ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

А. И. Гайдин, Н. Ю. Дутов
И. С. Тройнина, А. Н. Гущин,

ДЕЙСТВИЯ ДОЗНАВАТЕЛЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ ЧАСТЬЮ ПЕРВОЙ СТАТЬИ 163 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Методические рекомендации

Воронеж
2024

ББК 67.408
УДК 343

Рецензенты:

Малахов Д. В. – начальник информационно-аналитического отдела ГСУ ГУ МВД России по Воронежской области, подполковник юстиции;

Пытьев В. В. – заместитель начальника УУР ГУ МВД России по Воронежской области, полковник полиции.

Действия дознавателя при расследовании преступлений, предусмотренных частью первой статьи 163 Уголовного кодекса Российской Федерации, совершенных с использованием сети Интернет : методические рекомендации / А. И. Гайдин, Н. Ю. Дутов, И. С. Тройнина, А. Н. Гущин. – Воронеж : Воронежский институт МВД России, 2024. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

Методические рекомендации рассматривают особенности действий дознавателя при расследовании преступлений, предусмотренных частью первой статьи 163 Уголовного кодекса Российской Федерации, совершенных с использованием сети Интернет.

Предназначены для курсантов и слушателей юридического факультета, слушателей факультета заочного обучения и слушателей факультета переподготовки и повышения квалификации. Предоставляют возможность углубить теоретические знания, полученные в ходе изучения дисциплин «Расследование преступлений в сфере компьютерной информации», «Компьютерная криминалистика» и «Методы и способы получения доказательственной информации с электронных носителей».

ISBN 978-5-00229-107-6

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Динамика преступности в сфере киберпространства в последние несколько лет характеризуется постоянным увеличением доли киберпреступлений в общей структуре преступности, вследствие чего наблюдается и постоянный рост ущерба от IT-преступлений. Несмотря на усилия государства по реализации комплекса мер противодействия такого рода преступлениям, правонарушители, активно разрабатывая и внедряя в практику новые способы, расширяют круг видов деяний, совершаемых с использованием средств информационно-телекоммуникационных технологий. Подтверждением служит показатель динамики роста абсолютного числа уголовных дел по фактам вымогательства, количество которых в период с 2018 по 2022 годы возросло с 1 621 преступления до 5 721. Только за последний год прирост составил 42%[1].

За 12 месяцев 2022 года подразделениями дознания территориальных органов МВД расследовано всего 273 преступления, предусмотренных частью 1 ст. 163 УК РФ[2], совершенных в сфере информационно-телекоммуникационных технологий, из них направлены в суд уголовные дела по 197 преступлениям, а приостановлено по основаниям, предусмотренным п. 1–4 ч. 1 ст. 208 УК РФ, за этот же период 4 905 преступлений[3]. С целью анализа правоприменительной практики по преступлениям, предусмотренным ч. 1 ст. 163 УК РФ, Управлением по организации дознания МВД России в 2022 году выборочно истребованы и изучены уголовные дела данной категории. Их изучение показало, что с развитием информационно-телекоммуникационных технологий совершение вымогательств стало носить дистанционный характер. Требования о передаче имущества осуществляются преступниками посредством мобильной связи либо с использованием сети Интернет, в том числе различных мессенджеров. Большинство указанных преступлений связаны с неправомерным доступом к аккаунтам граждан, а также хранящейся там информации, в том числе личного характера. В данном случае объективной стороной выступает угроза распространения незаконно полученных сведений путем использования сети Интернет. Использование преступниками средств анонимизации в сети Интернет и способов сокрытия данных о транзакциях средств, полученных преступным путем, значительно

---

[1] Комплексный анализ состояния преступности в Российской Федерации по итогам 2022 года и ожидаемые тенденции ее развития / М. В. Гончарова, С. А. Невский, М. М. Бабаев, Р. В. Черкасов, Е. Б. Аблиязова, Е. М. Тимошина, Г. Ф. Коимшиди, Г. Э. Бицадзе. – Москва : ФГКУ «ВНИИ МВД России», 2023. – С. 63–71.

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

[3] Форма статистической отчетности «ИТТ» (280), книга 2 «Сведения о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий».

затрудняет процесс установления ключевых обстоятельств. В большинстве случаев деяния остаются нераскрытыми.

