ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА
РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ПРОКУРАТУРЫ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОКУРОРСКИЙ НАДЗОР ЗА ИСПОЛНЕНИЕМ ЗАКОНОВ ОРГАНАМИ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ ПРИ ВЫЯВЛЕНИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Научно-практическое пособие

Москва • 2023

УДК 343.16:343.9
ББК 67.721-91+67.408.135
П80

Одобрено Главным управлением по надзору за следствием, дознанием и оперативно-разыскной деятельностью Генеральной прокуратуры Российской Федерации.

***Рецензенты*:**
С.И. Золотарев, начальник Главного управления по надзору за следствием, дознанием и оперативно-разыскной деятельностью Генеральной прокуратуры Российской Федерации;
М.В. Зяблина, заведующий кафедрой прокурорского надзора за исполнением федерального законодательства и участия прокурора в гражданском, административном судопроизводстве и арбитражном процессе Университета прокуратуры Российской Федерации, кандидат юридических наук;
Е.В. Быкова, ведущий научный сотрудник отдела научного обеспечения прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Научно-исследовательского института Университета прокуратуры Российской Федерации, кандидат юридических наук;
М.В. Ульянов, ведущий научный сотрудник отдела научного обеспечения прокурорского надзора и укрепления законности в сфере федеральной безопасности, межнациональных отношений и противодействия экстремизму Научно-исследовательского института Университета прокуратуры Российской Федерации, кандидат юридических наук.

П80 **Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий**: науч.-практ. пособие / [А.Л. Аристархов, К.В. Камчатов и др.]; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. – М., 2023. – 122 с.

В пособии рассматриваются вопросы прокурорского надзора за процессуальной деятельностью органов дознания и органов предварительного следствия при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Авторами затронуты актуальные вопросы теории и правоприменительной практики, предложены пути их разрешения.

Для практических работников органов прокуратуры, научных работников, преподавателей, аспирантов и студентов юридических вузов.
ISBN 978-5-94952-052-9

УДК 343.16:343.9
ББК 67.721-91+67.408.135

Авторский коллектив

А.С. Анненкова, начальник отдела аналитического обеспечения управления методико-аналитического обеспечения надзора за процессуальной деятельностью органов предварительного расследования и оперативно-ра0зыскной деятельностью Главного управления по надзору за следствием, дознанием и оперативно-разыскной деятельностью Генеральной прокуратуры Российской Федерации, кандидат юридических наук, доцент (введение, разд. 2, приложения 1, 2, 3, 4 совместно с Н.М. Гудковым, разд. 3, 4, заключение совместно с Н.М. Гудковым, К.В. Камчатовым, А.Л. Аристарховым, Е.А. Игнатенко, К.В. Васильченко);

А.Л. Аристархов, ведущий научный сотрудник отдела научного обеспечения прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета прокуратуры Российской Федерации, кандидат юридических наук (разд. 3, 4, заключение совместно с А.С. Анненковой, Н.М. Гудковым, К.В. Камчатовым, Е.А. Игнатенко, К.В. Васильченко);

К.В. Васильченко, младший научный сотрудник отдела научного обеспечения прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета прокуратуры Российской Федерации (разд. 3, 4, заключение совместно с А.С. Анненковой, Н.М. Гудковым, К.В. Камчатовым, А.Л. Аристарховым, Е.А. Игнатенко, библиографический список);

Н.М. Гудков, старший прокурор отдела методико-аналитического обеспечения надзора за процессуальной деятельностью органов предварительного расследования и оперативно-разыскной деятельностью Главного управления по надзору за следствием, дознанием и оперативно-розыскной деятельностью Генеральной прокуратуры Российской Федерации (введение, разд. 2, приложения 1, 2, 3, 4 совместно с А.С. Анненковой, разд. 3, 4, заключение совместно с А.С. Анненковой, К.В. Камчатовым, А.Л. Аристарховым, Е.А. Игнатенко, К.В. Васильченко);

Е.А. Игнатенко, старший научный сотрудник отдела научного обеспечения прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент (разд. 3, 4, заключение совместно с А.С. Анненковой, Н.М. Гудковым, К.В. Камчатовым, А.Л. Аристарховым, К.В. Васильченко);

К.В. Камчатов, заведующий отделом научного обеспечения прокурорского надзора за исполнением законов при осуществлении оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве НИИ Университета прокуратуры Российской Федерации, кандидат юридических наук (разд. 3, 4, заключение совместно с А.С. Анненковой, Н.М. Гудковым, А.Л. Аристарховым, Е.А. Игнатенко, К.В. Васильченко);

К.В. Цепелев, ведущий научный сотрудник отдела научного обеспечения прокурорского надзора и укрепления законности в сфере уголовно-правового регулирования, исполнения уголовных наказаний и иных мер уголовно-правового характера Университета прокуратуры Российской Федерации, кандидат юридических наук (разд. 1).

Введение

Общемировые тенденции увеличения числа преступных посягательств, совершенных с применением информационно-телекоммуникационных технологий (далее – ИТТ), коррелируются с процессами, происходящими в Российской Федерации.

Количество таких посягательств за последние пять лет возросло в десятки раз, в связи с чем вопросы обеспечения информационной безопасности отнесены к числу приоритетных направлений деятельности органов государственной власти в соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400.

Так, согласно информационным обзорам и государственным статистическим данным, в Российской Федерации в последние годы ежегодно совершается свыше 500 тыс. преступлений в сфере высоких технологий, главным образом путем кражи денежных средств с банковского счета потерпевшего (порядка 120 тыс.) и мошенничества в самых различных дистанционных формах, а также в отношении электронных средств платежа (порядка 250 тыс.).

Новые технологии все чаще выступают средством совершения самого широкого круга преступлений: от хищений денежных средств с расчетных пластиковых карт до угроз критической инфраструктуре страны и ее безопасности.

Наибольшее количество противоправных деяний в рассматриваемой сфере связано с дистанционными кражами и мошенничеством, а также незаконным сбытом наркотических средств. Актуальны также неправомерный оборот средств платежей, посягательства, касающиеся сведений о частной жизни граждан, их персональных данных, совершение развратных действий в отношении детей и незаконное изготовление порнографических материалов с их изображением. Кроме того, информационное пространство широко используется в целях пропаганды экстремистских и террористических идей.

Данные тенденции в значительной степени обусловлены прогрессивным формированием новых способов совершения

противоправных деяний в условиях развития цифровой среды, недостаточным уровнем правового просвещения граждан, а равно недостатками международно-правового сотрудничества на этом направлении.

Качественно иной уровень при этом занимает организованная преступность, которая носит транснациональный характер, превратившись в глобальную индустрию использования средств и методов системного и широкомасштабного неправомерного доступа к IT-технологиям для самых различных целей.

Понимание глубины перечисленных угроз и вызовов, а также их существа позволило правоохранительной системе при координирующей роли Генеральной прокуратуры Российской Федерации своевременно переформатировать порядок организации работы, активизировать механизмы электронного взаимодействия, а также внедрить широкое использование компьютерно-криминалистических инструментов в области кибербезопасности.

В результате принятых мер темпы прироста преступлений в сфере ИТТ значительно замедлились. При этом отмечаются позитивные тенденции в части повышения раскрываемости преступлений рассматриваемой категории, особенно организованных их видов.

Вместе с тем вопросы раскрываемости преступлений, совершенных с использованием ИТТ или в сфере компьютерной информации, остаются актуальными. Так, в 2020 г. данный показатель составил 20%, в 2021 г. – 23,4%, а в 2022 г. – 27,8%[1]. О сложности ситуации свидетельствует и количество уголовных дел, приостановленных на основании п. 1 ч. 1 ст. 208 УПК РФ, по ряду из которых истекли сроки давности уголовного преследования.

По данным Банка России, в 2022 г. у россиян при помощи мошеннических схем похитили 14 млрд 165 млн 44 тыс. руб., в 2021 – 13 млрд 582 млн 23 тыс.[2]

---

[1] Сведения о раскрываемости преступлений в регионах России за 2020, 2021, 2022 гг. // Официально не опубликованы.

[2] Банк России. Обзор операций, совершаемых без согласия клиентов финансовых организаций. Общий объем и количество операций без согласия клиентов. URL: https://www.cbr.ru/analytics/ib/operations_survey_2022/ (дата обращения: 08.09.2023).

Рекордная сумма, которую телефонные мошенники украли у россиянина, составила 500 млн руб.[1] Усугубляет ситуацию совершение преступлений в отношении пенсионеров, участников Великой Отечественной войны и других лиц. Так, 82-летнего жителя г. Москвы мошенники убедили отдать им более 17 млн руб.[2]

Обращает на себя внимание и то, что с помощью средств мобильной связи в России ежегодно совершается значительное количество преступлений, связанных с заведомо ложными сообщениями об актах терроризма.

Отдельная проблема, на которую обращают внимание прокуроры, – в незаконном обороте персональных данных[3]. Взаимосвязанные с ней трудности сопряжены с упрощением процедуры оформления кредитов, когда присутствие заемщиков в банках не требуется и используется личный кабинет мобильного приложения интернет-банка потерпевшего[4].

Результаты прокурорского надзора по рассматриваемому направлению явились предметом анализа в научно-практических трудах[5], способствовали разрешению сложностей правоприменительной практики. При этом в силу причин объективного характера рассмотреть все вопросы правоприменительной практики в данном пособии затруднительно, в связи с чем проанализированы

---

[1] В МВД назвали рекордную сумму кражи телефонными мошенниками. URL: https://iz.ru/1471808/2023-02-17/v-mvd-nazvali-rekordnuiu-summu-krazhi-telefonnymi-moshennikami?ysclid=ll6huskrvs930577924 (дата обращения: 11.08.2023).

[2] Московский пенсионер отдал мошенникам более 17 млн руб. URL: https://www.mk.ru/social/2023/08/10/moskovskiy-pensioner-otdal-moshennikam-bolee-17-mln-rubley.html (дата обращения: 10.08.2023).

[3] Генеральной прокуратурой Российской Федерации совместно с Минцифры России осуществлялась проработка инициативы по вопросам, связанным с совершенствованием нормативного регулирования и усиления ответственности в области незаконного оборота персональных данных, в рамках проекта федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации».

[4] Информация к заседанию межведомственной комиссии по профилактике правонарушений при губернаторе Магаданской области // Официально не опубликована.

[5] *Прокурорский* надзор за исполнением законов при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации: монография. М.: Проспект, 2022; *Собирание* электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы: монография / Е.А. Архипова, Е.В. Быкова, П.А. Литвишко и др.; под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2022; *Методика* борьбы с компьютерными преступлениями: пособие / К.В. Камчатов и др.; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. М., 2020.

наиболее актуальные из них. Это касается и проанализированных преступлений в рассматриваемой сфере.

В то же время развитие технологий, их широкое распространение и повышенное влияние на все сферы жизнедеятельности предопределяют необходимость дальнейшего наращивания потенциала правоохранительных органов по противодействию им, включая совершенствование международного сотрудничества в целях усиления качества и эффективности такой деятельности.

При подготовке пособия авторы сформулировали рекомендации по повышению эффективности прокурорского надзора на данном направлении.

В ходе работы изучены результаты деятельности Генеральной прокуратуры Российской Федерации, Следственного департамента МВД России, прокуратуры Республики Алтай, прокуратур Красноярского, Приморского и Ставропольского краев, г. Москвы, прокуратур Волгоградской, Ивановской, Ленинградской, Магаданской, Московской, Новгородской, Саратовской, Свердловской, Челябинской областей, учтены результаты анкетирования 57 специализированных прокуроров по тематике пособия, проходивших обучение на факультете профессиональной переподготовки и повышения квалификации Университета прокуратуры Российской Федерации (г. Москва).

Раздел 1. Особенности квалификации преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Применение статей Особенной части УК РФ, содержащих составы преступлений, совершаемых с использованием информационно-коммуникационных технологий, связано со значительными затруднениями. Заметное место в правоприменительной деятельности занимают проблемы квалификации рассматриваемых преступлений, что обусловлено в первую очередь особенностью конструкций соответствующих составов преступлений, бланкетностью уголовно-правовых норм, их межотраслевым характером.

Основная часть проблем квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий, связана с применением положений, предусмотренных ст. 272–274[2] УК РФ, и образующих уголовно-правовой механизм противодействия преступлениям в сфере компьютерной информации.

Статьей 272 УК РФ предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, повлекший общественно опасные последствия в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. В соответствии с п. 1 примечаний к указанной статье под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Согласно п. 2 постановления Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (далее – постановление Пленума № 37) указанные сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах

(далее – компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе жестких дисках-накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

К числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом.

По смыслу ч. 1 ст. 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности[1].

В соответствии с Требованиями к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования, утвержденными приказом Минкомсвязи России от 27.06.2013 № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного

[1] Пункт 3 постановления Пленума № 37.

самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования», общедоступная информация, размещаемая на сайте в форме открытых данных, должна быть защищена от уничтожения, модификации, блокирования, а также от иных неправомерных действий в отношении такой информации.

Обозначенный подход широко используется в судебной практике.

> Так, по одному из уголовных дел суд указал, что в том случае, если владелец информации предпринял меры по ее защите, то информация признается охраняемой по закону в контексте ст. 272 УК РФ, равно как и информация, которая явно признана законом или другим нормативным актом в качестве таковой[1].

Эта позиция в целом соответствует законодательной формулировке предмета преступления, обеспечивая должный уровень уголовно-правовой охраны граждан, организаций и общества от посягательств на охраняемую законом компьютерную информацию. Вместе с тем следует отметить, что неправомерный доступ к находящейся в свободном доступе компьютерной информации, повлекший ее копирование, модификацию и т.д., может при определенных условиях не представлять общественной опасности. В этом случае содеянное в силу малозначительности деяния позволяет применить положения ч. 2 ст. 14 УК РФ.

Применительно к ст. 272 УК РФ неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа)[2].

Понятия уничтожения, блокирования, модификации и копирования компьютерной информации раскрываются в п. 4 постановления Пленума № 37. Ввод компьютерной информации –

---

[1] См., напр.: определение Курганского областного суда от 25.06.2013 № 22-1475/2013. URL: https://sudrf.ru (дата обращения: 26.05.2023).

[2] Пункт 5 постановления Пленума № 37.

это любой алгоритм действий по набору и (или) передаче, а также по электронной обработке сведений (сообщений, данных) для их дальнейшего распознавания и использования компьютерной техникой.

Понятие удаления компьютерной информации в специальной литературе синонимично понятию уничтожения названной информации, используемому в ст. 272 УК РФ. Понятия блокирования и модификации информации для целей ст. 159[6] УК РФ аналогичны соответствующим понятиям, используемым в ст. 272 УК РФ. Эти понятия также раскрываются в постановлении Пленума № 37.

Рассматриваемое преступление во многих случаях выступает способом совершения других неправомерных деяний. Это приводит к ошибкам квалификации, связанным с неполным вменением совершенных виновным лицом преступлений.

Например, А. признан виновным по ч. 1 ст. 272 УК РФ. Суд указал, что он совершил неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей юридическому лицу и содержащей сведения о персональных данных сотрудников, налогах, расчетных банковских счетах и движении денежных средств по ним, что составляет налоговую и банковскую тайну[1].

Вместе с тем неправомерные действия А. были осуществлены в отношении информации ограниченного доступа, в связи с чем должны квалифицироваться по совокупности преступлений, предусмотренных ст. 183 и 272 УК РФ.

Достаточно распространенными являются факты неправомерного доступа к компьютерной информации, хранящейся в электронных почтовых ящиках или на персональной странице пользователя в социальных сетях. В результате этого без согласия пользователя копируются его личные фотографии, переписка, после чего полученная информация зачастую размещается в сети «Интернет». В данном случае имеет место нарушение права гражданина на неприкосновенность частной жизни, личной и семейной тайны, тайны переписки, предусмотренного ч. 1 ст. 23 Конституции Российской Федерации. Названные деяния должны

[1] Апелляционное постановление Верховного Суда Республики Татарстан от 13.12.2016 по делу № 22-8753. URL: https://sudrf.ru (дата обращения: 01.06.2023).

квалифицироваться по ст. 137 (Нарушение неприкосновенности частной жизни), ст. 138 (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) и ст. 272 (Неправомерный доступ к компьютерной информации) УК РФ[1]. При использовании в указанных целях вредоносных компьютерных программ действия виновного лица подлежат квалификации и по ст. 273 УК РФ (Создание, использование и распространение вредоносных компьютерных программ).

Например, М. признана виновной в совершении преступлений, предусмотренных ч. 1 ст. 138 и ч. 1 ст. 272 УК РФ. Судом установлено, что М. на почве ревности получила сведения о PUK-коде абонентского номера потерпевшей. Далее М., используя сеть «Интернет», изменила пароль для входа в личный кабинет клиента, а также модифицировала личные данные абонента, указав вместо них свои. После этого вопреки воле потерпевшей и без ее согласия не менее четырех раз посредством подачи электронных заявок получала информацию о соединениях потерпевшей, их времени и продолжительности[2].

Статьей 273 УК РФ предусмотрена уголовная ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Исходя из разъяснений высшей судебной инстанции, под созданием вредоносных компьютерных программ или иной вредоносной компьютерной информации следует понимать деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, т.е. совершаемого без согласия обладателя информации лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блоки-

[1] См.: *Шарков А.Е.* Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук. Ставрополь, 2004. С. 8.
[2] Приговор Московского районного суда г. Твери от 21.11.2016 по делу № 1-308/2016. URL: https: //sudact.ru/regular/doc/uxdqStrbPMJq (дата обращения: 02.06.2023).

рования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты. При этом для квалификации действий лица по ч. 1 ст. 273 УК РФ как оконченного преступления достаточно установить создание части (фрагмента) кода вредоносной компьютерной программы, позволяющего осуществить неправомерный доступ к компьютерной информации. В таком случае, если еще не было завершено создание вредоносной компьютерной программы, действия лица подлежат квалификации как создание иной вредоносной компьютерной информации[1].

Из приведенного терминологического подхода, определяющего вредоносность программы ее функциональным предназначением – оказывать неправомерное (несанкционированное) воздействие на компьютерные данные и системы, исходит доктрина уголовного права[2] и правоприменительная практика.

Так, П. признан виновным в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ. Суд установил, что он, действуя умышленно, руководствуясь соображениями любопытства и совершенствования собственных навыков владения компьютерными программами, с целью просмотра видеоизображений с камер наружного видеонаблюдения, находясь в своем жилище и по месту работы, используя свои ноутбуки, имеющие доступ к сети «Интернет», путем неоднократных запусков осуществлял использование вредоносной компьютерной программы «Router Scan», заведомо предназначенной для несанкционированного копирования компьютерной информации и нейтрализации средств защиты компьютерной информации, с помощью которой осуществил подбор регистрационных данных (логин и пароль) к оконечному оборудованию пользователей сети «Интернет», в результате чего получил доступ к более чем 100 удаленным системам видеонаблюдения, подключенным к различным компьютерам[3].

---

[1] Пункты 9 и 10 постановления Пленума № 37.

[2] См., напр.: *Вехов В.Б.* Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8). С. 45; *Ефремова М.А.* Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015. С. 101; *Маслакова Е.А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук. Орел, 2008. С. 68.

[3] Приговор Вологодского городского суда от 24.09.2020 по делу № 1-1094/2020. URL: https://sudact.ru/regular/doc/CauwPP3H3Bml (дата обращения: 05.09.2023).

Сложности возникают и с пониманием содержания действий по распространению вредоносных компьютерных программ. Под таковым понимается предоставление доступа к вредоносным компьютерным программам или иной вредоносной компьютерной информации конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами.

Таким образом, лицо должно либо разместить вредоносную программу в общем доступе, либо непосредственно передать ее другому лицу. Однако в судебной практике имеются случаи неверной квалификации деяния, которое не подпадает под признаки преступления, предусмотренного ст. 273 УК РФ, в качестве преступного.

Так, П. осужден по ч. 1 ст. 273 УК РФ. Судом установлено, что он, находясь по месту своего проживания, используя личный компьютер, подключенный к сети «Интернет», желая оказать содействие пользователю социальной сети С. в неправомерном доступе к учетной записи третьего лица, переслал С. ссылку для скачивания вредоносного программного обеспечения, предназначенного для взлома и управления учетной записью пользователя социальной сети, а также подробную инструкцию по использованию указанного вредоносного программного обеспечения. С., перейдя по полученной им от П. ссылке, скачал вредоносное программное обеспечение на свой компьютер. После этого С. записал скачанные им файлы на оптический диск, который передал члену общественной организации «Кибердружина», а последний направил указанный диск в правоохранительные органы.

В обоснование своего решения суд указал, что П. осознавал, что своими действиями распространил в сети «Интернет» вредоносную программу, осуществляющую несанкционированный удаленный доступ к чужим компьютерным данным[1].

Вместе с тем в действиях П. не усматривается состава преступления, предусмотренного ст. 273 УК РФ, поскольку он не создавал вредоносное программное обеспечение, не размещал его в общем доступе, не пересылал программу, а только поделился ссылкой на компьютерный ресурс, на котором другое лицо раз-

[1] Приговор Тверского гарнизонного военного суда от 04.06.2018 по делу № 1-14/2018. URL: https://sudact.ru/regular/doc/9nYqcKNfSBZb (дата обращения: 08.06.2023).

местило вредоносное программное обеспечение. В связи с этим даже дальнейшее использование иными лицами вредоносной программы по своему назначению свидетельствовало бы о пособничестве (в виде предоставления информации) в совершении преступления, предусмотренного ст. 273 УК РФ. Разумеется, лицо, предоставившее ссылку, в этом случае должно знать, для чего другому лицу нужен доступ к вредоносной программе. Следует отметить, что предоставление таких ссылок на постоянной основе, в том числе платно, а также с использованием программных средств, разработанных как самим лицом, поделившимся ссылкой, так и другими лицами, может квалифицироваться по рассматриваемой статье. Указанные обстоятельства подлежат установлению в ходе предварительного расследования.

Использование вредоносных компьютерных программ или иной вредоносной компьютерной информации заключается в их применении, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты[1].

Зачастую создание, использование и распространение вредоносных компьютерных программ используется не само по себе, а для достижения определенного преступного результата. Как правило, вредоносные программы используются для получения неправомерного доступа к компьютерной информации с ее последующим копированием, блокированием, модификацией или удалением. Вместе с тем в правоприменительной практике рассматриваемые деяния не всегда получают надлежащую правовую оценку, в результате чего квалификация совершенного преступления оказывается неполной.

Например, А. осужден по ч. 1 ст. 273 УК РФ. Установлено, что он, находясь по месту своего фактического проживания, используя принадлежащий ему ноутбук марки «HP», имеющий доступ к сети «Интернет», осуществил поиск вредоносной компьютерной программы «Private Keeper», заведомо предназначенной для перебора учетных данных пользователей торговой площадки «ebay.com» и получения полного доступа к аккаунтам третьих лиц, т.е. есть предназначенной для несанкционированного копирования компьютерной информации без ведома законных

[1] Определение нейтрализации средств защиты компьютерной информации приводится в п. 4 постановления Пленума № 37.

пользователей. Найдя программу, А. в целях последующего использования записал ее на жесткий диск ноутбука.

Продолжая реализовывать свой преступный умысел, А., осознавая, что использование вредоносной компьютерной программы «Private Keeper» приведет к неправомерному копированию информации, осуществил запуск указанной программы и получил аутентификационные данные (логин, пароль), а также иные персональные данные 69 граждан Великобритании, США, Франции, Италии, Австралии, Швеции, Гваделупы и других стран, являющихся пользователями интернет-ресурса «ebay.com»[1].

Квалификация содеянного А. не учитывает того факта, что в результате использования вредоносной программы осуществлен неправомерный доступ к компьютерной информации с ее последующим копированием. В связи с этим действия А. надлежит квалифицировать по совокупности преступлений, предусмотренных ст. 272 и 273 УК РФ.

Встречаются на практике и такие случаи, когда в качестве вредоносных используются изначально легальные программы, часть программного кода которых намеренно изменена с целью совершения преступных деяний. В итоге легальная программа становится вредоносной, поскольку обладает уже другими характеристиками, которые не были предусмотрены правообладателем программы. Этот механизм используется, например, для незаконного пополнения баланса транспортных карт[2]. Такие действия также являются уголовно наказуемыми.

Еще одним уголовно-правовым запретом в рассматриваемой сфере является ст. 274 УК РФ, в которой установлена ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Главная сложность квалификации на практике обусловлена тем, что субъект преступления является специальным – это лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой законом

---

[1] Приговор Северского городского суда Томской области от 17.05.2018 по делу № 1-135/2018. URL: https://sudact.ru/regular/doc/FAkPg4JRxGYP (дата обращения: 08.06.2023).

