ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОСТОЧНО-СИБИРСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

И. А. Кузьмин

РАСКРЫТИЕ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ИРКУТСК

Федеральное государственное казенное образовательное учреждение
высшего образования
«Восточно-Сибирский институт
Министерства внутренних дел Российской Федерации»

И. А. Кузьмин

РАСКРЫТИЕ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

*Допущено Министерством внутренних дел Российской Федерации
в качестве учебного пособия
для курсантов и слушателей образовательных организаций
системы МВД России, сотрудников органов внутренних дел
Российской Федерации*

Иркутск
Восточно-Сибирский институт МВД России
2021

УДК 34
ББК 67.629.042
К89

Печатается по решению редакционно-издательского совета
Восточно-Сибирского института МВД России

Рецензенты:
В. О. Парамонов, заместитель начальника отдела организации деятельности подразделений уголовного розыска по борьбе с преступлениями против собственности ГУУР МВД России;
И. В. Шабетя, доцент кафедры ОРД ОВД Уфимского юридического института МВД России, канд. юрид. наук

Кузьмин И. А. Раскрытие мошенничеств, совершенных с использованием информационно-коммуникационных технологий: учебное пособие / И. А. Кузьмин. – Иркутск: ФГКОУ ВО ВСИ МВД России, 2021. – 80 с.

К89

В учебном пособии рассмотрены особенности деятельности органов внутренних дел по раскрытию мошенничеств, совершенных с использованием информационно-коммуникационных технологий.

Предназначено для курсантов и слушателей образовательных организаций системы МВД России, обучающихся по специальности: 40.05.02 – Правоохранительная деятельность

УДК 34
ББК 67.629.042

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие информационно-коммуникационных технологий (далее – ИКТ), активное их внедрение в жизнь людей существенно упростило и ускорило 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 из числа таких преступлений в настоящее время относятся различные виды мошенничеств, совершенных с использованием информационно-коммуникационных технологий.

Анализ статистических сведений о состоянии преступности показал, что в 2018 г. в Российской Федерации было зарегистрировано 1 991 532 преступления из них количество зарегистрированных мошенничеств (ст. 159, 159.1–159.6 УК РФ) составило 215 036 преступлений. Удельный вес мошенничеств в общей структуре преступности – 10,8 %. Основную массу таких преступлений составляют мошенничества, совершенные с использованием сети Интернет (56 321); телефонной, в том числе подвижной радиотелефонной связи (42 712); платежных систем и ресурсов, обеспечивающих обмен и передачу денежных ресурсов и их эквивалентов (4 250 преступлений), а также логистических и почтовых организаций (далее – мошенничества, совершенные с использованием ИКТ). С учетом традиционно высокой латентности преступлений данного вида можно предположить,

что фактическое число мошенничеств превышает официальные данные уголовной статистики.

Значительная часть мошенничеств с использованием ИКТ 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 ИКТ, постоянно развивающимися технологиями в сфере связи и телекоммуникационных технологий, высоким удельным весом преступлений в структуре преступности деятельность ОВД по их раскрытию требует активных мер, направленных на ее совершенствование.

В связи с тем, что постоянно расширяется видовое разнообразие используемых мошенниками средств для совершения преступления, увеличивается количество применяемых схем. Первая глава посвящена описанию таких значимых элементов оперативно-розыскной характеристики преступлений данного вида, как состояние, структура и динамика мошенничеств, совершаемых с использованием ИКТ; обстоятельства совершения и сокрытия преступлений; характеристика личности потерпевшего и лиц, совершающих мошенничества с использованием ИКТ; 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 диктует особые требования к качеству документирования и информационного обеспечения оперативно-розыскной деятельности по раскрытию преступлений в целом и мошенничеств с использованием ИКТ в частности, данное направление деятельности нашло подробное отражение во второй главе пособия.

Целью работы является раскрытие для курсантов и слушателей образовательных организаций, находящихся в ведении МВД России, различных аспектов деятельности органов внутренних дел по раскрытию мошенничеств, совершенных с использованием ИКТ, а также совершенствование отдельных актуальных аспектов данной деятельности.

ГЛАВА 1.
ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

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

Подробно осветить все применяемые преступниками схемы и методы в рамках настоящей работы не представляется возможным в связи с их значительным количеством, а также постоянно увеличивающимся видовым разнообразием в связи с совершенствованием ИКТ, поэтому целесообразно сосредоточиться на изучении, 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 связи, а также почтовой связи; платежных систем и ресурсов, обеспечивающих обмен и передачу денежных ресурсов и их эквивалентов, а также логистических и почтовых организаций.

Указанные способы совершения 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 ИКТ, проявляются как структурный элемент корыстной преступности.

Изучение совокупности данных, характеризующих мошенничества, совершенные с использованием ИКТ, показывает, что структуру их оперативно-розыскной характеристики формируют следующие, наиболее важные, по нашему мнению, элементы:

1) состояние, структура, и динамика мошенничеств, совершаемых с использованием ИКТ;

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

3) характеристика личности потерпевшего и лиц, совершающих мошенничества с использованием ИКТ;

4) особенности виртуальных следов.

Рассмотрим указанные элементы подробнее.

1. Состояние, структура и динамика мошенничеств, совершаемых с использованием ИКТ.

Данный элемент оперативно-розыскной характеристики мошенничеств, совершаемых с использованием ИКТ, имеет существенное значение для организации оперативной-розыскной деятельности 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 ИКТ, организацию межведомственного и межрегионального взаимодействия.

По данным ГИАЦ МВД России, общее число зарегистрированных преступлений в 2019 г. снизилось на 3,3 %. Количество зарегистрированных мошенничеств (ст. 159, 159.1–159.6) снизилось на 3,5 % и составило по итогам 2018 г. 215 036 преступлений. Удельный вес мошенничеств в общей структуре преступности составил 10,8 %. Таким образом, каждое десятое регистрируемое преступление на территории России – мошенничество.

Изучение статистических данных показывает, что количество мошенничеств, совершаемых с использованием ИКТ, 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 уже в 2017 г. – превысило. Такая динамика состояния преступности сохраняется в настоящее время и, можно предположить, что сохранится и в дальнейшем.

Наибольшее количество мошенничеств, совершенных с использованием сети Интернет, зарегистрировано в январе–марте 2019 года в г. Москве (1401), Тюменской области (743), Татарстане (713), Краснодарском крае (523), Красноярском крае (448), Ростовской области (438), Пермском крае (421), Самарской области (416), Кемеровской области (377), Новосибирской области (365).

Наибольшее количество мошенничеств, совершенных с использованием мобильной связи, зарегистрировано в январе–марте 2019 г. в Краснодарском крае (1 125), Москве (849), Татарстане (503), Красноярском крае (479), Алтайском крае (433), Ростовской области (430), Тюменской области (411), Самарской области (336), Ставропольском крае (323), Вологодской области (302).

Динамика и структура отдельных видов мошенничеств, совершаемых с использованием ИКТ, приведена в табл. 1.

Таблица 1

Структура и динамика отдельных видов мошенничеств, совершаемых на территории Российской Федерации в 2015–2019 гг.

	2015	2016	2017	2018	январь-март 2019
Зарегистрировано мошенничеств	174267	188246	202622	215036	62257
раскрыто	17483	17846	19278	56318	16926
установлено лиц	23994	23277	22924	37018	10150
Мошенничества, совершенные с использованием сети Интернет	нет данных	31190	50119	56321	16105
раскрыто		1201	2056	5120	1361
установлено лиц		н/д	н/д	4863	1327
Мошенничества с использованием средств мобильной связи	21562	31236	44081	42712	12779
раскрыто	1541	2381	3016	4190	997
установлено лиц	275	542	917	4063	991
Мошенничество совершено с использованием средств мобильной связи осужденным лицом, содержащимся в учреждении ФСИН	42	183	294	225	13
раскрыто	70	261	390	491	70
установлено лиц	14	37	73	491	70

Таким образом, анализ данных уголовной статистики показывает, что, уровень мошенничеств, совершенных с использованием ИКТ, высок; количество преступлений, совершенных с использованием ИКТ ежегодно увеличивается; самым распространенным видом мошенничеств, совершенных с использованием ИКТ являются мошенничества, совершенные путем фиктивной продажи товара посредством сети Интернет и SMS-рассылок; раскрываемость мошенничеств, совершенных с использованием ИКТ, продолжает оставаться низкой; деятельность ОВД по раскрытию мошенничеств, совершенных с использованием ИКТ остается неудовлетворительной, раскрывается лишь каждое девятое из числа совершаемых преступлений. При этом анализ состояния, структуры, динамики преступлений данного вида проводился на основании ведомственной статистики, с учетом зарегистрированных преступлений, без учета латентности.

2. 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 ИКТ.

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.

При описании мошенничеств, совершенных с использованием ИКТ, 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 ИКТ, позволяет их структурировать 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[2] (в том числе посредством приложения для мобильных устройств) или на форуме в социальной сети[3]. Также возможна публикация такого объявления посредством газет[4] 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[5]; идентификационный номер программы или приложения для мгновенного обмена сообщениями, осуществления аудио- и видеозвонков[6], адрес электронной почты. Цена товара или услуги, указанная в объявлении, как правило, ниже рыночной, для привлечения внимания потенциального потерпевшего. После того, как потерпевший

---

[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.).

[2] www.avito.ru, youla.io, drom.ru, kupiprodai.ru, market.yandex.ru и др.

[3] ВКонтакте, Одноклассники, Мой Мир и др.