В существующих условиях формирование навыков организации и осуществления расследования, фиксации хода и результатов процессуальной деятельности требует от дознавателей обращения к правовым, техническим, методическим и научным источникам, в которых соответствующая информация не всегда систематизирована. Поэтому для формирования единообразного подхода в производстве дознания по делам о вымогательстве и организации взаимодействия с оперативными подразделениями органов внутренних дел необходима подготовка методических рекомендаций.

Данные методические рекомендации были разработаны в ходе выполнения научно-исследовательской работы и представлены нами в виде памятки с основными рекомендациями для дознавателей органов внутренних дел по расследованию преступлений, предусмотренных частью первой статьи 163 УК РФ, совершенных с использованием сети Интернет.

1. СВЕДЕНИЯ О КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫХ ПРИЗНАКАХ МЕХАНИЗМА ВЫМОГАТЕЛЬСТВА С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ, ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ

Вымогательство в киберпространстве в основном представлено двумя группами преступлений. К первой группе относятся деяния, направленные в отношении владельцев сетевых ресурсов. Вымогатели используют различные средства и способы воздействия на элементы сетевой инфраструктуры, с целью выведения их из строя. Под угрозой продолжения таких действий они выставляют требования передачи им денежных средств или цифровых активов. Распространенным способом такого вымогательства является использование вредоносных программ-шифровальщиков, которые, внедряясь в компьютерную среду, преобразуют данные на электронном носителе в соответствии с криптостойким алгоритмом шифрования, тем самым блокируют доступ к этим данным. Также могут использоваться и иные программы, уничтожающие определенные файлы без возможности их восстановления или блокирующие доступ функциям операционной системы компьютера. Если объектом воздействия преступников выступает сетевой ресурс потерпевших, то способы воздействия концентрируются вокруг сетевых каналов связи с целью блокирования доступа к ресурсу пользователей путем организации проведения в часы пиковых нагрузок DDoS-атак, которые блокируют удаленный доступ и парализуют работу сетевых сервисов. Применительно к данной группе способов воздействия на компьютерное оборудование необходимо отметить, что ответственность по ст. 163 УК РФ наступает при условии, что такие действия создают угрозу и могут повлечь уничтожение или повреждение чужого имущества.

Другая группа способов кибервымогательства (кибершантажа) представляет собой требование передачи имущества или денежных средств под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, которые могут причинить существенный вред правам или законным интересам потерпевшего или его близких. Такого рода сведения злоумышленники, как правило, целенаправленно получают в результате введения в заблуждение потерпевшей стороны в процессе контактов в социальных сетях, интернет-мессенджерах, выдавая себя за другого человека или придумывая различного рода легенды. Компрометирующая информация может быть получена и в результате неправомерного доступа к охраняемой законом информации о личной жизни, медицинской тайне и иных видах тайны, при взломе аккаунтов социальных сетей, облачных хранилищ информации, персональных компьютеров пользователей или их мобильных средств сотовой связи.

Формирование следовых картин в сетевой среде предопределяет необходимость применения специфических средств и методов доказывания,

а также достаточно высокую их интенсивность, чтобы минимизировать риск утери доказательств в условиях негативного влияния временного фактора и возможных действий злоумышленников по уничтожению следов. Данное условие эффективности расследования должно реализовываться не только на стадии предварительного расследования, но и стадии возбуждения уголовного дела при планировании и проведении проверочных действий.

Сведения об обстоятельствах, подлежащих установлению, позволяют сотрудникам правоохранительных органов в указанных стадиях целенаправленно и динамично организовывать и проводить следственные и иные процессуальные действия, направленные на раскрытие и расследование преступлений данной категории, на плановой основе осуществлять совместную деятельность и использовать специальные знания.

Обстоятельства, подлежащие установлению по делам о вымогательстве в киберпространстве, складываются из обстоятельств, предусмотренных ст. 73 УПК РФ[1], с учетом специфики состава преступления и выявленных закономерностей механизма преступной деятельности, формирующих криминалистическую характеристику вида преступления.

Время совершения преступления. Указанное обстоятельство связано с установлением времени, когда вымогатель предъявил свои требования о передаче имущества. Применительно к сетевым вымогательствам время предъявления требования и момент, когда о нем стало известно потерпевшему, не всегда совпадают. Разрыв во времени возникает при использовании средств коммуникации, которые не обязательно предполагают онлайн общение (переписка в мессенджерах, использование электронной почты). Необходимо установить, были ли угроза и требование передачи имущества персонифицированы или они адресовались неопределенному кругу лиц, в отношении которых злоумышленнику удалось применить вредоносное программное обеспечение или заполучить сведения, распространение которых может повлечь негативные последствия. В таких случаях преступники формируют общие текстовые сообщения, которые рассылаются неопределенному кругу потенциальных жертв преступления и содержат общие требования. Необходимо также устанавливать время каждого факта предъявления преступных требований и угроз и в том случае, когда преступник конкретизировал требования или повторял их при повторности таких действий.

