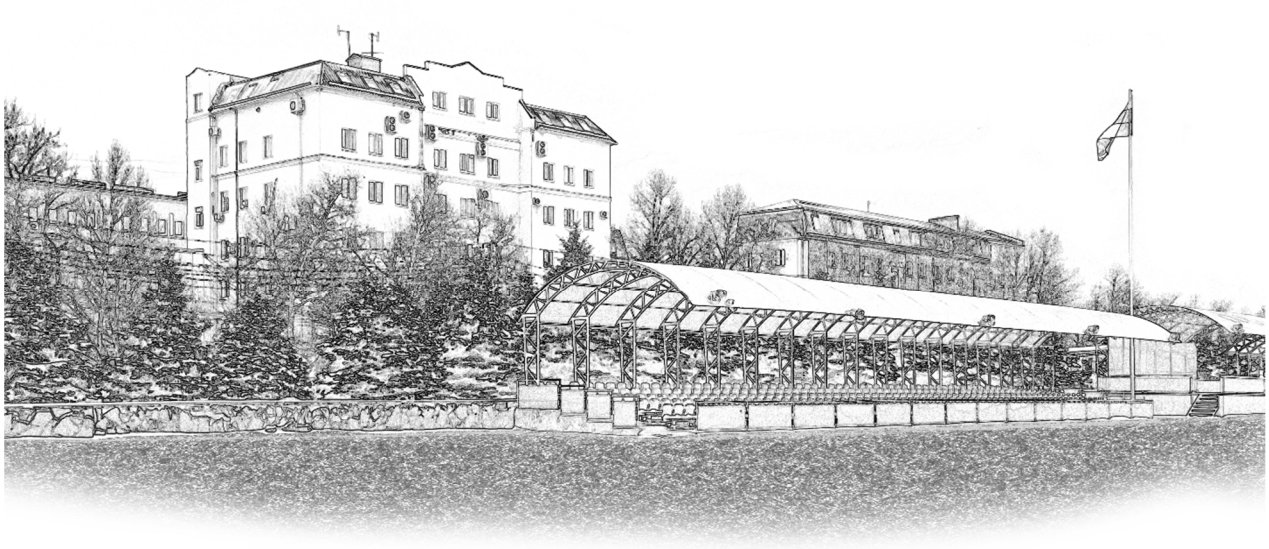
Краснодарский университет МВД России

В. С. Южанинов
А. С. Студнев
М. Ю. Савченко

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ



Краснодар
2024

Краснодарский университет МВД России

В. С. Южанинов
А. С. Студнев
М. Ю. Савченко

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Краснодар
2024

УДК 343.98
ББК 67
Ю174

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
А. А. Дягилев, кандидат юридических наук (Нижегородская академия МВД России);
П. Ю. Гензерский (Главное управление МВД России по Краснодарскому краю).

Южанинов В. С.

Ю174 Противодействие преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий : учебное пособие / В. С. Южанинов, А. С. Студнев, М. Ю. Савченко. – Краснодар : Краснодарский университет МВД России, 2024. – 88 с.

ISBN 978-5-9266-2052-5

Представлена оперативно-розыскная характеристика видов преступлений, связанных с использованием информационно-телекоммуникационных технологий, рассматриваются организационно-тактические особенности их раскрытия.

Для профессорско-преподавательского состава, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343.98
ББК 67

ISBN 978-5-9266-2052-5

Введение

Развитие информационно-телекоммуникационных технологий (далее – ИТТ), их активное внедрение в жизнь людей существенно упростили и ускорили множество действий и процессов, в том числе связанных с обменом информацией и осуществлением денежных расчетов. Данные факторы послужили предпосылками появления новых форм и методов совершения преступлений. К числу наиболее распространенных преступлений, совершаемых в сфере ИТТ, в настоящее время относятся различные виды мошенничеств.

Анализ статистических сведений о состоянии преступности показал, что в 2022 г. в Российской Федерации было зарегистрировано 1 966,8 тыс. преступлений, количество зарегистрированных мошенничеств (ст. 159, 159.3, 159.6 УК РФ) составило 343,1 тыс. преступлений (17,4% в общей структуре преступности). Основную массу таких преступлений составляют: мошенничества, совершенные с использованием ИТТ, – 257 606; мошенничества с использованием электронных средств платежа (ст. 159.3 УК РФ) – 7 288; мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) – 334. С учетом традиционно высокой латентности преступлений данного вида можно предположить, что фактическое число мошенничеств превышает официальные данные уголовной статистики. Раскрытие рассматриваемых преступлений остается на достаточно низком уровне. Так, в 2022 г. по ст. 159, 159.3, 159.6 УК РФ раскрыто 30 323 (+39,9%) преступлений, из них мошенничеств с использованием электронных средств платежа – 406 (-38,1%), мошенничеств в сфере компьютерной информации – 75 (-45,7%).

Значительная часть мошенничеств с использованием ИТТ совершается преступными группами, в том числе имеющими межрегиональный и межгосударственный характер, применяющими специальные приемы и методы совершения преступлений и сокрытия их следов, осуществляющими противодействие правоохранительным органам.

В силу специфики преступлений, совершаемых с использованием ИТТ, а также в связи с постоянным развитием технологий в рассматриваемой сфере, высоким удельным весом данных преступлений в структуре преступности необходимо совершенствование деятельности органов внутренних дел (далее – ОВД).

В первой главе настоящего учебного пособия описываются такие значимые элементы оперативно-розыскной характеристики преступлений данного вида, как состояние, структура и динамика; обстоятельства совершения и сокрытия преступлений; характеристика личности потерпевшего и лиц, совершающих мошенничества с использованием ИТТ; особенности виртуальных следов преступлений. Данная информация необходима оперуполномоченному для планирования и проведения оперативно-розыскных мероприятий, направленных на раскрытие преступления.

С учетом того, что современная судебно-следственная практика выдвигает особые требования к качеству документирования и информационного обеспечения оперативно-розыскной деятельности (далее – ОРД) по раскрытию преступлений в целом и мошенничеств с использованием ИТТ в частности, данное направление деятельности нашло подробное отражение во второй главе пособия.

1. Оперативно-розыскная характеристика мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий

Совокупность сведений об информационных особенностях отдельного вида или группы преступлений в теории ОРД образует оперативно-розыскную характеристику. Знание оперативно-розыскной характеристики конкретного вида преступлений является информационным базисом, который определяет алгоритм действий сотрудника при раскрытии какого-либо преступления.

Подробно раскрыть все применяемые преступниками схемы и методы в рамках настоящей работы не представляется возможным, поэтому целесообразно сосредоточиться на рассмотрении, описании и систематизации наиболее распространенных и актуальных в настоящее время видов и схем мошенничеств, совершаемых с использованием сети Интернет, телефонной (в том числе подвижной радиотелефонной), почтовой связи, платежных систем и ресурсов, обеспечивающих обмен денежными ресурсами и их эквивалентами и их передачу, а также логистических и почтовых организаций.

Способы совершения рассматриваемых преступлений квалифицируются по ст. 159 УК РФ (мошенничество), ст. 159.3. УК РФ (мошенничество с использованием платежных карт), ст. 159.6. УК РФ (мошенничество в сфере компьютерной информации).

Мошенничества, совершенные с использованием ИТТ, проявляются как структурный элемент корыстной преступности.

Совокупность данных, характеризующих мошенничества, совершенные с использованием ИТТ, показывает, что структуру их оперативно-розыскной характеристики формируют следующие наиболее важные элементы:

состояние, структура и динамика преступления;

обстоятельства совершения преступления (место, время, способ совершения (легенда) и сокрытия);

характеристика личности потерпевшего и лиц, совершающих преступления;

особенности виртуальных следов.

Рассмотрим указанные элементы подробнее.

Состояние, структура и динамика мошенничеств, совершаемых с использованием ИТТ

Данный элемент оперативно-розыскной характеристики мошенничеств, совершаемых с использованием ИТТ, имеет существенное значение для организации ОРД по раскрытию преступлений данного вида. Сведения о преступности позволяют выявлять оперативно значимые факторы, влияющие на численность и структуру оперативных подразделений, специализирующихся на раскрытии мошенничеств с использованием ИТТ, организацию межведомственного и межрегионального взаимодействия.

По данным ГИАЦ МВД России, общее число зарегистрированных преступлений в 2022 г. снизилось на 1,9%. Количество зарегистрированных мошенничеств увеличилось на 1% и составило по итогам 2022 г. 343 085 преступлений. Удельный вес мошенничеств в общей структуре преступности составил 17,4%. Таким образом, почти каждое шестое регистрируемое преступление на территории России – мошенничество.

Статистические данные свидетельствуют о том, что количество мошенничеств, совершаемых с использованием ИТТ, постоянно растет с 2015 г. При этом уже к 2016 г. число мошенничеств, совершаемых с использованием сети Интернет, практически сравнялось с числом мошенничеств, совершаемых с использованием средств мобильной связи, а в 2017 г. – превысило этот показатель. Такая динамика состояния преступности сохраняется и в настоящее время, можно предположить, что сохранится и в дальнейшем.

Наибольшие темпы прироста преступлений, совершенных с использованием ИТТ, зарегистрированы в январе-марте 2023 г. в Республике Ингушетия (106,8%), Ненецком автономном округе (103,4%), Магаданской (83%), Томской (81,9%) и Ярославкой (74,9%) областях.

Динамика и структура отдельных видов мошенничеств, совершаемых с использованием ИТТ, приведены в таблицах 1–6.

Таблица 1

ПРЕСТУПЛЕНИЯ, СОВЕРШЕННЫЕ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

РЕГИОНЫ С НАИБОЛЬШИМИ ТЕМПАМИ ПРИРОСТА ЗАРЕГИСТРИРОВАННЫХ ПРЕСТУПЛЕНИЙ, в %

Таблица 2

РЕГИОНЫ С НАИМЕНЬШИМИ ТЕМПАМИ ПРИРОСТА ЗАРЕГИСТРИРОВАННЫХ ПРЕСТУПЛЕНИЙ, в %

Таблица 3

УДЕЛЬНЫЙ ВЕС ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (В ОБЩЕЙ СТРУКТУРЕ ПРЕСТУПНОСТИ)

РЕГИОНЫ С НАИБОЛЬШИМ УДЕЛЬНЫМ ВЕСОМ, в %

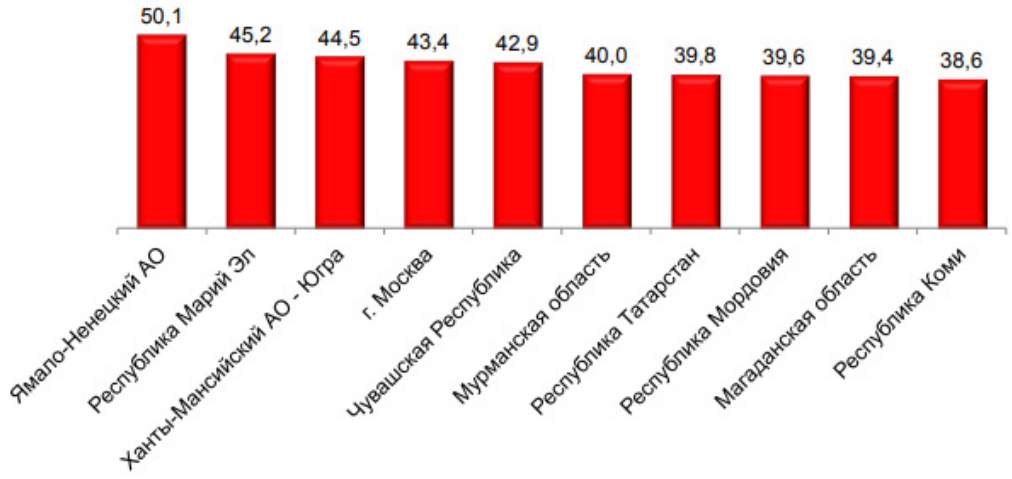


Таблица 4

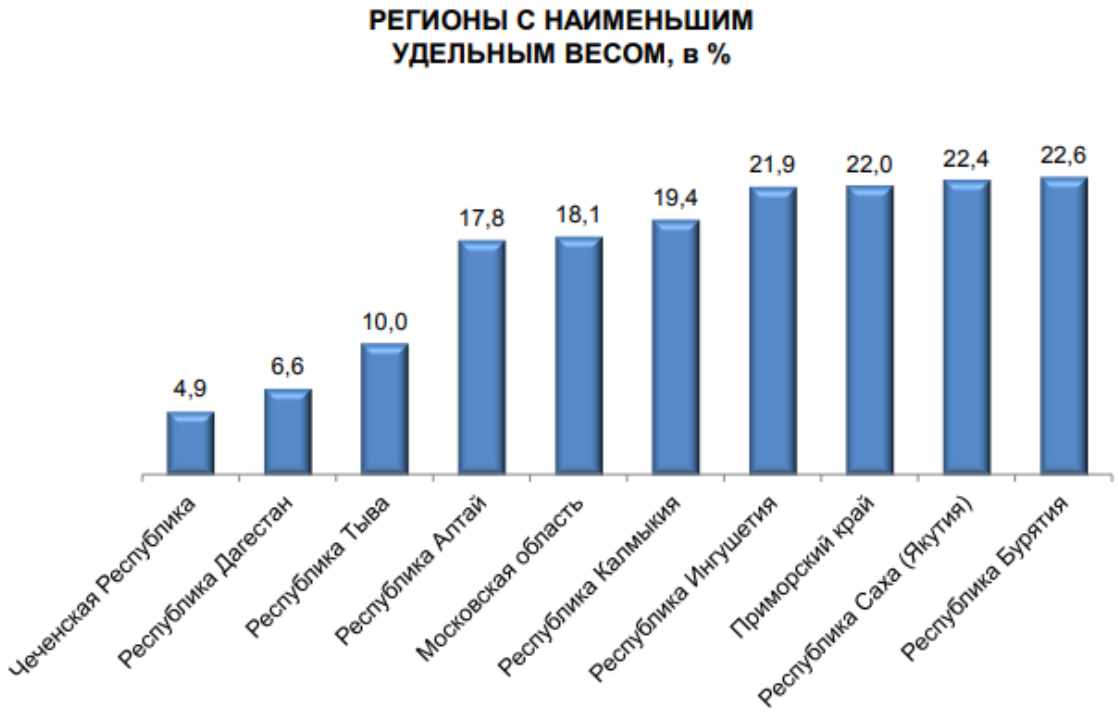


Таблица 5

РАСКРЫВАЕМОСТЬ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Таблица 6

Обстоятельства совершения преступления (место, время, способ совершения (легенда) и сокрытия преступлений)

Обстоятельства совершения преступления имеют важное значение для формирования оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИТТ. К ним относятся следующие элементы: место, время, способ совершения (легенда мошенничества)[1] и сокрытия следов преступления. Значимость данного элемента оперативно-розыскной характеристики рассматриваемых видов преступлений определяется тем, что в соответствии с п. 1 ч. 1 ст. 73 УПК РФ при производстве по уголовному делу подлежат доказыванию время, место, способ и другие обстоятельства совершения преступления.

[1] Здесь и далее легенда мошенничества понимается как совокупность сведений, предоставляемых преступником потерпевшему с целью убеждения последнего в том, что преступник действительно является тем, за кого себя выдает (сотрудник банка или правоохранительных органов; родственник, попавший в беду; продавец или покупатель товара и услуги и др.).

При описании мошенничеств, совершенных с использованием ИТТ, следует учитывать не только средства и способ коммуникации между потерпевшими и преступниками, но и легенду мошенничества, средства и способ передачи денежных средств, характеристику личности и особенности местонахождения преступника и потерпевшего.

Изучение массива данных о мошенничествах, совершенных с использованием ИТТ, позволяет структурировать их следующим образом.

1. Преступления, связанные с фиктивной продажей товаров или услуг посредством сети Интернет.

Алгоритм действий преступников следующий. Преступником создается объявление о продаже товара или оказании услуг на специализированном сайте в сети Интернет[1] (в том числе посредством приложения для мобильных устройств) или на форуме в социальной сети[2]. Помимо этого, возможна публикация такого объявления посредством газет[3] или «бегущей строки». При создании или публикации объявления указываются реквизиты для обратной связи. Товар или услуга могут быть практически любые, разрешенные правилами сайта или конкретного средства массовой информации.

В качестве средства для обратной связи преступниками могут использоваться: обычный абонентский номер телефонной связи (чаще – подвижной радиотелефонной, реже – стационарной); абонентский номер, предоставляемый посредством IP-телефонии[4]; идентификационный номер программы или приложения для мгновенного обмена сообщениями, осуществления аудио- и видеозвонков[5], адрес электронной почты. Цена товара или услуги,

---

[1] См., например: URL: http://www.avito.ru, URL: http://youla.io, URL: http://drom.ru, URL: http://kupiprodai.ru, URL: http://market.yandex.ru и др.

[2] См., например: ВКонтакте, Одноклассники, Мой Мир и др.

[3] См., например: «Из рук в руки».

[4] Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение посредством сети Интернет.

[5] Например: Skype, Hangouts, Алле, TOX, ooVoo, KakaoTalk и др.

указанная в объявлении, как правило, ниже рыночной (для привлечения внимания потенциального потерпевшего). После того как потерпевший свяжется с преступником, ему предлагается осуществить полную или частичную оплату товара или услуги.