[4] Напр., «Из рук в руки».

[5] 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.

[6] Skype, Hangouts, Алле, TOX, ooVoo, KakaoTalk и др.

свяжется с преступником, ему предлагается осуществить полную или частичную оплату товара или услуги.

Как правило, преступник готов предоставить «документы», удостоверяющие свою 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], тем самым создав в последнем уверенность в действительности сделки.

Денежные средства потерпевшим могут отправляться: на банковскую карту, лицевой счет в банке, электронный кошелек, путем перевода на предъявителя[3]. Данный вид мошенничеств совершается, как правило, мошенниками 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].

Данные преступления совершаются мужчинами в 62 % случаев, женщинами в 38 %.

Преступления, составляющие данную категорию, в настоящее время являются наиболее распространенными в структуре мошенничеств, совершенных с использованием ИКТ, 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 сайтам, указанным в описании мошенничеств при фиктивной продаже товара. Обнаружив объявление, преступник звонит потерпевшему и сообщает о своем желании приобрести товар

---

[1] Напр., 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, чтобы определить 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. См., напр., услугу ПАО Сбербанк России «Колибри».

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

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 сообщит необходимые данные, преступник производит перевод денежных средств потерпевшего со счета его банковской карты. Также 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 подключает свою банковскую карту к абонентскому номеру преступника и предоставляет ему код для первоначального входа в интернет-банкинг[3];

3) преступления, связанные с рассылкой SMS-сообщений. Алгоритм действий преступников следующий.

Потерпевшим рассылаются SMS-сообщения следующего содержания: «Ваша банковская карта заблокирована ЦБ РФ. Тел. для справок…», «Вы получили приз, дополнительная информация по телефону…», «С Вашей банковской карты списано **** рублей по решению суда. Доп. 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.

---

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

[2] В случае, если ресурс, используемый преступниками, не поддерживает технологии 3DSecure или MasterCard SecureCode (принятыми основными платежными системами, такими как Visa, MasterCard, Мир и другими), то СМС-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. Также в отдельных случаях возможна оплата без кода подтверждения услуг телефонной связи некоторых операторов связи, внесение денежных средств на игровые порталы и т.д.

[3] В соответствии с п. 2 постановления Пленума Верховного суда Российской Федерации 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 ИКТ. В связи с этим мы рассмотрим вопросы оперативно-розыскного противодействия преступлениям данной категории вместе с мошенничествами, совершенными с использованием ИКТ.

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

Альтернативным способом совершения таких преступлений является также 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, 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 за «доставку» 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. указывается диапазон номеров, на которые преступниками направлялись SMS-сообщения с ложным сообщением о выигрыше. При возникновении вопроса у потерпевших, почему номера указаны не полностью, это объясняется соблюдением закона о защите персональных данных.

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

Удельный вес преступлений в структуре мошенничеств, совершенных с использованием ИКТ, 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.) и 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 преступления. 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 ИКТ, а также с учетом необходимости 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 оплаты за услуги 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 одним и теми же лицами в небольшой промежуток времени, нередко живут в одном населенном пункте[1]. Описанный факт стал причиной еще одной особенности мошенничеств данного вида, которая заключается в следующем. Преступники стараются 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 также и тем, что не нужно вновь подыскивать нового посредника. Посредники не всегда сразу осознают тот факт, что участвуют в преступной деятельности. Часто понимание преступного характера своих действий наступает на втором или последующих преступлениях.

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

В данном случае выражен групповой характер совершения преступлений. 64 % преступлений совершены двумя и более лицами. Удельный вес таких преступлений в структуре мошенничеств, совершенных с использованием ИКТ, составляет 27 %;

[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.

5) преступления, связанные с фиктивным предоставлением кредитов.

Алгоритм действий преступников следующий. В социальных сетях создается фейковый[1] 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[2], 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.

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

Удельный вес описанных преступлений в структуре мошенничеств, совершенных с использованием ИКТ, 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, «бегущей строке» по телевидению, распространяется информация о проведении «компьютерного тестирования» состояния здоровья. Когда потерпевший звонит по указанному в объявлении телефону, ему предлагается отправить образцы слюны, ногтей, волос по указанному мошенниками почтовому адресу. Адрес, как правило, вымышленный 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

[1] От англ. fake – обман, фальсификация.

[2] 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.

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 особенностью 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 сообщается, что лица, которым потерпевший ранее отправлял деньги, задержаны и что потерпевшему полагается возмещение ущерба в сумме, многократно превышающей отправленную последним сумму. 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 чего 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 под вымышленными регистрационными данными. 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, заключаются в обналичивании денежных средств, направленных на их имя потерпевшими посредством банковских переводов и последующем направлении данных денежных средств преступникам. Посредники, как правило, участвуют в совершении мошенничеств данного вида не более одного раза.

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

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 ИКТ, составляет 4 %.

Изучение массива сведений о мошенничествах, совершенных с использованием ИКТ, позволило выявить основные ресурсы и средства, используемые при их совершении. Такой ресурс как «криптовалюта» в общей структуре мошенничеств с использованием ИКТ, 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 ИКТ, составляют мошенничества, связанные с фиктивной покупкой и продажей товаров или услуг посредством сети Интернет; все описанные мошенничества, совершенные с использованием ИКТ, объединяет факт использования средств мобильной связи, услуг кредитных организаций, сети Интернет.

Особое место в структуре оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИКТ, занимает 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 такого места совершения преступления с точки зрения криминалистики в первую очередь интересуют следы, которые могут способствовать установлению виновного лица, обстоятельств преступления и т. д. А с точки зрения криминологии интересуют особенности места преступления в контексте устранения причин и условий, способствующих его совершению.

В случаях мошенничеств, совершенных с использованием ИКТ, встреча потерпевшего и преступника в привычном понимании, как правило, не происходит. Одной из особенностей мошенничеств, совершенных с использованием ИКТ, является тот факт, что преступник и потерпевший проживают[1] 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 бан-

[1] До 80–85 % преступлений данной категории.

ках 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, совершенных с использованием ИКТ, становятся следы преступления, остающиеся только в особой информационной среде, за исключением преступлений, при совершении которых участвует посредник, встречающийся с потерпевшим. Причины, способствующие совершению мошенничеств с использованием ИКТ, обусловливаются, прежде всего, не особенностями какого-либо участка местности, а доступностью технологических решений, обеспечивающих связь между преступником и потерпевшим, и обмен денежными средствами.

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

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

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного суда Российской Федерации от 27 дек. 2007 г. № 51 // Доступ из справочно-правовой системы «Гарант».

Однако, на первоначальном этапе рассмотрения заявления о мошенничестве, совершенном с использованием ИКТ, 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 уголовное дело возбуждаться по месту выявления преступления, в соответствии с требованиями действующих нормативно-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 ИКТ, 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 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 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, преступления вида могут совершаться осужденными лицами, находящимися в учреждениях ФСИН и вне зависимости от режима работы учреждения. В связи с изложенным, временной критерий с практической точки зрения малоприменим. Это обусловлено тем обстоятельством, что время совершения преступления для потерпевшего не коррелирует со временем преступления для преступника.

Как указывалось ранее, 77,6 % уголовных дел о мошенничествах, совершенных с использованием ИКТ, возбуждены вне региона местонахождения преступника. Таким образом, в этих случаях время преступления для преступника не будет соответствовать времени преступления для потер-

[1] 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 РФ 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 Генер. прокуратуры РФ, МВД РФ, ФСБ РФ, СК РФ, ФСКН РФ, ФТС, ФСИН, Мин. обороны РФ, ФССП, МЧС от 26 марта 2014 г. № 147/209/187/23/119/596/149/196/110/154; Уголовно-процессуальный кодекс Российской Федерации, утв. Федеральным законом от 18.12.2001 № 174-ФЗ // Доступ из справочно-правовой системы «Гарант».

певшего из-за разницы часовых поясов. Кроме того, выполнение объективной стороны для отдельных видов мошенничеств, совершенных с использованием ИКТ, 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 ИКТ соучастники преступлений могут одновременно находится в разных регионах и для каждого «действующего лица» в преступлении, в том числе потерпевшего, будет «свое» время.

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

3. Характеристика личности потерпевшего и лиц, совершающих мошенничества с использованием ИКТ.

Анализ мошенничеств, совершенных с использованием ИКТ, позволяет сделать вывод, что личностные особенности и преступника, и потерпевшего имеют существенное значение для успешного завершения начатого преступления. Действительно, очень важным в этой связи становится умение преступника убеждать, менять свои слова и действия в зависимости от линии поведения потерпевшего. Легковерность потерпевшего, степень его осведомленности об ИКТ также зачастую имеет 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. Поэтому при анализе роли конкретной жизненной ситуации в совершении преступления необходима всесторонняя и объективная оценка значения поведения потерпевшего»[1].

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

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

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

Таблица 2

Возрастные категории потерпевших по мошенничествам, совершенным с использованием ИКТ

	Возраст до 35 лет	Возраст от 35 до 50 лет	Возраст от 50 до 65 лет	Старше 65 лет
Мошенничества, совершенные с использованием ИКТ	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 преступления по возрасту потерпевших распределены неравномерно в зависимости от средств, используемых преступниками. В отношении пожилых лиц чаще совершаются мошенничества, совершенные с использованием мобильного телефона. Преступления же, связанные с использованием сети Интернет, относительно равномерно распределены по возрасту между молодыми людьми и лицами средних лет. Это во 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 категории 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 в связи с тем, что именно мошенничества, связанные с фиктивными покупками и продажами в сети Интернет, в настоящее время составляют основную часть преступлений, совершенных с использованием ИКТ.

