

**МВД России
Санкт-Петербургский университет**

**РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ
И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ**

Учебно-методическое пособие

**Санкт-Петербург
2025**

УДК 343.985

ББК 67.52

P24

P24 **Расследование преступлений, совершаемых с использованием, компьютерных и телекоммуникационных технологий:** учебно-методическое пособие / Подружкина Т.А., Нисневич А.К., Лаур А.В. – Санкт-Петербург: СПбУ МВД России, 2025. – 112 с.

ISBN 978-5-00277-017-5

EDN: SJRTJJ

Учебно-методическое пособие представляет собой комплексное руководство, предназначенное для углубленного изучения и практического применения в сфере правоохранительной деятельности. В его содержании детально рассматривается порядок расследования преступлений, связанных с использованием компьютерных и телекоммуникационных технологий, включая такие аспекты, как выявление, документирование и анализ цифровых следов, сбор доказательств в виртуальной среде, взаимодействие с экспертами в области информационной безопасности и применение специализированного программного обеспечения.

УДК 343.985

ББК 67.52

Рецензенты:

Нугаева Э.Д., кандидат юридических наук, доцент
(Уфимский юридический института МВД России);

Усачев С.И., кандидат юридических наук
(Восточно-Сибирский институт МВД России)

ISBN 978-5-00277-017-5

© Санкт-Петербургский университет
МВД России, 2025

Оглавление

Введение	4
Список принятых сокращений.....	9
Глава 1. Общая характеристика преступлений, совершаемых с использованием информационных технологий	10
Глава 2. Понятие и признаки преступлений, совершаемых с использованием информационных технологий	18
Глава 3. Классификация киберпреступлений по российскому уголовному законодательству	35
Глава 4. Механизм совершения преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий	49
Глава 5. Особенности расследования преступлений в сфере компьютерной информации.....	71
Заключение.....	106
Список использованных источников	108

ВВЕДЕНИЕ

Двадцать первый век ознаменован тем, что мировое сообщество вступило в эру современных телекоммуникационных технологий, использование и совершенствование которых требует постоянной корректировки действующего законодательства. Эта эпоха характеризуется не только бурным развитием интернета, мобильной связи и высокоскоростных сетей, но и интеграцией информационных технологий (ИТ) во все сферы жизни общества. Глобализация информационного пространства, где границы между странами стираются благодаря цифровым платформам, создает новые возможности для сотрудничества, но одновременно порождает серьезные угрозы. Современные технологии, такие как искусственный интеллект (ИИ), блокчейн, интернет вещей (IoT), облачные вычисления и квантовые компьютеры, революционизируют экономику, здравоохранение, образование и транспорт. Однако их внедрение сопряжено с рисками, включая кибератаки, утечки конфиденциальных данных, манипуляции информацией и даже угрозы национальной безопасности. В условиях такого прогресса государства вынуждены адаптировать законодательство, чтобы балансировать между стимулированием инноваций и обеспечением защиты. Это включает разработку международных стандартов, таких как рекомендации ООН и ЕС по кибербезопасности, а также национальные стратегии, направленные на минимизацию рисков.

В Российской Федерации эта тенденция нашла свое отражение в новой редакции ст. 71 Конституции России, согласно п. «м» которой «применение информационных технологий» и «оборот цифровых данных» находятся в ведении государства. Эта поправка, принятая в ходе общероссийского голосования в 2020 году, подчеркивает стратегическую роль ИТ в обеспечении суверенитета, экономического роста и защиты прав граждан. Она возлагает на государство ответственность за регулирование цифровой сферы, включая меры по борьбе с киберугрозами, защиту персональных данных и развитие инфраструктуры. Данная норма является частью более широких конституционных изменений, направленных на укрепление вертикали власти в условиях цифровой трансформации, и отражает осознание того, что без государственного контроля над ИТ Россия рискует отстать в глобальной гонке технологий.

Внесенная поправка свидетельствует о необходимости дальнейшего совершенствования не только действующего уголовного и уго-

ловно-процессуального законодательства, но и других федеральных законов и подзаконных нормативных правовых актов, регламентирующих информационные технологии и оборот цифровых данных в России. Например, федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹ требует регулярных обновлений для учета новых угроз, таких как глубокое фейковое обучение и автоматизированные атаки на основе ИИ. Аналогично УПК РФ нуждается в адаптации к специфике цифровых доказательств: электронные следы, метаданные, облачные хранилища и блокчейн-транзакции часто требуют специальных методов сбора и верификации. Это обусловлено тем, что традиционные криминалистические подходы, разработанные для физических улик, неэффективны в виртуальной среде, где преступления могут быть совершены анонимно, через прокси-серверы или с использованием VPN. Кроме того, трансграничный характер киберпреступлений усложняет юрисдикцию, требуя международного сотрудничества. В связи с этим целесообразен анализ криминалистических аспектов расследования в целях разработки методических рекомендаций для правоохранительных органов, включая алгоритмы осмотра цифровых носителей, использование forensic-инструментов, таких как EnCase или Autopsy, и взаимодействие с экспертами в области кибербезопасности. Также рассматриваются вопросы подготовки кадров: необходимость обучения следователей навыкам работы с большими данными, машинным обучением для анализа паттернов преступлений и этическими аспектами использования ИИ в расследовании. Это пособие предназначено для студентов юридических факультетов, практикующих юристов и экспертов, способствуя повышению эффективности борьбы с киберпреступностью в условиях постоянной эволюции технологий.

Данные официальной статистики показывают неуклонный рост числа преступлений, совершаемых с использованием ИТ. Следует отметить, что пандемия COVID-19 ускорила цифровизацию, увеличив число онлайн-транзакций, удаленной работы и цифрового общения, что создало благоприятную среду для злоумышленников. Аналогичные тенденции наблюдаются глобально: отчеты Europol за 2020

¹ Здесь и далее – все нормативные правовые акты приводятся в соответствии с данными официального интернет-портала правовой информации pravo.gov.ru (дата обращения: 15.05.2023).

год фиксируют рост киберпреступлений на 35%, с общими потерями более 1 триллиона долларов США ежегодно. В России ущерб оценивается в сотни миллиардов рублей, включая инциденты, такие как атаки на банки (например, хакерская группа REvil в 2021 году) и государственные учреждения. Статистика показывает, что большинство киберпреступлений остаются латентными: по оценкам экспертов, регистрируется лишь 10–20% случаев, что искажает картину и затрудняет профилактику. Факторы роста включают увеличение числа интернет-пользователей — в России их более 100 миллионов, — распространение смартфонов и IoT-устройств, которые становятся точками входа для атак. Кроме того, эволюция преступных схем: от простых фишинговых писем до сложных ransomware-атак с использованием шифрования данных. В международном сравнении Россия занимает лидирующие позиции по числу DDoS-атак, что подчеркивает необходимость усиления мер защиты критической инфраструктуры.

При этом перечень преступлений, совершаемых с использованием ИТ, по УК РФ, за период с 2016 года значительно расширился. Если ранее акцент делался на статьях вроде ст. 272 (неправомерный доступ к компьютерной информации) и ст. 273 (создание и распространение вредоносного ПО), то теперь включены нормы о мошенничестве в сфере компьютерной информации (ст. 159.6), введенной в 2012 году и усиленной в 2020 году, а также о кибертерроризме и экстремизме в сети (ст. 280). Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» от 07.12.2011 № 420-ФЗ повысил максимальные сроки наказания за ИТ-преступления, а поправки 2020 года добавили квалифицирующие признаки, такие как использование нейросетей или криптовалют (например, в ст. 159.6 УК РФ). Это отражает эволюцию угроз: от индивидуального взлома до организованных кампаний, включающих социальную инженерию, deepfakes и атаки на блокчейн. В международном контексте Россия ратифицировала Будапештскую конвенцию Совета Европы о киберпреступности в 2001 году, что требует гармонизации с глобальными стандартами, такими как директивы ЕС по GDPR и NIS Directive. Расширение УК РФ также включает новые составы, связанные с цифровой экономикой, такие как ст. 274.1 (нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации), введенная в 2017 году. Эти изменения подчеркивают необходимость в специализированных методиках расследо-

вания, учитывающих волатильность цифровых улик и необходимость быстрого реагирования.

Использование информационных технологий возможно при совершении многих преступлений, посягающих на отношения собственности, безопасность личности, общества и государства, что в соответствии с УК РФ выступает либо конструктивным, либо квалифицирующим признаком (в частности, «использование электронных или информационно-телекоммуникационных сетей») состава преступления. Например, мошенничество (ст. 159) часто квалифицируется по признаку использования интернета или мобильных приложений, что повышает наказание до 10 лет лишения свободы. Аналогично, преступления против личности включают распространение порнографии (ст. 242) через даркнет или социальные сети, клевету (ст. 128.1) в онлайн-форумах и даже сексуальную эксплуатацию несовершеннолетних (ст. 242.1) с использованием видеоконференций. На уровне общества и государства ИТ используются в экстремизме (ст. 280), где пропаганда осуществляется через Telegram-каналы или VPN, и шпионаже (ст. 276), включая кражу данных с государственных серверов. Дополнительно, новые угрозы включают кибершантаж (sextortion), где злоумышленники используют deepfakes для манипуляции, и атаки на инфраструктуру, такие как хакинг энергосистем, квалифицируемые по ст. 215.2. Это многоаспектность требует междисциплинарного подхода: сочетания криминалистики с информатикой, психологией (для анализа мотивов) и международным правом.

Настоящее пособие предлагает систематизированные методики, включая алгоритмы осмотра места происшествия в цифровой среде (например, изъятие устройств с соблюдением цепочки хранения), экспертизу электронных носителей с использованием hashing и цифровой подписи, тактики допросов свидетелей в онлайн-пространстве и координацию с международными организациями, такими как Интерпол.

Таким образом, актуальность работы определяется не только ростом преступности, но и необходимостью защиты фундаментальных прав человека в цифровую эпоху, где виртуальные действия имеют реальные последствия, а границы между мирами стираются. Пособие способствует формированию компетентной системы расследования, способной адаптироваться к будущим вызовам, таким как квантовые угрозы и автономные системы. Кроме того, представленный материал охватывает ключевые этапы следственных действий, от первоначаль-

ной проверки информации до завершения уголовного дела, с учетом особенностей киберпреступлений, таких как хакинг, распространение вредоносного ПО, мошенничество в сети и нарушения конфиденциальности данных. Особое внимание уделяется правовым основам, тактическим приемам и методам преодоления технических барьеров в расследовании, а также интеграции современных технологий, таких как искусственный интеллект и блокчейн, в процесс правоохранительной работы органов внутренних дел Российской Федерации.

Издание предназначено для широкого круга специалистов системы МВД России, включая курсантов, слушателей, адъюнктов и научно-педагогический состав образовательных организаций высшего образования. Оно служит основой для формирования профессиональных компетенций в области кибербезопасности, способствует повышению квалификации преподавателей и исследователей, а также обеспечивает подготовку будущих сотрудников к реальным вызовам цифровой эпохи. Материалы пособия структурированы таким образом, чтобы быть полезными как для теоретического обучения, так и для практических занятий, включая кейс-стади, упражнения и рекомендации по проведению симуляций расследований.

Кроме того, анализ и рекомендации, представленные в пособии, могут быть успешно использованы при осуществлении организационно-управленческой деятельности сотрудниками территориальных органов внутренних дел. Они помогают в оптимизации процессов планирования операций по борьбе с киберпреступностью, координации межведомственного взаимодействия, разработке стратегий профилактики и реагирования на инциденты, а также в оценке эффективности работы подразделений. А это способствует повышению эффективности правоохранительной системы в условиях растущей угрозы кибератак, обеспечивая сотрудников необходимыми инструментами для адаптации к быстро меняющимся технологиям и законодательству в сфере информационной безопасности. В целом, оно является важным ресурсом для укрепления профессионализма и оперативности в борьбе с современными формами преступности.

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

ВТСС – вспомогательные технические средства и системы

ИТ – информационные технологии

ИС – информационная система

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

КИ – компьютерная информация

КТТ – компьютерные телекоммуникационные технологии

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОИ – объект информатизации

ОТСС – основные технические средства и системы

СВТ – средства вычислительной техники

СЗИ – система защиты информации

СЗИ НСД – система защиты информации от несанкционированного доступа

ТСОИ – технические средства обработки информации

ТКМТ – телекоммуникационные технологии

Глава 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Масштаб совершаемых противоправных действий с использованием «цифрового пространства» стирает привычное понимание применения норм уголовного законодательства, бросая все новые вызовы как теории, так и практике. В эпоху глобализации и цифровой трансформации общества, когда информационные технологии проникают во все сферы жизни — от финансовых операций до личных коммуникаций, — преступления, использующие эти технологии, приобретают беспрецедентный размах. Это не просто локальные инциденты, а глобальные угрозы, способные дестабилизировать экономики целых стран, нарушить национальную безопасность и подрвать доверие к цифровым системам. Например, кибератаки на Colonial Pipeline в США в 2021 году демонстрируют, как виртуальные действия могут иметь катастрофические реальные последствия. Ситуация усложняется, когда совершение преступления связано с использованием «цифрового пространства», охватывающего доступ множества государств и неограниченного круга лиц. В этом случае место совершения деяния и место наступления преступного результата могут не только не совпадать, но и находиться друг от друга на больших расстояниях, минуя все государственные границы. Это создает проблемы с юрисдикцией, экстрадицией и координацией расследований, требуя новых подходов к международному сотрудничеству.

Интерес представляет вопрос о возможности применения имеющихся в уголовном праве принципов действия уголовного закона в пространстве относительно цифровой среды. Необходимым представляется обоснование с позиции действующего законодательства и юридической науки определения «цифрового пространства» как места совершения преступления. Это возможно установить путем обращения к общему понятию «место совершения преступления» и дальнейшего разбора особенностей применения выработанных наукой положений относительно «цифрового пространства». Такой анализ должен учитывать эволюцию технологий: от простого доступа к интернету до использования облачных сервисов, блокчейна и ИИ, которые усложняют идентификацию и фиксацию преступных действий. Более того, цифровые преступления часто носят латентный ха-

ракт, что затрудняет их обнаружение и статистический учет, как отмечается в отчетах Interpol и Europol.

Понятие «цифровое пространство» не содержится в нормативных актах. Определить его возможно через анализ совокупности нормативных документов и имеющихся в науке таких определений, как «информационное пространство», «киберпространство», «интернет», «виртуальное пространство». В юридической литературе отмечается, что информационное пространство имеет ряд особенностей: трансграничность, отсутствие государственно-властного элемента. Трансграничность означает, что информация свободно пересекает границы, игнорируя территориальные ограничения, что делает традиционные модели юрисдикции устаревшими. Отсутствие государственно-властного элемента подразумевает, что в цифровом пространстве нет единого суверена, контролирующего все аспекты, что приводит к анархии и необходимости новых форм регулирования. Понятие «цифровое пространство» идентично пониманию информационного пространства. «Стратегия развития информационного общества Российской Федерации на 2017–2030 годы» определяет данную категорию как совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры. Это определение подчеркивает динамический характер пространства, включающий не только статичные ресурсы, но и процессы взаимодействия, что важно для понимания преступлений, где ключевыми являются коммуникации и обмен данными. При этом Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 05.12.2016 № 646, определяет информационную инфраструктуру Российской Федерации как совокупность объектов информатизации, информационных систем, сайтов в сети Интернет и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации. Следует отметить, что данное определение включает в себя не только все виды информации (сайты), содержащиеся в глобальной сети Интернет, но и информационных систем и сетей связи. Это расширяет понимание до включения мобильных сетей, спутниковой связи и даже IoT-устройств, которые становятся объектами преступлений, таких как DDoS-атаки или кража данных с умных домов.

Такой же вывод можно сделать, обращаясь к иным источникам. Так, в Проекте концепции Стратегии кибербезопасности Российской Федерации информационное пространство определяется как сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию, а также дается определение собственно киберпространству как сфере деятельности в информационном пространстве, образованной совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства). Указанные понятия позволяют связать совокупность двух явлений: действия лица в киберпространстве и его реальную территориальную привязку. Это важно для криминалистики, где необходимо сопоставлять виртуальные следы с физическими локациями, такими как IP-адреса, геолокация устройств или логи серверов. Также было упоминание о таком понятии, как «виртуальное пространство».

В юридической литературе встречается следующее определение: виртуальное пространство — это область технических, технологических и социальных отношений, возникающих, изменяющихся и прекращающихся в процессе использования компьютерной или иной электронной технической сети по поводу информации, информационных ресурсов, информационных услуг и средств связи. Данный термин позволяет в большей степени говорить о деятельности реальных лиц при воздействии и взаимодействии с различными объектами информационной инфраструктуры. Например, социальные сети как часть виртуального пространства формируют отношения, которые могут быть использованы для мошенничества или распространения экстремизма. Исходя из представленных понятий, следует сделать вывод о том, что определять только глобальную сеть Интернет как место совершения противоправных действий — значит, значительно сужать круг данных общественных отношений. Нормативного определения понятия «интернет» в российском законодательстве не существует, однако многие нормативно-правовые акты используют данное понятие, в т. ч. и уголовный закон. При этом законодательно определены следующие понятия: информация, информационные техноло-

гии, информационные системы, доступ, предоставление, распределение информации, сайт в сети Интернет, страница в сети Интернет и т. д. Анализ норм действующего законодательства позволяет отметить характеристики сети Интернет:

1. Это разновидность информационно-телекоммуникационной сети.

2. Это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Особенно следует отметить, что в связи с этим интернет является, в том числе, и средством международной коммуникации, что соответственно затрудняет применение имеющихся в законодательстве стандартных способов защиты от противоправных действий. Например, VPN и Tor-сети позволяют анонимизировать трафик, делая традиционные методы слежки неэффективными. Обобщая вышесказанное, предлагаем в настоящем исследовании широко понимать термин «цифровое пространство», определяя его как совокупность информационных ресурсов, созданных субъектами информационной сферы, средств взаимодействия таких субъектов, их информационных систем и сайтов в сети Интернет и сетей связи. Это определение охватывает все аспекты, включая мобильные приложения, облачные хранилища и даже будущие технологии, такие как метавселенные.

Рассматривая «цифровое пространство» как место совершения преступления, необходимо определить само понятие «место совершения преступления». В юридической литературе по сей день ведутся дискуссии касательно указанного понятия. Многообразие дефиниций обусловлено отсутствием нормативного закрепления в отечественном законодательстве, а также попытками доктринально его определить. Актуальность наличия оптимального, всецелого и емкого понятия «место совершения преступления» обосновывается также тем, что это важно при поиске ответа на многие материально-правовые и процессуальные вопросы. В частности, это имеет значение для уголовного права применительно к учению о действии уголовного закона в пространстве, определяя юрисдикцию государства, а также для определения признаков состава преступления, где «место» может выступать квалифицирующим признаком объективной стороны. При этом доктрина будто ведет речь о понятиях полярных, никак не соприкасающихся, без сосредоточения внимания относительно пространственных пределов действия уголовного закона. Рассмотр-

ние понятия «место совершения преступления» относительно цифровой среды необходимо и с позиции пространственных пределов и при определении данного факультативного признака одного из элементов состава преступления.

Помимо этого немаловажно понимание определения места совершения преступления в случаях с длящимся или продолжаемым деянием. Например, DDoS-атака может длиться часы или дни, требуя учета всей цепочки событий. Начнём с вопроса пространственного действия уголовного закона. В этой связи возникают, как минимум, несколько предположений:

1. Место совершения преступления — это место совершения действия (бездействия), содержащего все признаки состава преступления.

2. Место совершения преступления — это место наступления общественно опасных последствий.

3. Место совершения преступления — место нахождения лица, совершившего преступление.

В уголовно-правовой науке имеется мнение о том, что следует признавать местом совершения преступления ту территорию, где было реализовано деяние и наступило общественно опасное последствие, образующее объективную сторону преступления. Представляется, что данная позиция чрезмерно ограничена и не может отвечать современным вызовам, особенно в преступлениях, совершенных в цифровом пространстве. Вместе с тем в доктрине уголовного права разработана концепция, рекомендующая обращаться к имеющемуся в уголовном законе понятию «время совершения преступления» для понимания места совершения преступления. В соответствии с ч. 2 ст. 9 УК РФ: «Временем совершения преступления признается время совершения общественно опасного действия (бездействия) независимо от времени наступления общественно опасных последствий». Данная законодательная регламентация приводит к выводу о том, что раз время совершения преступления определяет только момент совершения общественно опасного деяния без последствий, то точно такое же заключение можно сделать и относительно места. Следовательно, место совершения преступления необходимо определить как территорию (например, России), даже если преступный результат наступил за пределами данной территории. Исходя из указанной позиции, категории «время» и «место» неразрывно связаны, а значит, должны определяться на основе одних и тех же обстоятельств.

Также сторонниками данной концепции обосновывается, что территория Российской Федерации не будет местом совершения преступления в том случае, если преступная деятельность была совершена на территории иностранного государства, а последствия должны были наступить в России. В юридической литературе встречается мнение о том, что место совершения преступления с формальным составом необходимо определять по месту совершения деяния, а преступления с материальным составом — по месту наступления общественно опасных последствий. Можно предположить, что в основу такого вывода положено понятие оконченного преступления, так как в деянии лица содержатся все признаки состава преступления.

Встречается также мнение о том, что преступление с формальным составом следует считать совершенным на территории государства, если деяние совершено в пределах его территориальных границ. В случае же с преступлениями с материальным составом необходимо решать вопрос в пользу государства как при совершении деяния на его территории, так и при наступлении последствий, вне зависимости от того, где было реализовано преступное деяние.

Существовала вместе с тем и точка зрения, в соответствии с которой местом совершения преступления в любом случае признается Российская Федерация, если преступная деятельность была хоть как-то связана с интересами государства. В литературе это встречается как теория повсеместности. Следует отметить, что практика предлагает отсылку ко всем известному сложившемуся принципу *forum delicti commissi* (лат. – совершение преступления, либо по месту совершения преступления), обосновывающему определение территориальной подсудности, исходя из места совершения преступления. Как следствие, нет четкого ответа на вопрос относительно преступлений, совершенных в цифровом пространстве — территорию какого государства следует признавать местом совершения преступления:

- места расположения сервера;
- места нахождения лица, реализующего преступление;
- места наступления последствий преступления?

Привлекательность совершения преступления с использованием возможностей цифрового пространства вполне обоснованна. Такой способ позволяет воздействовать на широкую аудиторию из любой точки мира, сохраняя анонимность. Также это объяснимо сложностью фиксации следов преступной деятельности и поиска лица, совершившего преступление. В то же время противодействие цифровой

преступности должно осуществляться именно посредством межгосударственного взаимодействия, совместно с приведением в соответствие норм внутригосударственного уголовного законодательства.