Как правило, преступник готов предоставить документы, удостоверяющие личность, подтверждающие наличие товара и его качество, факт отправления товара потерпевшему. Достигается это за счет предоставления реальных фотографий товара, документов, удостоверяющих личность или подтверждающих почтовое отправление товара, или за счет предоставления фиктивных фотографий таких товаров или документов, полученных с помощью программных средств[1]. В некоторых случаях преступник отправляет почтой или логистической организацией муляж товара, соответствующий весом реальному товару, для того чтобы иметь возможность предоставить потерпевшему трек-код[2], что создает уверенность в действительности сделки.

Потерпевшими денежные средства могут отправляться на банковскую карту, лицевой счет в банке, электронный кошелек, путем перевода на предъявителя[3]. Данный вид мошенничеств совершается, как правило, в одиночку (74% случаев), при этом к осуществлению отдельных действий могут привлекаться иные лица, не осведомленные об участии в конкретном преступлении. Например, широко распространена практика приобретения мошенниками банковских карт у третьих лиц посредством сети Интернет или при личном контакте[4].

Рассматриваемые преступления совершаются мужчинами в 62% случаев, женщинами – в 38%.

---

[1] Например, Photoshop.

[2] Трек-код – это номер отслеживания почтового отправления, уникальный почтовый идентификатор, по которому можно отследить посылку и узнать ее месторасположение. Трекинг посылок – это механизм, определяющий текущий статус с последующим отслеживанием почтового отправления.

[3] Данную услугу предоставляет большинство кредитных организаций. Для получения перевода требуется, как правило, предъявление паспорта и кода, который сообщается отправителю перевода при его оформлении. Получение возможно в любом отделении кредитной организации в любом регионе России, а также в некоторых отделениях за пределами страны. В качестве примера можно привести услугу ПАО Сбербанк России «Колибри».

[4] Стоимость такой банковской карты, как правило, составляет 500–1000 рублей.

Преступления, составляющие данную категорию, в настоящее время являются наиболее распространенными в структуре мошенничеств, совершенных с использованием ИТТ, их удельный вес от общего числа составляет 37%;

2. Преступления, связанные с фиктивной покупкой товаров или услуг посредством сети Интернет.

Алгоритм действий преступников следующий. Преступник осуществляет мониторинг сети Интернет с целью обнаружения объявлений о продаже товаров или предоставлении услуг. Чаще всего просматриваются специализированные сайты, аналогичные указанным в описании мошенничеств при фиктивной продаже товара. Обнаружив объявление, преступник звонит потерпевшему и сообщает о своем желании приобрести товар или услугу, просит сообщить полные данные банковской карты потерпевшего. После этого преступник посредством ресурсов, доступных в сети Интернет[1], предпринимает попытки перевода денежных средств с банковской карты потерпевшего. В некоторых случаях преступник просит сообщить также приходящие потерпевшему пароли[2].

После того как потерпевший сообщает необходимые данные, преступник производит перевод денежных средств потерпевшего со счета его банковской карты. Помимо этого, распространена форма хищения, связанная с подключением преступника к услугам интернет-банкинга. В данном случае преступник просит подойти к банкомату и выполнить действия, якобы связанные с осуществлением платежа. Фактически потерпевший самостоятельно

[1] Самые распространенные ресурсы (сервисы) предоставляются кредитными организациями. Общее название таких ресурсов «card-to-card» (от англ. «с карты на карту»). Для перевода необходимо, как правило, введение кода подтверждения операции, который приходит потерпевшему на телефон.

[2] В случае если ресурс, используемый преступниками, не поддерживает технологии 3DSecure или MasterCard SecureCode (принятые основными платежными системами, такими как Visa, MasterCard, Мир и другими), то SMS-сообщение с кодом потерпевшему не приходит. Ресурсы, не поддерживающие данные технологии, чаще всего связаны с внесением денежных средств на счета сайтов, специализирующихся на азартных играх, ставках на спортивные события и др. В отдельных случаях возможны оплата без кода подтверждения услуг телефонной связи некоторых операторов связи, внесение денежных средств на игровые порталы и т. д.

подключает свою банковскую карту к абонентскому номеру преступника и предоставляет ему код для первоначального входа в интернет-банкинг[1].

3. Преступления, связанные с рассылкой SMS-сообщений.

Алгоритм действий преступников следующий. Потерпевшим рассылаются SMS-сообщения следующего содержания: «Ваша банковская карта заблокирована ЦБ РФ. Телефон для справок…», «Вы получили приз, дополнительная информация по телефону…», «С Вашей банковской карты списано **** рублей по решению суда. Дополнительная информация по телефону…», «Банком проводятся операции по защите от краж с банковских карт. Вам необходимо пройти до банкомата и связаться со специалистом банка по телефону…» и т. д.

В случае если потерпевший перезванивает, ему предлагается сообщить полные данные банковской карты, а также приходящие коды подтверждения операций, после получения которых преступником осуществляется списание денежных средств.

Альтернативным способом совершения таких преступлений является убеждение преступником потерпевшего пройти к банкомату и выполнить действия, указанные «сотрудником банка». В ходе выполнения данных действий потерпевший подключает услугу «мобильный банк» к абонентскому номеру, указанному преступником, а также в отдельных случаях сообщает преступнику логин и пароль для первичного входа и подключения услуги интернет-банкинга. После этого потерпевшему перестают приходить SMS-оповещения (или push-оповещения) об операциях,

[1] В соответствии с п. 2 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если обман не направлен непосредственно на завладение чужим имуществом, а используется только для облегчения доступа к нему, действия виновного, в зависимости от способа хищения, образуют состав кражи или грабежа. В связи с этим преступления, совершенные описанным способом, стали квалифицироваться на практике с 2018 г. как кража. Несмотря на изменения, связанные с квалификацией таких преступлений, методики действий по их раскрытию не претерпели существенных изменений и аналогичны применяемым по отношению к иным мошенничествам, совершенным с использованием ИТТ. В связи с этим мы рассмотрим вопросы оперативно-розыскного противодействия преступлениям данной категории вместе с мошенничествами, совершенными с использованием ИТТ.

преступник похищает все денежные средства со всех счетов потерпевшего.

Несколько иначе реализуется алгоритм преступных действий при SMS-сообщениях о выигрыше в акции (чаще всего автомобиля). В таких ситуациях потерпевшему самостоятельно предлагается направить денежные средства, предназначенные для оплаты «налога» или «пошлины» за выигрыш, или «доставки» выигрыша потерпевшему.

При совершении преступлений таким способом преступниками нередко создается сайт в сети Интернет, действующий несколько дней. Сайт может дублировать дизайн известных организаций, специализирующихся на торговле автомобилями, при этом на нем размещается информация о проведении «акции», о которой сообщено в SMS-сообщении. Телефоны «победителей», как правило, указываются не полностью, а в формате 890251*****, 890866***** и т. д., т. е. используется диапазон номеров, на которые преступниками направлялись SMS-сообщения с ложной информацией о выигрыше. Неполное указание номера объясняется соблюдением закона о защите персональных данных.

Денежные средства могут направляться любым способом, чаще переводом на указанный преступником номер банковской карты.

Удельный вес преступлений в структуре мошенничеств, совершенных с использованием ИТТ, составляет 12%;

4. Преступления, связанные со звонками на стационарные или мобильные телефоны потерпевших с ложным сообщением о том, что их родственник попал в беду (сбил на машине пешехода, был задержан сотрудниками полиции с наркотиками, избил хулигана, а тот обратился в полицию и др.), в связи с чем требуются денежные средства для решения вопроса с правоохранительными органами или выплаты компенсации «пострадавшим».

Алгоритм совершения преступлений данной категории следующий. Преступник сообщает о факте совершения родственником потерпевшего какого-либо противоправного деяния. Как правило, потерпевшими по данному преступлению являются лица пожилого возраста (55–85 лет), женщины (94%), проживающие в одиночестве (87%). В случае если потерпевший указывает на то,

что голос не похож на голос предполагаемого родственника, это объясняется полученными в результате ДТП повреждениями, волнением и т. д., а телефон быстро передается для разговора иному лицу (например, «следователю»). После этого «следователь» сообщает, что для компенсации ущерба требуются деньги. В случае если потерпевший согласен предоставить денежные средства для помощи «родственнику», то «родственник» или «следователь» сообщают, что за ними подъедет третье лицо (83% случаев). Данный факт связан с преклонным возрастом потерпевших и обусловлен трудностями в перемещении и использовании ИТТ, а также необходимостью не допустить у потерпевшего мысли об обмане или консультации с иными лицами. Реже потерпевшему предлагается самостоятельно отправить денежные средства (17% случаев). Как правило, денежные средства передаются посреднику по месту жительства потерпевшего, в квартире, на лестничной площадке или возле дома. Чаще всего посредники подбираются из числа лиц, работающих водителями такси (76%), либо лиц, разместивших в сети Интернет объявления о поиске работы, в основном курьерской (24%). После получения от потерпевшего согласия передать деньги для освобождения «родственника» преступник осуществляет поиск посредника путем звонка в фирму такси или по объявлению в сети Интернет. Посреднику предлагается доехать до указанного адреса, забрать деньги и отправить их преступнику указанным последним способом. В качестве вознаграждения посредник берет часть денежных средств, переданных потерпевшим.

При совершении мошенничеств данной категории преступники, как правило, осуществляют поиск потерпевших путем сплошного набора абонентских номеров в выбранном диапазоне с изменением последней цифры.

В связи с этим потерпевшие по разным преступлениям, совершенным одними и теми же лицами в небольшой промежуток времени, нередко живут в одном населенном пункте[1]. Данный факт стал причиной еще одной особенности мошенничеств данного вида, которая заключается в том, что преступники стараются

[1] Этот факт связан с особенностью распространения SIM-карт, заключающейся в том, что часто серия абонентских номеров в одном диапазоне нередко распространяется в ограниченный период времени в одном населенном пункте.

поддерживать связь с посредниками, которые успешно выполнили требуемые от них действия (т. е. получили от потерпевших деньги и перевели их преступнику), для того чтобы при совершении других преступлений вновь воспользоваться их помощью. Это во многом обусловлено отсутствием необходимости подыскивать нового посредника. Посредники не всегда сразу осознают факт, что участвуют в преступной деятельности. Часто понимание преступного характера совершаемых действий наступает на втором или последующих преступлениях.

При совершении мошенничеств данного вида могут использоваться те же программно-технические средства, что и в первом случае: стационарные компьютерные системы и мобильные устройства, банковские счета, карты и т. д.

Данным противоправным деяниям свойственен групповой характер. 64% преступлений совершены двумя и более лицами. Удельный вес таких преступлений в структуре мошенничеств, совершенных с использованием ИТТ, составляет 27%.

5. Преступления, связанные с фиктивным предоставлением кредитов.

Алгоритм действий преступников следующий. В социальных сетях создается фейковый (от англ. fake – обман, фальсификация) аккаунт, указывающий на принадлежность его владельца к кредитной организации (например, «Ольга Сбербанк» или «Василий банк»), либо создается страница, имитирующая страницу официальных банков, где потерпевший размещает заявку на получение кредита. Преступником распространяется ссылка на данную страницу. Когда потерпевший обращается к владельцу страницы[1], ему сообщается, что владелец данной страницы может повлиять на положительное решение банка о предоставлении кредита, однако для этого необходима предварительная оплата. Чаще всего потерпевшему предлагается оплатить процент от суммы кредита (1–5%), иногда требуется направление фиксированной суммы. После получения денежных средств преступник прекращает переписку с потерпевшим и удаляет аккаунт в социальной сети.

[1] Общение может осуществляться как в форме сообщений, доступных для всех посетителей страницы, так и в личных сообщениях. Иногда после первичного обращения потерпевшего предлагается продолжить дальнейшее общение в одном из мессенджеров.

Удельный вес описанных преступлений в структуре мошенничеств, совершенных с использованием ИТТ, составляет 27%.

6. Преступления, связанные с распространением биологически активных добавок (далее – БАД), медицинских аппаратов, «чудодейственных» амулетов, мощей святых, икон.

Алгоритм совершения преступлений данной категории следующий. Преступниками посредством объявлений в газетах, текстов «бегущей строки» распространяется информация о проведении компьютерного тестирования состояния здоровья. Когда потерпевший звонит по телефону из объявления, ему предлагается отправить образцы слюны, ногтей, волос по указанному почтовому адресу. Адрес, как правило, является вымышленным или дублирует адрес какого-либо известного медицинского учреждения. В ходе беседы преступники стараются выяснить дополнительную информацию о потерпевшем, его возрасте, заболеваниях, артериальном давлении, частоте посещения поликлиник, вероисповедании и т. д. Через несколько дней после отправления потерпевшим образцов (факт их получения преступниками не имеет никакого значения), ему звонят и сообщают, что по результатам тестирования у него выявлено тяжелое заболевание, и предлагают приобрести средство для излечения. Основной упор преступниками в данном случае делается на то, что только они могут излечить потерпевшего от заболевания, указывается на мнимую некомпетентность сотрудников официальных учреждений здравоохранения. Могут делаться акценты на религиозности или суевериях потерпевшего (в случае предложения приобретения «мощей святых» или амулетов). Во всех случаях преступниками используется медицинская неграмотность потерпевших. Характерной особенностью данного вида мошенничеств является постоянная смена абонентских номеров, используемых преступниками, а также смена исполняемых «ролей». Мошенники могут представляться народными целителями, профессорами медицины, экстрасенсами и т. д. Отличительной чертой мошенничеств данного вида является то, что потерпевшие могут отправлять деньги многократно. Чаще всего денежные средства при данном виде мошенничеств направляются потерпевшими самостоятельно посредством переводов на предъявителя.

После того как потерпевшие осознают, что в отношении них было совершено преступление (когда предлагаемые мошенниками БАДы или амулеты и т. д. не поступают к потерпевшему, или когда родственники потерпевших узнают о данном факте и рассказывают о том, что они стали жертвой мошенников), преступники нередко предпринимают попытки повторного совершения преступления в отношении этих же лиц, меняют используемую легенду и часто действуют следующим образом.

Потерпевшему поступает звонок от имени «следователя прокуратуры» или несуществующего государственного учреждения, а также сообщается, что лица, которым потерпевший ранее отправлял деньги, задержаны. Потерпевшему полагается возмещение ущерба в сумме, многократно превышающей отправленную, однако для получения компенсации необходимо отправить «налог» или «пошлину» в сумме 13% (или ином процентом соотношении). После того как потерпевший направляет нужную сумму, ему сообщается, что расчет суммы компенсации был произведен неправильно и потерпевшему полагается значительно большая сумма. Для этого требуется вновь доплатить разницу в сумме «налога» или «пошлины». Данная ситуация повторяется до тех пор, пока потерпевший соглашается платить.

Для разговоров с потерпевшим используется, как правило, IP-телефония. При этом договор на оказание услуг связи заключается дистанционно с использованием вымышленных регистрационных данных. Преступниками предпринимаются меры по обеспечению анонимизации в сети Интернет. Для совершения преступлений арендуются офисные помещения, привлекаются группы людей, которые проходят специальную подготовку. Денежные средства получаются в отделениях банков разных регионов третьими лицами, установление которых затруднительно. Поиск таких посредников преступниками осуществляется посредством сети Интернет, закрытых групп в мессенджерах, а также случайным образом вблизи отделений кредитных организаций. Роль посредников при совершении таких преступлений, как правило, заключается в обналичивании денежных средств, направленных на их имя потерпевшими посредством банковских переводов,

и последующей передаче данных денежных средств преступникам. Посредники, как правило, участвуют в совершении мошенничеств данного вида не более одного раза.

Раскрытие преступлений рассматриваемой категории представляет особую сложность в связи с высокой степенью подготовленности совершающих их лиц.

При совершении мошенничеств данного вида могут использоваться стационарные и мобильные телефоны и устройства, банковские счета и карты, различные ресурсы сети Интернет, газеты и рекламные печатные издания, телевидение и т. д.

Удельный вес таких преступлений в структуре мошенничеств, совершенных с использованием ИТТ, составляет 4%.

Изучение массива сведений о мошенничествах с использованием ИТТ позволило выявить основные ресурсы и средства, применяемые при их совершении. Такой ресурс, как криптовалюта, в общей структуре мошенничеств с использованием ИТТ встречается в 0,2% случаев, при этом ни по одной из категорий преступлений данного вида криптовалюта не использовалась более чем в 0,3% случаев.

Наибольшую часть в структуре мошенничеств, совершенных с использованием ИТТ, составляют мошенничества, связанные с фиктивной покупкой и продажей товаров или услуг посредством сети Интернет. Все описанные мошенничества, совершенные с использованием ИТТ, объединяет факт обращения к средствам мобильной связи, услугам кредитных организаций, сети Интернет.

Особое значение в структуре оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИТТ, имеет место совершения преступления.

В традиционном понимании место совершения преступления воспринимается как участок местности с его географическими особенностями, рельефом, прилегающими объектами, на котором при встрече потерпевшего с преступником последним реализуются действия, запрещенные уголовным законодательством. При рассмотрении места совершения преступления с точки зрения криминалистики интерес в первую очередь представляют следы, которые могут способствовать установлению виновного лица, обсто-

ятельств преступления и т. д. В то же время с точки зрения криминологии важными являются особенности места преступления в контексте устранения причин и условий, способствующих его совершению.

