуществляться следователем также путем производства *иных процессуальных действий.* Иные процессуальные действия, направленные на собирание доказательств, предусмотрены законом, но в отличие от следственных действий процедура их производства детально не регламентирована. Так, ч. 4 ст. 21 УПК РФ, например, устанавливает правило, согласно которому требования, поручения и запросы следователя, предъявленные в пределах его полномочий, установленных уголовно-процессуальным законом, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

По запросу следователя администрации социальных сетей могут предоставить IP-адреса роутеров, к которым подключались технические устройства и при помощи которых осуществлялся выход в социальные сети.

Одной из особенностей расследования преступлений, совершенных с использованием информационных и телекоммуникационных технологий, является длительность сбора информации от интернет-провайдеров, операторов сотовой связи и администрации интернет-ресурсов (социальных сетей), а также ограниченность сроков ее хранения.

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ч. 3.1 ст. 10.1) организатор распространения сведений в сети Интернет обязан предоставлять информацию уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

К такой информации относятся:

а) информация о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео или иных электронных сообщений пользователей сети Интернет и информация об этих пользователях в течение одного года с момента окончания осуществления таких действий;

б) текстовые сообщения пользователей сети Интернет, голосовая информация, изображения, звуки, видео, иные электронные сообщения пользователей сети Интернет. Такие сообщения хранятся до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения информации устанавливаются Правительством РФ.

Ввиду неоднозначной практики рекомендуется предварительно выяснить вопрос в запрашиваемой организации, будет ли предоставлена информация по запросу органа, осуществляющего оперативно-розыскную деятельность. При необходимости следует обратиться с соответствующим ходатайством в суд в порядке, предусмотренном ст. 165 УПК РФ. При необходимости производства нескольких следственных действий одновременно (например, производство обыска в разных местах) следователь вправе поручить их производство органу дознания в порядке, предусмотренном ч. 1 ст. 152 УПК РФ.

Своевременно инициированные законодателем и рассмотренные в настоящей работе особенности досудебного производства по уголовным делам о преступлениях, совершенных с использованием информационных и телекоммуникационных технологий, коррелируют с происходящими процессами глобальной цифровизации общества и являются важной гарантией обеспечения прав участников уголовного судопроизводства при условии строгого соблюдения субъектами органов уголовного преследования уго-

ловно-процессуального законодательства при установлении истины по уголовному делу.

3.2. Цифровые технологии в уголовном процессе

Ю.А. Цветков[1]

С распространением Интернета цифровые технологии в правоохранительную и судебную деятельность внедряют за рубежом с начала 90-х годов прошлого века. Через 20 лет этот процесс распространился и на российскую юстицию. Вот уже более 10 лет отечественный законодатель последовательно вносит в УПК изменения и дополнения, направленные на цифровую трансформацию уголовного судопроизводства. Его катализатором как в России, так и во всем мире стала пандемия коронавирусной инфекции. Нововведения реализуются в трех направлениях:

1) применение дистанционных технологий производства следственных и судебных действий преимущественно путем расширения возможностей использования средств видео-конференц-связи (далее — ВКС);

2) дифференциация форм процессуальных документов (развитие электронного документооборота, аудио- и видеопротоколирование);

3) внедрение искусственного интеллекта (далее — ИИ) в правосудие и процессуальную деятельность следователя, прокурора и суда.

В рамках *первого направления* российский законодатель уже в 2010 г., вводя полноценное апелляционное производство, разрешил использовать ВКС для обеспечения участия в судебном заседании подсудимого, содержащегося под стражей, при рассмотрении уголовных дел судами апелляционной инстанции (ст. 389.12 УПК РФ)[2]. В 2011 г. внесены дополнения в ст. 240 и введена ст.

[1] Юрий Анатольевич Цветков — заведующий кафедрой уголовного процесса Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент.

[2] Федеральный закон от 29.12.2010 № 433-ФЗ (ред. от 31.12.2014) «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации и признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации».

278.1 УПК РФ, предоставившие суду право допроса свидетеля и потерпевшего с применением ВКС[1]. Так, в 1-м полугодии 2021 г. суды с использованием ВКС рассмотрели по первой инстанции 50 650 уголовных дел и материалов[2]. За аналогичный период 2022 г., когда эпидемиологические ограничения утратили силу, этот показатель только увеличился — до 50 849 дел и материалов[3].

Пионером в использовании ВКС между несколькими судами стали США. Там эта практика известна еще с начала 1990-х гг. под названием «телеправосудие» (telejustice). В результате его применения существенно сократились сроки отправления правосудия. Так, дела, рассматривавшиеся 120 дней, были разрешены всего за 10 дней[4].

В Казахстане реализовывается проект «SMART-суд», предоставивший сторонам по делу возможность дистанционного участия в судебных заседаниях с помощью мобильного приложения TrueConf. На середину 2020 г. все 100% судебных заседаний в этой стране проведены с использованием ВКС[5].

В канун 2023 г. Президент РФ подписал федеральный закон, распространивший право суда на использование ВКС при производстве любых судебных действий. Этим же законом введена ст. 241.1, предоставившая подсудимому по его ходатайству возможность дистанционного участия в рассмотрении уголовных дел любой категории (кроме тех, где участвуют присяжные заседатели). По делам о тяжких и особо тяжких преступлениях суд по просьбе любой из сторон вправе принять решение об участии содержащегося под стражей подсудимого в формате ВКС даже при

---

[1] Федеральный закон от 20.03.2011 № 39-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

[2] Ведомственное статистическое наблюдение «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции за 6 мес. 2021 г.».

[3] Ведомственное статистическое наблюдение «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции за 6 мес. 2022 г.».

[4] См.: *Концепция* построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию»): Монография / Отв. ред. Л.Н. Масленникова. М.: Норма — Инфра-М, 2022. С. 264.

[5] Там же. С. 265.

отсутствии согласия подсудимого[1]. Гипотетически возникает возможность дистанционного рассмотрения всего уголовного дела целиком, когда в зале судебного заседания будут собираться только профессионалы — председательствующий, государственный обвинитель, защитник и секретарь судебного заседания.

Годом ранее, также перед новогодними праздниками, возможность дистанционного проведения следственных действий получили следователи и дознаватели. В УПК РФ введена ст. 189.1 УПК РФ, разрешающая проведение с использованием ВКС трех следственных действия: допроса, очной ставки и опознания[2]. За год своего действия норма пока широкого применения не нашла. Необходимость в этом у следователей возникает гораздо реже, чем у судей, а привычный, хотя и далекий от совершенства механизм поручения позволяет решать эту проблему с наименьшими затратами времени и сил. Тем не менее если установленный новой статьей порядок все-таки зарекомендует себя на практике с положительной стороны, то его могут распространить и на другие следственные действия, например на производство выемки и обыска. Правда, уже сейчас ученые строят умозрительные прогнозы относительно трудностей его применения, в частности, дистанционного опознания. Они не без оснований отмечают, что суд изначально получил лишь полномочия по производству дистанционного допроса, но не опознания, несмотря на возможность проведения такого судебного действия в традиционном формате (ст. 289 УПК РФ)[3].

В то время как Россия по критерию расширения сферы использования дистанционных технологий судопроизводства движется в общемировом фарватере, в отдельных юрисдикциях континентальной правовой семьи этот процесс получил решительный отпор. Так, во Франции кратковременный рост популярности этой практики сменился жесткой реакцией. Правительственный ордонанс от 25 марта 2020 г. наделил суды полномочием по собственной инициативе использовать «средства аудиовизуальной

[1] Федеральный закон от 29.12.2022 № 610-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».
[2] Федеральный закон от 30.12.2021 № 501-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».
[3] См.: *Азаренок Н.В.* Вопросы практической реализации положений ст. 189[1] УПК РФ // Уголовное право. 2022. № 8. С. 75—80.

коммуникации» при рассмотрении всех уголовных дел, кроме дел о наиболее опасных преступлениях, подсудных судам ассизов. А ордонанс от 18 ноября 2020 г. распространил это порядок на все без исключения уголовные дела с той лишь разницей, что по большей их части допускалось применение любых средств связи, включая допрос по телефону, в то время как по наиболее сложным делам — только ВКС. Посягнув на такие архаичные принципы, как устность и непосредственность судебного разбирательства, новый порядок стал предметом обжалования со стороны адвокатского сообщества. Конституционный совет и Государственный совет своими решениями соответственно от 15 января 2021 г. и 12 февраля 2021 г. подтвердили фундаментальную ценность права обвиняемого лично предстать перед судом, быть им услышанным и увиденным, и по всем без исключения уголовным делам запретили применение ВКС. В своих решениях они провели принципиально важное для дальнейшего формирования доктрины уголовного процесса различение реального и виртуального общения с подсудимым, признав неравноценность замены первого на второе[1].

По *второму направлению* законодатель в 2016 г. внес дополнения в ст. 393 УПК РФ, дающие судье право направлять исполнительный лист для исполнения в органы принудительного исполнения в форме электронного документа, подписанного электронной подписью. В часть шестую УПК РФ введена ст. 474.1, в соответствии с которой ходатайство, заявление, жалоба, представление с приложенными к ним материалами могут быть поданы в суд в форме электронного документа, подписанного лицом, направившим такой документ, электронной подписью. Копия судебного решения, изготовленная в форме электронного документа и заверенная электронной подписью, по просьбе либо с согласия участника уголовного судопроизводства может быть направлена ему с использованием информационно-телекоммуникационной сети Интернет[2].

---

[1] См.: *Головко Л.В.* Изменение подходов к применению видео-конференц-связи в уголовном процессе Франции: от санитарно-технологического к ценностно-процессуальному дискурсу // Законность. 2022. № 6. С. 52—54.

[2] Федеральный закон от 03.07.2016 № 323-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации по вопросам совершенствования оснований и порядка освобождения от уголовной ответственности».

Тем же предновогодним Федеральным законом № 610-ФЗ ст. 474.1 УПК РФ изложена в новой редакции. В ней определен домен для электронного документооборота между судом и другими участниками уголовного процесса (Единый портал государственных и муниципальных услуг). Посредством этого портала будут направлять повестки лицу, давшему согласие на уведомление его в таком порядке. Это снимает хроническую проблему извещения участников уголовного судопроизводства о назначенных судебных заседаниях или следственных действиях. В статье упомянута единая система межведомственного электронного взаимодействия — прообраз *электронного уголовного дела*, легализация которого станет логическим завершением цифровизации уголовного процесса.

В этом плане показателен пример Казахстана, где все начиналось с введения в 2015 г. в действие Единого реестра досудебных расследований. В этой республике отсутствует институт возбуждения уголовного дела, поэтому досудебные расследования начинаются с момента регистрации сообщения о преступлении (заявления, явки с повинной, рапорта и т.д.) Поскольку принципиально важным является момент принятия решения о регистрации сообщения об уголовном правонарушении (по ст.10 казахского УК все уголовные правонарушения подразделяются на преступления и уголовные проступки), установлены жесткие критерии отнесения заявления к сообщению о преступлении. Каждый гражданин может получить доступ к порталу Единого реестра досудебных расследований. Для этого ему требуется получить электронную подпись, что он может сделать бесплатно в любом многофункциональном центре государственных услуг. Используя любой гаджет (компьютер, ноутбук, смартфон и т.д.), он входит на этот портал, с помощью электронной подписи авторизуется и становится обладателем своего личного кабинета. В нем гражданин может дистанционно реализовать все свои права в сфере уголовного судопроизводства (подать заявление об уголовном правонарушении и отслеживать изменения его статуса, а в случае его регистрации — подавать жалобы и ходатайства, получать ответы на них и знакомиться с открытыми для него материалами досудебного расследования)[1].

[1] См.: *Концепция* построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий. С. 211—215.

Таким образом, Единый реестр досудебных расследований — это один из модулей целой цифровой системы уголовного судопроизводства в Казахстане, выполняющий функции входа в ее ядро — «Электронное уголовное дело». Электронный формат уголовного судопроизводства введен в Казахстане с 2017 г.[1] Он действует наряду с традиционным бумажным форматом, однако к 2025 г. запланирован перевод всего уголовного процесса на цифровую платформу[2]. Формат уголовного дела определяет лицо, ведущее производство по уголовному делу, исходя из конкретной ситуации, при этом допускается переход из одного формата в другой. Согласно официальному определению, электронное уголовное дело — это обособленное производство, ведущееся органом уголовного преследования по поводу одного или нескольких уголовных правонарушений в электронном формате посредством модуля е-УД в рамках общей электронной системы ведения досудебного расследования[3]. Все производство осуществляется с использованием специальных электронных шаблонов документов, которые автоматически формируются самой системой. Процессуальные документы, созданные в бумажном формате, а равно видео-, аудио- и фотоматериалы в течение 24 ч подлежат оцифровыванию. Взаимодействие с участниками уголовного процесса (судом, прокурором и экспертами) осуществляется по электронным каналам связи через соответствующие порты. Эти участники, в свою очередь, размещают созданные ими документы (постановления суда, заключения экспертов и т.д.) в этой же электронной оболочке. Лица, имеющие в силу закона право знакомиться с материалами конкретного уголовного дела, получают посредством выделенного им домена доступ к тем материалам, с которыми они имеют право знакомиться. Формирование материалов электронного уголовного дела осуществляется в режиме реального

[1] Статья 42.1 «Формат уголовного судопроизводства» УПК Республики Казахстан (введена Законом Республики Казахстан от 21.12.2017 №118-VI).

[2] Указ Президента Республики Казахстан от 15.02.2018 №636 «Об утверждении Стратегического плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан».

[3] Приказ Генеральной прокуратуры Республики Казахстан от 03.01.2018 № 2 «Об утверждении Инструкции о ведении уголовного судопроизводства в электронном формате».

времени, что исключает в дальнейшем возможности их фальсификации[1].

С 2019 г. по всем уголовным делам, рассматриваемым в российских судах первой и апелляционной инстанций, наряду с подготовкой протокола судебного заседания в письменной форме осуществляется аудиопротоколирование[2]. О масштабе нововведения говорят статистические данные. Так, с использованием средств аудиозаписи за 2021 г. составлены протоколы по 1 млн 174 тыс. 721 уголовному делу и материалу[3]. Анализ практики первых лет применения технических средств протоколирования показал, что при оценке расхождений в содержании аудио- и письменного протокола вышестоящие суды используют его для разрешения явных противоречий по сугубо формальным вопросам. Так, когда в протоколе отсутствовало указание на предоставленную подсудимому возможность выступить в прениях, а на записи это сохранилось, сомнения были разрешены в пользу судьи. И напротив, вышестоящий суд удовлетворил жалобу, одним из доводов которой послужило то, что председательствующий не разъяснил сторонам их права. Несмотря на то что в протоколе содержалась ссылка на разъяснение сторонам их прав, вышестоящий суд жалобу удовлетворил, поскольку прослушивание записи этого не подтвердило. При наличии менее существенных расхождений между содержанием аудио- и письменного протокола вышестоящие суды оставляют жалобы без удовлетворения, а обжалуемые решения — без изменения. Наличие существенных противоречий между аудио- и письменным протоколом в части исследования доказательств (изложения показаний потерпевших, свидетелей и т.д.), требующих интерпретации, вышестоящими судами во внимание не принимается в принципе, за исключением очень редких, практически единичных случаев[4]. Следующим ша-

---

[1] См.: *Концепция* построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий. С. 211—226.

[2] Федеральный закон от 29.07.2018 № 228-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

[3] Ведомственное статистическое наблюдение «Отчет о работе судов общей юрисдикции по рассмотрению уголовных дел по первой инстанции за 2021 г.».

[4] См.: *Лямин А.А.* Аудиопротоколирование судебного заседания. Практика Верховного Суда РФ и кассационных судов // Уголовный процесс. 2022. № 7. С. 40—49.

гом в использовании звукозаписывающих систем может стать предложение о замене живого секретаря судебного заседания на кибернетического. В качестве такового будет предложено использовать транскрайбер — прибор для преобразования в режиме онлайн устной речи в письменный текст. Такой прибор основан уже на технологиях ИИ, что логично подводит нас к характеристике последнего направления цифровизации уголовного процесса.

Самым амбициозным и наиболее глубоко меняющим основы уголовного судопроизводства является *третье направление* его цифровизации — внедрение ИИ. Президент РФ Указом от 10.10.2019 № 490 утвердил Национальную стратегию развития искусственного интеллекта до 2030 г. В ней дано первое в России легальное определение ИИ, под которым понимается комплекс технологических решений, позволяющих имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека.

На основании того же Федерального закона с 2019 г.[1] во всех судах общей юрисдикции и арбитражных судах функционирует система автоматизированного распределения дел. По новой редакции ст. 30 УПК РФ состав суда для рассмотрения каждого уголовного дела ИИ формирует с учетом нагрузки и специализации судей. Он использует сравнительно простой алгоритм, основанный на линейном уравнении. По своей степени сложности этот алгоритм весьма далек от многослойных нейронных сетей. Однако компьютер выполняет функцию принятия решения, которую до него принимал человек (председатель суда), поэтому это уже простейший образец ИИ.

Ведущий китайский эксперт в области ИИ Кай-Фу Ли утверждает, что в настоящее время двумя основными сверхдержавами ИИ являются США и КНР. Разрыв между ними не так велик, как разрыв между этими странами, с одной стороны, и всеми остальными — с другой. Только эти державы обладают двумя основными преимуществами перед другими конкурентами: большой базой пользователей и мощным венчурным капиталом. Американские компании завладеют рынками развитых стран, а китай-

[1] Федеральный закон от 29.07.2018 № 228-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации».

ские — рынками Азии и Африки. Другим государствам, также ведущим свои разработки в этой сфере, останется «подбирать остатки», поскольку их отставание от лидеров непреодолимо. Супердержавы ИИ ожидает новый экономический взлет, а бедные страны станут еще беднее[1].

В свете такой оценки неудивительно, что пионером внедрения ИИ в правосудие стали именно США. С 2012 г. на территории трех североамериканских штатов (Нью-Йорк, Висконсин, Калифорния) и еще нескольких юрисдикций действует система COMPAS. Она оценивает риск повторного совершения преступления по шкале от 1 до 10. На основе ее рекомендаций судьи принимают решения о мере пресечения и об условно-досрочном освобождении. При значениях от 1 до 4 риск определяется как незначительный и подозреваемый (осужденный) оказывается на свободе. При более высоких значениях судьи принимают решение, как правило, не в пользу стороны обвинения. Оценка осуществляется на основе анализа данных о личности по 137 факторам, таким как пол, возраст, образование, наличие судимости, социальное окружение и т.д. Все эти факторы включаются в линейное уравнение, в котором каждый из них умножается на коэффициент корреляции между фактором и рецидивом. Машина идентифицирует семь предикторов риска, таких как «образовательные дефициты», «профессиональные дефициты» «дефицит социальных навыков достижения результатов», антисоциальные и криминальные контакты, дисфункции брачно-семейных отношений[2].

В таком революционном процессе, как внедрение в судопроизводство ИИ, принципиально важен первый шаг, и он уже сделан. Далее необратимая сила научно-технического прогресса затянет в свою воронку и этот сегмент общественного бытия. Модель того недалекого будущего, в котором скоро окажется российская юстиция, можно представить себе на примере самой большой юрисдикции мира, обслуживаемой 100-тысячным кор-

---

[1] См.: *Ли Кай-Фу.* Сверхдержавы искусственного интеллекта. Китай, Кремниевая долина и новый мировой порядок / Пер. с англ. Н. Константиновой. М.: Манн, Иванов и Фербер, 2019. С. 169—170.

[2] См.: *Бруссард М.* Искусственный интеллект: пределы возможного / Пер. с англ. Е. Арье. М.: Альпина Нон-Фикшн, 2020. С. 247.

пусом судей, — Китая. Верховный суд КНР с 2019 г. обязал судей при вынесении приговоров и принятии решений консультироваться с ИИ. Самообучающаяся система «Умный суд», в которую интегрированы все местные и региональные информационно-вычислительные системы судов, прокуратуры и полиции, ежедневно обрабатывает около 100 тыс. дел по всей стране. Если судья отклоняет рекомендацию ИИ и принимает иное решение, он обязан письменно мотивировать, почему не согласен с предложенным вариантом. С начала 2022 г. китайская прокуратура протестировала разработанный для нее алгоритм, который выдвигает собственные версии обвинения по уголовным делам о восьми наиболее распространенных преступлениях. Точность таких обвинений нашла свое подтверждение по 97% дел[1].

Цифровая трансформация уголовного судопроизводства, и прежде всего перспективы внедрения в него ИИ, встречает самые противоречивые оценки ученых и практиков, которые выражают озабоченность как незыблемостью фундаментальных принципов уголовного процесса, так и решением этических проблем, которые ставит перед обществом научно-технический прогресс.

Европейская комиссия по эффективности правосудия, предвосхищая возникновение подобных проблем в странах Европейского Союза, приняла 3 декабря 2018 г. *Европейскую этическую хартию об использовании ИИ в судебных системах и окружающих их реалиях*. Ее принятию предшествовало изучение довольно ограниченной практики применения такого рода технологий, в основном информационно-аналитической направленности, во Франции и Великобритании. В документе сформулированы пять принципов, на основе которых должны проводиться перспективные разработки и внедрение ИИ в правосудие: соблюдение основных прав и свобод; недопустимость дискриминации; качество и безопасность; прозрачность, беспристрастность и достоверность; контроль пользователем. Уже сейчас, забегая немного вперед, можно констатировать, что соблюдение четвертого принципа (прозрачности, беспристрастности и достоверности) в системах ИИ прогностического типа, основанных на технологиях много-

[1] См.: *Китайские* суды обязали консультироваться с искусственным интеллектом // Право.Ru. Июль 20, 2022 / URL: https://pravo.ru/news/242025/ (дата обращения: 25.01.2023).

слойных нейронных сетей, при современном уровне развития науки является утопией[1].

В России этические и доктринальные проблемы цифровизации уголовного судопроизводства пока не вышли на уровень органов государственной власти и обсуждаются преимущественно в научной среде. Так, профессор Л.В. Головко, ссылаясь на советского классика М.С. Строговича, оценивает попытки внедрения ИИ в процессуальную деятельность как этически ничтожные и политически вредные[2]. Он напоминает о работе М.С. Строговича «О применении средств кибернетики в оценке доказательств»[3] (1974), в которой тот попытался раз и навсегда закрыть этот вопрос, переведя его из технологической системы координат в этическую и дав на него отрицательный ответ: оценка доказательств с помощью компьютерной программы аморальна. В то же самое время другой профессор — Л.Н. Масленникова, апеллируя к авторитету того же ученого, делает прямо противоположные выводы: «Перефразируя слова М.С. Строговича, можно утверждать, что в настоящее время вопрос об упрощении, рационализации и цифровизации досудебного производства получает особую остроту и определенное политическое значение в связи с необходимостью построить уголовное судопроизводство, обеспечивающее доступ к правосудию»[4].

Не игнорируя ни в коей мере предостережение М.С. Строговича, следует в то же время учитывать исторический контекст, в котором оно было сделано. Ведь ученый хорошо помнил те времена, когда кибернетику заклеймили в СССР как буржуазную лженауку. Впрочем, фундаментальная ошибка, допущенная М.С. Строговичем, а вслед за ним и Л.В. Головко, лежит не в процессуальной и даже не в технологической, а именно в этиче-

---

[1] Подробнее см.: *Цветков Ю.А.* Искусственный интеллект в правосудии // Закон. 2021. № 4. С. 91—107.

[2] См.: *Головко Л.В.* М.С. Строгович и «искусственный интеллект»: о современной реинкарнации старых теорий и их этической ничтожности // Судебная власть и уголовный процесс. 2021. № 3. С. 29—36..

[3] См.: *Строгович М.С.* О применении средств кибернетики в оценке доказательств // Проблемы судебной этики / Под ред. М.С. Строговича. М.: Наука, 1974. С. 110—121.

[4] См.: *Масленникова Л.Н.* К вопросу о политическом значении цифровизации досудебного производства в уголовном процессе // Вестн. Моск. ун-та МВД России. 2020. № 3. С. 34—36.

ской плоскости. Управляемый алгоритмом, ИИ, в отличие от человека не подвержен ни предрассудкам, ни эмоциям, ни инстинктам. Он принимает решения сугубо рационально, на основе такого объема информации, который не доступен никакой, даже самой уникальной, человеческой памяти. Если нравственный идеал судьи — это беспристрастность, то ни один облаченный в мантию живой человек не достигнул по этому критерию уровня ИИ.

За год до публикации работы Строговича американский судья М. Франкел впервые вынес на публичное обсуждение проблему несовершенства человека в принятии судебных решений. В своей книге «Приговоры по уголовным делам: закон без порядка» он собрал и обобщил большое количество примеров, когда по разным уголовным делам об одинаково квалифицируемых преступлениях, совершенных при схожих обстоятельствах лицами, данные о личности которых также ничем не отличались, назначались совершенно разные наказания. Так, двоих не привлекавшихся ранее к уголовной ответственности мужчин судьи за обналичивание поддельных чеков на 58 и 32 долл. соответственно приговорили: одного к 15 годам, а второго — к 30 суткам лишения свободы[1].

Не только соображения политической конъюнктуры, но и уровень развития науки ограничивал М.С. Строговичу горизонт обзора. Когнитивные науки, расцвет которых пришелся на 2000-е годы, заставили нас полностью переосмыслить значение рационального мышления в принятии решений. Так, когда советский классик писал об аморальности применения кибернетики в оценке доказательств, упомянутая книга его американского коллеги инициировала целую серию исследований, самым масштабным из которых стал эксперимент с участием 208 федеральных судей. Им предложили рассмотреть 16 одинаковых дел, и лишь в трех из них судьи оказались единогласны в решении приговорить обвиняемых к тюремному заключению. По одному из дел, по которому участники эксперимента в среднем предложили 1,1 года, разброс мнений был таков, что самым суровым оказался приговор к 15 годам тюрьмы. В других исследованиях выяснилось, что судьи с большей вероятностью предоставляют условно-досрочное

[1] См.: *Frankel Marvin E.* Criminal Sentences: Law Without Order. N.Y.: Hill & Wang, 1973.