В научной литературе высказывается мнение не просто об унификации законодательства, а о формировании качественно новой отрасли — право киберпространства. Вместе с тем предполагается, что местом совершения преступления необходимо считать не какую-либо государственную территорию, а собственно «цифровое пространство». На данной «территории» должны действовать свое законодательство, а также специфичные судебные органы. Некоторые государства достаточно продвинулись в данном вопросе. Так, например, в Китае функционирует специализированный онлайн-суд, под юрисдикционными полномочиями которого находятся только преступления, совершенные в сети Интернет. Для признания цифрового пространства самостоятельной территорией необходимо, чтобы подобные суды были созданы если не всеми, то большинством государств, при этом обязательны действенные единые международно-правовые средства, но на современном этапе такое представляется невозможным. Поэтому требуется устанавливать реальное материальное место совершения преступления, реализованного в цифровой среде.

По данному вопросу существуют различные точки зрения. Так, А. Ю. Рыков предлагает исходить из адреса интернет-сайта (доменное имя, на котором он размещен), поскольку именно эта принадлежность доменного имени к конкретному государству и определяет применяемое законодательство. Однако данная позиция не учитывает, что адрес сайта не выступает признаком территориальной принадлежности к государству. В этом случае вряд ли возможно говорить о том, что местом совершения преступлений следует считать место нахождения оборудования, выступающего средством совершения преступления. Такая позиция не может быть поддержана ввиду того, что оборудование может быть размещено в разных странах.

Рассматривая вопрос о возможности признания местом совершения преступлений в цифровом пространстве место наступления общественно опасных последствий, стоит обратиться к следующему примеру. В. Левин с помощью компьютера, находящегося в офисе фирмы в Санкт-Петербурге, вводил ложные данные в систему банка «Ситибанк», расположенного в США, в результате чего со счетов вкладчиков было похищено более 10 000 000 долларов. В. Левин скрывался от следствия, но был задержан и осужден в Лондоне. При

этом Великобритания отказала в выдаче преступника и США, и России, мотивируя это тем, что законодательство страны не регламентирует ситуацию, когда преступление совершено на территории одного государства, а последствия совершения преступления наступили на территории другого. Однако если последствия совершенного противоправного деяния имели свое распространение в нескольких государствах, это может порождать целый ряд проблем, связанных в первую очередь с выбором юрисдикции государства.

Обращаясь к судебной практике, нельзя не отметить положений постановления Пленума Верховного суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». В случае если предметом преступления при мошенничестве являются безналичные денежные средства, то по смыслу положений п. 1 примечаний к ст. 158 УК РФ и ст. 128 ГК РФ содеянное должно рассматриваться как хищение чужого имущества. Такое преступление следует считать оконченным с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Исходя из данного положения можно сделать вывод о том, что в случае с использованием, например, сети Интернет, местом совершения преступления необходимо признавать место совершения общественно опасного деяния. Отсюда следует, что, если преступное деяние было совершено в России, а преступное последствие наступило на территории другого государства, деяние подлежит юрисдикции России. Поэтому не имеет значения конструкция состава преступления, совершенного в цифровом пространстве, в указанном смысле местом совершения (как усеченного, так формального и материального) следует считать территорию того государства, где было совершено общественно опасное деяние. В связи с тем, что практика стремится к единообразию применения и толкования норм права, а также неоспоримости факта единой природы уголовного права и административного права как публичных сфер.

Глава 2. ПОНЯТИЕ И ПРИЗНАКИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Определяя место совершения преступления, необходимо также определить понятие и признаки деяний, совершаемых с использованием ИТ. Информационные технологии проникают во все сферы жизни, играют весомую роль в вопросах оснащённости преступности и их использовании лицами при совершении преступления. Применение технических средств позволяет лицам эффективно координировать свои действия, включать такие способы, которые ранее не были известны уголовному праву. В литературе отмечается, что в преступных группах, создаваемых посредством сети Интернет, участники могут не иметь информации о других членах группы и никогда не встречаться с ними¹.

В юридической доктрине преступления, совершаемые с использованием ИТ, понимаются по-разному, толкуются неоднозначно и воспринимаются различными дефинициями. Основной проблемой является то, что официальное закрепление получила только одна группа деяний, объединённая в гл. 28 УК РФ «Преступления в сфере компьютерной информации».

Так, в литературе встречаются понятия «преступления в сфере высоких технологий», «преступления, совершаемые при помощи телекоммуникационных сетей, включая сеть Интернет, информационно-телекоммуникационных сетей», «киберпреступления» (в последнее время наиболее часто встречающийся термин), «компьютерные преступления», «преступления в сфере компьютерной информации» и т. д. Стоит отметить, что в исследованиях указывают два вида преступлений — преступления в сфере компьютерной информации в чистом виде, а также любые преступления, в которых используются информационные технологии в качестве средства их совершения, ответственность за которые закреплена в иных статьях уголовного закона.

При этом в большей части работ смешиваются уголовно-правовые и криминологические характеристики рассматриваемых нами преступлений, отмечая:

- 1) трансграничный характер деяний;

¹ Тропина Т. Л. Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86.

2) дистанционный характер (отсутствие физического взаимодействия с жертвой, воздействие лишь посредством ИТ, в связи с чем число потерпевших может быть неограниченным и находиться в любой точке мира);

3) латентный характер (ввиду сложности инфраструктуры, анонимности, особых познаний в области ИТ лиц, совершающих преступные посягательства);

4) постоянное совершенствование способов совершения преступления по причине быстрого развития ИТ;

5) отсутствие должной осведомленности о посягательствах у потерпевших¹.

Учёные-юристы долгое время пытаются выработать и закрепить единую терминологию понимания данных видов преступлений. Сложность выработки дефиниций кроется в отсутствии однообразного подхода относительно круга деяний, которые следует относить к преступлениям, совершаемым с использованием ИТ.

Исторически первым употребляемым термином, обозначающим рассматриваемый вид преступлений, указывают «Cybercrime» (киберпреступление)². Данное определение отражено в рекомендациях экспертов ООН, где термин «киберпреступность» обозначает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети³.

Отечественные ученые в своих трудах описывают киберпреступления по-разному. Некоторые отождествляют понятие «компьютерные преступления» и «киберпреступления». Например, И. М. Расолов указывает, что к киберпреступлениям относятся такие общественно опасные деяния, которые совершаются с применением средств компьютерной техники (СКТ) в отношении информации, об-

¹ См.: Сериева М. М. Киберпреступность как новая криминальная угроза // Новый юридический вестник. 2017. № 1. С. 104–106.

² См.: Дубко М. А. О понятии компьютерного преступления [Электронный ресурс] // Центр исследования компьютерной преступности. URL: <http://www.crime-research.ru/analytics/computercrime06> (дата обращения: 15.05.2023); Чекунов И. Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. №2. С. 37.

³ Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями. Вена, 10–17.04.2000.

рабатываемой и используемой в Интернете¹. Причиной этого является буквальный перевод, уяснение и разъяснение термина.

Следует отметить, что понятие «компьютерные преступления» характерно для ранних научных работ. Так, термин «компьютерные преступления» использовался при описании деяний с использованием информационно-вычислительных систем, либо с воздействием на них»².

Все чаще исследователи дают более широкое понимание термина. Так, Д. Н. Карпова указывает, что киберпреступление является актом социальной девиации с целью нанесения ущерба посредством любого технического средства с доступом в Интернет³.

По мнению И. Г. Чекунова, киберпреступность также следует рассматривать шире компьютерной преступности постольку, поскольку для совершения киберпреступлений используются не только компьютеры, но и мобильные (сотовые) коммуникационные технические устройства и системы связи⁴.

Указанные формулировки привязаны к термину «киберпреступность», отражающему преступную деятельность в объективно присущем обществу социальном виде, где единичное (преступление) является частью множества преступных явлений в определенной сфере.

В работах подчеркивается, что понятие «киберпреступление» не ограничивается рамками сети «Интернет», поскольку оно распространяется на все виды преступлений, совершенных в информационно-телекоммуникационной сфере⁵.

Некоторые исследователи, напротив, сужают определение киберпреступлений. Так, Д. Л. Шиндер указывает, что киберпреступность может определяться как подкатегория компьютерной преступ-

¹ Рассолов И. М. Право и Интернет. Теоретические проблемы. – М., 2009. С. 132–133; Чекунов И. Г. К вопросу о понятии и системе преступлений, совершаемых с использованием компьютерных сетей // Правовые вопросы связи. 2012. № 1. С. 18.

² Ахраменка Н. Ф. Проблемы криминализации общественно опасного поведения с использованием информационно-вычислительных систем: автореф. дис. ... канд. юрид. наук. – Минск, 1996. С. 7.

³ См.: Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

⁴ Чекунов И. Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53.

⁵ Соловьёв И. Н. Правовое обеспечение борьбы с преступлениями в сфере информационных технологий // Административное и муниципальное право. 2009. № 3. С. 63–65.

ности¹. Подобная точка зрения основывается на том, что относит к киберпреступлениям лишь преступления, совершенные в сети «Интернет». Анализ юридической литературы показывает, что такая позиция поддерживается наименьшим количеством исследователей. Вместе с тем в научных трудах используется понятие «информационные преступления».

Под информационными преступлениями понимаются общественно опасные деяния, запрещенные уголовным законом под угрозой наказания, совершенные в области широкого круга отношений:

1. Возникающих при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю информации.

2. Создающих и использующих информационные технологии и средства их обеспечения.

3. Защищающих информацию, права субъектов, участвующих в информационных процессах и информатизации².

Существует еще более широкое определение: информационными преступлениями признаются такие, состав которых включает в себя информацию³. Такая формулировка представляется не совсем удачной. Во-первых, круг общественных отношений в названном случае может быть неоправданно широк; во-вторых, нет четкого указания, к какому признаку состава преступления должна быть отнесена информация: является ли она средством или предметом, или же имеется в виду определенная информационная среда, в которой лицо реализует свою преступную деятельность.

В литературе также упоминается понятие «преступления, совершаемые с использованием высоких технологий». Данное понятие, как отмечают ученые, носит собирательный характер, употребляется в случаях, когда для совершения традиционных в уголовном праве преступлений применяются информационные технологии,

¹ Шиндер Д. Л. Киберпреступность: перед лицом проблемы // Центр исследования компьютерной преступности. URL: <http://www.crime-research.ru/library/cybercrimes3.html> (дата обращения: 15.05.2023).

² Крылов В. В. Основы криминологической теории расследования преступлений в сфере информации. – М., 1998. 50 с.

³ См.: Турышев А. А. Информация как признак составов преступлений в сфере экономической деятельности: автореф. дис. ... канд. юрид. наук. – Омск, 2006. С. 9.

ответственность за которые предусмотрена статьями различных глав УК РФ¹.

При этом подчеркивается, что преступления, ответственность за которые предусмотрена гл. 28 УК РФ, и преступления, совершаемые с использованием высоких технологий, не тождественны. Последние относятся к новым видам и способам совершения преступлений, возникшим в результате распространения сети «Интернет» и информационно-телекоммуникационных сетей².

Мнение ряда ученых фактически уравнивает высокие технологии и информационные технологии, в то же время отделяя информационные технологии от сферы компьютерной информации. Представляется, что это не совсем корректно. В первую очередь необходимо ответить на вопрос, что понимать под ИТ. Так, федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержит следующее определение: информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Термин «информационные технологии» был использован впервые в работах В. М. Глушкова. В его трудах ИТ рассматриваются как определенный способ работы с информацией, в частности:

1. Способ и средство сбора информации.

2. Обработка информации.

3. Передача информации для получения новой информации об исследуемом объекте (персональный компьютер (ПК), телекоммуникационные и мультимедийные средства — радиосвязь, мобильные телефоны, планшеты, ноутбуки)³.

При этом в примечании к ст. 272 УК РФ содержится понятие «компьютерной информации». Под ней понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, незави-

¹ Шевко Н. Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юрид. ин-та МВД России. 2016. Т. 1, № 1 (1). С. 13–16.

² См., например: Чирков Д. К., Саркисян А. Д. Преступность в сфере высоких технологий: тенденции и перспективы // Национальная безопасность. 2013. № 1 (24). С. 25–32.

³ Автоматизация производственных процессов с применением средств вычислительной техники: Материалы научно-технического совещания / под ред. И. Е. Панюшкина [и др.]. — М., 1962. С. 48.

симо от средств их хранения, обработки и передачи. Поэтому считаем, что компьютерная информация является составной частью ИТ, разделение информационных технологий и компьютерной информации ограничивает и делает невозможным понимание их содержания.

Анализ понятийного значения терминов «преступления в сфере компьютерной информации» и «преступления, совершаемые с использованием информационных технологий», позволяет утверждать, что первая указанная группа — это категория, отраженная в уголовном законе.

В российском законодательстве содержится достаточный понятийный аппарат, позволяющий охарактеризовать деяние как подпадающее или не подпадающее под признаки преступлений в сфере компьютерной информации. Разграничение происходит на основе анализа норм отечественной правовой системы, позволяющих отграничивать преступления в сфере компьютерной информации от иных деяний.

Решение вопроса о том, стоит ли относить преступление к категории, совершаемых в сфере компьютерной информации, невозможно без анализа объекта преступного посягательства. Важность определения данного признака кроется в сущности преступления в целом.

Оценка общественной опасности преступного деяния, определение тяжести вреда зависят, прежде всего, от того, что является объектом преступления, насколько ценное и важное благо нарушается таким деянием¹.

В характеристике объекта конкретного преступного деяния определяют вертикальное и горизонтальное деление. «По вертикали»: общий, родовой, видовой и непосредственный объекты. Разделение «по горизонтали» предполагает определение основного и дополнительного непосредственных объектов преступления².

Непосредственным объектом преступления является определенное благо (интерес), повреждение которого составляет социальную сущность данного преступления и в целях охраны которого издана уголовно-правовая норма или группа уголовно-правовых норм, предусматривающих ответственность за его совершение³.

¹ См.: Загородников Н. И. Преступления против жизни по советскому уголовному праву. — М., 1961. С. 26.

² См.: Уголовное право Российской Федерации. Общая и особенная части: учебник / под ред. А. И. Чучаева. — М., 2013. С. 105–106.

³ См.: Коржанский Н. И. Объект и предмет уголовно-правовой охраны. — М., 1980. С. 81.

В юридической литературе непосредственным объектом преступлений, указанных в гл. 28 УК РФ, признают общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз. При этом предметом преступлений в сфере компьютерной информации следует признавать следующее¹:

- информацию;
- объекты информатизации;
- информационные системы;
- сайты;
- сети связи;
- информационные технологии;
- деятельность субъектов, связанную с формированием и обработкой информации.

Предполагается, что к рассматриваемым нами преступлениям стоит относить как те составы преступлений, в которых общественные отношения в информационной сфере выступают в качестве основного объекта охраны, так и те, в которых указанный круг общественных отношений представляет собой дополнительный (факультативный) объект. Пример такого состава являет мошенничество, предусмотренное в ст. 159.6 УК РФ.

Вместе с тем при отсутствии указанного дополнительного или факультативного объекта преступного посягательства к анализируемым составам следует относить те преступления, в которых использование ИТ является способом совершения преступления, поскольку само по себе деяние значительно шире, чем просто способ совершения преступления.

Анализ объективной стороны преступлений рассматриваемой нами группы общественных отношений позволяет выделить некоторые общие характерные признаки. Логическое толкование норм, содержащихся в гл. 28 УК РФ, дает возможность говорить о том, что деяния выполняются путем активных действий. Об этом свидетельствуют такие формулировки, как «создание», «распространение», «использование», указывающие на альтернативный характер деяния. Представляется, что «нарушение правил эксплуатации средств хра-

¹ См.: Попов А. Н. Преступления в сфере компьютерной информации: учеб. пособие. СПб.: Санкт-Петербургский юрид. ин-т (филиал) Университета прокуратуры РФ, 2018. С. 22–23.

нения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям» может быть совершено также путем бездействия. При этом составы, сформулированные в ст. 272, 274 УК РФ, являются материальными, с указанием наступления таких последствий: «уничтожение, блокирование, модификация либо копирование компьютерной информации».

Указанные последствия альтернативны. Для наличия состава преступления достаточно хотя бы одного из названных последствий. Соответственно, в данном случае необходимо установление причинной связи между деянием и наступившими общественно опасными последствиями. Абстрактный способ изложения объективной стороны состава преступления, а также альтернативная диспозиция видятся обоснованным шагом законодателя, ввиду многоаспектности рассматриваемых нами деяний.

Общепринято, что способ является факультативным признаком объективной стороны. В этой связи преступления, объединенные гл. 28 УК РФ, содержат все необходимые признаки в основной характеристике деяния, как обязательного признака объективной стороны. Способ совершения преступления «только тогда способ, когда он сливается с деянием (действием или бездействием)»¹. Связь способа совершения преступления с основным деянием отражается в уголовном законе с помощью слов «посредством», «путем», «с использованием», «с применением» и т. п. При описании способа совершения преступления с использованием информационных технологий, применяются формулировки:

- с использованием средств массовой информации (СМИ) либо информационно-телекоммуникационных сетей, в т. ч. сети «Интернет»;
- в публичном выступлении, публично демонстрирующемся произведении, СМИ или информационно-телекоммуникационных сетях (включая сеть «Интернет»);
- распространение через СМИ, в т. ч. электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»).

¹ Кудрявцев В. Н. Способ совершения преступления и его уголовно-правовое значение // Советское государство и право. 1957. № 8. С. 67–68.

Представляется, что деяние может совершаться определенным способом, однако при этом способ не всегда является признаком объективной стороны состава преступления и может полностью не отражаться в законодательной конструкции состава. Как способ не охватывает собой преступного поведения индивида в целом, так и основное деяние не включает в себя целиком способ совершения преступления. И способ, и основное деяние как части входят в целое — в преступное поведение¹.

В связи с этим следует согласиться с определением, данным Г. Г. Зуйковым, предлагающим понимать под способом систему объективно и субъективно детерминированных, причинно и функционально связанных действий преступника по подготовке, совершению и сокрытию преступления, сопряженных с использованием условий места и времени, орудий и средств, соответствующих объему преступного замысла и достижению цели².

Неразрывность использования при таком способе совершения преступления орудий и средств совершения преступления очевидна. По мнению С. А. Яшкова, средство совершения преступлений выступает не только в форме вещей материального мира, но еще и в форме приемов, методов и способов совершения преступного посягательства. Орудием преступления при этом выступают непосредственно предметы материального мира³.

В связи с этим способ в преступлениях рассматриваемого вида может быть отражен в диспозиции статьи и являться обязательным признаком (влияет на наличие или отсутствие состава), может являться квалифицирующим признаком, а также может и должен быть учтен при индивидуализации наказания.

Таким образом, информационные программы, методики (информация, коды), при помощи которых было совершено преступление, оказываются средствами совершения преступления, а оборудование и устройства (материальные объекты) необходимо считать

¹ Кругликов Л. Л. Использование способа совершения преступления в качестве дифференцирующего средства в нормах главы 21 УК РФ // Вестник института: преступление, наказание, исправление. 2008. № 4. С. 17.

² Зуйков Г. Г. О способе совершения и способе сокрытия преступления // Оптимизация расследования преступлений. — Иркутск, 1982. С. 56–64.

³ Яшков С. А. Информация как предмет преступления: автореф. дис. ...канд. юрид. наук. — Екатеринбург, 2005. С. 19–22.

орудиями. Все это, в совокупности, выражается через способ совершения преступления.

Помимо этого ИТ могут использоваться не только для облегчения совершения преступления, но и для сокрытия совершенного преступления. В юридической литературе указывается несколько способов сокрытия следов. Не раскрывая их сущность, следует отметить, что принято считать в качестве таковых. Речь идет о создании с использованием информационных технологий вещей материального мира с измененными данными, уничтожение «виртуальных» следов деятельности лица, либо реальное уничтожение материальных объектов — носителей информации.

Характеристика субъективных признаков рассматриваемых составов преступления позволяет выделить некоторые особенности. В частности, законодатель вместе с общими признаками субъекта указывает на возможность использования лицом служебного положения (например, ч. 3 ст. 272 УК РФ).

Под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно выступает должностное лицо), т. е. тех, кто на законных основаниях пользуется компьютерной информацией и средствами ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных (БД), инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и пр.)¹.

Относительно субъективной стороны, специальных признаков, влияющих на квалификацию, для данных составов законодатель не выделяет; в основном деяния совершаются с умышленной формой вины.

Для единообразия понятийного аппарата целесообразно употреблять термин «преступления, совершаемые с использованием информа-

¹ Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. URL: <https://www.garant.ru/products/ipo/prime/doc/70542118> (дата обращения: 15.05.2020).

ционных технологий», включающий в себя помимо преступлений, рассматриваемых в гл. 28 УК РФ, еще и «некомпьютерные» статьи уголовного закона, которые фактически совершаются с помощью ИТ.

В связи с этим можно предложить следующее определение: «преступления, совершаемые с использованием информационных технологий, — это общественно опасные, противоправные деяния, причиняющие вред общественным отношениям в сфере безопасности информационных технологий (компьютерной информации) или создающие угрозу причинения такого вреда, а также иные запрещенные уголовным законом деяния, совершенные с помощью информационных технологий».

Следует отметить, что таковым нельзя признавать деяние, например, когда совершается хищение компьютера с целью дальнейшей продажи, поскольку компьютерная технология, вложенная в устройство, является только предметом посягательства. Для отнесения преступления к данной группе оно должно отвечать признаку направленности, для которого требуется наличие совокупности средства и способа.

Представляется, что у лица имеется любой вид ИТ (реальный предмет материального мира), используемый (его технические возможности) в реализации преступной деятельности.

Понятие «преступления, совершаемые с использованием информационных технологий» достаточно полно и точно отражает все указанные понятия, характеризующие данную группу преступлений. Подразумевается, что данное понятие в самом широком смысле отражает использование в преступной деятельности неограниченных информационных средств, способов и технологий. Информационные технологии постоянно развиваются. В связи с этим преступность, связанная с ИТ, приобретает различные, порой, изощренные формы, связанные с посягательством на разнообразные виды общественных отношений, ответственность за которые предусмотрена разными разделами и главами уголовного закона. Поэтому есть необходимость в применении одного обобщающего понятия для обозначения совокупности данного вида преступлений, которым является понятие «преступления в сфере информационных технологий». Выбранная здесь терминология основана еще и на том, что имеет нормативное отражение и позволяет избегать двусмысленного толкования.