В случаях совершения мошенничеств с использованием ИТТ встреча потерпевшего и преступника в привычном понимании, как правило, не происходит. Одной из особенностей мошенничеств, совершенных с использованием ИТТ, является то, что преступник и потерпевший проживают (до 80–85% преступлений данной категории) в различных регионах и их «встреча» осуществляется посредством мобильной связи или ресурсов сети Интернет. При этом сам факт общения потерпевшего и преступника не образует состав преступления. Для этого необходимо наступление вреда в виде материального ущерба, который выражен в получении виновным лицом возможности распоряжаться денежными средствами потерпевшего. В соответствии со ст. 140 ГК РФ платежи на территории Российской Федерации осуществляются путем наличных и безналичных расчетов, т. е. находящиеся на счетах в банках денежные суммы могут использоваться в качестве платежного средства. Исходя из этого с момента зачисления денег на банковский счет лица оно получает реальную возможность распоряжаться поступившими денежными средствами по своему усмотрению (например, осуществлять расчеты от своего имени или от имени третьих лиц, не снимая денежных средств со счета, на который они были перечислены в результате мошенничества). В указанных случаях преступление считается оконченным с момента зачисления этих средств на счет лица, которое путем обмана или злоупотребления доверием изъяло денежные средства со счета их владельца, либо на счета других лиц, на которые похищенные средства поступили в результате преступных действий виновного[1].

Таким образом, на первоначальном этапе значимыми обстоятельствами для установления места совершения мошенничеств с использованием ИТТ становятся следы преступления, остающи-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 27 дек. 2007 г. № 51. Доступ из справ. правовой системы «Гарант».

еся только в особой информационной среде, за исключением преступлений, при совершении которых участвует посредник, встречающийся с потерпевшим. Совершению мошенничеств с использованием ИТТ способствуют прежде всего не особенности какого-либо участка местности, а доступность технологических решений, обеспечивающих связь между преступником и потерпевшим, а также обмен денежными средствами.

Факт нахождения преступника и потерпевшего в разных регионах Российской Федерации в момент совершения преступления, а также недостатки нормативного правового регулирования данного вопроса стали причиной противоречий, возникающих между сотрудниками различных практических подразделений ОВД при определении места преступления по различным видам мошенничеств с использованием ИТТ.

Существуют следующие основные проблемы при установлении места совершения преступления по мошенничествам с использованием ИТТ: отсутствие законодательной регламентации места совершения преступления с материальным составом, а также недостаточность на первоначальном этапе информации об обстоятельствах мошенничеств, совершенных с использованием ИТТ, необходимых для установления фактического места совершения преступления.

В связи с изложенным представляется обоснованным следующий комбинированный подход к решению проблемы. Местом преступления по мошенничествам, совершенным с ИТТ, является место выполнения преступником действий, составляющих объективную сторону преступления, вне зависимости от места наступления последствий, места обналичивания денежных средств или местонахождения потерпевшего. Как правило, это место совпадает с фактическим местонахождением преступника.

В то же время на первоначальном этапе рассмотрения заявления о мошенничестве, совершенном с использованием ИТТ, редко имеется достоверная, документально подтвержденная информация о местонахождении преступника в момент выполнения действий, составляющих объективную сторону преступления. В таком случае доследственная проверка должна проводиться, а уго-

ловное дело возбуждаться по месту выявления преступления, в соответствии с требованиями действующих нормативных правовых актов, регламентирующих рассмотрение заявлений о преступлениях[1], т. е. по месту обращения потерпевшего в ОВД.

Время совершения преступления

Изучение информации о зарегистрированных мошенничествах, совершенных с использованием ИТТ, не позволило выявить закономерности во времени совершения таких преступлений, за исключением отдельного поискового признака мошенничеств, связанных с сообщением о родственнике в беде. При совершении преступлений данного вида возможно выдвижение версии о совершении преступления лицом, находящимся в учреждении ФСИН России, по времени первичного звонка, поступившего потерпевшему. При серии аналогичных преступлений данного вида и систематических звонках в один и тот же период времени можно предположить, что преступник при выполнении объективной стороны преступления связан временными рамками, обусловленными режимом работы учреждений ФСИН России с поправкой на регион местонахождения. В то же время до 40% преступлений данного вида (по отдельным регионам) совершаются лицами, не осужденными к лишению свободы и находящимися на свободе. Кроме того, рассматриваемые преступления могут совершаться осужденными лицами, находящимися в учреждениях ФСИН России, вне зависимости от режима работы учреждения. В связи с изложенным временной критерий с практической точки зрения малоприменим. Это обусловлено тем, что время совершения преступления для потерпевшего не коррелирует со временем преступления для преступника.

---

[1] См.: Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях: приказ МВД России от 29 авг. 2014 г. № 736; Об усилении прокурорского надзора и ведомственного контроля за законностью процессуальных действий и принимаемых решений об отказе в возбуждении уголовного дела при разрешении сообщений о преступлениях: приказ Генпрокуратуры России, МВД России, ФСБ России, СК России, ФСКН России, ФТС, ФСИН, Минобороны России, ФССП, МЧС от 26 марта 2014 г. 147/209/187/23/119/596/149/196/110/154; Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ. Доступ из справ. правовой системы «Гарант».

Как указывалось, 77,6% уголовных дел о мошенничествах, совершенных с использованием ИТТ, возбуждены вне региона местонахождения преступника. Таким образом, в этих случаях время преступления для преступника не будет соответствовать времени преступления для потерпевшего из-за разницы часовых поясов. Кроме того, выполнение объективной стороны для отдельных видов мошенничеств, совершенных с использованием ИТТ, занимает не одни сутки (например, для мошенничеств, связанных с фиктивной продажей товаров). В таких случаях только предварительная переписка может занимать не один день, а преступник в течение этого времени может неоднократно сменить свое местонахождение, в том числе регион. Кроме того, при совершении групповых мошенничеств с использованием ИТТ соучастники преступлений могут одновременно находиться в разных регионах, и для каждого действующего лица, в том числе потерпевшего, будет свое время.

Изложенное не позволяет утверждать о практической значимости углубленного изучения времени для организации оперативно-розыскного противодействия мошенничествам, совершенным с использованием ИТТ.

Характеристика личности потерпевшего и лиц, совершающих мошенничества с использованием ИТТ

Анализ мошенничеств, совершенных с использованием ИТТ, позволяет сделать вывод, что личностные особенности и преступника, и потерпевшего имеют существенное значение для успешного завершения начатого преступления. Действительно, очень важным становится умение преступника убеждать, менять свои слова и действия в зависимости от линии поведения потерпевшего. Легковерность потерпевшего, степень его осведомленности об ИТТ также зачастую имеют решающее значение. Аналогичное мнение высказывает В.В. Джумазаде: «Действия преступника часто зависят не только от его личностных особенностей, наклонностей и стремлений, но и от поведения потерпевшего, который своими неосторожными, аморальными и противоправными поступками может подать «идею» преступления, создать криминальную обстановку, облегчить наступление преступного результата. По-

этому при анализе роли конкретной жизненной ситуации в совершении преступления необходима всесторонняя и объективная оценка значения поведения потерпевшего»[1].

В связи с этим знание о личности преступника имеет большое значение для организации оперативно-розыскного противодействия мошенничествам, совершенным с использованием ИТТ.

По результатам анализа оперативно-следственной практики установлено, что преступления данной категории по возрасту потерпевших распределились следующим образом (табл. 7).

Таблица 7

Возрастные категории потерпевших при совершении мошенничеств с использованием ИТТ

Возраст / Противоправное деяние	до 35 лет	35–50 лет	50–65 лет	старше 65 лет
Мошенничества, совершенные с использованием ИТТ	21%	33%	39%	7%
Мошенничества, совершенные с использованием мобильных телефонов	7%	12%	62%	19%
Мошенничества, совершенные с использованием сети Интернет	32%	46%	17%	5%

Анализ полученных данных показывает, что средства, используемые преступниками при совершении преступлений, зависят от возрастной категории потерпевших (табл. 8). В отношении пожилых лиц чаще совершаются мошенничества с использованием мобильного телефона. Преступления, связанные с использованием сети Интернет, относительно равномерно распределены по возрасту между молодыми людьми и лицами средних лет. Это во

[1] Джумазаде В.В. Криминологическая характеристика жертв преступлений // Вестник Калининградского юридического института МВД России. 2010. № 1. С. 54.

многом обусловлено способами совершения преступления. Так, преступления, связанные с ложным сообщением о родственнике в беде, чаще совершаются в отношении лиц пожилого возраста, а сеть Интернет при таком способе используется преступниками достаточно редко. Преступления, связанные с фиктивными покупками и продажами посредством сети Интернет, совершаются практически в отношении всех категорий граждан. При этом доля потерпевших по возрастам в общем массиве преступлений практически коррелирует с долей лиц, совершающих покупки посредством сети Интернет[1]. Данный показатель важен, так как именно мошенничества, связанные с фиктивными покупками и продажами в сети Интернет, в настоящее время составляют основную часть преступлений, совершенных с использованием ИТТ.

Таблица 8

Распределение по полу и возрасту покупателей в сети Интернет (в %)

Мужчины (средний возраст 46)		Предпочтения покупателей в сети Интернет	Женщины (средний возраст 54)	
Всего выявлено	Возраст		Всего выявлено	Возраст
9	18–24	Приобретение купонов и товаров для хобби	10	18–24
16	25–34	Приобретение товаров для детей и дома, одежды и обуви	18	25–34
10	35–44	Приобретение товаров в интернет-супермаркетах и магазинах электроники	13	35–44
8	45–54	Приобретение билетов на авиа- и железнодорожный транспорт, бронирование отелей	8	45–54
3	55–64	Приобретение товаров для дома и книг	5	55–64

[1] Рынок интернет-торговли в РФ: отчет Национального исследовательского университета «Высшая школа экономики». URL: https://dcenter.hse.ru/data

Анализ возрастных категорий потерпевших показывает, что при совершении мошенничеств, связанных с использованием средств сотовой связи, потерпевшими чаще оказываются женщины (52%) (табл. 8). Таким образом, можно сделать вывод, что мошенничества, совершенные с использованием ИТТ, связаны с особенностями личности потерпевшего, его виктимным поведением, обусловленным невнимательностью, эмоциональностью и впечатлительностью. Изучение личности потерпевшего позволяет планировать и принимать меры профилактики мошенничеств, совершенных с использованием ИТТ.

К числу основных элементов оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИТТ, относится личность преступника: пол, возраст, образование, наличие судимости. Изучение материалов уголовных дел показало, что лицами, совершающими мошенничества с использованием ИТТ, в основном являются мужчины (74%). Чаще всего преступления данной категории совершаются лицами в возрасте от 18 до 35 лет (69%). Высшее и неоконченное высшее образование имелось у 16% преступников; среднее и среднее специальное образование – 39%; неполное среднее – 37%.

Возраст, а также обусловленные этим адаптивные навыки позволяют лицам, совершающим мошенничества с использованием ИТТ, быстрее осваивать возможности сети Интернет и мобильных устройств для успешной реализации преступных планов.

Анализ материалов уголовных дел позволяет утверждать о существенных отличиях местонахождения преступников на момент совершения преступления в зависимости от его способа. Так, 74% преступников находились в местах лишения свободы при совершении мошенничеств по схеме «родственник в беде», при этом 92% преступников находились на свободе при совершении иных видов мошенничеств с использованием ИТТ.

Проведенное исследование показало, что около 62% мошенников ранее привлекались к уголовной ответственности либо имели судимость на момент совершения преступления. Этот факт должен учитываться оперативными сотрудниками ОВД при планировании и проведении ОРМ.

Изучение сведений о личности обвиняемых показало, что их образ жизни часто не предполагает длительное нахождение на одном месте, а переезд на новое место жительства или пребывания часто сопряжен с уничтожением доказательственной базы. Кроме того, важнейшее значение в раскрытии преступлений имеет факт совершения противоправных деяний мошенниками, находящимися в одном регионе, в отношении жителей иных регионов.

В связи с этим правоохранительные органы региона местонахождения преступников и осуществления ими преступной деятельности, как правило, получат информацию о преступной деятельности мошенников только от правоохранительных органов других субъектов, что свидетельствует о необходимости совершенствования межрегионального и межведомственного взаимодействия ОВД.

При совершении противоправных деяний преступники реализуют как корыстный умысел, так и цели, связанные с уничтожением следов преступления. При опросе оперативных сотрудников были названы следующие причины большого количества мошенничеств, совершенных с использованием ИТТ: виктимное поведение потерпевших (61%); доступность сети Интернет и средств связи для населения (49%); технические уязвимости систем, обеспечивающих безналичные денежные переводы (27%); возможность обеспечения анонимности в сети Интернет (37%), недостатки в деятельности ОВД по противодействию данным видам преступлений (респондентам предлагалось указать несколько вариантов ответов).

Особенности виртуальных следов

При совершении мошенничеств остается три вида следов преступления: материальные, идеальные, а также особые виртуальные следы. Особый интерес представляет анализ именно виртуальных следов.

Как показывает практика, такие следы будут распределены в зависимости от средства, с помощью которого совершено преступление (мобильное устройство, сеть Интернет): в компьютерной системе, мобильных устройствах, электронных носителях информации преступника и потерпевшего, компьютерных системах опера-

торов связи. В связи с этим при проведении ОРМ необходимо уделять особое внимание обнаружению таких средств. При этом важно учитывать возможность уничтожения виртуальных следов и их электронных носителей, что непосредственно влияет на необходимость максимально быстрого обнаружения следов и носителей, а также обусловливает потребность в получении информации из альтернативных источников[1].

При осуществлении преступником действий с использованием сети Интернет характерным является нахождение следов преступления в разных местах одновременно и на большом расстоянии друг от друга. Они могут быть оставлены не только на рабочем месте, но и в месте хранения или резервирования информации, на местах подготовки к совершению мошенничества с использованием ИТТ (например, там, где подбирались вероятные жертвы преступления, хранились электронные копии различных баз данных физических и юридических лиц, телефонов, сведений о клиентах больниц и т. д.), а также в месте использования информации. Данные обстоятельства становятся объективной причиной необходимости проверки всех предполагаемых источников виртуальных следов.

Таким образом, виртуальные следы образуются: а) в компьютерных системах операторов связи; б) в компьютерах, мобильных устройствах и электронных носителях информации, имеющихся у потерпевших и преступников, в том числе телефонах; в) на различных устройствах, обеспечивающих функционирование сети Интернет, а также компьютерных устройствах сторонних пользователей сети Интернет.

Виртуальные следы формируют массив оперативно значимых данных, необходимых сотрудникам оперативных подразделений ОВД для проведения ОРМ, направленных на предупреждение, выявление и раскрытие мошенничеств, совершенных с использованием ИТТ.

---

[1] Информацию о соединениях между абонентами и (или) абонентскими устройствами можно получить как непосредственно из мобильного устройства потерпевшего или преступника, так и посредством проведения ОРМ «снятие информации с технических каналов связи».

К числу данных, остающихся в компьютерных системах операторов связи, можно отнести следующие:

сведения о соединениях между абонентами и (или) абонентскими устройствами, включая информацию о типе, направлении, продолжительности соединения, базовой станции, посредством которой осуществлялось соединение, и ее азимут;

учетные данные пользователей, включающие в себя логин и пароль, MAC-адреса устройств, использовавшиеся для выхода в сеть Интернет, IP-адреса, выделенные для сеанса связи;

сведения об особенностях компьютерных устройств и их программного обеспечения (операционная система, компьютерные программы), использовавшихся преступниками и потерпевшими, в том числе информация о пакетах данных, которые были отправлены либо получены на адрес пользователя сети Интернет, о времени отправки и приема, размер, тип, IP-адрес получателя или отправителя пакетов данных и другая информация; в некоторых случаях возможно получение данных о конфигурации компьютера преступника[1].

К числу виртуальных следов, остающихся в компьютерах, мобильных устройствах и электронных носителях информации, имеющихся у потерпевших и преступников, в том числе в телефонах, можно отнести следующие:

технические характеристики компьютера и мобильного устройства: идентификационный номер сотового телефона (IMEI-номер), абонентский номер (SIM-карта), IP-адрес, MAC-адрес, операционная система, информация о контактах (абонентские номера, учетные данные, фотографии, используемые мессенджеры, информация о дате, времени и продолжительности соединения), информация о посещаемых ресурсах сети Интернет, фотографии и видеофайлы (как отправленные другими лицами, так и сделанные пользователем самостоятельно). При этом даже удаленную инфор-

[1] См.: Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. 2007. Т. 310. № 1. С. 213.

мацию с компьютера или мобильного устройства можно восстановить посредством аппаратно-программных комплексов и программных средств[1].

Информация об элементах оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИТТ, позволяет моделировать механизм совершения преступления, что дает возможность планировать тактику проведения ОРМ, направленных на раскрытие преступлений. Данное обстоятельство особенно важно на первоначальном этапе раскрытия преступления. Информациях об отдельных признаках поведения преступника, используемых средствах, а также личностных особенностях потерпевшего является ключевым источником для формирования модели преступления.

В связи с этим изучение сотрудниками оперативных подразделений ОВД элементов оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИТТ, является одним из важных компонентов обеспечения организации противодействия преступлениям данной категории.

[1] Программно-технические комплексы «UFED», Мобильный криминалист», программные средства R-Studio, PhotoRescue Pro, GetDataBack FAT, GetDataBack NTFS, EasyRecovery, Recuva и др.

2. Организационно-тактические особенности раскрытия мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий

2.1. Информационное обеспечение и документирование деятельности по раскрытию мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий

Раскрытие преступлений – это вид правоохранительной функции ОРД, направленный на обнаружение подготавливаемых, совершающихся или уже совершенных преступлений, обстоятельств, подлежащих доказыванию, установление лиц, участвующих в эти х преступлениях, изобличение виновных, а также на принятие мер оперативного пресечения и создание условий, обеспечивающих применение к виновным уголовного наказания или других предусмотренных законом мер.