[2] Приговор Останкинского районного суда г. Москвы от 04.12.2017 по делу № 1-507/17. URL: https://sudrf.ru (дата обращения: 08.06.2023).

информации либо информационно-телекоммуникационным сетям и оконечному оборудованию[1] и обязано соблюдать установленные правила их эксплуатации.

В следственно-судебной практике встречаются случаи ошибочной квалификации действий лица по ст. 274 УК РФ.

Так, Ш. осужден за совершение ряда преступлений, в том числе предусмотренного ч. 1 ст. 274 УК РФ. В приговоре суд указал, что Ш., обладающий техническими познаниями в области использования вредоносных компьютерных программ в операционных системах терминалов самообслуживания кредитно-финансовых учреждений, подобрав электронные носители информации с вредоносной компьютерной программой, которая предоставляет возможность тайного хищения денежных средств, в нарушение Федерального закона от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием платежных карт», согласно которому эксплуатация устройства самообслуживания клиентом банка возможна лишь путем использования наличных денежных средств этого клиента либо его платежных карт, посредством неправомерного доступа к компьютерной информации и несанкционированного подключения к устройству самообслуживания для нарушения правил эксплуатации данного устройства самообслуживания как средства хранения, обработки и передачи компьютерной информации, с целью последующего хищения из него наличных денежных средств путем копирования перенес в операционную систему указанного устройства самообслуживания вредоносную компьютерную программу. Нарушение Ш. правил эксплуатации средств хранения, обработки, передачи компьютерной информации устройства самообслуживания в дальнейшем обеспечило тайное хищение Ш. денежных средств на сумму 1 млн 21 тыс. руб., что привело к причинению крупного материального ущерба на указанную сумму[2].

Вместе с тем Ш. не является субъектом рассматриваемого преступления. Кроме того, содеянное осужденным охватывается

---

[1] Под оконечным оборудованием понимаются устройства, которые находятся в конечной точке сети и обеспечивают взаимодействие пользователя с ней. Оперируя сигналами или дискретными данными, такое оборудование позволяет пользователям подключаться к сети, использовать ее ресурсы и передавать информацию. Примерами оконечного оборудования являются персональные компьютеры, смартфоны, планшеты, маршрутизаторы.

[2] Приговор Кировоградского городского суда Свердловской области от 05.08.2016 № 1-105/2016. URL: https://sudact.ru/regular/doc/b2ynlm3ERQJ9 (дата обращения: 01.06.2023).

ст. 272, 273 УК РФ и не требует дополнительной квалификации по ст. 274 УК РФ.

Существенные затруднения у правоприменителя вызывает определение содержания понятия «правила эксплуатации». В Методических рекомендациях Генеральной прокуратуры Российской Федерации указано, что ст. 274 УК РФ является бланкетной и отсылает к конкретным инструкциям и правилам, устанавливающим порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации. Эти правила должны устанавливаться правомочным лицом. Общих правил эксплуатации, распространяющихся на неограниченный круг пользователей глобальной сети «Интернет», не существует[1].

В отличие от ряда иных специальных правил, содержащихся в конкретных нормативных актах, правила эксплуатации средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей не являются консолидированными и закреплены во множестве источников. В связи с этим имеется необходимость четкого определения их перечня.

Рассматриваемые правила устанавливаются на уровне нормативных правовых актов. Примерами могут служить постановление Правительства Российской Федерации от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи» и приказ Минкомсвязи России от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости, функционирования и безопасности информационных систем общего пользования». Необходимо также отметить, что в Российской Федерации приняты национальные стандарты в сфере информационной безопасности: ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положе-

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генеральной прокуратурой России).

ния», ГОСТ 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» и др.

Отдельно следует остановиться на правилах, разработанных и утвержденных в конкретной организации (ведомстве) при определении обязанностей работников (служащих). Должностными инструкциями сотрудников, как правило, предусмотрены определенные ограничения по использованию компьютерной техники и сети «Интернет».

Если ст. 272–274 УК РФ существуют с момента принятия уголовного закона, то ст. 274[1] УК РФ является относительно новой[1]. Данная норма предусматривает ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации и включает все действия, предусмотренные ст. 272–274 УК РФ, которые совершены в отношении компьютерной информации, содержащейся в критической информационной структуре Российской Федерации. Из этого следует, что ст. 274[1] УК РФ является специальной нормой по отношению к ст. 272–274 УК РФ и в соответствии с ч. 3 ст. 17 УК РФ подлежит применению при конкуренции норм.

Нормы ст. 274[1] УК РФ имеют бланкетный характер и отсылают, прежде всего, к Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в ст. 2 которого раскрываются понятия критической информационной инфраструктуры, ее объектов и субъектов.

Следует отметить, что проблемы квалификации преступления, предусмотренного ст. 274[1] УК РФ, производны от проблем квалификации преступлений, ответственность за совершение которых установлена в ст. 272–274 УК РФ. Специфика заключается в особенностях предмета посягательства – критической информационной инфраструктуры.

Под тяжкими последствиями как квалифицирующим признаком в ст. 272–274[1] УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия,

[1] См.: Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»».

учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п. В случае, когда подсудимому вменяется признак создания угрозы наступления тяжких последствий, должна быть установлена реальность такой угрозы[1].

В связи с тем, что с момента дополнения в 2022 г. УК РФ ст. 274[2] (Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»)[2] не выработана правоприменительная практика (статистические показатели о количестве зарегистрированных преступлений и осужденных лиц являются нулевыми), проблемы квалификации новой нормы рассматриваться не будут.

С преступлениями в сфере компьютерной информации тесно связан уголовно-правовой запрет, предусмотренный ст. 159[3] УК РФ.

Статьей 159[3] УК РФ установлена ответственность за мошенничество с использованием электронных средств платежа, под которыми понимаются средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств[3].

С учетом того, что одним из электронных средств платежа являются платежные карты, на практике возникает вопрос об от-

---

[1] Пункт 14 постановления Пленума № 37.

[2] Федеральный закон от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации».

[3] Пункт 19 ст. 3 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – закон о платежной системе).

несении к орудиям (средствам) совершения рассматриваемого преступления дисконтных, бонусных, социальных и других карт. Для решения обозначенной проблемы следует исходить из того, что в ряде случаев такие карты, прежде всего социальные, могут использоваться для осуществления расчетов. Это позволяет, например, не только получать пособия, стипендии и другие выплаты на карту, но и пополнять ее баланс, производить снятие наличных денежных средств, осуществлять безналичные расчеты. Представляется, что такие карты можно считать средством совершения преступления, предусмотренного ст. 159^3 УК РФ. В том случае, если карта таких возможностей не предоставляет, к средствам совершения рассматриваемого деяния ее отнести нельзя.

При квалификации действий по неправомерному использованию платежных карт следует отметить, что хищение денежных средств путем оплаты товаров с использованием чужой банковской карты подлежит квалификации как кража, совершенная с банковского счета (п. «г» ч. 3 ст. 158 УК РФ)[1].

Следует отметить, что в том случае, если виновное лицо открыто похищает банковскую карту, знает или посредством применения насилия к потерпевшему узнает пин-код, то такие действия, несмотря на последующее снятие денежных средств в банкомате в отсутствие потерпевшего, надлежит квалифицировать в зависимости от конкретных обстоятельств по ст. 161 или 162 УК РФ[2].

Хищение денежных средств с банковского счета, а также в отношении электронных денежных средств, совершенное путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, влечет уголовную ответственность по п. «в» ч. 3 ст. 159^6 УК РФ.

Немало проблем на практике вызывает применение ст. 159^6 УК РФ, в которой установлена ответственность за мошенниче-

[1] Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021), утв. Президиумом Верховного Суда РФ 10.11.2021. Определение № 5-УДП21-44-К2.

[2] См., напр.: постановление Московского городского суда от 22.01.2018 № 4у-0362/2018, апелляционное определение Верховного Суда Чувашской Республики от 10.10.2017 по делу № 22-2299/2017.

ство в сфере компьютерной информации. В соответствии с диспозицией ч. 1 названной нормы оно представляет собой хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Применение к ст. 159^6 УК РФ усложняет то обстоятельство, что объект мошенничества в сфере компьютерной информации является сложным. Рассматриваемое преступление посягает на два непосредственных объекта: основным являются отношения собственности, дополнительным – безопасность в сфере компьютерной информации. Соответственно предметом преступления выступают как имущество (право на имущество), так и компьютерная информация.

По сравнению с другими формами хищения, в том числе остальными видами мошенничества, анализируемое деяние представляет собой особую, самостоятельную форму хищения чужого имущества, совершаемого посредством выполнения перечисленных в диспозиции ч. 1 ст. 159^6 УК РФ действий – ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Традиционный для мошенничества признак обмана или злоупотребления доверием в данном случае является необязательным[1].

Понятие вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей содержится в п. 20 постановления Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – постановление Пленума № 48).

Мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и

[1] См. подробнее: *Яни П.С.* Специальные виды мошенничества // Законность. 2015. № 8.

распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274[1] УК РФ.

В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконное воздействие на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием.

Вместе с тем на практике действия виновного лица нередко ошибочно квалифицируются по ст. 159[6] УК РФ[1]. Встречаются и обратные ситуации, когда действия лица ошибочно квалифицируются по ст. 158, а не по ст. 159[6] УК РФ[2].

Если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, использование электронной почты, смс-сообщений), то такое мошенничество следует квалифицировать по ст. 159, а не по ст. 159[6] УК РФ[3].

Таковы наиболее часто встречающиеся проблемы квалификации преступлений в сфере компьютерной информации и связанных с ними преступных посягательств.

---

[1] Приговор Карагайского районного суда Пермского края от 06.02.2018 по делу № 1-14/2018. URL: https://sudact.ru/regular/doc/2YnsQl5GiO14 (дата обращения: 09.06.2023).

[2] Приговор Первомайского районного суда г. Ижевска от 14.06.2018 по делу № 1-272/2018. URL: https://sudact.ru/regular/doc/JHkh07fp26LQ (дата обращения: 10.06.2023).

[3] Пункт 21 постановления Пленума № 48. См. также: апелляционное постановление Свердловского областного суда от 12.09.2017 по делу № 22-6725/2017. URL: https://sudact.ru/regular/doc/qwpCJ2EBYlLa (дата обращения: 10.06.2023).

Вторая группа исследуемых общественно опасных деяний – преступления, квалифицирующим признаком которых является использование информационно-коммуникационных технологий и которые не посягают непосредственно на безопасность компьютерной информации. Как показывает практика, в большинстве случаев использование при совершении преступлений указанных технологий, прежде всего глобальной сети «Интернет», позволяет размещать в открытом или закрытом доступе информацию, которая имеет противоправное содержание. Такие деяния считаются оконченными с момента размещения соответствующей информации[1].

Кроме того, распространенным способом совершения преступлений с использованием информационно-телекоммуникационных сетей является рассылка сообщений или писем по электронной почте, посредством мессенджеров и т.д. При этом для квалификации таких посягательств не имеет значения, какие именно информационно-телекоммуникационные средства (локальные или глобальные сети, коммуникационное оборудование и т.д.) используются виновным лицом.

В целом анализ правоприменительной практики показывает, что существенных затруднений квалификация преступлений, совершенных с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», не вызывает. Вместе с тем для правильной уголовно-правовой оценки названных деяний необходимо обратить внимание на следующее.

Стремительное развитие цифровых технологий на современном этапе развития общества обусловило широкое распространение на практике незаконного сбыта наркотиков с использованием дистанционных форм реализации – электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет».

В соответствии с п. 20 постановления Пленума № 37 по признаку, предусмотренному п. «б» ч. 2 ст. 228[1] УК РФ, при незаконном сбыте наркотических средств квалифицируются действия лица, которое с использованием сети «Интернет» подыскивает источник незаконного приобретения наркотических средств с це-

[1] Определение № 208-АПУ18-3 // Обзор судебной практики Верховного Суда Российской Федерации № 3 (2018), утв. Президиумом Верховного Суда РФ 14.11.2018.

лью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств.

По указанному признаку также квалифицируется совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (например, при незаконном сбыте наркотических средств обеспечивалась связь между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

Так, по одному из уголовных дел апелляционным определением судебной коллегии по уголовным делам Красноярского краевого суда от 23.03.2021 по жалобе осужденного изменен приговор Канского городского суда от 13.01.2021 в отношении Л., осужденного по ч. 3 ст. 30, п. «г» ч. 4 ст. 228[1] УК РФ. В своем решении суд апелляционной инстанции указал, что виновное лицо может быть осуждено по рассматриваемому квалифицирующему признаку только в тех случаях, когда данное лицо с использованием сети выполняет объективную сторону преступления. При этом использование программы мгновенного обмена сообщениями «Telegram» в переговорах между соучастниками, связанными со сбытом наркотических средств, не свидетельствует о том, что при сбытах наркотических средств, на которые покушался Л., использовались электронные или информационно-телекоммуникационные сети (включая сеть «Интернет»).

Согласно определению Восьмого кассационного суда общей юрисдикции от 01.09.2021 суд первой инстанции, описывая преступное деяние, совершенное Л., обоснованно посчитал доказанным, что Л. и неустановленное лицо совершили действия, направленные на сбыт наркотических средств, используя программу обмена сообщениями «Telegram» в информационно-телекоммуникационной сети «Интернет», посредством которой они вступили в предварительный сговор, координировали свои действия, в том числе обменивались информацией о месте нахождения оптовой партии наркотических средств, намеревались обмениваться информацией о местонахождении произведенных тайников-закладок с наркотическими средствами, что свидетельствует о наличии умысла на совершение последующего сбыта наркотических средств потребителям посредством сети «Интернет»[1].

[1] По информации прокуратуры Красноярского края.

Таким образом, для обоснованного вменения рассматриваемого квалифицирующего признака необходимо установить, что объективная сторона состава преступления была выполнена с использованием информационно-телекоммуникационных технологий. Обозначенный подход применим и к другим составам преступлений с аналогичным квалифицирующим признаком, в том числе предусмотренным ст. 222–222^2 УК РФ.

Вместе с тем следует отметить, что уголовно-правовая оценка преступлений, квалифицирующим признаком которых является использование ИТТ, включая сеть «Интернет», имеет определенную специфику в зависимости от вида преступления.

Зачастую на практике возникают вопросы с квалификацией незаконного изготовления и оборота порнографических материалов, совершенных с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1 УК РФ). Так, учитывая, что указанные материалы могут составлять сведения о частной жизни потерпевшего (потерпевшей), квалификация не всегда осуществляется в полном объеме.

М. осужден по п. «б» ч. 3 ст. 242 УК РФ. По делу установлено, что потерпевшая, находясь в его ванной комнате и принимая ванну с пеной, предложила ее сфотографировать, после чего М. часто снимал потерпевшую на свой телефон и она была не против. На вопрос потерпевшей, что он будет делать с ее фотографиями, М. обещал сохранить их на флешке и никому не показывать. Однако в дальнейшем он разместил фотографии на созданной им интернет-странице от имени потерпевшей. По заключению экспертизы, размещенный файл оказался материалом порнографического характера. При этом при совершении преступления подсудимый действовал умышленно, осознавал, что он, распространяя порнографические материалы и предоставляя возможность другим лицам получить к ним доступ, действует незаконно, в нарушение действующего законодательства, согласно которому распространение материалов, пропагандирующих порнографию, не допускается[1].

Вместе с тем суд, признав М. виновным в распространении порнографических материалов, не учел, что целью преступника было распространение не любых порнографических материалов,

[1] Приговор Щербинского районного суда города Москвы по уголовному делу от 08.12.2014 № 1-395/2014. URL: https://actofact.ru/case-77RS0034-1-395-2014-2014-09-30-2-0/?ysclid=lor50msgex646206339 (дата обращения: 08.07.2023).

а порнографических фотографий конкретного человека, т.е. распространение сведений о частной жизни потерпевшей. При таких условиях преступление подлежит квалификации по ч. 1 ст. 137 и п. «б» ч. 3 ст. 242 УК РФ[1].

В зависимости от конкретных обстоятельств содеянного незаконное изготовление и оборот порнографических материалов, совершенные с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», могут квалифицироваться и в совокупности с другими преступлениями, например, предусмотренными ст. 163, 272, 273 УК РФ.

Определенные трудности вызывает квалификация действий виновного лица по распространению порнографических материалов или предметов. Под такими действиями понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности использования порнографических материалов. Оно может совершаться путем направления в личном сообщении конкретному лицу (по электронной почте либо с использованием социальных сетей, мессенджеров или иных приложений), рассылки определенному или неопределенному кругу лиц (например, в чат в мессенджере), размещения на личных страницах и на страницах групп пользователей, в том числе в социальных сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания[2].

Преступление считается оконченным с момента предоставления виновным доступа к порнографическим материалам или предметам, например посредством предоставления возможности копирования в информационно-телекоммуникационной сети общего пользования[3].

В современной судебной практике действия пользователей информационно-телекоммуникационных сетей, включая сеть «Интернет», связанные с размещением порнографических мате-

---

[1] См.: *Соловьев В.С.* Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. 2017. № 6.

[2] Пункт 22 постановления Пленума № 37. В этом же пункте приводится определение публичной демонстрации с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», и рекламирования порнографических материалов или предметов.

[3] Кассационное определение Тульского областного суда от 26.10.2011 № 22-2581. URL: https://sudact.ru/regular/doc/R2GJhg3eMB68/?ysclid=lnd4gzv0lu154202759

риалов на общедоступных ресурсах не всегда расцениваются как распространение порнографических материалов, в том числе при осознании пользователем факта общедоступности размещенных материалов[1].

Вместе с тем это не означает, что сведения о размещении порнографических материалов на общедоступных ресурсах для личного использования автоматически свидетельствуют об отсутствии в действиях лица признаков рассматриваемых преступлений. В каждом конкретном случае необходимо тщательно разбираться в обстоятельствах содеянного.

Так, Судебной коллегией по уголовным делам Верховного Суда Российской Федерации 22.03.2022 по кассационному представлению Генеральной прокуратуры Российской Федерации отменены оправдательный приговор и последующие судебные решения в отношении лица, обвиняемого в распространении детской порнографии (дело № 14-УДП221-1-К1).

Кассационная инстанция согласилась с аргументами Генеральной прокуратуры Российской Федерации о том, что само по себе размещение на личных страницах в социальных сетях видеороликов порнографического содержания является фактическим распространением этой информации, поскольку ей придается статус публичности.

Состав преступления образует сам факт размещения в социальных сетях порнографических материалов, которые становятся доступными для просмотра неопределенным кругом лиц, что должно быть очевидно лицу, их разместившему. При этом диспозиция ст. 242[1] УК РФ не предполагает в качестве обязательного признака объективной стороны преступлений фактическую передачу таких материалов третьим лицам.

Аргументы нижестоящих судов о том, что распространение порнографических материалов может иметь место лишь тогда, когда виновное лицо совершает целенаправленные действия по передаче запрещенных материалов третьим лицам, Верховным Судом Российской Федерации отвергнуты[2].

---

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10.07.2019 № 16-УД19-7, определение Первого кассационного суда общей юрисдикции от 24.03.2020 № 77-291/2020.

[2] Информационное письмо заместителя Генерального прокурора РФ И.В. Ткачева от 12.05.2022 № 12-55102-21 «О правовой позиции Верховного Суда Российской Федерации по уголовным делам о преступлениях, связанных с распространением в социальных сетях детской порнографии».

Подводя итог анализу проблем квалификации преступлений, совершаемых с использованием информационно-коммуникационных технологий, следует отметить, что с целью совершенствования правоприменительной деятельности прокурорам при осуществлении надзора за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, дознание и предварительное следствие, а также при поддержании государственного обвинения в суде следует уделять особое внимание правильности квалификации действий лиц, совершивших преступления с использованием информационно-коммуникационных технологий, и при выявлении ошибок квалификации принимать незамедлительные меры к устранению допущенных нарушений.

Раздел 2. Координация деятельности правоохранительных органов по борьбе с преступностью и прокурорский надзор за исполнением законов в сфере профилактики, выявления и пресечения преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Результаты анализа докладных записок прокуроров субъектов Российской Федерации свидетельствуют о том, что многие вопросы, которые имеют значение для противодействия ИКТ-преступности, рассматриваются в рамках реализации как профилактических, так и координационных мероприятий.

Так, с целью исполнения требований Федерального закона от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» прокурорами организована соответствующая профилактическая работа с местным населением, участковыми уполномоченными полиции демонстрируются буклеты, направленные на предотвращение дистанционных мошенничеств, информация о возможных способах мошенничества доводится до граждан посредством распространения листовок[1].

Порядок такой деятельности определяется положениями приказа Генерального прокурора Российской Федерации от 02.08.2018 № 471 «Об организации в органах прокуратуры Российской Федерации работы по правовому просвещению и правовому информированию».

Особенности принятия указанных мер при профилактике дистанционных форм противоправной деятельности учтены при формировании поручения, предусмотренного п. 1.3 координационного совещания руководителей правоохранительных органов Российской Федерации от 17.07.2020 «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая крити-

[1] По информации прокуратуры Волгоградской области.

ческую информационную инфраструктуру Российской Федерации», которым предусмотрено принимать дополнительные меры, направленные на усиление эффективности профилактической работы с населением, повышение уровня правовой и финансовой грамотности граждан, пропаганду «компьютерной гигиены» среди физических и юридических лиц, а также на организацию надлежащего исполнения органами служб безопасности организаций финансово-кредитной и информационно-телекоммуникационной сфер. Использовать для этого различные способы распространения информации (в органах власти, муниципальных образованиях, государственных, медицинских, образовательных и других учреждениях, на объектах торговли и массового пребывания граждан). Привлекать к участию иные заинтересованные ведомства, службы и организации, в том числе общественные.

Наряду с этим прокурорам субъектов Российской Федерации, приравненным к ним военным и иным специализированным прокурорам 10.01.2022 Генеральной прокуратурой Российской Федерации направлено письмо «О дополнительных мерах, направленных на усиление профилактической работы с населением, повышение уровня правовой и финансовой грамотности», в соответствии с которым ими организовано распространение разработанных Генеральной прокуратурой Российской Федерации во взаимодействии с Банком России информационных видеороликов, направленных на развитие правовой грамотности граждан и пропаганду «компьютерной гигиены»[1].

Генеральной прокуратурой Российской Федерации координируется работа правоохранительных органов по пресечению деятельности межрегиональных организованных преступных групп, использующих иностранные сервисы IP-телефонии, предоставляющие возможность подмены абонентского номера, разработаны законодательные инициативы[2].

---

[1] Справка Генеральной прокуратуры РФ о результатах мониторинга в сфере профилактики правонарушений за 2022 год.

[2] Информационно-аналитическая справка во исполнение приказа Генерального прокурора РФ от 05.03.2018 № 119 «Об организации в органах прокуратуры Российской Федерации работы по исполнению требований федерального закона от 23.06.2016 № 182-ФЗ «Об основах профилактики правонарушений в Российской Федерации», подготовленная Главным управлением по надзору за следствием, дознанием и оперативно-разыскной деятельностью.

Одним из ключевых элементов организации работы органов прокуратуры на рассматриваемом направлении является надлежащая реализация положений, предусмотренных абз. 8 п. 2 ст. 1 Федерального закона от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации», по координации деятельности правоохранительных органов по борьбе с преступностью.

Так, прокуратурой г. Москвы в 2022 г. проведены заседания рабочей группы с участием должностных лиц ГУ МВД России по г. Москве, ФСБ России, Банка России, Минцифры России, Роскомнадзора по ЦФО, Правительства г. Москвы, а также представителей крупнейших кредитно-финансовых учреждений и операторов связи[1].

Прокуратурой Магаданской области в рамках противодействия рассматриваемым преступным посягательствам 17.03.2023 организован круглый стол с участием руководителей правоохранительных органов, представителей кредитных организаций ПАО «Сбербанк» и ПАО «ВТБ», а также Министерства труда и социальной защиты Магаданской области, на котором обсуждались вопросы влияния на криминальную активность в указанной сфере[2].

Генеральная прокуратура Российской Федерации отметила важность возможностей координационной деятельности и инструментов межведомственного взаимодействия с правоохранительными и контролирующим органами для установления обстоятельств и средств подмены телефонных номеров, почтовых сервисов, в том числе администрированных за пределами Российской Федерации, и их модификации[3].

При этом, учитывая специфику ИКТ-преступности в мероприятиях координационного характера, представляется важным участие контролирующих органов, представителей финансово-кредитных учреждений, операторов связи, провайдеров интернет-услуг и иных субъектов цифровой среды.