освобождение с утра и после обеденного перерыва, а голодные судьи более суровы. Жара также способствует вынесению более строгих приговоров. Когда в выходные местная футбольная команда проигрывает, в понедельник судьи выносят более строгие приговоры. Судьи, рассматривающие дела о предоставлении политического убежища, после двух удовлетворенных подряд заявлений в третьем случае отказывали на 19% чаще[1].

В чем историческое чувство действительно не подвело профессора Л.В. Головко, так это в том, что он совершенно точно определил основную угрозу, которую ИИ несет классическому уголовному процессу следственно-состязательной формы. Принятие решений с помощью ИИ — это возврат к формальной теории доказательств, поскольку и то и другое основаны на алгоритме. Инквизиционный процесс — это исторически первая попытка создать модель уголовного производства на основе научной системы доказательств. Другое дело, что научность в Средние века отождествлялась со схоластикой, а та, в свою очередь, ограничивалась переделами аристотелевской логики. С Ренессансом и последовавшей за ним эпохой Просвещения человек возвращается на пьедестал истории, который он занимал в период античности. Свойственная гуманистам вера в неограниченные возможности человеческого интеллекта и его нравственную силу породила и отказ от теории формальных оценок в пользу теории свободной оценки доказательств на основе своего внутреннего убеждения. Когнитивные науки поставили под сомнение идеалы гуманизма с его верой во всесилие человеческого разума. Судье, как и любому человеку, в целях минимизации уровня шума и повышения беспристрастности суждений требуются алгоритмы. И только теперь, спустя пять столетий, наука способна ему их предложить на цифровой платформе.

Масштабы и скорость цифровой трансформации всех сторон жизни общества определяются в том числе и таким фактором, как смена поколений. С 2019 г. стали выпускниками вузов и поступили на службу в следственные органы и прокуратуру представители поколения Z, для которых гаджеты не просто подспорье в работе и жизни, а часть их личности. Цифровые технологии уже не

[1] См.: *Канеман Д., Сибони О., Санстейн Касс Р.* Шум: несовершенство человеческих суждений / Пер. с англ. А. Котовой, С. Селифоновой, В. Тулаева. М.: АСТ, 2021. С. 21—31, 108—109, 245—246.

modus operandi нового поколения, это их *lebenswelt*. Еще год — и у них будет стаж работы по юридической специальности, достаточный для назначения на должности судей. В симбиозе с ИИ они могут коренным образом изменить уголовно-процессуальную деятельность на основе непохожих на нашу системы ценностей[1]. Русский философ Н.А. Бердяев ровно 100 лет тому назад констатировал: «Гуманизм новой истории изжит и во всех сферах культуры и общественной жизни переходит в свою противоположность, приводит к отрицанию образа человека»[2]. В уголовном процессе, как и многих других сферах деятельности, стремительное вытеснение человека алгоритмом несет с собой серьезные риски, не все из которых сейчас доступны идентификации и предупреждению. Пионеры в области цифровых технологий Илон Маск, Стив Возняк и еще около тысячи экспертов предложили ввести мораторий на обучение мощных нейронных сетей, поскольку их неконтролируемый рост может создать угрозу всему человечеству[3]. Исходя из этих предостережений, а также конституционно-правовых процессов в юрисдикциях в странах родственной нам континентальной правовой семьи (Франция), следует более осторожно подходить к вопросам цифровизации уголовного процесса, не допуская разрушения традиционных процессуальных институтов и форм.

3.3. Алгоритмы формирования доказательств и доказывания по уголовным делам о преступлениях, совершенных с использованием информационных технологий

В.А. Прорвич[4]

Одной из важнейших особенностей преступлений, совершенных с использованием информационных технологий, является широкое использование их субъектами электронных документов

[1] См.: *Черемисина Т.В.* Следователи поколения Z — новые акторы в уголовном процессе // Евразий. юрид. журн. 2020. № 5 (144). С. 286—288; *Она же.* Этика следователя в цифровую эпоху // Рос. следователь. 2019. № 12. С. 71—75.

[2] *Бердяев Н.А.* Новое средневековье (Размышление о судьбе России и Европы) // Философия неравенства / Н.А. Бердяев. М.: Ин-т рус. цивилизации, 2012. С. 520.

[3] См.: *ТАСС* (19.03.2023) // URL: https://tass.ru/ekonomika/17395655.

[4] Владимир Антонович Прорвич — профессор кафедры уголовного процесса Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доктор технических наук, профессор.

и иной электронной информации. Соответственно именно в этой документации следователь должен выявить и зафиксировать следы таких преступлений, а затем сформировать информационно полную совокупность доказательств по уголовному делу в полном соответствии с требованиями уголовно-процессуального законодательства.

Изучение соответствующих требований показывает, что в части шестой «Электронные документы и бланки процессуальных документов» УПК РФ имеется раздел XIX «Использование в уголовном судопроизводстве электронных документов и бланков процессуальных документов», в составе которого имеется глава 56 «Порядок использования электронных документов и бланков процессуальных документов», в которую включена в 2016 г. ст. 474.1 «Порядок использования электронных документов в уголовном судопроизводстве». Анализ содержания данной статьи показывает, что в ней регламентируется только порядок подачи ходатайств, заявлений, жалоб и иных электронных документов в суд, а также получение судебных решений и их копий в виде электронных документов.

В то же время статей, регламентирующих порядок использования электронных документов в досудебном производстве, а также порядок обращения следователей с электронной документацией при формировании доказательств по уголовному делу, в данной главе, разделе и части УПК РФ не имеется. Это существенно осложняет надлежащее выполнение следственных действий с использованием электронных документов и иной электронной информации, нацеленных на формирование необходимых доказательств и доказывание по соответствующим уголовным делам.

Фактически у следователя остаются лишь возможности копировать электронную информацию в соответствии со ст. 164.1 УПК РФ и приобщать ее носитель как вещественное доказательство к материалам дела, а также привлекать специалистов и судебных экспертов, для того чтобы визуализировать электронную информацию при осмотре вещественных доказательств и представить ее в виде заключения эксперта или заключения специалиста. Но при этом в «первичной» электронной информации он, в принципе, лишен возможности обнаружить и зафиксировать следы преступления, используя для этого криминалистический инст-

рументарий, а затем сформировать необходимые доказательства по расследуемому уголовному делу.

В результате во многих случаях выявление и фиксация закодированных программными средствами информационных следов преступлений в электронных документах и иной электронной информации осуществляются специалистами или судебными экспертами. А затем они же представляют следователю свои заключения как доказательства по расследуемому уголовному делу. Однако при этом эксперты ссылаются не на экспертные методики, как это требует п. 9 ч. 1 ст. 204 УПК РФ, а на названия использованных ими компьютерных программ, чаще всего созданных иностранными фирмами.

При этом следователь фактически лишается возможности надлежащей проверки и оценки таких доказательств в соответствии с требованиями ст. 17, 87 и 88 УПК РФ. Это создает высокий уровень рисков признания таких доказательств недопустимыми прокурором и судом в соответствии с требованиями ст. 75 УПК РФ, что существенно затрудняет надлежащее расследование преступлений рассматриваемого вида.

Такая ситуация требует принятия срочных мер для ее исправления. Многие ученые предлагают ввести в уголовно-процессуальное законодательство новые виды доказательств — электронные, цифровые и даже виртуальные. Более того, во многих учебниках по цифровой криминалистике предлагается в качестве доказательств использовать цифровые или электронные следы преступлений. А в качестве научного обоснования таких «кардинальных» мер даются ссылки на необходимость применения «естественного» права — электронного, цифрового, компьютерного или экономического уголовного права, вместо исчерпавшего, по их мнению, свои возможности для развития «позитивного» права.

Понятно, что такие подходы имеют мало общего с фундаментальными принципами юридических наук и отражают лишь накопившиеся проблемы их развития в новых условиях перехода к информационному обществу и экономике знаний[1]. Но они способствуют формированию весьма необычных представлений о новых явлениях в современной преступности, широко исполь-

[1] Стратегия развития информационного общества Российской Федерации на 2017—2030 годы, утвержденная Указом Президента РФ от 9 мая 2017 года № 203.

зующей информационные технологии, не отражающих реальной картины происходящего. Это тормозит разработку в рамках действующего законодательства необходимого инструментария для расследования конкретных преступлений, совершенных с использованием информационных технологий,

Исследования особенностей современной преступности в сфере цифровой экономики и финансов показали, что возможности позитивного права еще далеко не исчерпаны[1]. А существенная часть проблем создания научного фундамента для борьбы с современным криминалом связана с инерцией сложившихся представлений в ряде наук уголовно-правового блока. Соответственно особенности мышления явно проявляются и в особенностях языка, на котором выражаются соответствующие идеи, а затем и общие установки лидеров соответствующих наук[2].

Проведенные исследования показали наличие ряда качественно новых проявлений современной преступности в сфере цифровой экономики и финансов, а также позволили выявить ряд факторов, обусловливающих ее высокую латентность. Среди них выделяется применение разнообразного программного обеспечения, с помощью которого осуществляется проникновение криминала в современные информационно-телекоммуникационные сети, информационные системы различного вида и назначения, отдельные компьютеры и компьютеризованные устройства. При этом часто отмечается низкий уровень защищенности граждан — потребителей услуг финансовых, торговых и сервисных организаций от воздействия на них со стороны криминала — как с помощью технических средств, так и на психологическом уровне.

Отмечается и ряд проблем выявления признаков преступных деяний в системе обязательственных прав на уровнях продавец — покупатель, заказчик — исполнитель, заемщик — кредитор. При этом договорные обязательства сторон нередко формулируются в виде настолько громоздкой системы условий, что следствию далеко не просто выявить в них признаки конкретных преступле-

---

[1] См.: *Волынский А.Ф., Прорвич В.А.* Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): Монография. М.: Экономика, 2019.

[2] См.: *Волынский А.Ф., Прорвич В.А.* Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: Монография. М.: Экономика, 2020.

ний. Ситуация еще более осложнилась с введением в действующее законодательство Федеральным законом от 18 марта 2019 г. № 34-ФЗ цифровых прав, отнесенных законодателем к имущественным правам. При этом соответствующие уголовно-правовые и уголовно-процессуальные нормы, обеспечивающие надлежащую защиту субъектов таких прав, которыми становится большая часть граждан России, разработаны не были.

Более того, в соответствии с новой редакцией ст. 128 и ст. 141.1 ГК РФ цифровые права представляют собой «обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы». Но законодателем не было введено никаких требований о соответствии таких правил требованиям действующего законодательства, не говоря уже об ответственности за их нарушение.

Аналогичные выводы следуют и в отношении положений о цифровых финансовых активах, введенных Федеральным законом от 31 июля 2020 г. № 259-ФЗ. Под таковыми было предложено понимать цифровые права, выпуск, учет и обращение которых возможны только путем внесения записей в информационную систему на основе распределенного реестра. Они могут быть объектом залога, сделок купли-продажи, обмена одного вида цифровых финансовых активов на другой (в том числе выпущенных по правилам иностранных информационных систем) или на цифровые права иных видов. При этом цифровые финансовые активы не являются и не признаются средством платежа.

К тому же правила информационных систем, в рамках которых субъекты принимают на себя обязательства в системе цифровых прав, далеко не всегда и не полностью соответствуют требованиям действующего законодательства. А правила иностранных информационных систем не только не соответствуют требованиям российского законодательства, но и способствуют причинению ущерба российским субъектам различного вида и уровня. Наиболее яркой иллюстрацией соответствующих преступлений, совершенных с использованием информационных технологий, стало «замораживание» российских золотовалютных резервов в размере свыше 300 млрд долл. США, а также конфискация вкладов в иностранных банках у ряда российских физических и юридических лиц.

При формировании доказательств и доказывании по преступлениям данного вида необходимо учитывать, что отражаются такие обязательства и права требования в рамках электронных документов, которые регистрируются и хранятся в информационных системах в закодированном с помощью определенных компьютерных программ виде. Поэтому с точки зрения следственной практики необходимо создание специального программного обеспечения, позволяющего не только визуализировать содержание соответствующих электронных документов и иной электронной информации, имеющей значение для уголовного дела, но и выявить в них закодированные информационные следы преступлений, совершенных с использованием информационных технологий.

Проведенные исследования показали, что при отсутствии положений уголовно-процессуального права, регламентирующих порядок самостоятельной работы следователя с электронными документами и формирования доказательств на их основе с помощью компьютерных программ, правовой основой для надлежащей организации таких следственных действий может стать само определение доказательства, установленное законодателем в ст. 74 УПК РФ. Однако для этого необходимо подойти к раскрытию его содержательных особенностей не только в рамках традиционных формулировок многочисленных комментариев к данной статье. Подход к анализу структуры и содержания определения доказательства с точки зрения основных подходов, характерных для науки информатики, позволяет обратить внимание на ряд его новых аспектов.

Прежде всего, речь идет о групповом анализе положений нескольких статей уголовно-процессуального законодательства, в той или иной степени связанных с данным понятием. Изучение прямых и обратных связей положений этих статей с точки зрения науки информатики позволяет формализовать основные элементы ряда алгоритмов, связывающих ряд процессуальных действий, при формировании доказательств по расследуемому уголовному делу. С помощью этих алгоритмов открываются принципиально новые возможности для установления важнейших содержательных особенностей предмета доказывания, а также определения пределов доказывания по преступлениям рассматриваемого вида.

То есть применение подходов, развитых в рамках науки информатики, к анализу определенных положений уголовно-процессуального законодательства и их совокупностей, включая их прямые и обратные связи, позволяет проявить тот потенциал, который имеет позитивное право для решения наиболее актуальных задач уголовно-правовой защиты информационного общества от атак современного криминала. При этом речь идет совсем не о замене юридических понятий на весьма популярные термины, связанные со всеобщей цифровизацией, затрагивающей и уголовное судопроизводство. Реализация потенциала уголовно-процессуального права с использованием возможностей наук информационного блока позволяет осовременить арсенал тех средств, которые необходимы для решения задач, стоящих перед правоохранительными органами.

Важно обратить внимание и на то, что инструментарий наук информационного блока основан на применении принципиально иного способа мышления по сравнению с юридическими науками уголовно-правового блока. Это наиболее отчетливо проявляется в том языке, который используется представителями данных наук. К примеру, юристами нередко используются такие логические конструкции, в рамках которых, с одной стороны, делается логически обоснованный вывод, но, с другой стороны, оговаривается, что речь может идти о совсем другом выводе. А при учете еще одного условия оба первоначально сделанных вывода нуждаются в пересмотре или уточнении.

Подробное обсуждение подобных логических конструкций, их связь с русским языком, правотворчеством и правоприменением выходят за рамки настоящей монографии. Необходимо лишь констатировать, что в рамках алгоритмических языков их логические конструкции неизменно приводят к единственному результату. А при изменении начальных условий получается другой, но также единственный результат.

Это открывает обширные возможности для моделирования противоправного поведения субъектов различного вида и уровня, а также для расчетов размера последствий совершенных преступлений рассматриваемого вида. Соответственно формирование алгоритмов процессуальных действий следователя на основе существующих уголовно-процессуальных норм с последующим сопоставлением их возможностей с результатами моделирования

деятельности криминала позволяет своевременно выявить имеющиеся правовые пробелы. На данной основе может быть значительно лучше выполнено обоснованное введение определенных корректировок и дополнений в действующее законодательство.

Соответствующий анализ содержательных особенностей определения доказательства в ст. 74 УПК РФ показывает, что любые доказательства как совокупность формализованных сведений о признаках преступления и обстоятельствах, подлежащих доказыванию, по сути, являются особым видом документированной информации. Именно эта информация позволяет доказать наличие в рассматриваемом деянии характеристик конкретного преступления, установленных действующим уголовным законодательством, в порядке, предусмотренным уголовно-процессуальным законодательством. Но для этого необходимо решить ряд конкретных задач не только по формированию необходимых доказательств, но и по приведению их к единому информационному формату, что обеспечивает выполнение их надлежащей проверки и оценки.

Для надлежащего решения конкретных задач по формированию доказательств и доказыванию в рамках расследования преступлений рассматриваемого вида нельзя забывать о цели, предмете и пределах доказывания по соответствующим уголовным делам. Важно учитывать, что цель доказывания состоит в установлении в определенном «подозрительном» деянии не только фактов и обстоятельств, перечисленных в ст. 73 УПК РФ, а всех обязательных и факультативных признаков состава преступления. В противном случае в соответствии с ч. 1 ст. 24 УПК РФ уголовное дело не может быть возбуждено, а возбужденное уголовное дело подлежит прекращению.

То есть достижение цели доказывания связано как с установлением фактических обстоятельств, так и с их юридической оценкой. Но если первое лежит в плоскости доказательственного права (доказано / не доказано), то второе — в плоскости уголовно-правовой квалификации (если доказано, то что из этого следует с точки зрения уголовного закона). Здесь важно подчеркнуть, что уголовное право и уголовно-процессуальное право неразрывно связаны, формируя единый правовой фундамент российского уголовного судопроизводства[1].

[1] См.: *Курс* уголовного процесса / Под ред. Л.В. Головко. М.: Статут, 2016.

Рассмотрение особенностей обстоятельств, подлежащих доказыванию, в системе понятий, характеризующих обязательные и факультативные признаки состава преступления, позволяет более детально раскрыть содержание предмета доказывания. Это имеет существенное значение уже на самой первой стадии анализа информации о возможном преступлении, которая необходима для обоснования процессуально выверенного решения о возбуждении уголовного дела либо об отказе в возбуждении уголовного дела.

В процессе сбора, проверки и оценки доказательств на различных этапах расследования уголовного дела необходимо учитывать, что данные понятия уголовно-процессуального права находятся в неразрывной взаимосвязи. В то же время эти элементы доказывания можно лишь разграничить по характеру производства соответствующих следственных и иных процессуальных действий и их целевой установке. При сборе и оценке доказательств речь идет об установлении ранее неизвестных сведений, а при проверке доказательств — об анализе уже установленных сведений. Вместе с тем эти следственные действия относят к собиранию доказательств, поскольку в рамках предварительного расследования следователь или дознаватель собирает доказательства в целях проверки ранее собранных и оценивает их, тем самым проверяя.

С точки зрения информатики речь идет о соответствующем выстраивании алгоритмов процессуальных действий с соответствующими прямыми и обратными связями. При этом нельзя забывать о том, что речь идет об алгоритмах преобразования документированной информации с особым, уголовно-правовым статусом. Поэтому при формировании таких алгоритмов необходимо предусматривать специальные процедуры, позволяющие контролировать сохранение правового статуса промежуточных и итоговых результатов обработки информации, имеющей уголовно-правовое значение.

При формировании юридических алгоритмов проверки и оценки доказательств необходимо учитывать их обозначенные выше взаимные связи. Первый способ проверки доказательств, установленный ст. 87 УПК РФ, — взаимное сопоставление доказательств — является одним из обязательных условий оценки совокупности доказательств, установленных ст. 88 УПК РФ. Второй способ — установление их источника — предполагается при оценке допустимости доказательства, а реализация третьего спо-

соба — получение новых доказательств — возможна только путем их собирания.

Но при создании алгоритма реализации первого из трех способов проверки доказательств, установленных ст. 87 УПК РФ, — сопоставления проверяемого доказательства с другими доказательствами по данному делу — возникает ряд проблем. Прежде всего, речь идет о сопоставлении доказательств, содержание которых представлено в принципиально различных «информационных форматах». По преступлениям, совершенным с использованием информационных технологий, это могут быть вещественные доказательства различного вида, протоколы допросов подозреваемых, потерпевших, свидетелей, а также заключения судебных экспертов и специалистов, исследовавших электронные документы и иную электронную информацию по поручению следователя.

Для их надлежащей проверки путем взаимного сопоставления следователю необходимо научиться извлекать из каждого доказательства любого вида, содержательные особенности которых отражены в соответствующих положениях ст. 76—84 УПК РФ, необходимую информацию уголовно-правового характера и приводить ее к единому формату. Кроме того, нельзя забывать и о цели доказывания — установлении всех обстоятельств, подлежащих доказыванию, а также обязательных и факультативных признаков состава преступления. В связи с этим возникает необходимость дифференциации процесса сопоставления доказательств по конкретным признакам состава преступления или, по крайней мере, по определенным группам признаков, относящихся к объекту, объективной стороне, субъекту и субъективной стороне состава преступления.

Подобные информационные технологии могут быть использованы и при выполнении следователем оценки каждого из собранных доказательств по критериям относимости, допустимости и достоверности, установленным ст. 88 УПК РФ. Это создает возможность применения проблемно ориентированных алгоритмов для установления достаточности собранной совокупности доказательств в соответствии с требованиями ч. 2 ст. 140, ч. 1 ст. 171 и ч. 1 ст. 215 УПК РФ, которые обсуждаются ниже.

Проведенные исследования особенностей преступлений, совершаемых с использованием информационных технологий, позволили выделить несколько групп таких преступлений, сущест-

венно различающихся не только по содержательным особенностям предмета доказывания, но и по степени сложности формализации его важнейших признаков. Это предполагает ряд особенностей в структуре и функциях разрабатываемых юридических алгоритмов, позволяющих надлежащим образом обрабатывать закодированную электронную информацию из материалов уголовного дела при формировании доказательств и доказывании по соответствующим уголовным делам.

К первой группе с определенной долей условности можно отнести те хорошо известные преступления, способ совершения которых связан с использованием информационных технологий, а в качестве орудий и средств совершения преступлений использованы компьютеры и иные компьютеризованные устройства. Среди них законодателем в качестве самостоятельных видов преступлений криминализовано мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), незаконная организация и проведение азартных игр (ст. 171.2 УК РФ), а также ряд других преступлений.

Для выявления и фиксации следов таких преступлений, а также формирования необходимых доказательств по соответствующим уголовным делам требуется применение достаточно сложных, проблемно ориентированных информационных технологий. Соответственно имеется ряд особенностей и в системе юридических алгоритмов, на основе которых могут быть сформированы высокотехнологичные методики расследования преступлений данного вида, а также специализированное программное обеспечение.

Ко второй группе можно отнести преступления, совершаемые с помощью компьютерных сетей и информационно-телекоммуникационных технологий. При этом нередко приходится сталкиваться с проявлениями различных видов множественности таких преступлений, и прежде всего совокупностей «обычного» преступления с преступлениями в сфере компьютерной информации (гл. 28 УК РФ).

Формализация предмета доказывания для данной группы преступлений и раскрытие его содержательных особенностей требуют раздельного анализа по каждому из видов преступлений, образующих совокупность, в том числе с учетом отмеченных выше

особенностей правоотношений субъектов цифровых прав, с последующими выводами, определяющими дальнейший ход их расследования. При этом важно установить прямые и обратные связи отдельных признаков каждого из этих преступлений, включая различные формы соучастия их субъектов.

Специфика их значительной части связана еще и с тем, что при подготовке и совершении преступлений данной группы используются информационно-телекоммуникационные сети, для управления которыми применяются средства системного программирования. Поэтому для считывания и декодирования той части электронной информации, которая связана с использованием компьютерных сетей, также требуется применение системного программного обеспечения, особенности которого рассматриваются ниже. Эти особенности должны учитываться и при создании на основе данных юридических алгоритмов специального программного обеспечения

К третьей группе можно отнести ряд новых и весьма сложных для надлежащего расследования видов преступлений, совершаемых с использованием информационных технологий в сфере цифровых прав в информационном пространстве компьютерных сетей. Прежде всего, речь идет о высоколатентных преступлениях, связанных с манипулированием рынком ценных бумаг, производных финансовых инструментов, иностранной валюты и различных товаров, предусмотренных ст. 185.3 УК РФ[1].

Важно учитывать, что в соответствии с положениями действующего законодательства эмиссионные ценные бумаги и производные ценные бумаги выпускаются в электронном виде и регистрируются в соответствующих информационных системах. Сделки с ними оформляются с помощью электронных документов, которые регистрируются и хранятся в информационных системах профессиональных участников фондового рынка, а затем передаются в подобные информационные системы для совершения транзакций по их оплате и переходу прав к покупателю.

То есть фактически речь идет о преступлениях против субъектов цифровых прав, совершаемых другими субъектами цифровых

[1] См.: *Прорвич В.А.*, *Опальский А.П., Иванов Е.В.* и др. Особенности уголовно-правовой характеристики преступлений, связанных с манипулированием рынком: Науч.-практ. пособие / Под ред. проф. В.А. Прорвича и проф. А.П. Опальского. М.: Альпен-Принт, 2021.

прав с использованием информационных технологий. При этом криминализация данных деяний была осуществлена законодателем еще в 2010 г., задолго до введения в действующее законодательство системы цифровых прав. Но соответствующие положения, регламентирующие следственные действия с электронными документами и иной электронной информацией, включая порядок использования определенных компьютерных программ для формирования доказательств по уголовным делам о преступлениях данного вида, в Уголовно-процессуальный кодекс РФ до сих пор не введены.

Анализ практического опыта выявления и фиксации признаков преступлений, связанных с манипулированием рынком[1], показал наличие серьезных неопределенностей, допущенных уже при формировании диспозиции данной уголовно-правовой нормы. Соответственно из-за этого возникает ряд неопределенностей при формировании предмета доказывания по преступлениям данного вида. Для их решения возникает необходимость разработки и применения определенных математических моделей, описывающих процессы ценообразования применительно к различным сегментам фондового рынка, а также деятельность различных видов субъектов — профессиональных участников рынка.

На основе данных математических моделей создается возможность для разработки юридических алгоритмов, позволяющих осуществить моделирование деятельности законопослушных субъектов рынка, в том числе с учетом неопределенностей рыночного ценообразования, и сформировать базы данных соответствующих информационных эталонов. На их основе обеспечивается возможность разработки юридических алгоритмов, позволяющих осуществить моделирование противоправной деятельности субъектов рынка различного вида.