Раскрытие мошенничеств, совершенных с использованием ИТТ, – это сложная деятельность ряда взаимодействующих субъектов, направленная на своевременное получение, фиксацию и применение оперативно значимой информации, в связи с чем особую роль играет эффективная организация такой деятельности.

Организация ОРД представляет собой систему организационных, правовых, материально-технических (экономических) мер, обеспечивающих, с учетом современного состояния и перспектив изменения оперативной обстановки, специализированное и комплексное использование сил, средств, методов и форм ОРД для успешного решения профессиональных задач по борьбе с преступностью во взаимодействии с другими службами и органами[1].

Организация ОРД включает мероприятия, направленные на создание кадровых, структурных, информационных, материально-технических предпосылок эффективной борьбы с преступностью.

[1] См.: Утевский А.Б. Организация и тактика оперативно-розыскной деятельности органов внутренних дел на транспорте и научно-практические меры повышения ее эффективности: автореф. дис. … д-ра юрид. наук. М., 1968. С. 22.

К числу наиболее значимых мероприятий при организации ОРД, на наш взгляд, относятся мероприятия, направленные на повышение эффективности информационного обеспечения (далее – ИО) ОРД по раскрытию мошенничеств, совершенных с использованием ИТТ.

Под информационным обеспечением деятельности оперативных подразделений ОВД по раскрытию преступлений понимается «совокупность концепций, методов и средств, а также созданная на их основе система выявления, систематизации, хранения и использования оперативно-розыскных и иных данных в целях решения задач, стоящих перед оперативным подразделением»[1].

Информационное обеспечение деятельности оперативных подразделений ОВД по раскрытию мошенничеств, совершенных с использованием ИТТ, соответственно, можно определить как совокупность концепций, методов и средств, а также созданную на их основе систему выявления, систематизации, хранения и использования оперативно-розыскных и иных данных в целях выявления, пресечения и раскрытия мошенничеств, совершенных с использованием ИТТ, а также выявления и пресечения лиц, их подготавливающих, совершающих или совершивших.

Прежде чем приступить к описанию процесса информационного обеспечения ОРД по раскрытию мошенничеств, совершенных с использованием ИТТ, следует раскрыть понятие информации, а также оперативно-розыскной информации и определить наиболее значимые специфические элементы характеристики документирования деятельности, а также элементы оперативно-розыскной информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИТТ.

В соответствии с Федеральным законом от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и защите информации» информация – это сведения (сообщения, данные) независимо от формы их представления[2].

---

[1] См.: Луговик В.Ф. Информационное обеспечение деятельности оперативных подразделений органов внутренних дел по раскрытию преступлений. Омск, 2005. С. 11.

[2] Собр. законодательства РФ. 2006. № 31 (ч. I). Ст. 3448.

Оперативно-розыскную информацию с учетом требований нормативных документов МВД России можно определить как представляющие оперативный интерес сведения, полученные в результате ОРМ, а также фактические данные, послужившие основанием для проведения ОРМ.

Содержание оперативно-розыскной информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИТТ, составляют:

1) информация об оперативной обстановке по данной линии в определенный период времени;

2) информация о совершенных и подготавливаемых преступлениях;

3) информация об особенностях совершения таких преступлений;

4) информация о лицах, участвующих в подготовке и совершении преступлений данной категории, а также совершавших их ранее;

5) информация о ранее проведенных и проводимых ОРМ;

6) информация, имеющая значение для планирования и проведения ОРМ;

7) информация, необходимая для оперативно-розыскного обеспечения предварительного расследования.

Оперативно-розыскная информация, представляющая интерес для раскрытия преступлений, совершенных с использованием ИТТ, содержится в следующих базах, учетах, структурированных и неструктурированных информационных массивах:

1. Централизованные оперативно-справочные, криминалистические и розыскные учеты. Ведение данных учетов осуществляется ГИАЦ МВД России, информационными центрами на региональном уровне в порядке, установленном Наставлением по ведению и использованию централизованных оперативно-справочных, криминалистических и розыскных учетов, формируемых на базе органов внутренних дел Российской Федерации (далее –

Наставление о ведении учетов)[1]. В данных учетах содержится информация о лицах, привлеченных к уголовной ответственности и разыскиваемых за совершение мошенничеств с использованием ИТТ, а также о лицах, уголовное преследование в отношении которых прекращено по различным основаниям. Кроме того, в данных учетах содержится информация об уголовных делах, возбужденных по фактам мошенничеств, совершенных с использованием ИТТ. Изучение и систематизация данной информации позволяет планировать и проводить ОРМ и следственные действия, направленные на раскрытие преступлений рассматриваемой категории, а также осуществлять межведомственное и межрегиональное взаимодействие. Формирование учетов осуществляется следователями, дознавателями, оперуполномоченными, а также иными сотрудниками ОВД и иных правоохранительных органов.

2. Экспертно-криминалистические учеты ОВД. Данные учеты содержат экспертно-криминалистическую информацию. Экспертно-криминалистическая информация представляет собой индивидуальную совокупность криминалистически значимых признаков объекта учета, выявляемых и фиксируемых с использованием специальных знаний, экспертно-криминалистических методов и средств. В контексте оперативно-розыскного противодействия мошенничествам, совершенным с использованием ИТТ, перечисленные учеты могут содержать информацию о следах преступлений, представляющую интерес для данной деятельности. Экспертно-криминалистическая информация – это индивидуальная совокупность криминалистически значимых признаков объекта учета, выявляемых и фиксируемых с использованием специальных знаний, экспертно-криминалистических методов и средств. Формирование и использование экспертно-криминалистических учетов осуществляется следователями, дознавателями,

[1] Об утверждении Наставления по ведению и использованию централизованных оперативно-справочных, криминалистических и розыскных учетов, формируемых на базе органов внутренних дел Российской Федерации: приказ МВД России, Минюста России, МЧС России, Минфина России, Министра обороны Российской Федерации, ФСБ России, ФСКН России, ФСО России, СВР России, ФТС России, ФМС России, ГФС России, Следственного комитета Российской Федерации и Генпрокуратуры России от 12 февр. 2014 г. № 9дсп/19дсп/73дсп/1адсп/113дсп/108дсп/75дсп/93дсп/19дсп/324дсп/133дсп/ 63дсп/14/95дсп.

сотрудниками оперативных подразделений ОВД, а также сотрудниками экспертно-криминалистических подразделений ОВД в пределах их компетенции. Экспертно-криминалистические учеты ОВД ведутся в федеральном государственном казенном учреждении «Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации», в экспертно-криминалистических центрах на межрегиональных и региональных уровнях, а также в линейных управлениях внутренних дел МВД России на транспорте.

3. Оперативные учеты ОВД. Данные учеты содержат оперативную информацию органов, осуществляющих ОРД, о лицах, причастных к совершению мошенничеств с использованием ИТТ, и совершенных ими преступлениях, о делах оперативного учета. Данные учеты ведутся на местном, региональном и федеральном уровнях. Формирование и использование оперативных учетов осуществляется сотрудниками оперативных подразделений ОВД в порядке, установленном федеральными законами от 7 февраля 2011 г. № 3-ФЗ «О полиции», от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», Наставлением о ведении учетов, Наставлением по формированию, ведению и использованию информационной системы оперативно-розыскной информации и Положением о порядке проведения оперативно-аналитических мероприятий[1].

4. Информационные массивы и базы данных кредитных организаций. В данных массивах и учетах содержится информация:

о лице или организации, на которую зарегистрированы счет или карта;

об абонентских номерах, привязанных к данной карте или счету;

об абонентских номерах, которые пополнялись с данной карты или счета;

о наличии дубликатов данной карты и об их количестве, а также о транзакциях, в том числе сведения об их месте и времени;

[1] Утверждены приказом МВД России от 10 июля 2013 г. № 037.

о договорах об оказании различных банковских услуг, в том числе сведения о дате и месте их заключения, сторонах, условиях и иных обстоятельствах договора.

Формирование и ведение баз данных и массивов осуществляются кредитными организациями в порядке, регламентированном Федеральным законом от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности», внутренними правилами кредитной организации, а также иными нормативными правовыми актами. Данная информация нередко имеет ключевое значение при документировании мошенничеств, совершенных с использованием ИТТ.

5. Информационные массивы и базы данных операторов связи. В данных массивах и базах содержится информация:

о регистрационных данных пользователей услуг связи (абонентов);

о соединениях между абонентами и (или) абонентскими устройствами, в том числе информация о типе, направлении, продолжительности соединения, базовой станции, посредством которой осуществлялось соединение, и ее азимут;

о логине и пароле, MAC-адресах устройств, использовавшихся для выхода в сеть Интернет, IP-адресах, выделенных для сеанса связи; об особенностях компьютерных устройств и их программного обеспечения (операционная система, компьютерные программы), использовавшихся преступниками и потерпевшими, в том числе информация о пакетах данных, которые были отправлены либо получены на адрес пользователя сети Интернет;

о времени отправки и приема пакетов данных, размере, типе, IP-адресе получателя или отправителя пакетов данных и др.

В некоторых случаях возможно получение данных о конфигурации компьютера преступника.

Формирование и ведение информационных массивов и баз данных осуществляется операторами связи в порядке, предусмотренном Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи», Правилами взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД, «Требованиями к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть 1. Общие требования»;

внутренними правилами оператора связи, а также иными нормативными правовыми актами. В связи с тем что преступниками при совершении мошенничеств с использованием ИТТ в 100% случаев используются ресурсы связи, информация, содержащаяся в информационных массивах и базах данных операторов связи, не только имеет большое значение при раскрытии таких преступлений, но и входит в предмет доказывания по уголовному делу. Этот факт предопределяет необходимость обращения к базам данных и информационным массивам при работе по раскрытию всех видов мошенничеств, совершенных с использованием ИТТ.

6. Информационные массивы и базы данных государственных органов. В этих массивах и базах данных собирается и обрабатывается большой объем сведений о лицах, постоянно или временно проживающих на территории Российской Федерации, и оказанных им государственных услугах. Сведения включают в себя паспортные данные, информацию о месте регистрации, наличии автомобиля, штрафах и налогах, очередях в больницы и детские сады и др. Так, портал государственных услуг (https://www.gosuslugi.ru) объединяет информацию об услугах и проведенных операциях значительного количества государственных органов, а также регистрационные и многие другие данные (например, о фактически используемых банковских картах и абонентских номерах мобильной связи) десятков миллионов граждан. В связи с тем, что эта информация достаточно быстро обновляется, ее ценность для организации противодействия мошенничествам, совершаемым с использованием ИТТ, особенно высока. Мошенники, часто меняющие средства связи и банковские карты, тем не менее, как правило, остаются в сфере государственного управления и используют услуги, предоставляемые государственными органами. Формирование и ведение информационных массивов и баз данных осуществляются операторами связи в порядке, установленном Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также рядом иных нормативных правовых актов в зависимости от органа учета.

Информационные массивы и базы данных транспортных компаний и логистических организаций. В данных массивах и ба-

зах содержится информация об отправителе и получателе почтового отправления; о виде и типе отправления; дате и месте отправления и получения, включая адрес доставки и получения либо адрес местонахождения почтового отделения или филиала логистической организации; о наличии претензий по фактам нарушений в процессе доставки почтового отправления, в том числе о несвоевременности доставки или фактах недоставления отправления. При этом время отправки и доставления почтового отправления фиксируется по московскому времени, что необходимо учитывать при анализе информации, полученной в почтовых организациях. Формирование и ведение информационных массивов и баз данных осуществляются операторами почтовой связи и логистическими организациями, как правило, по месту расположения оператора почтовой связи или логистической организации в порядке, установленном федеральными законами от 17 июля 1999 г. № 176-ФЗ «О почтовой связи», от 28 декабря 2009 г. № 381-ФЗ «Об основах государственного регулирования торговой деятельности в Российской Федерации», а также иными нормативными правовыми актами.

Обращение к информационным массивам и базам данных актуально при работе по раскрытию мошенничеств с использованием ИТТ, при совершении которых потерпевшему посредством логистических организаций либо транспортных компаний направляются муляж товара, равный по весу приобретаемому товару, либо какие-либо предметы, не имеющие стоимости. Это осуществляется для того, чтобы получить в данной компании трек-код, предъявляемый потерпевшему в подтверждение легенды, а также чтобы потерпевший убедился в ее действительности и направил преступнику денежные средства.

7. Информационные массивы, базы данных и каналы связи Интерпола. Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола[1] предусмотрен ряд направлений информационного обеспечения борьбы

[1] Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России № 786, Минюста России № 310, ФСБ России 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 окт. 2006. Доступ из справ. правовой системы «Гарант».

с преступностью. К числу наиболее значимых в контексте раскрытия мошенничеств, совершенных с использованием ИТТ, относится информационное обеспечение борьбы с преступлениями в области высоких технологий (раздел 9 Инструкции).

При работе по раскрытию мошенничеств, совершенных с использованием ИТТ, по которым достоверно установлен их международный характер, взаимодействующие органы в процессе расследования преступлений по каналам Интерпола направляют запросы в правоохранительные органы иностранных государств – членов Интерпола о преступлениях, связанных:

с неправомерным доступом к компьютерной информации;

с созданием, использованием и распространением вредоносных программ для ЭВМ;

с сетевыми адресами, именами доменов и серверов организаций и пользователей;

с содержанием протоколов, трейсингов, логических файлов;

с электронной информацией, заблокированной в порядке оперативного взаимодействия правоохранительных органов при пресечении трансграничных правонарушений;

с провайдерами и дистрибьюторами сетевых и телекоммуникационных услуг;

с физическими и юридическими лицами, имеющими отношение к преступлениям в сфере высоких технологий;

со специализированным программным обеспечением, с методиками и тактикой борьбы с компьютерными и телекоммуникационными преступлениями, с периодическими и специальными изданиями, обзорами статистики, материалами о деятельности специализированных служб различных государств в данной области.

Указанные базы данных формируют систему информационного обеспечения деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ.

Организацию деятельности оперативных подразделений по получению оперативно-розыскной информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИТТ, структурно можно разделить на две части:

1) обеспечение полноты получаемой информации, а также сокращение сроков ее получения;

2) документирование (фиксация) полученной информации и передача ее следственным подразделениям.

Обеспечение полноты получаемой информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИТТ, а также сокращение сроков ее получения.

Для противодействия преступлениям в сфере ИТТ и компьютерных технологий правоохранительные органы должны обладать знанием способов совершения таких преступлений, тактики и методики выявления, раскрытия расследования преступлений данной категории; стремиться к превосходству над злоумышленниками в уровне технической оснащенности и скорости получения информации. В то же время сотрудники ОВД, осуществляющие противодействие преступлениям, совершенным с использованием ИТТ, сталкиваются с рядом существенных трудностей при получении необходимой информации, что негативно сказывается на итогах оперативно-служебной деятельности.

Анализ практической деятельности показывает, что основными проблемами организации информационного обеспечения в борьбе с преступлениями, совершенными с использованием ИТТ, являются следующие:

длительность получения справок по счетам и вкладам физических лиц из кредитных организаций;

длительность получения информации о соединениях между абонентами и (или) абонентскими устройствами, особенно в случаях, когда информация необходима от оператора связи, не имеющего представительств в регионе местонахождения инициатора запроса;

длительность получения информации от интернет-провайдеров, а также от владельцев и администраторов различных интернет-ресурсов;

сложности идентификации и обнаружения фактических собственников некоторых интернет-ресурсов, а также отдельных пользователей сети Интернет.

В ходе изучения информации о мошенничествах, совершенных с использованием ИТТ, было установлено, что в 98% случаев потерпевшие самостоятельно переводили денежные средства преступникам либо оказывали им содействие при хищении денежных

средств. При переводе использовались ресурсы ПАО Сбербанк России – в 68,9% случаев, ПАО ВТБ – в 5,1% случаев, АО Альфа-банк – в 3,2% случаев, иные кредитные организации – 9,4%. В остальных случаях использовались различные виды электронных кошельков[1].

Мошенничества с использованием ИТТ объединяет то, что все они совершены дистанционно, т. е. личный физический контакт между потерпевшим и преступником отсутствует. В связи с этим, вне зависимости от легенды мошенничества, местонахождения преступника или потерпевшего, других факторов, для реализации преступного умысла мошенникам необходимо решить два основных вопроса: организация какого-либо способа связи с потерпевшим (телефонная связь, сеть Интернет, мессенджеры и т. д.), а также способа перевода денежных средств. На основании изложенного получение информации в кредитных организациях и у операторов связи имеет ключевое значение для установления виновных лиц, получения доказательств их преступной деятельности, а также для обнаружения и изъятия похищенных денежных средств. При этом немаловажным является фактор времени, в течение которого осуществляется получение информации, так как лица, специализирующиеся на совершении мошенничеств с использованием ИТТ, как правило, очень часто меняют средства связи, банковские карты, счета и электронные кошельки. По результатам опроса оперуполномоченных и следователей, специализирующихся на раскрытии и расследовании преступлений данной категории[2], было установлено, что SIM-карта и электронный кошелек используются мошенниками в среднем около 3 суток, мобильный телефон – от 7 до 14 суток, банковские карты – до 30 суток.

Совершению мошенничеств с использованием ИТТ, как правило, предшествуют тщательные подготовительные мероприятия со стороны причастных к ним лиц, а именно:

---

[1] Под электронным кошельком (от англ. e-Purse или e-Wallet) понимается программное обеспечение, позволяющее производить операции пополнения, хранения и перечисления электронных денег.