Когда требования персонифицированы, то дополнительными обстоятельствами, которые относятся ко времени совершения

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СПС «КонсультантПлюс».

преступления, являются дата и время, которые были указаны преступником для передачи имущества или денег; время, когда были осуществлены транзакции потерпевшим; время, когда злоумышленник реализовал угрозы (например, распространил в сети Интернет компрометирующие данные).

Место совершения преступления. Сложность установления места совершения вымогательства в киберпространстве обусловлена тем, что преступник и жертва фактически не встречаются лично. Контакты осуществляются с использованием сетевых средств коммуникации, а передача требуемых средств осуществляется путем электронных транзакций. Местами совершения преступлений по данной категории дел могут быть и соответственно должны быть установлены: место нахождения злоумышленника в момент предъявления угроз и требования передачи средств; место осуществления транзакции или передачи имущества; место, где средства были обналичены преступником или получено имущество; место, где находился преступник в момент осуществления транзакций с целью сокрытия преступления.

Способ совершения преступления. Обстоятельства, характеризующие способ совершения вымогательства в сетевой среде, наиболее обширны. К ним относятся данные о подготовке преступника, к которым могут относиться действия по неправомерному доступу к сведениям о потерпевшем, подготовка, отладка и использование вредоносного программного обеспечения, обстоятельства знакомства, общения в сетевой среде, представление ложной информации пострадавшему с целью установления доверительных отношений и получения доступа к личной информации. Способ также характеризуют обстоятельства реализации преступного замысла: как предъявлены были преступные требования; в чем конкретно они выражались; угрозой каких конкретных действий подкреплялись требования; производилась ли демонстрация реальности выполнения угроз; каким образом было получено вымогаемое имущество; как преступник распорядился неправомерным доходом. Действия по сокрытию преступления должны быть установлены с учетом использования конкретных средств и методов анонимизации в сетевой среде, а также действий и использования конкретных финансовых инструментов для сокрытия следов производимых транзакций. Значительную сложность представляет оценка стоимости имущества, угроза уничтожения которого возникает при использовании вредоносного программного обеспечения. В данном случае речь идет о компьютерной технике, ином оборудовании, но не о данных, хранящихся на носителях информации, доступ к которым может быть заблокирован, они могут быть модифицированы или удалены. Последствия для информационной среды и иные последствия от преступления для потерпевшего тоже устанавливаются, так как имеют значение для оценки общественной опасности преступления.

Предмет вымогательства. По рассматриваемой категории дел в большинстве случаев предметом вымогательства выступают денежные средства в безналичной форме, которые по требованию преступника пострадавший переводит на карточные банковские счета или электронные кошельки небанковских платежных систем. В последнее время все чаще в качестве предмета вымогательства выступает цифровая валюта, которой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам[1]. Требования, как правило, выражаются в переводе определенного количества единиц распространенных видов «криптовалюты» (например, Bitcoin, Ethereum, Tether, USD Coin и т. п.) на указанный цифровой кошелек.

Данные, характеризующие вымогателя: пол; возраст; место жительства, учебы и работы; судимость; как характеризуется по месту работы и в быту; профессиональные криминальные навыки; мотив преступления (корысть); обстоятельства, характеризующие признаки объективной стороны преступления; причастность конкретных лиц к групповому или многоэпизодному вымогательству[2], роль и мотивы действий каждого члена преступной группы; характер и размер ущерба, причиненный всей преступной группой и каждым фигурантом в отдельности.

Сведения о потерпевшем: пол, возраст, имущественное положение, судимость, как характеризуется по месту работы и в быту; какой совокупный материальный ущерб причинён вымогательством; какие иные негативные последствия для потерпевшего наступили в результате преступления; почему расценивал угрозы, высказанные вымогателями, как реальные.

---

[1] См.: Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс»

[2] См.: Чхвимиани Эдуард Жульенович. Причины совершения вымогательств и социально-правовая характеристика вымогателей // Общество и право. 2010. № 3 (30). URL: https://cyberleninka.ru/article/n/prichiny-soversheniya-vymogatelstv-i-sotsialno-pravovaya-harakteristika-vymogateley (дата обращения: 15.02.2024).