Не менее серьезные проблемы возникают и при формировании юридических алгоритмов уголовно-процессуального характера, позволяющих выполнить надлежащее информационно-методическое сопровождение расследования преступлений, связанных с манипулированием рынком. Но высокий уровень неоп-

[1] См.: *Опальский А.П., Прорвич В.А., Гайворонская А.А.* и др. Уроки правоприменительной практики борьбы с манипулированием рынком: Науч.-практ. пособие / Под. ред. проф. А.П. Опальского. М.: Альпен-Принт, 2022.

ределенностей, характерных для фондового рынка, а также необходимость работы с электронной документацией создают неприемлемо высокий уровень рисков получения недопустимых доказательств из-за нарушения требований уголовно-процессуального законодательства. Поэтому при формировании алгоритмов уголовно-процессуального характера, нацеленных на надлежащее информационно-методическое обеспечение следственных действий по данной группе преступлений, необходимо особенно внимательно подходить к созданию их научно-правовых основ.

К четвертой группе можно отнести ряд наиболее сложных для надлежащего расследования видов преступлений, совершаемых с помощью специальных информационных технологий распределенного шифрования информации, которая получила название «блокчейн». Такие преступления также совершаются в сфере цифровых прав, в рамках определенных специализированных информационных систем по правилам, установленным их обладателями. При этом неотъемлемым атрибутом соответствующих деяний криминала в данной сфере является использование информационного пространства компьютерных сетей.

Пока подобные деяния не криминализованы, можно вести речь лишь об особенностях расследования, а также алгоритмах формирования доказательств и доказывании по некоторым «смежным» преступлениям, способ совершения которых связан с применением технологии блокчейн. К примеру, речь может идти о легализации (отмывании) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ), легализации (отмывании) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1 УК РФ), приобретении или сбыте имущества, заведомо добытого преступным путем (ст. 175 УК РФ), уклонении от исполнения обязанностей по репатриации денежных средств в иностранной валюте или в валюте Российской Федерации (ст. 193 УК РФ), коммерческом подкупе (ст. 204 УК РФ), а также о ряде других преступлений. Кроме того, подобный инструментарий может использоваться при финансировании экстремистской деятельности (ст. 282.3 УК РФ), получении взятки (ст. 290 УК РФ), даче взятки (ст. 291 УК РФ), посредничестве во взяточничестве (ст. 291.1 УК РФ) и многих других преступлениях.

Понятно, что в структуре алгоритма формирования развернутой уголовно-правовой характеристики таких преступлений или их совокупностей неизбежно возникновение «информационных разрывов», связанных с применением при их подготовке и совершении технологии блокчейн. Поэтому первоочередное внимание необходимо уделить информационным стыкам в области данных разрывов и анализу «скачкообразного» изменения информации на этих стыках.

Здесь речь идет о комплексном применении юридических алгоритмов не только уголовно-правового, но и уголовно-процессуального, а также криминалистического характера для установления содержательных особенностей предмета доказывания по соответствующим уголовным делам. Важную информацию можно получить с использованием специальных знаний судебных экспертов и специалистов на основе методического обеспечения, раскрывающего новые возможности соответствующих алгоритмов, в том числе реализующих ряд новых экономико-математических моделей.

Проведенные исследования показали, что для каждой из четырех групп преступлений, совершаемых с использованием информационных технологий, характерны принципиальные различия в формировании предмета и пределов доказывания, а также используемых при этом информационных технологий. При этом речь идет и о существенных различиях в структуре и взаимных связях тех юридических алгоритмов, которые могут использоваться для информационно-методического обеспечения следственных действий. В частности, были выделены следующие три основных направления исследований и разработок по созданию нового информационно-технологического инструментария наук уголовно-правового блока на основе соответствующих юридических алгоритмов.

1. В рамках *первого направления* речь идет о создании научно обоснованного и выверенного с правовой точки зрения алгоритмического инструментария для формирования развернутых характеристик предмета доказывания по уголовным делам о преступлениях, совершенных с использованием информационных технологий, по каждой из указанной выше групп таких преступлений. Для разработки научно обоснованных моделей каждого вида таких преступлений необходимо создание алгоритмов фор-

мирования их развернутых уголовно-правовых характеристик. Это позволит не только формализовать процессы выявления в рамках расследования таких преступлений всей совокупности их обязательных и факультативных признаков, но и раскрыть особенности всех обстоятельств, подлежащих доказыванию.

Но для надлежащего раскрытия особенностей бланкетных и смешанных диспозиций соответствующих уголовно-правовых норм приходится применять десятки и даже сотни положений гражданского и специального законодательства. Более того, нередко возникает необходимость применения положений регионального законодательства, а также многочисленных подзаконных актов. При этом применительно к особенностям формирования доказательств и доказывания по преступлениям рассматриваемого вида необходимо учитывать специфику той части действующего законодательства, которая регламентирует правоотношения субъектов различного вида и уровня в сфере цифровых прав, включая правила информационных систем различного вида и назначения.

С точки зрения информатики речь идет о формировании многомерной матрицы правовых норм, регламентирующих деятельность законопослушных субъектов с использованием самых разнообразных информационных технологий. С ее помощью можно выявить правонарушения в соответствующей сфере общественных отношений и получить их развернутую характеристику, позволяющую квалифицировать некоторые из них как преступления. При этом существенно повышается надежность идентификации каждого из признаков состава конкретного преступления рассматриваемого вида.

Безусловно, в рамках алгоритмов применения соответствующих многомерных матриц важнейшее значение имеет надлежащее осуществление перманентного контроля за тем, чтобы сформированные таким образом развернутые уголовно-правовые характеристики преступлений любой из четырех групп не выходили за рамки уголовного права. Организация соответствующего контроля на уровне алгоритмов с использованием системы критериев, сформированных на основе важнейших принципов уголовного и уголовно-процессуального права, позволит получить выверенные с правовой точки зрения результаты.

2. В рамках *второго направления* речь идет о формировании алгоритмов выполнения процессуальных действий, предусмотренных действующим законодательством, при расследовании преступлений, совершенных с использованием информационных технологий, отнесенных к любой из четырех групп. Что касается структурных и содержательных особенностей алгоритмов применения положений уголовно-процессуального права, то необходимо еще раз отметить ключевое значение понятия «доказательство», заложенное в их основу. Как уже отмечалось, при его определении законодатель в ст. 74 УПК РФ использовал в первую очередь понятие «сведения», неразрывно связанное с понятием «информация» в соответствии со ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ в действующей редакции.

Вместе с тем доказательствами по уголовному делу признаются только те сведения, которые позволяют установить наличие или отсутствие обстоятельств, подлежащих доказыванию (ст. 73 УПК РФ), а также иных обстоятельств, имеющих значение для уголовного дела (ст. 24 УПК РФ). То есть речь идет об информации, имеющей правовой статус и позволяющей установить наличие либо отсутствие в определенном деянии признаков состава конкретного преступления. При этом в ст. 24 УПК РФ установлен прямой запрет на расследование уголовного дела при отсутствии в деянии состава преступления.

Важно обратить внимание и на вторую часть определения понятия «доказательство», установленного ст. 74 УПК РФ, в рамках которой определенная в его первой части информация уголовно-правового характера может быть получена только из строго определенных в законе источников, закрытый перечень которых приведен в ч. 2 ст. 74 УПК РФ.

То есть понятие «сведения» отражает содержательную сторону доказательства (материальный аспект), а понятие «источник» — формальную сторону доказательства (формальный аспект). При этом доказательство существует только при наличии единства сведения и источника, т.е. оно требует обязательного одновременного присутствия как формальной, так и материальной (содержательной) стороны, а сведения должны иметь строго оговоренное содержание и могут быть получены только в порядке, установленном настоящим Кодексом.

Применительно к рассматриваемым процессам формирования и использования юридических алгоритмов важно обратить внимание на использованное в Законе об информации понятия «документирование», связанное с необходимостью присвоения документированной информации определенных реквизитов. При этом было указано, что обладателем информации является лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (конституционно-правовой смысл данного понятия раскрыт в постановлении Конституционного Суда РФ от 26 октября 2017 г. № 25-П). Анализ данных положений показывает, что в контексте формирования именно документированной информации при расследовании преступлений рассматриваемого вида они прямо относятся к полномочиям следователя, установленным действующим законодательством.

Таким образом, применительно к содержательным особенностям алгоритмов уголовно-процессуальных действий, нацеленных на получение документированной информации, а затем формировании на ее основе необходимых доказательств, следует вывод не только об их сложной, иерархически организованной структуре. В рамках данной структуры органически соединяются алгоритмы обработки документированной информации, которые регламентируются как уголовным, так и уголовно-процессуальным законодательством. Столь сложная и, по сути, комплексная регламентация преобразования документированной информации и создания новой информации при формировании необходимых доказательств по конкретным уголовным делам требует привлечения для разработки таких алгоритмов ученых-юристов, обладающих к тому же профессиональными знаниями высокого уровня в сфере информатики.

Не менее важна разработка алгоритмов уголовно-процессуальных действий, нацеленных на выполнение надлежащей проверки и оценки каждого из доказательств по соответствующим уголовным делам. При этом необходимо раскрыть содержательные особенности критериев оценки доказательств относимости, допустимости и достоверности, установленных ст. 88 УПК РФ. Особого внимания требуют алгоритмы установления достаточности собранной совокупности доказательств по уголовным делам

применительно к преступлениям, отнесенным к каждой из перечисленных выше четырех групп.

Необходимо подчеркнуть, что такие алгоритмы должны нацеливаться не на «автоматизированную» обработку информации, а на организацию интерактивного режима ее обработки, причем с обязательным участием юриста, обладающего необходимыми профессиональными компетенциями, либо нескольких юристов в многопользовательском режиме. Это обеспечивает возможность учета ряда практических ситуаций, когда заранее сформированных критериев автоматической оценки полученных результатов может оказаться недостаточно.

То есть не только ряд содержательных особенностей, но и организация интерактивного многоэтапного контроля процесса обработки документированной информации со стороны профессиональных юристов позволяет характеризовать данные алгоритмы как юридические. Соответственно возникает необходимость использования специального юридического алгоритмического языка не только при их разработке, но и последующей практической реализации в виде специального, проблемно ориентированного программного обеспечения.

3. В рамках *третьего направления* речь идет о формировании алгоритмов научно-методического и информационного обеспечения надлежащего применения специальных знаний для получения необходимых доказательств при расследовании уголовных дел о преступлениях, совершенных с использованием информационных технологий. Анализ положений более 20 статей Уголовно-процессуального кодекса РФ показывает, что их совокупное применение позволяет признать судебную экспертизу в качестве одного из институтов уголовно-процессуального права.

Главная цель данного института — получение необходимых доказательств по уголовным делам с помощью специальных знаний сведущих лиц — судебных экспертов, облеченных в строгую процессуальную форму. Ключевую роль в надлежащем применении возможности данного института для формирования значительной части доказательств по преступлениям рассматриваемого вида играет система парных отношений основных субъектов данного института. И для надлежащего формирования необходимых доказательств и доказывания по преступлениям, совершенным с

использованием информационных технологий, этот институт играет критически важную роль.

Первый из субъектов парных отношений в рамках данного института — *следователь* — не только назначает судебную экспертизу и конкретного эксперта или нескольких экспертов в случае возникновения такой необходимости в соответствии со ст. 200 и 201 УПК РФ, но и ставит экспертные задачи в виде вопросов к эксперту, формирует объект экспертизы из материалов уголовного дела в соответствии со ст. 195 УПК РФ. После передачи ему заключения эксперта следователь обязан выполнить его проверку и оценку как доказательства по расследуемому уголовному делу в соответствии с требованиями ст. 17, 87 и 88 УПК РФ.

Для этого ему предоставлено право допрашивать судебного эксперта, причем показания эксперта после их проверки и оценки также могут использоваться в качестве доказательства в соответствии с п. 3 ч. 2 ст. 74 УПК РФ. Кроме того, для проверки и оценки соответствующих доказательств следователь вправе привлекать специалиста, обладающего специальными знаниями в той же области. А в случае возникновения сомнений и новых вопросов он вправе назначить дополнительную или повторную судебную экспертизу.

Второй субъект парных отношений — *судебный эксперт*, получив постановление о назначении судебной экспертизы, материалы уголовного дела и дав подписку об уголовной ответственности за дачу заведомо ложного заключения, обязан не только выполнить необходимые экспертные исследования этих материалов, но и обосновать выводы по поставленным перед ним вопросам. А при оформлении заключения эксперта он обязан указать в нем на примененные им экспертные методики.

Однако, как показывают результаты проведенных исследований, ключевой проблемой является грубое нарушение многими экспертами указанного требования, когда вместо экспертной методики они ссылаются на иностранные названия использованных ими компьютерных программ. В некоторых случаях они дополнительно ссылаются на то, что данные программы сертифицированы. Но сертификация компьютерных программ для целей получения доказательств, не говоря уже о целях проверки и оценки таких доказательств, в уголовном судопроизводстве пока еще не производится.

В результате фактически второй субъект парных отношений рассматриваемого института — судебный эксперт — сам нарушает требования соответствующих статей Уголовно-процессуального кодекса РФ, что в соответствии со ст. 75 УПК РФ переводит его заключение в разряд недопустимых доказательств. Более того, он лишает первого субъекта парных отношений — следователя — возможности выполнить его обязанности по проверке и оценке каждого доказательства по расследуемому им уголовному делу. Но при этом возникают основания и для признания подобных заключений эксперта заведомо ложными, что может привести к уголовной ответственности эксперта.

Вместе с тем изучение причин сложившейся ситуации, тормозящей надлежащее формирование доказательств и доказывания по уголовным делам о преступлениях, совершенных с использованием информационных технологий, показывает следующее. Критически важной и нерешаемой много лет проблемой является создание экспертных методик, позволяющих выполнять исследование электронных документов и иной электронной информации, имеющей значение для уголовного дела, с надлежащим использованием определенных компьютерных программ.

Учитывая специфику предмета доказывания по преступлениям рассматриваемого вида, важно обратить внимание на то, что в рамках экспертных методик производится последовательное описание каждой процедуры преобразования исходной информации. То есть фактически речь идет об оригинальном алгоритме преобразования документированной информации, имеющей уголовно-правовой статус, нацеленном на решение конкретных экспертных задач, поставленных следователем. Именно такой подход к формированию экспертных методик как алгоритмов выполнения в последовательно-параллельном режиме определенных операций по преобразованию документированной информации, имеющейся в материалах уголовного дела и отобранной следователем в качестве объекта судебной экспертизы, описан в ряде известных публикаций[1].

Соответственно для форсирования работ по созданию необходимых экспертных методик, позволяющих получать значитель-

[1] См.: *Судебно-экономическая* экспертиза в уголовном процессе / Под ред. А.Ф. Волынского и В.А. Прорвича. 2-е изд., перераб. и доп. М.: Экономика, 2021.

ную часть доказательств по преступлениям, совершенным с использованием информационных технологий, необходимо формирование комплекса юридически выверенных алгоритмов проблемно ориентированного преобразования сведений из электронных документов и иной информации, имеющейся в соответствующих уголовных делах. Для этого возможно применение матричного подхода формирования экспертных методик применительно к той совокупности экспертных задач, которые ставятся следствием при формировании необходимых доказательств по конкретным уголовным делам о преступлениях рассматриваемого вида[1].

Разработка комплекса алгоритмов проблемно ориентированной обработки сведений, содержащихся в электронных документах и иной электронной информации из материалов конкретного уголовного дела с помощью специальных знаний судебных экспертов, позволяет не только продвинуться в создании остро необходимых экспертных методик. Каждый из данных алгоритмов может быть реализован для практического применения в виде текста соответствующей компьютерной программы. Наборами таких проблемно ориентированных компьютерных программ могут быть оснащены интерактивные экспертные системы, позволяющие эксперту в диалоговом режиме не только применять эти программы, но и фиксировать результаты такого применения в специальном протоколе.

Описания соответствующих алгоритмов обработки электронной информации из материалов уголовного дела, наборы проблемно ориентированных компьютерных программ, описание структуры и алгоритмов работы соответствующих экспертных систем и протоколы применения конкретных программ для обработки информации, имеющей уголовно-правовой статус, создают прочный научный фундамент для формализации текстов необходимых экспертных методик. Это существенно упрощает и те процедуры, которые необходимы для придания им необходимого правового статуса. Но не менее важно и то, что следователь мо-

[1] См.: *Прорвич В.А., Семенова Е.А.* Матричный подход к формированию частных экспертных методик для получения доказательств при расследовании криминальных банкротств // Проблемы экономики и юридической практики. Т. 15. № 1. 2019. С. 212—215.

жет использовать перечисленные выше части таких экспертных методик для проверки и оценки заключений экспертов, полученных с использованием соответствующих компьютерных программ.

Что касается информационно-методического обеспечения процесса доказывания при расследовании уголовных дел о преступлениях рассматриваемого вида, то для этого разработан ряд юридических алгоритмов, позволяющих не только обеспечить надлежащее выполнение следственных действий в рамках предмета доказывания. Специальная система алгоритмов позволяет осуществить информационную поддержку следственных действий по установлению пределов доказывания по уголовным делам о преступлениях, совершенных с использованием информационных технологий.

В основе данной системы алгоритмов лежат положения ст. 17 УПК РФ, конкретизированные в ч. 1 ст. 88 УПК РФ в части установления критерия достаточности собранной совокупности доказательств. Но содержательные особенности этого критерия законодателем не были раскрыты, оставляя его практическую реализацию на внутреннее убеждение следователей, дознавателей, прокуроров, судей и присяжных заседателей. И это притом, что на разных стадиях досудебного производства содержание данного критерия имеет существенные различия.

В ч. 2 ст. 140 УПК РФ законодатель указал в качестве основания для возбуждения уголовного дела на «наличие достаточных данных, указывающих на признаки преступления». Здесь прямо указано на необходимость раскрытия критерия достаточности, используемом в уголовно-процессуальном праве, с применением положений уголовного права.

Еще более явно об этом сказано в ст. 24 УПК РФ, где в качестве критериев, ограничивающих процесс доказывания по уголовному делу, были прямо использованы уголовно-правовые понятия «событие преступления» и «состав преступления». Более того, здесь законодатель прямо оговорил невозможность возбуждения уголовного дела либо его прекращение в случае отсутствия события или состава преступления.

Развивая эти положения, важно обратить внимание на то, что в уголовном праве для установления наличия в определенном деянии состава преступления выполняется его квалификация. При этом в процессе квалификации преступления происходит форми-

рование системы «юридических тождеств», в рамках которых производится сопоставление характеристик квалифицируемого деяния с обязательными и факультативными признаками состава конкретного преступления. Если обнаруживается отсутствие в квалифицируемом деянии хотя бы одного признака состава преступления, то в соответствии со ст. 8 УК РФ делается вывод об отсутствии в нем всего состава преступления.

Такой подход для установления достаточности собранной совокупности доказательств на различных стадиях досудебного производства был впервые использован в качестве основы соответствующих алгоритмов процессуального доказывания в книге, подготовленной большим коллективом авторов под общей редакцией А.И. Бастрыкина[1]. Для его практической реализации созданы различные варианты алгоритмов процессуально регламентированных действий, позволяющих сформировать юридическое тождество, используемое для квалификации преступления, а затем последовательно его детализировать, преобразовав в развернутую систему юридических тождеств. Вторая система юридических тождеств формируется на основе перечня обстоятельств, подлежащих доказыванию, перечисленных в ст. 73 УПК РФ.

Соответствующие алгоритмы формирования системы двойных юридических тождеств, их последовательной детализации по всем обязательным и факультативным признакам состава конкретного преступления, а также по обстоятельствам, подлежащим доказыванию, и уточнения содержательных особенностей каждой из составляющих данных тождеств успешно используются для уточнения пределов доказывания по конкретным уголовным делам[2].

На стадии решения вопроса о возбуждении уголовного дела либо об отказе в его возбуждении надлежащее формирование внутреннего убеждения следователя в соответствии со ст. 17 УПК РФ вряд ли возможно. Речь идет о том, что при наличии явных

---

[1] См.: *Организация* и методика расследования отдельных видов экономических преступлений / Под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: Спутник+, 2016.

[2] См.: *Новиков А.М., Прорвич В.А.* Доказательства и доказывание в следственной практике: Учеб. пособие. М.: Моск. акад. Следственного комитета России, 2022.

информационных пробелов из-за отсутствия необходимых данных в первоначально сформированной системе юридических тождеств в соответствии с ч. 2 ст. 140 УПК РФ следователь мысленно пытается заполнить их, предполагая успех своих будущих действий по формированию совокупности необходимых доказательств в рамках расследования уголовного дела.

То есть его внутреннее убеждение формируется в рамках подходов, близких к риск-менеджменту, когда лицо принимает решение в условиях информационной неопределенности. На первом шаге производится максимальная формализация рисков, затем принимаются организационные решения по их снижению, после чего осуществляются меры по покрытию оставшихся рисков.

Подобная ситуация возникает и при применении критерия достаточности собранной совокупности доказательств для обоснования решения о предъявлении обвинения подозреваемому лицу в соответствии с ч. 1 ст. 171 УПК РФ. Поскольку после предъявления обвинения расследование уголовного дела не заканчивается, а следственные действия по сбору новых доказательств продолжаются, то здесь также приходится сделать вывод о принятии решения в условиях информационной неполноты соответствующей системы юридических тождеств. Правда, структура и содержание рисков, характеризующих данное решение следователя и его обоснование, существенно отличаются от ситуации, связанной с принятием решения о возбуждении уголовного дела.

Наконец, в соответствии с положениями ч. 1 ст. 215 УПК РФ для принятия решения об окончании предварительного следствия следователю необходимо установить достаточность собранной совокупности доказательств по расследованному уголовному делу. Для этого ему также необходимо сформировать развернутые системы юридических тождеств, подобные описанным выше. Однако при их анализе используются совсем другие критерии.

Прежде всего, в данных завершающих системах юридических тождеств уже не должно быть информационных пробелов и противоречий. При их наличии предварительное следствие должно быть продолжено, причем речь идет не только о заполнении выявленных информационных пробелов с помощью новых доказательств. Как уже отмечалось, в рамках параметрического анализа собранной совокупности доказательств по критерию относимости создается

возможность установления их распределения по различным признакам состава преступления. Это позволяет выявить слабые места в собранной совокупности доказательств с учетом их локальной информационной избыточности либо локальной информационной недостаточности, чтобы принять необходимые меры по получению недостающих доказательств и анализу «лишних» доказательств.

При выявлении информационной избыточности в соответствующем юридическом тождестве необходимо выполнение анализа содержательных особенностей «лишних» доказательств, не соответствующих определенным признакам состава конкретного преступления либо обстоятельствам, подлежащим доказыванию. После этого необходимо формирование новых систем юридических тождеств на основе состава другого, «смежного» преступления либо двух преступлений. По результатам выполнения уже описанных выше алгоритмов установления достаточности собранной совокупности доказательств следователь получает возможность уточнить, о каком именно преступлении или совокупности преступлений идет речь, и принять соответствующие процессуальные решения.

Кроме того, важно обратить внимание и на «качество» отдельных доказательств, из-за которого информационные пробелы в сформированной системе юридических тождеств могут возникнуть при проверке и оценке собранной совокупности доказательств прокурором и судом.

Необходимо подчеркнуть, что создание на основе описанных юридических алгоритмов комплекса проблемно ориентированных компьютерных программ не только позволяет существенно продвинуться в формировании необходимых доказательств при расследовании преступлений, совершенных с использованием информационных технологий, но и выполнить их проверку и оценку. Данные подходы позволяют реализовать установки высшего руководства страны по форсированному созданию отечественного программного обеспечения для критически важных сфер нашего государства. При этом создаются и принципиально новые возможности для создания государственной системы сертификации компьютерных программ применительно к нуждам уголовного судопроизводства.

Важно также обратить внимание на то, что описанная выше система из нескольких десятков видов юридических алгоритмов и

способов их формирования и применения позволяет конкретизировать информационно-методическое обеспечение по каждому из видов преступлений, совершенных с использованием информационных технологий. При этом могут быть использованы и элементы ИИ на основе нейросетевых алгоритмов, гипертекстовых технологий, инженерии знаний и т.п.[1]

Практическая реализация рассмотренной системы алгоритмов предполагает использование соответствующих компьютерных программ. С технической точки зрения написание текстов соответствующих программ и их отладка не представляют особой сложности. Для этого могут быть использованы стандартизованные программные модули, а также компьютерные роботы на основе ИИ.

Но решающее значение имеют отладка таких программ и их последующее тестирование, для того чтобы убедиться, что созданная компьютерная программа позволяет выполнить все процедуры преобразования исходной документированной информации в рамках соответствующих юридических алгоритмов. Кроме того, существенное значение имеет практическая реализация средств программного контроля за сохранением правового статуса промежуточных и итоговых результатов обработки электронной информации из материалов уголовного дела в интерактивном режиме.

Особую роль такая организация работ по формированию необходимых доказательств и доказыванию играет в рамках использования не только прикладного, но и системного программного обеспечения для борьбы с преступлениями, совершенными с использованием информационных технологий и информационно-телекоммуникационных сетей. В «Большой российской энциклопедии» системное программирование определяется как раздел программирования, в котором сочетаются исследования новых архитектур, алгоритмов, структур данных и др., а также деятельность по проектированию, разработке, тестированию и сопровождению (поддержке) системного программного обеспечения (СПО), т.е. для создания новых информационных технологий. СПО является фун-

[1] См.: *Бычков В.В., Прорвич В.А.* Алгоритмы взаимодействия следователей с искусственным интеллектом в ходе раскрытия и расследования преступлений экстремистского характера, совершаемых с использованием Интернета // Правопорядок: история, теория, практика. 2021. № 2 (29). С. 92—98.