[1] Рынок интернет-торговли в РФ: отчет Национального исследовательского университета «Высшая школа экономики». URL: https://dcenter.hse.ru/data (дата обращения 10.07.2018 г.).

Таблица 3

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

Мужчины (46)		Предпочтения покупателей в сети Интернет	Женщины (54)	
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-супермаркетов 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

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

К числу основных элементов оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИКТ, относится личность преступника: пол, возраст, образование, наличие судимости. Изучение материалов уголовных дел показало, что лицами, совершающими мошенничества с использованием ИКТ, 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 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 ИКТ, быстрее осваивать возможности сети Интернет и мобильных устройств для успешной реализации своих преступных планов.

Изучение материалов уголовных дел показало существенное расхождение местонахождения преступников на момент совершения преступления в зависимости от его способа. Так, 74 % преступников находились в местах лишения свободы при совершении мошенничеств по схеме «род-

ственник в беде», при этом 92 % преступников находились на свободе при совершении иных видов мошенничеств с использованием ИКТ.

Проведенное исследование показало, что около 62 % мошенников ранее привлекались к уголовной ответственности либо имели судимость на момент совершения преступления. Таким образом, криминальный опыт преступников свидетельствует о стойкой противоправной направленности и возможности активного противодействия оперативно-розыскным средствам и методам. Этот факт должен учитываться оперативными сотрудниками ОВД при планировании и проведении ОРМ.

Изучение 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 преступления имеет факт совершения преступлений мошенниками, находящимися в одном регионе, в отношении жителей иных регионов.

В связи с этим правоохранительные органы региона местонахождения и 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 преступлений 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 ИКТ: 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 органов внутренних дел по противодействию данным видам преступлений (общая сумма превышает 100 %, так как респондентам предлагалось указать несколько вариантов ответов).

4. Особенности виртуальных следов.

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

Как показывает практика, такие следы будут распределены, в зависимости от средства, посредством которого совершено преступление (мобильное устройство, сеть Интернет): в компьютерной системе, мобильных устройствах, электронных носителях информации преступника и потерпевшего, компьютерных системах операторов связи, в связи с чем необходимо при проведении ОРМ особое внимание уделять обнаружению таких средств. При этом нужно учитывать возможность уничтожения виртуаль-

ных следов и их электронных носителей, что непосредственно влияет на необходимость максимально быстрого обнаружения следов и носителей, а также обусловливает необходимость получения 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 ИКТ (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. Изложенные 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 ИКТ.

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 ин-

[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.

формация. 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 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 информацию с компьютера или мобильного устройства можно восстановить посредством аппаратно-программных комплексов и программных средств[2].

Информация об элементах оперативно-розыскной характеристики мошенничеств, совершенных с использованием ИКТ, позволяет моделировать механизм совершения преступления, что позволяет планировать тактику проведения ОРМ, направленных на раскрытие преступления. 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 информационно-коммуникационных технологий, является одним из важных компонентов обеспечения организации противодействия преступлениям данной категории.

---

[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.

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

ГЛАВА 2.
ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ ОСОБЕННОСТИ РАСКРЫТИЯ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1. Информационное обеспечение и документирование деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ

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

Раскрытие мошенничеств, совершенных с использованием ИКТ, представляет собой сложную деятельность ряда взаимодействующих субъектов, направленную на своевременное получение, фиксацию и использование оперативно-значимой информации, в связи с чем особое значение приобретает эффективная организация такой деятельности.

Организация оперативно-розыскной деятельности 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 оперативно-розыскной деятельности для успешного решения профессиональных задач по борьбе с преступностью во взаимодействии с другими службами и органами[1].

Организация оперативно-розыскной деятельности включает в себя мероприятия, направленные на создание кадровых, структурных, информационных, материально-технических предпосылок эффективной борьбы с преступностью.

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

---

[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.

Под информационным обеспечением деятельности оперативных подразделений органов внутренних дел 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 органов внутренних дел по раскрытию мошенничеств, совершенных с использованием ИКТ, 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 ИКТ, а также выявления и пресечения лиц, их подготавливающих, совершающих или совершивших.

Прежде чем приступить к описанию процесса ИО оперативно-розыскной деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ, 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 ИКТ.

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

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

Содержание оперативно-розыскной информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИКТ, 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;

---

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

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

5) информация о ранее проведенных и проводимых оперативно-розыскных мероприятиях;

6) информация, имеющая значение для планирования и проведения оперативно-розыскных мероприятий;

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

Оперативно-розыскная информация, представляющая интерес для раскрытия преступлений, совершенных с использованием ИКТ, 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 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 ИКТ, 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 ИКТ, изучение и систематизация которой позволяет планировать и проводить оперативно-розыскные мероприятия и следственные действия, направленные на раскрытие преступлений данной 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 ИКТ, данные учеты могут содержать информацию о следах преступлений, представляющую интерес для данной деятельности. Экспертно-криминалистическая информация представляет собой индивидуальную

[1] Утверждено приказом 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 Генеральной прокуратуры Российской Федерации от 12 февр. 2014 г. № 9дсп/19дсп/73дсп/1адсп/113дсп/108дсп/75дсп/93дсп/19дсп/324дсп/133дсп/63дсп/14/95дсп.

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, сотрудниками оперативных подразделений органов внутренних дел, а также сотрудниками экспертно-криминалистических подразделений органов внутренних дел в пределах их компетенции. Экспертно-криминалистические учеты органов внутренних дел 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 ИКТ, 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 органов внутренних дел в порядке, установленном ФЗ «О полиции», ФЗ «Об ОРД», 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, включая сведения об их месте и времени;
- о договорах об оказании различных банковских услуг, включая сведения о дате и месте их заключения, сторонах, условиях и иных обстоятельствах договора.

Формирование и ведение баз данных и массивов осуществляется кредитными организациями в порядке ФЗ «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 ИКТ.

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

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

- о регистрационных данных пользователей услуг связи (абонентов);

- о соединениях между абонентами и (или) абонентскими устройствами, включая информацию 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; 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 пакетов данных, размере, типе, IP-адресе получателя или отправителя пакетов данных и другая информация.

В некоторых случаях возможно получение данных о конфигурации компьютера преступника.

Формирование и ведение информационных массивов и баз данных осуществляется операторами связи в порядке ФЗ «О связи», Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД; «Требований к сетям электросвязи для проведения оперативно-разыскных мероприятий. Часть 1. Общие требования»; внутренних правил оператора связи, а также иных нормативных правовых актов. В связи с тем, что преступниками при совершении мошенничеств с использованием ИКТ 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 ИКТ.

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, сведения о месте регистрации, наличии автомобиля, штрафах и налогах, очередях в больницы и детские сады и многое другое. Так, например, 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 ИКТ, 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 осуществляется операторами связи в порядке, установленном федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных"[1], а также рядом иных нормативных правовых актов в зависимости от органа учета.

7. Информационные массивы и базы данных транспортных компаний и логистических организаций. В данных массивах и базах 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 осуществляется по московскому времени, что необходимо учитывать при анализе информации, полученной в почтовых организациях. Формирование и ведение информационных массивов и баз данных осуществляется операторами почтовой связи и логистическими организациями, как правило, по месту расположения оператора почтовой связи или логистической организации в порядке, установленном федеральным законом от 17 июля 1999 г. № 176-ФЗ "О почтовой связи"[2], федеральным законом от 28 декабря 2009 г. № 381-ФЗ "Об основах государственного регулирования торговой деятельности в Российской Федерации"[3], а также иными нормативными правовыми актами.

Обращение к информационным массивам и базам данных актуально при работе по раскрытию мошенничеств с использованием ИКТ, при совершении которых потерпевшему посредством логистических организаций либо транспортных компаний направляется 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 и для того, чтобы потерпевший убедился в ее действительности и направил преступнику денежные средства.

8. Информационные массивы, базы данных и каналы связи Интерпола. Инструкцией по организации информационного обеспечения сотруд-

[1] СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.
[2] Там же. 1999. № 29. Ст. 3697.
[3] Там же. 1999. № 1. Ст. 2.

ничества по линии Интерпола[1] предусмотрен ряд направлений информационного обеспечения борьбы с преступностью. К числу наиболее значимых в контексте раскрытия мошенничеств, совершенных с использованием ИКТ относится информационное обеспечение борьбы с преступлениями в области высоких технологий (раздел 9 указанной инструкции).

При работе по раскрытию мошенничеств, совершенных с использованием ИКТ, 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 выше базы данных формируют систему ИО деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ.

Организацию деятельности оперативных подразделений по получению оперативно-розыскной информации, имеющей значение для раскрытия мошенничеств, совершенных с использованием ИКТ, 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 ИКТ, а также сокращение сроков ее получения.

[1] Утверждена приказом МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 06.10.2006 // Доступ из СПС «Гарант».

Для противодействия преступлениям в сфере ИКТ и компьютерных технологий правоохранительные органы должны обладать знанием способов совершения таких преступлений, тактики и методики выявления, раскрытия и расследования преступлений данной категории; стремиться к превосходству над злоумышленниками в уровне технической оснащенности и скорости получения информации. Однако сотрудники ОВД, осуществляющие противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий, 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 ИО в борьбе с преступлениями, совершенными с использованием ИКТ, являются следующие:

1. Длительность получения справок по счетам и вкладам физических лиц из кредитных организаций.