Способствовавшие совершению вымогательства причины и условия, которые использовались преступниками или были ими целенаправленно созданы в процессе подготовки и реализации преступного замысла. Обстоятельства, затруднявшие действия субъектов преступной деятельности, которые ими были устранены до начала или в ходе преступной деятельности.

Таким образом, изложенные в данном разделе сведения о способах вымогательства и обстоятельствах, подлежащих установлению, должны учитываться лицом, осуществляющим производство по уголовному делу, при планировании расследования и определении основных источников получения доказательственной информации.

2. ПЛАНИРОВАНИЕ ДОЗНАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ, ПРЕДУСМОТРЕННЫМ Ч. 1 СТ. 163 УК РФ, ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ С ОПЕРАТИВНЫМИ ПОДРАЗДЕЛЕНИЯМИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Расследование вымогательства в сфере киберпространства планируется на основе методических рекомендаций, формируемых с учетом типовых следственных ситуаций, складывающихся на первоначальном этапе.

Обобщение практики расследования такого рода преступлений позволяет выделить следующие типовые ситуации:

1. Сведения о вымогательстве поступили от потерпевшего. Данные вымогателя известны.
2. Сведения о вымогательстве поступили от потерпевшего. Данные вымогателя неизвестны.
3. Сведения о вымогательстве получены в рамках оперативно-розыскной деятельности.

Каждая из перечисленных ситуаций может включать варианты в зависимости от стадии реализации преступного замысла. Когда выдвинуты требования преступником о передаче имущества, но оно не передано потерпевшим, и когда факт передачи имущества, перевода требуемых денежных средств уже состоялся.

В подавляющем большинстве случаев поводом для возбуждения уголовных дел о вымогательстве, совершенном в сети Интернет, является заявление потерпевшего.

Получив заявление, орган дознания (оперативное подразделение) прежде всего должен правильно оценить сложившуюся ситуацию с целью организации исполнения необходимых проверочных мероприятий. Их перечень и соответственно особенности тактики проведения зависят от показаний заявителя об обстоятельствах произошедшего события.

Став жертвой вымогательства в условиях, когда преступник шантажирует распространением позорящей информации, потерпевшие зачастую замыкаются, длительное время скрывают возникшую ситуацию, что может привести к утере возможности обнаружения материальных следов преступления. Сильные эмоциональные переживания негативно влияют на объективность и точность показаний об обстоятельствах произошедшего криминального события.

Общие типовые версии, которые проверяются в условиях скудности первоначальной информации, включают предположения о совершении вымогательства, в ряде случаев о неправомерном доступе к компьютерной информации и использовании вредоносных компьютерных программ. Кроме того, целесообразно проверять предположение о многоэпизодности

в деятельности преступников. В ситуации, в которой потерпевший указывает на вымогателя, необходимо проверять версию об оговоре лица.

Частные типовые версии по рассматриваемой категории дел касаются неизвестных обстоятельств события. Однако следует отметить, что на первоначальной стадии расследования выдвижение и проверка предположений о лицах, совершивших преступление, не вполне обоснованы ввиду отсутствия территориальных ограничений при совершении преступления в киберпространстве. Ключевыми частными версиями по рассматриваемой категории дел на первоначальном этапе должны выступать предположения о местах возможного обнаружения виртуальных следов на локальных и удаленных электронных носителях в сетевой среде. Именно в отношении данных следов должна концентрироваться поисковая деятельность.

При поступлении сообщения о неквалифицированном вымогательстве сотрудники дежурной следственно-оперативной группы должны провести ряд неотложных следственных действий и оперативно-розыскных мероприятий:

1. Опросить заявителя и выяснить следующие вопросы:

- когда, сколько раз и на какой абонентский номер звонил преступник или поступали сообщения;
- на кого зарегистрирована SIM-карта;
- использовались ли для коммуникации интернет-мессенджеры;
- происходило ли общение в соответствующих сервисах социальных сетей Интернет;
- какие технические устройства использовались;
- что говорил звонивший;
- как он себя называл;
- какие требования выдвинул преступник;
- какое указал место, время или способ передачи денег;
- сколько раз происходило общение, какое оказывал психологическое давление, в чем конкретно заключалась угроза;
- откуда вымогатель получил сведения, распространением которых угрожал заявителю;
- какую сумму денег передал пострадавший;
- каким образом осуществлялась передача (перевод) денежных средств;
- сколько раз переводил (передавал) деньги;
- как выглядел преступник (если происходила очная встреча или использовалась видеосвязь)?