Важную роль в вопросах противодействия противоправной деятельности в области высоких технологий играет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор).

---

[1] По информации прокуратуры г. Москвы.

[2] По информации прокуратуры Магаданской области.

[3] Информационное письмо первого заместителя Генерального прокурора РФ А.В. Разинкина от 18.05.2022 № 69-09-2022 «О некоторых вопросах противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» (далее – информационное письмо от 18.05.2022).

В соответствии с постановлением Правительства Российской Федерации от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» Роскомнадзор является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных, а также функции по организации деятельности радиочастотной службы.

Немаловажным также является и то, что, согласно положениям подп. 1 п. 2 ст. 37 Федерального закона от 07.07.2003 № 126-ФЗ «О связи» (далее – закон о связи), Роскомнадзор, как лицензирующий орган в сфере связи вправе приостановить действие лицензии в случае выявления нарушений, которые могут повлечь за собой причинение ущерба правам, законным интересам, жизни или здоровью человека, а также обеспечению нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.

Роскомнадзор осуществляет свою деятельность непосредственно и через свои территориальные органы во взаимодействии с другими федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, общественными объединениями и иными организациями.

Важным элементом борьбы с ИКТ-преступниками является выявление и пресечение финансирования их деятельности, а также каналов легализации преступных доходов. В связи с этим взаимодействие с национальным подразделением финансовой разведки (ПФР), которым является Федеральная служба по финансовому мониторингу (Росфинмониторинг), – это необходимая составляющая работы правоохранительных органов на рассматриваемом направлении. Сотрудничество органов внутренних дел с подразделениями Росфинмониторинга осуществляется в порядке, установленном Инструкцией по организации информационного взаимодействия в сфере противодействия легализации (отмыва-

нию) денежных средств или иного имущества, полученных преступным путем, утвержденной межведомственным приказом Генеральной прокуратуры Российской Федерации, Федеральной службы по финансовому мониторингу, МВД России, ФСБ России, ФТС России, Следственного комитета Российской Федерации от 21.08.2018 № 11/244/541/433/1313/80 «Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем» (далее – совместный приказ от 21.08.2018).

В последние годы сформировалось несколько направлений сотрудничества подразделений по контролю за оборотом наркотиков и Росфинмониторинга. Начинается оно, как правило, в рамках документирования предикатного наркопреступления с целью установления лиц и действий, связанных с легализацией преступных доходов. Также практикуется совместная аналитическая работа в случае обнаружения признаков легализации наркодоходов для установления предиката, в результате совершения которого получена криминальная прибыль.

Финансовое расследование – процесс установления сотрудниками Росфинмониторинга и его территориальными подразделениями связи операций/сделок с уголовно наказуемыми деяниями. В ходе финансовых расследований анализируется информация о финансовой деятельности юридических и физических лиц, финансовые операции, сделки, контракты, договоры, банковские счета, реквизиты финансовых инструментов и связанные с ними сведения.

Материалы, полученные из ПФР, имеют разведывательный (ориентирующий) характер. Помимо специфики полномочий данного ведомства, такие условия призваны обеспечить сохранность банковской и иной охраняемой законом тайны, поскольку специального порядка их раскрытия в рамках национальной системы ПОД/ФТ, в отличие от результатов ОРД, не предусмотрено.

Соответственно, проверка данных должна осуществляться оперативно-розыскным путем, как правило, в рамках производства по ДОУ. Следователю предоставляются рассекреченные в установленном порядке результаты ОРД с включением в них информации Росфинмониторинга без ссылки на источник ее полу-

чения для последующего закрепления механизмами оперативно-розыскной и процессуальной деятельности.

В мероприятиях координационного характера также представляется важным участие налоговых органов ФНС России, информационные ресурсы которых также могут способствовать выявлению и расследованию преступлений в сфере ИТТ. Так, на основании п. 3 ст. 82 НК РФ, предусматривающего, что налоговые органы, таможенные органы, органы внутренних дел, следственные органы и органы управления государственными внебюджетными фондами Российской Федерации в порядке, определяемом по соглашению между ними, информируют друг друга об имеющихся у них материалах о нарушениях законодательства о налогах и сборах и налоговых преступлениях, о принятых мерах по их пресечению, о проводимых ими налоговых проверках, а также осуществляют обмен другой необходимой информацией в целях исполнения возложенных на них задач.

Кроме того, немаловажным является принятие мер по противодействию осуществлению переводов денежных средств без согласия клиента, а также пропуску в сети связи подменного трафика.

В соответствии со ст. 57^4 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, устанавливает обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними нормативными правовыми актами.

На основании ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» информация о случаях и (или) попытках осуществления переводов денежных средств без согласия клиента (в том числе сведения об операциях,

о счетах и вкладах, в отношении которых были зафиксированы случаи и (или) попытки осуществления переводов денежных средств без согласия клиента) представляется в ситуациях, предусмотренных Федеральным законом «О национальной платежной системе», кредитными организациями, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России. Последний вправе предоставлять получаемую в соответствии с настоящей частью информацию кредитным организациям, операторам платежных систем, операторам услуг платежной инфраструктуры в случаях, предусмотренных Федеральным законом «О национальной платежной системе».

В силу ч. 1 ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – закон о платежной системе) операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы услуг информационного обмена, поставщики платежных приложений, операторы платежных систем, операторы услуг платежной инфраструктуры, операторы электронных платформ, оператор платформы цифрового рубля обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации. Правительство Российской Федерации по согласованию с Банком России устанавливает требования к защите указанной информации.

В соответствии с ч. 4 ст. 27 закона о платежной системе операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры, операторы электронных платформ обязаны реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в порядке, установленном Банком России.

В дальнейшем в правоприменительной деятельности подлежат учету положения Федерального закона от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе», направленные на совершенствование механизма противодействия хищению денежных средств («антифрод») в качестве превентивных мер.

Для организации координационной работы важно учитывать, что в силу ст. 83 Федерального закона «О Центральном банке Российской Федерации (Банке России)» в систему Банка России входят центральный аппарат, территориальные учреждения, расчетно-кассовые центры, вычислительные центры, полевые учреждения, образовательные и другие организации, в том числе подразделения безопасности и Российское объединение инкассации, которые необходимы для осуществления деятельности Банка России.

Существенным элементом противодействия преступлениям, совершаемым с использованием IT-сервисов, является пресечение нарушений требований, предусмотренных законом о связи, влекущих пропуск телефонных звонков с подменных номеров и из иностранной юрисдикции, в том числе посредством IP-телефонии.

Так, в постановлении мирового судьи № 77 района Сокол г. Москвы от 15.07.2022 после проверки информации, полученной по результатам изучения уголовного дела, возбужденного по ч. 2 ст. 207 УК РФ, установлено, что через техническое оборудование оператора сотовой связи ООО «ИТСИ-ТЕЛЕКОМ» прошел 1 вызов от иностранного оператора сотовой связи компании, зарегистрированной в Чешской Республике, с нумерацией +7… на Б-номер + 7…. Оператор, пропуская поступивший звонок, не исполнил обязанность по его прекращению, что является нарушением п. 10 ст. 46 закона о связи[1].

В постановлении и.о. первого заместителя Пушкинского городского прокурора Московской области от 23.12.2022 о возбуждении в отношении заместителя директора Общества дела об административном правонарушении, предусмотренном ч. 2 ст. 13.2[1] КоАП РФ, указано о том, что приказом генерального директора общества на заместителя генерального директора общества возложена обязанность по контролю за взаимодействием с зарубежными контрагентами, в том числе согласование договоров, взаиморасчеты и соблюдение закона о связи.

В целях повышения эффективности работы на заданном направлении Генеральной прокуратурой Российской Федерации подготовлены информационные письма, направленные на пресе-

[1] Постановление мирового судьи № 77 района Сокол г. Москвы от 15.07.2022.

чение использования подменных номеров для совершения преступлений в рассматриваемой сфере[1].

Следует учитывать, что согласно информационному письму от 07.08.2023 в соответствии с абз. 4 и 5 ч. 10 ст. 46 закона о связи оператор связи обязан прекратить оказание услуг связи и (или) услуг по пропуску трафика в свою сеть связи в случае, если инициированное с сети связи иностранного оператора связи соединение, в том числе для передачи текстового сообщения, сопровождается нумерацией, соответствующей российской системе и плану нумерации[2] и если у оператора связи отсутствует информация об абонентском номере или уникальном коде идентификации абонента, инициировавшего это соединение. Несоблюдение названных положений влечет привлечение оператора связи к административной ответственности, предусмотренной ч. 2 ст. 12.3[1] КоАП РФ.

Подмена абонентского номера при инициировании телефонного вызова или соединения для целей передачи голосовой информации может совершаться непосредственно операторами, в сетях связи которых возникает (инициируется) данный вызов, в связи с чем оператор должен передать в сеть связи или сеть передачи данных другого оператора, участвующего в установлении соединения, в неизменном виде исключительно абонентский номер, выделенный на основании договора об оказании услуг связи абоненту, инициировавшему такой вызов.

Отсутствие возможности использования системы оператором связи, с сети связи которого инициируется телефонный вызов или соединение для целей передачи голосовой информации, не препятствует исполнению таким оператором обязанности по передаче абонентского номера или уникального кода идентификации в сеть связи другого оператора в неизменном виде, поскольку это должен быть абонентский номер, выделенный на ос-

---

[1] Информационное письмо первого заместителя Генерального прокурора РФ А.В. Разинкина от 18.05.2022 № 69-09-2022 «О некоторых вопросах противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий»; информационное письмо первого заместителя Генерального прокурора РФ А.В. Разинкина от 07.08.2023 № 708-105-2023 «О реализации требований статей 46 и 46[1] Федерального закона «О связи» и статей 13.2[1], 28.1 Кодекса Российской Федерации об административных правонарушениях» (далее – информационное письмо от 07.08.2023).

[2] Приказ Минцифры России от 31.01.2022 № 75 «Об утверждении российской системы и плана нумерации».

новании договора об оказании услуг связи его абоненту, инициировавшему телефонный вызов или соединение.

Для установления оператора связи, допустившего подмену абонентского номера при установлении телефонного соединения, инициированного в пределах Российской Федерации, необходимо направлять запросы оператору связи, завершившему вызов на своего абонента, о представлении информации об операторе, из сети связи которого поступил такой вызов, а также оператору связи, которому выделен абонентский номер, сопровождавший вызов[1].

При отсутствии подтверждения факта инициирования вызова абонентом оператора связи, которому в установленном порядке выделен сопровождавший телефонное соединение абонентский номер, запросы необходимо направлять последовательно каждому оператору связи, участвовавшему в установлении телефонного соединения, вплоть до момента установления оператора, в сети связи которого был подменен номер, или оператора, с сети связи которого был инициирован вызов с подмененным номером.

В случае получения от всех операторов связи, участвовавших в установлении телефонного соединения, информации об отсутствии факта подмены абонентского номера или неполучения ответа от операторов необходимо направлять в соответствующий территориальный орган Роскомнадзора требование о проведении проверок в отношении всех указанных операторов связи.

При осуществлении взаимодействия с перечисленными субъектами ИКТ-сферы важна оперативность истребования необходимой для раскрытия преступлений рассматриваемой категории информации.

Нужно учитывать, что согласно ст. 26 Федерального закона от 02.12.1990 № 395-I «О банках и банковской деятельности» (далее – закон о банках) справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются кредитной организацией в срок, установленный ст. 9 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»

[1] Данные и последующий абзацы раскрыты в Методических рекомендациях о порядке привлечения операторов связи к административной ответственности, предусмотренной ч. 1 и 2 ст. 13.2[1] КоАП РФ, подготовленных в Генеральной прокуратуре Российской Федерации.

(далее – закон об ОРД), на основании судебного решения должностным лицам органов, уполномоченных осуществлять ОРД, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном ст. 9 закона об ОРД, при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела. Перечни указанных должностных лиц устанавливаются нормативными правовыми актами соответствующих федеральных органов исполнительной власти.

На основании ч. 8 ст. 9 закона об ОРД в порядке, предусмотренном настоящей статьей, рассматриваются также ходатайства органов, осуществляющих ОРД, о предоставлении кредитными организациями справок по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц. Указанные справки предоставляются кредитными организациями на основании судебного решения в течение 10 рабочих дней со дня получения соответствующего постановления суда.

Наряду с этим следует также отметить, что согласно ч. 1 ст. 43 Федерального закона от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» запросы судей, следователей и должностных лиц органов дознания о пользовании, владении или распоряжении финансовыми средствами, иным имуществом либо об их местонахождении или размещении в связи с находящимися в производстве материалами и делами о незаконном обороте наркотических средств, психотропных веществ и их прекурсоров исполняются должностными лицами в течение трех суток со дня получения указанных запросов, не считая выходных и праздничных дней.

В случае неисполнения законных требований следователя, дознавателя имеет место практика привлечения виновных лиц к административной ответственности по ст. 17.7 КоАП РФ[1].

[1] По информации прокуратуры Челябинской области.

Нередко рассматриваемые преступления совершаются в составе организованных групп, а их организаторы зачастую остаются неустановленными.

Определение соответствующих ориентиров для органов, осуществляющих оперативно-розыскную деятельность, при реализации ст. 2 закона об ОРД видится важным для решения предусмотренных этим законом задач.

Некоторые прокуроры отмечают, что раскрываемость данного вида преступлений за 5 месяцев 2023 г. составила только 28,8%, достигнута в основном за счет многоэпизодных уголовных дел об очевидных преступлениях, привлечение же к ответственности организаторов дистанционных хищений, совершаемых в отношении лиц предпенсионного возраста, пенсионеров, а в отдельных случаях и ветеранов Великой Отечественной войны, ущерб по каждому из которых составляет миллионы рублей, осуществляется крайне неэффективно[1].

Так, прокуратура Свердловской области информировала, что по оперативным данным на территории Свердловской области противоправную деятельность по реализации наркотиков осуществляет значительное число интернет-магазинов, каждый из которых представляет собой высокоорганизованную преступную группу, включающую большое количество участников с четко определенной специализацией. Их организаторы активно вербуют новых участников наркогрупп посредством объявлений на интернет-форумах, в телеграм-каналах и на страницах социальных сетей.

Как пишут М.П. Васильева и А.Л. Кобелев, существование преступного сообщества не всегда очевидно и доказуемо на первоначальном этапе расследования, в связи с чем возбуждению уголовного дела должна предшествовать глубокая оперативная разработка со значительным количеством проводимых ОРМ, в том числе ограничивающих конституционные права граждан[2]. Здесь же отмечается, что у оперативных и следственных подразделений, как правило, разные позиции относительно достаточности данных для возбуждения уголовного дела по ст. 210 УК РФ.

[1] По информации прокуратуры г. Москвы.

[2] *Васильева М.П., Кобелев А.Л.* Особенности прокурорского надзора за оперативно-розыскной деятельностью при раскрытии и расследовании преступлений, связанных с деятельностью организованного преступного сообщества // Прокурорский надзор за исполнением законов в оперативно-розыскной деятельности: сб. материалов по обмену опытом: в 2 ч. М.: Акад. Ген. прокуратуры Рос. Федерации, 2011. С. 1. С. 36.

Несогласованность действий приводит к тому, что оперативные сотрудники преждевременно прекращают разработку либо ограничиваются некоторыми видами ОРМ, которые лишь подтверждают основной вид преступной деятельности, не закрепляя признаки преступного сообщества[1].

Например, по информации прокуратуры Саратовской области, в результате проведенного комплекса ОРМ на территории г. Москвы, Московской области и Ртищевского района Саратовской области пресечена деятельность межрегионального организованного преступного сообщества, специализирующегося на совершении мошеннических действий в сфере интернет-покупок.

Согласно информационному письму Генеральной прокуратуры Российской Федерации от 15.05.2023 № 12-17-2023, принимая решение об оправдании подсудимых по ст. 210 УК РФ, суды, как правило, указывают на неполноту предварительного следствия, а именно недоказанность структурированности преступной группы, отсутствие самостоятельного функционально и (или) территориально обособленных подразделений, а также других предусмотренных ч. 4 ст. 35 УК РФ признаков. Прокурорам предписано по делам указанной категории обеспечить эффективное взаимодействие с органами, осуществляющими предварительное следствие и ОРД[2].

Помимо ст. 210 УК РФ осуществляющие ОРД органы должны ориентироваться на возможную связь преступлений в сфере ИТТ с преступлениями, предусмотренными ч. 1 ст. 200^1 УК РФ о контрабанде наличных денежных средств и (или) денежных инструментов, ч. 1 ст. 205 УК РФ об акте терроризма, а равно о заведомо ложных сообщениях об акте терроризма (ст. 207 УК РФ), ст. 205^3 УК РФ об участии в террористическом сообществе, ст. 222 УК РФ о незаконном приобретении, передаче, сбыте, хранении, перевозке, пересылке или ношении оружия, основных частей огнестрельного оружия, боеприпасов, ст. 226^1 УК РФ о контрабанде сильнодействующих, ядовитых, отравляющих, взрывча-

[1] *Васильева М.П., Кобелев А.Л.* Указ. соч. С. 36.

[2] Информационное письмо заместителя Генерального прокурора РФ И.В. Ткачева от 15.05.2023 № 12-17-2023 «О результатах анализа причин, послуживших основанием к вынесению судами оправдательных приговоров и решений о прекращении уголовных дел о преступлениях, предусмотренных статьями 210 и 210^1 Уголовного кодекса Российской Федерации».

тых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных устройств, боеприпасов, иного вооружения, иной военной техники, а также сырья, материалов, оборудования, технологий, научно-технической информации или результатов интеллектуальной деятельности, которые могут быть использованы при создании вооружения или военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов, ст. 228^1 УК РФ о незаконном производстве, сбыте или пересылке наркотических средств, психотропных веществ или их аналогов, а также незаконном сбыте или пересылке растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, ст. 229^1 УК РФ о контрабанде наркотических средств, психотропных веществ, их прекурсоров или аналогов, растений, содержащих наркотические средства, психотропные вещества или их прекурсоры, либо их частей, содержащих наркотические средства, психотропные вещества или их прекурсоры, инструментов или оборудования, находящихся под специальным контролем и используемых для изготовления наркотических средств или психотропных веществ, ч. 2 ст. 281^3 УК РФ об участии в диверсионном сообществе, ч. 2 ст. 282^1 УК РФ об участии лица в экстремистском сообществе, ч. 1 ст. 282^3 УК РФ о предоставлении или сборе средств либо оказании финансовых услуг, заведомо предназначенных для финансирования организации, подготовки совершения хотя бы одного из преступлений экстремистской направленности либо для обеспечения деятельности экстремистского сообщества или экстремистской организации и др.

При этом каждое из приведенных противоправных деяний имеет свою специфику при квалификации, сборе доказательств и проведении процессуальных действий.

К примеру, на основании примечания 2 к ст. 282^1 УК РФ под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении ка-

кой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ и п. «е» ч. 1 ст. 63 УК РФ.

Уголовная ответственность по ч. 1 ст. 205 УК РФ предусмотрена за совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями.

Пленум Верховного Суда Российской Федерации разъясняет, что совершение взрыва, поджога или иных действий подобного характера влечет уголовную ответственность по ст. 205 УК РФ в тех случаях, когда установлено, что указанные действия имели устрашающий население характер и создавали опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий. Устрашающими население могут быть признаны такие действия, которые по своему характеру способны вызвать страх у людей за свою жизнь и здоровье, безопасность близких, сохранность имущества и т.п. Опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий должна быть реальной, что определяется в каждом конкретном случае с учетом места, времени, орудий, средств, способа совершения преступления и других обстоятельств дела (данных о количестве людей, находившихся в районе места взрыва, о мощности и поражающей способности использованного взрывного устройства и т.п.)[1].

В силу абз. 2 п. 22[1] постановления Пленума Верховного Суда Российской Федерации от 28.06.2011 № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» финансированием экстремистской деятельности следует признавать наряду с оказанием финансовых услуг предоставление или сбор не только денежных средств (в наличной или

[1] Постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» (п. 2).

безналичной форме), но и материальных средств (например, предметов обмундирования, экипировки, средств связи) с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений экстремистской направленности, либо для финансирования или иного материального обеспечения лица в целях совершения им хотя бы одного из этих преступлений, либо для обеспечения деятельности экстремистского сообщества или экстремистской организации (например, систематические отчисления или разовый взнос в общую кассу, приобретение недвижимости или оплата стоимости ее аренды, предоставление денежных средств, предназначенных для подкупа должностных лиц).

Определенные трудности наблюдаются при выявлении и раскрытии преступлений, предусмотренных ст. 207 УК РФ. Согласно информационному письму от 18.05.2022 интернет-ресурсы и средства телефонии все чаще задействуются с целью направления заведомо ложных сообщений об актах терроризма.

Данные преступления наносят существенный ущерб интересам государства и всего общества, приводят к нарушению нормальной деятельности органов МВД России и ФСБ России, а также работы организаций, предприятий и учреждений, срыву массовых мероприятий, порождают у граждан чувство опасения за свою безопасность, причиняют значительный имущественный вред. Массовое направление заведомо ложных сообщений о готовящихся взрывах объективно свидетельствует о том, что целью преступного деяния является дестабилизация деятельности органов власти путем масштабного отвлечения их сил и средств, что является квалифицирующим признаком, предусмотренным ч. 3 ст. 207 УК РФ.

Количество заведомо ложных сообщений о террористических актах в последние годы возросло многократно. Это обусловлено тем, что для распространения подобных сообщений все чаще задействуются интернет-ресурсы и средства телефонной связи, позволяющие преступникам скрывать свою личность, исполь-

зуются анонимные почтовые сервисы, подменные телефонные номера, IP-телефония[1].

При установлении фактов использования для отправки электронных писем о «лжеминировании» сервисов электронной почты, находящихся на территории Российской Федерации (Яндекс, Мэйл.ру, Рамблер и пр.), в указанные организации направляются соответствующие запросы. При этом получаемые ответы на запросы от российских почтовых сервисов свидетельствуют о том, что их владельцы используют средства обеспечения анонимности (TOR-сети, VPN-сервисы и пр.), находящиеся за пределами Российской Федерации. Нередко иностранные компании и правоохранительные органы отказывают в предоставлении значимой информации.

Изложенное свидетельствует о необходимости направления поручений в соответствующие подразделения органов, осуществляющих ОРД, а также запросы в подразделения Интерпола, что, однако, не всегда обеспечивается при осуществлении предварительного расследования таких преступлений.

Учитывая, что в ФСБ России и Роскомнадзоре существует алгоритм блокировки электронных почтовых адресов, с которых ранее направлялись заведомо ложные сообщения о минировании, информация об электронных почтовых адресах в рабочем порядке передается в УФСБ для инициирования блокировки данных адресов через центральный аппарат ФСБ России. Вместе с тем эффективность данного порядка реагирования осложнена тем, что такие сообщения приходят каждый раз с разных электронных почтовых адресов.

Также полезной практикой представляется проведение ежемесячных сверок размещенных в интегрированном банке данных федерального уровня (подсистеме ИБД-Ф «АБД-Центр») сведений о текстах заведомо ложных сообщений (их дословное содержание), адресах электронных почтовых ящиков, абонентских номерах телефонов по уголовным делам, возбужденным по ст. 207 УК РФ.

---

[1] *Состояние* законности и правопорядка в Российской Федерации и работа органов прокуратуры. 2022 год: информ.-аналит. записка / под общ. ред. И.М. Мацкевича. М.: Ун-т прокуратуры Рос. Федерации, 2023. С. 139.

По преступлениям анализируемого вида особое внимание необходимо уделять вопросам изобличения всех возможных участников преступной деятельности, а также установления у них имущества, на которое может быть наложен арест[1].

Прокуроры приводят положительные примеры работы на данном направлении.

По информации прокуратуры Свердловской области, в 2022 г. по результатам изучения дел оперативного учета в сфере незаконного оборота наркотиков и направления постановлений в порядке, предусмотренном п. 2 ч. 2 ст. 37 УПК РФ, органами внутренних дел по рассекреченным материалам ОРД возбуждено четыре уголовных дела по ст. 174[1] УК РФ.