даментом, на котором базируется все программное обеспечение (ПО) компьютеров. При этом различают СПО машинно-зависимое (предназначено для использования в семействах компьютеров с одной и той же системой команд) и переносимое (portable), используемое на компьютерах с разной архитектурой. СПО применяют для управления ПО компьютеров и сетевыми коммуникациями, а также для поддержки выполнения прикладных программ.

К СПО относятся операционные системы (ОС), программные средства организации компьютерных сетей и управления ими, системы управления базами данных (СУБД), средства промежуточного ПО (предоставляют выделенному классу приложений набор услуг, напрямую не предоставляемой ОС), инструментальные средства разработки и анализа программ, поддержки информационной безопасности и др. При разработке СПО используются методы программной инженерии; особое внимание уделяется качеству кода (включает минимизацию числа ошибок, простоту понимания и сопровождения, хорошую документированность и т.п.), надежности и безопасности программ[1].

Даже столь краткое изложение основ системного программирования помогает сделать однозначный вывод, что на основе описанной системы алгоритмов в кратчайшие сроки может быть создано соответствующее проблемно ориентированное программное обеспечение, включая СПО. В рамках правоприменения оно позволит следователю обеспечить формирование информационно полной системы обязательных и факультативных признаков конкретного преступления рассматриваемого вида, а также обстоятельств, подлежащих доказыванию, раскрывающих предмет доказывания по соответствующим уголовным делам. На этой основе обеспечивается возможность формирования системы необходимых доказательств, их надлежащей проверки и оценки, включая установление достаточности собранной совокупности доказательств.

Кроме того, использование данных компьютерных программ создает ряд новых возможностей для анализа имеющихся данных о преступных деяниях с использованием информационных технологий, совершенных за последние годы. На основе их сопоставления с системой признаков каждого из преступлений, рассмот-

[1] См.: *Кузнецов С.Д.* Системное программирование // Большая российская энциклопедия: В 35 т. Т. 30. М.: Большая российская энциклопедия, 2015. С. 301.

ренного судом, можно сформировать обширные массивы «информационных эталонов» совершенных преступлений для всех указанных выше четырех групп. С их помощью следователь сможет получить важную ориентирующую информацию при расследовании конкретного уголовного дела, а также использовать необходимое методическое обеспечение.

С другой стороны, исследование архивных уголовных дел, расследование которых было приостановлено, с применением указанных выше «информационных эталонов» позволит установить конкретные причины этого. Соответственно в результате могут быть внесены необходимые корректировки в использованное ранее методическое обеспечение. Кроме того, могут быть выявлены причины повышенной латентности таких преступлений, а также сформулированы конкретные предложения по внесению изменений и дополнений в действующее уголовное и уголовно-процессуальное законодательство.

Список литературы

1. *Барабаш А.С., Скоблик К.В.* Основание принятия решений в российском уголовном процессе: Монография. М.: Юрлитинформ, 2020.
2. *Волынский А.Ф., Прорвич В.А.* Компьютерная криминалистика в системе уголовно-правовой защиты «традиционной» и цифровой экономики: Монография. М.: Экономика, 2020.
3. *Волынский А.Ф., Прорвич В.А.* Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): Монография. М.: Экономика, 2019.
4. *Концепция* построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий (ГАС «Доступ к правосудию»): Монография / Отв. ред. Л.Н. Масленникова. М.: Норма — Инфра-М, 2022.
5. *Новиков А.М., Прорвич В.А.* Доказательства и доказывание в следственной практике. М.: Моск. акад. Следственного комитета России, 2022.
6. *О некоторых* вопросах применения судами Конституции Российской Федерации при осуществлении правосудия: постановление Пленума Верховного Суда Российской Феде-

рации от 31.10.1995 № 8 // СПС «КонсультантПлюс» (дата обращения: 17.03.2023).
7. *О практике* рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ): постановление Пленума Верховного Суда Российской Федерации от 01.06.2017 № 19 // СПС «КонсультантПлюс» (дата обращения: 17.03.2023).
8. *О Стратегии* развития информационного общества в Российской Федерации на 2017—2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203 // Президент России: официальный сайт. URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 13.03.2023).
9. *Об отказе* в принятии к рассмотрению жалобы гражданина Прозоровского Д.А. на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ: Определение Конституционного Суда Российской Федерации от 25.01.2018 № 189-О // СПС «КонсультантПлюс» (дата обращения: 15.03.2023).
10. *Об отказе* в принятии к рассмотрению жалобы гражданина Тимофеева В.В. на нарушение его конституционных прав частью шестой статьи 164 УПК РФ: Определение Конституционного Суда РФ от 31.05.2022 № 1366-О // СПС «КонсультантПлюс» (дата обращения: 15.03.2023).
11. *Опальский А.П., Прорвич В.А., Иванов Е.В.* и др. Уроки правоприменительной практики борьбы с манипулированием рынком: Науч.-практ. пособие / Под. ред. проф. А.П. Опальского. М.: Альпен-Принт, 2022.
12. *Организация* и методика расследования отдельных видов экономических преступлений / Под ред. А.И. Бастрыкина, А.Ф. Волынского, В.А. Прорвича. М.: Спутник+, 2016.
13. *Собирание* электронных доказательств по уголовным делам на территории России и зарубежных стран: Монография / Под общ. ред. С.П. Щербы. М.: Проспект, 2022.
14. *Способы* получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: Учеб. пособие / Под общ. ред. Б.Я. Гаврилова. М.: Проспект, 2017.
15. *Электронные* доказательства в уголовном судопроизводстве: Учеб. пособие / Под общ. ред. С.В. Зуева. М.: Юрайт, 2023.

Глава 4

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

4.1. Теория и практика расследования преступлений, совершенных с использованием информационных технологий, следственными органами Следственного комитета Российской Федерации

О.Ю. Антонов[1], Т.А. Сааков[2]

Среди отечественных ученых-криминалистов до сих пор продолжаются дискуссии об определении природы следов, образованных путем использования информационных технологий.

Так, В.А. Мещеряков, как и ряд других исследователей, предлагает назвать новый вид следов в криминалистике, образующихся компьютерными средствами и системами, *виртуальными следами*[3]. В.А. Мещеряков утверждает, что виртуальные следы по своей сути приближены к материальным следам, ввиду того что существуют реально на материальном носителе, но в то же

---

[1] Олег Юрьевич Антонов — декан факультета подготовки криминалистов Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.

[2] Тигран Артемович Сааков — старший преподаватель кафедры судебно-экспертной и оперативно-розыскной деятельности Московской академии Следственного комитета Российской Федерации, кандидат юридических наук.

[3] См.: *Агибалов В.Ю.* Виртуальные следы в криминалистике и уголовном процессе: монография. М., 2012; *Мещеряков В.А.* «Виртуальные следы» под «скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1 (4). С. 28—33; *Смушкин А.Б.* Виртуальные следы в криминалистике // Законность. 2012. № 817. С. 43—45.

время их обнаружение и изъятие возможны только с применением программно-технических средств, так как непосредственно они восприниматься не могут. При этом он отмечает, что виртуальные следы нельзя включить в состав материальных следов, так как их природа отчасти субъективна, что проявляется в специфике способа их считывания при отсутствии устойчивой корреляции с устройством, на которое осуществлялась запись информации, ввиду чего данные следы неустойчивы, что приближает их к идеальным следам. Однако идеальными виртуальные следы не являются, так как хранятся не в памяти человека, а на материальных объектах[1].

С таким подходом, по нашему мнению, никак нельзя согласиться. В криминалистике огромное количество следов может быть обнаружено, а в последующем изъято только при помощи технико-криминалистических средств, что и позволило ввести в криминалистику устойчивую классификацию следов по такому основанию, как степень различимости: *видимые*, *слабовидимые* и *невидимые* следы. Причем некоторые материальные следы могут быть весьма неустойчивы, недоступны непосредственному восприятию, могут зависеть от способа считывания, например пахнущие следы человека, следы сотен тысяч различных веществ и т.п.

Как и многие другие авторы, мы полагаем, что виртуальных следов не может быть в принципе, а описываемые следы являются материальными, поскольку зафиксированы на материальных носителях путем изменения свойств или состояния отдельных их элементов[2].

Ряд других отечественных исследователей для обозначения следов, сопряженных с использованием информационных технологий, предлагают термин «*электронные следы*». Так, по мнению В.Б. Вехова, электронные доказательства — это любые сведения (сообщения, данные), представленные в электронной форме, на основе которых суд, прокурор, следователь, дознаватель в определенном процессуальным законодательством порядке устанавливают наличие или отсутствие обстоятельств, под-

[1] См.: *Мещеряков В.А.* Указ. соч.

[2] См.: *Россинская Е.Р., Семикаленова А.И.,. Рядовский И.А, Сааков Т.А*. Теория информационно-компьютерного обеспечения криминалистической деятельности. М.: Проспект, 2022.

лежащих доказыванию при производстве по делу, а также иных обстоятельств, имеющих значение для правильного рассмотрения и разрешения дела[1].

Позволим себе не согласиться и с данной позицией, так как процессором электронно-вычислительных мощностей (ЭВМ) могут обрабатываться цифровые данные, которые вовсе не обязательно должны быть представлены в форме электрических сигналов. Так, например, QR-код, включающий в себя стандартизированные режимы кодирования (числовой, буквенно-цифровой, двоичный, кандзи), может быть зафиксирован не на электронном, а на ином носителе информации (бумаге, дереве, полимере и др.), т.е. в данном случае от цифровой информации (QR-кода) не будет исходить каких-либо электрических сигналов, но эта цифровая информация также может быть обработана любым электронным устройством (ноутбуком, смартфоном, электронным планшетом), позволяющим произвести декодирование QR-кода.

Полагаем, что следует разграничивать *компьютерную информацию*, которая может быть выражена как в аналоговом, так и в цифровом формате, но которая при этом должна подлежать обработке процессором электронно-вычислительных мощностей (компьютеров), и *цифровую информацию*, которая может быть обработана как при помощи электронно-вычислительной техники (жесткие диски, USB-флеш-накопители, CD-диски и др.), так и без нее (например, декодирование QR-кода может быть проведено лицом, обладающим специальными знаниями в соответствующей области, и без использования электронно-вычислительной техники)[2].

В свою очередь, А.Г. Себякин определяет след в компьютерной системе как *электронно-цифровой след*, который представляет собой компьютерные данные, содержащие криминалистически значимую информацию о событиях или действиях, отраженные в материальной среде. Однако термин «электронно-цифровые следы», предложенный А.Г. Себякиным, вряд ли можно признать

---

[1] См.: *Вехов В.Б.* Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. № 4 (11). С. 46—50.

[2] См.: *Россинская Е.Р., Сааков Т.А.* Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 106—123.

удачным, так как понятием «электронно-цифровые следы» охватываются далеко не все следы преступлений, которые были образованы при помощи использования электронно-вычислительных мощностей, о чем было сказано выше.

Вместе с тем интерес представляет механизм следообразования, предложенный А.Г. Себякиным, в соответствии с которым пользователь как отражаемый объект опосредованно воздействует на компьютерную систему, являющуюся отражающим объектом. Средством отражения является совокупность команд (логический уровень), сигналов электромагнитной природы (физический уровень). Компьютерные команды могут быть инициированы как самим объектом отражения (пользователем), так и транслированы посредством прикладного программного обеспечения, являющегося элементом средства отражения на логическом уровне. В качестве следообразующего объекта выступает системное программное обеспечение, следовоспринимающим объектом является массив памяти устройства[1].

Согласно теории информационно-компьютерного обеспечения криминалистической деятельности, разработанной Е.Р. Россинской, Т.А. Сааковым, А.И. Семикаленовой, И.А. Рядовским, следы, сопряженные с использованием информационных технологий, целесообразно обозначать как цифровые следы[2].

Данный подход представляется нам более удачным, так как указанный коллектив авторов рассматривает, во-первых, цифровые следы как имеющие исключительно материальную природу происхождения; во-вторых, отсутствует привязка данных следов к форме электрических сигналов (электронных или электронно-цифровых доказательств).

Наряду с этим следует сказать, что цифровые следы в зависимости от специфики их судебно-экспертного исследования могут быть расклассифицированы. Подтверждение сказанному находим в высказываниях Т.А. Саакова, который отмечает, что «объекты различных родов (видов) экспертиз все чаще пре-

---

[1] См.: *Себякин А.Г.* Механизм следообразования в компьютерных системах с точки зрения теории отражения // Сибирские уголовно-процессуальные и криминалистические чтения. 2021. № 2 (32). С. 89—99.

[2] См.: *Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А.* Указ. соч.

доставляются для производства экспертизы на цифровом носителе информации. При этом следует отметить, что если объектом судебной компьютерно-технической экспертизы выступают непосредственно сами цифровые следы, которые несут в себе значимую для органов следствия информацию, то объекты различных родов (видов) экспертиз предоставляются для производства экспертизы на электронно-цифровом носителе информации»[1].

Действительно, с данным утверждением сложно не согласиться, так как в одном случае цифровой след выступает результатом фиксации какой-либо криминалистически значимой информации на материальном носителе в цифровом формате (например, жесткий диск, на котором содержится видеозапись с камер наружного наблюдения), в другом — цифровой след выступает источником криминалистически значимой информации и непосредственным объектом судебно-экспертного исследования, содержащимся на материальном носителе (например, потенциально вредоносное программное обеспечение, содержащееся на жестком диске).

С точки зрения российского уголовного процесса, используя предложенную Е.Р. Россинской, А.И. Семикаленовой, И.А. Рядовским и Т.А. Сааковым классификацию цифровых доказательств, подразделяемых на оригинал, его дубликат и копию, можно определить рассматриваемые следы следующим образом.

Само компьютерное средство (персональный компьютер, мобильное устройство), содержащее носители данных (микросхемы памяти), выступает в качестве вещественного доказательства, а находящиеся в его памяти информационные объекты — в качестве оригинального доказательства. Компьютерное средство, на котором информация сохраняется пользователем путем удаленного доступа (удаленный сервер, облачное хранилище), может выступать в качестве вещественного доказательства только в случае его непосредственного изъятия, что практически невозможно.

Энергонезависимые носители данных (магнитные и лазерные диски, флеш-карты, портативные жесткие диски и др.), хранящие точную цифровую репродукцию информационных объектов, по-

[1] *Сааков Т.А.* К вопросу о профессиональных и квалификационных требованиях, предъявляемых к эксперту в эпоху цифровизации // Теория и практика судебной экспертизы в современных условиях: Материалы VIII Междунар. науч.-практ. конф. Москва, 28—29 января 2021 г. М.: РГ-Пресс, 2021. С. 278.

лученную путем копирования в ходе следственных действий, в том числе из удаленного сервера или облачного хранилища, являются дубликатом доказательств, выступая в уголовном процессе в качестве вещественного доказательства.

Распечатки информации, содержащейся в памяти компьютерных средств и носителей цифровых данных, и распечатанные скриншоты информации, отображенной на экране компьютерного средства, имеют непосредственное доказательственное значение в качестве иных документов, поскольку содержат копию (репродукцию) информации, хранящейся в том числе в режиме удаленного доступа.

Как видим, хотя понятие цифрового следа и представляется нам наиболее удачным из приведенных выше, но в то же время, исходя из уголовно-процессуального значения и природы судебно-экспертного исследования, дефиниция «цифровой след» может быть интерпретирована неоднозначно, что все же требует, по нашему мнению, дальнейшего гносеологического анализа данного концепта.

В целях обозначения следов, возникающих в результате использования информационных технологий, подходящей дефиницией нам представляется следующая: «следы преступной деятельности, образуемые при помощи использования информационных технологий».

Полагаем, что понятие «преступная деятельность» наиболее четко отражает акт человеческого поведения, квалифицированный в соответствии с уголовным законом преступным деянием[1]. При этом в предлагаемой дефиниции акт человеческого поведения может быть выражен только при помощи информационных технологий.

Развивая позицию А.Г. Себякина, подразделяющего электронно-цифровые следы на непосредственные и опосредованные[2], можно предложить классифицировать следы преступлений, образуемые с помощью информационно-телекоммуникационных

---

[1] См.: *Антонов О.Ю.* К вопросу о понятиях механизма и криминалистической характеристики (модели) преступлений и преступной деятельности // Вестн. Удмурт. ун-та. Сер. «Экономика и право». 2011. № 2. С. 111—117.

[2] См.: *Себякин А.Г.* Тактика использования знаний в области компьютерной техники. М.: Юрлитинформ, 2023. С. 22—23, 27.

технологий, по двум основаниям — степени опосредованности воздействия пользователя на компьютерную систему и результату этого воздействия — следующим образом:

- под непосредственно-пользовательскими следами будут подразумеваться цифровые следы, имеющие прямую (непосредственную) связь с причиной (целью) воздействия пользователя на компьютерную систему, по результатам которого пользователем создается новая компьютерная информация. В качестве таких следов выступают компьютерные данные, образованные пользователем посредством устройств ввода (клавиатура, микрофон, светочувствительная матрица и пр.), в результате чего создаются новые файлы или программное обеспечение, хранящиеся в памяти компьютерной системы или в режиме удаленного доступа;
- непосредственно-коммуникационные — это цифровые следы, имеющие прямую (непосредственную) связь с причиной (целью) воздействия, но образуемые программным обеспечением, фиксирующим действия пользователя по поиску или передаче компьютерной информации: скопированные (перемещенные) файлы, почтовые отправления, переписка с использованием мессенджеров, история запросов интернет-браузера, журнал вызовов, записи в прикладных базах данных и пр. Указанные следы также могут быть как локальными (т.е. находящимися непосредственно на носителе, который может быть изъят и подвержен исследованию), так и удаленными (находящимися на ресурсе, доступ к которому обеспечивается с применением средств телекоммуникации, т.е. канала связи);
- в качестве опосредованных следов будут рассматриваться цифровые следы, не имеющие прямой связи с причиной (целью) воздействия пользователя на компьютерную систему, но инициированные этим воздействием, обусловленные особенностями функционирования СПО, стандартами форматов файлов и протоколов передачи данных. К таким следам будут относиться находящиеся на используемой компьютерной системе записи в файлах журналирования системных событий, файлах реестра операционной системы, метаданные пользовательских файлов, записи служебных баз данных, таблиц размещения файлов и пр.;

- внешними электронными следами можно считать следы деятельности участников преступления, не связанной с воздействием на конкретную компьютерную систему, но инициированные различными компьютерными или информационно-телекоммуникационными системами, направленными на сбор информации, подпадающей под сферу их функционирования (камеры видеонаблюдения, базовые станции операторов связи, телематические системы автомобиля и т.п.), и отображаемые в устройствах памяти, установленных как в технических средствах участников преступления (например, электронных блоках управления или мультимедийных устройствах автомобиля), так и в указанных внешних системах.

При этом непосредственные следы в виде созданных пользователем файлов или программного обеспечения, например вирусной программы, а также опосредованные следы могут быть объектами компьютерно-технической судебной экспертизы, в том числе первые — в целях идентификации пользователя, их создавшего. Содержание данных файлов в печатном виде может стать объектом соответствующего вида судебной экспертизы, например судебно-бухгалтерской по исследованию документов, выгруженных из информационной базы «1С: Предприятие».

Непосредственно-коммуникационные и внешние следы могут выступать в качестве традиционных объектов различных видов судебных экспертиз, отображенных в электронно-цифровом виде. Например, файлы, содержащие электронные сообщения, отправленные в любом мессенджере (непосредственно-коммуникационный след), могут исследоваться в рамках судебных речеведческих экспертиз, в том числе в целях идентификации их автора, а видеозапись камеры наружного наблюдения (внешний след) — стать объектом судебно-портретной экспертизы, в том числе в целях идентификации запечатленного на ней лица.

Что касается внешних цифровых следов, то они фиксируют факт регистрации (нахождения, подключения) на объекте (территории) их обслуживания какого-либо средства, как электронного (например, транспортная карта или карта-пропуск), так и иного, например автотранспорта по его регистрационному номеру.

В случае большого объема информации, отображенной в опосредованных и внешних цифровых следах (Big Data) на но-

сителе данных, она может стать объектом нового вида судебных экспертиз — информационно-аналитической[1] или анализироваться с помощью аппаратно-программных комплексов в ходе осмотра цифровых носителей информации.

Отметим, что приведенные выше следы преступной деятельности, образуемые при помощи использования информационных технологий, могут быть подвергнуты исследованию в следственной практике по двум направлениям:

- обнаружение, фиксация и изъятие следов преступной деятельности, содержащихся на электронных носителях информации, путем их *предварительного исследования* в ходе проведения следственных действий. Здесь важно отметить, что в ходе предварительного исследования цифровых данных решается задача, связанная с обнаружением на электронном носителе *основной информации*, под которой, как указывает А.И. Семикаленова, следует рассматривать цифровую информацию, выраженную в виде *звука*, *текста*, *изображения,* которая в дальнейшем подлежит фиксации и изъятию[2];
- судебно-экспертное исследование следов преступной деятельности, содержащихся на электронных носителях информации, как в целях их обнаружения, фиксации и изъятия — *основной информации* (звук, текст, изображение), так и в целях установления механизма их образования (данные о способе, времени, создании, распространении и редактировании основной информации) посредством производства *компьютерно-технической экспертизы*.

При этом важно отметить, что для производства предварительного исследования в ходе проведения следственный действий зачастую бывает достаточно специальных знаний, которыми обладает следователь-криминалист, или в некоторых случаях необходимым уровнем знаний может обладать и отдельно взятый сле-

---

[1] См., напр.: *Антонов О.Ю.* Международные и национальные тенденции и перспективы развития информационно-аналитической судебной экспертизы // Международные и национальные тенденции и перспективы развития судебной экспертизы: Сб. докл. II Междунар. науч. конф., г. Нижний Новгород, 21—22 мая 2020 г. Н. Новгород: ННГУ, 2020. С. 30—37.

[2] См.: *Семикаленова А.И.* Цифровые следы: назначение и производство экспертиз // Вестн. Ун-та им. О.Е. Кутафина. 2019. № 5 С. 117.

дователь, обладающий практическими навыками работы с различными аппаратно-программными комплексами, способствующими обнаружению, фиксации и изъятию цифровых данных с электронных носителей информации (UFED, мобильный криминалист, XRY и др.).

Мы согласны с А.Г. Себякиным, который отмечает, что компьютерно-техническая экспертиза назначается в случаях, когда посредством использования различных АПК, применяемых в ходе следственных действий, не удалось обнаружить следов преступной деятельности[1].

Вместе с тем компьютерно-техническая экспертиза, по нашему мнению, должна назначаться во всех случаях, когда необходимо установить данные о способе, времени, создании, распространении и редактировании основной информации.

Ввиду того что технические средства, программные продукты и методические подходы к работе со следами, образованными с помощью информационно-телекоммуникационных технологий, в ряде случаев схожи, далее будут рассмотрены возможности использования специальных знаний в аспекте предварительного исследования электронных носителей информации.

Следует отметить, что мобильные устройства являются неотъемлемой частью жизни современного человека. В связи с этим данное средство коммуникации заслуживает особого внимания и требует отдельного предметного рассмотрения, так как смартфоны чаще всего встречаются в следственной практике в качестве источника, содержащего криминалистически значимую информацию.

Итак, информация, содержащаяся в памяти смартфонов участников уголовного процесса, практически всегда имеет криминалистическое значение. В некоторых случаях она напрямую уличает лицо в совершении преступления, а в других — помогает выстроить ход и содержание расследования, наметить или исключить те или иные версии.

На сегодняшний день у следствия есть несколько направлений работы с следами, содержащимися в памяти сотовых телефонов.

1. Извлечение и анализ полных данных (переписка в чатах, SMS-сообщения, список контактов, последние соединения, за-

[1] См.: *Себякин А.Г.* Тактика использования знаний в области компьютерной техники. М.: Юрлитинформ, 2023. С. 81.

метки, фотографии и видеозаписи, посещенные сайты, история интернет-браузера и пр.), имеющихся в мобильном устройстве, в том числе удаленных данных, с помощью универсального устройства UFED Touch, «Мобильный криминалист», XRY и ряда других. При использовании указанных комплексов извлечение информации с мобильного устройства осуществляется в ходе проведения осмотра предметов (документов) в соответствии со ст. 177 УПК РФ с участием следователя-криминалиста или специалиста в области компьютерных технологий. Однако следует учитывать, что возможности указанных выше устройств ограниченны. Во-первых, в случае если информация с мобильного устройства была удалена в результате его «перепрошивки», то, вероятнее всего, восстановить удаленные данные будет возможным только посредством назначения компьютерно-технической экспертизы; во-вторых, в отношении современных смартфонов, работающих на базе операционных систем IOS или Android, указанные программы неэффективны в случае, если следствию неизвестен ПИН-код устройства, так как преодолеть систему защиты таких смартфонов не представляется возможным даже посредством производства компьютерно-технической экспертизы.

2. Определение местонахождения электронного устройства (а следовательно, и его владельца). С помощью спутниковой навигации — функции геопозиционирования (GPS/ГЛОНАСС) или соединения с точками доступа сети WiFi, а также метаданных фотоснимков, видеороликов, веб-сайтов не сложно установить координаты местоположения мобильного телефона участника уголовного судопроизводства в определенное время.

Некоторую информацию можно получить и отобразить в протоколе, а также с помощью фотоаппаратуры непосредственно путем изучения содержимого телефона без каких-либо специальных устройств. Это касается контактов, журнала звонков, SMS-сообщений, содержания мессенджеров (WhatsApp, Viber и др.), переписки в социальных сетях[1], записной книжки, отметок календаря, интернет-истории (журнал браузеров), фотографий и видеофайлов.

[1] Зачастую пользователи смартфонов сохраняют пароли при входе в социальные сети, и вход происходит автоматически.

С помощью специальной высокотехнологичной криминалистической техники можно извлечь полную информацию (включая удаленную) из памяти мобильных телефонов, а также электронных накопителей (карт памяти, SIM-карт и др.) участников уголовного процесса как в ходе проверки сообщений о преступлениях, так и в ходе их расследования.