2. Осуществить немедленный выезд следственно-оперативной группы для проведения осмотра места происшествия. Осмотру подлежат места, где расположена компьютерная техника, использовавшаяся для коммуникации жертвы и преступника, места, где происходили их личные встречи, а также

места передачи (перевода) денег или имущества. Осмотр проводится с участием потерпевшего, специалиста-криминалиста, специалиста в сфере информационных технологий с целью фиксации обстановки и обнаружения традиционных материальных следов (следов рук, различных предметов, документов) и виртуальных следов на электронных носителях компьютерной техники. В рамках осмотра дополнительно осмотреть прилегающую территорию и помещения с целью обнаружения камер видеонаблюдения и изъять видеозапись, установить очевидцев преступления и опросить их.

3 Изъять и осмотреть компьютерную технику и мобильные устройства с целью обнаружения и фиксации переписки пострадавшего и преступника, времени и продолжительности их звонков, пересылаемых файлов и другой значимой информации.

4. В случае перевода денежных средств через терминалы банков или платежные терминалы установить, имеются ли в помещениях камеры видеонаблюдения, изучить содержание записанной информации и изъять её.

Эффективность расследования вымогательства, совершенного с использованием сети Интернет, во многом зависит от быстроты принятия решений о производстве следственных и иных действий, направленных прежде всего на обнаружение и фиксацию доказательств в электронном виде. В основе этого лежит своевременное принятие решения о возбуждении уголовного дела и принятие его к производству в соответствии с правилами определения подследственности.

На первоначальном этапе расследования таких вымогательств необходимо запланировать и провести следующие следственные и иные процессуальные и непроцессуальные действия:

- допрос потерпевшего;
- допрос свидетелей (родственников потерпевшего, иных лиц, кому известны обстоятельства преступления, представителей организации, работников банков (кредитных организаций) и подставных лиц);
- подготовка и направление поручений оперативным подразделениям;
- назначение и производство судебных экспертиз (компьютерной, трасологической, дактилоскопической и портретной);
- допрос подозреваемого;
- обыск у подозреваемого;
- выемка (документов в банке, у оператора электронной платежной системы, у провайдера);
- осмотр документов и предметов (банковских документов, компьютеров, электронных носителей информации);
- наложение ареста на почтово-телеграфные отправления, их осмотр и выемка;
- проверка показаний на месте;

- получение информации о соединениях между абонентами и (или) абонентскими устройствами;

- контроль и запись переговоров;

- осмотр и прослушивание фонограммы, полученной в результате контроля и записи переговоров, а также осмотр документов, содержащих информацию о соединениях между абонентами и (или) абонентскими устройствами;

- проверка по оперативно-справочным, криминалистическим и иным учетам, а также базам данных;

- выемка в кредитных организациях сведений и документов по счетам лиц, куда переведены потерпевшим денежные средства;

- осмотр и анализ сведений и документов с целью определения периода, конкретного времени, сумм и маршрута движения денежных средств, их обналичивания и т. п.

При установлении в ходе расследования вымогательства фактов неправомерного доступа («взлома») злоумышленниками к аккаунтам граждан в социальных сетях или иной информации ограниченного доступа на других интернет-ресурсах, дознаватель в порядке, предусмотренном ст. 155 УПК РФ, выделяет в отдельное производство материалы, содержащие сведения о преступлении, предусмотренном ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», и направляет их в установленном порядке начальнику органа дознания для принятия решения в соответствии со статьями 144, 145 УПК РФ.

Наиболее длительными по времени исполнения являются процессуальные действия по истребованию криминалистически значимой информации от субъектов – участников информационного обмена. Поэтому своевременность и полнота запросов, направляемых в организации, обеспечивают соблюдение сроков дознания. Затягивание времени с принятием решений об истребовании сведений у кредитных организаций, операторов платежных систем, операторов связи, провайдеров и организаций, администрирующих сетевые сервисы, закономерно приводит к необходимости приостановления производства по делу и утере доказательств в электронно-цифровой форме.