Обобщая результаты проведенного анализа относительно различных позиций, можно сделать следующие выводы:

1. Трактовка понятий данной группы преступных посягательств варьируется в работах ученых от признания таковыми только преступлений, содержащихся в гл. 28 УК РФ, до любых преступлений, совершенных с использованием любых технических устройств. Большая часть авторов указывает на двойственную природу рассматриваемых преступлений.

Выделяются основные группы:

- преступления, ответственность за которые предусмотрена нормами гл. 28 УК РФ «Преступления в сфере компьютерной информации»;
- любые другие преступления, в которых дополнительным объектом преступного посягательства выступает безопасность в информационной сфере;
- деяния, в которых использование ИТ выступает способом совершения преступлений, где основным объектом посягательства выступают иные общественные отношения.

Данные группы преступных деяний либо совершаются с помощью информационных технологий (с использованием информационно-телекоммуникационных технологий, в т. ч. сети Интернет), либо посягательство ставит под угрозу указанные общественные отношения. В случае если лицо при совершении деяния применяет цифровые технологии, в совокупности они выражают способ совершения преступления.

2. Без особых дискуссий большая часть ученых-юристов отмечают такие характерные признаки:

- трансграничность;
- использование специальных технологий и технических средств;
- латентный характер преступности;
- отсутствие физического контакта с потерпевшими.

3. Ввиду активного развития процессов информатизации общества, с учетом того, что совершение преступлений с использованием ИТ становится все более распространенным, облегчает виновному достижение преступной цели, представляется необходимым включение в качестве квалифицирующего признака совершение преступления «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет» во все статьи УК РФ. Речь идет только о тех составах преступления, где такой способ является физически возможным.

Уголовно-правовая характеристика и проблемы квалификации преступлений, совершаемых с использованием информационных технологий

Введение в проблематику и актуальность

Определение места совершения преступления является одной из фундаментальных задач уголовного права и процесса. Однако в условиях цифровой трансформации этот классический институт сталкивается с новыми вызовами. Для его корректного применения в современном мире необходимо с высокой степенью точности определить понятийный аппарат и выявить специфические признаки деяний, совершаемых с использованием информационных технологий. Информационные технологии, проникая во все без исключения сферы жизни общества, кардинально меняют криминальную картину мира. Они играют весомую, а зачастую и решающую роль в вопросах технической оснащённости преступности, предоставляя лицам, совершающим преступления, принципиально новые инструменты и возможности.

Применение современных технических средств позволяет преступникам не только эффективно и скрыто координировать свои действия на международном уровне, но и внедрять такие изощренные способы достижения преступных целей, которые ранее не были известны уголовному праву и не могли быть в полной мере им охвачены. В научной литературе справедливо отмечается уникальный феномен организации преступной деятельности в сети Интернет. Так, в виртуальных преступных группах, создаваемых на специализированных платформах и в мессенджерах, участники могут не иметь никакой информации о реальной личности других членов группы, их местонахождении и никогда не встречаться с ними в физическом мире. Это создает принципиально новую, децентрализованную и анонимную модель преступного сообщества, борьба с которой традиционными методами затруднена.

Плюрализм дефиниций в юридической доктрине

В современной отечественной и зарубежной юридической доктрине преступления, совершаемые с использованием ИТ, понимаются далеко не однозначно. Они толкуются широко и разнородно, получая различные наименования и дефиниции. Ключевой проблемой, усугубляющей терминологическую путаницу, является факт, что на законо-

дательном уровне в УК РФ официальное закрепление получила лишь одна, достаточно узкая группа деяний, объединенная в главе 28 «Преступления в сфере компьютерной информации». Данная глава охватывает лишь прямые посягательства на компьютерные системы и данные, оставляя за рамками непосредственного регулирования огромный пласт преступлений, где ИТ выступают лишь инструментом.

Таким образом, в научной и научно-практической литературе можно встретить целый веер понятий, зачастую используемых как синонимы, хотя они таковыми не являются. Среди них: «преступления в сфере высоких технологий», «преступления, совершаемые при помощи телекоммуникационных сетей, включая сеть Интернет», «киберпреступления» (в последнее время этот термин приобрел наибольшую популярность), «компьютерные преступления», «ИТ-преступления», «преступления в сфере компьютерной информации» и другие.

Анализ исследований позволяет выделить два основных подхода к классификации. Первый вид — это «чистые» компьютерные преступления, то есть непосредственные посягательства на компьютерную информацию и системы (гл. 28 УК РФ). Второй вид — это любые традиционные преступления (мошенничество, вымогательство, клевета и пр.), в которых информационные технологии используются в качестве основного или вспомогательного средства их совершения, и ответственность за которые установлена иными статьями УК РФ.

Стоит отметить, что значительная часть научных работ смешивает уголовно-правовые и криминологические характеристики рассматриваемых преступлений. К числу последних относят:

1. Трансграничный характер. Виртуальное пространство стирает государственные границы, позволяя преступнику, находясь в одной стране, совершать деяния, последствия которых наступают в другой, что создает сложности для юрисдикции и международного сотрудничества.

2. Дистанционный характер. Отсутствие физического взаимодействия с жертвой является ключевой чертой. Преступное воздействие осуществляется исключительно посредством ИТ, в связи с чем круг потерпевших может быть неограниченным и территориально распределенным по всему миру.

3. Высоколатентный характер. Обусловлен сложностью ИТ-инфраструктуры, использованием средств анонимизации, а также тем, что и потерпевшие, и правоохранительные органы зачастую не

обладают достаточными познаниями для выявления и фиксации факта преступления.

4. Постоянная эволюция способов. Быстрое развитие ИТ приводит к столь же стремительному совершенствованию и модификации способов совершения преступлений, что опережает скорость адаптации правовых норм.

5. Низкая осведомленность потерпевших. Многие пользователи не обладают должной цифровой грамотностью, чтобы распознать преступное посягательство, а зачастую не знают, куда и как обращаться за защитой своих прав.

Эволюция понятий: от «киберпреступности» до «информационных преступлений»

В юридической науке на протяжении нескольких десятилетий предпринимаются попытки выработать и законодательно закрепить единую, универсальную терминологию для понимания данных видов преступлений. Сложность этой задачи кроется в отсутствии консенсуса относительно того, какой круг деяний следует относить к данной категории.

Исторически первым широко употребляемым термином, обозначающим рассматриваемый вид преступлений, является «Cybercrime» (киберпреступление). Это определение отражено в международных документах, в частности, в рекомендациях экспертов ООН, где термин «киберпреступность» обозначает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, либо против компьютерной системы или сети. Это широкое определение задало тон дальнейшим дискуссиям.

Отечественные ученые в своих трудах описывают киберпреступления по-разному. Некоторые исследователи, как, например, И. М. Рассолов, фактически отождествляют понятия «компьютерные преступления» и «киберпреступления», указывая, что к последним относятся общественно опасные деяния, совершаемые с применением средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете. Подобный подход обусловлен буквальным переводом и первоначальным толкованием англоязычного термина.

Понятие «компьютерные преступления» характерно для ранних этапов развития научной мысли, когда основным объектом посягательств были именно информационно-вычислительные системы, либо совершалось воздействие на них. Со временем исследователи начали предлагать более широкие трактовки. Так, Д. Н. Карпова указывает, что киберпреступление является актом социальной девиации с целью нанесения ущерба посредством любого технического средства с доступом в Интернет. И. Г. Чекунов развивает эту мысль, утверждая, что киберпреступность следует рассматривать шире компьютерной, поскольку для совершения преступлений используются не только стационарные компьютеры, но и мобильные устройства, смартфоны, планшеты и сложные системы связи, образующие единую цифровую экосистему.

В противовес этому некоторые исследователи, напротив, сужают определение. К примеру, Д. Л. Шиндер определяет киберпреступность как подкатегорию компьютерной преступности, ограничивая ее рамками сети Интернет. Однако анализ литературы показывает, что такая узкая позиция поддерживается наименьшим количеством ученых.

Отдельного внимания заслуживает понятие «информационные преступления». Данная формулировка представляется наименее удачной. Под ней часто понимаются общественно опасные деяния в области широкого круга отношений, связанных с созданием, сбором, обработкой, распространением информации и защитой прав субъектов информационных процессов. Существует и еще более широкая дефиниция, согласно которой информационными преступлениями признаются такие, состав которых включает в себя информацию в любом качестве. Подобный подход критикуется за неоправданно широкий круг охватываемых общественных отношений и отсутствие четкого указания, является ли информация предметом, средством преступления или же средой его совершения, что размывает границы понятия.

Содержательное ядро: преступления с использованием ИТ и их юридический анализ

Более предпочтительным представляется понятие «преступления, совершаемые с использованием высоких технологий», которое, как отмечают ученые, носит собирательный характер и употребляется для обозначения ситуаций, когда для совершения традиционных пре-

ступлений применяются ИТ. При этом важно подчеркнуть, что преступления по гл. 28 УК РФ и преступления с использованием высоких технологий не тождественны. Последние относятся к новым видам и способам совершения преступлений, возникшим в результате глобального распространения сети Интернет.

Для прояснения терминологии необходимо обратиться к легальным определениям. Федеральный закон «Об информации, информационных технологиях и о защите информации» определяет информационные технологии как процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. В свою очередь, примечание к ст. 272 УК РФ содержит понятие «компьютерной информации» как сведений, представленных в форме электрических сигналов. Таким образом, компьютерная информация является неотъемлемой составной частью ИТ, и их искусственное разделение ограничивает понимание сути явления.

Проводя анализ понятийного значения, отметим, что «преступления в сфере компьютерной информации» — это строгая законодательная категория, в то время как «преступления, совершаемые с использованием ИТ» — это более широкий научно-практический конструкт. Российское законодательство содержит достаточный аппарат для характеристики деяния как подпадающего под гл. 28 УК РФ. Однако отнесение преступления к последней невозможно без тщательного анализа объекта преступного посягательства.

Глава 3. КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ ПО РОССИЙСКОМУ УГОЛОВНОМУ ЗАКОНОДАТЕЛЬСТВУ

Исследование преступлений, совершаемых с использованием информационных технологий, невозможно без комплексного подхода. Для этого необходимы достаточный объем информации и понятийный аппарат, а также различные инструменты систематизации данных. Одним из используемых в уголовном праве методов является классификация преступлений.

В юридической литературе отмечается, что таких классификаций в уголовном законодательстве несколько:

1. По характеру и степени общественной опасности (ст. 15 УК РФ).
2. По элементам состава преступления (по объекту, объективной стороне, субъекту и субъективной стороне).
3. По степени опасности внутри однородного состава.

Такие классификации также могут быть естественными и искусственными, отражающими социальное содержание различных по основаниям деления преступлений и помогающим в оценке конкретно совершенных деяний. Главное условие — правильный выбор критерия классификации¹.

Классификация любых преступлений необходима в целях:

- составления общего представления об изучаемой группе явлений;
- характеристики отдельных объектов из выбранного круга явлений;
- оценки степени соотнесенности отдельных видов и рядов явлений и на этом основании выделение определенных закономерностей такой соотнесенности;
- прогнозирования возможности развития явлений в том или ином направлении².

¹ См.: Кадников Н. Г. Классификация преступлений по уголовному праву России. – М., 2000. С. 5–16.

² Чуманов Е. В. Гносеологическая функция классификации в российском праве // Научные труды филиала МГЮА в г. Кирове. № 10. – Киров, 2005. С. 163.

Помимо этого классификация состоит в том, что она способствует правильной уголовно-правовой оценке рассматриваемых преступлений, т. е. облегчает процесс их квалификации¹.

Преступления, совершаемые с использованием ИТ, достаточно сложно обособить в рамках определенных групп. Быстрое внедрение цифровых устройств во все сферы жизни общества приводит к тому, что подобным способом можно совершить практически любое преступление.

В международной практике имеется отражение типов киберпреступности. Так, в проекте доклада Управления ООН по борьбе с наркопреступностью к киберпреступлениям относят:

1. Компьютерное мошенничество или подлог.
2. Компьютерные преступления, связанные с использованием персональных данных.
3. Распространение или контроль распространения спама.
4. Компьютерные преступления, касающиеся авторских прав или товарных знаков.
5. Деяния, предполагающие использование компьютера в целях причинения личного вреда.
6. Деяния, предполагающие использование компьютера в целях завлечения детей и груминга².

В юридической литературе встречаются различные позиции. Основываясь на Конвенции Совета Европы о киберпреступности 2001 г., выделяют несколько групп преступлений:

1. «Собственно компьютерные» преступления, включающие в себя незаконный доступ, перехват, вмешательство в данные, в систему.
2. Преступления, в которых компьютер является орудием (электронные хищения и мошенничества).
3. Преступления, при совершении которых компьютер является интеллектуальным средством (размещение на сайтах детской порно-

¹ Безверхов А. Г. Имущественные преступления: монография. – Самара, 2002. С. 188.

² Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Документ ООН. UNODC. Comprehensive Study on Cybercrime. Feb. 2013. P. XVII. URL: <http://www.unodc.org/UNODC/CCPCJ/EG.4/2013/2> (дата обращения: 20.05.2023).

графии, информации, разжигающей национальную, расовую, религиозную вражду¹).

И. М. Рассолов делит рассматриваемые деяния на «преступления в сфере компьютерной информации» и «кибернетические преступления»². Преступления в сфере компьютерной информации требуют правового закрепления в УК РФ, а кибернетические — попадают под квалификацию иных статей уголовного кодекса, но совершаются с данным квалифицирующим признаком.

Помимо этого встречаются иные варианты классификации. Некоторые авторы предлагают выделять «преступления, совершенные с использованием сети» и «преступления, зависящие от сети». К преступлениям, совершенным с использованием сети, относят деяния, которые уже являются незаконными и могли бы быть совершены без использования компьютерной сети, однако совершаются в ней. В свою очередь, преступления, зависящие от сети, обязаны своим существованием только появлению интернета³.

Закрепленная в УК РФ система позволяет условно разделить деяния на две группы:

1. Преступления, которые непосредственно являются «компьютерными»:

– ст. 272 «Неправомерный доступ к компьютерной информации»;

– ст. 273 «Создание, использование и распространение вредоносных компьютерных программ»;

– ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

– ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»;

– ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости,

¹ Тропина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Информационные технологии и безопасность: сб. науч. тр. междунар. конф. Вып. 3. – Киев, 2003. С. 176–177.

² См: Рассолов И. М. Право и Интернет. Теоретические проблемы. – М., 2009. С. 133–135.

³ Шиндер Д. Л. Киберпреступность: перед лицом проблемы // Центр исследования компьютерной преступности. URL: <http://www.crime-research.ru/library/cybercrimes3.html> (дата обращения: 20.05.2023).

безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования».

2. Преступления, при совершении которых ИТ существенно облегчают противоправную деятельность, выступая способом совершения преступления.

Этот вариант классификации представляется самым очевидным и простым в своем делении преступлений рассматриваемой нами группы на виды.

Выше уже косвенно упоминалось о второй классификации, которую возможно выделить при анализе преступлений, совершаемых с использованием информационных технологий.

Речь идет о классификации по объекту преступного посягательства:

– преступления, в которых общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз выступают в качестве основного объекта преступления. К таковым относятся все составы, указанные в гл. 28 УК РФ «Преступления в сфере компьютерной информации»;

– преступления, в которых общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз выступают в качестве дополнительного или факультативного объекта преступления. К таковым можно отнести следующие составы преступления: ст. 1593 УК РФ (мошенничество с использованием электронных средств платежа), ст. 1596 УК РФ (мошенничество в сфере компьютерной информации), ст. 1853 УК РФ (манипулирование рынком).

При вопросе квалификации деяний по совокупности преступлений, несмотря на указание в качестве дополнительного или факультативного объекта общественных отношений в информационной сфере, очевидна необходимость дополнительной квалификации по составам, указанным в гл. 28 УК РФ¹.

Преступления, совершенные с использованием ИТ, посягают на различные общественные отношения. Уголовный закон ставит под охрану только те общественные отношения, которые могут быть нормативно урегулированы, а также являются наиболее значимыми.

¹ См., например: Шеслер А. В. Мошенничество: проблемы реализации законодательных новелл // Уголовное право. 2013. № 2. С. 67–71.

В свою очередь, уголовный закон говорит об объектах уголовно-правовой охраны, закрепленных в ст. 2 УК РФ и объектах преступлений, содержащихся в конкретных составах. При этом стоит сказать, что ст. 2 УК РФ указывает неполный перечень таких объектов, а в Особенной части УК РФ предусмотрена охрана и иных объектов, например, порядок управления, интересы правосудия и т. д.

Используя систему уголовного закона, можно поделить и классифицировать киберпреступления по тем группам общественных отношений, на которые совершается посягательство:

- против жизни и здоровья;
- против свободы, чести и достоинства личности;
- против половой свободы и половой неприкосновенности личности и т. д.

Однако такая классификация требует дополнительного пояснения, так как не все группы общественных отношений, хоть и объединенные единым видовым объектом, могут быть совершены посредством информационных технологий, ввиду специфики конструкции объективной стороны.

Например, использование ИТ имеет место при посягательстве на жизнь в таких составах, как доведение до самоубийства, склонение к самоубийству, организация деятельности, направленной на побуждение к совершению самоубийства. Говорить о совершении убийства путем использования информационных технологий достаточно сложно ввиду специфичности такого способа. Речь не идет о ситуации, когда лицо применяет, например, компьютер (его физические свойства), нанося им удары по голове потерпевшего. Так, по мнению С. В. Бородин, когда «лицо ставит себе цель довести другое лицо до самоубийства, создает для этого все необходимые условия, содеянное следует квалифицировать как убийство, которое будет характеризоваться особым способом его совершения»¹.

Моделируя ситуацию, можно представить следующее: некое лицо совершает похищение близких для потерпевшего лица, используя информационно-телекоммуникационные сети, выходит на связь с потерпевшим в режиме «онлайн», угрожая лишением жизни в отношении близкого для потерпевшего лица, ставит ему условие, при котором требует от потерпевшего лишить себя жизни, в результате чего достигает данной цели. В таком случае деяние необходимо квалифи-

¹ Бородин С. В. Преступления против жизни. – М., 2001. С. 37.

цировать по ст. 105 УК РФ. В этой связи можно говорить и о причинении смерти по неосторожности и о причинении тяжкого вреда здоровью (например, по признаку наступления психического расстройства).

Относительно ст. 109 УК РФ, лицо может посредством ИТ направить потерпевшему, имеющему заболевание сердца, информацию «шокирующего характера», что может повлечь наступление смерти (с учетом обладания злоумышленника достоверным знанием о наличии заболевания возможно изменение квалификации). При причинении тяжкого вреда по неосторожности, по признаку наступления психического расстройства может быть использован подобный способ совершения преступления.

В связи с этим можно выделить следующую классификацию:

1. Преступления против личности, совершаемые с использованием информационно-телекоммуникационных сетей.
2. Преступления в сфере экономики, совершаемые с использованием информационно-телекоммуникационных сетей.
3. Преступления против общественной безопасности, совершаемые с использованием информационно-телекоммуникационных сетей.
4. Преступления против здоровья населения и общественной нравственности, совершаемые с использованием информационно-телекоммуникационных сетей.
5. Преступления против основ конституционного строя и безопасности государства, совершаемые с использованием информационно-телекоммуникационных сетей.

Вместе с тем, например, совершение убийства в состоянии аффекта с использованием цифрового пространства невозможно ввиду особенностей конструкции деяния. В этой связи предлагаем следующую классификацию:

1. Преступления, которые могут быть совершены с использованием ИТ (вне зависимости от специального упоминания в диспозиции).
2. Преступления, которые могут быть совершены с использованием ИТ (с отражением в диспозиции).
3. Преступления, которые по своим объективным признакам не могут содержать подобный способ совершения деяния.

Следующее основание, которое можно использовать при классификации преступлений, — выделение их в группы по характеру и

степени общественной опасности. В теории уголовного права выделяют основной состав, состав со смягчающими обстоятельствами, состав с отягчающими обстоятельствами. Традиционно составы с отягчающими обстоятельствами содержатся во 2, 3, 4 и т. д. частях состава преступления. В связи с этим возможно выделить:

1. Основные составы преступления, где использование ИТ выступает обязательным признаком состава преступления:

– ст. 1593 «Мошенничество с использованием электронных средств платежа»;

– ст. 1596 «Мошенничество в сфере компьютерной информации»;

– ст. 1712 «Незаконные организация и проведение азартных игр» (ч. 1);

– ст. 1853 «Манипулирование рынком» (ч. 1);

– ст. 187 «Неправомерный оборот средств платежей»;

– ст. 2381 «Обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок» (ч. 11);

– ст. 2581 «Незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации» (ч. 11);

– ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» (ч. 1);

– гл. 28 УК РФ «Преступления в сфере компьютерной информации».

2. Квалифицированные составы преступлений, где использование ИТ выступает отягчающим обстоятельством:

– ст. 110 «Доведение до самоубийства» (п. «д» ч. 2);

– ст. 1101 «Склонение к совершению самоубийства или содействие совершению самоубийства» (п. «д» ч. 3);

– ст. 1102 «Организация деятельности, направленной на побуждение к совершению самоубийства» (ч. 2);

– ст. 1512 «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего» (п. «в» ч. 2);

– ст. 2052 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма» (ч. 2);

– ст. 2281 «Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконный сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества» (п. «б» ч. 2);

– ст. 242 «Незаконное изготовление и оборот порнографических материалов или предметов» (п. «б» ч. 3);

– ст. 2421 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних» (п. «г» ч. 2);

– ст. 2422 «Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов» (п. «г» ч. 2);

– ст. 245 «Жестокое обращение с животными» (п. «г» ч. 2);

– ст. 2581 «Незаконная добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации» (п. «б» ч. 2);

– ст. 280 «Публичные призывы к осуществлению экстремистской деятельности» (ч. 2);

– ст. 2801 «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации» (ч. 2);

– ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» (ч. 2).

Также ввиду рассмотрения указанного основания классификации стоит выделить группу «нейтральных» к данному признаку деяний, которые могут быть совершены названным способом без специального указания в уголовном законе. При этом использование ИТ никак не учтено законодателем.