Поскольку программы указанных выше АПК предоставляют возможность построить, распечатать и сохранить подробный отчет об извлечении, который полностью отвечает требованиям УПК РФ и сложившейся следственной практике, протокол осмотра телефона с помощью АПК состоит, по сути, из данного отчета. Складывается практика, что даже фотографии упаковки, самого телефона, устройства и процесса извлечения с помощью АПК размещаются в описательной части протокола, а не оформляются отдельным приложением к нему.

В связи с тем что сводки об извлечении могут занимать сотни страниц (журнал звонков, SMS-переписка, содержание чатов, геопозиционирование и др.), специалисту (следователю-криминалисту) совместно со следователем целесообразно выделять лишь интересующие следствие данные и экспортировать (с помощью программ Excel, Word, PDF, HTML, XML, EML на выбор) только криминалистически значимую информацию.

Извлеченные на отдельный компьютер или флеш-карту данные анализируются с помощью специальных ПО, что позволяет создать подробный структурированный отчет с интересующей следствие информацией

Извлекать, анализировать информацию, содержащуюся в памяти телефона, а также выделять и экспортировать определенную информацию целесообразно специалисту (следователю-криминалисту) совместно со следователем. Ведь именно последний знает время, место, особенности механизма совершенного преступления, его подготовки или сокрытия. Поэтому следователь может уточнить и сузить границы искомой информации, уточнить интересующие даты и пр.

Сам смартфон как предмет осмотра признается вещественным доказательством и приобщается к уголовному делу, о чем выносится соответствующее постановление. Полученный с использованием АПК и распечатанный отчет (за определенный период времени или по отдельным номерам и пр.) об извлеченных дан-

ных может быть процессуально оформлен в качестве приложения к протоколу предмета либо непосредственно составлять описательную часть протокола. Причем в ряде следственных органов анализ полученного отчета проводят в рамках отдельного следственного действия — осмотра документов — и оформляют отдельным протоколом.

Упаковывать осмотренный смартфон целесообразно сначала в первоначальную (вскрытую) упаковку, а затем в новый бумажный конверт, который опечатывается и снабжается пояснительной запиской.

На основании изложенного более оптимальным предлагается использовать в науке криминалистике и следственно-судебной практике термин «следы преступной деятельности, образуемые с помощью информационно-телекоммуникационных технологий» и предлагаемую классификацию данных следов, порядок обнаружения, фиксации и изъятия которых в рамках отдельных следственных действий будет описан в п. 4.3 настоящей главы.

4.2. Тактика проведения отдельных следственных действий, направленных на обнаружение, фиксацию и изъятие следов преступной деятельности, образованных при помощи использования информационных технологий

Т.А. Сааков[1], *С.Ю. Скобелин*[2]

Цифровые данные, содержащиеся в сети Интернет или на электронном носителе информации, предполагают со стороны следователя соблюдение определенного алгоритма действий, позволяющего их обнаружить, зафиксировать, изъять и приобщить к материалам уголовного дела в рамках проведения следственных и иных процессуальных действий. Учитывая то обстоятельство, что ненадлежащее изъятие цифровых данных в ходе расследования преступлений может привести впоследствии к утрате их до-

[1] Тигран Артемович Сааков — старший преподаватель кафедры судебно-экспертной и оперативно-розыскной деятельности Московской академии Следственного комитета Российской Федерации, кандидат юридических наук.

[2] Сергей Юрьевич Скобелин — доцент кафедры информационных технологий и организации расследования киберпреступлений, кандидат юридических наук, доцент.

казательственной значимости, в настоящем параграфе будут рассмотрены тактические особенности проведения отдельных следственных действий, направленных на обнаружение, фиксацию и изъятие следов преступной деятельности, образуемых при помощи использования информационных технологий.

Тактика производства следственного осмотра удаленных серверов и электронных носителей информации

Обнаружение следов преступной деятельности, оставленных на удаленных серверах или электронных носителях информации, является поисковой деятельностью следователя, которая направлена на сбор криминалистически значимой информации, необходимой для познания истины и правильного разрешения уголовного дела. Обнаружение такой информации возможно посредством нескольких способов:

- поиск информации с использованием технических средств (ПК, ноутбука, электронного планшета и др.) для посещения различных контент-сайтов в сети Интернет, в том числе страницы пользователя социальной сети (интересующий следствие ID), где потенциально содержатся следы преступной деятельности с последующей фиксацией и изъятием криминалистически значимой информации. При этом обнаружение криминалистически значимой информации таким способом возможно в случае, если цифровые данные, интересующие органы следствия, находятся в открытом доступе либо удалось оперативно внедриться в установленном порядке, например подписаться на конкретную закрытую группу в социальной сети, в противном случае получение информации таким способом не представляется возможным;
- с электронных устройств подозреваемого/обвиняемого, потерпевшего и иных участников уголовного судопроизводства, на которых может содержаться криминалистически значимая информация. При этом в случае получения информации с удаленных серверов через электронные устройства участников уголовного судопроизводства следует учитывать, что, к примеру, при помощи авторизации через их аккаунт в социальной сети/мессенджере получение крими-

налистически значимой информации будет возможным только в отношении тех данных, к которым аккаунт конкретного пользователя имеет доступ;

- с электронно-вычислительных мощностей, содержащих криминалистически значимую информацию, например, о пользователях социальной сети и/или мессенджеров (серверы компаний, предоставляющих услуги пользования конкретной социальной сетью, мессенджером и т.д.).

В связи с тем что каждый из вышеперечисленных способов имеет свою специфику, обусловленную нормами как международного права, так и национального законодательства Российской Федерации, представляется целесообразным рассмотреть более подробно указанные способы обнаружения следов преступной деятельности, содержащихся на удаленных серверах и электронных носителях информации.

Отметим, что в настоящий момент в УПК РФ отсутствует норма, которая регламентировала бы порядок проведения следственного действия, связанного с получением цифровой информации с удаленных компьютерных сетей и систем[1]. В связи с этим на практике при проведении предварительной проверки по сообщению о преступлении, когда криминалистически значимая информация находится на удаленных серверах, например на страницах социальных сетей пользователей в сети Интернет, следователи руководствуются ст. 176, 177 УПК РФ, т.е. осуществляют осмотр и последующую фиксацию и изъятие следов преступной деятельности в рамках проведения такого следственного действия, как осмотр предметов (документов).

Вместе с тем отметим, что в соответствии со ст. 164.1 УПК РФ участие специалиста в следственных действиях является обязательным в случаях, когда изъятие и копирование информации осуществляются с электронных носителей. Однако следует констатировать, что положения ст. 164.1 УПК РФ лишь отчасти способствуют оптимизации и эффективности проведения следственных действий, связанных с изъятием цифровой информации.

---

[1] См.: *Семикаленова А.И., Рядовский И.А.* Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 180.

Во-первых, положения ст. 164.1 нельзя экстраполировать на удаленное получение информации с сайта в сети Интернет. Это связано с тем, что, согласно ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации», сайт в сети Интернет — это «совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» <…> по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»»[1]. Однако при осмотре сайта в сети Интернет фиксация и последующее изъятие информации осуществляются не с электронно-вычислительных мощностей (серверов), при помощи которых поддерживается работоспособность определенного контент-сайта, а из информационно-телекоммуникационной сети Интернет, отображающей информацию, хранящуюся в памяти устройств хранения информации (жестких дисков серверов) электронно-вычислительных мощностей. В свою очередь, в ст. 164.1 УПК РФ ничего не сказано о получении информации с удаленных серверов, а речь идет лишь об изъятии и копировании информации с электронных устройств. Следовательно, в отношении обнаружения, фиксации и изъятия цифровых следов из сайтов в сети Интернет, в частности со страниц социальных сетей пользователей, в УПК РФ образовалась «правовая лакуна».

Во-вторых, согласно ч. 2 ст. 164.1, участие специалиста является обязательным, в частности, в случаях, когда изъятию подлежат электронные носители информации. Однако диспозицию ч. 2 ст. 164.1 УПК РФ вряд ли можно признать успешно сформулированной, так как анализ следственной практики показывает, что необходимость в привлечении специалиста к участию в следственных действиях, связанных с изъятием электронных носителей информации, возникает довольно редко.

Проблема, на наш взгляд, заключается в том, что для непосредственного изъятия самого электронного носителя информа-

[1] См.: *Об информации*, информационных технологиях и о защите информации [Электронный ресурс] / ФЗ от 27 июня 2006 г. № 149-ФЗ: принят Гос. Думой Федер. Собр. РФ 8 июля 2006 г.: офиц. текст: по состоянию на 3 апр. 2020 г. // СПС «КонсультантПлюс».

ции (мобильного телефона, электронного планшета, ноутбука и др.), например, в рамках производства выемки (ст. 183 УПК РФ) участие специалиста является необязательным, так как в ряде случаев следователь в состоянии сам надлежащим образом произвести выемку электронного носителя информации и без участия специалиста, если изъятие электронного устройства не представляет сложностей и не требует для этого использования специальных знаний, которыми следователь не обладает. В связи с этим С.Б. Россинский совершенно справедливо отмечает, что «участие специалиста в следственных действиях не является безусловным. Обладая необходимыми специальными знаниями и умея применять их на практике, следователь вполне может обойтись и без его помощи»[1].

В то же время, по нашему мнению, участие специалиста обязательно, когда следователю нужно осуществить изъятие цифровой информации либо непосредственно с электронного носителя (ПК, мобильного телефона, электронного планшета и т.д.), либо с удаленных серверов (например, с определенного контент-сайта), а не самого электронного устройства (системного блока ПК, ноутбука, мобильного телефона и т.д.), так как фиксация и изъятие цифровых данных предопределяют необходимость соблюдения определенного порядка действий со стороны правоприменителя, вызванного спецификой данных объектов, в целях обеспечения их сохранности, достоверности и дальнейшей возможности приобщения в качестве вещественных доказательств по делу[2].

Исходя из вышеизложенного, нам представляется целесообразным внесение изменений в наименование ныне действующей ст. 164.1 УПК РФ, изложив ее в следующей редакции: «Изъятие компьютерной и цифровой информации с удаленных серверов и электронных носителей информации при производстве следственных действий». Таким образом, удалось бы восполнить про-

---

[1] *Россинский С.Б.* Следственные действия: Монография. М.: Норма, 2018.

[2] См., например: *Сааков Т.А*. Особенности изъятия речевых произведений, находящихся в цифровой среде // Современные проблемы цифровизации криминалистической и судебно-экспертной деятельности: Материалы науч.-практ. конф. М.: РГ-Пресс, 2019. С. 191—194; *Он же*. Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора // Законы России: опыт, анализ, практика. 2020. № 4. С. 98.

бел, связанный с отсутствием норм в УПК РФ, регулирующих порядок изъятия цифровой информации с удаленных серверов.

В свою очередь, обязательное участие специалиста, закрепленное в ч. 2 ст. 164.1 УПК РФ, представляется логичным вынести в отдельную ч. 4 рассматриваемой статьи и изложить в следующей редакции: «При проведении следственных действий, в ходе которых осуществляется изъятие цифровой информации с удаленных серверов или электронных носителей, участие специалиста обязательно». Такая редакция ст. 164.1 УПК РФ позволит четко обозначить обязательное участие специалиста, которое будет исключительно связано с фиксацией и изъятием *цифровой информации*, имеющей свою специфику и предопределяющей наличие у субъекта, осуществляющего ее фиксацию и изъятие, специальных знаний из области информационно-компьютерной безопасности. В то же время такая редакция ст. 164.1 УПК РФ позволит избежать на практике случаи обязательного привлечения специалиста к участию в следственном действии, когда изъятию подлежат сами электронные носители информации, если объективная потребность в его участии отсутствует.

Что касается поисковой деятельности следователя, связанной с обнаружением криминалистически значимой информации, находящейся на удаленных серверах (например, страницах пользователей социальных сетей), то представляется также целесообразным привлечение специалиста из области компьютерно-информационной безопасности для содействия в обнаружении доказательственно релевантной информации с удаленных серверов в соответствии со ст. 168 УПК РФ.

Такая необходимость обусловлена тем, что посредством визуального осмотра контент-сайта, не требующего использования специальных знаний, можно обнаружить лишь небольшую часть цифровых данных, интересующих органы следствия. Однако для получения детализирующей информации о цифровых данных, содержащихся на контент-сайте (странице пользователя социальной сети), необходимо использовать компилируемые программные модули, а в ряде случаев — отдельные программные продукты, позволяющие выявить исходящие с контент-сайта цифровые данные, например выраженные в виде скрытых ссылок. Более того, для обнаружения криминалистически значимой информации

зачастую представляется необходимым производить анализ исходного кода страницы сайта.

Проиллюстрируем это примером.

> Так, в Следственное управление по Северо-Западному административному округу г. Москвы от гражданина N. поступило сообщение о совершении преступления, предусмотренного ст. 280 УК РФ. По факту поступившего сообщения в рамках осмотра предметов (документов) в соответствии со ст. 177 УПК РФ следователем осуществлялась проверка содержания контент-сайта «XXXXXXX» на предмет наличия/отсутствия в нем призывов к осуществлению экстремистской деятельности, предусмотренных ст. 280 УК РФ. В ходе следственной проверки было обнаружено, что на осматриваемом контенте, помимо экстремистских материалов, также размещена информация, способствующая незаконному сбыту наркотических средств, которая выражена в виде всплывающих окон. По факту обнаружения признаков составов преступлений, предусмотренных ст. 280 УК РФ, 228.1 УК РФ, было возбуждено уголовное дело.
>
> Специалисту, участвующему в производстве следственного действия, удалось посредством анализа исходного кода страницы сайта определить путь к контенту сайта, из которого данная информация поступала для последующего размещения на проверяемом в ходе осмотра сайте.
>
> В дальнейшем следствию удалось доказать причастность к совершенному преступлению, предусмотренному ст. 280 УК РФ, гражданина А. и причастность к совершенному преступлению, предусмотренному ст. 228.1 УК РФ, гражданина В. — обладающего правами администратора сайта, который удалось обнаружить специалисту в ходе осмотра исходного кода страницы сайта, проверяемого в ходе следственного осмотра[1].

Как видно из приведенного выше примера, обнаружение цифровых следов преступлений, связанных с незаконным сбытом наркотических средств, оказалось возможным только лишь посредством анализа исходного кода страницы сайта, анализ которого невозможен без использования специальных знаний из области информационно-компьютерной безопасности. В связи с этим привлечение специалиста для оказания помощи следовате-

[1] См.: *Россинская Е.Р., Сааков Т.А*. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3(15). С. 106—123.

лю в обнаружении криминалистически значимой информации представляется нам также целесообразным.

Другой не менее важной проблемой собирания следов преступной деятельности с удаленных серверов и электронных носителей информации является отсутствие международно-правового акта общеобязательного характера по противодействию киберпреступности и (или) обеспечению кибербезопасности, который регулировал бы вопросы, связанные в том числе с собиранием криминалистически значимой информации с хостинг-провайдеров — иностранных компаний, предоставляющих услуги пользования конкретной социальной сетью или мессенджером.

Отметим, что у Российской Федерации имеется ряд заключенных договоров с иностранными государствами, в том числе регламентирующих оказание международно-правовой помощи сторонам при расследовании уголовных преступлений[1]. При этом следует учитывать складывающуюся международную обстановку и осознавать реальную возможность получения информации, интересующей органы следствия нашей страны, от иностранного государства. Проблемным является тот факт, что международные запросы могут быть оставлены без ответа[2], что связано с отсутствием международно-правовых норм, регулирующих порядок передачи цифровой информации между иностранными государствами.

Следует отметить, что ныне действующая Будапештская конвенция «О преступности в сфере компьютерной информации» (далее — Будапештская конвенция), во-первых, по своей сути является устаревшей, так как закрепленные в ней положение едва ли способны отвечать реалиям следственной практики. В Конвенции рассматриваются преступления против конфиденциальности, целостности и доступности компьютерных данных и систем, подлог и мошенничество с использованием компьютеров, преступления, связанные с содержанием данных, в особенности преступления, связанные с детской порнографией, а также преступления, связан-

---

[1] См.: *Официальный* сайт Министерства юстиции Российской Федерации [Электронный ресурс]. Режим доступа: https:// minjust.gov.ru/ (дата обращения: 21.07.2020).

[2] См.: *Колычева А.Н., Васюков В.Ф.* Расследование преступлений с использованием компьютерной информации из сети Интернет: Учеб. пособие / Под ред. А.Г. Волеводза. М.: Проспект, 2020. С. 25.

ные с нарушением авторского и смежных прав (глава II, раздел I, ч. 1—4). Однако, как уже отмечалось, на сегодняшний день перечень составов преступлений, которые совершаются при помощи использования информационных технологий, гораздо шире, чем перечень видов преступлений, регулируемых Будапештской конвенцией, по которым предусмотрено международное сотрудничество стран-участников в сфере компьютерной информации.

Во-вторых, отказ Российской Федерации от подписания Будапештской конвенции нам представляется вполне логичным и правомерным, так как прописанные в п. «b» ст. 32 Будапештской конвенции положения противоречат, в частности, ст. 4, 23, п. 1 ст. 24 Конституции РФ, а также ФЗ «О персональных данных», так как п. «b» ст. 32 Будапештской конвенции предусматривает возможность получения одной из сторон без согласия другой стороны компьютерных данных, хранящихся на серверах другого государства.

Исходя из изложенного выше, получение криминалистически значимой информации с хостинг-провайдеров — иностранных компаний, предоставляющих услуги пользования социальной сетью или мессенджером (Facebook, Instagram, WhatsApp и др.), на практике вызывает сложности у правоохранительных органов, что, безусловно, препятствует расследованию преступлений, связанных с получением цифровой информации с хостинг-провайдеров — юридических лиц, зарегистрированных на территории иностранных государств.

Таким образом, отсутствие международно-правовых норм в сфере противодействия киберпреступности в некоторых случаях затрудняет собирание цифровых доказательств, а в некоторых из них приводит следственные органы Российской Федерации к абсолютной невозможности сбора цифровых доказательств, хранящихся на серверах иностранных компаний.

Вместе с тем если у органов следствия возникает необходимость в получении криминалистически значимой информации, например, со страниц пользователей социальных сетей, представителями которых являются юридические лица, зарегистрированные в Российской Федерации («Вконтакте», «Одноклассники»), то в соответствии с подп. 4, 10 п. 1 ст. 13 ФЗ «О полиции» и п. 2 ст. 6 ФЗ об ОРД в целях предупреждения, выявления и раскрытия преступлений может быть направлен запрос с просьбой предоставить сведения о конкретном пользователе, который интересует следствие.

При этом представители юридического лица — социальной сети — имеют право предоставить только те сведения, которые не затрагивают конституционных прав человека и гражданина (адрес личной страницы пользователя; дата создания страницы; номер телефона и электронной почты пользователя; IP-адрес, с которого пользователь осуществлял вход на страницу; история изменений пароля, логина (имени пользователя), номера телефона; история обращений в службу поддержки; история блокировок страницы пользователя). Однако если есть соответствующее судебное решение (ч. 2 ст. 23 Конституции РФ), то может быть представлена вся интересующая органы следствия информация о пользователе.

Как отмечал Р.С. Белкин, «проблематика фиксации доказательственной информации — неотъемлемая часть комплекса проблем, связанного с изучением и использованием закономерностей собирания доказательств»[1]. В связи с этим процедура фиксации и изъятия следов преступной деятельности, находящихся на удаленных серверах, равно как и на электронных носителях информации, заслуживает отдельного внимания.

В цивилистических процессах имеются теоретические разработки к организационно-правовому обеспечению фиксации цифровой информации, находящейся в сети Интернет[2]. Вместе с тем относительно определен статус скриншотов в арбитражном процессе, о чем свидетельствуют требования к их фиксации, отраженные в судебной практике[3]. Анализ судебной практики показывает[4], что устоявшимся механизмом обеспечения представляе-

---

[1] См.: *Белкин Р.С.* Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории. М.: Юрид. лит., 1987. С. 217.

[2] См., например: *Танимов О.В., Кудашкин Я.В.* О правовой природе и возможности правового регулирования отношений в сети Интернет // Информационное право. 2012. № 2. С. 17—21; *Бабкин С.А.* Право, применимое к отношениям, возникающим при использовании сети Интернет: основные проблемы. М.: Центр ЮрИнфоР, 2003.

[3] См.: *Информационное* письмо Президиума ВАС РФ от 7 июля 2004 г. № 78 «Обзор практики применения арбитражными судами предварительных обеспечительных мер» // Вестн. ВАС РФ. 2004. № 8.

[4] См., например: решение Арбитражного суда Саратовской области от 4 марта 2019 г. по делу № А57-15203/2018; постановление Арбитражного суда Хабаровского края от 5 августа 2013 г. по делу № А73-14263/2012; решение Арбитражного суда Курской области от 29 мая 2018 г. по делу № А35-5996/2017. См.: https://sudact.ru/ (дата обращения: 26.03.2022).

мых доказательств, полученных из сети Интернет, является обращение одной из участвующих в деле сторон к нотариусу в целях проведения осмотра сайта в соответствии со ст. 102—103 Основ законодательства о нотариате[1] и последующей фиксации цифровых данных, находящихся в сети Интернет.

Следует сказать о том, что в отношении специфики фиксации и изъятия цифровых данных — речевых продуктов, находящихся в цифровой среде, — рядом авторов предпринимались попытки разрешения проблем, возникающих на практике, связанных с обеспечением достоверности зафиксированных на материальный носитель информации цифровых данных[2]. Однако единый унифицированный подход к фиксации и изъятию таких доказательств в уголовном процессе отсутствует. В связи с этим представляется целесообразным рассмотреть особенности фиксации и изъятия цифровых данных из удаленных серверов и электронных носителей информации на примере страниц пользователей социальных сетей и мессенджеров в целях обеспечения их достоверности и возможности приобщения к вещественным доказательствам.

Как отмечает А.И. Семикаленова, цифровые следы несут в себе значимую для следствия информацию, которую можно разделить на основную, выражающуюся в виде звука, изображения, текста, рисунка, и дополнительную, позволяющую судить о способе и времени создания, распространения и редактирования основной информации[3]. Исходя из этого, остановимся подробно на каждой из особенностей процедуры фиксации и изъятия цифровых данных, содержащихся на страницах пользователей в социальных сетях и мессенджерах.

Основополагающим фактором при работе с цифровыми данными выступает оперативность действий со стороны правоприменителя, связанная с фиксаций криминалистически значимой

---

[1] См.: *Основы* законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 26.07.2019) (с изм. и доп., вступ. в силу с 25.10.2019) офиц. текст: по состоянию на 25 октября 2019 г. // СПС «КонсультантПлюс».

[2] См.: *Сааков Т.А.* Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора. С. 96—104; *Россинская Е.Р., Сааков Т.А.* Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров. С. 106—123.

[3] *Семикаленова А.И.* Цифровые следы: назначение и производство экспертиз. С. 57.

информации, интересующей следствие, после ее обнаружения. Обусловлено это тем, что любой контент сайта поддерживается при помощи электронно-вычислительных мощностей, на которых хранится вся цифровая информация, отображающаяся на определенном контент-сайте (странице пользователя социальной сети).

Риск утраты криминалистически значимой информации, содержащейся на определенном контенте, заключается в том, что, с одной стороны, сервер[1], при помощи которого поддерживается определенный контент-сайт, может быть уничтожен злоумышленниками или подвержен полному/частичному удалению с него информации, представляющей интерес для правоохранительных органов, вследствие чего воспроизводимость информации на контенте окажется в последующем невозможной, что будет означать безвозвратную утрату криминалистически значимой информации.

Кроме того, значимая для следствия информация, содержащаяся на контенте сайта, может быть частично или полностью изменена, например, лицом, имеющим доступ к контенту на правах администратора. Таким образом, если не осуществить оперативно фиксацию и изъятие интересующих следствие данных с удаленных серверов, то в результате таких действий к моменту изъятия цифровых данных они могут уже быть подвергнуты удалению/изменению и, как следствие, не содержать криминалистически значимой информации, представляющей интерес для правоохранительных органов.

Исходя из вышеизложенного очевидно, что в зависимости от того, насколько оперативно правоприменителем будут предприняты действия по фиксации и изъятию криминалистически значимой информации с контента сайта в сети Интернет, напрямую будут зависеть сохранность цифровых данных и дальнейшая возможность их приобщения к материалам дела в качестве вещественных доказательств.

В равной степени это относится к фиксации и изъятию цифровых данных, находящихся на электронных устройствах (мобильных телефонах, электронных планшетах и др.), так как в противном случае также велик риск утраты криминалистически значимой информации. Это связано с тем, что на электронных носи-

[1] Аппаратный комплекс, настроенный на хранение данных или непрерывное решение определенных задач.

телях информации зачастую содержится потенциально доказательственно релевантная информация, имеющая значение для расследования преступлений, которая в большинстве случаев бывает размещена и опубликована в закрытых группах в социальных сетях, блогах, пабликах, мессенджерах и т.д., в результате чего к данной информации имеет доступ ограниченный круг лиц.

Исходя из сказанного выше следует, что, для того чтобы получить доступ к криминалистически значимой информации, которая, например, опубликована в закрытых группах в социальных сетях, необходимо подписаться на определенную группу в конкретной социальной сети. В дальнейшем для получения доступа к информации закрытой группы необходимо одобрение администратора группы («Вконтакте», «Одноклассники», Facebook). Аналогичный порядок действий необходимо произвести и для получения доступа к информации в закрытых чатах мессенджеров (WhatsApp, Viber, Telegram). Однако как в социальных сетях, так и в мессенджерах далеко не во всех случаях возможно получение криминалистически значимой информации соответствующим способом. Такие сложности возникают во многом из-за того, что, например, преступные экстремистские/террористические группировки представляют собой закрытую субкультуру, внедрение в которую зачастую оказывается крайне сложным для сотрудников правоохранительных органов. Таким образом, может возникнуть необходимость в фиксации и изъятии цифровых данных, содержащихся на электронном носителе информации (мобильном телефоне, электронном планшете и др.). При этом важно понимать, что не всегда удается изъять и зафиксировать всю необходимую криминалистически значимую информацию, интересующую следствие, с электронного носителя информации.