2. 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.

3. Длительность получения информации от интернет-провайдеров, а также от владельцев и администраторов различных интернет-ресурсов.

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

В ходе изучения информации о мошенничествах, совершенных с использованием ИКТ, 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, совершенные с использованием ИКТ, объединяет одна общая черта: все они совершены дистанционно, т. е. личный физический контакт между потерпевшим и преступником отсутствует. Поэтому 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. В этой связи получение информации в кредитных организациях и у операторов

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

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 ИКТ, 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[1], 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 ИКТ, как правило, предшествуют тщательные подготовительные мероприятия со стороны причастных к ним лиц, а именно:

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

2) частая смена места жительства;

3) 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 ИКТ относятся:

1) 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;

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

3) 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 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 ИКТ – получение и процессуальное закрепление следов преступления, оставленных в информационной среде. В отдельных

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

случаях для этого гласно и негласно задействуются десятки гражданских организаций и учреждений, а также подразделений и ведомств правоохранительных органов. В таких условиях особое значение приобретает выбор механизма реализации конкретного мероприятия, способ получения информации, имеющей значение для дела.

Выбор метода должен соответствовать действующему законодательству, при этом отвечать как решению задач оперативно-розыскной деятельности, так и обеспечивать реализацию общих принципов уголовного законодательства, в частности, неотвратимости наказания.

Изложенное объективно свидетельствует о том, что для повышения эффективности противодействия мошенничествам, совершаемым с использованием ИКТ, 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, последующую ее 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 ИКТ 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 оперативно-розыскную деятельность, у операторов связи посредством СОРМ, регламентированы Федеральным законом от 07.07.2003 № 126-ФЗ «О связи», правилами взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими ОРД, утвержденными постановлением Правительства Российской Федерации 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 опера-

тивного 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 и 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, обеспечивающие 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.

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 оперативно-розыскную деятельность, 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 «О банках и банковской деятельности» от 02.12.1990 № 395-1 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 отсылоч-

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

ных 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 ИКТ, 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 «О банках и банковской деятельности» от 02.12.1990 № 395-1, предусматривающих обязанность предоставления кредитными организациями сведений, содержащихся в базах данных кредитных организаций органам, осуществляющим оперативно-розыскную деятельность посредством закрытых каналов связи.

Пока же 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 органами внутренних дел на региональном уровне.

В качестве примера успешно реализованного ранее такого соглашения можно привести соглашение «Об электронном обмене документами и информацией для выполнения правоохранительным органом возложенных на него функций» № 31/1/1/75 – 2016, заключенного 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 1.1.5. (система передачи и обработки данных) – корпоративной системе ПАО Сбербанк России, включающей в себя совокупность программных и/или программно-аппаратных средств, устанавливаемых у органа внутренних дел 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 органе внутренних дел 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).

Также вышеуказанным 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 также позволит повысить эффективность деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ.

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 оперативных 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 должностного лица, ее получившего, мерами безопасности, предпринимаемыми в конкретном подразделении и т. д. Кроме того, за не-

[1] По состоянию на 15.11. 2019 г.
[2] По состоянию на 17.11. 2019 г.

правомерные действия, связанные с ее использованием и распространением, предусмотрены различные виды ответственности, а порядок доступа и использования такой информации регламентирован рядом федеральных законов и ведомственных нормативных правовых актов. Таким образом, решающее значение имеет решение технического аспекта получения такой 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 ИО по борьбе с мошенничествами, совершенными с использованием ИКТ 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, изложенных в главе 1 пособия.

Так, в статистической карточке формы № 1 на выявленное преступление[1], реквизитом № 28 (преступление совершено с использованием) предусмотрены коды: 007 (компьютерной техники), 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) и 49 (с использованием мобильной связи). При этом в статистические карточки не вносятся и не учитываются такие важные особенности совершения мошенничеств с использованием ИКТ, как:

1. Абонентские номера, IMEI-номера IP-адреса, MAC-адреса использованные преступниками для связи с потерпевшим, абонентские номера потерпевших.

2. Информация о дате, времени и продолжительности соединения между абонентскими номерами преступников и потерпевших.

3. Информация об операционной системе устройств, использованных преступниками для совершения мошенничеств с использованием ИКТ.

4. Учетные данные аккаунтов на интернет-сайтах, использованных преступниками для совершения преступлений.

5. Информация о фотографиях, переданных преступниками потерпевшим для обеспечения легенды мошенничества.

6. Информация о номерах банковских карт и счетов, используемых преступниками для совершения преступлений.

[1] Утверждена приказом 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.

7. Информация о доменных именах сайтов, на которых преступники размещали объявление о фиктивной покупке или продаже товаров или услуг, либо потерпевшие размещали объявление о продаже товаров или оказании услуг.

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

Анализ практики показывает, что отдельными органами внутренних дел на региональном уровне предпринимаются меры по формированию статистической отчетности в пределах имеющихся полномочий и возможностей. Так, Главным управлением внутренних дел МВД России по Иркутской области, а также рядом иных органов внутренних дел 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 ИКТ, 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 органов внутренних дел.

Органами внутренних дел должны формироваться региональные учеты с описанием и систематизацией вышеизложенных сведений в целях совершенствования ИО деятельности по противодействию мошенничествам, совершенным с использованием ИКТ, а в их отсутствие – на территориальном.

Описанные особенности совершения мошенничеств с использованием ИКТ позволяют систематизировать и анализировать полученную информацию и планировать на основании анализа данной информации оперативно-розыскные мероприятия и следственные действия.

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

На основании анализа нормативной правовой базы, а также теории и практики, ИО деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ, можно представить в виде указанной ниже схемы.

Документирование полученной информации и передача ее следственным подразделениям.

Под документированием преступных действий понимается выявление оперативно-розыскным путем фактических данных, свидетельствующих о причастности их к приготовлению или совершению преступления, и обеспечение возможности использования этих данных для предотвращения или раскрытия преступлений и принятия к виновным мер, предусмотренных законом.

Документирование мошенничеств, совершенных с использованием ИКТ, 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 ИКТ, следует использовать все находящиеся в распоряжении органов внутренних дел силы, средства, методы, а также помощь отдельных граждан. Однако в результате применения этих средств и методов часто получают сведения, которые требуют тщательной проверки с тем, чтобы убедиться, что данные будут способствовать установлению истины.

Проверка должна дать ответ на вопросы:

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

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

3) какова возможность использования полученных фактических данных в целях получения судебных доказательств при расследовании уголовного дела.

Оперативно-розыскные мероприятия 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 ИКТ.

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

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

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

3) обстоятельства, характеризующие личность обвиняемого;

4) характер и размер вреда, причиненного преступлением;

5) обстоятельства, исключающие преступность и наказуемость деяния;

6) обстоятельства, смягчающие и отягчающие наказание;

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

Зная предмет доказывания по отдельным видам мошенничеств, совершенных с использованием ИКТ, 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 получаемые 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 тем самым объективно провести проверку информации. Это позволит при использовании полученных данных, с одной стороны, избежать необосно-

ванного 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 получения судебных доказательств. Практика показывает, что не всегда имеется возможность использовать полученные негласным путем фактические данные при расследовании для получения 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. Поэтому при документировании нужно стараться получить такие сведения, которые можно проверить проведением следственных действий. В связи с этим лишь в том случае можно считать, что преступные действия задокументированы, если полученная информация содержат данные, которые поддаются проверке путем проведения следственных действий. С учетом того, что при работе по раскрытию мошенничеств с использованием ИКТ, основную часть доказательств формируют сведения кредитных организаций и операторов связи, в некоторых случаях целесообразно получение данной информации как оперативно-розыскным путем (в ходе документирования преступной деятельности), так и следственным (в процесс формирования массива сведений, образующих предмет доказывания).

Таким образом, получив сведения о наличии фактических данных, представляющих интерес для раскрытия мошенничества с использованием ИКТ, 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 и, 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 ИКТ, 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:

1) соблюдать законность;

2) объективность;

3) своевременность;

4) полнота документирования.

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

Объективность означает выявление обстоятельств как уличающих обвиняемого или отягчающих его вину, 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 того, чтобы тщательно проверять все сведения 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 оперативно-розыскных мероприятий следственных действий до возбуждения уголовного дела.

Своевременность документирования преступных действий мошенников заключается в том, чтобы действия оперативного работника в выявлении и сохранении данных, имеющих значение для расследования, опережали действия преступников, направленные на сокрытие или уничтожение этих данных. Поэтому 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 том, чтобы задокументировать преступные действия 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 тех данных и их источников, которая достаточна для признания выясненными обстоятельств, составляющих предмет документирования, которые будет трудно или невозможно установить следственным путем.

После выявления лиц, могущих быть свидетелями, необходимо осуществлять мероприятия по проверке их с тем, чтобы установить, что конкретно им известно о преступных действиях мошенников, в каких взаимоотношениях они находятся с ними 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 ИКТ. 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 ИКТ.

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

- предметы и документы, фиксирующие переговоры преступника 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, информация о 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:

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

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

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

Полученные в результате оперативно-розыскной деятельности 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 оперативно-розыскной деятельности – фактические данные, информация и сведения, полученные при проведении оперативно-розыскных мероприятий, предусмотренные ст. 6 Закона об ОРД 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 оперативно-розыскных мероприятий и составляемых в соответствии с ведомственными нормативными актами; в материалах фото-киносъемки, в звуко-, видеозаписях, произведенных в процессе оперативных мероприятий; в объяснениях лиц, участвовавших в их проведении; в

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: утв. приказом МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сент. 2013 г. № 776/703/509/507/1820/42/535/398/68 // Доступ из справ.-прав. системы «Гарант».