Основные выводы, которые необходимо сделать относительно рассматриваемых деяний:

1. Киберпреступления можно классифицировать:

– основываясь на системе УК РФ: преступления, которые непосредственно являются «компьютерными»; преступления, при совер-

шении которых информационные технологии существенно облегчают противоправную деятельность, выступая способом совершения преступления;

- по объекту преступного посягательства: преступления, в которых общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз выступают в качестве основного объекта преступления; преступления, в которых общественные отношения в информационной сфере выступают в качестве дополнительного или факультативного объекта преступления;

- по способу совершения деяния: преступления, которые могут быть совершены с использованием ИТ (вне зависимости от специального упоминания в диспозиции); преступления, которые могут быть совершены с использованием ИТ (с отражением в диспозиции); преступления, которые по своим объективным признакам не могут содержать подобный способ совершения деяния;

- по характеру и степени общественной опасности (по степени опасности внутри однородного состава): основные составы преступления, где использование ИТ выступает обязательным признаком состава преступления; квалифицированные составы преступлений, где использование информационных технологий выступает отягчающим обстоятельством; «нейтральные» к данному признаку преступления;

- по группам общественных отношений:

- преступления против личности, совершаемые с использованием информационно-телекоммуникационных сетей;

- преступления в сфере экономики, совершаемые с использованием информационно-телекоммуникационных сетей;

- преступления против общественной безопасности, совершаемые с использованием информационно-телекоммуникационных сетей;

- преступления против здоровья населения и общественной нравственности, совершаемые с использованием информационно-телекоммуникационных сетей;

- преступления против основ конституционного строя и безопасности государства, совершаемые с использованием информационно-телекоммуникационных сетей.

2. В результате рассмотрения различных оснований классификации, хотим отметить, что многие деяния могут быть совершены путем использования ИТ, но тем не менее указанный способ может ни-

как не отражаться в диспозиции статьи. При этом в некоторых составах законодатель заранее учел такую возможность, включив использование информационных технологий в качестве отягчающего обстоятельства.

3. Классификация по целевой направленности и бизнес-модели преступной деятельности.

В дополнение к юридическим критериям, крайне продуктивной является классификация, основанная на экономических и криминологических мотивах злоумышленников. Такой подход широко используется в международной практике, в частности, в аналитических отчетах Europol, Group-IB и других организаций. Она позволяет понять не «как» совершено преступление с точки зрения состава, а «зачем» и «с какой бизнес-моделью».

Киберпреступления, направленные на незаконное извлечение финансовой выгоды.

- фишинг и кардинг — целенаправленное получение реквизитов банковских карт, логинов и паролей от онлайн-банков и платежных систем;

- кибермошенничества — широкий спектр деяний, включая «скид-мошенничество» (с использованием скиммеров), мошенничество с криптовалютными активами, фиктивные интернет-магазины и т. д.;

- ransomware-атаки (шифровальщики) — блокирование или шифрование данных с последующим требованием выкупа за их восстановление. (Это одна из самых прибыльных и опасных моделей, парализующих деятельность как компаний, так и государственных учреждений.);

- торговля запрещенными товарами и услугами на теневых онлайн-площадках (даркнет) — использование анонимных сетей для оборота наркотиков, оружия, поддельных документов.

Киберпреступления, направленные на получение информации (кибершпионаж и хищение данных).

- корпоративный шпионаж — целенаправленные атаки (Targeted Attacks, APT) на компании с целью хищения коммерческой тайны, ноу-хау, перспективных разработок;

- государственный шпионаж — похищение информации, составляющей государственную, военную или дипломатическую тайну;

- кража персональных данных и баз данных — массовый сбор информации о физических лицах для ее последующей продажи или использования в мошеннических схемах.

Киберпреступления, направленные на нарушение функционирования критической инфраструктуры и информационных систем.

- DDoS-атаки (Distributed Denial of Service) — Организация массовых запросов к серверам с целью вызвать их отказ в обслуживании легитимным пользователям. Мотивацией может быть кибервандализм, политический протест (хактивизм) или недобросовестная конкурентная борьба.

- кибердиверсии — целенаправленные атаки на объекты критической информационной инфраструктуры (КИИ) (энергетические сети, системы водоснабжения, транспортные узлы, финансовые системы. Сюда в полной мере относятся составы, предусмотренные ст. 274.1 УК РФ).

Киберпреступления против личности и общественной нравственности.

- киберсталкинг и кибербуллинг — организованная травля, преследование и шантаж в цифровой среде;

- груминг — установление эмоциональной связи с несовершеннолетним для его последующей сексуальной эксплуатации;

- незаконный оборот материалов порнографического характера с участием несовершеннолетних (ст. 242.1, 242.2 УК РФ).

Такая классификация напрямую влияет на приоритеты правоохранительных органов, позволяя сосредоточить ресурсы на борьбе с наиболее социально и экономически опасными формами киберпреступности.

4. Классификация по технико-криминалистическому критерию: способу реализации кибератаки.

Для целей расследования и доказывания крайне важна классификация, основанная на технических методах, использованных злоумышленником. Эта классификация пересекается с объективной стороной преступления, но фокусируется на инструментарии и векторах атаки.

Атаки, нацеленные на уязвимости программного обеспечения:

- эксплойтирование уязвимостей в операционных системах, приложениях, протоколах связи;

- внедрение вредоносного кода (вирусы, черви, трояны, бэкдоры).

Атаки, нацеленные на человеческий фактор (социальная инженерия):

- фишинг и его разновидности (таргетированный фишинг, вишинг) — манипулирование людьми для добровольной передачи конфиденциальной информации.

Фарминг — перенаправление жертв на поддельные сайты через изменение записей DNS или файлов hosts.

Кви-прокси атаки — создание фальшивых точек доступа Wi-Fi для перехвата трафика.

Атаки на аппаратное обеспечение и физические носители:

- установка аппаратных закладок («жучков»);
- кража или несанкционированное копирование данных с физических носителей.

Комплексные многовекторные атаки (Advanced Persistent Threat - АРТ) — сочетание всех вышеперечисленных методов для длительного и скрытого пребывания в информационной системе жертвы.

Данная классификация незаменима для следователей и экспертов, так как определяет перечень необходимых следственных действий и судебных экспертиз (компьютерно-технической, сетевой, инженерно-технической).

5. Проблемы правоприменения и необходимость совершенствования уголовного закона

Несмотря на все многообразие классификаций, правоприменительная практика сталкивается с системными проблемами, которые не могут быть решены лишь за счет теоретического структурирования знаний.

Во-первых, сохраняется проблема квалификации по совокупности преступлений. Как справедливо отмечено в исходном тексте, даже если отношения в информационной сфере являются дополнительным объектом, зачастую требуется квалификация по главе 28 УК РФ. Однако на практике это происходит не всегда. Например, при хищении денежных средств со счета с использованием вредоносной программы, следователь нередко ограничивается статьей о мошенничестве (ст. 159 УК РФ или 159.6 УК РФ), не вдаваясь в технические детали, которые могли бы повлечь дополнительную квалификацию по ст. 273 УК РФ. Это обедняет юридическую оценку содеянного и не отражает всей полноты общественной опасности.

Во-вторых, предлагаемое авторами дополнение ст. 63 УК РФ новымотягчающим обстоятельством — «использование информационно-телекоммуникационных сетей» — является своевременным и обоснованным. Однако этого недостаточно. Целесообразно рассмотреть возможность введения специального квалифицирующего признака «с использованием информационных технологий» в те составы преступлений, где такой способ резко повышает общественную опасность.

Например, клевета (ст. 128.1 УК РФ), размещенная в личном блоге, и клевета, распространяемая через бот-сеть на миллионы пользователей, — это деяния разного порядка с точки зрения масштаба причиняемого вреда. Отсутствие в диспозиции ст. 128.1 УК РФ такого признака не позволяет дифференцировать наказание. Аналогичная ситуация с вымогательством (ст. 163 УК РФ), которое, будучи совершенным с использованием DDoS-атаки или угрозы утечки данных (доксинг), приобретает качественно новые черты.

В-третьих, требует развития институт конфискации орудий и средств преступления. В цифровой среде орудием преступления является не только компьютер, но и вредоносный код, доменные имена, аккаунты в социальных сетях и мессенджерах, криптокошельки. Современная правовая доктрина и практика должны выработать четкие процедуры обращения в доход государства таких нематериальных активов, используемых в преступных целях.

6. Перспективы: towards a динамической классификации

Будущее классификации киберпреступлений лежит в области создания гибких, динамичных моделей, способных адаптироваться к новым технологическим вызовам. Так, с появлением технологий искусственного интеллекта (ИИ) и машинного обучения возникает новый пласт преступлений:

- глубокие фейки (deepfakes) для шантажа, манипулирования рынком или дестабилизации политической обстановки;
- использование ИИ для взлома систем защиты методом перебора (brute force) или для создания свехубедительных фишинговых сообщений;
- атаки на системы, управляемые ИИ (беспилотный транспорт, «умные» города).

Классификация должна быть открыта для включения таких новых феноменов. Возможно, следующим шагом станет создание «жи-

вого» классификатора в форме базы данных, поддерживаемой на уровне Верховного Суда РФ или Генеральной прокуратуры, который будет оперативно актуализироваться с учетом изменений криминальной практики и разъяснений Пленума ВС РФ.

Таким образом, исследование преступлений, совершаемых с использованием информационных технологий, действительно невозможно без комплексного подхода, ядром которого является многоаспектная классификация. Рассмотренные основания — от традиционных, базирующихся на структуре УК РФ, до современных, учитывающих бизнес-модели и технические способы атак, — не противоречат, а взаимодополняют друг друга.

Уголовно-правовая классификация (по объекту, по степени общественной опасности) остается фундаментом для квалификации и назначения наказания.

Криминологическая и экономическая классификация (по мотивации и бизнес-модели) позволяет вырабатывать стратегические приоритеты в борьбе с киберпреступностью.

Технико-криминалистическая классификация (по способу атаки) является ключом к эффективному расследованию и доказыванию.

Только синтез этих подходов позволяет сформировать целостное представление о феномене киберпреступности. Дальнейшее совершенствование уголовного закона, в частности, введение универсального квалифицирующего признака, связанного с использованием ИТ, и развитие института конфискации цифровых активов, будет способствовать адекватной уголовно-правовой оценке этих опасных и постоянно эволюционирующих деяний.

Глава 4. МЕХАНИЗМ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационных технологий обусловило их применение в преступной деятельности. Анализ оперативной обстановки в области предупреждения, выявления и пресечения компьютерных преступлений свидетельствует о наличии устойчивой тенденции к изменению видов преступлений в сферах компьютерной информации и электронной коммерции в сегментах информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет).

Неконкретность понятий и отсутствие единого подхода к терминологии, применяемой при осуществлении количественного учета и классификации новых способов совершения преступлений в сфере информационных технологий, осложняет определение реальной степени их угроз.

Предлагаемая типология преступлений дает возможность создать единый механизм учетно-аналитических операций при оценке состояния и динамики киберпреступности, а также обосновать практические рекомендации и определить пути сотрудничества в рассматриваемой сфере.

1. Способы совершения мошеннических действий с использованием сети Интернет, средств подвижной связи и систем дистанционного банковского обслуживания.

Основную долю компьютерных инцидентов составляют распространение вредоносных программ, предназначенных для хищения учетных записей пользователей сети Интернет, и преступления, связанные с электронными платежными системами.

Способы совершения данных преступлений обусловлены особенностями их предмета и средств совершения: в преступных целях используется порядок осуществления банковских операций по переводу безналичных денежных средств, находящихся на счетах банковских платежных карт, с использованием средств мобильной связи, а также порядок оказания услуг подвижной (так называемой мобильной) связи операторами.

Мошеннические действия, в том числе с использованием мобильных средств связи, путем перевода денежных средств со счетов

банковских карт потерпевших на счета третьих лиц в большинстве случаев совершаются в отношении держателей банковских карт клиентов, подключенных к системам дистанционного банковского обслуживания.

Анализ материалов судебной практики позволяет классифицировать способы завладения денежными средствами, находящимися на счетах банковских карт, следующим образом.

1.1. Введение потерпевшего в заблуждение относительно целей перевода денежных средств путем совершения телефонных звонков или направления СМС-сообщений. Под влиянием заблуждения потерпевший самостоятельно переводит денежные средства со своего счета на счета третьих лиц через системы интернет-банкинга и мобильного банкинга, терминалы банков или иным способом.

1.1.1. Побуждение потерпевшего к переводу денежных средств со своего счета на счета третьих лиц путем сообщения ему по телефону или через СМС-сообщение ложных сведений о внезапно возникших у его близких родственников серьезных проблемах, связанных с несчастным случаем, дорожно-транспортным происшествием, причинением вреда здоровью третьих лиц, задержанием за хранение наркотических средств, совершением других преступлений либо с долговыми обязательствами, для незамедлительного решения которых срочно требуется определенная сумма денег.

При этом злоумышленники звонят или направляют СМС-сообщения потерпевшим по случайно подобранным номерам телефонов, как мобильных, так и стационарных, от имени их родственников, друзей, знакомых или сотрудников правоохранительных органов, указывают номер телефона или банковской карты, на который следует осуществить перевод, а также сумму денежных средств, которую необходимо перечислить. Во многих случаях мошенничество данным способом совершают лица, отбывающие наказание в местах лишения свободы.

1.1.2. Уведомление потерпевшего по телефону (в основном путем рассылки СМС-сообщений) о выпавшем ему крупном призе при розыгрыше лотереи и необходимости перевода определенной суммы денежных средств (якобы налоговых или иных платежей) на указанный номер телефона или платежного средства в качестве условия получения приза.

1.1.3. Направление потерпевшему (путем рассылки СМС-сообщений) ложного уведомления о зачислении на его банковский

счет определенной суммы денежных средств, а через некоторое время — сообщения об ошибочном зачислении этой суммы с просьбой о ее возврате посредством перевода на указываемый номер телефона или банковской карты.

1.1.4. Осуществление звонков потерпевшим от имени оператора связи с предложением подключить новую услугу и набрать для этого под диктовку определенный код, который в действительности является комбинацией для перевода денежных средств со счета абонента на счет третьего лица.

1.1.5. Сообщение потерпевшему заведомо ложных сведений (посредством телефонных звонков или СМС-сообщений от имени банка) о возникших технических или иных проблемах, препятствующих дальнейшему использованию им своей банковской карты, с предложением совершить для устранения данных препятствий определенные операции по банковскому счету через системы интернет-банкинга, мобильного банкинга или терминал банка. Совершение потерпевшим, введенным в заблуждение, данных операций в действительности влечет перевод денежных средств со счета его банковской карты на счет третьего лица.

Такие действия производятся лицами, совершающими мошенничество, как правило, двумя способами. Первый способ заключается в направлении потерпевшему ложного уведомления посредством СМС-сообщения от имени банка о временной блокировке банковской карты с предложением навести справки по указанному номеру телефона.

Когда потерпевший звонит по данному номеру, мошенник, представившись сотрудником службы безопасности банка, объясняет причины блокировки карты попытками посторонних лиц получить информацию о реквизитах банковской карты или о банковском счете, сбоями в работе сервера банка либо иными надуманными обстоятельствами.

Затем злоумышленник, в зависимости от информации, предоставленной потерпевшим при ответах на поставленные вопросы, предлагает совершить определенные действия посредством интернет-банкинга, мобильного банкинга либо через ближайший банкомат. При этом потерпевшему сообщается о важности оперативного совершения данных действий, поскольку в противном случае якобы возникнет необходимость замены банковской карты, которая может затянуться

на долгое время, и воспользоваться денежными средствами, хранящимися на карте, в течение этого периода будет невозможно.

Согласившись на выполнение ложной операции разблокировки карты, потерпевший, например, подходит к банкомату, звонит по сообщенному ему номеру телефона и, действуя по указанию, вставляет свою банковскую карту в банкомат, набирает на нем код доступа к карте, осведомляет мошенников об остатке денежных средств на ней. После этого он набирает под диктовку цифры, полагая, что вводит код для разблокировки карты, а в действительности переводит денежные средства со своей карты на банковскую карту или лицевые счета абонентских номеров сотовых операторов третьих лиц либо подключает услугу «Интернет-банк» или «Мобильный банк», позволяющую управлять счетом его банковской карты.

При этом потерпевшему становится известно по полученным чекам или поступающим СМС-уведомлениям об осуществлении им операции перевода денежных средств. Однако его убеждают, что переведенные денежные средства зарезервированы и в течение нескольких часов будут возвращены на счет, и предлагают ему не пользоваться картой до их поступления. Затем злоумышленники переводят поступившие денежные средства на банковские счета других лиц либо на счета до востребования через системы денежных переводов отдельных кредитных учреждений. Впоследствии лица, не осведомленные об истинном их происхождении этих денежных средств, за финансовое вознаграждение получают их в банке и передают незнакомым им лицам.

Используемые мошенниками для рассылки СМС-сообщений, разговоров с потерпевшими и перечисления денежных средств абонентские номера, как правило, оформляются ими на вымышленных лиц. Банковские карты, на которые перечисляются похищенные денежные средства, в основном принадлежат не имеющим отношения к мошенникам лицам, по просьбе или по собственной инициативе оформляющим их на свое имя и передающим полученные средства за денежное вознаграждение малознакомым или незнакомым лицам.

Второй способ состоит во введении держателя банковской карты (владельца счета) в заблуждение (в том числе с помощью методов социальной инженерии, т. е. с использованием познаний в области психологии) относительно сущности операций с целью получения информации, необходимой для несанкционированного доступа, либо принуждения потерпевшего совершить определенные действия.

Лица, совершающие мошенничество, при первом телефонном разговоре с потерпевшим выясняют, что абонентский номер его телефона подключен к системе дистанционного банковского обслуживания. Поводом к возникновению доверительных отношений может стать, например, то, что преступник представляется сотрудником службы социального обеспечения либо сотрудником банка, целью которого является перечисление потерпевшему дополнительной социальной выплаты и т. п.

Затем злоумышленники предлагают потерпевшему посредством данной системы совершить для разблокировки банковской карты операции якобы по временному резервированию денежных средств, находящихся на его банковском счете, а в действительности по переводу их на счета третьих лиц. Введенный в заблуждение держатель карты переводит, действуя по указанию мошенников, денежные средства на указанный ему счет банковской карты или абонентский номер, не сомневаясь, что переведенные им денежные средства в течение суток поступят обратно на его счет.

К разновидностям введения в заблуждение потерпевшего также следует отнести перевод средств со счета потерпевшего путем применения системы СМС-банкинга — технологии дистанционного банковского обслуживания посредством СМС-сообщений, в которой доступ к банковским счетам и операциям по банковским счетам предоставляется в любое время с использованием номера мобильного телефона клиента, предварительно зарегистрированного в банке. Эта технология, помимо «пассивного» СМС-оповещения о проведенных операциях и состоянии счета, позволяет осуществлять «активное» СМС-оповещение — отправку сообщений в ответ на получаемые от клиента СМС-запросы (например, о балансе банковской карты, предоставлении счета, мини-выписки или блокировке банковской карты), а также отправлять банку через сеть оператора подвижной связи команды на проведение операций с денежными средствами клиента банка (владельца сим-карты).

Мошенники также используют способ совершения операций по USSD-запросам: предлагают потерпевшему набрать USSD-команду или отправить СМС на специальный номер банка для совершения перевода. USSD (Unstructured Supplementary Service Data) — стандартный сервис в сетях GSM, позволяющий организовать интерактивное взаимодействие между абонентом сети и сервисным приложением в режиме передачи коротких сообщений. Основное направление ис-

пользования USSD-сервиса — предоставление абонентам возможности получать дополнительную информацию от приложений и управлять этими приложениями.

1.1.6. Вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем блокирования абонентского номера потерпевшего, восстановления его на дубликат сим-карты и перечисления денежных средств с банковского счета потерпевшего посредством системы мобильного банкинга на счета третьих лиц.

В некоторых случаях для получения дубликата сим-карты, установленной в телефоне потерпевшего, мошенники вступают в сговор с представителями оператора связи, работающими в офисах продаж и обслуживания клиентов. Иногда данные преступления совершаются представителями оператора связи самостоятельно.

Особенностью таких способов мошенничества является отсутствие непосредственного контакта лиц, их совершающих, с потерпевшими, поскольку последние вводятся в заблуждение и побуждаются к осуществлению определенных действий через средства дистанционной коммуникации.

1.2. Использование найденного, похищенного, приобретенного либо случайно оказавшегося у субъекта преступления чужого телефонного аппарата с абонентским номером владельца, подключенного к услуге «Мобильный банк».

Потерпевший, чей телефонный аппарат по тем или иным причинам выбыл из владения (утерян, похищен, продан вместе с сим-картой), своевременно не обращается в банк с просьбой отключить от его абонентского номера услугу «Мобильный банк», сам передает свой телефонный аппарат другому лицу во временное пользование или оставляет его без присмотра. Преступники, обнаружив при пользовании телефоном, что тот подключен к указанной услуге, совершают хищение денежных средств, находящихся на банковском счете потерпевшего.

1.3. Использование подключенного к услуге «Мобильный банк» абонентского номера, ранее принадлежавшего другому абоненту.

Данный способ мошенничества заключается в использовании лицами, его совершающими, того обстоятельства, что потерпевший, осуществив замену абонентского номера, подключенного к услуге

«Мобильный банк», не предупредил об этом кредитную организацию, а его абонентский номер впоследствии был перерегистрирован оператором связи на другое лицо. Обнаружив, что такой абонентский номер подключен к услуге «Мобильный банк», новый владелец номера посредством указанной услуги переводит денежные средства потерпевшего на свой банковский счет или на счета третьих лиц.

2. Способы совершения хищений через вмешательство в функционирование средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей путем подделки электронных средств идентификации платежей, использования идентификационных данных банковских карт.

Несанкционированное вмешательство в платежные системы — один из наиболее распространенных способов хищения денежных средств на территории государств — участников СНГ.

Основную долю (как по объему хищений, так и в количественном выражении) несанкционированных операций составляют CNP-транзакции (операции в сети Интернет).

Чаще всего хищение денежных средств физических и юридических лиц посредством так называемого карточного мошенничества совершается следующими способами.

2.1. Проведение банковских операций посредством несанкционированного доступа («хакерского взлома») к хранилищам данных и иной банковской информации.

2.1.1. Хищение денежных средств путем доступа к идентификационным данным сотрудников кредитных организаций.

Установление непосредственного контроля над компьютерными системами является распространенным способом совершения указанного вида преступлений. В таких случаях в зону риска попадают предприятия и организации, внутренняя сеть которых имеет точку доступа к сети Интернет. Злоумышленники, подобрав пароли к системе и получив полный контроль над ней, могут осуществлять шифрование данных либо похищение учетных данных. При этом оборудование жертвы без ее ведома на протяжении длительного времени может использоваться злоумышленниками в преступных целях (подбор паролей, рассылка нежелательных почтовых сообщений и т. п.).

2.1.2. Хищение и вымогательство денежных средств с помощью «банковских» вирусов.