[2] Были опрошены 46 оперуполномоченных и следователей ГУ МВД России по Иркутской области, Красноярскому краю, МВД по Республике Бурятия.

выбор финансовых инструментов и средств связи, исключающих идентификацию доступными официальными способами;

частая смена места жительства;

ограничение или исключение внешних контактов (контактов вне преступной группы или членов семьи).

К числу наиболее распространенных средств по обеспечению анонимности в сети Интернет и сетях связи при совершении мошенничеств с использованием ИТТ относятся:

приобретение SIM-карт, не имеющих регистрационных данных или зарегистрированных на вымышленных или третьих лиц; приобретение мобильных телефонов с измененным программным обеспечением, не позволяющим установить по детализации соединений предыдущие номера IMEI, или с «чистой» историей;

приобретение различными способами банковских карт у лиц, не имеющих прямой связи с преступниками, в том числе с помощью посредников или сети Интернет;

регистрация счетов в электронных платежных системах анонимным способом, без привязки к официально зарегистрированным абонентским номерам мобильной связи или адресам электронной почты.

Такие меры предосторожности требуют выработки особых алгоритмов действий, отличных от алгоритмов, применяемых для раскрытия других видов преступлений. При этом важно минимизировать время, затрачиваемое на получение доказательственной базы, в силу возможности ее уничтожения. При выработке алгоритмов следует учитывать одну из основных отличительных особенностей деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ, – получение и процессуальное закрепление следов преступления, оставленных в информационной среде. В отдельных случаях для этого гласно и негласно задействуются десятки гражданских организаций и учреждений, а также подразделений и ведомств правоохранительных органов. В таких условиях особое значение приобретают выбор механизма реализации конкретного мероприятия, способ получения информации, имеющей значение для дела.

Выбор метода должен соответствовать действующему законодательству, при этом отвечать решению задач ОРД, а также

обеспечивать реализацию общих принципов уголовного законодательства, в частности неотвратимости наказания.

Изложенное объективно свидетельствует о том, что для повышения эффективности противодействия мошенничествам, совершаемым с использованием ИТТ, необходимо совершенствование процедуры получения информации в кредитных организациях и у операторов связи, в том числе в экстренных и неотложных случаях.

Традиционная форма взаимодействия в виде запросов, направляемых почтой, имеет очевидный недостаток, связанный с потерей времени на обработку, сортировку, физическое перемещение корреспонденции, ее последующую обработку организацией-адресатом, подготовку и направление ответа инициатору запроса с последующей потерей времени на аналогичные процедуры. Такая форма взаимодействия представляется малоэффективной, в связи с тем что преступники могут избавиться от средств связи и иных орудий преступления до того, как правоохранительные органы получат информацию, которая может позволить пресечь преступные действия и задержать виновных лиц.

Развитие ИТТ в настоящее время позволяет организовать иную форму взаимодействия посредством закрытых каналов связи, препятствующих утечке информации, при этом потери времени на физическое перемещение запросов отсутствуют. Такая форма взаимодействия реализуется при получении информации из баз данных операторов связи посредством систем технических средств для обеспечения функций оперативно-розыскных мероприятий (далее – СОРМ). Порядок получения информации органами, осуществляющими ОРД, у операторов связи посредством СОРМ регламентированы Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи», правилами взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД, утвержденными постановлением Правительства РФ от 27 августа 2005 г. № 538 (далее – Правила), а также ведомственными нормативными правовыми актами МВД России.

В соответствии с Правилами получение информации от операторов связи посредством закрытых каналов связи организовано

путем предоставления государственным органам, осуществляющим ОРД, круглосуточного удаленного доступа к базам данных операторов связи. Несмотря на то что в Правилах отсутствуют причины выбора такого способа взаимодействия, очевидно, что к числу основных из них относится необходимость оперативного получения информации, содержащейся в базах данных операторов связи, в целях выявления, пресечения и раскрытия преступлений.

Технический аспект организации удаленного доступа к базам данных операторов связи регламентирован «Требованиями к сетям электросвязи для проведения оперативно-розыскных мероприятий. Часть 1. Общие требования», утвержденными приказом Министерства информационных технологий связи РФ от 16 января 2008 г. № 6 (далее – Требования)[1]. В соответствии с Требованиями базы данных об абонентах оператора связи и базы данных об оказанных оператором связи услугах, а также оборудование средств связи, в том числе программное обеспечение, обеспечивающее выполнение действий при проведении ОРМ, подключаются оператором связи к пункту управления ОРМ через точку (точки) подключения в соответствии с техническими условиями, устанавливаемыми уполномоченным органом. На пункт управления ОРМ информация от операторов связи передается посредством сетей электросвязи, которые обеспечивают возможность:

а) передачи на пункт управления ОРМ информации об абонентских номерах и (или) кодах идентификации, которые были использованы для установления контролируемого соединения и (или) передачи сообщений электросвязи;

б) передачи на пункт управления ОРМ информации, передаваемой в контролируемом соединении и (или) сообщении электросвязи, в том виде, в котором эта информация передается в сеть связи оператора связи с пользовательского (оконечного) оборудования или из присоединенной сети связи.

[1] Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Ч. I: Общие требования: приказ Министерства информационных технологий связи РФ от 16 янв. 2008 г. № 6. Доступ из справ. правовой системы «Гарант».

Сети связи обеспечивают возможность определения местонахождения пользовательского (оконечного) оборудования абонента (пользователя услуг связи) и передачи на пункт управления ОРМ такой информации.

Таким образом, сотрудники оперативных подразделений органов, осуществляющих ОРД, имеют возможность получения информации в установленном законом порядке от операторов связи в круглосуточном режиме, при этом использование закрытых каналов связи обеспечивает оперативность получения информации и предотвращает доступ к ней третьих лиц.

Анализ действующего законодательства показал, что в Российской Федерации не реализуется процедура получения информации от кредитных организаций, аналогичная процедуре получения информации от операторов связи. Так, Федеральным законом от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» установлена лишь обязанность кредитных организаций выдавать справки по операциям и счетам по запросам органов, осуществляющих ОРД, а также органов предварительного следствия. Данным нормативным правовым актом не предусмотрено отсылочных норм, устанавливающих обязанность кредитных организаций предоставлять круглосуточный удаленный доступ к своим базам данных.

На наш взгляд, факторов, объективно препятствующих предоставлению удаленного доступа правоохранительным органам к базам данных кредитных организаций, нет. Такой доступ может позволить повысить эффективность работы не только по противодействию преступлениям, совершенным с помощью ИТТ, но и широкому спектру других преступлений, в том числе экономических и налоговых, а также способствовать реализации законодательства, регламентирующего противодействие коррупции. Кроме того, оперативный доступ к такой информации может способствовать розыску скрывшихся преступников и установлению местонахождения лиц, пропавших без вести.

В современных условиях именно скорость и полнота получаемой информации – ключ к решению множества важных задач, в том числе по обеспечению защиты прав и законных интересов

граждан, защиты общества и государства от преступных посягательств.

В целях защиты прав и законных интересов граждан и организаций, обеспечения безопасности общества и государства от преступных посягательств необходимо внесение изменений в Федеральный закон от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности», предусматривающих обязанность предоставления кредитными организациями сведений, содержащихся в их базах данных, органам, осуществляющим ОРД, посредством закрытых каналов связи.

До тех пор пока предлагаемые изменения не внесены, целесообразно обеспечить решение вопроса о своевременном получении информации, составляющей банковскую тайну, посредством заключения соглашений о предоставлении информации между уполномоченными подразделениями кредитных организаций и ОВД на региональном уровне.

В качестве примера успешно реализованного ранее подобного соглашения можно привести соглашение «Об электронном обмене документами и информацией для выполнения правоохранительным органом возложенных на него функций» № 31/1/1/75 – 2016, заключенное между ГУ МВД России по Иркутской области и Байкальским банком ПАО Сбербанк России.

Данным соглашением были утверждены:

1. Порядок обмена электронными документами по СПОД «Текос-КБ» (система передачи и обработки данных) – корпоративной системе ПАО Сбербанк России, включающей совокупность программных и/или программно-аппаратных средств, устанавливаемых у ОВД на региональном уровне с целью обеспечения защиты отправки, приема и обработки документов в электронном виде. В систему «Текос-КБ» для обеспечения конфиденциальности информации при передаче по сетям связи встроено сертифицированное программное обеспечение, реализующее криптографические алгоритмы в соответствии с ГОСТ 28147-89.

2. Процедура проведения технической экспертизы при возникновении разногласий и спорных ситуаций, связанных с принятием или непринятием и/или исполнением или неисполнением электронного документа.

3. Перечень документации по обеспечению безопасности.

4. Спецификация средств обеспечения электронного документооборота между клиентом и банком.

5. Требования по обеспечению безопасности в процессе эксплуатации части системы электронного документооборота, установленной в ОВД на региональном уровне.

6. Соглашение об использовании публичных цифровых систем связи для обмена документами в электронном виде.

7. Требования по подключению клиентской части системы ЭДО (программное обеспечение – средство формирования транспортных пакетов, а также квитанций, содержащих сообщения о доставке файлов электронных документов с результатами проверки электронной подписи к сети Интернет).

Помимо этого, данным соглашением был утвержден ряд актов, устанавливающих порядок ввода в эксплуатацию оборудования для обмена информацией, технические требования и др.

Полагаем, что принятие на региональном уровне таких соглашений позволит повысить эффективность деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ.

Реализация данного предложения на практике, безусловно, связана с решением ряда организационных вопросов. В соответствии с информацией Центрального банка России в настоящее время действует 841 кредитная организация[1]. Обеспечение каналов связи, исключающих получение третьими лицами информации, составляющей банковскую тайну, в условиях многосубъектности кредитной деятельности – одна из главных задач в случае реализации предложений. С учетом того, что в настоящее время вопрос организации связи решен в отношении 31 946 действующих операторов связи[2], полагаем, что организация связи со значительно меньшим числом кредитных организаций – вполне решаемая задача.

При получении информации, составляющей банковскую тайну, существует риск ее использования сотрудниками оператив-

[1] По состоянию на 15.11.2019.

[2] По состоянию на 17.11.2019.

ных подразделений в неслужебных целях, однако такая возможность имеется и в случае получения любой другой информации. Полагаем, что риск незаконного использования служебной информации обусловлен не способом ее получения, а рядом иных факторов: характером информации, личностными особенностями получившего ее сотрудника, мерами безопасности, предпринимаемыми в конкретном подразделении, и т. д. Кроме того, за неправомерные действия, связанные с использованием и распространением подобных сведений, предусмотрены различные виды ответственности, а порядок доступа к такой информации и ее использования регламентирован рядом федеральных законов и ведомственных нормативных правовых актов. Таким образом, определяющее значение имеет решение технического аспекта получения данной информации. Полагаем, что выделенные каналы связи в сочетании с криптографическими средствами шифрования и персонализацией доступа, наряду с иными предпринимаемыми в настоящее время мерами, могут обеспечить конфиденциальность передаваемой информации.

Анализ организации информационного обеспечения по борьбе с мошенничествами, совершенными с использованием ИТТ, показывает, что, наряду с перечисленными, проблемой также являются особенности формирования ведомственной статистической отчетности, не предусматривающей систематизацию оперативно значимых сведений, необходимых для организации раскрытия преступлений данной категории, перечисленных в главе 1 пособия.

Так, в статистической карточке формы № 1 на выявленное преступление[1] реквизитом № 28 (преступление совершено с использованием) предусмотрены коды: 007 (компьютерной тех-

[1] О едином учете преступлений: приказ Генеральной прокуратуры Российской Федерации, Министерства внутренних дел Российской Федерации, Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерства юстиции Российской Федерации, Федеральной службы безопасности Российской Федерации, Министерства экономического развития и торговли Российской Федерации, Федеральной службы Российской Федерации по контролю за оборотом наркотиков от 29 дек. 2005 г. № 39/1070/1021/253/780/353/399. Доступ из справ. правовой системы «Гарант».

ники), 021 (поддельных кредитных (пластиковых) карт), 020 (расчетных (пластиковых) карт), 008 (программных средств), 023 (фиктивных электронных платежей), 137 и 237 (с использованием сети Интернет), а реквизитом 26 (способ совершения преступления) предусмотрены коды: 48 (с использованием сети Интернет), 49 (с использованием мобильной связи). При этом в статистические карточки не вносятся (и не учитываются) такие важные особенности совершения мошенничеств с использованием ИТТ, как:

абонентские номера, IMEI-номера IP-адреса, MAC-адреса, использованные преступниками для связи с потерпевшим, абонентские номера потерпевших;

информация о дате, времени и продолжительности соединения между абонентскими номерами преступников и потерпевших;

информация об операционной системе устройств, использованных преступниками для совершения данного вида мошенничеств;

учетные данные аккаунтов на интернет-сайтах, использованных преступниками для совершения преступлений;

информация о фотографиях, переданных преступниками потерпевшим для обеспечения легенды мошенничества;

информация о номерах банковских карт и счетов, используемых преступниками для совершения преступлений;

информация о доменных именах сайтов, на которых преступники размещали объявления о фиктивной покупке или продаже товаров или услуг либо потерпевшие размещали объявления о продаже товаров или оказании услуг;

информация о легенде мошенничества, позволяющая систематизировать различные преступления с целью выявления признаков серийности.

Анализ практики показывает, что отдельными ОВД на региональном уровне предпринимаются меры по формированию статистической отчетности в пределах имеющихся полномочий и возможностей. Так, ГУ внутренних дел МВД России по Иркутской области, а также рядом иных ОВД на региональном уровне на основе имеющихся реквизитов и кодировок сотрудниками информационных центров осуществляется систематизация статистической информации в виде статистических отчетов. Изучение статистики

об уголовных делах в сфере ИТТ, возбужденных на территории Иркутской области, позволило установить, что удельный вес мошенничеств, совершенных с использованием сети Интернет, а также мобильной связи, в общей структуре мошенничеств составил 37,8%. Значительное количество преступлений данной категории, а также объективные сложности в их выявлении, раскрытии и расследовании послужили причиной создания в структуре ГУ МВД России по Иркутской области специализированного подразделения по раскрытию хищений денежных средств, совершенных с использованием сети Интернет, мобильных телефонов и банковских карт.

Таким образом, изменения в уголовной статистике стали одной из причин для организационно-штатных изменений в структуре ОВД.

ОВД должны формироваться региональные учеты с описанием и систематизацией перечисленных сведений в целях совершенствования информационного обеспечения деятельности по противодействию мошенничествам, совершенным с использованием ИТТ, а в их отсутствие – на территориальном.

Описанные особенности совершения мошенничеств с использованием ИТТ позволяют систематизировать и анализировать полученную информацию и планировать ОРМ и следственные действия.

При отсутствии на федеральном уровне систематизации сведений о преступлениях, совершенных в сфере ИТТ, а также о результатах работы по их раскрытию и расследованию невозможно организовать эффективное использование имеющихся ресурсов. Доступ к такой информации необходим для каждого подразделения ОВД, осуществляющего противодействие преступлениям, совершаемым с использованием современных ИТТ.

Документирование полученной информации и ее передача следственным подразделениям

Под документированием преступных действий понимается выявление оперативно-розыскным путем фактических данных, свидетельствующих о причастности их к приготовлению или со-

вершению преступления, и обеспечение возможности использования этих данных для предотвращения или раскрытия преступлений и принятия к виновным мер, предусмотренных законом.

Документирование мошенничеств, совершенных с использованием ИТТ, состоит из двух элементов:

выявление фактических данных;

обеспечение возможности использования их при расследовании.

Первый элемент – выявление фактических данных – означает получение первичных сведений и их проверку. Для получения фактических данных, имеющих значение для раскрытия мошенничеств с использованием ИТТ, следует использовать все находящиеся в распоряжении ОВД силы, средства, методы, а также помощь отдельных граждан. В то же время в результате применения этих средств и методов часто получают сведения, которые требуют тщательной проверки (в связи с необходимостью убедиться в том, что данные будут способствовать установлению истины).

Проверка должна дать ответ на вопросы:

соответствуют ли эти данные действительности, т. е. их достоверность;

каково значение этих данных для последующего доказывания, т. е. их относимость к будущему предмету доказывания;

какова возможность использования установленных фактических данных в целях получения судебных доказательств при расследовании уголовного дела.

ОРМ осуществляются в целях обнаружения только таких фактических данных, которые в результате производства соответствующих следственных действий могут быть использованы для документирования преступных действий лиц, совершающих мошенничества с использованием ИТТ.

В ходе документирования фиксируются фактические данные об обстоятельствах, которые будут составлять предмет доказывания при расследовании. В связи с этим в процессе документирования устанавливаются и закрепляются следующие фактические данные, что обусловлено требованиями уголовно-процессуального законодательства (ст. 73 УПК РФ):

событие преступления (время, место, способ и другие обстоятельства совершения преступления);

виновность лица в совершении преступления, форма его вины и мотивы;

обстоятельства, характеризующие личность обвиняемого;

характер и размер вреда, причиненного преступлением;

обстоятельства, исключающие преступность и наказуемость деяния;

обстоятельства, смягчающие и отягчающие наказание;

обстоятельства, которые могут повлечь за собой освобождение от уголовной ответственности и наказания.

Зная предмет доказывания по отдельным видам мошенничеств, совершенных с использованием ИТТ, выясняя обстоятельства, при которых готовилось или совершено преступление, устанавливая способ совершения преступления и каналы сбыта похищенного, оперативный работник определяет, какие фактические данные необходимо выявить по конкретному преступлению, чтобы успешно разоблачить преступников.