предметах, материалах и сообщениях, изъятых при осуществлении оперативно-розыскных мероприятий; в сообщениях конфиденциальных источников.

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

Результаты оперативно-розыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-розыскных мероприятий по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц и иных целей.

Результаты оперативно-розыскной деятельности могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится 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, и в иных случаях, установленных настоящим Федеральным законом при соблюдении требований ст. 89 УПК РФ.

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

Использование результатов оперативно-розыскной деятельности 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 оперативно-розыскной деятельности 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 оперативно-розыскных мероприятий 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, то 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, могущих быть свидетелями по делу, и не устанавливает каких-либо оснований для из вызова. Поэтому, 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 противоречит уголовно-процессуальным нормам, а значит, допустим.

Оперативно-розыскные данные, полученные в результате проведения оперативно-розыскных мероприятий, могут использоваться для проведения других оперативно-розыскных мероприятий. Фактические данные, на основе которых принимается решение о проведении оперативно-розыскных мероприятий, 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 пп. 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 оперативно-розыскной деятельности 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 ОТМ. Результаты ОРД могут быть зафиксированы также на материальных (физических) носителях информации. Представляемые материалы должна сопровождать информация о времени, месте и обстоятельствах изъятия в ходе оперативно-розыскной деятельности предметов и документов, получения 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 отвечает требованиям, установленным уголовно-процессуальным законодательством, и признаны таковыми следователем (вынесено соответствующее постановление).

Если на проведение оперативно-розыскного мероприятия было получено в установленном порядке разрешение суда, то результаты оперативно-розыскной деятельности представляются вместе с копией соответствующего судебного постановления.

Если оперативно-розыскное мероприятие осуществлялось на основании постановления руководителя органа или подразделения, осуществляющего оперативно-розыскную деятельность, то результаты оперативно-розыскной деятельности представляются вместе с оригиналом соответствующего постановления.

Если при проверке результатов оперативно-розыскной деятельности 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 оперативно-розыскных мероприятий, 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 оперативно-розыскную деятельность, с изложением прямых или обобщенных сведений, содержащихся в делах

оперативного учета (например, о принадлежности того или иного лица к организованной преступной группе). Однако их доказательственное значение практически ничтожно, поскольку часто не поддается проверке достоверности представленных сведений.

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

С учетом изложенного, процедура предоставления результатов оперативно-розыскной деятельности по мошенничествам, совершенным с использованием ИКТ, 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 ИКТ, 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 и ответов в соответствующие организации и учеты в печатном виде; 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) и 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 оперативно-розыскную деятельность, либо уполномоченным заместителем постановления 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 оперативно-розыскных мероприятий, 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 ИКТ, редко проводятся оперативно-розыскные мероприятия проверочная закупка, контролируемая поставка, оперативный эксперимент или оперативное внедрение, однако в случае их проведения и представлении следователю результатов ОРД, к ним прилагается постановление руководителя органа или подразделения, осуществляющего оперативно-розыскную деятельность, 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 указывается только вид мероприятия в соответствии с ФЗ «Об ОРД» 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 установлена обязанность оперативного подразделения, предоставляющего такие сведения, согласовывать их с исполнителями соответствующих мероприятий и осуществлять 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 оперативно-розыскную деятельность, либо уполномоченным заместителем постановления о предоставлении результатов оперативно-розыскной деятельности. Постановление составляется в двух экземплярах, один из которых подлежит хранению в органе, осуществляющим опера-

тивно-розыскную деятельность и приобщается к материалам дела оперативного учета или, в случае его отсутствия к материалам номенклатурного (литерного) дела. В постановлении указываются конкретные результаты оперативно-розыскной деятельности; длительность, место и вид проводимого оперативно-розыскного мероприятия; вид материального носителя, на котором они задокументированы.

7. Подготовка сообщения о результатах оперативно-розыскной деятельности или рапорта об обнаружении признаков состава преступления. В сообщении или рапорте так же, как и в постановлении о предоставлении результатов оперативно-розыскной деятельности, указываются конкретные результаты оперативно-розыскной деятельности; длительность, место и вид проводимого оперативно-розыскного мероприятия; 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 ИКТ

При поступлении заявления или сообщения о мошенничестве, совершенном с использованием ИКТ, 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 оперативно-розыскной деятельности для выявления, пресечения и раскрытия преступлений данной категории.

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

1) опрос потерпевшего;

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

3) участие в осмотре места происшествия;

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

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

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

7) фиксация на материальных носителях первоначальных данных об обстоятельствах преступления;

8) выдвижение версий.

Выполнение перечисленных действий не всегда зависит от сотрудников и может занимать значительный период времени. В частности, на сроки получения информации влияет, например, региональная специфика, в том числе следственно-судебная практика, наличие специальных каналов связи для получения информации в электронном виде, наличие договорных отношений между ОВД и кредитными организациями, местонахождение кредитной организации, оператора связи и соответствующего ОВД и множество иных факторов.

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

1) опрос;

2) наведение справок;

3) снятие информации с технических каналов связи;

4) получение компьютерной информации;

5) прослушивание телефонных переговоров;

6) получение образцов для сравнительного исследования;

7) других 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 ИКТ.

При опросе потерпевшего (примерный образец приведен в прил. 4) 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 по-

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

средством приложения для смартфона или личного кабинета абонента на сайте оператора связи, при этом детализация направляется на указанный абонентом адрес электронной почты. В детализации отражается точное время соединений и абонентские номера, использовавшиеся преступниками при совершении преступлений. Данная мера применяется в случаях, 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 Федерального агентства связи (Россвязь) www.rossvyaz.ru/activity/num_resurs/registerNum/, 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 запрашивается следующая информация у операторов связи:

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

б) 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;

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

г) 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.

При получении указанных сведений в ходе оперативно-розыскной деятельности, сотрудник в своих действиях руководствуется Федеральным Законом «О связи» от 07.07.2003 № 126-ФЗ и ФЗ «Об ОРД». Для получения информации необходимо получение разрешения суда в порядке, предусмотренном ст. 9 ФЗ «Об ОРД». 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 выхо-

да 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 в случае, 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. 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, подъез-

[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.

да 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 выявлений 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 информационных центрах на региональном уровне, так как централизация полной информации о мошенничествах, совершенных с использованием ИКТ, на федеральном уровне не осуществляется.

В ряде регионов (Красноярский край, Алтайский край, Иркутская область и др.) формируются иные формы учетов, позволяющие реализовывать вышеуказанные функции на региональном уровне. В перечисленных регионах территориальными подразделениями полиции информация о мошенничествах, совершенных с использованием ИКТ, 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, материалов проверки сообщений и заявлений о преступлениях, дел оперативного учета. При изучении таких материалов необходимо установить, какие следственные и процессуальные действия, оперативно-розыскные мероприятия проводились ранее, их результаты. С учетом первичной информации, полученной при опросе потерпевшего, при осмотре места происшествия и других мероприятий, совместно со следователем выдвигаются версии, планируются следственные и процессуальные действия, намечаются дальнейшие оперативно-розыскные мероприятия.

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

Также необходимо на первоначальном этапе запросить информацию в учреждениях, предприятиях, организациях, как-либо задействованных преступником или преступниками при совершении преступления. В первую очередь, оперативный интерес представляет информация от опера-

торов связи и кредитных организаций. В зависимости от обстоятельств преступления у операторов связи запрашиваются следующие сведения:

1. 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).

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

3. Адрес электронной почты, посредством которой осуществлялось создание аккаунта и иные привязанные к аккаунту адреса электронной почты.

4. 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 ИКТ, 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 которую 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.

Также в кредитных организациях 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». Такую практику нельзя признать в полной мере 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 которого 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 правоохрани-

тельных 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 получения 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, а также возможно установление региона или района местонахождения лица, осуществлявшего обналичивание похищенных денежных средств. Однако 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 к совершению 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 оперативно-розыскных мероприятий, в связи с чем необходимо разграничение действий оперуполномоченного и следователя по ее получению.

Из анализа федерального закона «О банках и банковской деятельности» от 02.12.1990 № 395-1 следует, что данным нормативным актом предусмотрены различные процедуры получения информации, составляющей банковскую тайну, для органов, осуществляющих оперативно-розыскную деятельность 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 оперативно-розыскную деятельность, при выполнении ими функций по выявлению, предупреждению и пресечению преступлений по их запросам, направляемым в суд в порядке, предусмотренном ФЗ об ОРД, при наличии сведений о признаках подготавливаемых, совершаемых или совершенных преступлений, а также о лицах, их подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела.

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 это возникает 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 нормативно-правовыми актами МВД России, регламентирующими оперативно-розыскную деятельность, 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 оперативно-розыскных мероприятиях от сотрудников операторов сотовой связи, имеющих отношение к обработке и выдаче ин-

формации о соединениях между абонентами и обеспечивается соблюдение требования конфиденциальности документирования.

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

Анализ практики раскрытия преступлений свидетельствует, что эффективное сочетание оперативно-розыскных мероприятий и следственных действий, качественное межрегиональное и межведомственное взаимодействие позволяет 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 ИКТ, выдвигаются следующие типичные версии.

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

2. Преступление совершено лицом, ранее судимым за совершение аналогичных преступлений, находящимся в регионе, в котором выявлено преступление.

