

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»
(КЮИ МВД РОССИИ)

Кафедра оперативно-разыскной деятельности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему

Организация оперативно-розыскной деятельности органов внутренних дел
по выявлению и документированию мошенничеств
общеуголовной направленности

Выполнил:

Желудкова Елена Эдуардовна
слушатель 042 учебной группы факультета
подготовки специалистов по программам
высшего образования КЮИ МВД России
(Правоохранительная деятельность, 2014 год),
младший лейтенант полиции

Руководитель:

Начальник кафедры оперативно-разыскной
деятельности КЮИ МВД России
полковник полиции
Шляхтин Евгений Павлович

Рецензент:

(должность, специальное звание)

(фамилия, имя, отчество)

К защите _____

(допущена, дата)

Начальник кафедры

_____ Е.П. Шляхтин

Дата защиты: «___» _____ 2019 г.

Оценка _____

Казань 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
Глава 1. ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ ОБЩЕУГОЛОВНОЙ НАПРАВЛЕННОСТИ:	7
§1. Уголовно-правовая характеристика мошенничеств общеуголовной направленности.	7
§2. Оперативная обстановка и способы совершения мошенничеств общеуголовной направленности	17
§3. Особенности личности мошенника и способов совершения преступлений	33
Глава 2. ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЕ МОШЕННИЧЕСТВ ОБЩЕУГОЛОВНОЙ НАПРАВЛЕННОСТИ	41
§1. Основные положения выявления мошенничеств общеуголовной направленности	41
§2. Документирование мошенничеств общеуголовной направленности на первоначальном этапе раскрытия	50
§3. Документирование мошенничеств общеуголовной направленности на последующем этапе раскрытия	71
ЗАКЛЮЧЕНИЕ	85
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ	90
I. Законы, нормативные правовые акты и иные официальные документы .	90
II. Монографии, учебники, учебные пособия	93
III. Статьи, научные публикации.....	95

ВВЕДЕНИЕ

На протяжении всей истории человечество сопровождает мошенничество. Издавна оно имело различные виды. Вместе с развитием общества и научно техническим прогрессом, охватывающим множество сфер человеческой жизнедеятельности, мошенничество также приобретает различные формы и способы совершения.

В нашей стране предусмотрена уголовная ответственность за мошенничества общеуголовной направленности. Под подобными преступлениями в Уголовном кодексе РФ понимаются хищения чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием¹, а также в сферах кредитования, страхования, компьютерной информации, с использованием платежных карт и при получении выплат, предусмотренные соответствующими статьями Особенной части Уголовного кодекса Российской Федерации.

Анализ соответствующей оперативно-розыскной и следственно-судебной практики свидетельствует, что лица, совершающие вышеуказанные преступления, прекрасно осведомлены о возможных последствиях своей противоправной деятельности, и, как правило, желают их скорейшего наступления. Все вышеуказанное требует комплексного подхода к решению указанных проблем, в том числе с применением оперативно-розыскных сил, средств и методов и обуславливает необходимость исследования вопросов, связанных с совершенствованием организации и тактики оперативно-розыскной деятельности в этом направлении.

В последнее время вопросам противодействия мошенничествам общеуголовной направленности, в том числе и с помощью оперативно-розыскной деятельности² территориальных и иных органов МВД России³,

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : в ред. от 12.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 19.12.2018).

² Далее – ОРД.

уделяется определенное внимание. Различные аспекты оперативно-розыскных проблем борьбы с преступлениями, в том числе связанными с мошенничествами общеуголовной направленности, освещались в работах Ю. М. Антоняна, В. М. Аتماжитова, Э. И. Бордиловского, В. В. Волченкова, С. С. Галахова, К. К. Горяинова, В. Г. Гриба, А. И. Гурова, Ю. Н. Демидова, Р. А. Журавлева и др. Однако в них частично рассматривались оперативно-розыскные аспекты проблем раскрытия вышеуказанных мошенничеств общеуголовной направленности (ст.ст. 159 – 159.6 УК РФ). В то же время, в данных работах не рассматривалась специфика совершения и, соответственно, выявления и документирования таких преступлений.