Проверка достоверности полученных данных, имеющих значение для расследования, необходима, потому что установленные первоначальные сведения могут быть противоречивы или недостоверны в силу различных обстоятельств. Это заставляет оперативного работника тщательно проверять полученную информацию.

Таким образом, проверка достоверности полученных сведений в данном случае позволяет собрать не вызывающие сомнения данные и объективно провести проверку информации. Это позволит при использовании полученных данных, с одной стороны, избежать необоснованного возбуждения уголовного дела в отношении честных граждан, а с другой – не дать действительному преступнику уйти от ответственности.

Важное значение при проверке имеет также определение возможности использования полученных негласным путем фактических данных для формирования судебных доказательств. Практика показывает, что не всегда имеется возможность использовать полученные негласным путем фактические данные при расследовании для формирования судебных доказательств.

Сведениями, получаемыми из оперативно-розыскных источников, как правило, нельзя оперировать при расследовании, их нельзя разглашать.

В то же время для успешного расследования необходимы такие сведения, которые можно предать гласности. В связи с этим при документировании нужно стараться получить сведения, которые можно проверить проведением следственных действий. Следовательно, преступные действия можно считать задокументированными, только если полученная информация содержит данные, которые поддаются проверке путем проведения следственных действий. С учетом того, что при работе по раскрытию мошенничеств с использованием ИТТ основную часть доказательств формируют сведения кредитных организаций и операторов связи, в некоторых случаях целесообразно получение данной информации как оперативно-розыскным (в ходе документирования преступной деятельности), так и следственным (в процесс формирования массива сведений, образующих предмет доказывания) путем.

Таким образом, получив сведения о наличии фактических данных, представляющих интерес для раскрытия мошенничества с использованием ИТТ, тщательно проверив их и убедившись в том, что они имеют значение для будущего доказывания и нет никаких препятствий для их использования, можно считать, что решена первая задача документирования преступных действий – выявление фактических данных, которые позволяют принять меры, предусмотренные законом.

Вторым элементом документирования преступных действий мошенников является обеспечение возможности использования выявленных фактических данных при расследовании преступления. Сюда должны включаться все меры, которые принимает оперативный работник с целью обеспечения возможности использования негласно полученных данных. Эти меры могут быть различными в зависимости от того, каков характер фактических данных, главным образом каков источник их получения.

Если возможные будущие доказательства, предметы или документы выявлены негласным путем и они могут быть уничтожены, то их необходимо сохранить (зафиксировать) до момента

предоставления их следователю, тем самым обеспечить возможность их использования.

При документировании преступных действий лиц, совершающих мошенничества с использованием ИТТ, следует учитывать, что документирование по отношению к доказыванию играет хотя и вспомогательную, но очень важную роль.

Для того чтобы документирование было наиболее эффективным, необходимо руководствоваться следующими требованиями:

законность;

объективность;

своевременность;

полнота документирования.

Соблюдение законности при документировании мошенничеств, совершенных с использованием ИТТ, состоит в следующем. В результате документирования выявляются не только конкретные противоправные действия разрабатываемых, но и фактические данные, свидетельствующие о причастности их к преступлению. Для установления объективной истины по уголовному делу при его расследовании необходимо, чтобы в целях обеспечения законности документирование проводилось объективно.

Объективность означает выявление как уличающих обвиняемого или отягчающих его вину обстоятельств, так и обстоятельств, оправдывающих его или смягчающих его вину. Объективность при документировании заключается в том, что все данные о причастности мошенника к приготовлению или совершению преступления должны быть достоверны, соответствовать действительности. Добиться этого можно лишь в том случае, если принимаются все меры для тщательной проверки всех сведений о преступных действиях разрабатываемых, поступающие к оперативному работнику.

Соблюдение законности состоит также и в том, чтобы не допускать:

фальсификации полученных данных;

провокации на совершение противоправных действий;

ущемления охраняемых прав и законных интересов участвующих лиц;

проведения вместо ОРМ следственных действий до возбуждения уголовного дела.

Своевременность документирования преступных действий мошенников заключается в том, что действия оперативного работника в выявлении и сохранении данных, имеющих значение для расследования, опережают действия преступников, направленные на сокрытие или уничтожение этих данных. В связи с этим оперативный работник должен стремиться как можно быстрее выявить намерения и преступные действия разрабатываемых и принять меры к сохранению данных, свидетельствующих о преступных действиях разрабатываемых лиц, обеспечить возможность их использования при расследовании. Оперативный работник должен закончить оперативную разработку в короткий срок, чтобы своевременно предотвратить подготавливаемое или быстро раскрыть совершенное преступление. Промедление в этом случае ведет к утрате возможности получить ценные для расследования фактические данные, а также к совершению разрабатываемым новых преступлений.

Полнота документирования состоит в фиксации преступных действий каждого из преступников в полном объеме. В то же время не следует ставить перед собой задачу задокументировать все преступные действия всех участников преступных групп мошенников, так как это потребует большого количества времени и может привести к увеличению времени документирования. Это часто ведет к тому, что мошенники в процессе документирования совершают ряд новых преступлений.

Определяя пределы документирования, необходимо установить такие его границы, которые бы:

конкретизировали каждое из обстоятельств, подлежащих выявлению в ходе документирования;

обеспечивали правильность выдвинутых версий и обоснованность выводов, вытекающих из них;

определяли совокупность данных и их источников, достаточную для признания выясненными обстоятельств, составляющих предмет документирования, которые будет трудно или невозможно установить следственным путем.

После выявления лиц, способных быть свидетелями, необходимо осуществлять мероприятия по проверке их с целью установления, что конкретно им известно о преступных действиях мошенников, в каких взаимоотношениях они находятся и насколько объективны будут их показания; в состоянии ли они правильно воспроизвести все, что им известно (не страдают ли психическими или иными заболеваниями, снижающими их ценность как будущих свидетелей).

Предварительное решение этих вопросов во многом облегчает впоследствии задачу проведения быстрого, всестороннего и объективного расследования.

Предметы и документы, выявленные в процессе документирования, играют очень важную роль при раскрытии преступления и определении степени виновности каждого из выявленных лиц, совершающих мошенничества с использованием ИТТ. Чаще всего при возбуждении уголовного дела они являются вещественными доказательствами. Поскольку вещественные доказательства и доказательства-документы играют важную роль в расследовании преступлений, необходимо принимать меры к их выявлению и обеспечивать возможность их использования при раскрытии мошенничеств, совершенных с использованием ИТТ.

К предметам и документам, которые необходимо выявить в ходе документирования, относятся:

предметы и документы, фиксирующие переговоры преступников с потерпевшим и между собой (детализации соединений между абонентами и (или) абонентскими устройствами);

предметы и документы, фиксирующие место и время перевода денежных средств от потерпевшего преступнику или его соучастнику;

предметы и документы, фиксирующие место и время перевода денежных средств от соучастника преступнику;

предметы и документы, фиксирующие место и время перевода денежных средств от соучастника преступнику;

документы, косвенно подтверждающие те или иные доказательственные факты (информация о приобретенных авиа- или ж/д билетах, взятых в аренду автомобилях и т. д.).

После того как такие предметы и документы выявлены, необходимо убедиться в их относимости к предмету доказывания и в их доказательственном значении.

После того как предметы и документы, которые могут быть доказательствами, выявлены, часто возникает необходимость принять меры к их сохранности, чтобы иметь возможность использовать при расследовании.

Для этого необходимо:

знать, где именно находятся предметы и документы, чтобы изъять их при обыске или выемке;

не допустить уничтожения предметов или средств совершения преступления или их сбыта через неизвестные каналы или неизвестным лицам;

создать условия для приобщения к уголовному делу предметов и документов в качестве вещественных доказательств.

Полученные в результате ОРД предметы и документы должны быть предоставлены следователю в порядке, установленном Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд (далее – Инструкция)[1].

Результаты ОРД – фактические данные, информация и сведения, полученные при проведении ОРМ, предусмотренные ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» и устанавливающие обстоятельства, связанные с подготавливаемым или совершенным преступлением, розыском лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших.

Они могут содержаться в оперативно-служебных документах, фиксирующих ход ОРМ и составляемых в соответствии с ведомственными нормативными актами; в материалах фото-, кино-

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утв. приказом МВД России, Минобороны России, ФСБ России, ФСО России, ФТС, Службы внешней разведки РФ, ФСИН, ФСКН России, Следственного комитета РФ от 27 сент. 2013 г. № 776/703/509/507/1820/42/535/398/68. Доступ из справ. прав. системы «Гарант».

съемки, в звуко-, видеозаписях, произведенных в процессе оперативных мероприятий; в объяснениях лиц, участвовавших в их проведении; в предметах, материалах и сообщениях, изъятых при осуществлении ОРМ; в сообщениях конфиденциальных источников.

Показания допрошенных в качестве свидетелей лиц, проводивших ОРМ или принимавших в них участие, надлежит считать уголовно-процессуальными доказательствами (при условии их отношения к делу).

Результаты ОРД могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения ОРМ по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц и иных целей.

Результаты ОРД могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находятся уголовное дело или материалы проверки сообщения о преступлении, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства Российской Федерации, регламентирующими собирание, проверку и оценку доказательств, а также в иных случаях, установленных Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» при соблюдении требований ст. 89 УПК РФ.

Применительно к следственным и судебным действиям наличие возможности и пределы использования результатов ОРД определяются уголовно-процессуальным законом, поскольку именно в нем регламентированы основания производства соответствующих следственных, судебных действий.

Использование результатов ОРД при подготовке к проведению следственных действий ничем, кроме необходимости обеспечить соблюдение правил конспирации, не ограничено. На этапе подготовки к проведению следственных действий оперативно-розыскная информация имеет важное значение преимущественно в организационно-тактическом аспекте: с ее помощью орган дознания, следователь могут наиболее оптимально определить время, место, участников производства следственного действия, привлечь необходимые научно-технические и транспортные средства,

конкретных специалистов, оперативных работников для оказания содействия, правильно спланировать выбор и последовательность тактических приемов проведения следственного действия.

Под использованием результатов ОРД для осуществления следственных действий понимается возможность учета названных результатов:

при принятии решения о производстве этих действий;

при непосредственном их проведении.

Некоторые следственные действия (например, очная ставка) проводятся только на основании фактических данных (доказательств), содержащихся в уголовном деле. Основанием проведения других следственных действий может служить совокупность доказательств и фактических данных, почерпнутых из оперативно-розыскных источников. Так, в соответствии с УПК РФ обыск производится при наличии достаточных оснований полагать, что в определенном месте находятся объекты, имеющие значение для дела, т. е. закон не связывает проведение обыска с наличием исключительно доказательств.

Оперативно-розыскные данные могут дополнять имеющуюся совокупность процессуальных сведений о нахождении в определенном помещении или месте, у какого-либо лица объектов, устанавливающих обстоятельства, подлежащие доказыванию по делу. Если, например, задержанный за мошенничество на допросе показал, что он приезжий, в городе постоянно не проживает, что временно остановился у знакомых, то оснований для производства обыска в квартире знакомых в данном случае недостаточно. При получении в результате проведения ОРМ информации о том, что задержанный совершил ряд мошенничеств и в помещении, где он временно проживает, имеются фактические данные (процессуальные и оперативно-розыскные) о следах его преступной деятельности, они в совокупности могут быть признаны следователем достаточными для принятия решения о производстве обыска, который может быть проведен в порядке ст. 164 УПК РФ.

Вызов и допрос свидетеля могут осуществляться на основе одних лишь оперативно-розыскных данных, поскольку уголовно-процессуальный закон практически не ограничивает круг лиц, способных быть свидетелями по делу, и не устанавливает ка-

ких-либо оснований для их вызова. В связи с этим, если соображения конспирации не препятствуют вызову на допрос в качестве свидетеля лица, об осведомленности которого об обстоятельствах дела сообщил конфиденциальный источник, такой вызов и допрос не противоречат уголовно-процессуальным нормам, а значит, допустимы.

Оперативно-розыскные данные, полученные в результате проведения ОРМ, могут использоваться для проведения других ОРМ. Фактические данные, на основе которых принимается решение о проведении ОРМ, подлежат проверке и оценке в их совокупности.

Непосредственным обнаружением признаков преступления следует считать факты выявления кем-либо из компетентных должностных лиц в процессе служебной деятельности сведений об обстоятельствах, указывающих на совершение или подготовку к совершению уголовно наказуемых деяний, если ранее они не располагали заявлением (сообщением) или другим источником информации о преступлении, которое можно отнести к поводам, предусмотренным п. 1 и 2 ч. 1 ст. 140 УПК РФ.

В рапорте об обнаружении признаков состава преступления подробно излагаются обстоятельства совершенного деяния и сведения об источнике получения информации.

Для того чтобы результаты ОРД могли служить основанием для возбуждения уголовного дела, они должны быть достаточны для вывода о наличии в выявленных фактах преступной деятельности признаков преступления.

Результаты ОРД отражаются в оперативно-служебных документах (рапортах, справках, отчетах и т. п.). К оперативно-служебным документам могут прилагаться предметы и документы, полученные при проведении ОРМ. Результаты ОРД могут быть зафиксированы также на материальных (физических) носителях информации. Представляемые материалы должна сопровождать информация о времени, месте и обстоятельствах изъятия в ходе ОРД предметов и документов, получении видео- и аудиозаписей, кино- и фотоматериалов, копий и слепков. При этом должно быть проведено описание индивидуальных признаков указанных предметов и документов.

При использовании в доказывании результатов ОРД следует учитывать, что они доказательствами в уголовно-процессуальном смысле не являются. Результаты ОРД могут быть признаны доказательствами только в случае, если они отвечают требованиям, установленным уголовно-процессуальным законодательством, и признаны таковыми следователем (вынесено соответствующее постановление).

Если на проведение ОРМ было получено в установленном порядке разрешение суда, то результаты ОРД представляются вместе с копией соответствующего судебного постановления.

Если ОРМ осуществлялось на основании постановления руководителя органа или подразделения, осуществляющего ОРД, то результаты ОРД представляются вместе с оригиналом соответствующего постановления.

Если при проверке результатов ОРД будет установлено, что их получение привело к незаконному ограничению конституционных прав граждан, то содержащиеся в них сведения не могут быть использованы в доказывании, что коррелирует со ст. 89 УПК РФ.

Сведения о совершенном преступлении могут содержаться в различных письменных документах, составляемых при проведении гласных ОРМ, а также в протоколах изъятия предметов и материалов. К уголовному делу такие материалы приобщаются в качестве иных документов. Формально «иными документами» могут считаться справки органов, осуществляющих ОРД, с изложением прямых или обобщенных сведений, содержащихся в делах оперативного учета (например, о принадлежности того или иного лица к организованной преступной группе). В то же время их доказательственное значение практически ничтожно, поскольку часто не поддается проверке достоверности представленных сведений.

В соответствии с требованиями Инструкции, если результаты ОРД получены по ранее возбужденному уголовному делу, то они предоставляются следователю в виде сообщения о результатах ОРД. В случае если по выявленным фактам преступной деятельности не было возбуждено уголовное дело, то результаты ОРД предоставляются следователю в виде рапорта об обнаружении признаков состава преступления.

С учетом изложенного процедура предоставления результатов ОРД по мошенничествам, совершенным с использованием ИТТ, осуществляется по следующему алгоритму.

1. Определение перечня результатов ОРД, зафиксированных на материальных носителях информации, соответствующих требованиям уголовно-процессуального законодательства, посредством которых возможно формирование предмета доказывания, подлежащих передаче следователю. Как правило, по мошенничествам, совершенным с использованием ИТТ, такие материалы представляют собой информацию о данных пользователей услуг связи, в том числе почтовой; соединениях между абонентами и (или) абонентскими устройствам; прослушивании телефонных переговоров; банковских транзакциях; активности пользователей сети Интернет. Данные материалы могут быть зафиксированы в виде запросов в соответствующие организации и ответов на них; аудиозаписей (фонограмм), зафиксированных на оптических дисках; стенограмм и иных материальных носителей информации. Полученные при проведении ОРМ материалы могут предоставляться в копиях (выписках), в том числе с переносом наиболее важных частей (разговоров, сюжетов) на единый носитель, о чем обязательно в дальнейшем указывается в сообщении (рапорте) на бумажном носителе записи переговоров. В этом случае оригиналы материалов, документов и иных объектов, полученных при проведении ОРМ, хранятся в органе, осуществившем ОРМ, до завершения судебного разбирательства и вступления приговора в законную силу либо до прекращения уголовного дела (уголовного преследования).

2. Принятие решения о рассекречивании сведений, составляющих государственную тайну, определение объема таких сведений с учетом необходимости формирования доказательственной базы преступной деятельности и необходимости соблюдения конспирации. Не подлежат рассекречиванию и хранению материалы, содержащие информацию о частной жизни, личную и семейную тайну лиц, совершающих мошенничества, если они не относятся к предмету документирования их преступной деятельности.

3. Вынесение руководителем органа или подразделения, осуществляющего ОРД, либо уполномоченным заместителем поста-

новления о рассекречивании сведений, составляющих государственную тайну. В ряде регионов судебно-следственная практика сложилась таким образом, что в постановлении также указывается конкретное местонахождение оригиналов постановлений суда, разрешающих проведение ОРМ, ограничивающих конституционные права и свободы граждан в целях обеспечения подтверждения законности и проверяемости доказательств, полученных в результате таких мероприятий.