Установлено, что согласно результатам ОРМ и финансового расследования Росфинмониторинга на банковские счета Б. и П. через платежные системы «Visa Direct», «MC MONEYSEND», «ONECLICK-MONEY», «P2P», «MR CARDHOLDER», «Open.ru», «C2C RB-SITE E2E MOSCOW» из неустановленных источников (криптообменников) поступали денежные средства, которые в дальнейшем переводились на банковские счета физических лиц, зарегистрированных на территориях других субъектов Российской Федерации. После чего указанные денежные средства вводились в наличный оборот через банкоматы кредитных организаций г. Екатеринбурга. Всего совершено 354 противоправных финансовых операции. Сумма легализованных денежных средств составила 2 млн 700 тыс. 470 руб.[2]

Учитывая, что выявление и раскрытие преступлений, а также установление имущества, необходимого для обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий, или имущества, подлежащего конфискации, являются непосредственными задачами, предусмотренными ст. 2 закона об ОРД, эти вопросы должны иметь приоритетное значение для прокуроров при осуществлении прокурорского надзора за исполнением законов органами, осуществляющими ОРД.

Учитывая характер рассматриваемых преступлений, совершение которых сопряжено с оставлением цифровых следов каждым из участников преступной группы, особую актуальность при-

[1] Протокол заседания межведомственной рабочей группы по вопросам профилактики и борьбы с кражами и мошенничествами, совершенными с использованием ИТТ на территории Челябинской области, от 25.03.2021 (далее – Протокол межведомственной рабочей группы от 25.03.2021 на территории Челябинской области).

[2] По информации прокуратуры Свердловской области.

обретает качественное и эффективное наполнение и взаимодействие с подсистемой «Дистанционное мошенничество» ИБД-Ф[1].

Следует отметить, что в настоящее время возможности данной системы значительные и позволяют осуществлять поиск необходимой информации по многим параметрам, реквизитам и продолжают совершенствоваться. Алгоритм внесения данных в подсистему позволяет формировать сведения начиная с регистрации сообщения о преступлении, заканчивая сведениями, установленными в ходе предварительного расследования, а также в процессе осуществления ОРД по результатам их легализации. При этом важным элементом являются сведения данной подсистемы, которые могут способствовать выявлению преступлений, предусмотренных ст. 210 УК РФ. Важность при этом играет возможность выявления признаков серийных преступлений, в том числе с межрегиональными совпадениями, осуществление поиска раскрытых уголовных дел, имеющих пересечение по серийности преступлений в разных регионах.

К примеру, по данным прокуратуры Саратовской области, при проверке информации, содержащейся в базе данных, по уголовному делу, возбужденному в отношении неустановленного лица по признакам преступления, предусмотренного ч. 3 ст. 159 УК РФ, выявлены совпадения по способу совершения с четырьмя уголовными делами, возбужденными на территории г. Саратова, и одним уголовным делом, преступление по которому раскрыто на территории Тульской области, по обвинению гражданина Украины, задержанного на территории Донецкой Народной Республики. В результате раскрыты пять эпизодов мошеннических действий в отношении жителей г. Саратова, уголовные дела соединены в одном производстве, инициирована передача уголовного дела из правоохранительных органов Тульской области в СУ УМВД России по г. Саратову для соединения и дальнейшего расследования.

[1] Приказ МВД России от 29.12.2020 № 925 «Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество ПТК «ИБД-Ф» (далее – приказ МВД России № 925).

Раздел 3. Прокурорский надзор за исполнением законов органами, осуществляющим дознание и предварительное следствие при приеме, регистрации и разрешении сообщений о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий

Согласно позиции 80,7% прокуроров, участвующих в социологическом опросе, при проведении процессуальной проверки сообщений о преступлениях рассматриваемого вида имеются особенности.

По данным прокуратуры Челябинской области, в целях создания препятствий правоохранительным органам для раскрытия подобных преступлений злоумышленники меняют сотовые телефоны, места своего нахождения, оформляют сим-карты и открывают счета в банках на подставных лиц, используют анонимные электронные кошельки, прокси-серверы и различные программы, скрывающие фактические IP-адреса и места нахождения, привлекают лиц, не осведомленных о противоправности их действий, применяют иные способы конспирации.

Порядок проверки сообщений о преступлениях в сфере ИТТ регламентирован положениями УПК РФ, ведомственных нормативных актов.

Прежде всего, при осуществлении прокурорского надзора за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях, важное значение имеет указание Генеральной прокуратуры Российской Федерации № 401/11, МВД России № 2 от 19.06.2023 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности», включающее Перечень № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Так, в соответствии с Протоколом заседания межведомственной рабочей группы в прокуратуре Челябинской области от 25.05.2022 прокурорам предписано проводить проверки обоснованности отнесения преступлений к совершенным с использованием ИТТ в соответствии с требованиями, отраженными в перечне.

Специфика начала процессуальной проверки сообщений о преступлениях рассматриваемого вида обусловлена общими положениями УПК РФ, которые дифференцируют порядок проверки сообщений о преступлениях, уголовное преследование за совершение которых осуществляется в частном, частно-публичном и публичном порядке (ст. 20 УПК РФ).

В силу ч. 4 ст. 20 УПК РФ руководитель следственного органа, следователь, а также с согласия прокурора дознаватель возбуждают уголовное дело о любом преступлении, указанном в ч. 2 и 3 ст. 20, и при отсутствии заявления потерпевшего или его законного представителя, если данное преступление совершено в отношении лица, которое в силу зависимого или беспомощного состояния либо по иным причинам не может защищать свои права и законные интересы. К иным причинам относятся также случаи совершения преступления лицом, данные о котором не известны.

На основании ч. 3 ст. 20 УПК РФ к уголовным делам частно-публичного обвинения не могут быть отнесены уголовные дела о преступлениях, предусмотренных ст. 159–159^3, 159^5, 159^6, 160, 165, ч. 1 ст. 176, ст. 177, 180, 185^1, ч. 1 ст. 201 УК РФ, в случаях, если преступлением причинен вред интересам государственного или муниципального унитарного предприятия, государственной корпорации, государственной компании, коммерческой организации с участием в уставном (складочном) капитале (паевом фонде) государства или муниципального образования либо если предметом преступления явилось государственное или муниципальное имущество.

В соответствии со ст. 23 УК РФ, если деяние, предусмотренное гл. 23 УК РФ, причинило вред интересам исключительно коммерческой или иной организации, не являющейся государственным или муниципальным предприятием либо организацией с участием в уставном (складочном) капитале (паевом фонде) государства или муниципального образования, и не причинило вреда интересам других организаций, а также интересам граждан, общества или государства, то уголовное дело возбуждается по заявлению руководителя данной организации или с его согласия. Причинение вреда интересам организации с участием в уставном (складочном) капитале (паевом фонде) государства или муници-

пального образования одновременно влечет за собой причинение вреда интересам государства или муниципального образования[1].

На основании п. 15 разд. III Положения о едином порядке регистрации уголовных дел и учета преступлений – приложения № 2 к приказу Генеральной прокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29.12.2005 № 39/1070/1021/253/780/353/399 (далее – приказ о едином учете) учет преступлений по уголовным делам частного обвинения, рассмотренным мировыми судьями (районными судами в случае принятия ими заявлений по составам частного обвинения), осуществляется в ИЦ, на территории оперативного обслуживания которых они находятся. В случаях производства предварительного расследования по данной категории уголовных дел преступления учитываются органом, производящим дознание или предварительное следствие.

Важное значение в данном случае также имеют Методические рекомендации о порядке рассмотрения органами внутренних дел заявлений о преступлениях, уголовное преследование по которым осуществляется в частном порядке, а также осуществлении прокурорского надзора за законностью принимаемых решений, разработанные Генеральной прокуратурой Российской Федерации и МВД России в 2014 г.

По результатам надзорной деятельности прокуроры сообщают о фактах необоснованного списания поступивших сообщений о преступлениях рассматриваемого вида в специальных номенклатурные дела.

Так, по информации прокуратуры Магаданской области, при проверке прокурором специальных номенклатурных дел отдела внутренних дел установлено необоснованное списание сообщения, содержащего признаки преступления, предусмотренного ч. 3 ст. 30, ст. 159 УК РФ, требующего принятия решения о возбуждении уголовного дела по факту обращения Ч., которая сообщила о попытке побудить ее оформить в банках два кредита на сумму 500 тыс. руб. Выполняя указания неуста-

[1] Более подробно эти вопросы раскрыты в постановлении Пленума Верховного Суда РФ от 29.06.2021 № 21 «О некоторых вопросах судебной практики по делам о преступлениях против интересов службы в коммерческих и иных организациях (статьи 201, 201[1], 202, 203 Уголовного кодекса Российской Федерации)».

новленных лиц, Ч. подала заявки в банки, в ходе рассмотрения которых работник одного из банков сообщил о совершении в отношении нее мошеннических действий.

Согласно абз. 6 п. 1.2 приказа Генерального прокурора Российской Федерации от 17.09.2021 № 544 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия» прокурорам предписано, выявляя нарушения порядка приема, регистрации и разрешения сообщений о преступлениях, добиваться их устранения, а при обнаружении признаков должностного правонарушения принимать меры к привлечению виновных лиц к ответственности, в том числе уголовной.

Прокуроры отмечают, что анализ материалов уголовных дел свидетельствует о том, что к предварительному расследованию не привлекаются специалисты, обладающие достаточными познаниями в сфере ИТТ. Из числа прокуроров, участвующих в социологическом опросе, 98,2% сообщили о значимости помощи специалиста для раскрытия преступлений данного вида.

В прокуратуре Челябинской области сообщили, что участие специалистов необходимо уже на самых ранних стадиях для подготовки запросов в организации, оказывающие услуги связи, при анализе поступающих ответов, планировании на их основании дальнейших следственных действий.

В частности, согласно ст. 26 закона о банках справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, Фонду пенсионного и социального страхования Российской Федерации и органам принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия руководителя следственного органа – органам предварительного следствия по делам, находящимся в их производстве.

К неполноте проверки приводят также следующие обстоятельства: в материалах проверки отсутствует информация об IMEI мобильных телефонов, в которых использовались SIM-карты с установленными абонентскими номерами; об IMSI-номере, ис-

пользуемом данным абонентским номером; о месторасположении офиса по обслуживанию и продаже SIM-карты, с которой совершен звонок преступником (при установлении офиса запрашивают сведения о приобретателе карты, истребуют запись камер видеонаблюдения); комплексный анализ телефонных соединений проверяемых лиц, его формальный или бессистемный характер[1].

Не направляются запросы владельцам социальных сетей с целью установления источника создания и администрирования учетной записи (аккаунта) в социальных сетях, запросы на сайты (электронные торговые площадки) по оказанию услуг или продаже товаров о предоставлении информации об объявлениях, где был указан интересующий следствие абонентский номер в качестве контактного, запросы в e-mail.ru о предоставлении информации о профиле (при этом регистрация в сети «Интернет» предусматривает наличие электронной почты), запросы интернет-провайдерам об установлении MAC-адресов ноутбуков, сетевых карт (встроенных сетевых интерфейсов) компьютерной техники, а также Wi-Fi-роутеров, с использованием которых осуществлялся доступ к сети «Интернет»2.

Прежде всего, результаты изучения уголовных дел о преступлениях рассматриваемого вида свидетельствуют о том, что органами предварительного расследования производится осмотр места происшествия (места нахождения банкоматов) с участием самого заявителя. При этом зачастую заявители контактируют с работниками банков, а также третьими лицами, осуществляющими посреднические функции.

Согласно ч. 1 ст. 176 УПК РФ осмотр места происшествия, местности, жилища, иного помещения, предметов и документов производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела. В силу ч. 3 ст. 177 УПК РФ изъятию подлежат только те предметы, которые могут иметь отношение к уголовному делу.

Соответственно в данном случае в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела, на территориях банков могут быть

[1] *Методика* борьбы с компьютерными преступлениями: пособие / К.В. Камчатов и др.; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. М., 2020. С. 89.
[2] Там же.

изъяты записи с камер видеонаблюдения, а также другие источники информации, позволяющие установить обстоятельства совершения преступления.

При необходимости изъятия документов, содержащих банковскую тайну, следует учитывать положения закона о банках, а также п. 7 ч. 2 ст. 29 УПК РФ, свидетельствующие о необходимости получения судебного решения в общем порядке.

В соответствии с ч. 3 ст. 164^1 УПК РФ следователь в ходе производства следственного действия вправе осуществить копирование информации, содержащейся на электронном носителе информации. В протоколе следственного действия должны быть указаны технические средства, примененные при осуществлении копирования информации, порядок их применения, электронные носители информации, к которым эти средства были применены, и полученные результаты. К протоколу прилагаются электронные носители информации, содержащие информацию, скопированную с других электронных носителей информации в ходе производства следственного действия.

Более того, зачастую заявители самостоятельно истребуют от операторов сотовой связи и банков документы, которые не содержат необходимых реквизитов (печать и т.д.) и нуждаются в интерпретации экспертом (специалистом).

Заявитель Б. в ходе опроса сообщил, что на номер в мессенджере «WhatsApp» позвонил неизвестный и сообщил, что он является представителем службы безопасности ПАО «ВТБ-банк», на имя заявителя оформлен кредит, идет проверка по данному факту и необходимо оформить встречный кредит для того, чтобы вернуть эти деньги в банк на резервную ячейку. В дальнейшем Б. поехал в банк, в котором оформил кредит. Все это время неизвестный находился на связи. Он сказал, что Б. нужно купить смартфон в салоне сотовой связи, что тот и сделал, продиктовал ему, как установить приложение для удаленного доступа к сотовому телефону, затем настроил ему приложение для бесконтактной оплаты мобильным устройством. Далее неизвестный велел Б. направиться к банкомату, произвести снятие денежных средств с банковской карты и перевести их по реквизитам, которые он указал. Переводы денежных средств осуществлялись в банкоматах. Общая сумма переведенных денежных средств составила 230 тыс. руб.

Из материалов уголовного дела также следовало, что через мобильное приложение инициирована заявка на выдачу потребительского кредита. По заявке принято положительное решение и представлены индивидуальные условия кредитования по договору в электронном виде. На но-

мер телефона было направлено смс-сообщение, содержащее пароль, посредством указания которого в приложении было подтверждено согласие с индивидуальными условиями кредитования простой электронной подписью. В результате между банком и заявителем заключен договор кредитования.

Несмотря на то что заявителем Б. были представлены банковские выписки и выписки о телефонных соединениях от операторов сотовой связи, в дальнейшем официально понадобилось истребование соответствующих документов с соблюдением УПК РФ[1].

В ходе проверки сообщений о преступлениях в сфере ИТТ органам, осуществляющим ОРД, в порядке, предусмотренном ч. 1 ст. 144 УПК РФ, возможно давать поручения в целях установления необходимых сведений о принадлежности номеров сотовых телефонов, банковских карт, банковских счетов, на которые были совершены транзакции, связанные с переводом денежных средств, данных о владельцах расчетных счетов с указанием ФИО, места регистрации и других важных сведений, позволяющих их установить, локализации звонков (биллинга) и компании сотовой связи, которая изначально нарушила требования закона о связи, данных, подтверждающих обналичивание денежных средств, их дальнейшее движение, подтвердить возможную контрабанду наличных денежных средств.

Необходимо также учитывать имевшую место практику совершения преступлений по признакам «колл-центров» в исправительных учреждениях, а также лиц, которые совершали данные противоправные деяния.

Генеральная прокуратура Российской Федерации сообщала о производимых в учреждениях ФСИН России масштабных изъятиях предметов, запрещенных к обороту, включая наркотики и сотовые телефоны.

Прокуроры отмечают, что при установлении нарушений закона о связи и закона о платежной системе одним из условий, способствующих совершению преступлений указанного вида, является бездействие должностных лиц уголовно-исполнительной системы по пресечению фактов поступления запрещенных предметов на территории пенитенциарных учреждений и по установлению каналов их поступления[2].

---

[1] По материалам уголовного дела, изученного в прокуратуре Московской области.

[2] По информации прокуратуры Челябинской области.

На заседании коллегии ФСИН России отмечено, что служба начала вести радиомониторинг для поиска нелегальных телефонов в исправительных колониях. Для установления абонентских номеров, незаконно используемых на территории учреждений уголовно-исполнительной системы, организовано проведение оперативно-технических мероприятий с применением специализированного оборудования радиомониторинга. Работа идет во взаимодействии с подразделениями МВД России и ФСБ России, она уже позволила выявить более 27 тыс. абонентских номеров на территории колоний. Всего по итогам 2020 г. в исправительных учреждениях было найдено и изъято почти 66 тыс. мобильных устройств, что на 20% больше, чем годом раньше[1].

Сотрудникам ФСИН России предоставлены учетные записи для регистрации в качестве пользователей подсистемы ИБД-Ф «Дистанционное мошенничество», осуществлены мероприятия по обеспечению сетевой связанности оборудования МВД России и ФСИН России.

Вопрос о соблюдении правил подследственности преступлений в сфере ИТТ является значимым. Почти 60% прокуроров, участвующих в социологическом опросе, сообщили о трудностях с определением подследственности преступлений в сфере ИТТ.

Отмечается, что киберпреступления имеют смешанную подследственность, т.е. расследуются следственными подразделениями выявившего их органа[2]. Такой подход соответствует абз. 2 п. 7 разд. III Положения о едином порядке регистрации уголовных дел и учета преступлений – приложению № 2 к приказу о едином учете, согласно которому в случае, если не представляется возможным определить место совершения преступления, оно подлежит учету по месту его выявления.

Прокуроры приводят факты необоснованной передачи сообщений о преступлениях по подследственности. Факты необоснованной передачи сообщений о преступлениях в сфере ИТТ по

---

[1] ФСИН ввела радиомониторинг для выявления «call-центров» в колониях. URL: https://www.rbc.ru/rbcfreenews/604b59ab9a7947255fa9bec8?ysclid=llb3szmpnw104393189 (дата обращения: 14.08.2023).

[2] *Лебедева А.А.* Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6.

подследственности встречаются в деятельности прокуратур субъектов Российской Федерации[1].

Например, по информации прокуратуры Магаданской области, сформулированный следователем следственного отдела по г. Магадану, вывод о необходимости передачи сообщения о преступлении по территориальности в УМВД России по Новосибирской области не основывался на материалах проверки. В связи с этим принятое процессуальное решение отменено прокурором, материал возвращен для проведения проверочных мероприятий.

Неправильная пересылка в отмеченных случаях приводит к многократной пересылке материалов процессуальных проверок и уголовных дел зачастую по формальным, надуманным основаниям, по территориальной и ведомственной подследственности, что не только увеличивает латентность такого рода деяний, но и нарушает конституционные права граждан на разумный срок уголовного судопроизводства, а также ведет к утрате доказательств, и следовательно, уменьшает вероятность установления всех обстоятельств и совершивших преступления лиц[2].

Более того, в информационном письме Генеральной прокуратуры Российской Федерации от 10.06.2014 № 16-17-2014/Ип3945-14 «О состоянии законности при передаче органами дознания и органами предварительного расследования сообщений о преступлениях по территориальной подследственности» указано, что фактическое непроведение проверочных мероприятий ввиду необоснованной передачи материалов из одного органа в другой, длительное затягивание решения вопроса о возбуждении уголовного дела свидетельствуют о преднамеренном характере действий сотрудников полиции по укрытию преступлений от учета, об их стремлении таким образом повысить показатель раскрываемости, что привело к грубым нарушениям принципа осуществления уголовного судопроизводства в разумный срок и права на доступ потерпевших к правосудию, осложнило собирание доказательств по уголовным делам.

---

[1] По информации прокуратуры г. Москвы.

[2] Информационное письмо Генеральной прокуратуры РФ и МВД России от 08.02.2022 № 36-49-22/1/1322 «О практике рассмотрения сообщений о преступлениях, совершаемых с использованием информационно-коммуникационных технологий, и об иных проблемных вопросах» (далее – совместное письмо от 08.02.2022).

Для разрешения сложившейся ситуации в феврале 2022 г. подписано совместное письмо от 08.02.2022. В нем предусмотрено, что в соответствии с ч. 1 ст. 145 УПК РФ по результатам рассмотрения сообщения о преступлении должно быть принято одно из следующих решений: о возбуждении уголовного дела, о передаче сообщения по подследственности или об отказе в возбуждении уголовного дела.

Вместе с тем стадия проверки сообщения о преступлении, совершенном дистанционным способом, ограничена имеющимися в распоряжении правоохранительных органов пояснениями заявителя или очевидцев (как правило, родственников), полученными из банковских учреждений материалами (чеками и выписками по счету), а также информацией, сохранившейся в средствах связи и компьютерной технике, что на первоначальном этапе не позволяет в полной мере сделать верный вывод обо всех обстоятельствах и нередко приводит к спорам о подследственности.

Рассматриваемые деяния нередко имеют межрегиональный или трансграничный характер, совершаются дистанционным способом при обеспечении анонимности виновного, что усложняет своевременное установление не только отмеченных, но и иных обстоятельств по делу.

Кроме того, в настоящее время не все кредитно-финансовые организации имеют территориальные подразделения, где владельцем денежных средств открывается счет либо ведется учет электронных денежных средств.

При таких обстоятельствах трудно достоверно установить место совершения преступления исходя только из местонахождения подразделения финансово-кредитной организации, в котором потерпевшим был открыт счет или велся учет электронных денежных средств, либо был открыт счет подозреваемого (обвиняемого) или производилось снятие наличных денежных средств, а равно места регистрации абонента сотовой связи или интернет-услуг.

В связи с изложенным в указанных ситуациях предлагается исходить из следующего.

При принятии решений по сообщениям о хищениях денежных средств, совершенных с использованием ИТ-технологий, а также при оценке их обоснованности следует руководствовать-

ся прежде всего необходимостью соблюдения разумных сроков уголовного судопроизводства и баланса прав его участников. Для этого в указанных в ст. 152 УПК РФ случаях предусмотрена возможность альтернативного определения подследственности: по месту совершения большинства преступных деяний или наиболее тяжкого из них, по месту нахождения обвиняемого или большинства свидетелей, а также по месту жительства или пребывания потерпевшего.

Таким образом, проведение проверки по сообщениям о преступлениях, предусмотренных ст. 158, 159–159^3, 159^5, 159^6, 163 УК РФ, совершенных с использованием платежных карт, средств мобильной связи, информационно-коммуникационной сети «Интернет» и иными дистанционными способами, следует осуществлять территориально по месту их первичной регистрации. При этом решение о возбуждении уголовного дела в случае наличия повода и достаточных оснований целесообразно принимать в органе внутренних дел, в который поступило соответствующее сообщение.

Дальнейшая передача уголовного дела в установленном ч. 5 ст. 152 УПК РФ порядке для направления по подследственности возможна лишь после производства неотложных следственных действий.

В целях недопущения перенаправления такого рода сообщений о преступлениях либо уголовных дел по территориальности по формальным либо надуманным основаниям прокурорам надлежит реализовывать приоритетные полномочия в разрешении вопросов подследственности.

Порядок осуществления расследования уголовных дел рассматриваемой категории также должен исходить из установленных ч. 4 ст. 152 УПК РФ правил территориальной подследственности, которые в отсутствие специальных на то указаний в уголовно-процессуальном законодательстве не требуют принятия специального решения о производстве предварительного расследования по месту нахождения обвиняемого, большинства свидетелей или потерпевших.

Исходя из характера дистанционных посягательств, которые требуют неотложных мер для их пресечения, только такое правоприменение позволит обеспечить достижение целей неотврати-

мости уголовного наказания, в случае если это не оказывает влияния на относимость, достоверность, допустимость и достаточность собранных доказательств по уголовному делу и не влечет нарушение прав обвиняемого (подозреваемого) и потерпевшего.

Аналогичный подход отражен в информационном письме заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 03.11.2015 № 36-11-2015 «Об определении места производства предварительного расследования мошенничеств, совершенных с использованием телефонной (сотовой) связи», а также в приказе МВД России от 03.04.2018 № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений».

Однако в данном случае возникают другие проблемы, которые обусловлены возложением нагрузки по процессуальной проверке (предварительному расследованию) преступлений в сфере ИТТ фактически на один орган – МВД России. Учитывая, что специализированные подразделения по расследованию преступлений в сфере ИТТ созданы не только в МВД России[1], но и в СК России[2], можно вести речь о перераспределении нагрузки при реализации прокурором полномочий, предусмотренных п. 12 ч. 2 ст. 37 УПК РФ. Такая практика должна учитывать положения информационного письма Генеральной прокуратуры Российской Федерации от 06.04.2023 № 69-09-2023 «О недостатках, допускаемых прокурорами при реализации полномочий по изъятию уголовных дел из производства органов дознания и их передаче следователям Следственного комитета Российской Федерации».

Кроме того, следователям и дознавателям при учете перечня № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере компьютерной информации[3], необходимо обращаться в подсистему «Дистанционное мошенничество» ИБД-Ф с целью

---

[1] В структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий. URL: https://mvdmedia.ru/news/official/v-strukture-mvd-rossii-sozdano-upravlenie-po-organizatsii-borby-s-protivopravnym-ispolzovaniem-infor/ (дата обращения: 15.08.2023).