В некоторых случаях цифровые следы могут содержаться только в «облачном» хранилище. Такое положение дел означает, что криминалистически значимая информация не имеет резервной копии на самом электронном устройстве, следовательно, ее получение в этом случае возможно посредством авторизации через аккаунт пользователя электронного устройства (подозреваемого/обвиняемого) и последующей фиксации. Если цифровая информация выражена в виде письменных продуктов речевой деятельности, то по аналогии с утвердившейся практикой фиксации доказательств в цивилистических процессах представляется целе-

сообразным осуществлять снятие скриншотов образов экрана электронного устройства (мобильного телефона, ноутбука, электронного планшета и т.д)[1] либо фотофиксацию. Однако при этом следует учитывать, что скриншоты образов экрана отражают более качественно информацию, содержащуюся на контенте сайта, чем фотоснимки экрана электронного устройства, для которых неизбежен «муаровый узор» и блики, которые могут привести к частичной утрате фиксируемой с контент-сайта криминалистически значимой информации.

Если осуществляются фиксация и изъятие аудио- и видеофайлов с контент-сайтов (страниц пользователей социальных сетей), то целесообразно проводить трассировку[2], так как в результате таких действий представляется возможным отследить путь доступа от сервера, при помощи которого осуществлялся вход в информационно-коммуникационную сеть следователем, до сервера, на котором расположен осматриваемый информационный ресурс (контент сайта). Результаты трассировки, приобщаемые к протоколу осмотра, позволяют верифицировать факт соединения сервера, используемого в ходе следственного осмотра, с контентом конкретного осматриваемого сайта, а также подтвердить отсутствие постороннего информационного влияния при осуществлении фиксации и изъятия текстовых, аудио- и видеофайлов, находящихся на странице пользователя, в частности если подлежащие изъятию файлы расположены в облачном хранилище интересующего следствие ID. Наряду с этим данная процедура позволит также удостоверить факт, что в браузере были отображены страницы подлинного сайта, с которого была скопирована информация.

Следует также учитывать, что если у посторонних лиц имеются данные о реквизитах пользователя (логин и пароль) подозреваемого/обвиняемого в социальной сети («Вконтакте», Facebook, «Одноклассники»), то при помощи сети Интернет возможно подключение к соответствующему профилю со стороны третьих лиц, которыми могут быть предприняты действия по удалению кри-

[1] См.: *Сааков Т.А.* Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора. С. 101—103.

[2] Произвести трассировку можно с использованием программы Tracert или аналога.

миналистически значимой информации, находящейся в облачном хранилище.

Еще одной не менее важной проблемой при получении информации с электронных устройств является возможность удаленного подключения к электронному устройству (смартфону, планшету) со стороны посторонних лиц. Как справедливо отмечают исследователи, «при изъятии автономных устройств (ноутбуков, смартфонов), экран которых заблокирован, но сами они находятся во включенном состоянии. При наличии доступа к сети Интернет, например по стандартам передачи данных в сотовых сетях, возможно удаленное подключение к ним посторонних лиц и внесение изменений в хранящуюся на них компьютерную информацию»[1].

Таким образом, оперативность в действиях дознавателя или следователя с момента обнаружения цифровых данных до момента их фиксации напрямую предопределяет сохранность криминалистически значимой информации, содержащейся на контенте сайта или на электронном устройстве подозреваемого/обвиняемого, потерпевшего.

Общие криминалистические рекомендации по изъятию и фиксации доказательств содержат требования фиксировать в протоколе индивидуальные признаки изъятых устройств и электронных носителей информации (размер, форму, номер и т.д.), позволяющие идентифицировать их и хранящуюся на них информацию; предъявляют требования к обеспечению их сохранности, механической целостности. Однако, как справедливо отмечается в научной литературе, «такие общие требования по отношению к компьютерной информации нельзя признать достаточными для обеспечения ее сохранности и дальнейшей идентификации»[2].

Несмотря на то что с процессуальной точки зрения доказательством будет протокол следственного действия и электронный носитель информации, на который копируется криминалистически значимая информация, содержащаяся на оригинале

---

[1] *Чекунов И.Г., Рядовский И.А., Пузарин А.В., Русскевич Е.А.* Методические рекомендации по расследованию преступлений в сфере компьютерной информации: Учеб. пособие. 2-е изд. М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2019. С. 196.

[2] Там же. С. 195.

(контент сайта, мобильного телефона, электронного планшета), наряду с этим также еще необходимо верифицировать зафиксированную на электронном носителе (CD-диске, USB-накопителе) информацию.

Верифицировать цифровые данные, полученные из социальных сетей или мессенджеров, вне зависимости от типа файла (текстовый, графический, аудио, видео) и их расширений (txt, docx, pdf, jpg, png, mp3, mp4, mkv, avi) возможно с помощью вычисления контрольной суммы (хеш-суммы[1]) файла по определенному алгоритму (MD5, SHA-1, SHA-2[2]). Именно с помощью хеш-суммы на любом из этапов расследования преступления становится возможным подтвердить идентичность изъятой и зафиксированной на электронном носителе информации. При этом сведения о хеш-сумме изъятого файла должны быть занесены в протокол следственного действия. Необходимость в производстве расчета контрольной суммы файла при фиксации и изъятии цифровых следов обусловливается, тем что:

- во-первых, исключается возможность внесения изменений в первоначальное содержание файла (скриншотов образов

[1] Расчет контрольной суммы файла можно произвести с помощью программ: Arpoon Checksum, HashTab, Alternate HASH-Generator или иных аналогов, позволяющих рассчитать хеш-сумму файла по определенному алгоритму. Расчет хеш-суммы файла позволят в дальнейшем подтвердить его идентичность, исключить сомнения о внесении изменений в первоначальное содержание изъятого и зафиксированного на материальном носителе информации файла. Таким образом, при помощи расчета контрольный суммы файла можно подтвердить достоверность цифровой информации.

[2] Отметим, что традиционно используемый в следственной практике расчет хеш-суммы по алгоритму MD5 в настоящее время признан небезопасным. Например, рабочим информационным документом RFC 6151, выпускаемым под эгидой ISOC, и стандартом компьютерной безопасности правительства США FIPS 140-2 (ANNEX 2). Это связано с тем, что у двух разных файлов при расчете по алгоритму MD5 не исключается возможность появления одинаковой хеш-суммы, следовательно, подтвердить идентичность изъятой и зафиксированной информации не представляется возможным. Безопасный алгоритм хеширования, версия SHA-2, включает в себя алгоритмы, наиболее часто используемые в следственной практике: SHA-512/256, именно расчет по такому алгоритму позволяет подтвердить идентичность изъятой и зафиксированной на электронном носителе информации, поэтому с точки зрения обеспечения достоверности доказательств целесообразно использовать алгоритм расчета контрольной сумм файла по SHA-2.

экрана, аудио- и видеофайлов). Так, в случае если, например, файл будет смонтирован при помощи современных программ обработки изображений (Adobe Photoshop, GIMP, PhotoEditor), то хеш-сумма файла будет отличной от той, которая зафиксирована в протоколе следственного действия, что будет свидетельствовать о внесении каких-либо изменений в файл, содержащейся на электронном носителе информации;

- во-вторых, в случае если электронный носитель, на котором содержится изъятая информация, будет поврежден, то это не повлечет ее утраты, если информация скопирована на другие электронные носители. Достоверность и идентичность содержащейся информации можно будет подтвердить при помощи расчета хеш-суммы файла, содержащегося на другом электронном носителе информации, посредством соотношения контрольных сумм файлов, указанных в протоколе следственного действия и полученных с электронного носителя информации.

Основываясь на приведенных выше особенностях фиксации и изъятия цифровых данных, находящихся на страницах социальных сетей пользователей или мессенджеров, предлагаем сформулировать следующие рекомендации для следователей при работе с такими доказательствами в целях признания их надлежащими:

1) оперативно фиксировать и изымать цифровые данных при их обнаружении;

2) привлекать по необходимости специалиста в области информационно-компьютерной безопасности (ст. 168 УПК РФ) для оказания помощи в обнаружении, фиксации и изъятии цифровых данных, размещенных в сети Интернет, при производстве такого следственного действия, как осмотр предметов (документов) в соответствии со ст. 177 УПК РФ;

3) верифицировать факт того, что символьный адрес сайта соответствует его настоящему IP-адресу, что должно подтверждаться соответствующей записью в протоколе посредством осуществления трассировки сайта;

4) производить расчет контрольной суммы файла(ов) (хеш-суммы), зафиксированной на электронном носителе информации).

Протокол следственного действия, приложением к которому является определенный файл(ы) (цифровые данные), содержащийся на электронном носителе информации (pdf, docx, mp4, mkv, avi и др.), должен обязательно включать в себя:

- дату и время фиксации;
- данные о лице, которое производило фиксацию, его подпись;
- данные о специалисте, который был привлечен для участия в следственном действии;
- данные о соответствии символьного адреса сайта его настоящему IP-адресу, что должно подтверждаться соответствующей записью в протоколе;
- данные о хеш-сумме файла, зафиксированного на электронном носителе информации;
- данные об используемых технических средствах (программном обеспечении, компьютерной технике)[1].

Таким образом, процедура фиксации и изъятия следов преступной деятельности, образованных при помощи использования информационных технологий, требует определенного порядка, вызванного спецификой данных объектов, несоблюдение правил работы с такими доказательствами может привести к признанию полученных цифровых данных из сети Интернет или электронных носителей информации недостоверными и, как следствие, недопустимыми доказательствами по делу.

Тактика производства осмотра места происшествия

Местом происшествия по рассматриваемой категории преступлений выступают места использования цифровых устройств для совершения преступлений: выхода преступника в сеть Интернет, совершения телефонных звонков, встреч преступника с жертвой (жилища, административные здания, служебные кабинеты, салоны транспортных средств, участки местности и др.).

В целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для дела, узловой точкой в ос-

[1] См.: *Сааков Т.А.* Судебная автороведческая экспертиза объектов из цифровой среды при установлении демографических характеристик автора. С. 101—103.

мотре места происшествия является рабочее место лица, совершающего преступные действия с использованием информационных технологий. В зависимости от объекта преступных посягательств (конституционный строй, половая неприкосновенность и свобода личности, общественная безопасность или нравственность, собственность и т.д.) внимание следователя должно быть обращено не столько на само электронное устройство (его сразу же необходимо перевести в авиарежим, исключив сетевую активность и возможность дистанционного блокирования), с помощью которого лицо устанавливало связь с жертвой или распространяло запрещенный контент (его необходимо изъять и осмотреть отдельно), а на иные прямые или косвенные доказательства.

Это связано с трудностями идентификации конкретного лица, совершившего преступление с обнаруженного места, и даже конкретного электронного носителя информации (смартфона, электронного планшета, ноутбука и т.д.). Обнаружение таких мест и устройств, даже если это место жительства (работы) или электронное устройство конкретного лица, далеко не всегда позволяет установить тот факт, что именно данное лицо совершало противоправные действия. В таких ситуациях на помощь следователю может прийти комплексный подход, использование всего арсенала криминалистического учения о следах преступной деятельности.

Внимательному изучению, фиксации и изъятию подлежат объекты, на которых преступник мог оставить свои следы в виде пятен крови, спермы, волос, следов пальцев рук, обуви, транспортного средства, микроволокон и других. В связи с этим фиксации и изъятию могут подлежать не только компьютер, смартфон, роутер, а также иные цифровые устройства и внешние накопители, но и клавиатура, компьютерная мышь, коврик, принтер, сканер, кресло, на котором сидел злоумышленник, данные видеокамер. Целесообразно делать смывы со стола, за которым предположительно находился преступник, изъять объекты, вероятно находящиеся в непосредственном контакте с подозреваемым (посуда, остатки пищи, записные книжки и пр.). Интерес представляет имеющаяся на месте происшествия литература, визитные карточки, распечатанные тексты (в том числе черновики), одежда подозреваемого.

Безусловно, что подробной фотофиксации и описанию в протоколе подлежит сам компьютер, а также все подключенное пе-

риферийное оборудование, планшет, смартфон или иные электронные устройства — средства коммуникации. В случае если компьютер выключен, включать его не рекомендуется, его марка, модель, возможно инвентаризационный номер указаны, как правило, на тыльной стороне моно- или системного блока.

Если же компьютер включен, необходимо зафиксировать содержимое экрана, все прикрытые вкладки, историю браузера (программы просмотра содержимого сайтов) за последние сутки, а также открыть параметры (свойства) компьютера (системы) и отразить в протоколе конфигурацию операционной системы. Криминалистическое значение в последующем может иметь «имя устройства», характеристики фото- и видеокамер, данные процессора, код устройства и продукта, а также данные учетной записи и пароль для открытия самого компьютера. Последний (при наличии) целесообразно уточнить у пользователя, его работодателя, родственников, представителей охраны непосредственно в ходе следственного действия. Данные рекомендации, безусловно, экстраполируются на все иные электронные устройства, в идентификации которых в дальнейшем может возникнуть необходимость.

После указанных действий целесообразно зафиксировать с помощью фото- и видеоаппаратуры все сетевые подключения, которые описываются специалистом и заносятся в протокол. В случае большого количества кабелей их рекомендуется нумеровать и маркировать цветными обозначениями (стикерами).

Следует обращать внимание на место нахождения и возможного сокрытия мобильных телефонов, и в особенности извлекаемых из них накопителей (например, sim-карт, micro SD), а также на поведение участников уголовного судопроизводства, пытающихся воспользоваться мобильным устройством для создания препятствий расследованию, либо удалить какую-либо информацию, блокировать устройство непосредственно или дистанционно.

Так, при осмотре места происшествия по данной категории уголовных дел (как и в ходе обыска или выемки) следует изымать все компьютеры, планшеты, мобильные устройства, sim-карты, micro SD, находящиеся у подозреваемых, для установления, в частности, их последних контактов, местонахождения в интересующее следователя время, а также иных обстоятельств.

При обнаружении мобильного телефона того или иного участника уголовного судопроизводства, алгоритм действий следователя должен быть следующим:

1) перевести телефон в авиарежим, исключив сетевую активность (возможное блокирование устройства), и выяснить, не синхронизирован ли аппарат с компьютером и другими гаджетами пользователя;

2) зафиксировать в протоколе следственного действия и сфотографировать место расположения телефона.

При этом следует иметь в виду возможность и необходимость в последующем назначения по данному объекту молекулярно-генетической экспертизы / экспертизы запаховых следов человека, например, при отказе лица признавать принадлежность обнаруженного мобильного устройства, или, когда принадлежность установить невозможно, такое положение дел предполагает необходимость соответствующей упаковки данного объекта в соответствии с криминалистическими рекомендациями по работе с биологическим следами.

Далее, необходимо описать в протоколе и сфотографировать переднюю, заднюю панели телефона, его повреждения, информацию с экрана, все слоты, модель, IMEI и другие сведения о телефоне, а также все внешние источники (sim-карты, карты памяти), батарею, чехол. Напомним, что модель и IMEI телефона (GSM) указаны под аккумулятором сверху. Также IMEI можно определить путем набора следующей комбинации - *#06#. Информацию о модели, операционной системе телефона можно получить и зафиксировать с помощью фотоаппарата в памяти телефона (Меню — Настройки — Информация об устройстве);

3) необходимо, прежде чем выключить телефон, просмотреть и зафиксировать в протоколе, а также с помощью фотоаппарата последние контакты;

4) изъять телефон и комплектующие к нему (зарядное устройство, провода питания);

5) выключить-включить телефон и убедиться, отсутствует ли пароль на включение-активацию. В случае наличия пароля, ПИН-кода постараться выяснить его у владельца и занести в протокол.

Изъятые в ходе следственного действия электронные устройства и другие объекты предъявляются понятым и иным лицам,

присутствующим при проведении следственного действия, фотографируются, упаковываются и опечатываются таким образом, чтобы исключить несанкционированный доступ к информации, т.е. любое подключение к устройству (в картонные коробки или полиэтиленовые мешки в выключенном состоянии).

Тактические производства обыска (выемки)

Обыск по данной категории дел целесообразно проводить с применением соответствующих технических средств, позволяющих обнаружить мобильные устройства и электронные накопители в помещениях, автотранспорте и на открытых участках местности, в частности нелинейные локаторы («Лорнет-36» «NR-2000», «Люкс», «ORION HGO-4000» и др.). Кроме того, возможно использование приборов по обнаружению мобильных средств, как находящихся в режиме регистрации, так и работающих в режиме приема-передачи голосового и текстового сообщений (например, приборы Р-100, BVS WH, «Семафор» и др.).

При производстве обыска участвует лицо, в помещении которого производится обыск, либо совершеннолетние члены его семьи. В протоколе обыска (выемки) должно быть указано, в каком месте и при каких обстоятельствах были обнаружены мобильные устройства, выданы они добровольно или изъяты принудительно. Все изымаемые устройства должны быть перечислены с точным указанием их количества, индивидуальных признаков и стоимости. Если в ходе обыска были предприняты попытки уничтожить или спрятать мобильные устройства (стереть информацию, хранящуюся в их памяти), то об этом в протоколе делается соответствующая запись и указываются принятые меры.

Ввиду специфики цифрового следообразования и возможности утраты таких следов обыск (выемка, осмотр) в жилище проводят неотложно в соответствии с ч. 5 ст. 165 УПК РФ без получения судебного решения на основании постановления следователя или дознавателя с последующим уведомлением судьи и прокурора о производстве следственного действия.

Особняком в данном случае находится ряд экономических преступлений (ч. 4.1 ст. 164 УПК РФ), по которым не допускается

необоснованное изъятие электронных носителей информации, за исключением случаев, предусмотренных ч. 1 ст. 164.1 УПК РФ:

1) вынесено постановление о назначении судебной экспертизы в отношении электронных носителей информации;

2) изъятие электронных носителей информации производится на основании судебного решения;

3) на электронных носителях информации содержится информация, полномочиями на хранение и использование которой владелец электронного носителя информации не обладает, либо которая может быть использована для совершения новых преступлений, либо копирование которой, по заявлению специалиста, может повлечь за собой ее утрату или изменение.

В соответствии с требованиями ст. 164.1 УПК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий» электронные носители информации изымаются в ходе производства следственных действий с участием специалиста. По ходатайству законного владельца изымаемых электронных носителей информации или обладателя содержащейся на них информации специалистом, участвующим в следственном действии, в присутствии понятых с изымаемых электронных носителей информации осуществляется копирование информации.

В данном случае следует учитывать два момента. Во-первых, в качестве специалиста в данном случае может приглашаться любое лицо, обладающее знаниями в области электронных устройств (консультанты специализированных магазинов, программисты, сотрудники технических подразделений правоохранительных органов и др.), а во-вторых, в ходе проведения данных следственных действий копировать информацию все-таки не желательно, так как это может повлечь ее утрату либо спорные вопросы о консервации имеющейся информации на момент проведения следственного действия.

Следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные

носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

В протоколе должны быть указаны также технические средства, примененные при производстве следственного действия, условия и порядок их использования, объекты, к которым эти средства были применены, и полученные результаты, а также отмечено, что лица, участвующие в следственном действии, были заранее предупреждены о применении при производстве следственного действия технических средств.

В случае задержания подозреваемого в ходе производства его личного обыска также целесообразно изымать его мобильный телефон. Кроме того, рекомендуется с этой же целью произвести обыски в местах его жизнедеятельности (учебы, работы, проживания и др.).

Фиксация хода и результатов следственных действий производится по описанным выше правилам.

Тактика производства следственного эксперимента

В ходе расследования рассматриваемых уголовных дел следственный эксперимент может производиться в следующих формах.

1. Как предшествующее (подготовительное) получению информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) следственное действие, нацеленное на сбор информации о базовых станциях (их номерах и идентификаторах), зонах их покрытия на месте происшествия или по маршрутам предполагаемого движения преступника.

Такой эксперимент заключается, во-первых, в примерном моделировании поведения участника исходя из анализа следовой обстановки, показаний самого проверяемого или других участников процесса; во-вторых, в измерениях радиоэлектронной обстановки и сбора данных о базовых станциях. Так, по неочевидным преступлениям в ходатайстве в суд и, соответственно, в постановлении суда перечисляются конкретные базовые станции, которые необходимо проверить (с зоной покрытия в месте совершения преступления, обнаружения трупа либо по маршруту движения преступников и пр.).

Современные криминалистические приборы — датчики оценки радиоэлектронной обстановки, стоящие на вооружении правоохранительных органов, а также находящиеся в свободном доступе программы Netmonitor , G-nettrack и др. позволяют следователям самостоятельно или с привлечением специалиста (работников радиочастотных центров или инженеры операторов связи) в рамках следственного эксперимента отследить и зафиксировать в конкретном месте или по определенному маршруту базовые станции различных типов сети (2G, 3G, LTE) всех операторов связи одновременно и сделать оператору точечный запрос с указанием идентификационных данных станций (LAC[1], CID[2] — для типа сети 2G, 3G либо TAC и CL — для LTE). В этом случае оператор будет точно знать, какие базовые станции ему необходимо проверить на предмет телефонных голосовых соединений абонентов и передачи текстовых сообщений в указанный следователем период времени.

2. Проверка навыков лица, его профессиональных способностей создания вредоносных программ, программирования и пр.

Тактика получение информации о соединениях между абонентами[3] и (или) абонентскими устройствами[4]

Данное следственное действие проводится после возбуждения уголовного дела и состоит в истребовании следователем по судебному решению у операторов сотовой связи и последующем осмотре (чаще с помощью специалиста) сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием),

---

[1] Local Area Code — код территории обслуживания.

[2] Cell IDentificator — идентификатор базовой станции внутри территории обслуживания.

[3] Абонент — это пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации (п. 1 ст. 2 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»).

[4] Абонентское (пользовательское или оконечное) оборудование (базовая станция) — это технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей (п. 10 ст. 2 Закона «О связи»).

номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций.

Исходя из наименования следственного действия, оператор вправе предоставить по судебному решению информацию: а) о соединениях между абонентами; б) о соединениях между абонентскими устройствами.

Ключевым моментом в данном случае является именно факт соединения (входящий, исходящий, даже непринятый звонок), SMS-сообщение, интернет-соединение). Если же соединения не производилось, а сотовый телефон (смартфон, планшет с sim-картой) был включен и, соответственно, «привязан» к конкретной базовой станции (технический биллинг), суд не может удовлетворять ходатайства следствия об установлении места расположения базовых станций, а оператор их исполнять, несмотря на то что технически это возможно.

В то же время получение информации о пополнении счета, перечне подключенных услуг, факте регистрации в сети конкретного мобильного устройства (по номеру IMEI[1]), принадлежности абонента по MSISDN, либо ICC (ФИО, адрес регистрации по месту жительства) по известному номеру (такая информация фиксируется оператором при заключении договора и выдаче sim-карты), либо, наоборот, об абонентском номере и номере IMEI по известным анкетным данным не относится к данному следственному действию. Такая информация является справочной и может быть получена следствием без судебного решения путем запросов к оператору связи либо дачи поручений органу дознания о проведении оперативно-розыскного мероприятия — наведения справок.

Дату активации мобильного телефона, новый абонентский номер, ФИО абонента, число, месяц и год его рождения, адрес регистрации по месту жительства, а также непосредственно детализацию звонков и месторасположения базовых станций возможно в дальнейшем получить уже по судебному решению путем проведения рассматриваемого следственного действия.

---

[1] IMEI (англ. International Mobile Equipment Identity — международный идентификатор мобильного оборудования) — это уникальный номер для идентификации телефонов стандартов GSM, WCDMA и IDEN, а также некоторых спутниковых телефонов (15 цифр).

В соответствии со ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» при проведении уполномоченными государственными органами следственных действий операторы связи обязаны оказывать этим органам содействие в соответствии с требованиями уголовно-процессуального законодательства.

Отметим, что, несмотря на включение в уголовно-процессуальный закон данного следственного действия, единая практика непосредственного получения у оператора связи по судебному решению указанной информации отсутствует. В ряде регионов страны следователи по-прежнему получают информацию за счет выемки, другие — дают поручение органу дознания, третьи — получают информацию о соединениях самостоятельно.

По мнению О.Ю. Антонова, данное следственное действие носит комплексный характер и состоит из следующих этапов.

1. Анализ следственной ситуации и принятие решения о его проведении.

2. Подготовительный этап, подразделяемый на стадии:

2.1) следственный осмотр в целях оценки радиоэлектронной обстановки (факультативно);

2.2) процессуальная (подготовка и направление в суд ходатайства следователя о производстве следственного действия),

2.3) организационная (направление следователем решения суда осуществляющей услуги связи организации);

2.4) организационно-техническая (действия оператора связи по формированию и предоставлению информации).

3. Рабочий этап — следственный осмотр полученной информации:

3.1) стадия принятия решения о проведении непосредственно следователем с участием специалиста либо по поручению — следователем-криминалистом;

3.2) рабочая стадия — проведение анализа непосредственно либо с применением аппаратно-программных комплексов (далее — АПК);

3.3) стадия фиксации хода и результатов.

4. Оценка и использование результатов следственного осмотра, по результатам которых могут появляться новые факультативные стадии:

4.1) направление повторного или дополнительного запроса оператору связи;

4.2) допрос представителя осуществляющей услуги связи организации;

4.3) производство новых следственных действий, в том числе связанных с получением новой информации о соединениях между абонентами и (или) абонентскими устройствами[1].

Данное следственное действие направлено на решение следственными органами следующих криминалистически важных *задач*:

1) детализация соединений абонента (возможно, еще не установленного[2]) в определенное время — получение сведений о дате, времени, продолжительности, частоте соединений между абонентами (либо отсутствии соединений), типе соединения (входящий, исходящий звонок, SMS-сообщение);

2) получение информации о втором абоненте, с которым производилась связь (абонентский номер, ФИО, адрес регистрации, в свою очередь, дальнейшее получение информации о его соединениях);

3) определение места нахождения устройства (телефона, смартфона, планшета) и его пользователя на момент первого соединения с базовой станцией (адрес базовой станции, участок местности, в котором находился абонент в определенное время);

4) установление маршрута и способа (пешком или на транспорте) движения абонента в определенное время по адресам базовых станций, азимуту — зоне покрытия ее ретранслятора, мест встреч абонентов.