4. При документировании мошенничеств, совершенных с использованием ИТТ, редко проводятся ОРМ «проверочная закупка», «контролируемая поставка», «оперативный эксперимент» или «оперативное внедрение», однако в случае их проведения и представления следователю результатов ОРД к ним прилагается постановление руководителя органа или подразделения, осуществляющего ОРД, либо уполномоченного заместителя о проведении данных ОРМ. Копии указанных постановлений органа, осуществляющего ОРД, подлежат хранению в материалах дела оперативного учета, материалах оперативной проверки, а в случае их отсутствия приобщаются к материалам номенклатурного (литерного) дела.

5. Принятие решения о предоставлении следователю результатов ОРД, содержащих сведения об организации и тактике проведения оперативно-поисковых и оперативно-технических мероприятий, используемых при их проведении технических средствах, о штатных негласных сотрудниках оперативно-технических и оперативно-поисковых подразделений. Как правило, такие сведения следователю не предоставляются, а указываются только вид мероприятия в соответствии с Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» и конкретные результаты. При этом местом проведения мероприятия в случае, например, прослушивания телефонных переговоров или снятия информации с технических каналов связи является абонентский номер или номер IMEI мобильного телефона. Напрямую запрет предоставления таких сведений законодательством не установлен, однако Инструкцией закреплена обязанность оперативного подразделения, предоставляющего такие сведения, согласовывать их с исполнителями соответствующих мероприятий и осу-

ществлять в соответствии с требованиями, предъявляемыми к обращению со сведениями, составляющими государственную тайну. На практике совместить факт предоставления таких материалов и при этом обеспечить конфиденциальность сведений, составляющих государственную тайну, зачастую не представляется возможным.

6. Вынесение руководителем органа или подразделения, осуществляющего ОРД, либо уполномоченным заместителем постановления о предоставлении результатов ОРД. Постановление составляется в двух экземплярах, один из которых подлежит хранению в органе, осуществляющим ОРД, и приобщается к материалам дела оперативного учета или в случае его отсутствия – к материалам номенклатурного (литерного) дела. В постановлении указываются конкретные результаты ОРД; длительность, место и вид проводимого ОРМ; вид материального носителя, на котором они задокументированы.

7. Подготовка сообщения о результатах ОРД или рапорта об обнаружении признаков состава преступления. В сообщении или рапорте так же, как и в постановлении о предоставлении результатов ОРД, указываются конкретные результаты ОРД; длительность, место и вид проводимого ОРМ; вид материального носителя, на котором они задокументированы, прилагаются материальные носители сведений, полученных в результате ОРД.

8. Избрание способа фактической передачи результатов ОРД следователю. К числу наиболее распространенных способов относятся передача нарочным и пересылка по почте. При этом возможно предоставление сведений иным способом (например, посредством электронной почты). Способ передачи сведений избирается органом, осуществляющим ОРД, с учетом требований законодательства, нормативных правовых актов, регулирующих организацию делопроизводства, а также в зависимости от конкретной следственно-оперативной ситуации.

9. Фактическое предоставление полученных результатов ОРД.

2.2. Действия оперативных подразделений при проверке заявлений (сообщений) о мошенничествах, совершенных с использованием информационно-телекоммуникационных технологий

При поступлении заявления или сообщения о мошенничестве, совершенном с использованием ИТТ, сотрудники оперативных подразделений должны использовать в полной мере систему научных положений и разрабатываемых на их основе методических указаний и рекомендаций по эффективному использованию сил, средств и методов ОРД для выявления, пресечения и раскрытия преступлений данной категории.

К числу действий оперативных подразделений при проверке заявлений (сообщений) о мошенничествах, совершенных с использованием ИТТ, относятся следующие:

опрос потерпевшего;

документирование первоначальной информации, полученной от потерпевшего и из иных открытых источников информации;

участие в осмотре места происшествия;

запрос информации в организациях, оказывавших услуги связи, в том числе у интернет-провайдеров;

запрос информации в кредитных организациях, а также иных организациях, оказывающих услуги по переводу безналичных денежных средств и их эквивалентов;

запрос информации в логистических организациях, фирмах такси, иных организациях и у физических лиц, участвовавших в качестве посредников при совершении мошенничеств с использованием ИТТ;

фиксация на материальных носителях первоначальных данных об обстоятельствах преступления;

выдвижение версий.

Выполнение перечисленных действий не всегда зависит от сотрудников и может занимать значительный период времени. На сроки получения информации влияет, например, региональная специфика, в том числе следственно-судебная практика, а также наличие специальных каналов связи для получения информации в

электронном виде, договорных отношений между ОВД и кредитными организациями, местонахождение кредитной организации, оператора связи и соответствующего ОВД и множество иных факторов.

Данные действия оперативных подразделений реализуются, как правило, посредством следующих ОРМ:

опрос;

наведение справок;

снятие информации с технических каналов связи;

получение компьютерной информации;

прослушивание телефонных переговоров;

получение образцов для сравнительного исследования;

другие ОРМ, перечень которых определяется в зависимости от результатов ОРМ, проведенных ранее.

Рассмотрим подробнее действия оперуполномоченного при поступлении заявления или сообщения о мошенничестве, совершенном с использованием ИТТ.

При опросе потерпевшего необходимо установить использованные обеими сторонами абонентские номера мобильной связи; адреса электронной почты; доменные имена сайтов; сведения об использованных аккаунтах, в том числе в социальных сетях, мессенджерах; номера банковских карт, электронных кошельков, а также точное время использования каждого из перечисленных ресурсов.

По каждому абонентскому номеру на первоначальном этапе целесообразно попросить потерпевшего самостоятельно запросить у оператора связи детализацию телефонных соединений[1]. Это возможно как путем личного обращения гражданина в отделение оператора связи, так и посредством приложения для смартфона или личного кабинета абонента на сайте оператора связи, при этом детализация направляется на указанный абонентом адрес электронной почты. В детализации отражаются точное время соединений и абонентские номера, использовавшиеся преступниками при совершении преступлений. Данная мера применяется в случаях,

[1] Операторами сотовой связи такая детализация называется «детализация оказанных услуг».

когда отсутствует возможность быстрого получения данной информации посредством ресурсов, имеющихся в ОВД.

В дальнейшем оперуполномоченный проводит ОРМ по наведению справок, в первую очередь на официальном интернет-сайте Центрального научно-исследовательского института связи (https://zniis.ru), оперативный сотрудник самостоятельно определяет оператора связи по абонентскому номеру или номерам, использованным преступником, а также устанавливает субъект Российской Федерации, в котором он зарегистрирован. Факт регистрации абонентского номера в субъекте Российской Федерации не означает факт нахождения там мошенника. Эту информацию можно установить посредством одного из приложений для смартфонов (например, «Сотовые операторы»).

В дальнейшем у операторов связи запрашивается следующая информация:

о регистрационных данных абонентского номера или номеров, использованных преступником для совершения мошенничества;

о фактах пополнения баланса данных абонентских номеров с указанием даты, времени, сумм, а также данных банковских карт, банковских счетов, электронных кошельков или иных абонентских номеров, посредством которых пополнялся баланс абонентских номеров мошенников;

о фактах пополнения баланса других абонентских номеров с использованием абонентских номеров мошенников;

о соединениях между абонентами и (или) абонентскими устройствами, включая информацию о типе, направлении, продолжительности соединения, базовой станции, посредством которой осуществлялось соединение, и ее азимут.

При получении указанных сведений в ходе ОРД сотрудник в своих действиях руководствуется федеральными законами от 7 июля 2003 г. № 126-ФЗ «О связи» и от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Для получения информации необходимо получение разрешения суда в порядке, предусмотренном ст. 9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Полученная в таких

случаях информация может быть передана следователю в установленном порядке для приобщения к материалам уголовного дела.

При использовании для совершения преступления электронной почты также целесообразно попросить потерпевшего предоставить скриншоты переписки с указанием точного времени отправки и получения письма. Эта информация имеет значение для установления IP-адреса, с которого осуществлялась отправка письма. Если пользователь использует для выхода в сеть Интернет услуги связи, то при каждом новом доступе к электронной почте ему предоставляться новый динамический IP-адрес[1].

Когда для совершения преступления использовались регистрационные аккаунты на страницах сети Интернет, запрос направляется владельцу либо администратору соответствующего интернет-ресурса.

Скриншоты переписки потерпевшего с преступником позволяют в дальнейшем при направлении запроса сервису электронной почты конкретизировать время отправки почты. Фиксация переписки может иметь доказательственное значение при задержании подозреваемых и изъятии у них в ходе обысков смартфонов, планшетных и иных компьютеров, использовавшихся при совершении преступления. Кроме того, содержание переписки, стилистические и иные особенности письменной речи подозреваемого являются его характерными признаками, которые могут способствовать установлению личности.

Аналогичным образом необходимо зафиксировать переписку потерпевшего и преступника, если она осуществлялась посредством мессенджеров. В этом случае также могут быть выявлены характерные признаки, имеющие значение для установления личности преступника.

При опросе потерпевшего также целесообразно выяснить, не включена ли в его телефоне функция автоматической записи телефонных переговоров. На практике нередки случаи, когда такая функция включена, а потерпевший об этом не знает или не помнит.

---

[1] Статический IP-адрес – это постоянный IP-адрес в Интернете. Динамический IP-адрес изменяется каждый раз при входе в сеть Интернет, закрепляется за конкретным абонентом и не изменяется до отключения услуги.

При наличии записей переговоров на телефоне, необходимо принять меры к их фиксации. Фиксация информации возможна посредством предоставления ее оперуполномоченному потерпевшим посредством копирования на электронный носитель информации с отражением данного факта в опросе потерпевшего. Данная практика распространена в ряде территориальных подразделений на региональном и районном уровнях. Необходимо учитывать объем запоминающего устройства (встроенной памяти телефона и карты памяти) и принять скорейшие меры к фиксации записей переговоров, не допустив уничтожения ранних записей новыми. В дальнейшем при установлении преступника такие записи могут иметь доказательственное значение и использоваться при проведении фонетической экспертизы.

При совершении ряда мошенничеств денежные средства передаются посредникам по месту жительства потерпевшего либо по месту отделения ПАО Сбербанк России. Чаще всего такой способ передачи денежных средств практикуется при совершении мошенничеств, связанных со звонками на стационарные или мобильные телефоны потерпевших с ложным сообщением о том, что их родственник попал в беду. В таком случае необходим осмотр места происшествия в установленном порядке. В ходе осмотра нужно установить и отработать пути вероятного подхода, подъезда или отхода предполагаемых преступников, установить свидетелей и очевидцев передачи денежных средств и обнаружить следы лиц, получающих денежные средства от потерпевших, а также используемых ими транспортных средств. Полученная информация в дальнейшем может также использоваться для анализа и выявления серийных преступлений.

После получения первичной информации от потерпевшего, ее фиксации, а также проведения комплекса мероприятий по месту передачи денежных средств от потерпевшего посреднику или преступнику необходимо обратиться к учетам ОВД с целью установления фактов совершения аналогичных мошенничеств.

Для получения такой информации возможно обращение к централизованным криминалистическим учетам, ведущимся в ин-

формационных центрах на региональном уровне, так как централизация полной информации о мошенничествах, совершенных с использованием ИТТ, на федеральном уровне не осуществляется.

В ряде регионов (Красноярский край, Алтайский край, Иркутская область и др.) формируются иные формы учетов, позволяющие реализовывать указанные функции на региональном уровне. В перечисленных регионах территориальными подразделениями полиции информация о мошенничествах, совершенных с использованием ИТТ, по утвержденным формам (с указанием абонентских номеров телефонов, IMEI, номеров банковских карт и расчетных счетов, доменных имен сайтов, аккаунтов в различных интернет-ресурсах, электронных кошельков) направляется в региональные информационные центры, где объединяется в единый массив. По нужным реквизитам или по словам из фабулы преступления возможен экспресс-поиск.

Если сотрудник оперативного подразделения при обращении к учетам выявил аналогичные преступления, совершенные ранее, необходимо изучить материалы возбужденных уголовных дел, а также проверки сообщений и заявлений о преступлениях, дел оперативного учета. При изучении таких материалов необходимо установить, какие следственные и процессуальные действия, ОРМ проводились ранее, их результаты. С учетом первичной информации, полученной при опросе потерпевшего, при осмотре места происшествия и в ходе других мероприятий совместно со следователем выдвигаются версии, планируются следственные и процессуальные действия, намечаются дальнейшие ОРМ.

Реализация такого алгоритма препятствует дублированию мероприятий, способствует координированности действий подразделений ОВД в различных районах и регионах.

Помимо этого, на первоначальном этапе необходимо запросить информацию об учреждениях, предприятиях, организациях, как-либо задействованных преступником или преступниками при совершении преступления. В первую очередь оперативный интерес представляет информация от операторов связи и кредитных организаций. В зависимости от обстоятельств преступления у операторов связи запрашиваются следующие сведения:

регистрационные данные аккаунта (дата и время регистрации; IP-адрес регистрации; последние 5 IP-адресов, посредством которых осуществлялось использование аккаунта; дата и время использования; данные указанные при регистрации, в том числе реальные или вымышленные ФИО; хобби, подписи и цитаты, фотографии, анимационные картинки; «друзья» аккаунта на данном интернет-ресурсе);

MAC-адрес компьютера (стационарного, планшетного или иного), операционная система;

адрес электронной почты, посредством которой осуществлялось создание аккаунта, и иные привязанные к аккаунту адреса электронной почты;

иная информация, содержание которой может варьироваться в зависимости от конкретного интернет-ресурса, особенностей программного обеспечения, обстоятельств преступления, сроков и времени хранения информации на сервере.

Получение информации в кредитных организациях при работе по раскрытию мошенничеств, совершенных с использованием ИТТ, имеет ряд отличительных особенностей.

При наличии у потерпевшего информации о реквизитах счета или банковской карты, на которые он перевел деньги, необходимо получить информацию о лице (или организации), на которое(-ую) зарегистрированы данные счет или карта; об абонентских номерах, привязанных к данным карте или счету, об абонентских номерах, которые пополнялись с данных карты или счета; о наличии дубликатов данной карты и об их количестве.

В кредитных организациях также запрашивается информация о транзакциях по банковской карте или счету с указанием номеров и адресов местонахождения банкоматов и платежных терминалов. В ряде территориальных подразделений ОВД существует практика направления в кредитные организации запроса о предоставлении сведений о транзакциях по банковской карте или счету, при этом одновременно запрашиваются видеозаписи с формулировками «при наличии» или «в случае обналичивания денежных средств». Подобную практику в полной мере нельзя признать обоснованной в имеющихся условиях, так как в зависимости от

степени технической оснащенности кредитных организаций информация с записями с камер видеонаблюдения может храниться:

непосредственно в устройствах памяти в банкомате или платежном терминале, с которых осуществлялось снятие денежных средств;

на серверах в населенном пункте, в котором расположены зоны самообслуживания, банкоматы и платежные терминалы.

Информация о транзакциях может храниться на серверах кредитных организаций и выдаваться как в регионе совершения преступления, так и в операционных центрах, не представленных в данных регионах.

В качестве примера можно привести ПАО Сбербанк России, в котором в настоящее время существует ряд ЦСКО (центры сопровождения клиентских операций), которыми обрабатываются запросы правоохранительных органов на выдачу информации о транзакциях, при этом количество таких ЦСКО значительно меньше количества регионов и структурно соответствует количеству территориальных банков в структуре ПАО Сбербанк России.

Таким образом, при направлении единого запроса на получение информации о транзакциях и видеозаписей с камер видеонаблюдения могут возникнуть трудности. За предоставление информации о транзакциях отвечает соответствующий ЦСКО, а за предоставление видеозаписей – техническое подразделение, находящееся в регионе местонахождения банкомата или платежного терминала, к тому же в ряде случаев регионы их местонахождения не совпадают. Это негативно сказывается на скорости получения информации.

Кроме того, в ряде случаев денежные средства обналичиваются посредством не того банка, которым выдавалась банковская карта, и, соответственно, получить видеозаписи можно только после установления информации о транзакциях в кредитной организации, выдававшей банковскую карту, и последующего направления запроса в кредитную организацию, с банкомата которой осуществлялось снятие похищенных в результате мошенничества денежных средств.

Информацией о банковских транзакциях подтверждается факт хищения денежных средств, помимо этого, возможно установление региона или района местонахождения лица, осуществлявшего обналичивание похищенных денежных средств. В то же время этой информации чаще всего недостаточно для полноценного планирования и осуществления мероприятий, направленных на раскрытие преступлений.

В кредитных организациях можно получить следующую информацию:

о лице или организации, на которую зарегистрированы счет или карта;

об абонентских номерах, привязанных к данной карте или счету, об абонентских номерах, которые пополнялись с данной карты или счета;

о наличии дубликатов данной карты и об их количестве, а также о транзакциях;

о дате, времени, месте и суммах проведенных транзакций и (или) операций по обналичиванию денежных средств;

иную оперативно значимую информацию.

Полученная информация подлежит незамедлительной проверке по имеющимся учетам с целью выявления фактов использования абонентских номеров, банковских карт и счетов при совершении иных аналогичных преступлений ранее и (или) в других регионах.

Информацию кредитных организаций и операторов связи можно получить как в порядке, установленном уголовно-процессуальным законодательством, так и в ходе ОРМ, в связи с чем необходимо разграничение действий оперуполномоченного и следователя по ее получению.

Федеральным законом от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» предусмотрены различные процедуры получения информации, составляющей банковскую тайну, для органов, осуществляющих ОРД, и для органов предварительного следствия.