В ситуациях совершения кибершантажа зачастую возникает необходимость направления запросов в организации, которым принадлежат сайты социальных сетей, почтовых сервисов, либо которые обеспечивают предоставление услуг хостинга сайтов, с целью установления сведений о лице, которому принадлежит определенный идентификатор, логин, ник, почтовый ящик или сайт.

Чтобы установить пользователя того или иного аккаунта в социальной сети или разместившего интересующий контент, необходимо обладать информацией о его IP-адресе. Искомая информация может быть

предоставлена непосредственно владельцами того интернет-ресурса, которым разыскиваемый абонент пользуется.

Знание IP-адреса пользователя позволяет установить город и страну проживания субъекта, а также получить информацию о его провайдере. В свою очередь провайдер уже имеет данные о фактическом местоположении пользователя проводного Интернета или о лице, которое приобрело SIM-карту.

Для получения сведений об IP-адресе дознавателю в соответствии с ч. 4 ст. 21 УПК РФ необходимо направить запрос руководству компании – владельцу социальной сети с просьбой предоставить используемый IP-адрес и время выхода в сеть конкретного субъекта. Время выхода в сеть позволит индивидуализировать разыскиваемое лицо в случае использования им динамического IP-адреса.

Для установления провайдера, предоставившего пользователю возможность выхода в Интернет, необходимо использовать базу данных IP-адресов интернет-провайдеров, размещенную в открытом доступе на интернет-ресурсе http://www.2ip.ru.

После установления провайдера ему необходимо направить запрос о предоставлении регистрационных данных пользователя, которому в конкретное время присваивался конкретный IP-адрес. В запросе рекомендуется также предоставлять информацию и о посещаемых искомым субъектом в указываемое время интернет-ресурсах. Это позволит индивидуализировать пользователя в случае предоставления интернет-провайдером услуг связи нескольким пользователям через единый узел связи под идентичным IP-адресом (преимущественно встречается при предоставлении услуг выхода в Интернет сотовыми компаниями).

Информация, возникающая в холе эксплуатации средств сотовых систем подвижной связи, может быть получена путем направления запросов операторам связи в порядке, предусмотренном ч. 4 ст. 21 УПК РФ. Однако операторы связи предоставляют по запросам только информацию справочного характера и отказывают в предоставлении конфиденциальной информации. Целесообразно оформлять получение сведений о детализации соединений абонентов сотовой связи по правилам ст. 165 УПК РФ, регламентирующей судебный порядок получения разрешения на производство следственных действий, ограничивающих права граждан.

При производстве следственного действия – получение информации о соединениях между абонентами и (или) абонентскими устройствами можно установить информацию о соединениях между абонентами и (или) абонентскими устройствами (дата, время, продолжительность соединений), номерах абонентов, других данных, дающих возможность идентифицировать абонентов, а также сведения о номерах и месте расположения приемопередающих базовых станции. Указанный процесс именуется биллингом. Его результаты позволяют не только выдвинуть и

проверить следственные версии, но и установить ряд различных обстоятельств, прямо или косвенно связанных с совершением преступления. В частности, определить круг лиц, с которыми ранее общался обвиняемый, установить период общения, конкретные даты, их соотношение со временем совершения преступления, факт общения с соучастниками (иными лицами) непосредственно перед совершением преступления. По номерам абонентов можно установить конкретных физических лиц, последующая проверка которых позволит установить степень их информированности о противоправной деятельности подозреваемых.

Под «информацию о соединениях между абонентами и (или) абонентскими устройствами» применительно к рассматриваемым преступлениям подпадает и информация о соединениях между абонентскими устройствами, в качестве которых выступает сетевое оборудование потерпевшего, преступника, иных лиц, провайдера сети Интернет, организации – платежной системы. К такой информации относятся IP-адреса, интервалы подключения к сети Интернет, иная информация о сетевых соединениях.

У сотовых компаний и Интернет-провайдеров типично истребуется информация:

- номеров IMEI сотового телефона преступника;

- сведений о номерах SIM-карт, ранее использовавшихся в сотовом телефоне преступника, с получением протоколов телефонных соединений на эти SIM-карты;

- о владельцах, на которых зарегистрированы номера сотовых телефонов, с которыми созванивался преступник, согласно ранее полученным сведениям о телефонных соединениях.

Запросы, адресованные руководителям операторов электронных платежных систем, чаще связаны с необходимостью в получении информации о движении денежных средств с электронного кошелька, зарегистрированного на имя конкретного лица, и средств на электронном кошельке получателя, установления его данных.