Ввиду появления новых технологических решений по усовершенствованию средств противодействия бот-сетям большая часть преступных групп, работающих против банков и их клиентов, отказывается от стандартных методов при распространении своих вредоносных программ-троянов («троянских коней») в пользу спам-рассылок с возможностью автоматического цикла, например когда вредоносная программа перенаправляет интересующий трафик на другие серверы. Бот-сеть, или ботнет, - компьютерная сеть, состоящая из некоторого количества хостов с запущенными ботами (автономным программным обеспечением). Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять определенные действия с использованием ресурсов зараженного компьютера. Обычно используется для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удаленной системе, атак на отказ в обслуживании (DoS- и DDoS-атаки).

Вредоносные программы-трояны осуществляют не санкционированные пользователем действия: уничтожают, блокируют, модифицируют или копируют информацию, нарушают работу компьютеров или компьютерных сетей. В отличие от вирусов и червей, вредоносные программы-трояны не создают свои копии, не способны к самовоспроизведению.

В настоящее время наиболее распространенным способом использования вредоносных программ является отправление на персональный компьютер жертвы спам-сообщения, содержащего замаскированный загрузчик, который после исполнения загружает новую модификацию программы-трояна, загружающую, в свою очередь, компьютерного червя. После этого червь использует установленный на скомпрометированных устройствах почтовый клиент с целью рассылки спам-сообщений, к которым прикреплен вредоносный загрузчик. Червь отправляет спам-сообщения не контактам жертвы, а на адреса почты, полученные с сервера злоумышленников, а по окончании рассылки писем самоуничтожается.

Участились случаи совершения хищений с использованием банковских троянов, которые способны вести электронный шпионаж за пользователем (копировать вводимые с клавиатуры данные, изображения экрана, список активных приложений и т. д.), похищать конфиденциальную информацию пользователей для доступа к системам онлайн-банкинга.

С целью сокрытия следов своей противоправной деятельности злоумышленники активно используют средства анонимизации (VPN, TOR, Ргоху), шифрования интернет-трафика, компьютерной техники и личной переписки.

Большое распространение получили программы malware типа ransomware (иначе — «трояны-вымогатели») — вредоносное программное обеспечение, предназначенное для вымогательства. Их можно разделить на два основных типа — шифровальщики (cryptoransomware, крипторы) и блокировщики (blockers, блокиеры). Шифровальщики, попадая в компьютер, шифруют ценные файлы (документы, фотографии, базы данных и т. п.) таким образом, что их нельзя открыть. За расшифровку мошенники требуют выкуп.

2.2. Способы получения учетных данных держателей банковских карт: пароля, логина, номера и кода проверки подлинности карты и т. д. (фишинг).

2.2.1. Получение путем обмана или иным неправомерным способом реквизитов банковской карты, идентификаторов ее держателя и последующее осуществление с использованием полученных данных и средств мобильной связи перевода денежных средств, находящихся на банковском счете потерпевшего, на счета третьих лиц.

Например, широко распространена рассылка от имени банка СМС-сообщений о блокировке банковской карты с указанием номера телефона для получения справок. Позвонившему на указанный номер потерпевшему сообщается о произошедшем техническом сбое в работе компьютерной системы банка и предлагается для разблокировки или перерегистрации карты сообщить представителю банка номер и код карты либо пароли для ее использования.

Нередко мошенники получают идентификационные данные (номер и код проверки подлинности) банковской карты под предлогом необходимости этих сведений для осуществления перевода денежных средств на банковский счет потерпевшего, в частности в качестве оплаты за товар, объявление о продаже которого размещено в сети Интернет.

2.2.2. Получение учетных данных путем обмана потерпевшего в момент использования им платежной карты для осуществления операций через банкомат.

Мошенники обращаются к неосведомленному потерпевшему с просьбой проверить с помощью его карты, находящейся в картоприемнике банкомата, работу раздела «Интернет-обслуживание». Согла-

сившись, потерпевший под диктовку проводит операции, завершающиеся распечаткой чека с полной информацией о его банковской карте, включая идентификатор и пароли для пользования системой интернет-банкинга, который попадает в распоряжение преступников.

2.2.3. Создание, распространение и использование вредоносных компьютерных программ, перенаправляющих потерпевших на ложный IP-адрес (pharming, фарминг).

Осуществляется с помощью вредоносного программного обеспечения, которое «перебрасывает» пользователя с запрошенных интернет-страниц на их мошеннические копии. В случаях с торговосервисными предприятиями по карте пользователя могут быть проведены мошеннические транзакции за не приобретаемые в действительности товары и услуги.

Например, мошенники осуществляют массовую рассылку СМС-сообщений, в которых предлагается скачать музыкальные или иные клипы, либо направляют ложные уведомления, в том числе от имени банков, с предложением установить для повышения уровня защиты своих персональных данных программу с сайта банка, ссылка на который приводится в сообщении. От имени банка жертвам может направляться письмо с указанием подтвердить правильность их реквизитов на специальном веб-сайте в связи с возникшими проблемами технического характера. Также злоумышленники могут сообщить клиенту банка, что он превысил максимально допустимую отсрочку платежа и его счет будет заблокирован, отметив необходимость для получения более подробной информации открыть прикрепленные документы.

2.2.4. Создание двойников сайтов по продаже авиабилетов и железнодорожных билетов, а также двойников сайтов финансовых организаций.

2.2.5. «Обход» используемой большинством банков двухфакторной аутентификации в системах интернет-банкинга с помощью СМС-сообщения.

Мобильное устройство жертвы заражается банковским трояном. После запуска пользователем подлинного банковского приложения на своем смартфоне троян определяет, приложение какого банка используется, и перекрывает его интерфейс своим, показывая пользователю поддельный экран. Внешне поддельное приложение максимально похоже на настоящее. На поддельном экране пользователь вводит свои логин и пароль, а троян отправляет их злоумышленникам, кото-

рые таким образом получают возможность использовать эти данные для входа в банковское приложение. Затем злоумышленники инициализируют перевод денежных средств на свой счет. Системой дистанционного обслуживания на зараженный смартфон пользователя отправляется СМС-сообщение с одноразовым паролем, однако троян перехватывает пароль и пересылает его злоумышленникам. При этом пострадавший не видит СМС-сообщение и ни о чем не подозревает, пока не проверит список транзакций. Используя перехваченный одноразовый пароль, преступники подтверждают транзакцию и получают денежные средства.

2.3. Использование в банкоматах или POS-терминалах накладок и других устройств, копирующих данные магнитной полосы и запоминаящих ПИН-код держателя (skimming, скимминг), в целях подделки карт (создания их копий).

Для реализации этого способа мошенники устанавливают на банкоматы считывающие устройства — скиммеры. На картридер устанавливаются рамки с магнитной головкой, считывающей информацию с магнитной полосы и записывающей электронные копии (дампы) карт на встроенную микросхему памяти. На клавиатуру приклеивается накладка, очень похожая на настоящую клавиатуру, которая запоминает нажатия клавиш и записывает их на встроенную микросхему. Кроме того, на банкомат может быть прикреплена миниатюрная видеокамера, которая сохраняет в модуле памяти либо передает на компьютер мошенника информацию о вводимом ПИН-коде.

Одним из вариантов такого способа считывания данных карты является установка на картридер, используемый для входа в помещение банка (в случае расположения банкоматов в закрытых помещениях, открывающихся посредством считывания карты), скимминговой накладки для считывания информации с карт входящих клиентов, а также ложной клавиатуры или накладки на клавиатуру. Дамп карты записывается на любую карточку с магнитной полосой, которая становится клоном карты пострадавшего и используется для доступа к его денежным средствам вместе с похищенным ПИН-кодом. Если ПИН-код мошенникам неизвестен, покупки совершаются с использованием поддельной банковской карты в магазинах по предварительному сговору с кассиром.

Мошенники нередко пересылают дампы карт для изготовления подделок и обналичивания в другие страны. Это делается с целью усложнения расследования и переноса ответственности за мошенни-

чество на банки, поскольку при отсутствии в паспорте клиента отметки о пересечении границы банк не может возложить вину за несанкционированную операцию на владельца карты.

Скимминг сложный и затратный способ хищения, так как современное оборудование терминалов и банкоматов, как правило, не позволяет устанавливать скимминговые устройства либо оснащено устройствами активного антискимминга.

2.4. Кража или использование утерянных карт.

Одна из технологических разновидностей этого способа мошенничества — траппинг (trapping), т. е. захват карты в картридере с помощью специальных устройств. Мошенник вставляет в картридер терминала кусок пленки, надрезанный таким образом, что карта, попадая в прорезь, не возвращается владельцу, а остается в конверте, который впоследствии извлекается мошенником.

В тот момент, когда карта попадает в ловушку, злоумышленник оказывается рядом с потерпевшим и предлагает ему повторно ввести ПИН-код, мотивируя это тем, что с ним накануне произошла подобная ситуация и данная операция помогла вернуть карту. После дополнительных вводов ПИН-кода карта не возвращается. Мошенник советует жертве обратиться в банк и, после ее ухода, извлекает конверт из банкомата. В итоге у преступника оказывается банковская карта потерпевшего и информация о ПИН-коде.

3. Иные способы хищений и причинения имущественного ущерба посредством использования средств подвижной связи.

3.1. Взимание повышенных сборов за телефонные звонки.

Преступники присваивают обманным путем денежные средства клиентов компаний телефонной связи, совершающих звонки на зарубежные номера, за которые взимается повышенный сбор.

Схема мошенничества состоит в «сброшенных» звонках на номер телефона жертвы. Потерпевший, желая узнать, кто ему звонил, перезванивает по соответствующему номеру телефона, после этого с него взимается повышенный сбор за звонок на платный номер.

К этому способу следует отнести также отправку клиентам компаний телефонной связи текстовых сообщений с незнакомого номера. Если потерпевший отвечает на СМС из любопытства, с него взимается плата за СМС-сообщение по специальному тарифу.

3.2. Мошенничество на платформах бесплатных объявлений.

Схема мошенничества заключается в размещении в сети Интернет бесплатных объявлений о продаже различных видов продукции по цене, которая в несколько раз ниже цены аналогичной продукции на рынке. При этом выставленный на продажу товар не имеет никаких технических или внешних недостатков, а заниженная цена объясняется его собственником срочной потребностью в денежных средствах.

Невозможность связаться с ними через указанные в объявлении контактные данные преступники объясняют тем, что находятся за пределами страны, предлагая альтернативные средства связи: адрес электронного почтового ящика, имена профилей в системах мгновенных сообщений, таких как WhatsApp, Viber, Telegram.

Во время переговоров, которые ведутся посредством альтернативных контактов, преступники под предлогом подтверждения реальности намерений просят покупателя перечислить аванс через различные международные системы денежных переводов. В некоторых случаях мошенники просят совершить такими способами дополнительные платежи, ссылаясь на различные надуманные причины (ремонт выставленного на продажу товара, отсутствие денег на счете мобильного телефона и т. д.). Получив деньги, преступники прекращают любые контакты с жертвой.

3.3. Мошенничество в виде конкурса СМС-сообщений или теста на общие знания.

Как правило, преступники отправляют жертве текстовое сообщение, призывающее ее принять участие в конкурсе на получение ценного приза. Мошенники устанавливают крайне высокие тарифы на сообщения, которые отправляются потерпевшими и получаются ими. Первые вопросы делаются очень легкими, чтобы поощрить потерпевших к продолжению игры, а на последний вопрос или два последних вопроса очень сложно или даже невозможно ответить верно.

4. Использование информационных технологий для совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров.

Компьютерные сети и телекоммуникационные технологии весьма широко используются в сфере незаконного оборота наркотических средств.

Организованные группы наркоторговцев все чаще прибегают к бесконтактным способам сбыта наркотиков, широко используя при этом средства мобильной связи, интернет-ресурсы, электронные платежные системы.

Одной из тенденций последнего времени стала активизация нелегального производства синтетических наркотиков на территории стран Содружества Независимых Государств, что определяется их доступностью по цене и способу приобретения, в том числе через сеть Интернет.

Основным способом распространения наркотиков является бесконтактный сбыт путем организации тайников-закладок и перевода денежных средств, включая криптовалюту, через различные платежные системы. С целью увеличения числа потребителей участники наркобизнеса все активнее используют сеть Интернет не только для рекламы наркотических средств и психотропных веществ, но и для анонимного осуществления оперативного поиска продавцов и покупателей, организации так называемого регионального маркетинга.

Организаторы торговли наркотиками активно используют ресурсы «темной сети» (DarkNet), или «глубокой паутины» (DeepWeb), которая обеспечивает анонимность, так как закрыта от поисковиков и отслеживания. Попасть в DarkNet можно через один из прокси-серверов, самый популярный из которых — сеть Tor (The Onion Router) и ее браузер (Tor Browser). Сайты сети Tor имеют доменное имя первого уровня onion.

Сайты наркоторговцев устроены по принципу обычных интернет-магазинов — в них можно оформить заказ, почитать отзывы и описание, поделиться мнением о качестве продукта и сервиса, связаться со службой поддержки. Оплата покупок возможна любыми способами: банковскими картами, через интернет-кошельки, криптовалютой (например, биткоинами).

DarkNet также используется организаторами и подстрекателями создания преступных групп для так называемого трудоустройства, в том числе вовлечения в свою деятельность «кладменов», которые делают закладки наркотиков, «гроверов», которые выращивают траву, химиков, которые производят ЛСД и экстази, курьеров, которые перевозят товар, «дропов», которые снимают деньги, трафаретчиков, которые пишут объявления на асфальте и заборах.

5. Использование информационных технологий с целью совершения преступлений против половой неприкосновенности несовершеннолетних, а также преступлений против здоровья населения и общественной нравственности.

С развитием научно-технического прогресса сеть Интернет становится все более популярной среди детей и подростков. Растет количество времени, проводимого в ней несовершеннолетними. Одно из наиболее востребованных направлений использования Интернета — социальные сети, которые дают несовершеннолетним возможность общаться и обмениваться информацией с друзьями.

5.1. Преступления против половой неприкосновенности несовершеннолетних.

Находясь в виртуальном пространстве, дети и подростки неизбежно сталкиваются с комплексом киберугроз, среди которых одной из наиболее опасных выступает угроза стать жертвой преступления против половой неприкосновенности, так как преступники, используя информационные технологии, получают возможность дистанционно связываться с несовершеннолетними, осуществлять в их отношении развратные действия.

Для обозначения действий совершеннолетнего лица, направленных на установление в Интернете доверительного контакта с ребенком с целью склонить его к вступлению в сексуальную связь, используется термин «кибергруминг», или «онлайн груминг».

Термин «груминг» происходит от английского слова grooming — уход, забота. Суть этого метода — создание у несовершеннолетнего ощущения, что о нем заботятся, им искренне интересуются, чтобы способствовать возникновению психологической связи, завоевать доверие ребенка или подростка на основе его интересов. Этим понятием охватываются как действия, преследующие цель получения лицом, страдающим расстройством сексуального предпочтения (педофилией), сексуального удовлетворения, так и действия, направленные на вовлечение ребенка в коммерческую сексуальную эксплуатацию.

Типичный механизм кибергруминга заключается в том, что злоумышленник общается в сети Интернет с ребенком, выдавая себя за ровесника либо ребенка немного старше, знакомится в чате, на форуме или в социальной сети с жертвой, пытается установить с ней дружеские отношения и перейти на личную переписку. Основные спосо-

бы совершения преступлений против половой неприкосновенности и половой свободы несовершеннолетних:

1) участие в организации производства порнографической продукции (фото- и видеосъемка);

2) сбор из различных источников и распространение чужих «произведений»;

3) размещение на своих информационных ресурсах в сети Интернет ссылок на сайты, содержащие порнографические изображения несовершеннолетних (рекламирование).

5.2. Основные способы склонения несовершеннолетних к совершению самоубийства.

Несмотря на успешное противодействие преступной деятельности лиц, занимавшихся склонением несовершеннолетних к самоубийствам, возникновение в сети Интернет «групп смерти» обладает высоким потенциалом опасности.

Выделяются следующие формы (способы) сетевого склонения к самоубийству:

1) размещение на информационном ресурсе сведений о способах совершения самоубийства;

2) размещение мультимедийных материалов (фото-, видео- и аудиоконтента, простых и креолизованных текстов);

3) онлайн-переписка.

Вербовщики в «группы смерти» действуют в социальных сетях. После того как ребенок вступает в игру, кураторы подключают его к мессенджерам, позволяющим распространять мгновенные анонимные сообщения. В результате происходит активное влияние на несовершеннолетнего с целью склонения его к самоубийству.

6. Использование информационных технологий для совершения преступлений террористического и экстремистского характера.

Роль сети Интернет в расширении пропаганды терроризма в наши дни очень велика. Информационные сети и сервисы являются удобным, эффективным средством и одновременно средой распространения экстремистской идеологии.

Одной из разновидностей терроризма является кибертерроризм, для которого свойственно использование преступниками в качестве средств достижения своих целей информационных технологий, спе-

циального программного обеспечения, предназначенного для несанкционированного проникновения в компьютерные системы.

Способы совершения кибертеррористических преступлений с учетом доктринальных позиций можно классифицировать следующим образом:

1) несанкционированное проникновение в атакуемую сеть или перехват управления сетью путем взлома, в том числе через подбор либо хищение идентификационных данных, позволяющих войти в систему (повысить пользовательские привилегии);

2) применение программного кода или последовательности команд, находящихся и использующих уязвимости в программном обеспечении;

3) распространение компьютерных вирусов, которые модифицируют и уничтожают информацию или блокируют работу вычислительных систем;

4) введение в программу вирусов — логических бомб, программ, которые запускаются (срабатывают) при определенных условиях (временных или информационных) для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных);

5) использование «троянских коней», выполняющих передачу информации на удаленные компьютеры либо иные вредоносные действия без ведома владельца зараженной системы;

6) применение средств нарушения и подавления информационного обмена в сетях (в частности, нарушение функционирования серверов и сайтов путем применения DoS/DDoS-атак).

7. Поиск уязвимостей программного обеспечения в целях продажи третьим лицам и иные компьютерные преступления.

Вышеописанные способы кибернападений террористической направленности свойственны атакам, совершаемым для демонстрации возможностей организованных преступных групп и хакеров-одиночек в целях поиска заказчиков (работодателей).

Существуют сервисы по поиску определенных уязвимостей в корпоративных сетях с последующей их продажей третьим лицам. Ведутся активные исследования программного обеспечения и сервисов операционных систем для выявления «угроз нулевого дня» — ошибок в программном обеспечении, приводящих к повышению

пользовательских привилегий, о которых неизвестно даже разработчику.

Происхождение термина «угроза нулевого дня» связано с тем обстоятельством, что об уязвимости программного обеспечения или атаке на него становится известно до момента выпуска производителем программного обеспечения, позволяющего исправить ошибки (т. е. уязвимость может быть использована на работающих копиях приложения без возможности защиты от нее).

«Угрозы нулевого дня» влекут за собой появление новых способов распространения вредоносного кода, что активно используется киберпреступниками для создания эффективного механизма заражения через программные продукты массового использования. Эксплуатация данных уязвимостей осуществляется через так называемые связки эксплойтов, реализующие удаленный доступ к операционной системе с последующей загрузкой вредоносного программного обеспечения.

Значительная часть «угроз нулевого дня» — это критические уязвимости, т.е. бреши, позволяющие злоумышленнику, имеющему готовый хакерский эксплойт, получить полный контроль над системой при условии отсутствия доступных исправлений программного обеспечения и антивирусных сигнатур. Обеспечение информационной безопасности особенно осложняет игнорирование пользователями необходимости установки исправлений даже после их выпуска, в особенности для программного обеспечения, не входящего в состав операционной системы.

Противодействие использованию информационных сетей преступными группами, специализирующимися на вымогательстве, мошенничестве, кражах, совершении преступлений в сфере компьютерной информации, а также защита важнейших информационных инфраструктур от кибератак имеют ключевое значение для внешней и внутренней безопасности как отдельных государств, так и СНГ в целом.

Решение этой задачи предполагает совместную работу правоохранительных и иных государственных органов, выстраивание сотрудничества и обмена информацией на национальном и межгосударственном уровне, а также разработку и реализацию комплекса нормативно-правовых и организационных мер по противодействию деятельности террористических и других преступных организаций и сообществ. Продолжая исследование механизма совершения пре-

ступлений с использованием компьютерных и телекоммуникационных технологий, углублённый анализ позволяет систематизировать и расширить существующую типологию, выявив новые векторы киберугроз и детализировав правовые аспекты квалификации.

1. Расширенная типология способов совершения киберпреступлений (продолжение)

1.1. Вишинг (Vishing) и фишинг (Phishing) с использованием методов социальной инженерии.

Эти способы мошенничества направлены на психологическое манипулирование жертвой с целью получения конфиденциальных данных.

Углубленный механизм вишинга: Злоумышленники осуществляют массовые звонки с использованием IP-телефонии, что позволяет подменять номер абонента и выводить на экране жертвы номер, похожий на официальный номер банка или государственного органа. В ходе разговора, представляясь сотрудником службы безопасности банка, они сообщают о подозрительных операциях или блокировке счета, создавая у жертвы чувство паники. Для «разблокировки» или «защиты средств» жертву убеждают сообщить реквизиты карты (номер, срок действия, CVV/CVC-код) или одноразовые SMS-коды, либо под предлогом «проверки» побуждают установить программу удаленного доступа (например, AnyDesk, TeamViewer), маскирующуюся под мобильное приложение банка. Получив доступ к устройству, преступники получают полный контроль над банковскими аккаунтами жертвы.

Современные фишинговые схемы: Распространена рассылка писем и сообщений в мессенджерах, имитирующих коммуникацию от известных брендов (например, онлайн-маркетплейсов, служб доставки). В сообщении содержится ссылка на фишинговый сайт – точную копию официального, где пользователь, введя свои учетные данные и реквизиты карты, добровольно передает их злоумышленникам. Примером является схема обмана на площадках объявлений, когда мошенник, притворяясь покупателем или продавцом, высылает продавцу или покупателю ссылку на поддельную страницу, имитирующую сервис доставки или интернет-банкинг, для ввода данных карты под видом получения оплаты или оформления доставки.

1.2. Вымогательство с использованием вредоносного программного обеспечения (Ransomware).

Данный способ относится к наиболее разрушительным и финансово опасным киберпреступлениям.

Механизм работы программ-вымогателей: В систему жертвы проникает специальное вредоносное ПО – ransomware. Оно подразделяется на два основных типа: шифровальщики (cryptoransomware), которые с использованием стойких алгоритмов шифруют ценные файлы пользователя (документы, базы данных, фотографии), и блокировщики (blockers), которые блокируют доступ к операционной системе. После этого злоумышленники предъявляют требование о выплате выкупа (как правило, в криптовалюте) за восстановление доступа к данным или системе.