Так, справки по операциям и счетам юридических лиц и индивидуальных предпринимателей, по операциям, счетам и вкладам физических лиц выдаются на основании судебного решения

кредитной организацией 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 Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», 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.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией органам предварительного следствия по делам, находящимся в их производстве, при наличии согласия руководителя следственного органа.

Анализ этих правовых конструкций показывает, что механизм получения информации, составляющей банковскую тайну, для органов предварительного следствия не предусматривает дополнительных процедур, связанных с необходимостью обращения в суд, как в случае необходимости получения аналогичной информации органами, осуществляющими ОРД.

В связи с этим на практике представляется целесообразным получение информации, составляющей банковскую тайну, в порядке, установленном уголовно-процессуальным законодательством.

Получение информации о соединениях между абонентскими устройствами было возможно в порядке, установленном ст. 186.1, ст. 165 УПК РФ, путем направления соответствующего запроса следователя по уголовному делу, находящемуся в его производстве, с приложением постановления суда оператору связи. Оба решения, на наш взгляд, правомерны и могут применяться на практике, однако выбор должен быть обусловлен рядом обстоятельств, имеющих важное значение для раскрытия преступления.

Так, получение информации о соединениях между абонентами в порядке, установленном ведомственными нормативными правовыми актами МВД России, регламентирующими ОРД,

предусматривает проведение мероприятий с использованием ресурсов оперативно-технических подразделений без участия в процессе лиц, не являющихся субъектами ОРД, т. е. исключается вероятность утечки информации о проводимых ОРМ от сотрудников операторов сотовой связи, имеющих отношение к обработке и выдаче информации о соединениях между абонентами, и обеспечивается соблюдение требования конфиденциальности документирования.

Кроме того, получение информации о соединениях между абонентами путем проведения ОРМ имеет, как правило, еще одно преимущество: позволяет сократить время на почтовую пересылку сведений между регионами.

Анализ практики раскрытия преступлений свидетельствует, что эффективное сочетание ОРМ и следственных действий, качественное межрегиональное и межведомственное взаимодействие позволяют минимизировать время, необходимое для установления преступников и пресечения их преступной деятельности.

Исходя из особенностей совершения рассматриваемых преступлений и анализа сведений, полученных в результате выполнения действий по проверке заявлений и сообщений о мошенничествах, совершенных с использованием ИТТ, выдвигаются следующие типичные версии:

преступление совершено лицом, ранее судимым за совершение аналогичных преступлений, находящимся за пределами региона, в котором выявлено преступление;

преступление совершено лицом, ранее судимым за совершение аналогичных преступлений, находящимся в регионе, в котором выявлено преступление;

преступление совершено лицом, отбывающем наказание в исправительном учреждении ФСИН России;

преступление совершено лицом, ранее не судимым, находящимся за пределами региона, в котором выявлено преступление;

преступление совершено лицом, ранее не судимым, находящимся в регионе, в котором выявлено преступление.

При осуществлении дальнейших мероприятий необходимо учитывать такие элементы управленческой деятельности, как планирование мероприятий, межведомственное и межрегиональное

взаимодействие подразделений ОВД, а также ведомственный контроль деятельности ОВД по раскрытию мошенничеств, совершенных с использованием ИТТ.

Планирование в деятельности оперативных и следственных подразделений можно рассматривать как управленческую деятельность, состоящую в согласовании целей и задач на предстоящий период и выработке наиболее рациональных путей и средств их достижения с учетом особенностей оперативной обстановки на обслуживаемой территории или объекте, ресурсных возможностей подразделения, а также вероятных (прогнозируемых) изменений оперативной обстановки.

К особенностям планирования работы при осуществлении противодействия мошенничествам, совершаемым с использованием ИТТ, следует отнести необходимость учета информации о лицах и фактах, неравномерно распределенной в различных базах данных и неструктурированных информационных массивах, а также участия в проведении ОРМ и следственных действий сотрудников оперативных и иных подразделений ОВД различных районов и регионов. При планировании следует также учитывать необходимость своевременного оповещения и возможного привлечения к проведению следственных действий и ОРМ подразделений, участие которых не предполагалось и не являлось очевидным при первоначальном планировании. В связи с этим представляется важным предварительное решение вопроса организации взаимодействия.

Обеспечение ведомственного и межведомственного взаимодействия. Признаками взаимодействия применительно к ОРД следует считать:

координацию проводимых совместных ОРМ и следственных действий;

согласованность места и времени проведения;

правовую и нормативную регламентированность;

достижение единых целей и решение единых задач борьбы с преступностью.

В условиях, когда признаки противоправной деятельности преступников и преступных групп проявляются практически од-

новременно в разных регионах, скоординированные и единонаправленные действия различных оперативных и иных подразделений приобретают особое значение.

Осуществление таких действий возможно путем координации усилий нижестоящих оперативных подразделений соответствующим подразделением на федеральном уровне, а также обеспечения равного доступа всех заинтересованных подразделений (участвующих в проведении конкретных ОРМ) к информации о месте и времени проведения мероприятий, точным и конкретным перечням действий, требуемых от каждого задействованного сотрудника и подразделения.

В случае проведения мероприятий одновременно в нескольких районах и регионах, особенно при реализации материалов оперативных разработок, крайне важно организовать единовременное задержание подозреваемых, проведение обысков и иных мероприятий с целью обеспечения сохранности материальных носителей следов преступления – планшетных и стационарных компьютеров, мобильных телефонов и смартфонов, SIM-карт, банковских карт и иных объектов.

В случае многосубъектности проводимых одновременно в разных регионах мероприятий, т. е. участия в мероприятиях нескольких представителей одного или разных оперативных и иных подразделений, целесообразны на каждом отдельном участке назначение руководителей проводимых мероприятий и организация закрытого канала связи, обеспечивающие эффективное взаимодействие и обмен аудиовизуальной и иной информацией.

К числу оперативных подразделений, организация взаимодействия с которыми в силу специфики деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ, имеет приоритетное значение, относятся подразделения уголовного розыска, подразделения специальных технических мероприятий (оперативно-технические подразделения), оперативно-поисковые подразделения, подразделения оперативно-розыскной информации (далее – ПОРИ).

При взаимодействии подразделений уголовного розыска наибольшее практическое значение имеют обмен информацией о

совершенных преступлениях данной категории, эффективное и рациональное распределение функций по осуществлению ОРМ как в пределах одного региона, так и на территориях, в которых зарегистрированы преступления, имеющие признаки серийности.

В настоящее время эффективная деятельность по раскрытию мошенничеств, совершенных с использованием ИТТ, практически невозможна без использования сил и средств подразделений специальных технических мероприятий и оперативно-поисковых подразделений.

Лицами, совершающими мошенничества с использованием ИТТ, предпринимаются активные меры по обеспечению собственной безопасности, сохранению анонимности в сети Интернет, предотвращению идентификации с помощью средств связи и различных платежных ресурсов. В связи с этим широкое использование возможностей подразделений специальных технических мероприятий и оперативно-поисковых подразделений – эффективное средство обеспечения деятельности ОВД по раскрытию мошенничеств с использованием ИТТ, дополняющее традиционные средства борьбы с преступностью. Особенно важными являются изучение различных организационно-тактических форм мероприятий, выполняемых данными подразделениями, а также выбор тех из них, реализация которых в конкретной оперативно-тактической ситуации будет способствовать изобличению преступников и формированию доказательственной базы. Важно понимать, что инициатором мероприятий, проводимых подразделениями специальных технических мероприятий и оперативно-поисковых подразделений, является оперативный сотрудник, в связи с чем необходимо особое внимание уделять подготовке мероприятий и их информационному обеспечению.

Подразделения ПОРИ являются неотъемлемым дополнением системы информационного обеспечения деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ, так как обеспечивают систематизацию негласной информации, которая зачастую не может быть получена оперативными подразделениями из других источников. Обращение к учетам ПОРИ позволяет обеспечить эффективность взаимодействия подразделений уголовного розыска различных регионов.

Наряду с ведомственным, большое значение имеет межведомственное взаимодействие.

Межведомственное взаимодействие оперативных подразделений правоохранительных органов представляет собой сложный многоаспектный процесс, эффективность которого находится в зависимости от различных факторов, носящих как объективный, так и субъективный характер. К числу наиболее существенных проблем организации межведомственного взаимодействия при осуществлении противодействия мошенничествам, совершаемым с использованием ИТТ, относится организация взаимодействия с оперативными подразделениями ФСИН при работе по раскрытию мошенничеств, совершаемых лицами, отбывающими наказание в учреждениях ФСИН.

Взаимодействие с иными государственными и негосударственными фондами, организациями и учреждениями осуществляется при работе по раскрытию мошенничеств, совершенных с использованием ИТТ, как правило, посредством запросов о предоставлении информации.

Контроль – это система наблюдения и проверки соответствия процесса функционирования принятым управленческим решениям, выявление результатов воздействия субъекта на объект, отклонений от требований управленческих решений.

Контроль в системе ОВД осуществляется уполномоченными руководителями на различных уровнях (федеральном, региональном, районном). Полагаем, что при проведении ОРМ в отношении лица или группы лиц, совершающих мошенничества с использованием ИТТ, применима действующая система контроля, при которой действия в пределах одного региона контролируются уполномоченным руководителем ОВД данного региона, а при проведении ОРМ в рамках одного дела оперативного учета или уголовного дела на территории разных регионов действия контролируются уполномоченными руководителями ОВД данных районов. В то же время в последнем случае требуется активизация руководящей и организационной составляющей данной деятельности на федеральном уровне.

Таким образом, документирование преступной деятельности лиц, совершающих мошенничества с использованием ИТТ, – одно

из направлений совершенствования деятельности по раскрытию преступлений данного вида. Незнание оперативным сотрудником установленных законом требований к документированию преступных событий и фактов может привести к утрате доказательственной базы и нарушению принципа неотвратимости наказания.

Наличие у оперативного сотрудника комплексного представления о системе информационного обеспечения деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ, является неотъемлемым условием для планирования и проведения ОРМ, осуществления оперативно-розыскного обеспечения предварительного следствия.

Заключение

Быстрое развитие ИТТ в сочетании с формированием широкого спектра услуг, предоставляемых кредитными организациями дистанционно, привели к появлению новых видов преступлений, совершаемых с их использованием.

В сложившихся условиях традиционные методы деятельности ОВД по раскрытию преступлений не всегда ведут к положительному результату. Очевидна необходимость овладения оперативными сотрудниками новыми формами и методами борьбы с такими преступлениями.

Первым этапом раскрытия рассмотренных преступлений должно стать изучение особенностей их совершения, образующих в совокупности их оперативно-розыскную характеристику. Невозможно эффективно планировать и проводить мероприятия по раскрытию преступлений, не понимая механизм их совершения, не владея информацией о лицах, их совершающих.

Дальнейшая работа должна быть направлена на изучение особенностей информационного обеспечения деятельности по раскрытию мошенничеств, совершенных с использованием ИТТ, в сочетании с изучением особенностей документирования полученных результатов. Данная деятельность в условиях акцентуации правового института защиты прав и свобод граждан является частью деятельности по обеспечению прав и законных интересов как пострадавших в результате совершения преступлений граждан, так и граждан, подозреваемых в их совершении.

Литература

Нормативные правовые акты

1. Об оперативно-розыскной деятельности: федер. закон от 12 авг. 1995 г. № 144-ФЗ // Собр. законодательства РФ. – 1995. – № 33. – Ст. 3349.

2. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ // Собр. законодательства РФ. – 2001. – № 52 (ч. I). – Ст. 4921.

3. О полиции: федер. закон от 7 февр. 2011 г. № 3-ФЗ // Собр. законодательства РФ. – 2011. – № 7. – Ст. 900.

4. О связи: федер. закон от 7 июля 2003 г. № 126-ФЗ // Собр. законодательства РФ. – 2003. – № 28. – Ст. 2895.

5. О банках и банковской деятельности: федер. закон от 2 дек. 1990 г. № 395-I // Ведомости съезда народных депутатов РСФСР. – 1990. – № 27. – Ст. 357.

6. Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях: приказ МВД России от 29 авг. 2014 г. № 736. – Доступ из справ. правовой системы «Гарант».

7. Об усилении прокурорского надзора и ведомственного контроля за законностью процессуальных действий и принимаемых решений об отказе в возбуждении уголовного дела при разрешении сообщений о преступлениях: приказ Генпрокуратуры России, МВД России, ФСБ России, СК России, ФСКН России, ФТС, ФСИН, Минобороны России, ФССП, МЧС России от 26 марта 2014 г. № 147/209/187/23/119/596/ 149/196/110/154. – Доступ из справ. правовой системы «Гарант».

8. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС, Службы внешней разведки РФ, ФСИН России, ФСКН, Следственного комитета РФ от 27 сент.

2013 г. № 776/703/509/507/1820/42/535/398/68. – Доступ из справ. правовой системы «Гарант».

9. Об эффективности работы по выявлению, пресечению, расследованию и предупреждению преступлений, совершенных с использованием современных информационно-коммуникационных технологий: решение Координационного совещания руководителей правоохранительных органов МВД России: утв. распоряжением МВД России от 12 дек. 2016 г. 1/13128. – Доступ из справ. правовой системы «Гарант».

10. Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Ч. I: Общие требования: приказ Министерства информационных технологий и связи Российской Федерации от 16 янв. 2008 г. № 6. – Доступ из справ. правовой системы «Гарант».

11. Об утверждении общих технических требований к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на сетях (службах) документальной электросвязи: приказ Госкомсвязи России от 27 марта 1999 г. № 47. – Доступ из справ. правовой системы «Гарант».

Основная литература

1. Абышов Д.З., Потапова Н.Н. Некоторые особенности выявления и раскрытия бесконтактного мошенничества // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 4 (40). – 88–93.

2. Акчурин А.В., Шаутаева Г.Х. О некоторых обстоятельствах совершения мошенничества осужденными, отбывающими наказание в исправительных колониях // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 2 (38). – С. 58–63.

3. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. – 2015. – № 4 (34). – С. 209–216.

4. Гилязов Р.Р. Определение места преступлений, предусмотренных ст. 159 УК РФ, совершенных с использованием средств сотовой телефонной связи // Вестник БИСТ (Башкирского института социальных технологий). – 2016. – № 4 (33). – С. 116–121.

5. Горбанев В.М. Оперативно-розыскная характеристика мошенничеств, связанных с использованием средств сотовой связи // Общество и право. – 2016. – № 4 (58). – С. 137–141.

6. Десятов М.С., Васильченко Д.А. Алгоритм действий оперуполномоченного при раскрытии мошенничеств, совершенных с использованием мобильных телефонов // Полицейский сыск. – 2014. – Вып. 3. – С. 118–125.

7. Десятов М.С., Васильченко Д.А. Организационно-тактические аспекты взаимодействия подразделений уголовного розыска и ФСИН России при раскрытии и предупреждении «телефонных» мошенничеств // Полицейский сыск. – 2015. – Вып. 4 . – С. 49–55.

8. Закурдаев А.Н. Основные способы мошенничеств совершенных с использованием мобильных средств связи // Полицейский сыск. – 2015. – Вып. 4. – С. 71–75.

9. Ковалёв С.Д., Полуянова Е.В., Томилин С.М. Содержание тактики применения технических средств при осуществлении оперативно-розыскных мероприятий в исправительных учреждениях // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2017. – 2 (12). – С. 34–39.

10. Кузьмин И.А. Раскрытие мошенничеств, совершаемых с использованием информационно-коммуникационных технологий // И. А. Кузьмин. – Иркутск: Восточно-Сибирский институт МВД России, 2021. – С. 18–25.

11. Кукарцев В.Н. Действия оперативных сотрудников на первоначальном этапе раскрытия мошенничеств, совершенных с использованием средств сотовой связи // Проблемы теории и практики оперативно-розыскной деятельности органов внутренних дел: межвуз. сб. науч. тр. / под ред. Ю.В. Денисенко. – Барнаул: Барнаульский юридический институт МВД России, 2016. – Вып. 13. – С. 99–107.

12. Наливайко Е.О. Противодействие мошенничеству, совершаемому с использованием средств мобильной связи: международный опыт // Актуальные проблемы современности. – 2017. – № 3(17). – С. 15–19.

13. Романовский Г.Б. Банковская тайна и оперативно-розыскная деятельность правоохранительных органов // Наука. Общество. Государство. – 2016. – Т. 4. – № 1 (13). – С. 55–60.

14. Серебряков А.А. Проблемы отнесения сведений к информации, составляющей банковскую тайну // Известия Алтайского государственного университета. – 2016. – № 3 (91). – С. 150–154.

15. Францифоров Ю.В. Определение места совершения телефонного мошенничества // Законность. – 2016. – № 2. – С. 51–53.

16. Фрост С., Федосов А. Проблемы определения места расследования мошенничества с использованием электронных форм платежей // Законность. – 2015. – № 1. – С. 52–53.

17. Чайковский А.А., Крюков И.В. Оперативно-розыскная характеристика мошенничеств, совершенных с использованием средств мобильной связи и интернета в учреждениях УИС // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2016. – № 4 (10). – С. 53–56.

Оглавление

Учебное издание

Южанинов Василий Сергеевич
Студнев Александр Сергеевич
Савченко Михаил Сергеевич

ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Редактор *Э. В. Абрамкина*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-2052-5

9 785926 620525

Подписано в печать 31.10.2024. Формат 60х84 1/16.
Усл. печ. л. 5,3. Тираж 70 экз. Заказ 289.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.