[2] Интервью руководителя отдела по расследованию киберпреступлений и преступлений в сфере высоких технологий СК России Константина Комарды ИА «ТАСС». URL: https://sledcom.ru/press/interview/item/1529946/?print=l (дата обращения: 15.08.2023).

[3] Совместное указание от 19.06.2023.

проверки совпадений по искомым данным. В соответствии с подп. 8.1 и 8.2 п. 8 разд. III Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество» программно-технического комплекса интегрированного банка данных коллективного пользования федерального уровня – приложения к приказу МВД России от 29.12.2020 № 925 основаниями для постановки объектов учета в подсистему и для корректировки соответствующих данных являются регистрация в установленном порядке сообщения (заявления) о преступлениях, совершенных дистанционным способом с использованием ИТТ, постановление о возбуждении уголовного дела по факту совершения преступления дистанционным способом с использованием ИТТ.

Представляется, что в настоящее время при, казалось бы, ясной определенности в части подследственности преступлений в сфере ИТТ в ряде случаев ее необходимо дополнительно определять. В конкретных ситуациях можно вести речь о применении ч. 3 ст. 12 УК РФ, согласно которой иностранные граждане и лица без гражданства, не проживающие постоянно в Российской Федерации, совершившие преступление вне пределов Российской Федерации, подлежат уголовной ответственности по УК РФ в случаях, если преступление направлено против интересов Российской Федерации либо гражданина Российской Федерации или постоянно проживающего в Российской Федерации лица без гражданства.

Распространение уголовной юрисдикции Российской Федерации как в отношении преступлений, совершенных на юго-востоке Украины, так и в других ее областях и городах, основывается на совокупности принципов экстерриториальной юрисдикции, признаваемых современным международным правом, – пассивного и активного персональных, защитного и универсального, имеющих внутригосударственное нормативное закрепление в ст. 12 УК РФ[1].

[1] *Литвишко П.А.* Особенности реализации Следственным комитетом Российской Федерации экстерриториальной уголовной юрисдикции в отношении международных и транснациональных преступлений на Украине // Следственный комитет Рос. Федерации: место и роль в обеспечении национальной безопасности гос-ва: сб. ст. Общерос. науч. практ. конф. (Москва, 17 февр. 2016 г.) / отв. ред. О.И. Александрова. М., 2016. С. 57.

В силу абз. 3 п. 1.2 указания Генерального прокурора Российской Федерации от 19.12.2011 № 433/49 «Об усилении прокурорского надзора за исполнением требований закона о соблюдении подследственности уголовных дел» в случае очевидности подследственности прокурорам предписано незамедлительно передавать сообщение для дальнейшей процессуальной проверки в соответствующий орган предварительного расследования или должностному лицу, уполномоченному на основании ст. 151 УПК РФ производить дознание или предварительное следствие.

Безусловно, что на данном этапе также необходимо межведомственное взаимодействие. Согласно Методическим рекомендациям «Вопросы взаимодействия и прокурорского надзора за организацией расследования и раскрытия тяжких и особо тяжких преступлений против личности, в том числе прошлых лет» в субъектах действуют межведомственные контрольно-аналитические рабочие группы по противодействию экстремизму, координационно-аналитические, оперативно-следственные группы, межведомственные группы, межведомственные рабочие группы по противодействию экстремизму, в работе которых принимают участие наиболее опытные сотрудники следственных управлений Следственного комитета Российской Федерации, подразделений ФСБ России и МВД России, а также органов прокуратуры[1]. При учете схожести обстоятельств совершения преступлений, связанных с заведомо ложными сообщениями об акте терроризма и дистанционными мошенничествами, такое межведомственное взаимодействие актуально на этапе проверки (предварительного расследования) указанных преступлений.

Типичными нарушениями законов при проведении процессуальных проверок является их неполнота, обусловленная отсутствием у сотрудников необходимых познаний в информационно-телекоммуникационной сфере, позволяющих эффективно производить необходимые процессуальные действия, своевременно направлять мотивированное запросы в адрес организаций, которые располагают значимыми сведениями об обстоятельствах совершенных преступлений.

[1] Письмо заместителя Генерального прокурора РФ Гриня В.Я. от 20.12.2017 № 36-11-2017.

В правоприменительной практике возникают различные ситуации, требующие принятия мер прокурорского реагирования.

Так, по материалам прокуратуры Челябинской области, сотрудник полиции не принял заявление о хищении 5488 руб. с расчетного счета ПАО «Сбербанк России» по причине того, что к заявлению не была приложена выписка из банка. В дальнейшем по данному факту проведена служебная проверка, по результатам которой сотруднику органов внутренних дел объявлен выговор. По результатам рассмотрения сообщения о преступлении следователем следственного отдела территориального органа внутренних дел возбуждено уголовное дело по п. «г» ч. 3 ст. 158 УК РФ.

В соответствии с аналитической справкой прокуратуры Челябинской области от 03.02.2022 в отделе полиции зарегистрировано сообщение П. о том, что неустановленное лицо вымогает денежные средства, угрожая распространением видео интимного характера посредством сети «Интернет». По результатам процессуальной проверки участковым уполномоченным полиции дважды выносились постановления об отказе в возбуждении уголовного дела по ч. 1 ст. 163 УК РФ на основании п. 2 ч. 1 ст. 24 УПК РФ, которые отменялись прокуратурой Троицкого района в связи с неполнотой проверочных мероприятий. По результатам дополнительной проверки дознавателем возбуждено уголовное дело по ч. 1 ст. 163 УК РФ.

По информации прокуратуры Магаданской области, дознавателем полиции вынесено постановление об отказе в возбуждении уголовного дела по п. «г» ч. 3 ст. 158 УК РФ на основании п. 2 ч. 1 ст. 24 УПК РФ при учете пояснений К. о том, что он совершил ряд покупок на сумму менее 1 тыс. руб., а всего на сумму 5 тыс. 702 руб. Отменяя данное постановление, прокурор указал, что покупки были совершены в короткий промежуток времени. Материал проверки направлен для решения вопроса о возбуждении уголовного дела.

Одно из ключевых нарушений – принятие незаконных решений об отказе в возбуждении уголовного дела со ссылкой на наличие гражданско-правовых отношений.

Так, 27.02.2020 Генеральная прокуратура Российской Федерации отмечала, что за последние два года правоохранительными органами Российской Федерации зарегистрировано свыше полумиллиона сообщений о преступлениях в сфере ИТТ или компьютерной информации. При этом без надлежащего разрешения в установленном УПК РФ порядке оставлена треть из них. Практически каждое девятое сообщение направлено по подследственно-

сти или территориальности, а по каждому пятому принято решение об отказе в возбуждении уголовного дела, в том числе при наличии очевидных признаков преступления[1].

С учетом данных примеров представляется, что актуальным вопросом, который возникает в практике прокурорского надзора, является вопрос о возможности возбуждения уголовного дела по ст. 159 УК РФ в случаях, когда разговор с мошенником был прерван, а конкретному физическому лицу вред не причинен.

В частности, указанный вопрос затрагивался в обращении прокуратуры Красноярского края в Главное управление по надзору за следствием, дознанием и оперативно-разыскной деятельностью Генеральной прокуратуры Российской Федерации (от 17.04.2023 № 14/2-17-2023), в котором было указано, что правоприменительная практика по данному вопросу единообразной не является. Это обусловлено тем, что в ряде случаев принимаются решения об отказе в возбуждении уголовного дела либо о приобщении заявления к материалам номенклатурного дела. В данном обращении отмечено, что правоохранительные органы ориентированы на квалификацию преступления по ч. 3 ст. 30, ст. 159 УК РФ в случае, если потерпевшему обозначена денежная сумма, подлежащая перечислению, но он ее не переводит, осознавая, что в отношении него совершается мошенничество[2].

При этом в ряде случаев прокуроры формируют практику возбуждения уголовных дел по ч. 3 ст. 30, ст. 159 УК РФ по фактам покушения на совершение телефонных мошенничеств без фактического причинения ущерба гражданам. Практически по всем уголовным делам вынесены постановления о приостановлении предварительного следствия за неустановлением лица, подлежащего привлечению в качестве обвиняемого[3].

За основу по данному вопросу можно взять абз. 2 п. 24 постановления Пленума Верховного Суда Российской Федерации от 27.12.2202 № 29 «О судебной практике по делам о краже, гра-

[1] Справка о состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации, подготовленная в Генеральной прокуратуре Российской Федерации.

[2] По материалам Генеральной прокуратуры Российской Федерации.

[3] По информации прокуратуры Ставропольского края.

беже и разбое», согласно которому, если ущерб, причиненный в результате кражи, не превышает указанного размера либо ущерб не наступил по обстоятельствам, не зависящим от виновного, содеянное может квалифицироваться как покушение на кражу с причинением значительного ущерба гражданину при условии, что умысел виновного был направлен на кражу имущества в значительном размере.

В целом по смыслу сложно подвергать сомнению, что действия мошенника, пытавшегося обмануть лицо, не образуют покушения на совершение мошенничества. Ключевой вопрос в данном случае заключается не в отсутствии последствий, связанных с причинением имущественного вреда, а совокупных обстоятельствах такого разговора.

Еще один вопрос, на который обращают внимание прокуроры, связан с возможностью отказа в возбуждении уголовного дела, когда речь идет о малозначительности.

Согласно данным ГИАЦ МВД России, ежегодно выносится от 1,2 до 1,8 тыс. решений о прекращении уголовных дел рассматриваемой категории по реабилитирующим основаниям, в частности в отношении лиц, совершивших преступления, сумма ущерба по которым не превышала 1 тыс. руб. А также порядка 1-2 тыс. таких решений – по нереабилитирующим основаниям, в том числе в связи с примирением сторон, деятельным раскаянием и назначением судебного штрафа.

К примеру, в 2022 г. апелляционным определением Московского городского суда отменен приговор Чертановского районного суда, которым несовершеннолетний Т. осужден по п. «г» ч. 3 ст. 158 и по ч. 3 ст. 30, п. «г» ч. 3 ст. 158 УК РФ. Уголовное дело прекращено в связи с отсутствием в его деяниях составов преступлений ввиду их малозначительности.

При этом судом первой инстанции Т. признан виновным в краже, совершенной с банковского счета в сумме 631 руб. 50 коп., и покушении на кражу с банковского счета 69 руб. при следующих обстоятельствах. Последний нашел утерянную потерпевшим К. банковскую карту и, используя ее, приобрел в магазине «Фикс Прайс» продуктовые товары общей стоимостью 631 руб. 50 коп., после чего, используя эту карту, пытался приобрести бутылку минеральной воды стоимостью 69 руб., однако не смог этого сделать в связи с блокировкой карты[1].

[1] По материалам Генеральной прокуратуры Российской Федерации.

В данном случае, прежде всего, необходимо отметить, что согласно абз. 2 п. 25.4 постановления Пленума № 29 при решении вопроса о том, является ли малозначительным деяние, например кража, формально содержащая квалифицирующие признаки состава данного преступления, судам необходимо учитывать совокупность таких обстоятельств, как степень реализации преступных намерений, размер похищенного, роль подсудимого в преступлении, совершенном в соучастии, характер обстоятельств, способствовавших совершению деяния, и др. Однако в данном случае речь идет об уголовном деле.

Вместе с тем, что касается этапа проверки сообщения о преступлении, то на данном этапе сведений о лице, совершившем преступление, может не быть. При этом по уголовным делам о преступлениях, предусмотренных ст. 159 УК РФ, когда лицо, совершившее преступление не установлено, действуют положения ч. 4 ст. 20 УПК РФ, позволяющие принимать решение о возбуждении уголовного дела в публичном порядке по факту совершения преступления.

Кроме того, в соответствии с абз. 3 п. 30 постановления Пленума № 48, если стоимость имущества, похищенного путем мошенничества (за исключением ч. 5 ст. 159 УК РФ), присвоения или растраты, составляет не более 2500 руб., а виновный является лицом, подвергнутым административному наказанию за мелкое хищение чужого имущества стоимостью более 1 тыс. руб., но не более 2500 руб., и в его действиях отсутствуют признаки преступлений, предусмотренных ч. 2, 3 и 4 ст. 159, ч. 2, 3 и 4 ст. 159^1, ч. 2, 3 и 4 ст. 159^2, ч. 2, 3 и 4 ст. 159^3, ч. 2, 3 и 4 ст. 159^5, ч. 2, 3 и 4 ст. 159^6, ч. 2 и 3 ст. 160 УК РФ, то содеянное подлежит квалификации по ст. 158^1 УК РФ.

Однако вопрос о том, подвергалось ли лицо административному наказанию за мелкое хищение чужого имущества, может быть разрешен после установления правонарушителя и данных о его личности, что, по всей вероятности, сложно как на этапе процессуальной проверки, так и на этапе предварительного расследования.

Раздел 4. Прокурорский надзор за процессуальной деятельностью органов дознания и органов предварительного следствия при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий

При раскрытии предусмотренных наименованием параграфа вопросов необходимо учитывать следующее.

В первую очередь, как уже было указано ранее, определенная часть преступлений в сфере ИТТ носит бытовой характер. При этом в правоприменительной практике имеются разночтения при расследовании таких преступлений. Другие преступления являются дистанционными мошенничествами. Но практику предварительного расследования данных преступлений сложно признать повсеместной (разработанной) по причине их низкой раскрываемости. Имеются и другие особенности правоприменительной практики по некоторым преступлениям, о чем будет сказано далее. При этом многие вопросы правоприменительной практики раскрыты в постановлении Пленума № 37.

Применительно к совершению преступлений в сфере ИТТ, которые носят бытовой характер, необходимо привести следующие примеры.

Так, по одному из уголовных дел К. после распития спиртных напитков со знакомой зашел в террасу, открыл шкаф-купе, обнаружил черную кожаную куртку, в правом кармане которой лежала банковская карта ПАО «Сбербанк». Похитив карту, К., осознавая, что денежные средства ему не принадлежат, зная пин-код карты, путем обмана уполномоченных работников, умолчав о незаконном владении указанной картой, в нескольких магазинах оплатил сделанные им покупки, всего на сумму 6060 руб. Действия К. квалифицированы по ч. 2 ст. 159^3 УК РФ.

По другому уголовному делу Т. обнаружила на тротуарной плитке банковскую карту ПАО «Сбербанк». Достоверно зная, что при оплате до 1 тыс. руб. введения пин-кода не требуется, путем обмана уполномоченных работников торговых организаций неоднократно совершала покупки в магазинах, всего на общую сумму 11 077 руб. Действия Т. квалифицированы по ч. 2 ст. 159^3 УК РФ[1].

[1] По материалам уголовных дел, изученных в прокуратуре Московской области.

Согласно следующему примеру В. нашел на улице банковскую карту АО «Альфа-банк». В дальнейшем со своей знакомой стал ходить по магазинам и совершать покупки, осознавая, что денежные средства ему не принадлежат. Всего, при учете возможности совершения одной покупки до 1 тыс. руб., похитил 12 901 руб. Действия В. квалифицированы по п. «г» ч. 3 ст. 158 УК РФ.

Есть и другие примеры квалификации действий виновных лиц при несколько других обстоятельствах, когда речь идет о так называемых бытовых хищениях.

Так, Е. попросил сотовый телефон матери, чтобы позвонить. Увидев, что в телефоне имеется мобильное приложение ПАО «Сбербанк», а за ним никто не наблюдает, перевел с банковского счета матери на свой счет денежные средства в размере 10 тыс. руб. Действия Е. квалифицированы по п. «г» ч. 3 ст. 158 УК РФ[1].

Согласно абз. 2 п. 25[1] постановления Пленума № 29 по п. «г» ч. 3 ст. 158 УК РФ квалифицируются действия лица и в том случае, когда оно тайно похитило денежные средства с банковского счета или электронные денежные средства, использовав необходимую для получения доступа к ним конфиденциальную информацию владельца денежных средств (например, персональные данные владельца, данные платежной карты, контрольную информацию, пароли).

Конституционный Суд Российской Федерации указал, что Верховным Судом Российской Федерации устранена существовавшая в правоприменительной практике неопределенность в разграничении составов кражи, совершенной с банковского счета, а равно в отношении электронных денежных средств, и мошенничества с использованием электронных средств платежа. В данном случае речь идет о постановлении Пленума Верховного Суда Российской Федерации от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам». При этом в абз. 6 п. 5.1 определения Конституционного Суда Российской Федерации от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей статьи 158 и статьи 159.3 Уголовного кодекса Российской Феде-

[1] По материалам уголовных дел, изученных в прокуратуре Московской области.

рации в связи с запросом Железнодорожного районного суда города Рязани» (далее – определение КС РФ от 09.07.2021) также указано, что само по себе использование чужой платежной карты с целью хищения денежных средств с банковского счета законного владельца этой карты путем отправления лицом распоряжения в адрес конкретной кредитной организации о списании денежных средств с названного банковского счета допустимо считать как основанное на обмане (злоупотреблении доверием) кредитной организации, уполномоченной в установленном порядке на осуществление операций по данному счету.

Очевидно, что рассмотренная выше ситуация не так однозначна с точки зрения квалификации преступления, что может повлечь сложности в принятии решений о возбуждении уголовного дела.

Так, кассационным определением Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10.08.2021 № 3-УДп21-18-К3 приговор Сосногорского городского суда Республики Коми от 26.02.2020 и последующие судебные решения оставлены без изменения.

В описательно-мотивировочной части данного кассационного определения указано, что по приговору суда С. признан виновным в том, что 13.06.2019, находясь в отделении ПАО «Сбербанк»: по адресу Республика Коми, г. <...>, имея при себе банковскую карту потерпевшего К. ПАО «Б» и зная пин-код указанной карты, действуя с умыслом на тайное хищение денежных средств со счета потерпевшего, с использованием банкомата в период времени с 10 часов 33 минут до 11 часов 16 минут обналичил 60 тыс. руб., затем прибыл к ТЦ «Мегакуб» по адресу: Республика Коми, г. <...>, где в период времени с 11 часов 45 минут до 11 часов 53 минут с использованием банкомата обналичил 10 тыс. руб.; он же в указанный день, находясь в магазинах, расположенных на территории пгт. Нижний Одес г. Сосногорска Республики Коми, имея при себе банковскую карту потерпевшего К. ПАО «Б» и зная пин-код указанной карты, не ставя в известность продавцов о незаконном владении банковской картой, в период времени с 8 час. 28 мин. до 12 час. 22 мин. произвел в кассовых терминалах различных магазинов посредством данной карты потерпевшего оплату за приобретенный товар на сумму 109 901 руб. 20 коп.

Органами предварительного расследования и судом, который рассмотрел дело с учетом требований ст. 252 УПК РФ, действия С. были квалифицированы в части обналичивания денежных средств в сумме 70 тыс. руб. с банковского счета потерпевшего по п. «г» ч. 3 ст. 158 УК

РФ как кража денежных средств с банковского счета с причинением значительного ущерба потерпевшему, а действия по оплате с этой банковской карты товаров на сумму 109 901 руб. 20 коп. – по ч. 2 ст. 159[3] УК РФ как мошенничество с использованием электронных средств платежа с причинением потерпевшему значительного ущерба[1].

Полагаем, что разрешению данной ситуации может послужить учет позиции Верховного Суда Российской Федерации.

Согласно определению Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 09.03.2021 № 11-УД20-35-К6 судами нижестоящих инстанций правильно установлено, что Я. похитил у потерпевшей З. кошелек стоимостью 1 тыс. руб., в котором находились деньги в размере 1920 руб., не зная о том, что там находится еще и банковская карта. Лишь после окончания данного преступления он обнаружил в кошельке банковскую карту с пин-кодом. У него возник умысел на хищение с нее денежных средств, и он снял с банковского счета 10 500 руб. То есть им совершены в другое время, в другом месте иные преступные действия с вновь возникшим умыслом. При таких обстоятельствах в действиях Я. усматривается реальная совокупность преступлений – кража кошелька с деньгами и кража денег с банковского счета, и его действия судами нижестоящих инстанций квалифицированы правильно[2].

Если рассматривать банковскую карту в значении кошелька, а безналичные денежные средства в качестве объекта гражданских прав, которые являются неотъемлемой частью такой карты, то хищение банковской карты сложно не рассматривать в качестве хищения банковской карты с безналичными денежными средствами (если они имеются на счете). Так, на основании ст. 128 ГК РФ к объектам гражданских прав относятся вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, в том числе цифровые рубли, бездокументарные ценные бумаги, цифровые права).

Поскольку в полной мере безналичные денежные средства при отсутствии знания пин-кода снять сразу невозможно, не исключена возможность совершения покушения на хищение безна-

[1] Кассационное определение Судебной коллегии по уголовным делам Верховного Суда РФ от 10.08.2021 № 3-УДп21-18-К3.

[2] Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 09.03.2021 № 11-УД20-35-К6.

личных денежных средств. Такая позиция соответствует абз. 2 п. 5 постановления Пленума № 48, согласно которому если предметом преступления при мошенничестве являются безналичные денежные средства, в том числе электронные 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.

В большинстве случаев хищение безналичных денежных средств прекращается после обращения в банк потерпевшего в связи со списанием денежных средств с карты неизвестным лицом. И теоретически в случае бездействия потерпевшего могут быть похищены все безналичные денежные средства, находящиеся на банковской карте (в том числе если на карте находилась ровно похищенная злоумышленником сумма – 1 тыс. руб.).

Тем самым важны обстоятельства преступления, при котором хищение безналичных денежных средств происходило частями вплоть до момента блокирования карты банком, после такового, а также сведения об общей сумме находившихся на банковской карте безналичных денежных средств и похищенных безналичных денежных средств. В случае продолжения попыток списания безналичных денежных средств после блокирования банковской карты можно вести речь об умысле на хищение всех безналичных денежных средств, находящихся на карте, который не удалось реализовать по не зависящим от лица обстоятельствам. Уникальность такой ситуации состоит в том, что применительно к покушению на хищение безналичных денежных средств умысел будет подтверждать продолжающееся периодическое их хищение.

Говоря о дистанционных мошенничествах, необходимо отметить, что прокуроры отмечают сложности, связанные с определением потерпевшего по уголовному делу. Формируется практика признания лица потерпевшим в случае совершения дистанционного мошенничества.

В соответствии с п. 1 ст. 154 ГК РФ для заключения договора необходимо выражение согласованной воли двух сторон.

В соответствии с п. 1 ст. 432 ГК РФ договор считается заключенным, если между сторонами в требуемой в подлежащих случаях форме достигнуто соглашение по всем существенным условиям договора. В ситуации, когда кредитный договор оформляется без ведома гражданина, его воля не направлена на возникновение прав и обязанностей, вытекающих из такого договора. Неправомерные действия не являются основанием для возникновения прав и обязанностей и не влекут перехода права собственности на кредитные денежные средства. В случае, когда установлен факт отсутствия волеизъявления гражданина на возникновение гражданско-правовых отношений по кредитному договору, следует признавать потерпевшими по уголовным делам соответствующие кредитные учреждения. Указанными положениями необходимо руководствоваться как в тех случаях, когда кредит оформляется посредством получения у потерпевших путем обмана персональных данных для доступа к системам дистанционного банковского обслуживания, так и в случаях, когда преступники получают доступ к мобильным устройствам потерпевшего в результате противоправных действий (например, в результате хищения смартфона)[1].

Дальнейший порядок участия потерпевшего по уголовному делу может определяться с учетом итогового судебного решения, принятого в рамках гражданского судопроизводства.

Прокуратура Красноярского края указала, что в соответствии со ст. 420 ГК РФ договором признается соглашение двух или нескольких лиц об установлении, изменении или прекращении гражданских прав и обязанностей. Договор считается заключенным, если между сторонами в требуемой форме достигнуто соглашение по всем существенным условиям договора. В случае совершения мошеннических действий, в результате которых преступники получают средства доступа к услугам дистанционного банковского обслуживания, гражданин не подозревает об оформлении на его имя кредитного договора. Тем самым нарушается необходимое условие его заключения – наличие волеизъявления

[1] Методические рекомендации по осуществлению надзора при приеме, регистрации и рассмотрении сообщений о преступлениях и расследовании уголовных дел о кражах и мошенничествах, совершенных с использованием ИТТ, подготовленные в прокуратуре Челябинской области.

сторон, что дает основание для признания договора недействительным. Получение кредита является способом совершения преступления, объектом фактически выступают денежные средства банка, а не физического лица, поскольку самих средств у него не имеется, они в его реальное владение не поступают и из него не изымаются[1].