В ответах на запросы от указанных юридических лиц будут содержаться следующие сведения:

- IP-адрес, с которого был создан электронный кошелек, время его создания;

- сведения, которые указал о себе пользователь при регистрации (электронный почтовый ящик, абонентский номер мобильного телефона, адрес и другие);

- детальная информация о движении виртуальных денежных средств по интересующему электронному кошельку, с указанием IP-адресов и конкретного времени совершения операций.

Если вымогаемые деньги на определенном этапе совершения преступления были переведены на счет номера мобильного телефона, то необходимо направить запрос оператору сотовой связи, с целью установления личности владельца номера SIM-карты. Информацию о перемещении денежных средств также можно получить из ответов на запросы, полученных от соответствующих операторов связи.

Необходимо помнить, что информация, касающаяся движения средств по счетам, сведения о соединениях абонентов и абонентских устройств и т. п. информация относится к различным видам тайны и ее получение требует судебного решения.

Результаты записи телефонных переговоров могут быть исследованы в рамках фоноскопической экспертизы. Цель данной экспертизы – проверка подлинности фонограммы, отсутствия признаков ее монтажа, идентификация говорившего и звукозаписывающей аппаратуры.

Проведением экспертизы могут устанавливаться: пригодность звукозаписей телефонных переговоров для идентификации по голосу; принадлежность конкретных речевых фрагментов, реплик конкретным лицам; непрерывность звукозаписи разговора и отсутствие (наличие) признаков ее монтажа и др.

В условиях высокого риска уничтожения следов преступлений на ресурсах сети Интернет эффективность проверки версий требует быстрой организации и проведения поисковых действий, а также скоординированности всех участников процесса расследования со стороны обвинения. В таких ситуациях особую значимость приобретают шаблоны типовых тактических операций, которые разрабатываются с учетом вида совершенного преступления и особенностей ситуации расследования.

Одной из таких операций является «Деанонимизация», которая включает в себя следственные действия, оперативно-розыскные и технические мероприятия, направленные на установление оборудования и лиц, которые его использовали при удаленном соединении с сетевым оборудованием потерпевшей стороны, иных участников уголовного дела или для осуществления вербальной или текстовой коммуникации. Основная цель такой операции – обнаружение виртуальных следов, оставшихся на ресурсах сети Интернет, которые были задействованы в механизме коммуникации.

Планирование и реализация тактической операции должны начинаться как можно раньше и проходить во взаимодействии с сотрудниками оперативных подразделений органов внутренних дел, осуществляющих сопровождение расследования.

Важную роль в этом процессе играют процессуальные формы взаимодействия, такие как поручение дознавателя оперуполномоченным о производстве розыскных и следственных действий, а также уведомление дознавателя о результатах оперативно-розыскных мероприятий по делам,

переданным ему сотрудниками оперативных подразделений до установления преступника. Выполнение поручений дознавателя о проведении оперативно-розыскных мероприятий основывается на письменном задании с ясными задачами, выполнение которых требует применения оперативно-розыскных средств и методов.

Типично по рассматриваемой категории уголовных дел дознаватели поручают установить оперативно-розыскным путем:

- наименование оператора связи, выдававшего сим-карту, и его местонахождение и т. п. информацию;

- сведения о наименовании и местонахождении интернет-провайдера, выдававшего интересующий следствие IP-адрес;

- сведения о хостинг-провайдере интересующего следствие интернет-сайта.

Получение информации оперативным путем обеспечивает скорость и своевременность ее обработки. Однако, принимая решения об определении способов установления криминалистически значимых данных, необходимо учитывать, что при получении сведений по уголовным делам, находящимся в производстве подразделений дознания, от коммерческих организаций, функционирующих в информационно-телекоммуникационной сфере, возможности реализуемых средств уголовно-процессуального и оперативно-розыскного познания отличаются незначительно. Сотрудники оперативных подразделений ограничены в возможности применения всего арсенала оперативно-тактических средств по преступлениям, производство предварительного следствия по которым необязательно. В частности, к ним относится проведение оперативно-розыскных мероприятий (включая получение компьютерной информации), которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища. Исключение составляет лишь прослушивание телефонных и иных переговоров, производство которого допускается по делам о преступлениях средней тяжести[1].