3. Преступление совершено лицом, отбывающем наказание в исправительном учреждении ФСИН России.

4. Преступление совершено лицом, ранее не судимым, находящимся за пределами региона, в котором выявлено преступление.

5. 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 ИКТ.

Планирование в деятельности оперативных и следственных подразделений можно рассматривать как управленческую деятельность, состоящую в согласовании целей и задач на предстоящий период и выработку 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 ИКТ, следует отнести необходимость учета информации о лицах и фактах, неравномерно распределенной в различных базах данных и неструктурированных информационных массивах, а также участия в проведении оперативно-розыскных мероприятий и следственных действий сотрудников оперативных и иных подразделений ОВД различных районов и регионов. Также при планировании сле-

дует 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 этой связи представляется важным предварительное решение вопроса организации взаимодействия.

Обеспечение ведомственного и межведомственного взаимодействия.

Признаками взаимодействия применительно к оперативно-розыскной деятельности следует считать:

1) координацию проводимых совместных оперативно-розыскных мероприятий и следственных действий;

2) согласованность места и времени проведения;

3) правовую и нормативную регламентированность;

4) достижение единых целей и решение единых задач борьбы с преступностью.

В условиях, когда признаки противоправной деятельности преступников и преступных групп проявляются практически одновременно в разных регионах, скоординированные и единонаправленные действия различных оперативных и иных подразделений приобретают особое значение.

Достижение таких действий возможно путем координации усилий нижестоящих оперативных подразделений соответствующим подразделением на федеральном уровне, а также обеспечением равного доступа всех заинтересованных подразделений (участвующих в проведении конкретных ОРМ) к информации о месте и времени проведения мероприятий, точным и конкретным перечнем 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, целесообразно на каждом отдельном участке назначение руководителей проводимых мероприятий и организация закрытого канала связи, обеспечивающих 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 ИКТ, имеет приоритетное значение, относятся подразделения уголовного розыска, подразделения специальных технических мероприятий (оперативно-технические подразделения), оперативно-поисковые подразделения, подразделения оперативно-розыскной информации.

При взаимодействии подразделений уголовного розыска наибольшее практическое значение имеет обмен информацией о совершенных преступлениях данной категории, эффективное и рациональное распределение функций по осуществлению оперативно-розыскных мероприятий как на территории одного региона, так и на территориях, в которых зарегистрированы преступления, имеющие признаки серийности.

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

Лицами, совершающими мошенничества с использованием ИКТ, 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 ИКТ, дополняющее традиционные средства борьбы с преступностью. Особенно важным является 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 оперативно-розыскной информации (далее – ПОРИ) являются неотъемлемым дополнением системы информационного обеспечения деятельности по раскрытию мошенничеств, совершенных с использованием ИКТ, 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 организация и межведомственного взаимодействия.

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 ИКТ, относится организация взаимодействия с оперативными подразделениями Федеральной службы исполнения

наказаний (далее – 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 ИКТ, 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 ИКТ, применима действующая система контроля, при которой действия в пределах одного региона контролируются уполномоченным руководителем ОВД данного региона, а при проведении ОРМ в рамках одного ДОУ 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 ИКТ, – 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 ИКТ, является неотъемлемым условием для планирования и проведения оперативно-розыскных мероприятий, осуществления оперативно-розыскного обеспечения предварительного следствия.

ЗАКЛЮЧЕНИЕ

Быстрое развитие информационно-коммуникационных технологий 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 преступления, 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 ИКТ, 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 граждан как пострадавших в результате совершения преступлений, так и граждан, подозреваемых в их совершении.

Приложение 1

Образец сообщения о результатах оперативно-розыскной деятельности по мошенничеству, совершенному с использованием ИКТ

ГУ МВД России по Иркутской области

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ОБЛАСТИ
(ГУ МВД России по области)
ул. Иванова, д.77, г. 667777

16.06.2019г. № 10/77-7777
на №_____ от _____

Начальнику ГСУ ГУ МВД России по области

генерал-майору юстиции
И. И. Иванову

О результатах оперативно-розыскной деятельности

Уважаемый Иван Иванович!

В соответствии со статьей 11 федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» и приказом МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России. ФСКН России и Следственного комитета Российской Федерации от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд" для приобщения к материалам уголовного дела № 11901250037007777, направляем в Ваш адрес результаты оперативно-розыскного мероприятия прослушивание телефонных переговоров, проведенного по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019.

Приложения:

1. Постановление начальника полиции ГУ МВД России по области генерал-майора полиции П. П. Петрова, исх. № 10/77-7776 от 16.06.2019 о рассекречивании сведений, составляющих государственную тайну и их носителей на одном листе.

2. Постановление начальника полиции ГУ МВД России по области генерал-майора полиции П. П. Петрова исх. № 10/77-7775 от 16.06.2019 о предоставлении результатов оперативно-розыскной деятельности.

3. Постановление судьи Иркутского областного суда Сидорова С. С. № 141 от 16.06.2019 о рассекречивании постановления суда на одном листе.

4. Копия постановления судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 года о разрешении проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров на одном листе.

5. Оптический носитель № 12549786 информации с аудиозаписью телефонных переговоров состоявшихся в ходе проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019, упакованный в бумажный конверт, опечатанный печатью «Для справок № 77», заверенный подписью старшего оперуполномоченного по ОВД УУР ГУ МВД России по области майора полиции Федорова Ф. Ф. и снабженный пояснительной надписью «оптический носитель № 12549786 с аудиозаписью телефонных переговоров. состоявшихся по сотовому телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019».

6. Бумажный носитель записи телефонных переговоров по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019.

Заместитель начальника –
начальник полиции
генерал-майор полиции П. П. Петров

исп. Федоров
т. 77-77-77

Приложение 2

Образец постановления о рассекречивании сведений, составляющих государственную тайну, и их носителей

ПОСТАНОВЛЕНИЕ № 10/77-7776
о рассекречивании сведений, составляющих государственную тайну, и их носителей

г. Энск 16 июня 2019 года

Начальник полиции ГУ МВД России по области, генерал-майор полиции П. П. Петров, рассмотрев материалы оперативно-розыскного мероприятия, проведенного сотрудниками УУР МУ МВД России по Иркутской области,

УСТАНОВИЛ:

Сотрудниками УУР ГУ МВД России по области в отношении Кудрявцева Константина Константиновича 01.01.2019 г. рождения, урож. г. Энск, зарегистрированного по адресу г. Энск, ул. Иванова, д. 12, кв. 10, в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019 на основании постановления судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 г. о разрешении проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров проводилось оперативно-розыскное мероприятие, связанное с ограничением конституционных прав, а именно прослушивание телефонных переговоров, по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К. для совершения мошенничеств.

30.05.2019 г. судьей областного суда Сидоровым С. С. по результатам рассмотрения постановления заместителя начальника ГУ МВД России по Иркутской области начальника полиции генерал-майора полиции П. П. Петрова № 10/77-7770 от 30.05.2019 г. и в соответствии со ст. ст. 6–9 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в установленном законом порядке было вынесено постановление, разрешающее проведение оперативно-розыскного мероприятия, связанного с ограничением конституционных прав прослушивание телефонных переговоров, ведущимся по мобильному телефону с 1234567891012130, использовавшемся Кудрявцевым К. К. для совершения мошенничеств.

Результаты оперативно-розыскного мероприятия «прослушивание телефонных переговоров» по сотовому телефону с IMEI 1234567891012130 в виде оптического носителя информации № 12549786 находятся в УУР ГУ МВД России по области и могут быть рассекречены без нанесения ущерба интересам оперативно-розыскной деятельности органов внутренних дел.

Постановление судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 г. о разрешении проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К., находятся в УУР ГУ МВД России по области.

Принимая во внимание вышеизложенное, руководствуясь ст. ст. 5, 11, 12 федерального закона РФ от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», п. п. 8–12 «Инструкции о порядке предоставления результатов, оперативно-розыскной деятельности органу дознания, следователю или в суд»,

ПОСТАНОВИЛ:

1. Рассекретить постановление начальника полиции генерал-майора полиции П. П. Петрова № 10/77-7770 от 30.05.2019 г.

2. Рассекретить результаты оперативно-розыскной деятельности в части оперативно-розыскного мероприятия прослушивание телефонных переговоров проведенного по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К., зафиксированного на оптический носитель информации № 12549786 посредством аудиозаписи телефонных переговоров состоявшихся в ходе проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019.

3. Ходатайствовать перед областным судом о рассекречивании постановления судьи областного суда Сидорова С. С. № 130с от 30.05.2019 г., разрешающего проведение оперативно-розыскного мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К.

Заместитель начальника –
начальник полиции
генерал-майор полиции П. П. Петров

Приложение 3

Образец постановления о предоставлении результатов оперативно-розыскной деятельности

ПОСТАНОВЛЕНИЕ
о предоставлении результатов оперативно-розыскной деятельности

г. Энск 16 июня 2019 года

Начальник полиции ГУ МВД России по области, генерал-майор полиции П. П. Петров, рассмотрев материалы оперативно-розыскного мероприятия, проведенного сотрудниками УУР МУ МВД России по Иркутской области,

УСТАНОВИЛ:

Сотрудниками УУР ГУ МВД России по области в отношении Кудрявцева Константина Константиновича 01.01.2019 г. рождения, урож. г. Энск, зарегистрированного по адресу г. Энск, ул. Иванова, д. 12, кв. 10, в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019 на основании постановления судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 г. о разрешении проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров проводилось оперативно-розыскное мероприятие, связанное с ограничением конституционных прав, а именно прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К. для совершения мошенничеств.