Отдельные аспекты противодействия мошенничествам общеуголовной направленности становились предметом исследований А. И. Долговой, В. С. Овчинского, В. П. Ревина и др.

Уголовно-правовые, криминологические, оперативно-розыскные и иные аспекты мошенничеств общеуголовной направленности стали предметом ряда диссертационных исследований А. А. Южина (2016), Р. С. Атаманова (2012), Н. В. Олинбера (2017), В. В. Коломинова (2017) и др.

В то же время проблема выявления и документирования с помощью оперативно-розыскной деятельности мошенничеств общеуголовной направленности должным образом не исследовалась, в связи с чем по этому направлению деятельности органов внутренних дел отсутствует необходимое количество методических материалов, чем и обусловлен выбор темы и актуальность выпускной квалификационной работы.

Цель и основные задачи исследования. Целью выпускного квалификационного исследования является разработка комплексных научно обоснованных предложений и рекомендаций по совершенствованию организационных и тактических основ ОРД ОВД по выявлению и документированию преступлений, связанных с мошенничествами общеуголовной направленности. В соответствии с поставленной целью

³ Далее – орган(ы) внутренних дел и (или) ОВД.

определен круг взаимосвязанных **задач**, теоретическое решение которых составляет содержание настоящей выпускной квалификационной работы.

К ним относятся:

- 1) изучение оперативно-розыскной характеристики мошенничеств общеуголовной направленности;
- 2) рассмотреть организацию информационного обеспечения оперативно-розыскной деятельности оперативных подразделений полиции по противодействию мошенничествам общеуголовной направленности;
- 3) дать характеристику оперативно-розыскного и иного документирования противоправных фактов, связанных с мошенничествами общеуголовной направленности;
- 4) исследование практики выявления замышляемых и подготавливаемых мошенничеств общеуголовной направленности;
- 5) выработка теоретико-прикладного подхода по повышению эффективности тактики проведения оперативно-розыскных мероприятий по установлению лиц, причастных к мошенничествам общеуголовной направленности.

Объект и предмет исследования. Объектом исследования является оперативно-розыскная деятельность органов внутренних дел по выявлению и раскрытию преступлений, связанных с мошенничествами общеуголовной направленности. Предмет исследования составляют тенденции и особенности вышеуказанных мошенничеств общеуголовной направленности, их характеристика, организационные и тактические аспекты деятельности оперативных подразделений ОВД по выявлению и документированию рассматриваемых преступлений.

Методология и методика исследования. Методологической основой выпускного квалификационного исследования является диалектический метод познания явлений и процессов реальной действительности, рассматривающий их в постоянном изменении, развитии, тесной взаимосвязи и взаимозависимости. В процессе исследования предполагается использовать

совокупность таких общенаучных методов исследования, как сравнение, анализ, синтез, а также формально-логический, сравнительно-правовой и другие частнонаучные методы, включая:

- статистический (при анализе данных о распространенности рассматриваемых деяний);
- конкретно-социологических исследований (при изучении уголовных дел, дел оперативного и иного учета, материалов первоначальной оперативной проверки и др.);
- контент-анализа (при изучении специальной литературы, законодательства и аналитических материалов).

В качестве нормативной базы будет использоваться Конституция Российской Федерации, действующее уголовное, уголовно-процессуальное, оперативно-розыскное законодательство, указы Президента РФ, постановления Правительства Российской Федерации, а также ведомственные нормативные правовые акты МВД Российской Федерации.

Теоретической основой исследования станут труды ученых в области теории оперативно-розыскной деятельности, криминалистики, уголовного, уголовно-процессуального права и других отраслей наук.

Эмпирическую базу исследования составят статистические данные МВД РФ, аналитические материалы Главного управления уголовного розыска⁴ МВД России, МВД по республикам, Главных управлений (Управлений)⁵ МВД России по иным субъектам Российской Федерации, результаты экспертных исследований, технические ориентировки, решения коллегий, указания, рекомендации МВД РФ, материалы научно-практических конференций, относящиеся к теме исследования и др.

По структуре выпускная квалификационная работа состоит из введения, двух глав, заключения и списка литературы.