Так, в постановлении Красноярского краевого суда от 01.09.2023, которым отменено постановление Минусинского городского суда Красноярского края от 06.05.2022 о возвращении уголовного дела прокурору в порядке, предусмотренном ст. 237 УПК РФ, ввиду того, что потерпевшим по уголовному делу признан представитель ПАО «Сбербанк России», указано, что умыслом Ш. охватывалось хищение денежных средств, принадлежащих ПАО «Сбербанк», а не денежных средств, принадлежащих Л., которых у него фактически не имелось. В связи с этим преступление было окончено в момент поступления денежных средств на счет Л. Факт изъятия Ш. похищенных у банка денежных средств с банковского счета Л. является лишь способом завладения денежными средствами банка[2].

Единственным важным уточнением в данном случае следует указать, что согласно ст. 169 ГК РФ сделка, совершенная с целью, заведомо противной основам правопорядка или нравственности, ничтожна и влечет последствия, установленные ст. 167 ГК РФ. В протоколе допроса потерпевшего необходимо обеспечить уточнение следователями (дознавателями) данных о наличии его волеизъявления на заключение кредитного договора.

На это же также обращает внимание представитель Краснодарского университета МВД России А.В. Михалев, поясняя, что необходимо правильно допросить потерпевшего[3].

Желательно также учитывать, что в соответствии с п. 21 приказа Генерального прокурора Российской Федерации от 07.12.2007 № 195 «Об организации прокурорского надзора за исполнением законов, соблюдением прав и свобод человека и граж-

[1] Методические рекомендации «Профилактика хищений, совершаемых с использованием информационно-телекоммуникационных технологий», подготовленные в прокуратуре Красноярского края.

[2] По информации прокуратуры Красноярского края.

[3] *Михалев А.В.* Особенности расследования телефонных мошенничеств с банковскими картами на первоначальном этапе // Приоритетные направления развития науки и образования. 2014. № 3.

данина» предписано деятельность прокуроров по надзору за исполнением законов, законностью правовых актов, соблюдением прав и свобод человека и гражданина оценивать исходя из правомерности и своевременности вмешательства, полноты использования предоставленных им полномочий, принципиальности и настойчивости в устранении нарушений закона, восстановлении нарушенных прав, привлечении виновных к ответственности.

В таком случае также необходимо учитывать, что, если преступлением причинен вред интересам государственного или муниципального унитарного предприятия, государственной корпорации, государственной компании, коммерческой организации с участием в уставном (складочном) капитале (паевом фонде) государства или муниципального образования либо если предметом преступления явилось государственное или муниципальное имущество, уголовное дело по ст. 159 УК РФ подлежит возбуждению в публичном порядке.

Отдельным является вопрос о возможности расширительного толкования понятия «место совершения преступления», когда речь идет о преступлениях в сфере ИТТ.

С одной стороны, эти вопросы разъяснены. На основании абз. 3 п. 5 постановления Пленума № 48 местом совершения мошенничества, состоящего в хищении безналичных денежных средств, исходя из особенностей предмета и способа данного преступления, является, как правило, место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие денежных средств.

В силу п. 25^2 постановления Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое» кражу, ответственность за которую предусмотрена п. «г» ч. 3 ст. 158 УК РФ, следует считать оконченной 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 особенностей предмета и способа данного преступления местом его совершения является, как правило, место совершения лицом действий, направленных на незаконное изъятие денежных средств (например, место, в котором лицо с использованием чужой или поддельной платежной карты снимает наличные

денежные средства через банкомат либо осуществляет путем безналичных расчетов оплату товаров или перевод денежных средств на другой счет).

С другой стороны, в правоприменительной практике возникают ситуации, не исключающие возможности того, что местом совершения преступления, когда, например, речь идет о звонке с Украины, может быть место, связанное с пребыванием потерпевшего. Очевидно, что в данном случае могут быть различные ситуации, не связанные с местом открытия банковского счета.

Так, по одному из уголовных дел установлено, что потерпевшему Б. по мессенджеру «WhattsApp» позвонил неизвестный, который представился представителем службы безопасности ПАО «ВТБ-банк» и сообщил, что на его имя оформлен кредит, по данному факту проводится проверка и для того, чтобы найти причастного к оформлению кредита, ему (потерпевшему) нужно оформить кредит на себя. После этого неизвестный указал ближайший офис ПАО «ВТБ-банк», в котором потерпевший подошел к оператору и оформил на себя кредит «Потребительский» на сумму 1 млн 205 тыс. 134 руб. под 9,9% годовых на 84 месяца и страховку 242 567 руб. В дальнейшем сумму кредита он перевел по реквизитам, указанным звонившим. Все это время, в том числе при нахождении в банке, потерпевший продолжал разговаривать с неизвестным мужчиной и выполнять его указания[1].

В соответствии с информационным письмом заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 18.09.2017 «О порядке проведения оперативно-розыскного мероприятия «обследование помещений, зданий, сооружений, участков местности и транспортных средств» действующее законодательство предусматривает возможность проведения ОРМ как по инициативе органов, уполномоченных на осуществление ОРД, так и по поручениям следователя, руководителя следственного органа, дознавателя, органа дознания или по определению суда по уголовным делам и материалам проверки сообщений о преступлении, находящихся в их производстве (перенос в ходе следствия).

Вопросы, связанные с реализацией положений ст. 152 УПК РФ, могут осуществляться следователем самостоятельно.

[1] По материалам уголовного дела, изученного в прокуратуре Московской области.

Прокуроры отмечают, что использование базы данных «Дистанционное мошенничество» ИБД-Ф позволяет установить серийный характер регистрируемых преступлений[1].

В соответствии с аналитической справкой прокуратуры Челябинской области от 03.02.2022 при выявлении совпадений по базе данных подсистемы «Дистанционное мошенничество» ИБД-Ф как по абонентским номерам, так и по банковским счетам, как в рамках процессуальных проверок, так и в рамках возбужденных уголовных дел осуществляется взаимодействие с должностными лицами иных территориальных органов МВД России с целью получения информации по реквизитам, которые имеют совпадение. При оперативном получении значимой информации в другие территориальные отделы МВД России направляются поручения о представлении интересующих сведений, имеющих значение для раскрытия преступлений. При поступлении информации от оперативных служб, а также кредитных организаций и сотовых операторов по приостановленным уголовным делам производство возобновляется.

В качестве недостатка предварительного расследования прокуроры отмечают ненадлежащую отработку полученных в том числе посредством использования подсистемы «Дистанционное мошенничество» ИБД-Ф сведений и информации, способствующей раскрытию преступлений и установлению причастных к их совершению лиц. В ряде случаев процессуальные решения отменяются прокурорами по причине неучета данных этой подсистемы, что не в полной мере согласуется с требованиями УПК РФ[2].

Соответствующий порядок ведения данной подсистемы предусмотрен приказом МВД России № 925.

Практика применения подсистемы «Дистанционное мошенничество» ИБД-Ф нарабатывается в Следственном департаменте МВД России и региональных (территориальных) следственных отделах МВД России.

Так, согласно данным подсистемы «Дистанционное мошенничество» из производства следственного отдела ОМВД России по Куединскому району Пермского края изъято уголовное дело, возбужденное в отношении обвиняемой по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ. С уголовным делом в единое производство соединено еще 37 эпизодов преступной деятельности последней. Учитывая, что обвиняемая находится на территории Пермского края, в целях обеспечения

[1] Информация к заседанию межведомственной комиссии по профилактике правонарушений при губернаторе Магаданской области.

[2] По информации прокуратуры Челябинской области.

полноты, объективности и соблюдения процессуальных сроков уголовное дело подлежит изъятию из следственного отдела ОМВД России по Дубовскому району Волгоградской области и передаче в ГСУ ГУ МВД России Пермского края для производства дальнейшего расследования.

Такое решение принимается руководителем следственного органа со ссылкой на положения ч. 4 ст. 152 УПК РФ, согласно которой предварительное расследование может производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков.

Вместе с тем важными являются положения ч. 3 ст. 152 УПК РФ, согласно которой если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них. Согласно ч. 3 ст. 153 УПК РФ соединение уголовных дел, находящихся в производстве следователя, производится на основании постановления руководителя следственного органа.

В то же время необходимо учитывать, что согласно совместному письму от 08.02.2022 № 36-49-22/1/1322 возбуждение уголовного дела в случае наличия повода и достаточных оснований целесообразно принимать в органе внутренних дел, в который поступило соответствующее сообщение. Дальнейшая передача уголовного дела в установленном ч. 5 ст. 152 УПК РФ порядке для направления по подследственности возможна лишь после производства неотложных следственных действий. В целях недопущения перенаправления такого рода сообщений о преступлениях либо уголовных дел по территориальности по формальным либо надуманным основаниям прокурорам надлежит реализовывать приоритетные полномочия в разрешении вопросов подследственности.

В данном случае также необходимо отметить практику нахождения уголовных дел о преступлениях в сфере ИТТ в производстве дознавателей, которые также нуждаются в соединении с уголовными делами по совпадению признаков подсистемы «Дистанционное мошенничество» ИБД-Ф.

Согласно ч. 3 ст. 153 УПК РФ решение о соединении уголовных дел о преступлениях, подследственных в соответствии со

ст. 150 и 151 УПК РФ разным органам предварительного расследования, принимает руководитель следственного органа на основании решения прокурора об определении подследственности.

Например, согласно методическим рекомендациям прокуратуры Челябинской области, принимая решение о соединении в одном производстве уголовных дел, находящихся в производстве органов дознания, а также надзирая за законностью соответствующих решений руководителей следственных органов, нужно исходить из того, что соединение уголовных дел должно обеспечить полноту расследования, его объективность и соблюдение процессуальных сроков[1].

В ряде случаев уголовные дела изымались прокурорами в предусмотренном УПК РФ порядке и передавались в органы предварительного следствия.

По информации прокуратуры Челябинской области, в производстве дознания полиции находилось уголовное дело, возбужденное в отношении Д. по ч. 1 ст. 158 УК РФ. Установлено, что Д., пользуясь приложением и услугой «Мобильный банк», поняла, что списание с ее банковской карты не производится и услуга «Мобильный банк» подключена к банковской карте другого человека. Вследствие этого тайно похитила денежные средства в размере 4250 руб. с банковской карты Р. По результатам дознания уголовное дело прекращено на основании ст. 25 УПК РФ в связи с примирением сторон. По результатам изучения уголовного дела прокурором установлено, что данное постановление является необоснованным, поскольку действия Д. подлежат квалификации по п. «г» ч. 3 ст. 158 УК РФ. Вследствие этого необоснованное постановление о прекращении уголовного дела прокурором отменено, уголовное дело изъято прокурором в предусмотренном УПК РФ порядке и передано в органы предварительного следствия. По результатам предварительного следствия уголовное дело направлено в суд для рассмотрения по существу.

Особого внимания прокуроров в данном случае требует изучение уголовных дел, соединенных в порядке, предусмотренном ч. 2 ст. 152 УПК РФ. В соответствии с данной нормой соединение уголовных дел допускается также в случаях, когда лицо, подлежащее привлечению в качестве обвиняемого, не установле-

[1] Методические рекомендации по осуществлению надзора при приеме, регистрации и рассмотрении сообщений о преступлениях и расследовании уголовных дел о кражах и мошенничествах, совершенных с использованием ИТТ (далее – методические рекомендации прокуратуры Челябинской области).

но, но имеются достаточные основания полагать, что несколько преступлений совершены одним лицом или группой лиц. При отсутствии такой достаточности уголовные дела подлежат выделению для дальнейшего предварительного расследования, о чем возможно указывать в требованиях, предусмотренных п. 3 ч. 2 ст. 37 УПК РФ. Согласно ч. 6 ст. 154 УПК РФ срок предварительного следствия по уголовному делу, выделенному в отдельное производство, исчисляется со дня вынесения соответствующего постановления, когда выделяется уголовное дело по новому преступлению или в отношении нового лица. В остальных случаях срок исчисляется с момента возбуждения того уголовного дела, из которого оно выделено в отдельное производство.

В соответствии с протоколом межведомственной рабочей группы от 25.03.2021 на территории Челябинской области подавляющее большинство анализируемых хищений совершается с применением методов социальной инженерии[1].

В настоящее время широкое распространение получило мошенничество, связанное с добровольной передачей физическим лицом сведений (например, номеров платежных карт, кодов, паролей), которые используются преступниками в целях осуществления несанкционированных операций, в том числе переводов денежных средств без согласия клиентов (социальная инженерия)[2].

Работники отдела психологического обеспечения прокурорской деятельности НИИ Университета прокуратуры Российской Федерации для подготовки данного исследования подготовили аналитические материалы, в которых указали, что киберзлоумышленник использует специальные манипулятивные приемы и техники, пытаясь узнать у абонента конфиденциальную информацию и вовлечь его в мошенническую схему. Манипуляция является одним из самых известных и распространенных методов так называемого информационно-коммуникативного, а по сути психологического воздействия на человека среди большого разнообразия его существующих форм и видов[3].

---

[1] По информации прокуратуры Челябинской области.

[2] Справка Генеральной прокуратуры Российской Федерации.

[3] См.: *Психологическое* воздействие в межличностной и массовой коммуникации / отв. ред. А.Л. Журавлев, Н.Д. Павлова; Ин-т психологии РАН. М., 2014.

Цель манипуляции – изменение сознания субъекта – по разным причинам открыто не провозглашается, а достигается посредством скрытого или неявного побуждения его к совершению определенных действий. При этом манипулятивное воздействие апеллирует к рассудку человека, предполагается, что сообщаемая ему логически аргументированная значимая информация будет принята, усвоена и окажет влияние на его поведение. Характерно, что пострадавшие от злоумышленников, использующих методы социальной инженерии для кражи денег со счетов, как правило, редко обращаются в правоохранительные органы. Специальный опрос выявил, что сообщает в полицию только каждая десятая жертва мошенников[1]. И хотя компетенция в кибербезопасности россиян, их уверенность в защищенности своих данных в онлайн-сервисах в последнее время заметно повышаются, тем не менее две трети граждан все еще чувствуют себя неуверенно, используя цифровые технологии, и опасаются стать жертвами кибермошенников[2].

Способы совершения дистанционных мошенничеств известны, что должно обусловливать и методику их расследования.

Выделятся несколько основных способов совершения мошенничества. При этом этот перечень способов не является исчерпывающим.

1. *Мошенник предлагает перевести денежные средства на другой счет*. Правонарушитель сообщает, что произошла утечка данных. Чтобы защитить сбережения, нужно перевести их на другу карту. После получения денежных средств мошенник исчезает.

2. *Мошенник сообщает, что произошло незаконное списание денежных средств.* Правонарушитель представляется сотрудником банка и сообщает, что кто-то пытается списать со сче-

[1] Только 9% россиян обращаются в полицию при столкновении с финансовыми мошенниками // IZ.RU. URL: https://iz.ru/1260423/2021-12-06/tolko-9-rossiian-obrashchaiutsia-v-politciiu-pri-stolknovenii-s-finansovymi-moshennikami (дата обращения: 09.12.2021).

[2] См.: *Андрианов М.С.* Активизация деятельности кибермошенников и актуализация проблемы информационной защиты граждан в условиях пандемии // Психология и право в современной России: сб. тезисов участников Всерос. конф. по юрид. психологии. М.: МГППУ, 2022.

та денежные средства. Чтобы остановить подозрительную операцию, просит назвать полные данные карты.

3. *Мошенник хочет купить ваш товар и просит данные карты.* Это происходит, когда товар размещается по объявлению, данные необходимы для перечисления денежных средств. Пытается получить не только номер карты, срок ее действия, но и трехзначный код.

4. *Мошенник просит передать данные карты правоохранительным органам.* Правонарушитель представляется сотрудником банка, сообщает, что расследуется преступление о хищении денежных средств со счетов, и говорит, что завтра позвонят из полиции и попросят данные карты, чтобы помочь следователям.

5. *Мошенник просит перевести денежные средства потому, что попал в тяжелую ситуацию.* Правонарушитель выдает себя за друга и говорит, что попал в ДТП, а полицейские просят взятку, поэтому необходимо срочно перевести денежные средства на его карту.

Следует обратить внимание на указанный выше официально разработанный Следственным департаментом МВД России алгоритм расследования преступлений и макет уголовного дела. В данном случае возможно выделить первоначальный комплекс следственных действий, который подлежит производству.

К содержанию данного комплекса относится необходимость неотложного направления запросов в кредитные организации, операторам связи, компании, предлагающие сервисы агрегатора такси, организации-регистратора или арендодателя хостинга, интернет-сервисы, на которых размещены объявления, подготовка ходатайства в суд и прилагаемые к нему копии материалов уголовного дела о разрешении получения у оператора связи сведений о соединениях между абонентами и абонентскими устройствами, а также ходатайство в суд и копии материалов уголовного дела о наложении ареста на денежные средства, находящиеся на банковских счетах, электронных кошельках, лицевом счете абонентского номера, передача назначенному руководителем (начальником) соответствующего подразделения системы МВД России оператору для последующего ввода информации в подсистему «Дистанционное мошенничество» ПТК ИБД-Ф сведения о возбуждении уголовного дела и полученную информацию в ходе

проведенных следственных действий в дежурные сутки, подлежащую внесению в указанную подсистему.

А.В. Михалев в данном случае к неотложным действиям с участием обвиняемого также относит производство обыска, в ходе которого необходимо изымать все телефонные аппараты, средства для выхода в Интернет, системные блоки, ноутбуки, с целью проведения в дальнейшем компьютерной экспертизы. Необходимо также иметь в виду, что преступники могут выдать себя тем, что долго используют одни и те же телефонные аппараты, что может быть распознано по регистрации IMEI телефона в сотовых сетях[1].

Отдельным вопросом по преступлениям рассматриваемого вида является необходимость использования компьютерно-технической судебной экспертизы. Предметом ее исследования являются фактические данные о создании, изменении, удалении информации на компьютерных носителях, которые требуется установить для получения доказательств по делу[2].

Кроме того, важность также представляет банковская судебная экспертиза. Предмет ее исследования составляют фактические данные о финансово-хозяйственной деятельности экономического субъекта по привлечению, размещению и использованию финансовых ресурсов (финансирования, кредитования, страхования и др.), в том числе с применением специализированных банковских инструментов, а также об их отражении в учете, которые зафиксированы на материальных носителях информации, исследование которых имеет значение для получения доказательств по делу[3].

Видится важным участие Росфинмониторинга, прежде всего ввиду необходимости реализации совместного приказа от 21.08.2018. На основании п. 18.1[4] данного совместного приказа на Росфинмониторинг возлагается задача подготовки, в том числе по запросам правоохранительных органов, информации и ма-

---

[1] *Михалев А.В.* Указ. соч. С. 5.

[2] *Жильцова Ю.В., Саванина И.Р.* Обоснование применения комплексного подхода в судебной экспертизе на примере биометрической системы идентификации банковских пользователей // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2021. № 14.

[3] Там же.

териалов, необходимых для принятия органами предварительного расследования мер по обеспечению возможной конфискации путем наложения ареста на денежные средства или иное имущество, полученные в результате совершения преступлений, предусмотренных ст. 174 и 174[1] УК РФ, предикатных по отношению к ним преступлений, а также на доходы от этого имущества.

Потенциал материалов, которые могут быть получены из Росфинмониторинга, не всегда используется правоохранительными органами при выявлении и расследовании преступлений. Вместе с тем реализация назначения уголовного судопроизводства (ст. 6 УПК РФ) невозможна без установления имущества, добытого преступным путем, при расследовании каждого преступления, предполагающего получение дохода, выявление и пресечение фактов его легализации, ареста и конфискации преступных активов[1].

При этом использование криптовалюты как средства защиты от возможной конфискации имущества при осуждении за совершение компьютерных преступлений по уголовным делам о преступлениях в сфере ИТТ в правоприменительной практике встречается все чаще[2].

Очевидно, что криптовалюта обладает рядом безусловных преимуществ для легализаторов и дельцов теневой экономики: доступность и простота использования (бесплатное открытие электронного кошелька, его использование не требуют специальных знаний), мобильность (пользователь может осуществлять управление кошельком из любого места), оперативность (транзакции по счету происходят в течение нескольких секунд), безопасность (информация передается с использованием криптографической защиты), анонимность[3].

---

[1] *Тисен О.Н.* Особенности использования правоохранительными органами материалов Росфинмониторинга в доказывании // Актуал. вопр. производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства: сб. науч. тр. по материалам Всерос. науч.-практ. конф., 7 апр. 2023 г. М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2023. С. 250.

[2] *Методика* борьбы с компьютерными преступлениями / К.В. Камчатов и др. С. 100.

[3] *Прокурорский* надзор за исполнением законов при выявлении и расследовании легализации (отмывания) доходов, полученных преступным путем: науч.-практ. пособие / Е.В. Быкова и др.; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. М., 2020. С. 35.

Имеющиеся пробелы в законодательном регулировании указанной сферы не всегда позволяют обеспечить эффективное противодействие преступлениям рассматриваемой категории, терроризму, экстремизму, организованной преступности, коррупционным преступлениям, совершаемым с использованием цифровой валюты.

Действующая редакция ст. 128 ГК РФ вынуждает правоприменителей всякий раз, сталкиваясь с посягательствами, предметом которых является криптовалюта, субъективно решать, относится ли она к имуществу, что неоправданно усложняет процесс и создает условия для злоупотреблений при оценке фактических обстоятельств уголовного дела.

В настоящее время наиболее часто средства в цифровой валюте по окончании преступных действий конвертируются злоумышленниками в фиатные средства и размещаются на различных банковских счетах и электронных кошельках, откуда потом изымаются в рамках уголовных дел. Кроме того, подозреваемым (обвиняемым) разъясняется возможность добровольного возмещения ущерба, активного содействия в розыске имущества, добытого преступным путем, и правовые последствия этих действий. При этом последние под контролем следователя переводят цифровую валюту на банковские счета или электронные кошельки, на которые в дальнейшем накладывается арест.

Вместе с тем, несмотря на ряд положительных примеров правоприменительной практики, сохраняется актуальность положений информационного письма заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 21.02.2016 № 69-09-2016 «О совершенствовании прокурорского надзора за разрешением в органах наркоконтроля сообщений о незаконном обороте наркотиков с использованием информационно-коммуникационной сети «Интернет», согласно которому вопреки требованиям закона об ОРД, проведение ОРМ, направленных на выявление реальных IP-адресов пользователей ICQ, установление получателей денежных средств, поступающих от сбыта наркотиков, и документирование их преступной деятельности игнорировались.

В отсутствие соответствующих механизмов в настоящее время правоприменительная практика сталкивается с рядом проблемных вопросов, возникающих на стадии документирования

преступлений и оперативного сопровождения уголовных дел рассматриваемой категории. Особенно в сфере незаконного оборота наркотиков, структура которого базируется на использовании IT-технологий в сочетании с электронными и цифровыми средствами платежа (в различных инфраструктурных расчетах, включая оплату деятельности участников преступных форм, в отмывании наркодоходов).

Стартом документирования бесконтактных форм совершения преступлений является отработка технологической и финансовой составляющих преступной деятельности, что требует от оперативных сотрудников не только специальных знаний в области ИТТ, но и самостоятельного использования специальных программных, технических, финансовых, цифровых и иных инструментов для выполнения задач оперативно-розыскной деятельности.

Под перечисленными инструментами понимаются разрешенные к использованию в целях ОРД компьютерные программы, технические устройства и электронные носители информации, финансовые документы и электронные средства платежа (например, платежные карты, электронные и криптографические кошельки).

Особая роль в сфере противодействия бесконтактным формам совершения преступлений отводится использованию методов автоматической обработки данных. В связи с этим приоритетом выступает переход оперативной аналитики к электронным технологиям.

Уже сейчас разработаны и введены в эксплуатацию программные комплексы, обеспечивающие поиск и фиксацию оперативно значимой информации в сети «Интернет», которые не только способствуют выполнению функций по выявлению, предупреждению и пресечению преступлений, но и формируют основу доказательственной базы. Полученные цифровые данные, например, могут исследоваться посредством специально разработанных аналитических программных продуктов (в частности, «Прозрачный блокчейн»).

В случае выявления соответствующих транзакций и лиц, их совершивших, в настоящее время наиболее часто средства в цифровой валюте под контролем сотрудников правоохранительных

органов и специалистов в рамках расследования уголовных дел конвертируются злоумышленниками в фиатные средства и размещаются на различных банковских счетах и электронных кошельках, на которые в дальнейшем накладывается арест. При этом подозреваемым (обвиняемым) разъясняется возможность добровольного возмещения ущерба, активного содействия в розыске имущества, добытого преступным путем, и правовые последствия этих действий. При этом последние под контролем следователя переводят цифровую валюту на банковские счета или электронные кошельки.