Причем описываемое следственное действие позволяет анализировать указанные сведения не только в ретроспективе — за уже прошедшее время, но и в перспективе — в будущем — на период до шести месяцев. При этом организация, осуществляющая услуги связи в течение всего срока производства данного следственного действия, обязана предоставлять следователю указанную информацию по мере ее поступления, но не реже одного раза в неделю[3].

---

[1] См.: *Антонов О.Ю.* Принципы получения информации о соединениях между абонентами и (или) абонентскими устройствами // Вестн. Воронеж. гос. ун-та. Сер. Право. 2021. № 1 (44). С. 241.

[2] В таком случае копии постановления направляются всем операторам связи, обслуживающим определенную территорию.

[3] В то же время следует иметь в виду, что оператор вправе заблокировать sim-карту и передать абонентский номер другому пользователю при длительном неиспользовании данного номера (2—6 месяцев).

Рассматриваемое следственное действие целесообразно применять не только по тем преступлениям, в ходе которых преступники завладели мобильными устройствами жертвы (кражи, грабежи, разбои, убийства и др.), но и по иным преступлениям при подготовке, совершении или сокрытии которых преступники могли использовать сотовую связь, к примеру, в ходе расследования коррупционных, серийных преступлений, преступлений террористической, экстремистской направленности прошлых лет, безвестных исчезновений людей. Важно, что соединения в виде входящих звонков, SMS-сообщений, мгновенной переписки в мессенджерах происходят без воли на то владельцев гаджетов.

Данное следственное действие проводится не только в ситуациях, когда следователю стали известны установочные данные абонента (ФИО, адрес регистрации по месту жительства) либо его абонентский номер, IMEI мобильного устройства, но и по неочевидным преступлениям, когда есть предположение, что на месте происшествия преступник (свидетель, потерпевший) пользовался сотовой связью (были соединения).

Суд удовлетворяет ходатайство следствия о получении информации о соединениях между абонентами и (или) абонентскими устройствами лишь при наличии достаточных оснований полагать, что такая информация имеет значение для уголовного дела. Поэтому, принимая решение о проведении следственного действия, следователь оценивает обстановку произошедшего, моделирует деятельность всех участников и решает вопрос о необходимости его проведения, обосновывает в ходатайстве целесообразность этого, заранее предполагая, какие результаты он хочет получить (детализация соединений абонента в определенное время; выяснение номеров иных абонентов и их идентификация, установление места нахождения устройства и его пользователя, маршрута его движения).

В зависимости от того, какие задачи стоят перед следствием, в постановлении о возбуждении перед судом ходатайства о производстве следственного действия, помимо фабулы дела и обоснования целесообразности получения данной информации, указываются дополнительные необходимые для следствия данные.

При этом возможны следующие исходные следственные ситуации относительно информации об абоненте, которой располагает следствие:

1) установочные данные абонента и номер его телефона известны;

2) известен только абонентский номер участника, но не известны его установочные данные (ФИО, адрес регистрации);

3) установлены ФИО проверяемого, но не известен абонентский номер;

4) информации о проверяемом(ых), нет, но есть обоснованное предположение о том, что на месте приготовления, совершения или в ходе постпреступного поведения у лиц были соединения через сотовую связь[1].

В первых двух ситуациях, когда известен оператор связи (МТС, «Вымпелком», «Мегафон», «Теле-2» и др.), постановление передается чаще в отдел безопасности конкретного оператора. В третьей ситуации сначала уточняется абонентский номер (справочная информация — путем запроса), а затем запрашивается детализация. А в четвертой — копии судебных решений направляются всем операторам одновременно. В Следственном комитете Российской Федерации распространена практика, когда следователи и следователи-криминалисты, исходя из сложившейся ситуации, особенностей обстановки совершенного преступления (к примеру, убийство и предшествующее перемещение живого человека или в последующем сокрытие трупа в ином месте, похищение, перемещение и удержание человека, изнасилование группой лиц, грабеж и изъятие сотового телефона жертвы, террористический акт, где средством инициирования взрыва был мобильный телефон, безвестное исчезновение ребенка с телефоном и т.п.), для решения вышеуказанных задач тщательно готовятся к проведению следственного действия, проводя следственные эксперименты в целях радиоэлетронной разведки.

При тщательной подготовке к следственному действию, прогнозировании ожидаемых результатов эффективность получения

[1] См.: *Антонов О.Ю.* Тактика получения и использования криминалистически значимой информации от операторов связи. С. 5.

информации о соединениях обеспечивается также последующим тщательным осмотром полученной информации как на бумажных, так и на электронных носителях.

Если ситуация несложная, преступление очевидное и следственное действие проводится для так называемого закрепления доказательственной базы, следователь может произвести осмотр детализации (документов) самостоятельно. Однако по сложным, многоэпизодным делам, неочевидным преступлениям осмотр производится с участием специалиста, а также с помощью специальных аналитических программ (например, Belkasoft) и программно-аппаратных комплексов (Сигмет-С, Глобус — клиент).

В первом случае — в бесконфликтной ситуации — чаще всего подтверждаются:

1) нахождения смартфона (планшета, телефона) и его пользователя — потерпевшего, свидетеля, подозреваемого или обвиняемого — в конкретном месте в известное время;

2) маршрут их движения относительно базовых станций;

3) выявление номеров иных лиц, с которыми происходило соединение, и их проверка в порядке ст.186.1 УПК РФ (этими лицами могут быть преступники либо, наоборот, жертвы при явке с повинной виновного лица), а также проверка показаний свидетелей произошедшего.

Также это следственное действие можно проводить как в отношении подозреваемых (обвиняемых), так и в отношении потерпевших и свидетелей для подтверждения места их нахождения в определенное время в конкретном месте либо для выявления номеров преступников для последующего получения детализации уже их соединений.

Если ряду следственных действий обязательно предшествует иное следственное действие (например, опознанию и проверке показаний на месте всегда предшествует допрос), то в данном случае, наоборот, после получения информации о соединениях, как правило, следует осмотр полученной детализации (осмотр документов), а также нередко и повторение анализируемого следственного действия, но уже относительно новых, выявленных в ходе первого обстоятельств (по иным номерам и абонентам). В то же время решение о проведении данного следственного действия

принимается чаще всего после осмотра места происшествия, следственного эксперимента, осмотра документов (видеозаписей преступных событий), допросов, когда следователь убежден в том, что преступник (потерпевший, иной участник) использовал мобильное абонентское устройство.

Внимательный анализ полученной по решению суда от оператора информации о соединениях между абонентами и (или) абонентскими устройствами (детализации соединений или биллинговой информации) позволяет ответить на ряд иных вопросов, интересующих следователя, и решить дополнительные задачи:

- подтвердить факт подготовительной преступной деятельности, ее сокрытие;
- раскрыть неочевидное преступление и выявить всех его соучастников, свидетелей (в том числе с помощью фильтрации местных жителей от преступников-«гастролеров» либо выявления скрывшихся после совершения преступления лиц, которые прекратили соединения, выключили или выбросили телефон);
- установить место нахождения пропавшего без вести, скрывающегося преступника;
- вскрыть новые эпизоды противоправной деятельности, ее серию;
- доказать структуру, устойчивость преступной группы;
- идентифицировать труп абонента; и др.

Типовой формы и исчерпывающей информации о соединениях между абонентами операторами сотовых сетей не разработано. Примерно различные операторы предоставляют в распоряжение следователя следующие таблицы биллинга[1].

В таблицу также включаются сведения о номере проверяемого абонента (например, +79034567777), идентификатор его мобильного устройства IMEI (15-значный код, к примеру — 983456403377228).

[1] Для успешного последующего анализа информации о соединениях с использованием аппаратно-программных комплексов необходимо, чтобы такие данные предоставлялись в формате Exel, о чем в ходатайстве делается соответствующая отметка.

Дата	*Время*	*Номер абонента (с которым связь)*	*Продолжительность*	*Тип звонка*	*Адрес базовой станции*
05.11.18	10.35	+79054836573	00:02:50	Исходящий	г. Энск, ул. Красина, д. 17 (ТРЦ «Огни»)
07.11.18	17.20	+79103077690	00:05:30	Входящий	г. Энск, ул. Печная, д. 235 (столб)
8.11.18	05.12	+79035466999	—	SMS	г. Энская обл. дер. Иваново ул. Ленина, д. 2 (Башня на крыше гаража)

Кроме того, могут быть дополнительно включены (а если следователь об этом укажет в ходатайстве, то включаются): азимут зоны покрытия базовой станции[1] (угол от 0 до 360 градусов, например 140 градусов) и время прохождения сигнала от мобильного устройства до базовой станции (TA - Timing Advance — опережение по времени, т.е. приблизительное расстояние звонившего до базовой станции). Последний показатель от 1 до 20 применим лишь для типа сети 2G, где каждому показателю соответствует значение в 550 метров[2].

Таким образом, зная азимут базовой станции и показатель TA в формате связи 2G, можно определить и нанести на карту сектор,

[1] Базовая станция покрывает угол, равный 60 градусам. Азимут (угол), который указывает оператор в таблице, — это вектор, который высчитывается от 0 градусов (севера) и разделят угол покрытия пополам, т.е. по 30 градусов в разные стороны.

[2] Таким образом, если показатель TA равен 0, то мобильное устройство и, скорее всего, его пользователь находились на расстоянии от 0 до 550 метров от базовой станции, показатель 1 — от 550 до 1100 метров в направлении указанного азимута (60 градусов) и т.д.

в котором находилось мобильное устройство и его пользователь. Это зачастую оказывает неоценимую пользу следствию при поиске пропавших людей, подтверждении (опровержении) нахождения участника уголовного судопроизводства в определенное время в конкретном месте и т.п.

Указанные сведения можно получить за счет того, что оператор, предоставляющий услуги связи, осуществляет учет всех соединений в соответствии с гражданским законодательством и договором об оказании услуг связи в целях фиксации трафика, платежей и отчетности перед абонентом. Это и называется биллингом[1].

В ходе осмотра детализации обращается внимание на тип соединения (входящий или исходящий звонок, SMS-сообщение), частоту соединений. Следственная практика подтверждает, что в ходе подготовки, совершения и сокрытия преступления интенсивность и продолжительность соединений соучастников либо преступника и жертвы резко увеличиваются. В случаях когда в таблице детализации отражаются данные о текстовых сообщениях (SMS-сообщение, чаты), в последующем необходимо изымать гаджеты проверяемых лиц и знакомиться с соответствующей текстовой информацией, содержащейся в них, восстанавливать с помощью специализированной криминалистической техники (X-RAY, UFED, «Мобильный криминалист») удаленные сообщения, скорее всего уличающие данных лиц в совершенном преступлении либо ориентирующие следователя, помогающие ему выбрать верное, оптимальное направление расследования.

При анализе времени соединений необходимо сопоставлять время совершения преступления, смерти пострадавшего. Часто преступления против личности совершаются в ночное время, следовательно, ночные соединения всегда привлекают внимание следствия. Продолжительность соединений может указывать за тщательную проработку деталей планируемого или скрываемого преступления в ходе разговора по сотовому телефону либо, наоборот, коротких команд организаторов.

---

[1] Биллинг в электросвязи — комплекс процессов и решений на предприятиях связи, ответственных за сбор информации об использовании телекоммуникационных услуг, их тарификацию, выставление счетов абонентам, обработку платежей.

По номеру абонента и типу соединения можно определить регион и страну оператора связи, а также марку мобильного телефона. Такая информация представляет интерес в ситуациях, когда в качестве основной проверяется версия о том, что преступление совершил преступник-«гастролер», т.е. житель другого региона или страны.

Адреса базовых станций указывают на место нахождения гаджета в момент соединений и его владельца, маршрут движения проверяемого лица. По делам об изнасилованиях, убийствах, похищении человека или корыстно-насильственных преступлениях, в которых предметом хищения является смартфон, преступник и потерпевший (следовательно, и их телефоны) находятся в одном месте их встречи, передвигаются в одном направлении, либо похищенный телефон находится у преступника.

Полезно в этом случае получать одновременно информацию о соединениях потерпевшего и подозреваемого. Если же преступление не раскрыто и личность (как и абонентский номер) преступника не установлена, производится массовый биллинг по тем базовым станциям, с которыми соединялся телефон потерпевшего. Таким образом, с использованием указанных программ и комплексов можно вычислить абонентский номер, который регистрировался в тех же местах, с теми же базовыми станциями, т.е. двигался параллельно с телефоном потерпевшего.

Решению этой задачи способствует то обстоятельство, что на смартфоны приходит большое количество рекламных сообщений либо сообщений в групповых чатах, а также и звонки родственников, самих сотрудников правоохранительных органов, SMS-сообщения. Причем, даже если гаджет выключен, а SMS-сообщение отправлено, оно хранится несколько суток на сервере оператора и при включении телефона доставляется, т.е. происходит соединение.

В связи с этим сотрудники правоохранительных органов отправляют SMS-сообщения даже на выключенные номера лиц, пропавших без вести, которых похитили и т.п., для последующего определения точки регистрации их телефона с базовой станцией и, соответственно, предположительного места нахождения разыскиваемого лица.

На основании п. 22 постановления Правительства РФ от 9 декабря 2014 г. № 1342 «О порядке оказания услуг телефонной свя-

зи» (вместе с «Правилами оказания услуг телефонной связи») оператор при заключении договора с абонентом — физическим лицом и предоставлении сим-карты обязан осуществлять проверку достоверности сведений об абоненте и вносить договор следующие данные: ФИО, место жительства, дату рождения, реквизиты документа, удостоверяющего личность (серию и номер паспорта), место регистрации по месту жительства.

В то же время лица, замышляющие преступления, пытаются обойти эти требования, нарушая данные правила, пользуются абонентскими номерами, зарегистрированными на юридические либо подставные (умершие или вымышленные) лица. В таких случаях их идентификация затруднена.

Кроме того, преступники в целях противодействия следствию, выстраивания себе или иным лицам ложного алиби порой специально оставляют свой телефон в ином месте и организуют соединения (звонки, SMS-сообщения). Поэтому, безусловно, в ходе расследования преступлений необходимо использовать весь арсенал следственных и иных процессуальных действий в комплексе, не полагаться лишь на единственный аргумент или результат.

Помощь специалиста необходима в тех случаях, когда преступление неочевидное и (или) серийное, когда следователю сложно разобраться в большом объеме полученной детализации, сопоставлении нескольких детализаций.

По делам, связанным с безвестным исчезновением людей, полезным для их поиска является установление точки последней регистрации абонента. Также осуществляется розыск лиц, скрывающихся от следствия в отдельном месте и производящих звонки с привязкой к конкретной (одной и той же) базовой станции.

Имея информацию о месте нахождения такой станции, зная азимут ее действия и показатель Timing Advance, с помощью компаса, карты и транспортира можно определить участок местности и даже высоту (этаж), где находились и, возможно, еще находятся смартфон и его пользователь.

Подобные иллюстрированные приложения к протоколу осмотра детализации (документов) в виде социального графа связей, участков карт с обозначением зон покрытия и маршрутов движения довольно успешно ложатся в основу доказательств в судах, в том числе с участием присяжных заседателей.

На заключительной стадии осмотра полученной информации детализация приобщается к материалам уголовного дела в полном объеме на основании постановления следователя как вещественное доказательство и хранится в опечатанном виде в условиях, исключающих возможность ознакомления с ней посторонних лиц и обеспечивающих их сохранность.

4.3. Использование в ходе расследования преступлений, совершенных с использованием информационных технологий, информации из открытых источников (OSINT)

А.А. Бессонов[1]

Сегодня в условиях активного развития информационного общества и виртуального пространства, генерирующих экспоненциально увеличивающиеся большие данные (Big Data), информационно-телекоммуникационные сети представляют собой важнейший источник криминалистически значимой информации, выступающей одной из ключевых основ получения сведений обо всех обстоятельствах совершенных преступлений различных видов, в первую очередь совершенных с использованием IT-технологий, и о причастных к ним лицах.

Проиллюстрируем сказанное некоторой статистикой. Так, по состоянию на начало 2023 г. во Всемирной паутине зарегистрировано более 1,9 млрд сайтов и более 5,4 млрд пользователей (68,4% населения Земли)[2], на январь этого же года — 4,6 млрд чел. являются участниками социальных сетей (58,4%) и 5,3 млрд чел. используют мобильные телефоны (67,1%)[3]. Становится очевидным, что более 60% жителей нашей планеты оставляют цифровые следы о своей личности и жизнедеятельности, в том числе анкетные данные, фотографии, номера телефонов, сведения о геолокации и т.п. Уже привычным для слуха стал термин «цифровой портрет (профиль) личности». Большое количество таких

[1] Алексей Александрович Бессонов — ректор Московской академии Следственного комитета Российской Федерации, доктор юридических наук, доцент.
[2] https://www.internetlivestats.com (дата обращения: 20.01.2023).
[3] https://www.hootsuite.com/resources/digital-trends (дата обращения: 20.01.2023).

следов несет информацию о криминальной активности как отдельных личностей, так и организованных групп, позволяя вести речь о возрастающем потенциале ее использования в выявлении, раскрытии, расследовании и предупреждении преступлений.

Согласно статистическим сведениям МВД России, за 2022 г. зарегистрировано 522 065 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что составляет 26,5% числа всех деяний (в 2021 г. — 517 722 преступления, это 25,8% от всех преступлений; в 2020 г. — 510 396, что составило 25% всех преступлений; 2019 г. — 294 409, от числа всех деяний — 14,5%). Основной массив криминалистически значимой информации о таких преступлениях содержится в их цифровых следах, между тем 70—75% из них остаются нераскрытыми.

К сказанному добавим, что не меньшее значение цифровые следы имеют в раскрытии преступлений общеуголовной направленности. Например, 54% преступлений, связанных с безвестным исчезновением несовершеннолетних, раскрываются с использованием сведений о телефонных соединениях, 5,7% — с помощью информации из социальных сетей[1]. Если обратиться к серийным преступлениям, совершенным из сексуальных побуждений, то 10% из них раскрывается на основе анализа сведений о телефонных соединениях, а 1% — благодаря информации из социальных сетей, содержащей переписку преступника и потерпевшего[2]. По 12,6% уголовных дел о преступлениях, связанных с умышленным уничтожением или повреждением имущества, такие следы приводят к установлению причастного к ним лица[3].

---

[1] См.: *Расследование* преступлений, связанных с безвестным исчезновением несовершеннолетних (первоначальный этап расследования): Науч.-практ. пособие / Под ред. докт. юрид. наук, проф. А.И. Бастрыкина. М.: Юрлитинформ, 2021. С. 89.

[2] Данные приведены по результатам изучения управлением научно-исследовательской деятельности (Научно-исследовательским институтом криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской Федерации 1068 преступлений, совершенных 184 серийными преступниками.

[3] См.: *Делов Н.С.* Криминалистическое обеспечение расследования умышленного уничтожения или повреждения имущества: Автореф. дис. … канд. юрид. наук. Ростов н/Д, 2022. С. 19.

Все указанное подтверждает насущную необходимость использования в поиске, выявлении и фиксации криминалистически значимой информации технологии, представленной совокупностью методов и имеющей название «Поиск и анализ информации из открытых источников» (OSINT — Open Source Intelligence), в числе преимуществ которой отмечается возможность работы с «большими» и разрозненными (неструктурированными) данными[1]. Суть этой технологии состоит в мониторинге с использованием информационно-аналитических методов (Data Mining) открытых источников информационно-телекоммуникационной среды и элементов ее инфраструктуры в целях поиска, обнаружения и фиксации криминалистически значимой информации, связанной с подготавливаемым, совершаемым или совершенным преступлением (преступлениями).

Иными словами, это техническое мероприятие, связанное с поиском и анализом значимой для расследования преступления общедоступной информации, содержащейся в информационно-коммуникационной сети Интернет.

Однако, как отмечают различные исследователи, имеются определенные уголовно-процессуальные и криминалистические сложности работы с такого рода следами и информацией:

- в УПК РФ не предусмотрено следственное действие, связанное с получением компьютерной информации, в том числе с удаленных компьютерных сетей и систем;
- отсутствуют международно-правовые нормы в сфере противодействия киберпреступности, регламентирующие транснациональную процедуру собирания криминалистически значимой информации;
- технология фиксации и изъятия цифровых следов преступлений и информации из открытых источников, необходимой для их расследования, находится в стадии активного

[1] См.: *Осипенко А.Л.* Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности // Оперативно-розыскная деятельность в цифровом мире: Сб. науч. тр. / Под ред. В.С. Овчинского. М.: Инфра-М, 2021. С. 164.

развития при отсутствии единого унифицированного подхода по этому вопросу[1];

- отсутствие четкой границы между возможностью неограниченного исследования информации из открытых источников, относящейся к категории персональных данных, и препятствием к этому ввиду отсутствия согласия субъекта таких данных на их обработку[2].

Обратимся к предусмотренному Федеральным законом от 12 августа 1995 г. № 144-ФЗ[3] (в редакции Федерального закона от 28 июня 2022 г. № 202-ФЗ) «Об оперативно-розыскной деятельности» оперативно-розыскному мероприятию «получение компьютерной информации» (ст. 6). Проводится это мероприятие с использованием оперативно-технических сил и средств органов Федеральной службы безопасности и органов внутренних дел на основании судебного решения.

Получение компьютерной информации представляет собой техническое мероприятие, связанное с копированием оперативно-розыскной информации с помощью специальных технических и программных средств путем проникновения в аппаратные компьютерные средства и системы, принадлежащие физическим и юридическим лицам[4].

---

[1] См.: *Семикаленова А.И., Рядовский И.А.* Использование специальных знаний при обнаружении и фиксации цифровых следов: анализ современной практики // Актуальные проблемы российского права. 2019. № 6 (103). С. 180; *Теория* информационно-компьютерного обеспечения криминалистической деятельности: Монография / Под ред. Е.Р. Россинской. М.: Проспект, 2022. С. 108—118.

[2] См.: *Абышко А.О.* Конец общедоступных персональных данных в России? К вопросу о Федеральном законе от 30 декабря 2020 года № 519-ФЗ // Закон. 2022. № 3. С. 97—107; *Щукина А.* Персональные данные в открытых источниках: «ВКонтакте», Instagram, Twitter и др. Их правовой статус и можно ли обрабатывать их без согласия пользователей // Zakon.ru [Электронный ресурс]. Режим доступа: URL: https://zakon.ru/blog/2020/8/18/personalnye_dannye_v_otkrytyh_istochnikah_vkontakte_instragram_twitter_i_dr_ih_pravovoj_status_i_moz?ysclid = l8n5lgnp 28292931026 (дата доступа 01.10.2022).

[3] См.: *СЗ* РФ.1995. № 33. Ст. 3349.

[4] См.: *Теория* оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского. 5-е изд., испр. и доп. М.: Инфра-М, 2021. С. 363; *Яковец Е.Н.* К вопросу о сущности и содержании оперативно-розыскного мероприятия «получение компьютерной информации» // Оперативно-розыскная деятельность в Инфра-М, 2021. С. 182.

Стоит отметить, что аналогичного по своей правовой и технологической природе следственного действия действующим уголовно-процессуальным законом не предусмотрено. Соответствующие цифровые следы, содержащиеся на электронных носителях информации, следователь (дознаватель) получает путем осмотра либо назначения и производства судебной экспертизы.

Согласно ч. 1 и ч. 4 ст. 7 Федерального закона от 27 июля 2006 г. № 149-ФЗ[1] (в ред. Федерального закона от 14 июля 2022 г. № 325-ФЗ) «Об информации, информационных технологиях и о защите информации», к *общедоступной информации* относятся общеизвестные сведения и иная информация, доступ к которой не ограничен, а применительно к сети Интернет — допускающая автоматизированную обработку без предварительных изменений человеком.

Исходя из этого и применительно к последней упомянутой сложности работы с цифровыми следами и информацией из открытых источников в процессе расследования преступлений отметим, что, во-первых, в момент регистрации в социальных сетях у пользователя испрашивается согласие на обработку его персональных данных и предоставление сведений о них третьим лицам в случаях, установленных национальным законодательством. Во-вторых, при получении информации, относящейся к персональным данным, в ходе осуществления оперативно-розыскной деятельности и/или производства расследования по уголовным делам ключевое значение имеет особая правовая природа этих видов государственной деятельности, регламентированной Федеральным законом «Об оперативно-розыскной деятельности» и УПК РФ. В связи с этим неверно экстраполировать на эти виды деятельности высказанную некоторыми судами позицию относительно того, что не являются общедоступными данные, содержащиеся в таких открытых источниках, как социальные сети и интернет-порталы объявлений («Авито», «Авто.ру»).[2] Последнее более справедливо относится к бизнес-аналитике.

В качестве примера практической реализации рассматриваемой технологии можно привести систему ePOOLICE, применяе-

---

[1] См.: *СЗ* РФ. 2006. № 31 (ч. 1). Ст. 3448.

[2] См.: *Постановление* арбитражного суда Московского округа от 09.11.2017 № Ф05-16382/2017 по делу № А40-5250/2017 // СПС «КонсультантПлюс».

мую в оперативно-розыскной и следственной деятельности с 2013 г. странами Европейского Союза и предназначенную для сканирования больших данных из всевозможных источников в поисках сведений, указывающих на различные виды преступлений, совершаемых организованными группами, в целях их выявления, раскрытия и предупреждения[1].

Технология получения и анализа информации из открытых источников, доступная для использования отечественным органам следствия и дознания, представлена бесплатными сервисами с открытым кодом, рядом коммерческих продуктов, специализированным программным обеспечением ограниченного распространения.