⁴ Далее – ГУУР.

⁵ Далее – ГУ (У).

Глава 1. ОПЕРАТИВНО-РОЗЫСКНАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ ОБЩЕУГОЛОВНОЙ НАПРАВЛЕННОСТИ:

§1. Уголовно-правовая характеристика мошенничеств общеуголовной направленности.

Преступность против отношений собственности в повседневной жизни сопровождает нас во всех сферах человеческой жизнедеятельности. Данная группа преступлений одна из наиболее опасных, характеризуясь высоким числом совершенных преступлений. Среди корыстных преступлений наиболее разнообразным по способам и видам совершения является мошенничество. В статье 159 Уголовного кодекса РФ⁶ дается законодательное определение мошенничества: - «Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

По мнению В.М. Лебедева, мошенничество - это «форма хищения, для которой характерны все основные признаки хищения»⁷. Н.А. Лопашенко определяет мошенничество как «хищение в форме мошенничества в отношении чужого имущества или права на чужое имущество, совершенное путем обмана или злоупотребления доверием»⁸. А.Г. Безверхов трактует мошенничество как: «склонение путем обмана к передаче имущества, уступке имущественного права или к совершению иного действия (бездействия) имущественного характера, если это деяние совершено в значительном размере» и «получение имущественной выгоды в значительном размере»⁹. А.В. Анистратенко приходит к выводу, что в

⁶ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : в ред. от 12.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 19.12.2018). Далее – УК РФ.

⁷ Комментарий к Уголовному кодексу Российской Федерации /отв. ред. В.М. Лебедев. - 13-е изд., перераб. и доп. - М.: Юрайт, - 2015. –С. 278.

⁸ Анистратенко, А. В. Понятие мошенничества как формы хищения / А.В. Анистратенко // Вестник ВУиТ. - 2010. - №74. - С.57-65.

⁹ Анистратенко, А. В. Указ. соч. - С.57-65.

научной литературе нет единого мнения по поводу природы мошенничества. Одни ученые (В.М. Лебедев, Н.А. Лопашенко) традиционно относят мошенничество к одному из видов хищения чужого имущества, другие же, среди которых упомянутый выше А.Г. Безверхов, не считают мошенничество особой формой хищения, т.к. «термин «склонение» говорит о «мнимой» добровольности к передаче имущества и прав на имущество»¹⁰. Если исходить из законодательного определения мошенничества как формы хищения чужого имущества, представляется возможным выделить такие признаки мошенничества, как: 1) безвозмездность и противоправность изъятия; 2) осуществление изъятия с корыстной целью; 3) причинение вреда собственнику или законному владельцу похищенного имущества.

Российское уголовное законодательство в Особенной части УК РФ выделяет «специальные виды мошенничества». Так, например, в УК РФ в статье 159.1. «Мошенничество в сфере кредитования», в статье 159.2. «Мошенничество при получении выплат», в статье 159.3. «Мошенничество с использованием платежных карт», в статье 159.5. «Мошенничество в сфере страхования», в статье 159.6. «Мошенничество в сфере компьютерной информации». При квалификации данных действий следует руководствоваться разъяснениями, содержащимися в постановлениях пленумов Верховного Суда Российской Федерации от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое»¹¹ и от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»¹², а также некоторых других.

Действия виновных лиц квалифицируются по статье 159 УК РФ, если они были связаны с введением владельца денежных средств или иного

¹⁰ Анистратенко А.В. Понятие мошенничества как формы хищения // Вестник ВУиТ. - 2010. - №74. - С.57-65. **Указываете Безверхова?**

¹¹ О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда РФ от 27.12.2002 № 29 : в ред. от 16.05.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 07.04.2019).

¹² О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 07.04.2019).

имущества в заблуждение или с использованием доверительных отношений с ним, в результате чего тот передал денежные средства или иное имущество (право на имущество) – осуществил отчуждение имеющихся у него безналичных денежных средств путем перевода на указанный расчетный счет (банковскую карту, электронный кошелек, номер мобильного телефона и пр.). Примером совершения такого мошенничества является введение в заблуждение лица или использование доверительных отношений с ним в ходе телефонного разговора (в том числе – рассылка сообщений на мобильные средства связи, электронных писем и пр.), путем сообщения заведомо ложной, недостоверной информации, основываясь на которой заявитель действует в интересах виновного.