Так, следственным подразделением УМВД России по Курганской области расследовалось уголовное дело по обвинению Д. в ряде преступлений, связанных с незаконным сбытом наркотических средств в составе преступного сообщества. В ходе следствия изъяты ноутбук и сотовый телефон, при осмотре которых обнаружена информация о посещении интернет-биржи, установлены логин, пароль и специализированная программа для входа в личный кабинет сайта-обменника и интернет-ресурса по продаже наркотических средств. Осмотр информации, содержащейся в личных кабинетах, подтвердил, что вознаграждение в виде цифровой валюты (биткоинов) за распространение наркотических средств поступало на неперсонифицированный электронный счет на площадке «XXX», после чего Д. с использованием интернет-биржи осуществлял конвертацию биткоинов в российские рубли и их перечисление на свои счета. В ходе осмотра обнаружено наличие на электронном счете злоумышленника 2,2 BTC (Bitcoin). Ввиду невозможности наложения ареста на указанный виртуальный актив, принадлежащий Д., проведены следственные эксперименты с участием последнего, в ходе которых он добровольно конвертировал биткоины в российские рубли с одновременным переводом на счета, оформленные на его имя. После чего Курганским городским судом наложен арест на денежные средства Д. на общую сумму более 1 млн руб. В ходе рассмотрения уголовного дела судом следственные и иные процессуальные действия признаны законными и допустимыми[1].

Учитывая, что Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» де-факто уже позволяет рассматривать цифровые валюты как имущество для целей ст. 17, 19, 20 и 21 в рамках ряда

[1] По материалам Генеральной прокуратуры Российской Федерации.

федеральных законов для решения возникающих вопросов в рамках УПК РФ, процедура установления, фиксации и изъятия цифровой валюты может быть представлена в такой последовательности:

получение доказательств о существовании и держателе криптовалюты, о ее связи с производством по уголовному делу, а также о количественных (стоимостных) показателях;

получение надлежащего (судебного) решения на применение правоограничения в виде блокирования действий с криптовалютой;

получение доступа к операциям с цифровой валютой, в том числе путем установления цифрового ключа, получения к нему доступа;

ограничение (замораживание, блокирование) в платежных системах транзакций с цифровой валютой;

правовые и технические действия уполномоченных органов, приводящие к минимизации негативных имущественных потерь, обусловленных применением правоограничения (обеспечение сохранности цифровой валюты до завершения разбирательства по делу с определением ее правовой судьбы).

На первом этапе важным является установление: вида актива (валюты, ценной бумаги, программного кода); как и когда именно они были (и были ли) приобретены лицом, принадлежат ли они ему; порядка расчета стоимости и др.

В рамках производства обыска или выемки в протоколе следственного действия должны быть указаны все действия, направленные на фактическое обнаружение цифровой валюты в известном следствию электронном кошельке фигуранта уголовного дела, которые по форме соответствуют проводимым мероприятиям в ходе осмотра соответствующего предмета – компьютерной техники, смартфона или иного технического устройства, с помощью которого осуществляются обнаружение и последующие операции с цифровой валютой.

При этом в ходе обыска или выемки следует проводить не только поиск цифровой валюты (установление ее типа, размера, ключей доступа с описанием фактического использования браузера, программного и технического обеспечения), но и изъятие,

связанное с созданием условий по противодействию возможным операциям владельца с изъятой у него криптовалютой.

Вместе с тем производство обыска или выемки с соблюдением установленных УПК РФ требований к работе с компьютерной информацией не в полной мере подходит к операциям с цифровой валютой, поскольку:

изъятие электронных носителей, содержащих данные (ключи) электронного кошелька, без копирования и возвращения владельцу не является гарантией обеспечения сохранности цифровой валюты, поскольку рассматриваемая информация может как в электронном, так и в распечатанном виде храниться в нескольких местах у привлекаемого к ответственности лица, а также у иных лиц.

На втором этапе требуется решить вопрос о возбуждении перед судом ходатайства о наложении ареста на имущество. В соответствующем постановлении о наложении ареста необходимо указывать: в зависимости от вида имущественного взыскания, обеспечивающегося арестом, конкретный вид цифровой валюты, подлежащей аресту (наименование, название и публичный адрес электронного кошелька), его количественно-стоимостные характеристики, способ хранения (перевод активов на электронные адреса предварительно созданных криптосчетов правоохранительных и судебных органов либо конвертация в фиатную валюту), должностное лицо, ответственное за сохранность, кому адресуется процессуальное решение (непосредственно пользователю, оператору (кастодиану) или иным посредникам – владельцам площадок по обмену криптоактивов (бирж или миксеров) и др.

При этом следует учитывать тот факт, что стоимость криптовалюты определяется на соответствующих цифровых площадках, не имеющих государственного регулирования и официального представительства, в связи с чем органам предварительного расследования достаточно сложно оценить стоимость цифровой валюты и предоставить в материалы уголовного дела документ, определяющий ее официальный курс на дату перевода, с целью исключения последующих обращений по факту возмещения ущерба от упущенной выгоды. Более того, стоимость указанных активов может меняться в значительной степени в течение нескольких минут, а курс одной и той же криптовалюты также мо-

жет быть разным на различных биржевых и обменных площадках.

На третьем и четвертом этапах в зависимости от позиции лица, чья цифровая валюта арестовывается, возможны следующие варианты действий. При добровольном предоставлении доступа к цифровой валюте судебное решение может исполняться должностным лицом органа предварительного следствия. При отказе в предоставлении вышеуказанного доступа могут быть ситуации, когда нет технической возможности совершить правоограничительные действия без участия держателя цифровой валюты или такая техническая возможность имеется. В последнем случае судебное решение о наложении ареста требуется направить оператору (кастодиану) либо иному посреднику – владельцу площадок по обмену криптоактивов. При этом судебное решение о наложении ареста на цифровую валюту может исполняться путем непосредственного «замораживания» действий с цифровой валютой, т.е. установления ограничения, исключающего транзакции в платежной системе, когда кому-либо невозможно совершать манипуляции с арестованной валютой, в том числе третьему лицу, имеющему соответствующие логин и пароль.

На пятом этапе, включающем дальнейшие правовые и технические действия, направленные на минимизацию негативных имущественных потерь, необходимо обеспечить сохранность цифровой валюты до завершения разбирательства по делу. Данные действия должны учитывать свойства и качества таковой, правовые и технические возможности законной манипуляции с валютой.

В ходе реализации данных следственных и процессуальных действий важно составлять протокол, в котором в процессе описания факта, хода, содержания и результатов произведенного процессуального действия отражаются указанные выше сведения из постановления об аресте цифровой валюты, в том числе ее наименование, реквизиты электронного кошелька, какая точно часть содержимого кошелька арестовывается, расчет среднего курса обмена единицы цифровой валюты (рыночная цена ее купли-продажи) по отношению к рублю, общая сумма, дата и время расчета, факт добровольного предоставления реквизитов арестовываемого кошелька или отказ в этом, все действия с активами

(за исключением реквизитов приватного ключа), сведения о лице, которому вверяется хранение данных, касающихся цифровой валюты, а также место и условия хранения цифровой валюты.

Как отмечают прокуроры, результаты надзорной деятельности свидетельствуют о необходимости повышения качества проводимого МВД России предварительного расследования по уголовным делам о преступлениях, предусмотренных ст. 158 и 159 УК РФ[1]. Имеют место несвоевременное направление запросов в кредитные учреждения, операторам сотовой связи, владельцам интернет-сайтов, отсутствие контроля за поступлением ответов на запросы, длительное ненаправление необходимых запросов[2].

Безусловно, при осуществлении прокурорского надзора за процессуальной деятельностью органов дознания и органов предварительного следствия важен следующий случай.

Положительным примером совместной оперативно-служебной деятельности подразделений следствия системы МВД России, отдела БСТМ ГУ МВД России по Саратовской области, управления ФСБ России по Саратовской и Самарской областям является результат расследования преступления, предусмотренного ч. 2 ст. 272 УК РФ.

В ходе расследования установлено, что в период с апреля по август 2021 г. С., зарегистрировав в Даркнете учетную запись, приобрел базы данных, содержащие логины и пароли аккаунтов электронных почт пользователей почтового сервиса ООО «Мэйл.Ру», аккаунтов пользователей ООО «Т2 Мобайл», а также специальное программное обеспечение, позволяющее осуществлять проверку аккаунтов на возможность их авторизации, поиск информации по ключевым словам аккаунта, а также поиск аккаунтов с ранее полученными письмами от микрофинансовых организаций, банков, платежных систем и интернет-магазинов.

Используя вышеуказанные базы данных и программное обеспечение, С. осуществлял вход в аккаунты почтового сервиса ООО «Мэйл.Ру», блокировал доступ легальных пользователей путем изменения абонентских номеров телефонов и паролей, используемых при авторизации, подменял IP-адреса прокси-серверов и совершал хищения безналичных денежных средств путем их электронных переводов на подконтрольные ему счета виртуальных банковских карт.

Кроме того, таким же способом С. осуществлял вход в аккаунты легальных пользователей интернет-приложения ООО «Т2 Мобайл»,

[1] По информации прокуратуры Магаданской области.
[2] По информации прокуратуры Челябинской области.

блокировал их абонентские номера с перерегистрацией (перевыпуском) и в виде виртуальных SIM-карт, затем, используя подменные IP-адреса, осуществлял вход на сайты микрофинансовых организаций и подавал заявки на выдачу микрозаймов с указанием учетных данных владельцев SIM-карт с последующим выводом денежных средств на подконтрольные ему виртуальные банковские карты.

В результате проведенного в 2022 г. комплекса оперативно-розыскных (оперативно-технических) мероприятий, следственных и иных процессуальных действий, несмотря на принятые С. средства анонимизации, удалось обнаружить, зафиксировать и изъять электронные следы его преступной деятельности и использовать полученную информацию для доказывания его вины.

Обвиняемый полностью признал вину в совершении преступлений. Совокупность собранных по уголовному делу доказательств позволила прокуратуре г. Саратова утвердить обвинительное заключение и направить уголовное дело в суд для рассмотрения по существу.

По результатам рассмотрения уголовного дела 29.08.2022 Энгельсским районным судом Саратовской области С. признан виновным в совершении 11 преступлений, предусмотренных ч. 2 ст. 272 УК РФ, 10 преступлений, предусмотренных п. «в» ч. 3 ст. 159^6 УК РФ, а также преступления, предусмотренного п. «г» ч. 3 ст. 158 УК РФ[1].

К числу недостатков предварительного расследования можно отнести следующее:

несвоевременный допрос потерпевшего, в том числе об обстоятельствах перечисления денежных средств неустановленному лицу;

непринятие мер по установлению абонентских номеров, которые использовались неустановленными лицами для общения с потерпевшими;

непринятие мер к установлению фактических пользователей абонентских номеров операторами сотовой связи;

непринятие мер к детализации телефонных соединений с привязкой к базовым станциям, сведений о номере SIM-карты и IMEI-коде телефона, данных о соединения абонентских номеров, лица, которым принадлежат номера телефонов из детализации, не установлены и не допрошены;

неустановление, каким образом оплачивались услуги сотовой связи;

[1] По информации прокуратуры Саратовской области.

неустановление владельцев счетов, с которых оплачивались услуги сотовой связи, если они оплачивались посредством безналичных расчетов;

непринятие мер к установлению организации, оказывающей соответствующие услуги, в случае, если телефонная связь по абонентским номерам осуществляется по протоколу IP;

непроизводство допроса представителя организации о том, каким образом можно идентифицировать фактического пользователя абонентского номера;

отсутствие отработки адреса электронной почты, указанного в регистрационных данных абонента, а также факта оплаты соответствующих услуг;

непроизводство осмотра мобильных телефонов потерпевших в целях установления абонентских номеров, с помощью которых неустановленные преступники выходили на связь с потерпевшим;

неустановление того, сохранились ли в памяти телефона мультимедийные данные, связанные с переговорами потерпевшего и неустановленного преступника (звукозапись переговоров и т.п.);

непроизводство допроса представители юридического лица по обстоятельствам совершения переводов;

неустановление механизмов совершения соответствующих переводов, учета денежных средств, выяснения, когда и при каких обстоятельствах денежные средства были получены, кто выдавал денежные средства, была ли произведена идентификация получателя денежных средств;

непроизводство допроса ответственных лиц по сведениям и документам, связанным с получением переводов, а также имеющимся документам, подтверждающим факт получения переводов и дальнейшее движение денежных средств;

непроизводство допроса представителей банка, через который осуществлялись переводы, о том, каким образом осуществлялся перевод денежных средств, принимали ли в этом участие работники банка либо переводы осуществлялись с помощью программного обеспечения без участия работника банка, какие команды поступали от потерпевшего, каким образом происходила идентификация потерпевшеего и подтверждение переводов;

неустановление, куда перечислены денежные средства, каким образом можно отследить их передвижение, были ли они обналичены, переведены на другой счет;

непринятие мер к установлению лица, получившего реальную возможность распорядиться похищенными денежными средствами;

непривлечение к участию по уголовному делу специалиста в области компьютерных технологий;

необоснованное вынесение постановлений о приостановлении предварительного следствия.

Основными причинами возвращения прокурорами уголовных дел для дополнительного расследования явились неполнота предварительного следствия, ненадлежащее описание обстоятельств совершения преступлений в постановлении о привлечении лица в качестве обвиняемого и обвинительном заключении (акте, постановлении), ошибочная квалификация деяния, нарушение прав участников уголовного процесса.

Например, при изучении уголовного дела, возбужденного в отношении К. по п. «г» ч. 3 ст. 158 УК РФ, установлено, что К. обвинялся в совершении кражи с банковского счета, а равно в отношении электронных денежных средств. В то же время установлено, что К. совершил хищение денежных средств в сумме 4 тыс. руб. со счета знакомой при помощи программы «Мобильный банк», которая была установлена потерпевшей на сотовом телефоне обвиняемого. По результатам дополнительного расследования уголовное дело направлено в суд для рассмотрения по существу[1].

В другом случае прокурором для дополнительного расследования возвращено уголовное дело, возбужденное по п. «г» ч. 3 ст. 158 УК РФ, поскольку в обвинительном заключении отсутствовали сведения о движении денежных средств по счету потерпевшей, следователем не были приняты меры по возмещению потерпевшему вреда[2].

Для решения указанных проблем и устранения недостатков прокуроры принимают активные меры надзорного и координационного характера.

По информации прокуратуры Челябинской области, в 2020 г. прокурорами области внесено 1062 требования, предусмотренного п. 3 ч. 2

[1] По информации прокуратуры Челябинской области.
[2] По информации прокуратуры Свердловской области.

ст. 37 УПК РФ, 59 представлений. Вопросы, которые затрагиваются прокурорами во вносимых актах прокурорского реагирования, различные.

По информации прокуратуры Волгоградской области, в требовании прокурора, предусмотренном п. 3 ч. 2 ст. 37 УПК РФ, указано о том, что дознавателем ОВД на основании постановления суда о производстве выемки не истребованы сведения об операциях по банковскому счету, а также не получен ответ об информации о соединении между абонентами и абонентскими устройствами, не приобщены ответы с сайтов «ВКонтакте», «Юла».

По информации прокуратуры той же области, другой прокурор указал на необходимость должной оценки действиям неустановленного лица, а именно по ч. 1 ст. 163 УК РФ, которое направляло на принадлежащий потерпевшему сотовый телефон смс-сообщения с требованиями о переводе денежных средств в сумме 40 тыс. руб. под угрозой похищения членов его семьи.

В постановлении координационного совещания руководителей правоохранительных органов г. Москвы от 07.10.2022 также отмечается необходимость обеспечения прокурорами качества и полноты ОРМ, процессуальных проверок и предварительного расследования преступлений по фактам участия в преступных схемах при реализации похищенных со счетов денежных средств с использованием дропперов.

Согласно информации прокуратуры Ставропольского края, органами предварительного расследования не принимаются меры к установлению личностей владельцев расчетных счетов, на которые потерпевшие переводят денежные средства, дальнейшего перенаправления (обналичивания) денежных средств.

В качестве примера такой ситуации необходимо привести установление прокурором недостатков по результатам изучения уголовного дела, возбужденного по ч. 1 ст. 159 УК РФ по факту хищения денежных средств ООО «Мегантрейд», которое было приостановлено по п. 1 ч. 1 ст. 208 УПК РФ. Из материалов дела следовало, что в ходе телефонного разговора с неустановленным лицом, которое представилось директором указанной организации, П. осуществила перевод денежных средств на счет продиктованного ей абонентского номера. В дальнейшем указанные денежные средств были перечислены на расчетный счет, к которому подключены два абонентских номера. Мер к установлению владельцев указанных номеров не принято, сведения о причастности к совершению преступления К. не проверены, что явилось основанием для отмены прокурором указанного процессуального решения[1].

[1] По информации прокуратуры Магаданской области.

В соответствии с аналитической справкой прокуратуры Челябинской области от 03.02.2022 по уголовному делу о преступлении, предусмотренном ч. 2 ст. 159 УК РФ, в адрес начальника органа полиции внесено представление, в котором в том числе указано о том, что следователем было вынесено постановление о приостановлении предварительного следствия, которое отменено. Установлено, что по уголовному делу не произведены необходимые следственные действия, в том числе не проведена компьютерная экспертиза для выяснения характеристик программы, посредством применения которой было совершено хищение. По результатам рассмотрения представления руководителем следственного органа даны письменные указания, два должностных лица привлечены к дисциплинарной ответственности.

На основании постановления координационного совещания руководителей правоохранительных органов Челябинской области от 22.12.2022 руководителям правоохранительных органов поручено по каждому уголовному делу в соответствии с ч. 2 ст. 158 УПК РФ устанавливать обстоятельства, способствовавшие совершению преступления. В случае, если таким обстоятельством явилось неисполнение оператором обязанностей, касающихся передачи абонентского номера и (или) услуг по пропуску трафика и подключения к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования, после установления данного факта направлять информацию в прокуратуру области для решения вопроса о привлечении операторов связи к административной ответственности по ст. 13.2^1 КоАП РФ в рамках реализации полномочий, предусмотренных п. 1 ч. 1 ст. 25.11 КоАП РФ. Здесь же прокурорам указано принимать меры к устранению нарушений в сфере профилактики и противодействия преступлениям, совершаемым с использованием ИТТ, при наличии оснований обращаться в суд с заявлением в порядке ст. 45 ГПК РФ, ст. 39 КАС РФ.

Заключение

Выявление, процессуальная проверка и предварительное расследование преступлений в сфере ИТТ в настоящее время сопряжены со множеством сложностей, обусловленных возможностями ИТТ, которыми злоупотребляют злоумышленники.

К числу таких сложностей относятся вопросы квалификации преступлений в сфере ИТТ, в том числе в случаях, когда речь идет о неправомерном доступе к компьютерной информации, создании, использовании и распространении вредоносных компьютерных программ, нарушении правил эксплуатации средств хранения, об обработке или передаче компьютерной информации и информационно-телекоммуникационных сетей, о мошенничестве, незаконном обороте наркотических средств, изготовлении и обороте материалов или предметов с порнографическими изображениями несовершеннолетних и других преступлениях. Следует также отметить разрешение многих вопросов правоприменительной практики Пленумом Верховного Суда Российской Федерации.

Прокуроры отмечают недостаточные усилия по выявлению и раскрытию преступлений в сфере ИТТ со стороны органов, осуществляющих ОРД. Несмотря на меры координационного характера, количество раскрытия преступлений данного вида нуждается в повышении. Остаются неразрешенными и многие других вопросы, актуальные для органов, осуществляющих ОРД.

В ходе прокурорского надзора отмечаются трудности правоприменительной практики, которые возникают на этапе проверки сообщений о преступлениях. Некоторые трудности касаются длительности исполнения запросов, в ряде случаев подлежит определению место совершения преступления. Возникают трудности, связанные с применением административной преюдиции, а также с определением возможности возбуждения уголовных дел по результатам звонков телефонных мошенников, когда потерпевшему вред не причинен. При этом необходимо отметить разрешение ряда вопросов Пленумом Верховного Суда Российской Федерации.

Этап предварительного расследования является важным с точки зрения установления обстоятельств совершения преступлений, его мотивов, причиненного вреда и т.д. Однако в настоящее время практику изобличения подозреваемых и обвиняемых за совершение дистанционных мошенничеств сложно признать повсеместной. Остаются неразрешенными многие вопросы, которые, как представляется, могут быть решены в рамках работы следственных групп.

Важным является вопрос об определении потерпевших по уголовным делам о преступлениях рассматриваемого вида. Необходимо повышать взаимодействие с органами, осуществляющими ОРД, расширять круг версий совершения преступлений.

При это данные меры необходимо принимать при учете ключевой проблемы латентности преступлений рассматриваемого вида, невозможности сразу установить уголовно-процессуальными средствами значимые обстоятельства, позволяющие принять законное и обоснованное процессуальное решение, нагрузку в органах МВД России и становление информационных ресурсов, направленных на оптимизацию работы органов предварительного расследования в системе МВД России.

Несмотря на то что преступления в сфере ИТТ носят виртуальный характер, вне учета возможностей объективной реальности раскрыть их невозможно.

Полагаем, что в настоящее время у органов, осуществляющих ОРД и предварительное расследование, а также у прокуроров имеются значимые потенциальные возможности для раскрытия преступлений данного вида. Для этого потребуется более детальный учет материалов, подготовленных Генеральной прокуратурой Российской Федерации, в том числе совместно с Университетом прокуратуры Российской Федерации, Следственным департаментом МВД России, Следственным комитетом Российской Федерации и др.

При этом не исключается определенное уточнение разработанных методик правоприменительной практики с учетом данных, о которых сообщили прокуроры субъектов Российской Федерации.

Представляется, что в полной мере об анализе сложностей правоприменительной практики и предложений по их разреше-

нию возможно будет говорить после повышения показателей раскрытия преступлений, обеспечения полноты предварительного расследования и исследования конкретных процессуальных решений (позиций) по раскрытым уголовным делам в сфере дистанционного мошенничества.

Общим выводом можно назвать то, что требуется продолжение кропотливой, значимой и одновременно существенной совместной работы, которая будет отвечать назначению уголовного судопроизводства, позволяя обеспечивать права его участников.

Значимой гарантий в этом процессе остается прокурорский надзор за исполнением законов органами, осуществляющими ОРД, дознание и предварительное следствие.

Приложение 1

Сведения, представляющие интерес для расследования уголовного дела

Сведения, которые необходимо запрашивать у сотовых операторов:

паспортные данные владельца абонентского номера;

детализация звонков за последние три месяца – эти сведения позволяют определить, сколько у злоумышленника сотовых аппаратов (IMEI), как часто он меняет абонентские номера, а также избавляется ли он от SIM-карты после совершения хищения или же использует повторно;

использованные для связи IMEI за последние три месяца;

использованные для связи базовые станции за последние три месяца с указанием следующих технических характеристик: количество секторов (антенных блоков в месте установки), азимут направленности использованных антенных блоков и угол охватываемой ими территории;

информация о входящих и исходящих платежах по лицевому счету абонентского номера;

информация об IP-адресах, использованных для входа в личный кабинет сотового оператора по управлению данным номером, поскольку в большинстве случаев мошенник использует абонентские номера зарегистрированные на подставных лиц, и все операции по управлению абонентским номером проводит через личный кабинет, тем самым оставляя след в виде своего IP-адреса;

копия регистрационной формы – документ, который заполняет продавец SIM-карты при ее регистрации. Помимо установочных данных держателя карты в нем содержатся сведения об адресе торговой точки, где она была реализована, а также данные продавца, которого целесообразно допросить в качестве свидетеля по обстоятельствам расследуемого уголовного дела.

Сведения, которые необходимо запрашивать по банковским картам и расчетным счетам:

информация о паспортных данных владельца банковской карты;

информация о движении денежных средств по банковской карте и местах их обналичивания за последние полгода с указанием точного времени проведения приходных и расходных операций, номера и коды транзакций и др. Проанализировав полученную информацию за последние полгода, возможно определить наиболее часто используемые банкоматы, которые, как показывает практика, находятся рядом с домом преступника или местом частого посещения (работа, торговый центр, адрес родственников и т.д.), информацию о регулярно оплачиваемых абонентских номерах (личный номер, номер родственников или друзей), а также о торговых точках или интернет-магазинах, где совершались покупки. Каждый интернет-магазин предоставит информацию об адресе клиента, на который почтовым переводом был отправлен приобретенный товар;

информация об абонентских номерах, привязанных к данной банковской карте услугой «мобильного банкинга», где и каким образом они были подключены;

информация об адресе офиса банка, в котором была открыта банковская карта;

информация об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой.