В случаях, когда потерпевший выполнил требования преступника и перевел денежные средства, эффективность расследования может быть достигнута через тактическую операцию «Финансы». Она позволяет выявить участников электронных платежей, связанных с преступной деятельностью. В каждом преступлении, совершаемом в сети Интернет, присутствуют действия, связанные с осуществлением платежей и транзакций через электронные платежные системы. Кроме финансовых операций, которые являются частью способа совершения и сокрытия

[1] См.: Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ // СПС «КонсультантПлюс».

преступления, существуют платежи, которые обеспечивают возможность преступникам использовать сервисы и ресурсы сети Интернет. Это включает в себя платежи провайдеру за доступ в сеть, платежи хостинг-провайдерам, платежи за использование платных прокси-серверов и VPN, а также платежи за пользование другими сервисами и аренду оборудования. Эти действия создают обширную следовую картину у операторов платежных систем и администраторов интернет-сервисов, что позволяет восстановить цепочки платежей и выявить лиц, причастных к совершению преступления.

Примером, подтверждающим необходимость одновременного проведения названных тактических операций, может выступать уголовное дело № 1-21/2022, рассмотренное Шарыповским городским судом Красноярского края. Расследованием установлено, что реализуя преступные намерения «Н», используя личный мобильный телефон, подключенный к телекоммуникационной сети Интернет и имея доступ к странице потерпевшей в социальной сети, содержащей фотографии интимного характера и личную переписку последней, направил ей сообщение в мессенджере с требованием передачи ему 10 000 рублей под угрозой распространения, посредством социальных сетей среди её родственников и знакомых, фотографий интимного характера и личной переписки. Потерпевшая «А», опасаясь осуществления угрозы, перевела денежные средства на счёт банковской карты, указанный «Н». Доказательства по уголовному делу составили протокол осмотра документов о проведенной транзакции, протокол осмотра переписки в мессенджере, протокол осмотра документов с детализацией телефонных соединений абонентского номера, протокол осмотра электронных документов о движении денежных средств по счету банковской карты на CD-диске, протоколы выемки и осмотра мобильного устройства сотовой связи подозреваемого и другие доказательства[1].

Таким образом, предложенные рекомендации по производству дознания по делам о вымогательстве с использованием сети Интернет позволяют в оптимальные сроки, с учетом складывающихся на первоначальном этапе ситуаций расследования, с наименьшей затратой сил и средств, во взаимодействии с оперативными подразделениями органов внутренних дел собрать доказательства по делу и обеспечить успешное расследование.

[1] См.: Приговор № 1-21/2022 1-285/2021 от 7 февраля 2022 г. по делу № 1-21/2022. URL: https://sudact.ru/regular/doc/7UTgZ4SdBAHW/ (дата обращения: 11.01.2024).

ЗАКЛЮЧЕНИЕ

Применение изложенных рекомендаций обеспечивает реализацию обоснованных и эффективных приемов планирования дознания, производства процессуальных действий при расследовании по уголовным делам о преступлениях, предусмотренных частью первой статьи 163 Уголовного кодекса Российской Федерации, совершенных с использованием сети Интернет, точную и единообразную фиксацию их хода и результатов в процессуальных документах. Формирование понятных и доступных в реализации алгоритмов действий способствует более эффективной организации расследования, что оказывает положительное влияние на скорость расследования и его качество.

Представленные рекомендации, конечно, не могут в полной мере отразить все многообразие ситуаций расследования вымогательства, особенно в современных условиях криминального совершенствования механизма преступной деятельности – используемых средств и методов сокрытия следов в киберпространстве.

Предназначены для сотрудников территориальных подразделений дознания органов внутренних дел, могут быть использованы в рамках их служебной подготовки. Представленный материал также может применяться при изучении дисциплин «Криминалистика», «Расследование преступлений в сфере компьютерной информации», «Расследование отдельных видов преступлений, совершенных с использованием информационно-телекоммуникационных технологий» слушателями образовательных организаций МВД России.

Учебное издание

Александр Иванович Гайдин,
кандидат юридических наук, доцент;

Николай Юрьевич Дутов,
кандидат юридических наук, доцент;

Ирина Сергеевна Тройнина,
кандидат юридических наук;

Александр Николаевич Гущин,
кандидат юридических наук.

ДЕЙСТВИЯ ДОЗНАВАТЕЛЯ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, ПРЕДУСМОТРЕННЫХ ЧАСТЬЮ ПЕРВОЙ СТАТЬИ 163 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

Методические рекомендации

В авторской редакции.

Компьютерный набор И. С. Тройниной.

Объем 0,44 МБ.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53