Под различными вымышленными предложениями достаточно часто сообщается информация о необходимости разблокирования банковской карты, для чего необходимо совершить ряд действий с мобильным средством связи; о предоставленной компенсации за ранее приобретенные медицинские препараты; о перечислениях от Пенсионного фонда, для чего необходимо сообщить реквизиты банковской карты; о необходимости перевода денежных средств за решение возникших проблем у родственника, который попал в ДТП, совершил преступление; электронное письмо (сообщение) о взломе (блокировке) страницы в социальной сети, для разблокировки которой необходимо перевести определенную сумму денег и пр.

Анализ положений статьи 159.1 УК «Мошенничество в сфере кредитования» показывает, что совершение данного вида мошенничества возможно только в области кредитных отношений как особой группы экономических отношений, в основе которых лежит движение стоимости. При этом сущность кредита заключается в экономических отношениях между заемщиком (получателем денег в долг) и кредитором, и предусматривающие возврат стоимости в денежной или товарной форме. Объектом кредитных отношений выступает ссуженная стоимость, которую кредитор передает заемщику на время. Основу кредита составляет

оговоренное договором разрешение одному лицу пользоваться деньгами другого лица. Кредитные отношения выражаются в различных формах: коммерческий кредит, ипотечный кредит, потребительский кредит, автокредит, банковский кредит, государственный кредит, заем, лизинг, ломбард и т.д. Исходя из формы ссуженной стоимости выделяют также денежный, товарный и смешанный кредиты.

В свою очередь, анализ положений статьи 159.2 УК «Мошенничество при получении выплат» показывает, что совершение данного вида мошенничества возможно только в сфере получения определенных выплат, к которым относятся пособия, компенсации, субсидии и иные социальные выплаты, установленные законами и другими нормативными правовыми актами.

Действия лица следует квалифицировать по статье 159.3 УК РФ в случаях, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты на законных основаниях либо путем умолчания о незаконном владении им платежной картой.

Хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной или поддельной кредитной либо расчетной карты, следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя). Аналогичным образом должно квалифицироваться и использование похищенной либо поддельной платежной карты для оплаты товаров или услуг, даже если от виновного лица

не потребовалось вводить ПИН-код карты¹³, предъявлять паспорт или расписываться вместо законного владельца карты.

Анализ положений статьи 159.5 УК «Мошенничество в сфере страхования» показывает, что совершение данного вида мошенничества возможно только в области страховых отношений как особого вида экономических отношений, включающих различные виды страховой деятельности (первичное страхование, перестрахование и др.). Страхование – отношения между страхователем и страховщиком по защите имущественных интересов физических и юридических лиц (страхователей) при наступлении определенных событий (страховых случаев) за счет страховых фондов, которые формируются из уплачиваемых страхователями страховых взносов. Страховщиком и страхователем определяется, каким образом будет формироваться страховой фонд и как он будет расходоваться.

Согласно п. 21 постановления пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»: - «В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного

¹³ ПИН-код - (англ. PIN - personal identification number) – персональный идентификационный номер, являющийся секретным кодом карты, при этом на ней он не хранится. Его длина варьирует от 4 до 12 цифр, на практике чаще всего встречается из 4. ПИН-код может состоять также из букв. Он вводится с помощью специального криптографического модуля, входящего в состав терминального устройства (банкомата, POS-терминала и т. п.) и передается в адрес эмитента, где он проверяется. Знание ПИН-кода, известного только держателю карты, по которой производится транзакция, является основанием считать, что лицо, совершающее операцию, и держатель карты являются одним лицом.

воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети»¹⁴.

В случае, когда неправомерное завладение чужим имуществом (денежными средствами) или приобретение права на имущество осуществлялись без ведома и помимо воли законного владельца путем неправомерного вмешательства в функционирование компьютерных устройств или информационно-телекоммуникационных сетей, путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, такие действия необходимо квалифицировать по статье 159.6 УК РФ.