Способы доставки: Основными каналами проникновения являются фишинговые письма с вредоносными вложениями, эксплуатация уязвимостей в программном обеспечении, а также использование скомпрометированных учетных записей для удаленного развертывания вредоносного ПО в корпоративных сетях.

1.3. Использование информационных технологий для совершения иных преступлений.

Наркоторговля и DarkNet: Организованные преступные группы активно используют ресурсы «темной сети» (DarkNet), доступ к которым обеспечивается с помощью специального ПО, например, браузера Tor. В DarkNet действуют анонимные онлайн-маркеты, по структуре напоминающие обычные интернет-магазины, где осуществляется торговля наркотиками и иными запрещенными товарами. Оплата часто происходит с использованием криптовалют, а доставка организуется бесконтактным методом – через систему тайников-«закладок».

Кибергруминг: Преступники используют социальные сети, мессенджеры и онлайн-игры для установления доверительного контакта с несовершеннолетними, часто выдавая себя за сверстников. Целью является последующее склонение ребенка к сексуальным действиям, шантажу или производству порнографических материалов. Этот метод, известный как «груминг», основан на глубоком психологическом манипулировании.

Распространение запрещенного контента: Сети используются для незаконного оборота порнографических материалов, в том числе с участием несовершеннолетних. Действия злоумышленников могут квалифицироваться как распространение, публичная демонстрация или рекламирование таких материалов. Под распространением, согласно судебной практике, понимается не только размещение на об-

щих ресурсах, но и направление материалов конкретному лицу в личном сообщении (по электронной почте, в мессенджерах).

2. Правовые аспекты квалификации и проблемы расследования

2.1. Квалификация преступлений, совершенных с использованием сетей.

Согласно разъяснениям Верховного Суда РФ, преступление признается совершенным с использованием информационно-телекоммуникационных сетей, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения преступления или входящих в его объективную сторону, лицо использовало такие сети. Это включает в себя подбор соучастников, размещение информации для сбыта наркотиков или планирование преступной деятельности.

Определение места совершения преступления: Установление территориальной подсудности является одной из ключевых проблем. Местом совершения такого преступления считается территория, на которой лицо использовало компьютерное устройство для совершения действий, входящих в объективную сторону состава преступления (например, разместило противоправную информацию в интернете), независимо от места наступления последствий.

Умышленный характер деяний: Для квалификации необходимо установить, что лицо действовало умышленно, осознавало характер распространяемой информации и общественную опасность своих действий.

2.2. Проблемы международного сотрудничества.

Интернет-преступления по своей природе носят трансграничный характер, когда преступник, сервер и жертва могут находиться в разных юрисдикциях. Это порождает сложности:

- отсутствие единых правовых стандартов — деяние должно быть криминализировано как в стране, где ведется расследование, так и в стране, где находится обвиняемый (принцип двойной криминальности);

- сложность определения юрисдикции — возникают вопросы, территорию какой страны считать местом совершения преступления: местонахождение сервера, место деятельности преступника или место наступления последствий;

- скорость и объемы взаимодействия — запросы правоохранительных органов о правовой помощи часто требуют длительного вре-

мени для исполнения, в то время как цифровые доказательства могут быть быстро уничтожены.

3. Совершенствование механизма противодействия.

Для эффективного противодействия описанным угрозам необходим комплексный подход:

3.1. Развитие законодательства. Требуется дальнейшая детализация и унификация составов преступлений, а также включение использования ИТ в качестве универсального квалифицирующего признака в составы традиционных преступлений, где это резко повышает общественную опасность.

3.2. Техническое оснащение правоохранительных органов. Необходимо внедрение передовых систем мониторинга сетевого трафика, анализа больших данных и средств криминалистического анализа цифровых устройств.

3.3. Усиление международного сотрудничества. Развитие механизмов оперативного взаимодействия в рамках международных организаций (Интерпол, Европол) и на двусторонней основе для быстрого обмена информацией и выполнения следственных поручений.

3.4. Повышение цифровой грамотности населения. Просветительская работа, информирующая граждан о распространенных схемах мошенничества и правилах кибербезопасности, является ключевым элементом профилактики.

Механизм совершения преступлений с использованием компьютерных и телекоммуникационных технологий продолжает стремительно эволюционировать, приобретая все более изощренные и транснациональные формы. Адекватный ответ на этот вызов требует от правоохранительной системы и общества в целом не только технической оснащенности, но и гибкости правового регулирования, а также глубокого понимания социотехнической природы современных киберугроз.

Глава 5. ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Криминалистическая характеристика преступлений в сфере компьютерной информации — это совокупность обобщенной криминалистически значимой информации о системе взаимодействующих и взаимозависимых элементов, образующих типовую картину события преступления, служащей для решения непосредственных задач раскрытия и расследования этих преступлений¹.

Для преступлений в сфере компьютерной информации характерна следующая структура элементного состава криминалистической характеристики:

- предмет и объект преступления;
- обстановка совершения преступления;
- способ совершения преступления;
- лица, потерпевшие от преступления; личность преступника и его профессиональные навыки.

Изучим подробнее элементы, входящие в состав криминалистической характеристики преступлений рассматриваемого вида.

Предметом по данному виду преступлений является компьютерная информация, представляющая собой машинный код, вводимый и (или) выводимый микропроцессорным изделием. Такой код состоит из системы команд, которую задает пользователь (человек) при помощи языка программирования (рис. 1²). В настоящее время сложно ответить, сколько языков программирования существует. Так, одних только диалектов BASIC более трехсот, а языков программирования всего насчитывается более восьми тысяч.

Кроме того, машинный код хранится на оперативном запоминающем устройстве (рис.2³) и постоянном запоминающем устройстве

¹ См., напр.: Белоусов А. В. Особенности расследования краж, совершаемых на железнодорожном транспорте из одежды, сумки или другой ручной клади, находившихся при потерпевшем: монография / под ред. Е. В. Смахина. – Тюмень, 2014. С. 14.

² Рисунок взят из: URL: <https://cf2.ppt-online.org/files2/slide/v/v1LjYlue4qSdwhJnNQZrazfAKW7BPG56boX302/slide-13.jpg> (дата обращения: 02.10.2023).

³ Рисунок взят из: URL: <https://ds03.infourok.ru/uploads/ex/0e1b/000405ba852d8332/4/img2.jpg> (дата обращения: 02.10.2023).

(ПЗУ) (рис. 3¹) компьютерно-телекоммуникационного технического средства (КТТС).

Микропроцессорное изделие состоит из одного или нескольких изделий (рис. 4²), главным образом содержит в себе микропроцессор (рис. 5³) и (или) микроконтроллер (рис. 6⁴). В последующем машинный код представляется пользователю в привычной для восприятия форме (например, текст, картинка, 3D-модели и т. п.) при помощи различных устройств (например, монитор, проектор, принтер и т. п.).

Машинный код и язык ассемблера

```
00 61      LD 1
01 62      LD 2
02 10      ADD
03 53 06   GT A
05 18      SGN
06 41      A: ST 1
07 50      STOP
```



Рис. 1 Машинный код и Код и язык ассемблера

Рис. 2 Оперативные запоминающие устройства

Рис. 3 Постоянные запоминающие устройства



Рис. 4 Микропроцессорное устройство



Рис. 5 Микропроцессор



Рис. 6 Микроконтроллер

¹ URL: <https://cf2.ppt-online.org/files2/slide/a/Anz8fvMT420DjHt76Rx3klhbYpsauEcrN5igOKJZG/slide-6.jpg> (дата обращения: 02.10.2023).

² URL: <https://clearpc.pl/wp-content/uploads/2016/12/modding.jpg> (дата обращения: 02.10.2023).

³ URL: https://img.tehnomaks.ru/img/prod/full/1534912987_2.jpg (дата обращения: 02.10.2023).

⁴ URL: https://www.gme.cz/data/product/1024_1024/pctdetail.958-104.1.jpg (дата обращения: 02.10.2023).

Таким образом, преступник неправомерным способом получает доступ и воздействует по данному виду преступления на машинный код, а уже весь массив кода представляет из себя компьютерную информацию (картинка, документ, программа и т. п.), который не только содержит цифровое выражение, но и может содержать авторские права, коммерческую или государственную тайну.

В результате воздействия преступника на компьютерную информацию возникают общественные отношения, образующие объект преступления. Значение для криминалистики имеет следующая информация, условно включенная нами в объект:

- *персональные данные*, к которым относятся:
 - фамилия, имя, отчество (ФИО), дата и место рождения, гражданство;
 - прежние ФИО, дата, место и причина изменения (в случае изменения);
 - образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
 - выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т. п.);
 - места рождения, работы и домашние адреса близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
 - фамилии, имена, отчества, даты рождения, места рождения, работы и домашние адреса бывших мужей (жен);
 - паспорт (серия, номер, кем и когда выдан);
 - номер телефона;
 - отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
 - идентификационный номер налогоплательщика;
 - номер страхового свидетельства обязательного пенсионного страхования;
 - наличие (отсутствие) судимости;
 - допуск к государственной тайне, оформленный за период работы, службы, учебы (форма, номер и дата);

– результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;

– сведения о доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов семьи¹;

– *авторские, смежные, изобретательские и патентные права, а также незаконное использование товарного знака.* К указанным объектам относятся как обнародованные, так и необнародованные произведения науки, литературы и искусства, являющиеся результатом творческой деятельности и существующие в какой-либо объективной форме (письменной, устной, звуко- или видеозаписи, изобразительной, объемно-пространственной)²;

– *коммерческая тайна*, к которой относятся сведения любого характера (производственные, технические, экономические, организационные и др.), в т. ч. о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны³;

– *государственная тайна*, к которой относятся защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации⁴.

Следующим элементом криминалистической характеристики является обстановка совершения преступления. Проведя теоретический анализ этого понятия, можно сделать вывод о том, что под ней понимается система, ограниченная рамками отдельного преступного события. Входящие в ее состав элементы несут определенную кри-

¹ Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 24.04.2020) «О персональных данных».

² Постановление Пленума ВС РФ от 26.04.2007 № 14 «О практике рассмотрения судами уголовных дел о нарушении авторских, смежных, изобретательских и патентных прав, а также о незаконном использовании товарного знака».

³ Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

⁴ Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».

миналистическую нагрузку и могут быть использованы в расследовании преступления¹.

Говоря об особенностях обстановки совершаемого вида преступлений, необходимо учитывать следующие обстоятельства:

- противоправные действия могут быть начаты в одной стране, а наступление последствий произойти в другой;
- разные часовые пояса обуславливают возникновение сложностей, связанных с точным определением времени совершения преступления;
- условия, способствующие совершению преступления, будут зависеть от степени защищенности КТТС от несанкционированного доступа и воздействия на компьютерную информацию, а именно: какая, например, антивирусная программа использовалась при защите компьютерной информации во время совершенного преступления.

Представляется правильной позиция М. М. Менжега об обстановке совершения преступления рассматриваемого вида. Он считает, что преступление может совершаться в любом месте, где функционирует КТТС. При этом существенным фактором, влияющим на обстановку, является отсутствие, либо низкий уровень защиты компьютерной информации, например, на объекте юридического лица, от несанкционированного доступа и воздействия на компьютерную информацию².

Рассматривая структуру способа совершения преступлений, отметим, что подготовка и сокрытие преступления входят в структуру способа совершения преступления, если только эти элементы способа изначально охватывалось преступным умыслом виновного и не требуют дополнительной квалификации. Если же действия по подготовке и сокрытию не были охвачены преступным умыслом, то они должны оцениваться самостоятельно³.

¹ Белоусов А. В., Смахтин Е. В. Специфика обстановки краж, совершаемых на железнодорожном транспорте из одежды, сумки или другой ручной клади, находившихся при потерпевшем // Вестник Тюменского гос. ун-та. 2012. № 3. С. 180–181.

² Менжега М. М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ...канд. юрид. наук: 12.00.09. – Саратов, 2005. С. 32–33.

³ Карагодин В. Н. Криминалистическое понятие способа сокрытия преступления // Проблемы развития криминалистики в условиях научно-технического прогресса: межвуз. сб. науч. тр. Свердловск, 1982. С. 109; Беляков А. А. Кри-

Рассмотрим особенности полноструктурного способа совершения компьютерного преступления.

Способы подготовки:

- определение компьютерной информации для неправомерного доступа или воздействия;
- подбор пароля или электронного ключа при помощи компьютерной программы;
- поиск и изучение соответствующей документации системного обеспечения КТТС;
- определение назначения (изменить, заблокировать или удалить компьютерную информацию) вредоносной компьютерной программы;
- определение языка программирования при создании вредоносной компьютерной программы;
- определение способа распространения (удаленно или непосредственно) вредоносной компьютерной программы.

Способы совершения:

- преступные действия, связанные с доступом к компьютерной информации;
- преступные действия, связанные с воздействием на компьютерную информацию;
- преступные действия, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- преступные действия, связанные с созданием, использованием и распространением вредоносных компьютерных программ.

Перечисленные выше преступные действия совершаются, как правило, удаленно, через Wi-Fi или Bluetooth-каналы связи, непосредственно через использование КТТС путем копирования, изменения, блокирования или удаления машинного кода.

Способы сокрытия:

- неправомерный доступ и воздействие на компьютерную информацию под чужим паролем, электронным ключом;
- использование чужого MAC- или IP-адреса;

миналистическая характеристика и особенности расследования краж, совершаемых лицами без определенного места жительства и работы: дис. ...канд. юрид. наук. Свердловск, 1986. С. 35.

– маскировка или внедрение вредоносной компьютерной программы в лицензионное системное обеспечение КТТС.

При изложении вопросов о личности преступника и потерпевшего важно, что их показания с позиций криминалистики иногда именуются идеальными следами. Наиболее точно это определил Л. Б. Филонов, который писал, что «все следы можно восстановить, оживить и зафиксировать, но это следы особого рода. С такими следами можно работать так же, как работают со всеми латентными следами, только здесь нужен особый "проявитель"; для того чтобы они стали отчетливыми, нужны особые средства и особые способы работы с личностью, которая может раскрыть эти следы»¹.

По рассматриваемому виду преступления в соответствии со ст. 42 УПК РФ потерпевшими лицами будут:

– физическое лицо — граждане Российской Федерации, иностранные граждане или лица без гражданства, а также граждане, имеющие правовой статус индивидуального предпринимателя (ИП) или самозанятые;

– юридическое лицо — государственные и муниципальные предприятия; фонды; учреждения; автономные НКО; религиозные организации; публично-правовые компании; полное товарищество; товарищество на вере; крестьянское (фермерское) хозяйство; общество с ограниченной ответственностью (ООО); акционерное общество (АО); производственный кооператив; хозяйственное партнерство; потребительский кооператив; общественные организации граждан; общественные движения; ассоциации и союзы; товарищества собственников недвижимости; казачьи общества, внесенные в государственный реестр казачьих обществ в Российской Федерации; общины коренных малочисленных народов Российской Федерации; адвокатские палаты; адвокатские образования, являющиеся юридическими лицами.

Личность преступника, совершающего действия в сфере компьютерной информации. Его профессиональные навыки имеют существенное значение для криминалистической характеристики.

Так, по данным М. Вершинина, большая часть компьютерных преступлений совершается мужчинами в возрасте от 18 до 40 лет, обладающими глубокими или профессиональными знаниями в обла-

¹ Филонов Л. Б. Психологические способы выявления скрываемого обстоятельства. – М., 1979. С. 4.

сти IT-технологий. Кроме того, они совершаются группами лиц по предварительному сговору или так называемыми «хакерскими движениями»¹.

Обобщение профессиональных навыков преступников условно позволяет выделить следующие разновидности:

- неквалифицированный пользователь стационарного или мобильного КТТС. К данным пользователям относятся лица, не обладающие специальными познаниями в области системного обеспечения и функционирования КТТС;

- квалифицированный пользователь стационарного или мобильного КТТС. Это лицо, получившее квалификацию, например, в области IT-технологий (инженер или IT-специалист), имеющее диплом о высшем или среднем специальном образовании.

1. Типичные следственные ситуации и версии, выдвигаемые в процессе расследования преступлений в сфере компьютерной информации.

Возникновению следственных ситуаций, как показывает практика расследования рассматриваемого вида преступлений в большинстве случаев, предшествует поступление информации о совершении неустановленным лицом преступления. Из всей информации, содержащейся в материалах проверки, на стадии возбуждения уголовного дела формируется следственная ситуация.

Рассмотрим более подробно неблагоприятные типичные следственные ситуации, которые представляют наибольшую сложность в расследовании.

Ситуация № 1. Неустановленным лицом совершен неправомерный доступ и воздействие на компьютерную информацию.

Так, например, из материалов уголовного дела № 1-405/2012 следует, что А. совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование, кроме того, совершил незаконное разглашение сведений, составляющих коммерческую тайну без согласия их владельца лицом, которому она

¹ Вершинин М. Современные молодежные субкультуры: хакеры. URL: <http://yurpsy.com/files/xrest/2/222.htm> (дата обращения: 30.09.2023).

была доверена по работе. Указанные действия совершил из корыстной заинтересованности¹.

Ситуация № 2. Неустановленным лицом нарушены правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Так, например, из материалов уголовного дела № 1-149/2019 следует, что лица № 1, № 2 и № 3, являясь работниками Института теоретической и математической физики (ИТМФ), действуя умышленно, из корыстной заинтересованности, обладая специальными познаниями в сфере компьютерной техники, заведомо зная о действующих в ФГУП «РФЯЦ-ВНИИЭФ» правилах доступа к охраняемой законом компьютерной информации, договорились об использовании вычислительных мощностей находящегося в ИТМФ неиспользуемого компьютерного оборудования и возможностей системы локальных вычислительных сетей (СЛВС) для вычисления (майнинга) криптовалюты и ее последующего обращения в свою пользу, вопреки служебным интересам ФГУП «РФЯЦ-ВНИИЭФ».

Таким образом, нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации, совершенное лицами № 1, № 2 и № 3, повлекло причинение ФГУП «РФЯЦ-ВНИИЭФ» крупного материального ущерба, составляющего 1 140 157 рублей 10 копеек².

Ситуация № 3. Неустановленным лицом создана, использована и распространена вредоносная компьютерная программа.

Так, например, из материалов уголовного дела № 1-326/2017 следует, что С. из корыстной заинтересованности создавал и распространял компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, копирования, модификации

¹ Приговор Орджоникидзевского районного суда г. Екатеринбурга № 1-405/2012 1-405/2017 от 25.07.2017 по уголовному делу № 1-405/2012 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/9NiHUPYjCWw/?regular-txt> (дата обращения: 02.10.2023).

² Приговор Саровского городского суда Нижегородской области № 1-149/2019 от 17.09.2019 по уголовному делу № 1-149/2019 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/VkskjgQYZaHT/?regular-txt> (дата обращения: 02.10.2023).

компьютерной информации и нейтрализации средств защиты компьютерной информации¹.

Как видим, основной информационный компонент рассматриваемых типичных ситуаций — это отсутствие сведений о лице, совершившем компьютерное преступление. В зависимости от квалификации действий неустановленного преступника, следователь выдвигает следующие типичные версии о лице (лицах), причастном к совершению преступления в сфере компьютерной информации. Очевидно, что основным подозреваемым будет являться лицо — пользователь компьютера, с которого совершено преступление. Однако это могут быть и другие лица. Например:

- преступление может быть совершено кем-либо из родственников, друзей, знакомых, имеющих удаленный или прямой доступ к КТТС, с которого совершено компьютерное преступление;
- преступление совершено лицом, работающим в настоящее время в организации либо ранее работавшим и уволенным в настоящее время;
- преступление совершено посторонним лицом, которое воспользовалось компьютером юридического лица для совершения преступления;
- к совершению преступления причастно лицо, ранее судимое за аналогичные преступления;
- к совершению преступления причастны недобросовестные конкуренты юридического лица;
- произошел непреднамеренный технический сбой в работе КТТС, т. е. компьютерного преступления не было.

В рассматриваемых следственных ситуациях при проверке выдвинутых версий в ходе производства проверочных действий и оперативно-розыскных мероприятий осуществляется следующая программа (алгоритм) действий, включающая в себя:

На этапе проверки сообщения о преступлении:

- получают объяснения от заявителя (например, представителя юридического лица и очевидцев) о произошедшем событии;

¹ Приговор Калининского районного суда г. Челябинска № 1-326/2017 от 04.07.2017 по уголовному делу № 1-326/2017 // Судебные и нормативные акты РФ. URL: <https://sudact.ru/regular/doc/y6SVe82Q1ZHr/?regular-txt> (дата обращения: 02.10.2023).

– проводится осмотр места происшествия с целью обнаружения, фиксации и изъятия следов, таких как:

неправомерный доступ и воздействие на компьютерную информацию;

нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

создание, использование и распространение вредоносных компьютерных программ (например, червь, троян, spyware, adware, keylogger, ботнет, руткит, баннеры-вымогатели, фишинг, спам и т. п.);

– проводится осмотр изъятых КТТС, их компонентов или системного обеспечения на предмет обнаружения следов преступления, ранее не обнаруженных в ходе осмотра места происшествия;

– запрашиваются сведения из информационно-справочных учетов правоохранительных органов (например, оперативно-розыскные, криминалистические и др.), от провайдеров предоставления услуги доступа к сети Интернет и иным связям, а также документы (например, должностные инструкции, документы финансовой отчетности, локальные акты, регулирующие правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и т. п.);

– проводятся оперативно-розыскные мероприятия:

наведение справок;

сбор образцов для сравнительного исследования;

проверочная закупка;

исследование предметов и документов;

наблюдение;

отождествление личности;

обследование помещений, зданий, сооружений, участков местности и транспортных средств;

контроль почтовых отправлений, телеграфных и иных сообщений;

прослушивание телефонных переговоров;

снятие информации с технических каналов связи;

оперативное внедрение;

оперативный эксперимент.

В ходе проведения оперативно-розыскных мероприятий могут быть получены сведения:

о лице, совершившем неправомерный доступ и воздействие на компьютерную информацию и его местонахождении;

месте осуществления неправомерного доступа и воздействия на компьютерную информацию;

месте сокрытия объектов, содержащих вредоносную компьютерную программу;

месте хранения цифровых носителей информации; подвергшихся неправомерному доступу и воздействию вредоносной компьютерной программой;

месте хранения записных книжек или черновиков, содержащих пароли, электронные ключи для преодоления средств защиты от неправомерного доступа к компьютерной информации;

сведения о способе и средствах, используемых для неправомерного доступа и воздействия на компьютерную информацию;

– проводится ревизия (например, с целью выявления действий по использованию вредоносных компьютерных программ для снижения или неуплаты налогов).