По расчетному счету необходимо запрашивать аналогичную информацию, а также информацию о банковских картах, открытых по данному расчетному счету.

Сведения, которые необходимо запрашивать по электронным кошелькам Qiwi, Яндекс.Деньги и др.:

информация о паспортных данных владельца электронного кошелька;

информация о способе и месте идентификации электронного кошелька;

информация об абонентском номере, с использованием которого создан электронный кошелек;

информация об абонентских номерах, привязанных к электронному кошельку;

информация о виртуальных банковских картах, которые выпущены по данному электронному кошельку;

информация о пластиковых картах, выпущенных по данному кошельку, способ их получения (адрес почтового отправления);

информация о входящих и исходящих платежах по электронному кошельку с момента его регистрации;

информация об IP-адресах, использованных для совершения денежных транзакций, а также администрирования электронного кошелька.

Сведения, которые необходимо запрашивать по социальным сетям:

информация о пользователе страницы в социальной сети (ссылка на страницу, например https://vk.com/id410077130):

установочные данные пользователя;

использованные им для регистрации абонентские номера и электронные почты;

IP-адреса, использованные для создания и доступа к странице за последние три месяца;

аналогичная информация по иным страницам социальной сети «ВКонтакте» данного пользователя, установленным при анализе cookie-файлов.

Сведения, которые необходимо запрашивать по доменному имени сайта:

информация о паспортных данных регистратора доменного имени;

информация об использованных для регистрации абонентских номерах и электронных почтах;

информация о том, каким образом произведена регистрация пользователя;

информация об IP-адресах, использованных для регистрации доменного имени;

информация об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени;

информация об оплате услуг регистрации и аренды доменного имени с указанием полных реквизитов плательщика;

аналогичная информация по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе cookie-файлов.

Сведения, которые необходимо запрашивать по арендуемому хостингу:

информация о паспортных данных арендатора хостинга;

информация об использованных для аренды абонентских номерах и электронных почтах;

информация о том, каким образом произведена регистрация пользователя;

информация об IP-адресах, использованных для аренды хостинга;

информация об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования хостинга;

информация об оплате услуг аренды хостинга с указанием полных реквизитов плательщика;

аналогичная информация по иным хостингам, арендуемым данным пользователем, установленным при анализе cookie-файлов.

Сведения, которые необходимо запрашивать у интернет-провайдера:

информация о пользователе и адресе использованного оборудования, которому был выдан интересующий IP-адрес в представляющий интерес период времени.

Сведения, которые необходимо запрашивать по электронной почте:

информация о паспортных данных владельца электронной почты;

информация об использованных для регистрации абонентских номерах;

информация об IP-адресах, использованных для доступа к электронной почте за максимально известный период;

аналогичная информация по иным электронным почтам, зарегистрированным данным пользователем, установленным при анализе cookie-файлов.

Сведения, которые необходимо запрашивать у провайдера SIP-телефонии:

информация о паспортных данных владельца абонентского номера;

информация об использованных для регистрации абонентских номерах, электронных почтах;

информация о том, каким образом произведена регистрация пользователя;

информация об IP-адресах, использованных для регистрации абонентского номера;

информация об IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером;

информация об IP-адресах, использованных для осуществления звонков;

информация об абонентских номерах, на которые шла переадресация звонков;

статистика звонков за интересующий период;

информация об оплате услуг связи с указанием полных реквизитов плательщика.

Приложение 2

Алгоритм допроса потерпевшего

В целом протокол допроса потерпевшего должен содержать следующее.

Подробное описание способа хищения принадлежащих потерпевшему денежных средств, дату, время, абонентский номер, с которого поступил телефонный звонок, кем представился мошенник, изложение предмета разговора со злоумышленником, подробное описание его голоса (хриплый, высокий, низкий, молодой или старый, наличие акцента, как говорил преступник, медленно или скороговоркой, иные особенности речи). Наличие у потерпевшего возможности опознать голос мошенника при предъявлении аудиозаписи голоса. Имеется ли у потерпевшего аудиозапись разговора с мошенником при наличии специальной программы в его телефоне. На какой счет или с использованием какой банковской карты переведены похищенные денежные средства, использовались ли какие-то системы быстрых переводов, куда потерпевшему необходимо было обращаться для переводов денежных средств (например, при предложении мошенника зачислить их на безопасный счет), какие терминалы кредитных организаций использовались для внесения денежных средств на банковские счета для якобы их сохранения на безопасном счете. На какие абонентские номера они были зачислены потерпевшим. Какова сумма причиненного ущерба, с учетом материального положения является ли она для него значительной. В ходе допроса потерпевшего устанавливать его финансовое поведение (какова сумма его доходов, ежедневных платежей, проводимых им за оплату товаров, услуг, суммы кредитных обязательств и ежемесячные платежи по ним).

Приложение 3

Перечень вопросов при назначении компьютерно-технической экспертизы

Учитывая разнородность объектов, представляемых для проведения компьютерно-технических экспертиз и исследований, имеющиеся в ГБУ г. Москвы «МИЦ» программно-техническое обеспечение и методические подходы, используемые для решения поставленных задач, при составлении обращений (запросов) о проведении исследования и вынесении постановлений о назначении экспертизы целесообразно руководствоваться следующим общим списком вопросов:

1. Находится ли представленный на исследование объект в рабочем состоянии?

2. Каково функциональное назначение представленного на исследование объекта?

3. Имеет ли представленный на исследование объект функциональную возможность подключения к информационно-телекоммуникационной сети «Интернет»?

4. Каковы MAC-адреса сетевых контроллеров представленного на исследование объекта?

5. Имеет ли представленный на исследование объект признаки специальных технических средств для негласного получения информации?

6. Имеет ли представленный на исследование объект признаки игрового оборудования?

7. Имеются ли на носителе информации представленного на исследование объекта скрытые, зашифрованные, заархивированные данные и разделы?

8. Содержатся ли в памяти представленного на исследование видео записывающего устройства записи, сделанные в период с … по … (указать точный временной отрезок)? Если да, то сохранить выявленную информацию в удобном для просмотра виде на носитель информации.

9. Содержатся ли в памяти представленных на исследование объектов пользовательские текстовые и медиафайлы, в том числе

среди удаленных? Если да, то записать выявленные файлы на носитель информации.

10. Содержатся ли в памяти представленных на исследование объектов пользовательские медиафайлы, в том числе среди удаленных, имеющие в метаданных сведения о месте их создания (геолокационные данные)? Если да, то записать выявленные файлы на носитель информации.

11. Содержатся ли в памяти представленных на исследование объектов фотографические файлы, имеющие признаки внесения в них изменений с помощью графических редакторов и (или) о монтаже?

12. Содержатся ли в памяти представленных на исследование объектов видеофайлы, имеющие признаки межкадрового или внутрикадрового монтажа?

13. Содержатся ли в памяти представленных на исследование объектов фотографические и видеофайлы, в том числе среди удаленных, с изображениями обнаженных лиц, демонстрирующих различные позы и осуществляющих различные действия? Если да, то записать выявленные файлы на носитель информации.

14. Имеется ли в видеозаписях, полученных в ходе проведения ОРМ, содержащихся на представленном на исследование носителе информации, визуализация игрового процесса, аналогичная игре на игровом автомате с денежным выигрышем?

15. Содержатся ли в памяти представленных на исследование объектов текстовые файлы, в том числе среди удаленных, содержащие определенные ключевые слова? Если да, то записать выявленные файлы на носитель информации.

16. Какое программное обеспечение содержится в памяти представленных на исследование объектов?

17. Имеет ли программное обеспечение, содержащееся в памяти представленных на исследование объектов, признаки отличия от лицензионно используемых программных продуктов?

18. Содержит ли выявленное в памяти представленных на исследование объектов программное обеспечение сведения о правообладателях данных программных продуктов на территории Российской Федерации?

19. Содержатся ли в памяти представленных на исследование объектов сведения об IP-адресах, использовавшихся при подключении к информационно-телекоммуникационной сети «Интернет»?

20. Содержится ли в памяти представленных на исследование объектов история доступа программ-обозревателей (браузеров) к ресурсам (сайтам), размещенным в информационно-телекоммуникационной сети «Интернет»? Если да, то сохранить выявленную информацию в удобном для просмотра виде.

21. Содержатся ли в памяти представленных на исследование объектов сведения о просматриваемых посредством программ-обозревателей (браузеров) видеороликах? Если да, то сохранить выявленную информацию в удобном для просмотра виде.

22. Содержатся ли в памяти представленных на исследование объектов сведения о псевдонимах (никнеймах), использовавшихся при посещении каких-либо ресурсов (сайтов), размещенных в информационно-телекоммуникационной сети «Интернет»? Если да, то сохранить выявленную информацию в удобном для просмотра виде.

23. Содержится ли в памяти представленных на исследование объектов списки контактов, истории вызовов и обмена сообщениями в программах-клиентах служб обмена сообщениями (мессенджерах), служб электронной почты, социальных сетей? Если да, то сохранить выявленную информацию в удобном для просмотра виде.

24. Содержится ли в памяти представленных на исследование объектов программное обеспечение, предназначенное для автоматизации подачи ценовых предложений на электронные торговые площадки?

25. Содержится ли в памяти представленных на исследование объектов программное обеспечение, предназначенное для осуществления интернет-банкинга и электронных платежей?

26. Содержится ли в памяти представленных на исследование объектов программное обеспечение, предназначенное для диагностики автотранспортных средств, в том числе конкретных автомобильных марок?

27. Содержится ли в памяти представленных на исследование объектов программное обеспечение, предназначенное для

распространения медиа файлов через локальные сети или информационно-телекоммуникационную сеть «Интернет» (в том числе P2P)?

28. Содержится ли в памяти представленных на исследование объектов программное обеспечение, предназначенное для реализации игрового процесса, предусматривающего возможность выигрыша, в том числе денежных средств?

29. Содержатся ли в памяти представленных на исследование объектов сведения, ассоциирующие внутри игровые платежные средства с денежными средствами?

30. Содержатся ли в памяти представленных на исследование объектов сведения о приходе и/или расходе внутриигровых платежных средств (кредитов/баллов)? Если да, то сохранить выявленную информацию в удобном для просмотра виде.

Приложение 4

Перечень вопросов для назначения судебно-бухгалтерской экспертизы

1. Имеются ли нарушения ведения бухгалтерского учета в ... (указать предприятие) в период времени с ... по ...? Если имеются нарушения, то в чем они заключаются?

2. Каким нормативным актам противоречат выявленные в ходе экспертизы нарушения ведения бухгалтерского учета?

3. Соответствует ли бухгалтерский баланс предприятия (согласно представленным документам и материалам дела) действительным финансово-экономическим показателям предприятия?

4. Соответствует ли проведенный бухгалтерский учет нормативным актам, регулирующим ведение бухгалтерского учета?

5. Правильно ли оформлены операции по расходованию денежных средств организации ... (указать организацию) с ... по ... (указать временной период)?

6. Имеются ли расхождения в учетных данных о приходе и расходе денежных средств предприятия в период с ... по ... (указать временной промежуток)?

7. Соответствуют ли записи в системе счетов бухгалтерского учета о затратах данным, указанным в первичной документации?

8. Отражена ли в бухгалтерском учете хозяйственная операция (указать операцию)?

9. Является ли обоснованной бухгалтерская операция (указать операцию)?

10. Правильно ли были составлены балансы, проводки и записи в учетных регистрах? Если неправильно, то в чем это заключается?

11. Совпадают ли данные счетов бухгалтерского учета и первичных документов?

12. Противоречат ли бухгалтерские операции (указать), исполненные лицом (указать должность, ФИО), требованиям бухгалтерского учета?

13. Чем объясняется расхождение в различных документах бухгалтерского учета, отражающих хозяйственную операцию (указать)?

14. Товарной или бестоварной является бухгалтерская операция (указать операцию)?

15. Правильно ли и обосновано были списаны материальные ценности (указать какие именно)?

16. Имеется ли искажение производственных расходов? Какова их величина?

17. Имеется ли завышение списанных материалов (указать) за период времени с ... по ... (указать)?

18. Какова общая сумма излишне списанных материалов?

19. Правильно ли при оформлении бухгалтерской операции (указать) использована норма естественной убыли?

20. Правильно ли была проведена ревизия на предприятии (указать название)? Если нет, то в чем это заключается? Перечислить нарушения.

21. Отражены ли соответствующим образом все проводимые финансовые операции в организации (указать название) в период с ... по ... (указать)?

22. Имеется ли нецелевое расходование перечисленных денежных средств? Если имеется, то как были израсходованы перечисленные денежные средства?

Библиографический список

Нормативные акты

Конституция Российской Федерации.

Гражданский кодекс Российской Федерации.

Кодекс Российской Федерации об административных правонарушениях.

Таможенный кодекс Евразийского экономического союза.

Уголовный кодекс Российской Федерации.

Уголовно-процессуальный кодекс Российской Федерации.

Федеральный закон от 02.12.1990 № 395-I «О банках и банковской деятельности».

Федеральный закон от 17.01.1992 № 2202-I «О прокуратуре Российской Федерации».

Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

Федеральный закон от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах».

Федеральный закон от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».

Федеральный закон от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации».

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»».

Федеральный закон от 24.07.2023 № 369-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе».

Постановление Правительства Российской Федерации от 31.12.2021 № 2607 «Об утверждении Правил оказания телематических услуг связи».

Приказ Министерства связи и массовых коммуникаций Российской Федерации от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости, функционирования и безопасности информационных систем общего пользования».

Приказ Министерства связи и массовых коммуникаций Российской Федерации от 27.06.2013 № 149 «Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети «Интернет» в форме открытых данных, а также для обеспечения ее использования».

«ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. и введен в действие приказом Ростехрегулирования от 18.12.2008 № 532-ст).

«ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения» (утв. и введен в действие приказом Росстандарта от 28.01.2014 № 3-ст).

«ГОСТ Р 56939-2016. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. и введен в действие приказом Росстандарта от 01.06.2016 № 458-ст).

Решения Конституционного Суда Российской Федерации

Определение Конституционного Суда Российской Федерации от 09.07.2021 № 1374-О «О прекращении производства по делу о проверке конституционности пункта «г» части третьей

статьи 158 и статьи 159^3 Уголовного кодекса Российской Федерации в связи с запросом Железнодорожного районного суда города Рязани».

Решения, разъяснения и обобщения Верховного Суда Российской Федерации

Постановление Пленума Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое».

Постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности».

Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

Постановление Пленума Верховного Суда Российской Федерации от 29.06.2021 № 21 «О некоторых вопросах судебной практики по делам о преступлениях против интересов службы в коммерческих и иных организациях (статьи 201, 201^1, 202, 203 Уголовного кодекса Российской Федерации)».

Постановление Пленума Верховного Суда Российской Федерации от 29.06.2021 № 22 «О внесении изменений в отдельные постановления Пленума Верховного Суда Российской Федерации по уголовным делам».

Постановление Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Обзор судебной практики Верховного Суда Российской Федерации № 3 (2018) (утв. Президиумом Верховного Суда Российской Федерации 14.11.2018).

Обзор судебной практики Верховного Суда Российской Федерации № 3 (2021) (утв. Президиумом Верховного Суда Российской Федерации 10.11.2021).

Судебная практика

Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10.07.2019 № 16-УД19-7.

Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 09.03.2021 № 11-УД20-35-К6.

Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 10.08.2021 № 3-УДп21-18-К3.

Кассационное определение Тульского областного суда от 26.10.2011 № 22-2581.

Определение Курганского областного суда от 25.06.2013 № 22-475/2013.

Апелляционное постановление Верховного Суда Республики Татарстан от 13.12.2016 по делу № 22-8753.

Апелляционное постановление Свердловского областного суда от 12.09.2017 по делу № 22-6725/2017.

Постановление Московского городского суда от 22.01.2018 № 4у-0362/2018.

Определение Первого кассационного суда общей юрисдикции от 24.03.2020 № 77-291/2020.

Приговор Щербинского районного суда г. Москвы по уголовному делу от 08.12.2014 № 1-395/2014.

Приговор Кировградского городского суда Свердловской области от 05.08.2016 № 1-105/2016.

Приговор Московского районного суда г. Твери от 21.11.2016 по делу № 1-308/2016.

Приговор Останкинского районного суда г. Москвы от 04.12.2017 по делу № 1-507/17.

Приговор Карагайского районного суда Пермского края от 06.02.2018 по делу № 1-14/2018.

Приговор Тверского гарнизонного военного суда от 04.06.2018 по делу № 1-14/2018.

Приговор Первомайского районного суда г. Ижевска от 14.06.2018 по делу № 1-272/2018.

Приговор Вологодского городского суда от 24.09.2020 по делу № 1-1094/2020.

Постановление мирового судьи № 77 района Сокол г. Москвы от 15.07.2022.

Организационно-распорядительные и иные документы

Приказ Минцифры России от 31.01.2022 № 75 «Об утверждении российской системы и плана нумерации».

Приказ Генерального прокурора Российской Федерации от 07.12.2007 № 195 «Об организации прокурорского надзора за исполнением законов, соблюдением прав и свобод человека и гражданина».

Приказ Генерального прокурора Российской Федерации от 02.08.2018 № 471 «Об организации в органах прокуратуры Российской Федерации работы по правовому просвещению и правовому информированию».

Приказ Генерального прокурора Российской Федерации от 17.09.2021 № 544 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия».

Приказ Генерального прокурора Российской Федерации от 19.01.2022 № 11 «Об организации прокурорского надзора за процессуальной деятельностью органов дознания».

Указание Генерального прокурора Российской Федерации № 401/11, МВД России № 2 от 19.06.2023 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности».

Информационное письмо Генеральной прокуратуры Российской Федерации и МВД России от 08.02.2022 № 36-49-22/1/1322 «О практике рассмотрения сообщений о преступлениях, совершаемых с использованием информационно-коммуникационных технологий, и об иных проблемных вопросах».

Информационное письмо первого заместителя Генерального прокурора Российской Федерации А.В. Разинкина от 18.05.2022 № 69-09-2022 «О некоторых вопросах противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий».

Информационное письмо заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 10.06.2014 № 16-17-2014/Ип3945-14 «О состоянии законности при передаче органами дознания и органами предварительного расследования сообщений о преступлениях по территориальной подследственности».

Информационное письмо заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 03.11.2015 № 26-11-2015 «Об определении места производства предварительного расследования мошенничеств, совершаемых с использованием с использованием телефонной (сотовой) связи».

Информационное письмо заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 21.02.2016 № 69-09-2016 «О совершенствовании прокурорского надзора за разрешением в органах наркоконтроля сообщений о незаконном обороте наркотиков с использованием информационно-коммуникационной сети «Интернет».

Информационное письмо заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 18.09.2017 «О порядке проведения оперативно-розыскного мероприятия «обследование помещений, зданий, сооружений, участков местности и транспортных средств».

Информационное письмо заместителя Генерального прокурора Российской Федерации И.В. Ткачева от 12.05.2022 № 12-55102-21 «О правовой позиции Верховного Суда Российской Федерации по уголовным делам о преступлениях, связанных с распространением в социальных сетях детской порнографии».

Информационное письмо первого заместителя Генерального прокурора Российской Федерации А.В. Разинкина от 06.04.2023 № 69-09-2023 «О недостатках, допускаемых прокурорами при реализации полномочий по изъятию уголовных дел из производства органов дознания и их передаче следователям Следственного комитета Российской Федерации».

Информационное письмо заместителя Генерального прокурора Российской Федерации И.В. Ткачева от 15.05.2023 № 12-17-2023 «О результатах анализа причин, послуживших основанием к вынесению судами оправдательных приговоров и решений о прекращении уголовных дел о преступлениях, предусмотренных статьями 210 и 210^1 Уголовного кодекса Российской Федерации».

Информационное письмо первого заместителя Генерального прокурора Российской Федерации А.В. Разинкина от 07.08.2023 № 708-105-2023 «О реализации требований статей 46 и 46.1 Федерального закона «О связи» и статей 13.2^1, 28.1 Кодекса Российской Федерации об административных правонарушениях.

Письмо заместителя Генерального прокурора Российской Федерации Гриня В.Я. от 20.12.2017 № 36-11-2017 «О направлении Методических рекомендаций «Вопросы взаимодействия и прокурорского надзора за организацией расследования и раскрытия тяжких и особо тяжких преступлений против личности, в том числе прошлых лет».

Приказ Генерального прокурора Российской Федерации № 39, МВД России, № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 «О едином учете преступлений».

Приказ Генерального прокурора Российской Федерации № 511, Росфинмониторинга № 244, МВД России № 541, ФСБ России № 433, ФТС России № 1313, СК России № 80 от 21.08.2018 «Об утверждении Инструкции по организации информационного взаимодействия в сфере противодействия легализации (отмыванию) денежных средств или иного имущества, полученных преступным путем».

Приказ МВД России от 29.12.2020 № 925 «Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество ПТК «ИБД-Ф».

Научные, практические и методические публикации

Андрианов М.С. Активизация деятельности кибермошенников и актуализация проблемы информационной защиты граждан в условиях пандемии // Психология и право в современной России. М., 2022.

Васильева М.П., Кобелев А.Л. Особенности прокурорского надзора за оперативно-розыскной деятельностью при раскрытии и расследовании преступлений, связанных с деятельностью организованного преступного сообщества // Прокурорский надзор за исполнением законов в оперативно-розыскной деятельности: сб.

материалов по обмену опытом: в 2 ч. / под общ. ред. С.В. Иванова. М.: Акад. Ген. прокуратуры Рос. Федерации, 2011.

Вехов В.Б. Вредоносные компьютерные программы как предмет и средство совершения преступления // Расследование преступлений: проблемы и пути их решения. 2015. № 2 (8).

Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015.

Лебедева А.А. Особенности расследования киберпреступлений // Безопасность бизнеса. 2021. № 6.

Литвишко П.А. Особенности реализации Следственным комитетом Российской Федерации экстерриториальной уголовной юрисдикции в отношении международных и транснациональных преступлений на Украине // Следственный комитет Российской Федерации: место и роль в обеспечении национальной безопасности государства: сб. ст. Общерос. науч. практ. конф. (Москва, 17 февр. 2016 г.) / отв. ред. О.И. Александрова. М., 2016.

Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук. Орел, 2008.

Михалев А.В. Особенности расследования телефонных мошенничеств с банковскими картами на первоначальном этапе // Приоритет. направления развития науки и образования. 2014. № 3.

Соловьев В.С. Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. 2017. № 6.

Состояние законности и правопорядка в Российской Федерации и работа органов прокуратуры. 2022 год: информ.-аналит. записка / под общ. ред. И.М. Мацкевича. М.: Ун-т прокуратуры Рос. Федерации, 2023.

Тисен О.Н. Особенности использования правоохранительными органами материалов Росфинмониторинга в доказывании // Актуал. вопр. производства предварительного следствия в современных условиях совершенствования уголовно-процессуального законодательства: Всерос. науч.-практ. конф., 7 апр. 2023 г.: сб. науч. тр. М.: Моск. ун-т МВД России им. В.Я. Кикотя, 2023.

Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук. Ставрополь, 2004.

Яни П.С. Специальные виды мошенничества // Законность. 2015. № 8.

Методика борьбы с компьютерными преступлениями: пособие / К.В. Камчатов и др.; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. М., 2020.

Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России).

Методические рекомендации о порядке привлечения операторов связи к административной ответственности, предусмотренной ч. 1 и 2 ст. 13.2^1 КоАП РФ, подготовленные в Генеральной прокуратуре Российской Федерации.

Прокурорский надзор за исполнением законов при выявлении и расследовании легализации (отмывания) доходов, полученных преступным путем: науч.-практ. пособие / Е.В. Быкова и др.; Ген. прокуратура Рос. Федерации; Ун-т прокуратуры Рос. Федерации. М., 2020.

Прокурорский надзор за исполнением законов при выявлении, расследовании и предупреждении преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и в сфере компьютерной информации: монография. М.: Проспект, 2022.

Собирание электронных доказательств по уголовным делам на территории России и зарубежных стран: опыт и проблемы: монография / Е.А. Архипова, Е.В. Быкова, П.А. Литвишко и др.; под общ. и науч. ред. С.П. Щербы. М.: Проспект, 2022.

Содержание

Прокурорский надзор за исполнением законов органами предварительного расследования при выявлении и расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий

Научно-практическое пособие

Редактор В.А. Третьякова
Корректор Л.А. Перовская

Подписано в печать 20.11.2023. Формат 60х90/16. Печ. л. 7,625.
Тираж 300 экз. Заказ 42.

Университет прокуратуры Российской Федерации.
123022, Москва, ул. 2-я Звенигородская, 15.