30.05.2019 г. судьей областного суда Сидоровым С. С. по результатам рассмотрения постановления заместителя начальника ГУ МВД России по Иркутской области начальника полиции генерал-майора полиции П. П. Петрова № 10/77-7770 от 30.05.2019 года и в соответствии со ст. ст. 6–9 федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в установленном законом порядке было вынесено постановление, разрешающее проведение оперативно-розыскного мероприятия, связанного с ограничением конституционных прав прослушивание телефонных переговоров, ведущимся по мобильному телефону с 1234567891012130, использовавшемся Кудрявцевым К. К. для совершения мошенничеств.

Результаты оперативно-розыскного мероприятия «прослушивание телефонных переговоров» по сотовому телефону с IMEI 1234567891012130 в виде оптического носителя информации № 12549786 находятся в УУР ГУ МВД России по области и могут быть рассекречены без нанесения ущерба интересам оперативно-розыскной деятельности органов внутренних дел.

Постановление судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 г. о разрешении проведения оперативно-розыскного

мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130, использовавшемуся Кудрявцевым К. К., находятся в УУР ГУ МВД России по области.

Принимая во внимание вышеизложенное, руководствуясь ст. ст. 5, 11, 12 федерального закона РФ от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», п. п. 8–12 «Инструкции о порядке предоставления результатов, оперативно-розыскной деятельности органу дознания. следователю или в суд»,

ПОСТАНОВИЛ:

Направить в ГСУ ГУ МВД России по области для приобщения к уголовному делу № 11901250037007777 следующие результаты оперативно-розыскной деятельности:

1. Постановление начальника полиции ГУ МВД России по области генерал-майора полиции П. П. Петрова исх. № 10/77-7776 от 16.06.2019 о рассекречивании сведений, составляющих государственную тайну и их носителей на одном листе.

2. Постановление начальника полиции ГУ МВД России по области генерал-майора полиции П. П. Петрова исх. № 10/77-7775 от 16.06.2019 о предоставлении результатов оперативно-розыскной деятельности.

3. Постановление судьи Иркутского областного суда Сидорова С. С. № 141 от 16.06.2019 о рассекречивании постановления суда на одном листе.

4. Копия постановления судьи Иркутского областного суда Сидорова С. С. № 130с от 30.05.2019 года о разрешении проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров на одном листе.

5. Оптический носитель № 12549786 информации с аудиозаписью телефонных переговоров состоявшихся в ходе проведения оперативно-розыскного мероприятия прослушивание телефонных переговоров по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019, упакованный в бумажный конверт, опечатанный печатью «Для справок № 77», заверенный подписью старшего оперуполномоченного по ОВД УУР ГУ МВД России по области майора полиции Федорова Ф. Ф. и снабженный пояснительной надписью «оптический носитель № 12549786 с аудиозаписью телефонных переговоров, состоявшихся по сотовому телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019».

6. Бумажный носитель записи телефонных переговоров по мобильному телефону с IMEI 1234567891012130 в период с 12 ч. 00 мин. 01.06.2019 по 15 ч. 00 мин. 15.06.2019.

Заместитель начальника –
начальник полиции
генерал-майор полиции П. П. Петров

Приложение 4

Образец опроса по мошенничеству, совершенному с использованием ИКТ

ПРОТОКОЛ
опроса

г. Иркутск « 16 » ноября 2019 г.
(место составления)

Опрос начат в 10 ч 20 мин
Опрос окончен в 11 ч 05 мин

Старший оперуполномоченный отдела по раскрытию мошенничеств и дистанционных преступлений УУР ГУ МВД России по Иркутской области
(должность следователя (дознавателя),
капитан полиции И.А. Феоктистов
классный чин или звание, фамилия, инициалы)
в помещении «Ломбард» по адресу: г. Иркутск, ул. Петрова, 27
(каком именно)
в соответствии со ст. 144 УПК РФ опросил:

1. Фамилия, имя, отчество Иванов Иван Иванович
2. Дата рождения 21.03.1985
3. Место рождения г. Ленинград
4. Место жительства и (или) регистрации Зарег. г. Иркутск, ул. Петрова, 27-121
Проживает там же
телефон 89999999998
5. Гражданство Российская Федерация
6. Образование средне-специальное
7. Семейное положение, состав семьи Не женат, 1 несовершеннолетний ребенок
8. Место работы или учебы ИП Иванов И. И.
телефон
9. Отношение к воинской обязанности не в/о
(где состоит на воинском учете)
10. Наличие судимости не судим
(когда и каким судом был_ осужден, по какой статье УК РФ, вид и размер
наказания, когда освободился)
11. Паспорт или иной документ, удостоверяющий личность потерпевшего
Иванов И. И.
(подпись)
12. Иные данные о личности не имеются

Иные участвующие лица не участвуют
(процессуальное положение,
фамилии, имена, отчества, в необходимых случаях - адреса)

Лица, участвующие в следственном действии, были заранее предупреждены о применении при опросе технических средств компьютер, принтер
(каких именно)

Мне разъяснены права и обязанности, предусмотренные УПК РФ в той части, в которой производимые процессуальные действия и принимаемые процессуальные решения затрагивают мои интересы, в том числе права не свидетельствовать против самого себя, своего супруга (своей супруги) и других близких родственников, круг которых определен пунктом 4 статьи 5 УПК РФ, пользоваться услугами адвоката, а также приносить жалобы на действия (бездействие) и решения дознавателя, начальника подразделения дознания, начальника органа дознания, органа дознания, следователя, руководителя следственного органа в порядке, установленном главой 16 УПК РФ. Разъяснено, что я могу быть предупрежден о неразглашении данных досудебного производства в порядке, установленном статьей 161 УПК РФ. Разъяснена возможность обеспечения безопасности участника досудебного производства в порядке, установленном частью девятой статьи 166 УПК РФ, в том числе при приеме сообщения о преступлении.

Иванов И. И.

_____
(подпись)

По существу могу показать следующее: по вышеуказанному адресу я проживаю один.

Около 5 лет назад я зарегистрировался в качестве индивидуального предпринимателя. У меня имеется скупка ювелирных изделий «Lombard», расположенная по адресу: г. Иркутск, ул. Петрова, 27 На сайтах «Авито», «Юла» у меня размещены объявления о продаже и скупке ювелирных изделий, где указан мой абонентский номер 89999999998, которым пользуюсь более 1 года.

Примерно в конце марта, 28 или 29 марта, точно не помню, мне на мой абонентский номер 89999999998 поступил звонок с ранее незнакомого мне номера 89999999999. Со мной разговаривал парень по голосу около 25–30 лет, речь без дефектов, без акцента. Представлялся ли данный парень, я не помню. Парень спросил у меня, принимаем ли мы ювелирные изделия, я ответил, что да. Также он спросил, возможна ли оплата безналичным способом с карты на банковскую карту, я ответил, что возможно. Парень сказал, что подойдет его знакомый, который принесет ювелирное изделие, и деньги нужно будет перевести на карту. Я ответил, что пускай приходят, посмотрим изделие и дальше определимся.

В результате 30.03.2019 в скупку по адресу: г. Иркутск, ул. Петрова, 27 пришел мужчина, как я позже узнал, его фамилия Сидоров. Сидоров принес золотое кольцо с бриллиантом и сказал, что желает его продать в скупку. В этот момент мне также звонил парень с номера 89999999999 и спрашивал, пришел ли его друг с кольцом, то есть речь шла про Сидорова. Также этот парень постоянно говорил, что оплату нужно произвести обязательно безналичным способом, на карту которую сообщит Сидоров. Я посмотрел кольцо, которое принес Сидоров и оценил его в 150 000 рублей, о чем сообщил Сидорову. Сидоров сказал, что цена устраивает и что оплату нужно произвести на банковскую карту. Также я понял, что парень, который звонил мне с номера 89999999999 также общался с Сидоровым, когда тот был в скупке. Затем Сидоров дал мне свой телефон и па-

рень продиктовал мне номер карты (№ 1234567891011121), на которую необходимо перевести деньги.

Так как у меня не было карты ПАО «Сбербанк», то я обратился к своей сотруднице Ивановой Марии Ивановне, которая работает в должности приемщика-оценщика ювелирных изделий. По моей просьбе Иванова М. И. перевела со своей банковской карты ПАО «Сбербанк» 150 000 рублей на карту ПАО «Сбербанк» № 1234567891011121 на имя «Ирины Николаевны П.». После перевода денег я хотел забрать кольцо у Сидорова, но он отказался его отдавать, поясняя, что ему на его карту не поступили деньги. В результате мы стали разбираться в данной ситуации. От Сидорова я узнал, что ему звонил парень с номера 89999999999, который говорил, что он проверяет сеть ломбардов и готов купить ювелирное изделие за стоимость, указанную в объявлении, но только с условием оплаты безналичным способом. Сидоров пояснил, что у него размещено объявление о продаже данного кольца, где указана стоимость 1 000 000 рублей. Также Сидоров пояснил, что парень сказал, что сначала нужно зафиксировать перевод на его карту в меньшей сумме, так как у него не сходится суммы по финансовому отчету, а после этого он (парень) уже переведет деньги ему (Сидорову) в полной сумме. Также парень просил Сидорова не называть настоящую стоимость ювелирного изделия в скупке, так как якобы он проверял сотрудников ломбарда. Таким образом, данный парень обманул меня и Сидорова, в результате чего я перевел на неизвестную карту 150 000 рублей.