В ходе предварительного расследования:

допрос потерпевшего; допрос свидетелей; поручения о производстве следственных действий (оперативно-розыскных мероприятий);

международные поручения;

опознание (опознание по фотографии);

дополнительный осмотр места происшествия;

производство судебной экспертизы;

осмотр и приобщение к уголовному делу вещественных доказательств;

выемка;

обыск;

задержание;

истребование и осмотр документов, удостоверяющих личность преступника;

допрос подозреваемого;

проверка показаний на месте;

очная ставка;

следственный эксперимент;

допрос обвиняемого;

допрос специалиста, эксперта;

дополнительные допросы потерпевшего, свидетелей.

Представленный алгоритм (краткая программа) действий следователя позволяет повысить эффективность расследования рассматриваемого вида преступлений.

2. Организационные и тактические решения при производстве отдельных следственных действий в процессе расследования преступлений в сфере компьютерной информации

Организации и тактике проведения следственных действий по рассматриваемому виду преступлений в криминалистической литературе уделено достаточное внимание. Так, организационные и тактические решения по производству отдельных следственных действий обусловлены тактическими и процессуальными особенностями доказывания различных обстоятельств совершения преступления. Рассмотрим некоторые из них.

Допрос является одним из наиболее распространенных следственных действий. При его проведении необходимо руководствоваться общими тактическими правилами, которые подробно изложены в криминалистической литературе. После принятия решения о проведении данного следственного действия следователь на подготовительном этапе:

1. Осуществляет сбор информации о допрашиваемом лице. Источниками будут выступать: материалы проверки сообщения о преступлении, например, из объяснений, характеристик (с места учебы, работы или по месту жительства), информационно-справочных учетов правоохранительных органов; глобальной сети (Интернет), например, в мессенджере (Skype, iMessage, Viber, Line, WhatsApp, Threema, Confide, Telegram, Wickr, Signal), социальной сети («Одноклассники.ru», «ВК», Facebook, YouTube), форумах сайтов.

2. Выбирает время, место и способ вызова лица на допрос.

3. В необходимых случаях изучает специальную литературу, проводит консультации со специалистом.

4. Обеспечивает присутствие специалиста и (или) иных участников уголовного судопроизводства.

5. Подготавливает материально-техническое обеспечение, например, компьютерную технику, аудио- или видеосредства записи.

6. Определяет план проведения допроса, который при необходимости составляется письменно.

Представленный выше перечень подготовительных мероприятий не является исчерпывающим, но будет основным на первоначальном этапе расследования рассматриваемого вида преступлений.

Начинать допрос следует со свободного рассказа: исследования психологов показывают, например, что количество ошибок меньше в свободном рассказе, чем в ответах на конкретные вопросы¹. Планируя стадию свободного рассказа, следователь должен помнить, что допрашиваемые не всегда могут давать показания в свободной форме.

Выслушав свободный рассказ и определившись с индивидуальным подходом к допрашиваемому, следователь переходит к постановке дополняющих или уточняющих вопросов, которые способствуют выявлению неизвестных фактов и помогают наиболее полно воссоздать картину события преступления.

При допросе потерпевшего следователю необходимо акцентировать внимание на следующих вопросах:

1. Физического лица:

- время неправомерного доступа или воздействия на компьютерную информацию;
- место неправомерного доступа или воздействия на компьютерную информацию;
- место нахождения потерпевшего в момент совершения преступления;
- какие КТТС использовались;
- какими знаниями обладает допрашиваемый о компьютерно-телекоммуникационной технике;
- навыки работы на КТТС;
- владеет ли допрашиваемый языками программирования;
- какие используются средства защиты от несанкционированного доступа;
- с каким провайдером заключен договор на услуги доступа к сети Интернет и иные связанные с Интернетом услуги;
- из каких источников информации допрашиваемое лицо узнало о совершенном преступлении;
- подозревает ли кого в совершении преступления, в какой форме осуществлялась взаимосвязь;

¹ Еникеев М. И. Основы общей и юридической психологии: учебник. М.: Юрист, 1996. С. 139.

- сможет ли опознать лицо, совершившее преступление, по каким признакам;

- какая компьютерная информация подверглась неправомерному доступу и (или) воздействию;

- размер причиненного ущерба.

2. Представителя юридического лица:

- время и место неправомерного доступа или воздействия на компьютерную информацию;

- вид деятельности и организационно-правовая форма юридического лица;

- график работы юридического лица;

- наличие охраны объектов юридического лица, виды и средства охраны;

- правовое обеспечение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

- отмечались ли ранее сбои в работе КТТС;

- лицензионное или нелицензионное ПО используется;

- содержание и объем компьютерной информации, которая была подвержена незаконному доступу и воздействию;

- кто из персонала юридического лица или родственников имеет доступ к данной информации, средства защиты от несанкционированного доступа;

- предположения о лице, причинах, условиях и способе неправомерного доступа и (или) воздействия на компьютерную информацию;

- размер причиненного ущерба.

При допросе свидетеля:

1. IT-специалиста юридического лица:

- дата и время неправомерного доступа к компьютерной информации;

- тип и характеристики используемого КТТС;

- используемые средства защиты компьютерной информации от неправомерного доступа и вредоносных воздействий;

- механизмы автоматической регистрации и протоколирования работы КТТС;

- отмечались ли ранее сбои в работе КТТС, какого характера;

- время и место обнаружения материальных и (или) электронных следов, средств преступления;

- какой был использован способ доступа и воздействия на компьютерную информацию (удаленный или прямой);
- предполагаемые лица, способные совершить неправомерный доступ и воздействие на компьютерную информацию;
- предполагаемые лица, нарушившие правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- предполагаемые лица, связанные с созданием, использованием и распространением вредоносных компьютерных программ; характер причиненного вреда.

2. Коллег по работе подозреваемого (обвиняемого):

- о характере взаимоотношений допрашиваемого с подозреваемым;
- о цели и мотивах совершения преступления (по мнению допрашиваемого);
- имел ли подозреваемый по роду своей деятельности доступ к СКТ;
- имело ли место совершение неправомерного доступа к компьютерной информации подозреваемым с использованием служебного положения;
- знает ли допрашиваемый, где может храниться добытая преступным путем компьютерная информация или где она использовалась (реализовалась) подозреваемым;
- известен ли допрашиваемому круг общения подозреваемого (друзья, знакомые, род их деятельности)¹.

3. Сотрудники оперативных подразделений допрашиваются по представленным результатам оперативно-розыскной деятельности, например, послужившим поводом и основанием для возбуждения уголовного дела.

4. Эксперт допрашивается с целью разъяснения выданного им заключения по судебной экспертизе на возникшие у следователя или иных участников уголовного судопроизводства вопросы, например, по методике проведения экспертизы или функционированию конкретных компонентов (узлов) КТТС.

¹ Егорышев А. С. Расследование и предупреждение неправомерного доступа к компьютерной информации: дис. ... канд. юрид. наук: 12.00.09. Уфа, 2004. С. 99–103.

При допросе подозреваемого (обвиняемого):

1. В первую очередь задаются общие вопросы: каковы цели и мотивы совершения преступления, навык и уровень работы с компьютером, место работы, есть ли компьютер дома и на работе, что входит в обязанности допрашиваемого на работе (если преступление связано с производственной деятельностью)¹.

2. В последующем у подозреваемого (обвиняемого) выясняются:

- способы преодоления средств защиты компьютерной информации от неправомерного доступа и вредоносных воздействий;
- какие программные и технические средства использованы при совершении преступления;
- с какой компьютерной информацией и с каким ПО обычно работает подозреваемый, обвиняемый (по роду его служебной деятельности);
- было ли использовано служебное положение при совершении преступления;
- разработана ли программа собственноручно или заимствована из каких-либо других источников;
- на каком оборудовании разрабатывалась программа;
- для какой операционной системы она была разработана;
- какие от этой вредоносной программы должны быть последствия;
- каков способ использования вредоносной программы;
- какие и сколько компьютеров заражено;
- посредством чего осуществлялось заражение;
- сколько раз и как часто осуществлялись такие посягательства;
- способы сокрытия неправомерного доступа и воздействия на компьютерную информацию;
- в случае совершения преступления ОПГ, установить количество участников группы, наличие и характер сговора, распределение

¹ Шевченко Е. С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук: – М., 2016. С. 96.

ролей, инициатора преступления, техническое обеспечение группы, иные преступления, совершенные этой группой¹.

На заключительном этапе осуществляется обобщение полученной информации и ее фиксация в протоколе. В необходимых случаях следователь использует вспомогательные средства фиксации (аудио-, видеозапись).

В процессе проведения различных видов следственного осмотра следователь изучает отдельный объект или комплекс объектов, в результате чего получает информацию о событии, его механизме, личности преступника и других обстоятельствах, подлежащих установлению по делу. Кроме того, полученные данные важны для определения направленности расследования, организации розыска преступника по горячим следам, проведения иных следственных и оперативно-розыскных мероприятий².

По рассматриваемому виду преступлений объектами осмотра являются места, где обнаружены и откуда совершены:

- неправомерный доступ и воздействие на компьютерную информацию;
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- создание, использование и распространение вредоносных компьютерных программ.

В большинстве случаев, как показывает практика расследования, ими являются жилые или нежилые помещения с расположением в них КТТС.

Таким образом, обнаружение, фиксация и изъятие следов преступления будет осуществляться в помещении, на конструкции и в ПО компьютерно-телекоммуникационного технического средства.

Особое значение имеет качественное проведение осмотра места происшествия, традиционно включающего в себя подготовительный, рабочий и заключительный этапы.

¹ См., например: Егорышев А. С. Указ. соч. С. 107–109; Менжега М. М. Криминалистические проблемы расследования создания, использования и распространения вредоносных программ для ЭВМ: дис. ... канд. юрид. наук. – Саратов, 2005. С. 118–119.

² Баев О. Я. Тактика следственных действий: учеб. пособие. – Воронеж, 1995. С. 23–24.

По рассматриваемому виду преступлений на подготовительном этапе рекомендуется:

1. Проанализировать материалы уголовного дела с обращением внимания на ориентирующую информацию:

- о помещении и находящихся в нем КТТС;
- путях подхода и отхода;
- системном обеспечении компьютерно-телекоммуникационных технических средств;
- размещении узлов подключения к электропитанию, локальной и глобальной сети;
- способах подключения к узлам локальной и глобальной сети (проводной или беспроводной).

2. Определить состав участников осмотра места происшествия (понятые, специалист, оперативный сотрудник). Разъяснить участникам следственного действия меры предосторожности, алгоритм их действий, прав и обязанностей.

3. Подготовить специальные технические средства, системные программы для обнаружения, фиксации и изъятия следов преступления, упаковочный материал (например, для электронных компонентов — антистатистический пакет, экранированные сумки или мешки от внешнего электромагнитного воздействия).

Рабочий этап по рассматриваемому виду преступлений начинается с рассредоточения сил и средств на месте осмотра, с целью предотвращения входа или выхода граждан из зданий, сооружений или помещений, а также электромагнитного воздействия.

Необходимо обеспечить:

- постоянный контроль места неправомерного доступа и воздействия на компьютерную информацию, узлов подключения к электропитанию, локальной и глобальной сети;
- фото- и видеофиксацию расположения объектов, КТТС, стационарных узлов подключения к электропитанию, локальной и глобальной сети, а также схематическое их расположение;
- обследование помещения и конструкции компьютерно-телекоммуникационного технического средства на предмет обнаружения материальных следов преступления (например, следы пальцев, ладоней руки, обуви, микрочастиц и т. п.);
- при обследовании обращать внимание на объекты, в которых могут быть скрыты технические средства, принимающие или передающие электромагнитные, звуковые, световые импульсы.

Способы обнаружения, изъятия и фиксации материальных следов преступления достаточно подробно описаны в криминалистической литературе, в связи с чем уделим внимание особенностям работы с виртуальными или «электронными» следами.

После обследования и изъятия имеющихся материальных следов с конструкции КТТС необходимо обеспечить работу специалиста в области IT-технологий. С его участием определяется и фиксируется в протоколе осмотра места происшествия:

- в каком состоянии (выключенном или включенном) находится КТТС;
- если исследуемое средство включено и имеет экран для вывода информации, необходимо в момент начала осмотра, фото- или видеосъемкой зафиксировать отображаемую на экране информацию;
- марка, модель, используемое системное обеспечение;
- время, место, способ неправомерного доступа, воздействия, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также создание, использование и распространение вредоносных компьютерных программ;
- при изъятии отдельного электронного компонента из КТТС, описываются и указываются его заводской номер, модель;
- при необходимости копируется (создается образ) информации с ОЗУ и с ПЗУ.

В настоящее время существует достаточно специальных технических средств, способных посекторно (побайтово) копировать информацию с электронных носителей, включая блокираторы записи, производящие запись на свой внутренний диск, обеспечивая неизменность информации на исследуемом компьютере¹. Компьютерная информация может копироваться. Однако в тех случаях, когда требуется дальнейшее экспертное исследование, КТТС изымается.

На заключительном этапе следователь обходит место происшествия, убеждается, что все значимые объекты выявлены, зафиксированы, описаны в протоколе осмотра места происшествия и изъяты по правилам работы с вещественными доказательствами.

¹ Гаврилин Ю. В. [и др.] Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учеб. пособие: в 2 ч. – М., 2019. С. 127.

Общие вопросы тактики проведения обыска и выемки достаточно подробно освещены в криминалистической литературе. Применительно к особенностям расследования компьютерных преступлений уточним:

- на подготовительном этапе особое внимание уделяется изучению личности преступника;
- прорабатывается план внезапного проведения обыска и выемки особенно, если такие действия планируются одновременно (параллельно);
- в ходе обыска или выемки необходимо обращать внимание на рукописные записи в виде цифр, букв, знаков, которые могут обозначать пароли или машинный код (например, вредоносной программы).

Рекомендуемые объекты изъятия:

- компонент или полноценное КТТС;
- средства защиты от неправомерного доступа к компьютерной информации (пароли, электронные ключи и т. п.);
- БД или их копии;
- должностные инструкции;
- локальные нормативные акты, регулирующие правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей организации;
- сведения или документы финансовой отчетности организации.

Особое значение при расследовании всех киберпреступлений, в т. ч. преступлений в сфере компьютерной информации, имеет назначение и производство судебных экспертиз.

Перед вынесением постановления (определения) о назначении судебной компьютерной экспертизы рекомендуется связаться с экспертной организацией или экспертом, занимающимся экспертизами данного направления. В предварительной беседе с экспертом необходимо уточнить экспертные задачи и формулировку вопросов, выносимых на разрешение эксперта. В рамках подготовительных мероприятий перед назначением экспертизы может быть проведен осмотр предметов и документов с участием специалиста в области компьютерной экспертизы, направленный на корректировку перечня объектов, передаваемых на исследование. Наряду с осмотром также может быть весьма эффективным исследование электронных носителей ин-

формации, которое производится в более короткие сроки, чем судебная компьютерная экспертиза.

В описательной части постановления (определении) о назначении судебной компьютерной экспертизы необходимо указывать следующие сведения:

- краткое изложение обстоятельств уголовного дела;
- события, при которых был изъят электронный носитель информации (в рамках следственного действия, либо оперативно-розыскного мероприятия);
- какие события необходимо установить в связи с изъятием электронного носителя информации;
- описание изъятого объекта (название, марка, модель, уникальный код устройства, для мобильных телефонов IMEI и т. п.);
- коды доступа к устройству для разблокировки (при наличии).

В случаях, когда устройство имеет систему защиты, которую эксперт имеющимися у себя в наличии силами и средствами преодолеть не может, он вносит ходатайство инициатору назначения экспертизы о предоставлении ему информации, необходимой для разблокировки устройства. Если такие данные не представляются на экспертизу, то её производство становится невозможным.

Экспертной задачей сотрудников компьютерной лаборатории является поиск компьютерной информации по заданным критериям:

- поиск информации, созданной с помощью прикладных программ;
- поиск информации о действиях пользователя.

Объектом исследования является компьютерная информация, содержащаяся на следующих носителях:

- накопителях на жестких магнитных дисках (НЖМД);
- мобильных телефонах и планшетах;
- гибких магнитных дисках (ГМД), zip- и jaz-дисках;
- CD и DVD-дисках;
- flash-накопителях;
- банковских пластиковых карт с магнитной полосой;
- картах памяти и прочих носителях, информация на которых представлена в виде файловых систем.

Исследование объектов осуществляется с использованием специализированных программно-аппаратных комплексов, имеющих в своем составе устройства для работы с информационными носителями, и обладающие следующими возможностями:

- блокирование записи информации на исследуемом носителе;
- посекторное копирование информации;
- вычисление хеш-функции файлов, каталогов, разделов, диапазона секторов;
- доступ к файловой системе информационных носителей;
- восстановления удаленной информации;
- просмотр и приведение в удобочитаемый вид информации, создаваемой наиболее распространенным программным обеспечением (офисными программами, графическими редакторами, системами управления базами данных, программами, предназначенными для работы в локальных и глобальных сетях, и т. п.);
- просмотр и интерпретация системной и служебной информации (следовой картины);
- поиск и манипуляция с информацией по различным критериям (контексту, свойствам, хеш-функциям и пр.).

Организовано проведение следующих видов исследований:

- 1) поиск и восстановление удаленной информации с носителей (накопители на магнитных жестких дисках, flash-накопители);
- 2) поиск сведений о работе пользователя в системе (удаление и/или изменение файлов, системных настроек);
- 3) поиск файлов, по ключевым фразам (названия организаций, имена, документы). Актуально при поиске следов экономической деятельности организаций;
- 4) поиск изображений и видеофайлов (поиск отсканированных копий документов, подделка документов и денежных билетов, детская порнография и т. д.);
- 5) поиск программ, детектируемых антивирусным программным обеспечением как вредоносные;
- 6) просмотр и копирование видео с видеорегистраторов за указанный период;
- 7) поиск переписки в программах электронной почты и в программах обмена сообщениями (ICQ, Brosix, Skype и т. д.);
- 8) определение списка посещенных страниц в сети Интернет
- 9) поиск баз данных «1С: Предприятие»;

10) поиск сведений об установленном программном обеспечении, а также программ, предназначенных для преодоления технической защиты программных продуктов (по вопросам, связанным с нелицензионным использованием программ «Windows», «AutoCAD», «Компас 3D», 3DS Max» и т. д.);

11) исследование GPS-навигаторов (поиск маршрутов передвижения);

12) исследование банковских пластиковых карт с магнитной полосой (получение информации, записанной на магнитную полосу: данные о владельце, дата окончания действия карты, BIN, сведения о платежной системе). Актуально для расследования уголовных дел по «кардерам», лицам, собирающих информацию о пластиковых картах граждан, изготавливающих дубликаты и снимающих с них деньги);

13) исследование сотовых телефонов и смартфонов (получение списка контактов, списка звонков и sms-сообщений; переписка в программах обмена сообщениями и почта. Списки посещенных страниц в сети Интернет; поиск фото, видео, аудио-файлов; поиск вредоносных программ).

Рассмотрим вопросы, которые могут быть поставлены перед экспертом при назначении наиболее распространенной экспертизы — судебной компьютерно-технической.

1. Диагностические вопросы:

КТТС какой модели представлено на исследование?

Каковы технические характеристики электронного компонента КТТС?

Где и когда изготовлено, собрано данное КТТС, каковы его комплектующие?

Не внесены ли какие-либо изменения и в чем это выражается?

Исправно ли КТТС и его электронные компоненты? Каковы причины неисправности?

Какая операционная система использована в КТТС?

Каково содержание информации, хранящейся на внутренних и внешних носителях информации?

Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем?

Не вносились ли в программы какие-либо изменения?

Каков механизм утечки информации из локальных вычислительных сетей? Возможно ли восстановление удаленных файлов?

Когда производилась последняя корректировка БД компьютерно-телекоммуникационного технического средства?

Каков уровень профессиональной подготовки пользователя?

Является ли представленный электронный компонент носителем информации?

Является ли объект экспертизы компьютерной системой либо представляет какой-либо ее компонент (аппаратный, программный, информационный)?

Имеются ли на электронных носителях информации изображения документов (в т. ч. и среди удаленных), которые были бы полностью или частично идентичны представленным на экспертизу объектам?

Имеется ли на электронных носителях информации ПО, с помощью которого могли быть подготовлены представленные на экспертизу объекты?

Решаются ли с помощью представленной электронной системы определенные (указывается, какие конкретно) функциональные (потребительские) задачи?

Находится ли системное обеспечение в рабочем состоянии? Имеются ли какие-либо неисправности в ее работе?

Имеются ли признаки (указывается интересующий перечень конкретных признаков) нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей?

Реализована ли в компьютерной системе какая-либо система защиты доступа к информации?

Каковы возможности по ее преодолению? Имеются ли программы с признаками (указывается перечень конкретных признаков) вредоносности?

Какую общую характеристику и функциональное предназначение имеет ПО представленного объекта?

Каковы реквизиты разработчика, правообладателя представленного программного средства?

Каково функциональное предназначение представленной прикладной программы?

Имеются ли в системном обеспечении представленного средства признаки (указывается перечень конкретных признаков) неправомерного доступа к данным?

Когда и каким образом осуществлялся несанкционированный (санкционированный) доступ к информации?

Каково время создания (последней модификации) представленных данных?

Какие сведения о собственнике (пользователе) КТТС (в т. ч. имена, пароли, права доступа и пр.) присутствуют на электронных носителях информации?

Имеются ли признаки функционирования КТТС в локальной или глобальной сети?

Каково содержание установленных сетевых компонентов?

Каково содержание установок удаленного доступа и протоколов соединений?

2. Идентификационные вопросы:

Не составлена ли представленная компьютерная программа определенным лицом?

Имеют ли комплектующие КТТС единое происхождение?

Перечень вопросов не является исчерпывающим. Он может корректироваться в зависимости от объекта, направляемого на исследование. Для правильной постановки вопросов следователю рекомендуется предварительно согласовывать их с экспертом.

Следует отметить, что для исследования электронных носителей информации и сведений, содержащихся в них, используется различное программное обеспечение, реализуемое и в рамках уголовного судопроизводства. Например, программно-аппаратный комплекс «Мобильный Криминалист» — программное обеспечение российского производства для проведения криминалистической экспертизы мобильных устройств, облачных сервисов, ПК и дронов.

Возможности данного программного обеспечения позволяют:

1) извлечь и расшифровать ключи из Android KeyStore. Android KeyStore — системного хранилища программных и аппаратных ключей шифрования на устройствах с операционной системой Android.

Каждое приложение, шифрующее свои данные, имеет свои уникальные ключи шифрования, которые также зависят от версии операционной системы устройства.