Методы, составляющие эту технологию, подразделяются на пассивные и активные. Первые не предполагают непосредственного взаимодействия с интересующим следствие субъектом, а вторые предусматривают легендированное взаимодействие с ним. Следует отметить, что зарубежные оперативно-розыскные органы в противодействии киберпреступности зачастую применяют активные методы в форме специальных полицейских операций, включающих оперативное внедрение в киберпространство, установление контроля за сетевым криминальным общением, применение специального программного обеспечения[2].

Широкие возможности получения криминалистически значимой информации рассматриваемая технология несет при работе с системами мгновенного обмена сообщениями (мессенджерами). К примеру, набирающий все бóльшую популярность Telegram привлекателен для преступников в первую очередь своей функцией секретных чатов, возможностью при использовании скрыть свой абонентский номер мобильной связи. Этот мессенджер используется криминалом для незаконного оборота наркотиков и оружия, распространения детской порнографии, экстремистских идей и ложной политически значимой информации (фейков), ко-

---

[1] См.: *Brewster, Ben & Andrews, Simon & Polovina, Simon & Hirsch, Laurence & Akhgar, Babak*. (2014). Environmental Scanning and Knowledge Representation for the Detection of Organised Crime Threats. ICCS 2014, LNAI 8577, pp. 275—280. DOI 10.1007/978-3-319-08389-6_22.

[2] См.: *Осипенко А.Л.* Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. 2021. № 1. С. 50—52.

ординации действий участников групповых преступлений и функционирования криминальных сообществ. Поиск оперативно-розыскной информации в Telegram возможен с помощью встроенных функций внешних поисковых систем (Google, «Яндекс» и др.) и ботов.

Фамилия, имя, никнейм (прозвище), аватар относятся к изменяемым параметрам пользователя, в то время как уникальный идентификационный номер (ID) является неизменяемым, поскольку необходим системе для точной идентификации пользователя. Что касается номера телефона, то преступники часто используют тот, который зарегистрирован на третьих лиц, либо применяют способы регистрации аккаунта без него. Между тем, отталкиваясь от ID пользователя, можно установить и другие связанные с его личностью данные, в том числе во внешних от обозначенного мессенджера онлайн-сервисах, к примеру, социальных сетях, интернет-сервисах для размещения объявлений. Также вполне возможен сбор данных о личностях администраторов информационных каналов и сообществ в Telegram.

Нельзя не упомянуть, что интересны функциональные возможности этого мессенджера, связанные с поиском пользователей, находящихся поблизости, созданием территориальных геочатов в радиусе от 100 метров до 10 километров. В конечном итоге это позволяет отслеживать перемещение конкретного пользователя на местности, а в некоторых случаях — даже в прошлые периоды времени. Существенную пользу это может принести в части получения оперативно-розыскной информации о разыскиваемом лице, членах преступных групп, организаторах и участниках массовых беспорядков.

Логирование[1] действий пользователей открывает возможности в установлении сведений об используемом им устройстве (модели, версии операционной системы и браузера), IP-адресе, провайдере услуг связи, часовом поясе, геолокации, средствах анонимизации интернет-трафика.

Таким образом, используя мессенджер Telegram, можно установить личность подозреваемого либо иного интересующего

[1] Логирование (журналирование) — метод записи в логи (текстовые файлы) в хронологическом порядке действий пользователя, работы приложений, системы и т.д.

следствие лица по ID пользователя, его IP-адресу, используемым некнейму, имени и фамилии, номеру телефона, сведениям об устройстве связи, геолокации, фотографиям, связанным с ним другим пользователям, а также по привязанным к нему чатам и каналам, в частности по платежным реквизитам и отправленным сообщениям.

Как пример успешного использования технологии OSINT при работе с Telegram можно привести уголовное дело об убийстве 10 октября 2018 г. в поселке Архангельское Московской области следователя по особо важным делам управления МВД на транспорте по Центральному федеральному округу Шишкиной, несколько месяцев остававшемся нераскрытым. Цифровые следы, оставленные преступниками в Telegram в процессе подготовки этого деяния, позволили установить их личности, включая заказчика[1].

Все описанное с определенной спецификой применимо и к иным сервисам мгновенного обмена сообщениями — WhatsApp, Viber, Signal, ICQ и др.

Еще большие возможности получения оперативно-розыскной информации из открытых источников раскрываются при работе с сетью Интернет. В качестве реализованных ресурсов отметим OSINT Framework[2] с открытым исходным кодом, предоставляющий возможности осуществлять поиск людей, адресов e-mail, номеров телефонов, IP-адресов и т.д., а также OSINT-SAN Framework[3], являющийся русскоязычной версией подобного программного продукта.

Следует также отметить, что при правильном использовании даже поисковики Google, «Яндекс» и т.п. становятся инструментами рассматриваемой технологии. К примеру, с их помощью возможен поиск профилей в социальных сетях, пользователей адресов электронной почты, интересующих объектов по фотографиям, информации об утечках учетных данных, файлов и страниц с определенным содержанием и т.д.

В частности, анализ профиля конкретного пользователя в социальных сетях позволяет получить информацию о круге его об-

[1] Уголовное дело № 2-34/2020, находящееся в архиве Московского областного суда.
[2] https://osintframework.com (дата доступа: 10.10.2022).
[3] https://osintsan.ru (дата доступа: 10.10.2022).

щения, использовавшихся при регистрации номере телефона и адресе электронной почты, месте нахождения и посещенных местах, психологических особенностях, включая эмоциональные, коммуникативные, мотивационные и ценностно-нравственные качества, а также данные о его психологическом благополучии[1]. Также там может содержаться информация о воздействии на его сознание третьих лиц в целях побуждения к каким-либо противоправным действиям (например, склонение к суициду, вербовка в террористические организации, побуждение к распространению экстремистских материалов и т.п.). При наличии у интересующего следствие лица нескольких страниц в различных социальных сетях, в том числе зарегистрированных под вымышленными данными, возможна его идентификация в качестве их пользователя[2]. Также возможно установление места нахождения скрывающегося от следствия лица, в том числе подозреваемого и обвиняемого.

Для получения криминалистически значимой информации вполне подойдут и онлайн-инструменты для бизнес-аналитики. К примеру, сервис Интегрум[3] предоставляет отчет, в том числе в форме визуализации в виде графа, об организациях и индивидуальных предпринимателях, зарегистрированных на территории Российской Федерации, их взаимосвязях между собой, участии в государственных закупках и упоминаниях в средствах массовой информации.

Автоматизированный поиск такой информации по открытым источникам, социальным сетям и теневому сегменту Интернета — Даркнету (Dark Net) возможен с программным комплексом

---

[1] См.: *Сумкин К.С., Тараненко Л.О.* Анализ страницы пользователя социальной сети «Вконтакте» // Молодой ученый. 2016. № 12 (116). С. 189—194; *Черемисова И.В.* Контент-анализ страниц активных пользователей социальной сети «Вконтакте» // Вестн. Волгоград. гос. ун-та. Сер. 11. Естественные науки. 2016. № 2 (16). С. 74—80.

[2] См.: *Бакаев В.А., Благов А.В.* Анализ профилей в социальных сетях // Информационные технологии и нанотехнологии (ИТНТ-2017): Сб. тр. III Междунар. конф. и молодежной школы. Самарский национальный исследовательский университет им. С.П. Королева. Самара: Предприятие «Новая техника», 2017. С. 1868—1871; *Бождай А.С., Тимонин А.Ю.* Исследование процесса идентификации человека в сетях открытого доступа и построения его социального профиля на основе технологии Big Data // Модели, системы, сети в экономике, технике, природе и обществе. 2016. № 2 (18). С. 112—119.

[3] https://contragent.integrum.ru/search/ (дата доступа: 20.01.2023).

«Охотник»[1] российского производителя ООО «Ти Хантер». К решаемым с его помощью задачам относятся:

- установление людей и связей между ними, включая скрытые и удаленные данные, социальные сети;
- выявление связей людей с юридическими лицами и юридических лиц между собой;
- поиск различных объектов и событий по географическим координатам;
- мониторинг закрытых преступных сообществ, форумов и маркетплейсов Даркнета;
- работа с мессенджерами WhatsApp, Telegram, Skype;
- анализ контента социальных сетей и веб-страниц;
- анализ операций с криптовалютами.

В качестве примера обзорно упомянем еще ряд сервисов, позволяющих использовать рассматриваемую технологию в интересах расследования преступлений. Так, сервис «Яндекс.Аудитории» предоставляет возможность поиска пользователей в сети Интернет по номерам их телефонов, адресам электронной почты, ID устройств[2]. IP Logger — сервис расширенной аналитики для поиска IP-адресов, отслеживания точного местоположения любого мобильного устройства или персонального компьютера, проверки URL-адресов путем анализа трафика посетителей веб-сайтов, блогов и т.п.[3] Существует еще и такой платный сервис, как Maltego, предоставляющий возможности поиска информации о различных объектах (номера телефонов, адреса электронной почты, ID пользователей социальных сетей и пр.) и установления их связей между собой[4].

Нередко при поиске значимой для следствия информации нужно обратиться к старым (более ранним) версиям веб-сайтов или архивным веб-сайтам. Например, при необходимости получения сведений об организациях или о людях, которые ранее работали в них, может оказаться, что текущий веб-сайт организации не содержит искомых сведений. При решении этой проблемы

[1] Свидетельство о государственной регистрации программ для ЭВМ № 20216 80077 от 07.12.2021.
[2] https://audience.yandex.ru (дата доступа: 20.02.2023).
[3] https://iplogger.org (дата доступа: 20.02.2023).
[4] https://www.maltego.com (дата доступа: 20.02.2023).

ценным ресурсом может оказаться платформа Wayback Machine[1], предоставляющая возможность обнаружения связей между различными веб-сайтами, их предыдущие версии и старые файлы, кэшированные изображения, имена людей и номера телефонов, адреса электронной почты и даже метаданные из старых версий интересующего веб-сайта.

При наличии потребности проведения анализа криптокошелька или транзакций криптовалюты в качестве первого действия рекомендуется применение именно рассматриваемой технологии OSINT, способствующей установлению информации о владельце криптокошелька или участнике транзакций криптовалют[2]. К примеру, следователем (дознавателем) в интересах расследования может быть использована платформа Tokenscope, предназначенная для оценки риска использования криптовалюты[3]. В этом плане также следует упомянуть сервис Росфинмониторинга «Прозрачный блокчейн», предназначенный для мониторинга криптовалютных транзакций, выявления конечных бенефициаров цифровых активов.

В качестве хорошего источника криминалистически значимой информации можно рекомендовать сведения из утечек баз данных разнообразных российских сервисов («Яндекс.Еда», Delivery Club, «Гемотест», СДЭК, «Почта России» и др.). После сбора из сети Интернет таких утечек их целесообразно объединить в одну базу данных и проиндексировать, например, с помощью программы типа «Архивариус 3000». Такие данные содержат в различных сочетаниях фамилии, имена, отчества людей, даты их рождения, почтовые адреса, номера телефонов, адреса электронной почты, регистрационные знаки автомобилей[4].

Следует иметь в виду, что в основе успеха поиска и анализа информации из открытых источников лежит комплексный под-

---

[1] https://digitalinvestigator.blogspot.com (дата доступа: 20.01.2023).

[2] См.: *Особенности* расследования преступлений, совершаемых с использованием цифровой валюты: Колл. монография / Колл. авторов; Под ред. Е.В. Емельяновой и О.С. Бутенко. СПб.: Следственный комитет Российской Федерации, 2021. С. 142.

[3] https://tokenscope.com (дата доступа: 20.02.2023).

[4] См.: *Bederov I.S.* Mobile database with information leaks [Электронный ресурс] // Режим до ступа: https://medium.com/@ibederov_en/mobile-database-with-information-leaks-e6f14bfe2f22 (дата доступа: 20.01.2023).

ход. Поиск совпадающих данных пользователя, представляющего интерес для решения задач расследования конкретного преступления либо серии преступлений, в различных онлайн-сервисах и базах данных — это путь установления его личности и иной связанной с ним значимой информации.

В системе Следственного комитета Российской Федерации на поиске цифровых следов и иной криминалистически значимой информации по расследуемым преступлениям с использованием технологии OSINT специализируется технико-криминалистическое управление Главного управления криминалистики (Криминалистического центра). Сотрудниками названного управления осуществляется поиск в открытом сегменте Интернета информационных следов, ассоциированных с пользователями социальных сетей (интернет-сайтов), и фотоизображений путем анализа биометрических характеристик лица, отличительных особенностей предметов или местности, похожих либо тождественных объектов; проведение информационно-аналитических исследований добытой информации в целях оперативного получения и структурирования достоверных разрозненных данных о пользователях интернет-ресурсов и хозяйствующих субъектах; выгрузка данных из стриминговых ресурсов и т.п.[1] Подобную работу в территориальных следственных органах проводят следователи-криминалисты и даже следователи самостоятельно.

Подводя итог, отметим, что информационно-телекоммуникационная среда и элементы ее инфраструктуры применительно к преступной деятельности содержат, во-первых, ее цифровые следы; во-вторых, иную информацию о механизме преступления, причастном к нему субъекте и связанных с ним иных лицах. Эти следы и информация обнаруживаются и фиксируются путем производства оперативно-розыскных мероприятий либо следственных действий с помощью специальных методов и инструментов рассмотренной технологии, реализуемых в форме наведения справок (в частности, его автоматизированной разновидности «информационного поиска») либо осмотра.

---

[1] См.: *Современные* возможности Главного управления криминалистики (Криминалистического центра) в сфере технико-криминалистического обеспечения расследований преступлений // Вестн. Гл. управления криминалистики. 2022. № 11 (80). С. 15.

4.4. Практика расследования преступлений, совершенных с использованием информационных технологий, следственными органами Следственного комитета Российской Федерации

А.И. Бастрыкин[1]

Следственным комитетом Российской Федерации в настоящее время организация расследования преступлений, совершенных с использованием информационных технологий, проводится по следующим направлениям.

Для организации системной работы в этой сфере в центральном аппарате Следственного комитета функционирует специализированный отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий, криминалистические и экспертные подразделения компьютерно-технических и инженерно-технических исследований, сотрудники которых осуществляют предварительное следствие, криминалистическое обеспечение и производство экспертиз по делам об указанных преступлениях. Для повышения эффективности и качества работы на данном направлении в территориальных следственных органах ведомства введена специализация следователей по расследованию указанного вида преступных деяний. С учетом особенностей конкретного уголовного дела проведение следственных действий, а также формирование исчерпывающей доказательственной базы поручаются наиболее опытным следователям, имеющим большой профессиональный стаж и обладающим необходимыми навыками работы.

В современных реалиях цифровизации важнейшее значение в борьбе с преступностью в сфере высоких технологий имеет организация взаимодействия на уровне профильных министерств и ведомств. Сотрудники СК России принимают участие в деятельности межведомственных рабочих групп и тематических совещаний, в рамках которых рассматриваются вопросы актуализации нормативной и методической базы по противодействию преступ-

[1] Александр Иванович Бастрыкин — Председатель Следственного комитета Российской Федерации, заслуженный юрист Российской Федерации, доктор юридических наук, профессор.

лениям в сфере информационных технологий. Особое внимание в коллективной работе уделяется вопросам расширения использования в практической деятельности автоматизированных поисковых систем, направленных на выявление, предупреждение и пресечение указанных преступлений. В частности, сотрудниками центрального аппарата ведомства на постоянной основе применяется сервис Росфинмониторинга для отслеживания операций с криптовалютой «Прозрачный блокчейн», возможности которого используются для установления цифровых транзакций по уголовным делам и деанонимизации пользователей.

В целях своевременного реагирования на вновь возникающие вызовы и угрозы, которые несут в себе риски совершения преступлений, связанных с использованием информационно-коммуникационных технологий, Следственным комитетом принимаются системные меры, в том числе связанные с внедрением технических комплексов и средств, межведомственных автоматизированных поисковых систем, региональных разработок, направленных на выявление, предупреждение и пресечение указанных преступлений.

С помощью криминалистической техники производится осмотр массивов открытых данных из информационно-телекоммуникационных сетей, преимущественно сети Интернет, сервисов обмена мгновенными сообщениями, а равно их производных, полученных в результате применения криминалистической и специальной техники (исследование и актуализация возможностей провайдеров хостинга, владельцев сайтов в информационно-телекоммуникационных сетях (Интернет, Deepnet, или Darknet), пиринговых ресурсов, а равно организаторов сервисов обмена мгновенными сообщениями для раскрытия преступлений, установления подлежащих доказыванию обстоятельств, обнаружения и закрепления таких следов преступления и ориентирующих следствие сведений в виртуальном пространстве, проведения поисковых мероприятий и розыска подозреваемых (обвиняемых), решения проблем противодействия киберпреступности в целом.

Так, осуществляются поиск в открытом сегменте Интернета информационных следов, ассоциированных с пользователями социальных сетей (интернет-сайтов), проведение информационно-аналитических исследований в целях оперативного получения и структурирования достоверных разрозненных данных о хозяй-

ствующих субъектах, выгрузка данных из стриминговых ресурсов и т.п., используются алгоритмы на основе нейросетей — путем анализа биометрических характеристик лица, отличительных особенностей предметов или местности осуществляется поиск фотоизображений, похожих или тождественных объектов среди различных источников в Интернете.

В целях анализа сведений из открытых источников информации (OSINT) в технико-криминалистическом управлении Главного управления криминалистики (Криминалистического центра) Следственного комитета (далее — ТКУ ГУК (КЦ) СК России) эффективно применяются ресурсы, перечень которых формируется с 2020 г. и постоянно актуализируется; инициативно создан информационный массив (Big Data) с рабочим названием Hunter Harpy, который непрерывно наполняется данными из Интернета (насчитывает более 23 млрд строк) и позволяет осуществлять автоматизированные проверку и установление личности пользователя Telegram, поиск по фотоизображению пользователя и его идентификацию с построением связей «друзей» в социальной сети «ВКонтакте», обнаружение информации по «утечкам баз данных» в сети Интернет, выделение IP-адресов из заданного текста, интернет-поиск информации по IP-адресу, а также выдачу отчетов. Для служебного пользования в ТКУ ГУК (КЦ) СК России разработаны: макрос для Microsoft Word, позволяющий существенно сократить работу по составлению объемных фототаблиц; приложение Ainobill для обобщения результатов оценки радиоэлектронной обстановки на месте происшествия (преступления) и подготовки проекта печатной версии протокола следственного действия (осмотр места происшествия или следственный эксперимент); приложение «Объектив» для сбора и систематизации фотоизображений в фотоархиве ТКУ ГУК (КЦ) СК России по рубрикам; приложение «ВК-архив», предназначенное для извлечения и группировки фотоизображений из переписки, предоставляемой социальной сетью «ВКонтакте», позволяющее быстро определить характер общения (используется при криминалистическом сопровождении дел о преступлениях против половой неприкосновенности и половой свободы личности); приложение Simple Searcher для сбора информации из групп и сообществ в социаль-

ных сетях («ВКонтакте», Telegram). Создание указанных инструментов благодаря внутренним ресурсам СК России и без привлечения дополнительных бюджетных средств на государственные закупки дорогостоящих программных решений позволяет обеспечить существенную экономию и планировать затраты на другую криминалистическую технику.

Прорабатывается вопрос о заключении соглашений о сотрудничестве с рядом компаний, функционирующих в сфере информационных технологий, кибербезопасности и обладающих инструментами обработки больших объемов данных. Такие соглашения ускорят обмен информацией по электронным каналам связи с этими компаниями. Возможности, которыми они располагают, значительно помогают следствию в расследовании преступлений. При этом необходимо исключить любые возможности нанесения вреда государственным органам и гражданам со стороны таких компаний в силу ставшей им известной информации. При выстраивании взаимодействия с частными организациями необходимо опираться на отечественные компании.

В то же время существующая активность правоохранительного блока в сегменте повышения оперативности и эффективности извлечения следов, образуемых в ходе преступной деятельности в сфере информационных технологий, при работе с открытыми источниками информации в сети Интернет представляется недостаточной и требующей корректировки. Так, в настоящее время сотрудники, осуществляющие оперативно-розыскную деятельность, осведомлены о постоянно изменяющихся возможностях получения оперативной и криминалистически значимой информации, позволяющей в сжатые сроки идентифицировать фигурантов уголовных дел, включая совершивших преступления в различных регионах страны, а также лиц, обладающих ценными сведениями, в том числе находящихся за пределами нашего государства. В связи с изложенным представляется необходимым проработать вопрос создания криминалистической системы, позволяющей идентифицировать пользователей сети Интернет по следам, образуемым в ходе преступной деятельности в сфере информационных технологий, обеспечив допуск 24/7 к такой системе представителей всех правоохранительных органов.

Необходимо отметить, что выявление, пресечение, расследование и предотвращение преступлений, совершаемых с использованием информационных технологий, требует серьезных специальных знаний от следователей, сотрудников, осуществляющих оперативное сопровождение, и вовлеченных специалистов и экспертов. По этой причине огромное значение приобретают непрерывный процесс изучения достижений науки и техники, а также вопросы обеспечения качественного обучения в целях актуализации компетенций указанных сотрудников. В целях повышения профессионального уровня следователей Следственного комитета разработаны специализированные учебные программы, например «Расследование преступлений в сфере информационных, телекоммуникационных и высоких технологий», «Расследование преступлений, совершенных с использованием цифровой валюты и цифровых финансовых активов». К реализации таких программ привлекаются лучшие российские ученые и практики, имеющие опыт работы в сфере информационных технологий, в том числе представители Росфинмониторинга, Банка России и др. Вместе с тем представляется, что применительно ко всем правоохранительным органам процесс обучения, повышения квалификации и обмена передовыми достижениями, в том числе с компетентными органами зарубежных партнеров, в области борьбы с постоянно обновляющимися способами совершения преступлений с использованием информационных технологий носит недостаточно систематизированный характер и требует корректировки.

В связи с этим планируется создать единый информационный ресурс-портал с ограниченным доступом, содержащий необходимую литературу, методические рекомендации по расследованию киберпреступлений, с персональной авторизацией следователей и криминалистов для использования информации о возможностях расследования.

Продолжается работа по внедрению российской криминалистической техники и программного обеспечения. Так, в настоящее время имеется положительный опыт использования специальных аппаратно-программных комплексов для анализа цифро-

вой информации, произведенных в России, эффективность которых не уступает зарубежным аналогам.

С 2020 г. прошли апробацию и рекомендованы к использованию аппаратно-программные средства, предназначенные для осмотра и исследования компьютерной информации, а также программный комплекс для габитоскопической (портретной) экспертизы.

С учетом изложенного представляются необходимыми дальнейшее формирование межведомственных механизмов по борьбе с преступлениями, совершаемыми с использованием информационных технологий, и разработка научно-практических средств и методов, в первую очередь в области криминалистики, расширяющих рекомендации, изложенные в предшествующих параграфах настоящей главы.

Список литературы

1. *Агибалов В.Ю.* Виртуальные следы в криминалистике и уголовном процессе: Монография. М., 2012.
2. *Бычков В.В., Лебедева А.А., Скобелин С.Ю.* Расследование преступлений, совершенных с использованием Интернета и мобильной телефонии: Учеб. пособие. М.: Моск. акад. СК России, 2021.
3. *Колычева А.Н., Васюков В.Ф.* Расследование преступлений с использованием компьютерной информации из сети Интернет: Учеб. пособие / Под ред. А. Г. Волеводза. М.: Проспект, 2020.
4. *Оперативно-розыскная* деятельность в цифровом мире: Сб. науч. тр. / Под ред. В.С. Овчинского. М.: Инфра-М, 2021.
5. *Оперативно-розыскная* деятельность и современность: Сб. науч. тр. / Под ред. д-ра юрид. наук В.С. Овчинского. М.: Инфра-М, 2022.
6. *Особенности* расследования преступлений, совершаемых с использованием цифровой валюты: Колл. монография / Колл. авторов; Под ред. Е.В. Емельяновой и О.С. Бутенко. СПб.: Следственный комитет Российской Федерации, 2021.

7. *Себякин А.Г.* Тактика использования знаний в области компьютерной техники. М.: Юрлитинформ, 2023. (Сер. «Библиотека криминалиста»).
8. *Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А*. Теория информационно-компьютерного обеспечения криминалистической деятельности. М.: Проспект, 2022.
9. *Теория* оперативно-розыскной деятельности: Учебник / Под ред. К.К. Горяинова, В.С. Овчинского. 5-е изд., испр. и доп. М.: Инфра-М, 2021.
10. *Цифровые* следы преступлений: Монография. М.: Проспект, 2021.
11. *Яковлев А.Н., Грачев О.В., Шухнин М.Н., Ненашев С.М., Мещеряков В.А.* Информационно-аналитические исследования больших массивов цифровой информации с помощью IBM i2 Analyst's Notebook: Учеб.-метод. пособие. М.: Перо, 2016.

ОГЛАВЛЕНИЕ

Монография

Информационные технологии в уголовно-правовой сфере

Редактор *Л.П. Кравченко*
Оригинал-макет *М.А. Бакаян*
Оформление художника *А.П. Яковлева*

Подписано в печать 07.08.2023 (с готовых ps-файлов)
Изд. № 3743 (от 30.06.2023)
Формат 60×90 1/16
Бумага офсетная
Усл. печ. л. 17,5. Уч.-изд. л. 16,0
Тираж 500 экз.
Заказ

ООО «ИЗДАТЕЛЬСТВО ЮНИТИ-ДАНА»
Генеральный директор *В.Н. Закаидзе*

123298, Москва, ул. Ирины Левченко, 1
Тел.: 8-499-740-60-14
Тел./факс: 8-499-740-60-15
E-mail: unity@unity-dana.ru
www.unity-dana.ru

Отпечатано в типографии ООО «Буки Веди»
117393, г. Москва, вн. тер. г. Муниципальный округ Обручевский,
ул. Профсоюзная, д. 56, этаж 3, помещение XIX, ком. 321.
Тел.: (495) 926-63-96, www.bukivedi.com, info@bukivedi.com