В результате данного преступления мне причинен ущерб на сумму 150 000 рублей, данный ущерб причинен мне как индивидуальному предпринимателю, так как для оплаты изделия я использовал денежные средства из своей предпринимательской деятельности.

С номера 89999999999 мне звонил один и тот же парень, так как голос был всегда один и тот же. Голос парня возможно узнаю.

Ранее не обращался в полицию, так как думал, что лицо, совершившее данное преступление установить невозможно.

Иванов И. И. _____

(подпись)

Приложение 5

Образец направления запроса (проведения ОРМ наведение справок) по мошенничеству, совершенному с использованием ИКТ

ГУ МВД России по Иркутской области

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ОБЛАСТИ
(ГУ МВД России по области)
ул. Иванова, д.77, г. 667777

Председателю правления
АО "Киви банк"
Салонину С.А.

117648, г. Москва,
мкр. Чертаново Северное,
д. 1А, корп. 1

__16.11.2019 г._ № _10/77-7778_____
на №_____ от _____

На основании ч. 5 ст. 26 ФЗ №395-1 от 02.12.1990 г. «О банках и банковской деятельности», п. 2 ст. 6 и ст. ст. 7–9 ФЗ №144-ФЗ от 12.08.1995 г. «Об оперативно-розыскной деятельности» и постановлении судьи Иркутского областного суда № 123 от 09.11.2019 г., прошу предоставить в наш адрес справку по банковской карте № 1234 5678 9101 1121, открытой в ЗАО «Киви Банк», в период времени с момента её открытия и по 05.11.2019 года, содержащую следующие сведения:

1. ФИО владельца, дата открытия счета, телефонный номер, указанный при составлении договора, другие телефонные номера.

2. Движение денежных средств по счету в период времени с момента открытия и по настоящее время с указанием точных сумм, времени и источников поступления и расходования денежных средств (полные данные вносителя платежа).

3. Места снятия денежных средств, с указанием номеров банкоматов и адресов их расположения.

4. IP-адреса, с которых производилась регистрация личного кабинета и дальнейшее его администрирование.

5. Абонентские номера, привязанные к вышеуказанной карты с момента её открытия и по настоящее время.

Приложение: постановление судьи Иркутского областного суда.

Ответ прошу Вас направить электронной почтой iivanov222@mvd.ru и продублировать почтой.

Начальник П. П. Петров

исп. И. И. Иванов,
тел 8 (3952) 00-00-00

Приложение 6

Образец направления запроса (проведения ОРМ наведение справок) по мошенничеству, совершенному с использованием ИКТ

ГУ МВД России по Иркутской области

ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ОБЛАСТИ
(ГУ МВД России по области)
ул. Иванова, д.77, г. 667777

Генеральному директору
ООО "Контел"
О. В. Плахотнюку

117246, г. Москва, пр-д Научный,
дом 20, стр. 2

__16.11.2019 г._ № _10/77-7779_____
на №_____ от _____

В связи с проведением оперативно-розыскных мероприятий по уголовному делу № 1190000000000000, возбужденному 15.11.2019 по признакам состава преступления, предусмотренного ч. 2 ст. 159 УК РФ, на основании п. 2 ст. 6 и ст. ст. 7–9 ФЗ №144-ФЗ от 12.08.1995 г. «Об оперативно-розыскной деятельности» и п. 4 ст. 13 ФЗ от 07.02.2011 № 3 «О полиции» прошу Вас поручить подчиненным сотрудникам предоставить информацию по IP-адресу 11.1.211.111 с указанием имеющихся сведений о его пользователе, способе оплаты услуг и физическом адресе абонента в указанное время.

14.11.2019 17.53.30	14.11.2019 19.23.20
14.11.2019 18.54.34	14.11.2019 19.52.40
14.11.2019 19.13.50	14.11.2019 20.33.15

Ответ прошу Вас направить электронной почтой iivanov222@mvd.ru и продублировать почтой.

Начальник П. П. Петров

исп. И. И. Иванов
тел 8 (3952) 00-00-00

Приложение 7

Сводные статистические сведения о состоянии преступности, связанной с совершением мошенничеств с использованием ИКТ, за 2015–2019 годы

	2015	2016	2017	2018	январь-март 2019
Зарегистрировано мошенничеств	174267	188246	202622	215036	62257
раскрыто	17483	17846	19278	56318	16926
установлено лиц	23994	23277	22924	37018	10150
Мошенничества, совершенные с использованием сети Интернет	нет данных	31190	50119	56321	16105
раскрыто		1201	2056	5120	1361
установлено лиц		н/д	н/д	4863	1327
Мошенничества с использованием средств мобильной связи	21562	31236	44081	42712	12779
раскрыто	1541	2381	3016	4190	997
установлено лиц	275	542	917	4063	991
Мошенничество сов. с исп. средств моб. связи осужденным лицом, содержащимся в учр. ФСИН	42	183	294	225	13
раскрыто	70	261	390	491	70
установлено лиц	14	37	73	491	70

Приложение 8

Сводные статистические сведения о регионах с наибольшим количеством зарегистрированных мошенничеств, совершенных с использованием сети Интернет за январь–март 2019 г.

Регион	зарегистрировано	раскрыто	установлено лиц	не раскрыто
г. Москва	1401	292	291	879
Тюменская область	743	38	37	586
Респ. Татарстан	716	50	50	591
Краснодарский край	523	16	15	382
Красноярский край	448	23	23	383
Ростовская область	438	14	14	252
Пермский край	421	27	25	364
Самарская область	416	12	11	367
Кемеровская область	377	21	20	307
Новосибирская область	365	36	35	178

Приложение 9

Сводные статистические сведения о регионах с наибольшим количеством зарегистрированных мошенничеств, совершенных с использованием средств мобильной связи за январь–март 2019 г.

Регион	зарегистрировано	раскрыто	установлено лиц	не раскрыто
Краснодарский край	1125	65	64	765
г. Москва	849	111	111	747
Респ. Татарстан	503	40	40	359
Красноярский край	479	7	7	329
Алтайский край	433	44	43	261
Ростовская область	430	15	15	231
Тюменская область	411	29	29	321
Самарская область	336	63	63	246
Ставропольский край	323	48	48	269
Вологодская область	302	26	26	194

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Об оперативно-розыскной деятельности: федеральный закон Российской Федерации от 12 авг. 1995 г. № 144-ФЗ; ред. от 20 июля 2016 г. // СЗ РФ. – 1995. – № 33. – Ст. 3349.

2. Уголовно-процессуальный кодекс Российской Федерации: федеральный закон Российской Федерации от 18 дек. 2001 г. № 174-ФЗ; ред. от 12 апр. 2019 г. // Там же. – 2001. – № 52 (ч. I). – Ст. 4921.

3. О полиции: федеральный закон Российской Федерации от 7 февр. 2011 г. № 3-ФЗ; ред. от 06 июня 2019 г. // Там же. – 2011. – № 7. – Ст. 900.

4. О связи: федеральный закон от 7 июля 2003 г. № 126-ФЗ; ред. от 06 июня 2019 г. // Там же. – 2003. – № 28. – Ст. 2895.

5. О банках и банковской деятельности: федеральный закон от 2 дек. 1990 г. № 395-I; ред. от 18 июня 2019 г. // 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 Министерства внутренних дел Российской Федерации от 29 авг. 2014 г. № 736 // доступ из справ.-прав. 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 Генеральной прокуратуры Российской Федерации, Министерства внутренних дел Российской Федерации, Федеральной службы безопасности Российской Федерации, Следственного комитета Российской Федерации, Федеральной службы Российской Федерации по контролю за оборотом наркотиков, Федеральной таможенной службы, Федеральной службы исполнения наказаний, Министерства обороны Российской Федерации, Федеральной службы судебных приставов, Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий от 26 марта 2014 г. № 147/209/187/23/119/596/149/196/110/154 // Там же.

8. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сент. 2013 г. № 776/703/509/507/1820/42/535/398/68 // Там же.

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 // Там же.

10. Об утверждении Требований к сетям электросвязи для проведения оперативно-розыскных мероприятий. Ч. I: Общие требования: приказ Мин-ва информационных технологий и связи Российской Федерации от 16 янв. 2008 г. № 6 // Там же.

11. Об утверждении общих технических требований к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на сетях (службах) документальной электросвязи: приказ Госкомсвязи РФ от 27 марта 1999 № 47 // Там же.

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). – С. 88–93.

2. Акчурин А.В., Шаутаева Г.Х. О некоторых обстоятельствах совершения мошенничества осужденными, отбывающими наказание в исправительных колониях // Там же. – 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 // Там же. – 2015. – Вып. 4 .– С. 49–55.

8. Закурдаев А.Н. Основные способы мошенничеств совершенных с использованием мобильных средств связи // Там же. – 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. 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. научн. трудов / под ред. Ю.В. Денисенко. – Барнаул: Барнаульский юридический институт МВД России, 2016. – Вып. 13. – С. 99–107.

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

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

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

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

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

16. 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.

Учебное издание

Кузьмин Иван Алексеевич

РАСКРЫТИЕ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Подписано в печать 24.02.2021 Формат 60х84.16
Усл. печ. л. 5,0 Тираж 100 экз. Заказ № 9

Восточно-Сибирский институт МВД России, ул. Лермонтова, 110