Чтобы получить доступ к зашифрованным данным приложения, нужно открыть «Мастер Извлечения Данных» и произвести извлечение физического образа исследуемого устройства на ОС Android подходящим инструментом.

Во время извлечения физического образа «Мобильный Криминалист» извлечёт и аппаратные ключи шифрования и после анализа полученных данных предоставит полный образ исследуемого устройства, в том числе данные шифрованного приложения, которые извлекаются и расшифровываются в максимальном объеме и являются полностью идентичными данным приложения на устройстве. В секции «Пароли» помимо учетных данных различных сервисов и приложений, также имеются аппаратные ключи шифрования отдельных приложений.

Следует обратить внимание, что в этом случае имеются некоторые ограничения. Во-первых, версия ОС Android должна быть не выше 7 версии. Во-вторых, во время извлечения физического образа мобильного устройства, программа должна его дешифровать.

2) использовать утилиту, которая после предварительной установки Jailbreak checkra1n на iOS-устройство извлекает из него полную файловую структуру и секретное хранилище Keychain, а с версии 1.7/12.1, обладает функцией получения полного доступа к файловой системе и данным Keychain на:

- iPhone 5s, iPhone 6, iPhone 6s Plus (iOS 12.2 – 12.5);
- iPhone 6s, iPhone SE (1st gen), iPad (5th gen) (iOS 12.1.4 - 14.3);
- iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus и iPhone X (iOS 13.0 – 14.3);
- iPad (5th gen), iPad 4 Mini (iOS 12.4 – 14.3);
- iPad Pro 1st/2nd gen и iPad (6th gen) (iOS 13.0 – 14.3).

Извлечение сведений из перечисленных выше устройств происходит с помощью автоматического применения уязвимости checkm8 (при работе с ПО «Мобильный Криминалист» на персональных компьютерах с операционной системой Windows 10).

Более того, данная утилита (начиная с версии 1.6/12.0 и выше) обходит USB Restricted Mode (принудительный ввод пароля при подключении устройства к ПК, если устройство до этого было заблоки-

ровано в течение часа). Обход этого защитного механизма позволяет извлечь часть сведений из телефона или планшета, даже если устройство заблокировано, в режиме BFU. В таком случае, есть возможность получить следующие сведения: информацию о сетевых подключениях (имена сетей, точки доступа, местоположение, уровень сигнала, переданные и полученные пакеты), артефакты ОС, данные о звонках и СМС/iMessage (временные базы данных), данные некоторых приложений и голосовой почты.

Если же устройство находится в разблокированном состоянии, то извлечение происходит без использования режима BFU.

С помощью инструмента «Расширенное извлечение iOS» программного продукта «Мобильный Криминалист» из Apple-устройств можно извлечь:

- данные только выбранных приложений, установленных на устройстве;
- данные секретного хранилища Keychain;
- полную файловую систему устройства в виде .tar-архива.

Важно отметить, что доступ к данным зависит от того, в каком состоянии находится устройство. Если оно разблокировано, то для извлечения доступна вся база его данных. Если же экран устройства заблокирован, то возможно только частичное извлечение информации.

3) получить информации из Умных устройств на базе процессоров МТК – это китайские кнопочные телефоны и смарт-часы на операционной системе, отличной от Android. Из смарт-часов «Мобильный Криминалист» извлекает телефонную книгу, сообщения, журнал вызовов, файлы мультимедиа, историю поиска и закладки в браузерах, информацию об устройстве.

Из кнопочных китайских телефонов извлекаются информация об устройстве, телефонная книга, сообщения, журналы вызовов, календарь, заметки, файлы мультимедиа, история браузера.

4) использовать права root-доступа к устройствам под управлением ОС Android для извлечения всех данных пользователя:

- данные приложений — имена пользователя, пароли, истории, временные файлы и многое другое;
- геоинформация о предыдущих местоположениях подозреваемого;
- удаленные данные и таблицы баз данных.

5) извлекать данные из заблокированных устройств Samsung. На устройствах Samsung с ОС Android версии не ниже 4.4.x и обновлением безопасности до 2018 имеется уязвимость, которая позволяет вычитывать данные из файлового браузера устройства в MTP режиме. MTP режим — протокол, разработанный компанией Microsoft, который используется для передачи данных из мультимедийных устройств (планшетов, смартфонов, плееров) на компьютер.

6) извлекать данные из Huawei-устройств. Возможности «Мобильного Криминалиста» позволяют извлекать и расшифровывать полный физический образ устройств на базе процессоров Kirin 659, 710, 710F, 810, 960, 970, 980, 990 и 990 5G с операционной системой Android от 9 до 10 версии, вне зависимости от вида шифрования.

Также в указанном программном обеспечении имеется возможность использования Мобильного Криминалиста Скаута — это модуль программы «Мобильный Криминалист Детектив». Он позволяет находить и извлекать такую важную информацию из исследуемого персонального компьютера, как:

- учетные записи и токены, закладки, данные форм автозаполнения, историю посещений и файлы куки из интернет-браузеров Google Chrome, Mozilla Firefox, Opera, Microsoft Edge, Internet Explorer;

- учетные данные и токены из программ iCloud for Windows, Telegram Desktop, Unigram X, WhatsApp Desktop, TamTam Destop, Wickr Me Desktop;

- Wi-Fi точки доступа и пароли к ним;

- резервные копии iTunes;

- учетные данные и токены из портативных версий программ и программ, установленных по нестандартному пути.

Важно отметить, что указанные данные доступны только в том случае, если владелец компьютера включил функции автоматического сохранения вводимых паролей к учетным записям и Wi-Fi точкам доступа.

Кроме того, данное программное обеспечение проводит и аналитические мероприятия по интересующей информации:

- анализ биллингов;

– секция «Важная улика» позволяет эксперту работать только с ключевыми доказательствами — без лишней отвлекающей информации. При работе в разных секциях эксперт может отметить любую запись как важную, а затем работать со всеми отмеченными записями сразу в отдельном списке. При этом неважно, к какой секции данные были отнесены первоначально.

Секция представляет собой объединенный список, содержащий записи из телефонной книги, календаря, сообщения, снимки камеры, точки выхода в интернет, данные приложений и т. д. Список позволяет проверять и анализировать информацию на одном экране, концентрируясь на том, что действительно важно;

– «Граф связей» наглядно демонстрирует сложные связи внутри криминальной группы. Этот аналитический инструмент позволяет отследить соединения между владельцами мобильных устройств и их контактами, отметить связи между владельцами нескольких устройств, а также найти общие контакты;

– «Лента событий» отображает все факты использования мобильного устройства в одном списке. Показаны все звонки, сообщения, геоданные и другие виды активности в хронологическом порядке, чтобы можно было просмотреть историю без необходимости переключаться между разными разделами. «Лента событий» доступна как для одного т. п. устройства, так и для всех устройств, отнесенных к делу;

– Модуль карт. Программа извлекает географические координаты из различных источников: мобильные устройства, облачные сервисы, карты памяти и т. д. Геокоординаты в программе показываются на онлайн- и оффлайн-картах и т. п.

Кроме того, в рамках одной или нескольких тактических операций, в зависимости от характера разыскиваемого объекта для рассматриваемого вида преступлений важное значение имеет организация взаимодействия с отдельными участниками уголовного судопроизводства.

По рассматриваемым видам преступления взаимодействие осуществляется, как правило, с оперативными подразделениями органов внутренних дел и ФСБ России. Из непроцессуальных видов отметим совместную работу субъектов взаимодействия в рамках следственно-оперативной группы, которая, как правило, создается на весь период расследования. При этом составляется согласованный план след-

ственных и оперативно-розыскных мероприятий. В рамках данного плана следователь организывает задания по розыску искомых объектов, проведение оперативно-розыскных мероприятий, уточняет информацию о лицах, возможно причастных к совершению преступления.

При взаимодействии с Национальным центральным бюро Интерпола сотрудники правоохранительных органов имеют возможность:

- получить информацию из Международного банка криминальной информации;
- отправить международное поручение и запросы в правоохранительные органы иностранных государств.

Таким образом, в соответствии с приказом МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России № 971/786/310/470/454/333 от 06.10.2006 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» может быть получена следующая информация:

- о сетевых адресах, именах доменов и серверов организаций и пользователей;
- содержании протоколов, трейсингов, логических файлов;
- электронной информации, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений;
- провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг;
- физических и юридических лицах, имеющих отношение к преступлениям в сфере высоких технологий;
- специализированном ПО, методиках и тактике борьбы с компьютерными и телекоммуникационными преступлениями, периодических и специальных изданиях, обзорах статистики, материалах о деятельности специализированных служб различных государств в данной области¹.

¹ Приказ МВД России, Минюста России, ФСБ России, ФСО России, ФСКН России, ФТС России № от 06.10.2006 3786/310/470/ 454/333/971 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола».

3. Углубленный анализ элементов криминалистической характеристики.

3.1. Криминалистическая характеристика личности преступника.

Современные исследования в области криминологии позволяют выделить несколько типологий киберпреступников в зависимости от их профессиональных навыков, мотивации и социально-демографических характеристик. Согласно исследованиям Р. Сабирова, структура киберпреступности в России включает две группы преступлений: преступления в сфере компьютерной информации, а также преступления с применением информационно-телекоммуникационных технологий. На основе анализа научной литературы можно предложить следующую классификацию:

По уровню технической подготовленности:

- неквалифицированные пользователи — лица, использующие готовые инструменты и программное обеспечение для совершения преступлений без глубокого понимания принципов их работы;

- квалифицированные IT-специалисты — лица, обладающие профессиональными знаниями в области программирования, сетевых технологий и систем безопасности, способные создавать специализированное вредоносное программное обеспечение и эксплуатировать уязвимости;

- эксперты в области кибербезопасности — высшая категория преступников, обладающая глубокими экспертными знаниями о методах обхода систем защиты и сокрытия следов противоправной деятельности.

По мотивационной направленности:

- корыстно-ориентированные преступники — мотивацией которых является получение материальной выгоды (например, посредством хищения денежных средств, вымогательства);

- идеологически мотивированные ("хактивисты") — руководствующиеся политическими, религиозными или социальными убеждениями;

- исследователи-экспериментаторы — движимые познавательным интересом и желанием самоутвердиться в профессиональном сообществе;

- кибершпионы — осуществляющие деятельность по хищению информации в интересах государств или коммерческих структур.

По социально-демографическим характеристикам: как показывают исследования, большинство компьютерных преступлений совершается мужчинами в возрасте от 18 до 40 лет, обладающими глубокими или профессиональными знаниями в области IT-технологий. Однако в последнее время наблюдается тенденция к омоложению контингента преступников за счет лиц подросткового возраста, активно осваивающих информационные технологии.

Будапештская конвенция о киберпреступности — первый международный договор, направленный на борьбу с компьютерными преступлениями путем установления единых стандартов в национальных законодательствах и создания процедур международного сотрудничества.

Соглашения о правовой помощи — двусторонние и многосторонние договоры между государствами, регулирующие вопросы взаимодействия правоохранительных органов.

Интерпол — международная организация, обеспечивающая взаимодействие правоохранительных органов различных стран, включая обмен информацией и проведение совместных операций.

3.2. Механизмы международного взаимодействия

В соответствии с приказом МВД России № 786 и других ведомств «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» правоохранительные органы имеют возможность:

- получать информацию из Международного банка криминальной информации;
- направлять международные поручения и запросы в правоохранительные органы иностранных государств;
- получать данные о сетевых адресах, именах доменов и серверов организаций и пользователей;
- получать информацию о содержании протоколов, трейсингов, логических файлов;
- получать сведения о провайдерах и дистрибьюторах сетевых и телекоммуникационных услуг;
- обмениваться информацией о физических и юридических лицах, имеющих отношение к преступлениям в сфере высоких технологий.

Эффективность международного сотрудничества существенно повышается при создании совместных следственно-оперативных групп, объединяющих специалистов разных стран для расследования сложных транснациональных киберпреступлений.

3.3. Проблемы трансграничного расследования.

Несмотря на существующие механизмы сотрудничества, расследование транснациональных компьютерных преступлений сталкивается с рядом проблем:

- различия в национальных законодательствах — несовпадение составов преступлений и санкций в разных странах;
- отсутствие унифицированных процедур — различия в процессуальных нормах, регулирующих сбор и фиксацию доказательств;
- языковые и культурные барьеры — затрудняющие непосредственное взаимодействие специалистов;
- политические аспекты — ограничения в сотрудничестве между некоторыми государствами;
- преодоление этих проблем требует дальнейшей гармонизации законодательств и развития международно-правовой базы сотрудничества в сфере борьбы с киберпреступностью.

4. Перспективные направления развития криминалистической методики расследования компьютерных преступлений

Современный этап развития информационных технологий характеризуется появлением новых вызовов для правоохранительных органов, связанных с развитием таких технологий, как:

- квантовые вычисления — создающие как новые угрозы для существующих систем шифрования, так и новые возможности для криминалистического анализа;
- искусственный интеллект — используемый преступниками для создания адаптивных вредоносных систем и автоматизации атак;
- интернет вещей (IoT) — расширяющий поле для компьютерных преступлений за счет подключения к Интернету бытовых устройств и систем критической инфраструктуры;
- блокчейн-технологии — создающие новые возможности для анонимных платежей и организации преступной деятельности.

В этих условиях дальнейшее развитие криминалистической методики расследования преступлений в сфере компьютерной информации должно осуществляться по следующим направлениям:

- ✓ Разработка стандартизированных протоколов сбора и исследования цифровых доказательств с учетом новых технологий.
- ✓ Создание автоматизированных систем поддержки принятия следственных решений на основе технологий искусственного интеллекта.
- ✓ Развитие международной правовой базы сотрудничества в области борьбы с киберпреступностью.
- ✓ Подготовка специалистов в области компьютерной криминалистики, владеющих современными методами расследования.
- ✓ Разработка криминалистических классификаторов и баз данных цифровых следов киберпреступлений.

Реализация этих направлений позволит повысить эффективность противодействия компьютерной преступности в условиях цифровой трансформации общества.

Таким образом, криминалистическая характеристика преступлений в сфере компьютерной информации продолжает развиваться и усложняться вместе с технологическим прогрессом. Совершенствование методов расследования, основанное на глубоком понимании элементов криминалистической характеристики и использовании современных технологий, является необходимым условием эффективного противодействия киберпреступности в современных условиях.

ЗАКЛЮЧЕНИЕ

В соответствии с Доктриной информационной безопасности Российской Федерации национальная безопасность страны существенно зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет неуклонно возрастать. Расширение и развитие информационной сферы закономерно влечет за собой появление технических, социальных и правовых проблем. Среди последних наиболее острой является проблема уголовного преследования за преступления, совершаемые в сфере компьютерной информации и высоких технологий.

Причиной большого числа совершаемых противоправных деяний в данной сфере является отставание уровня правовой культуры общества от технических навыков специалистов или заинтересованных лиц в области технико-программного обеспечения, высокий уровень латентности, отсутствие базовых знаний в сфере компьютерных технологий у потребителей соответствующей продукции и услуг и сотрудников правоохранительных органов, непонимание истинных угроз и последствий совершения таких преступлений со стороны потенциальных жертв. Полученные данные могут быть использованы для предотвращения и эффективного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей.

Подводя итог, отметим, что информационные технологии прочно вошли в нашу жизнь. В то же время наряду с их развитием повышается уровень активности преступников, совершающих не только компьютерные, но и общеуголовные преступления с применением ИТ (кражи, мошенничества и др.), что не могло не сказаться и на особенностях уголовно-правовой охраны общественных отношений.

Однако признавая информационно-телекоммуникационные сети обстоятельством, повышающим общественную опасность деяния, законодатель проявляет непоследовательность по ряду вопросов.

Во-первых, это проявляется в установлении соответствующего признака, выступающего в одних составах квалифицирующим признаком, в других — конструктивным.

Во-вторых, заметна рассогласованность в наименовании соответствующего признака, когда в одних составах информационно-телекоммуникационные сети названы как часть средств массовой информации, в других наряду с ними, а в отдельных составах упомина-

ются также и электронные сети. Ни говоря уже и о том, что в одних случаях законодатель употребляет фразу «в том числе сеть Интернет», а в других — «включая сеть Интернет».

В-третьих, не всегда понятна логика законодателя в установлении в одних составах квалифицирующего признака в виде использования информационных технологий, но незакрепление его в других составах, схожих по объективной стороне. Подобный подход нарушает системность уголовно-правовых норм и правила законодательной техники.

Необходима четкая и обоснованная уголовно-правовая политика в криминализации деяний, совершаемых посредством ИТ, от единообразного понимания и закрепления использования таких технологий в качестве признака конкретного состава преступления до определения круга деяний, в которых использование информационных технологий имеет составообразующее значение, либо повышает степень общественной опасности деяния.

Многие деяния могут быть совершены путем использования ИТ, но, тем не менее, указанный способ может никак не отражаться в диспозиции статьи. Совершение преступления с использованием информационных технологий существенно облегчает его совершение, нарушает предусмотренный действующим законодательством порядок использования сетевого пространства, позволяет значительно увеличить количество лиц, на которых осуществляется неправомерное воздействие, что увеличивает степень общественной опасности содеянного. Поэтому то, что преступление, в т. ч. и против общественной безопасности, совершено с использованием электронных или информационно-телекоммуникационных сетей, в т. ч. сети Интернет, должно влиять либо на квалификацию содеянного, либо на назначение наказания.

Список использованных источников

Нормативные правовые акты¹

1. Конституция Российской Федерации.
2. Уголовный кодекс Российской Федерации.
3. Уголовно-процессуальный кодекс Российской Федерации.
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
5. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции».
6. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».
7. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
8. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».
9. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».
10. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».
11. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».
12. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
13. Закон РФ от 05.03.1992 № 2446-1. «О безопасности».
14. Указ Президента РФ от 17.03.1998 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
15. Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера».

¹ Все нормативные правовые акты приводятся по данным официального интернет-портала правовой информации pravo.gov.ru (дата обращения: 15.05.2025).

16. Указ Президента РФ от 18.04.1994 № 1706 «Об основах государственной политики в сфере информатизации».

17. Указ Президента РФ от 28.06.1993 № 966 «О Концепции правовой информатизации России».

18. Приказ МВД России от 01.03.2014 № 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях».

19. Приказ МВД России от 29.06.2005 № 511 «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации».

20. Приказ МВД России от 10.02.2006 № 70 «Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации».

Литература

1. Амосов С. Н. Совмещение возможностей техники видеозаписи и компьютерных технологий для формирования следственных документов // Судебная реформа и эффективность деятельности органов суда, прокуратуры и следствия: науч.-практ. конф. молодых ученых. 25 апреля 1998 г.: тезисы выступлений аспирантов, адъюнктов, соискателей. — Санкт-Петербург, 1998. — С. 91–93.

2. Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ / под ред. Б. П. Смагоринского. — Волгоград: ВА МВД России, 2004. — 304 с.

3. Вехов В. Б., Ковалев С. А. Теоретические и прикладные проблемы применения программного обеспечения специального назначения при расследовании преступлений в сфере компьютерной информации // Вестник Воронежского института МВД России. — 2012. — № 1. — С. 38–41.

4. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступностями. — Запорожье: ГУ «ЗИГМУ», 2003. — 336 с.

5. Голубев В. А. Расследование компьютерных преступлений. — Запорожье: ГУ «ЗИГМУ», 2003. — 296 с.
6. Грицаев С. И., Помазанов В. В., Заболотная Ю. А. Компьютеризация целеопределения и планирования расследования // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. — 2015. — № 108. — С. 1–9.
7. Зотов А. Б., Зудин С. И. О тестировании компьютерных программ для составления субъективных портретов // Экспертная практика: сборник статей / ВНИИ МВД России. — Москва, 1996. — № 40. — С. 79–84.
8. Колычева А. Н., Васюков В. Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учебное пособие / под ред. А. Г. Волеводза. — Москва: Проспект, 2019. — URL: <https://books.yandex.ru/books/CBMIDRsi/readonline> (дата обращения: 24.11.2025).
9. Компьютерные технологии в правоохранительной сфере: сборник научных трудов / Академия МВД России. — Москва, 1993. — 192 с.
10. Кофман Д. В. Применение баз данных информационных систем для расследования преступлений // Молодой ученый. — 2023. — № 45 (492). — С. 319–321.
11. Криминалистика: учебник для вузов / под общ. ред. А. И. Бастрыкина. — Москва: Юрайт, 2025. — 643 с.
12. Кулешов Ю. Н., Подольный Р. Н. Методика расследования преступлений, совершённых с применением цифровых технологий: учебное пособие. — Москва: Ай Пи Ар Медиа, 2025. — 84 с.
13. Полевой Н. С. Криминалистическая кибернетика: Теория и практика математизации и автоматизации информ. процессов и систем в криминалистике: учеб. пособие для студентов вузов, обучающихся по спец. «Правоведение». — 2-е изд., перераб. и доп. — Москва: Изд-во Моск. ун-та, 1989. — 325 с., ил.
14. Проблемы взаимодействия при расследовании мошенничеств, совершенных с использованием информационных технологий // Вестник Евразийской науки. — 2024. — № 1. — С. 199–206.
15. Расследование преступлений в сфере компьютерной информации и электронных средств платежа: учебное пособие для вузов / отв. ред. С. В. Зуев, В. Б. Вехов. — Москва: Юрайт, 2022. — 243 с.

16. Современные информационные технологии при расследовании и раскрытии преступлений // Антивирусная защита. — 2017. — 10 янв.
17. Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора: монография / В. В. Пушкарев, В. Б. Вехов, С. А. Ковалев. — Москва: Прометей, 2019. — 124 с.
18. Цифровая криминалистика: учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. — 2-е изд., перераб. и доп. — Москва: Юрайт, 2025. — 490 с.
19. Шинкаренко И. Р., Голубев В. О., Карчевський Н. В., Харабрюш І. Ф. Преступления в сфере использования компьютерной техники: квалификация, расследование и противодействие. — Донецк: РВВ ЛДУВС, 2007. — 267 с.
20. Электронные доказательства в уголовном судопроизводстве: учебник для вузов / отв. ред. С. В. Зуев. — Москва: Юрайт, 2025. — 193 с.

Учебное издание

Подружкина Татьяна Александровна

кандидат педагогических наук

Нисневич Алена Константиновна

Лаур Александр Владимирович

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ,
СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ
И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебно-методическое пособие

Печатается в авторской редакции

Корректорная правка *Свикиш Н.О.*

Компьютерная вёрстка *Свикиш Н.О.*

ISBN 978-5-00277-017-5



EDN: SJRTJJ



Подписано в печать 30.11.2025. Формат 60×84 ¹/₁₆

Печать цифровая. 7,0 п. л. Тираж 25 экз. Заказ № 151/25

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1