Под неправомерным вмешательством необходимо понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него.

Типичным примером мошенничества в сфере компьютерной информации (статья 159.6 УК РФ) является получение путем обмана или иным незаконным способом, в частности с помощью распространения по сети Интернет вредоносных компьютерных программ, кодов доступа к банковским счетам и последующий перевод находящихся на этих счетах денежных средств. Некоторые действия по незаконному переводу денежных средств посредством воздействия на компьютерную информацию,

¹⁴ О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 07.04.2019).

совершаемые без ведома и помимо воли потерпевшего, в правоприменительной практике органов дознания и предварительного следствия нередко квалифицируются как кража по статье 158 УК РФ. Однако судами подобные действия квалифицируются в основном как мошенничество в сфере компьютерной информации, и действия виновных нередко переквалифицируются на статью 159.6 УК РФ, что следует признать правильным. К данному виду мошенничеств можно отнести распространение вредоносного программного обеспечения, которое блокирует компьютер или делает его использование невозможным (экран или часть экрана закрыта заставкой, либо хаотичнодвигающаяся по экрану заставка, мешающая просмотру информации на экране монитора, на весь экран изображено требование отправить СМС-сообщение на короткий номер для разблокирования компьютера); сообщение в виде электронного письма с вложенной (прикрепленной к электронному письму) ссылкой, переход по которой перенаправляет пользователя на определенный Интернет-ресурс (страницу), на которой имеется предложение заведомо несуществующей услуги или методики (генератора электронных денег, пополнения так называемых кошельков с электронными деньгами, ставки на спорт) и пр.

Вышеописанные действия квалифицируются по статьям 159, 159.3 и 159.6 УК РФ, если общая стоимость похищенного имущества выше, чем размер мелкого хищения. В соответствии со статьей 7.27 Кодекса Российской Федерации об административных правонарушениях¹⁵ размер мелкого хищения составляет в настоящее время не более 2500 рублей. В соответствии с примечанием 2 к статье 158 УК РФ значительный ущерб гражданину в статьях УК РФ, предусматривающих ответственность за преступления против собственности, за исключением части 5 статьи 159 УК РФ, определяется с учетом его имущественного положения, но не может составлять менее пяти тысяч рублей.

¹⁵ Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ : в ред. от 18.03.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019). Далее – КоАП РФ.

Анализируя диспозицию статьи ст. 159 УК РФ, можно прийти к выводу, что предметом мошенничества являются: 1) имущество; 2) право на имущество. К имуществу, согласно ст. 130 Гражданского кодекса РФ¹⁶, относят недвижимые («земельные участки, участки недр и все, что прочно связано с землей, то есть объекты, перемещение которых без несоразмерного ущерба их назначению невозможно, в том числе здания, сооружения, объекты незавершенного строительства, а также подлежащие государственной регистрации воздушные и морские суда, суда внутреннего плавания») и движимые («вещи, не относящиеся к недвижимости, включая деньги и ценные бумаги»).

В науке существует следующая классификация мошенничества. Так, мошенничество делится на общеуголовное и экономическое. Далее в нашей выпускной квалификационной работе речь пойдет об общеуголовных мошенничествах, поэтому возникает необходимость их разграничения.

Общеуголовные мошенничества – категория преступлений, связанная с хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием, рассмотрение которой подлежит компетенции оперативных подразделений уголовного розыска¹⁷.

В совместном указании Генеральной прокуратуры России № 853/11, МВД России № 5 от 25.12.2018 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности»¹⁸ определены статьи УК РФ,

¹⁶ Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ : в ред. от 03.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019). Далее – ГК РФ.

¹⁷ Перечень оперативных подразделений полиции определен в приказе МВД России от 19.06.2012 № 608 «О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России» (в ред. от 14.08.2018) // СТРАС «Юрист» (дата обращения: 07.04.2019).

¹⁸ О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генпрокуратуры России № 853/11, МВД России № 5 от 25.12.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 31.03.2019).

относящиеся к компетенции оперативных подразделений экономической безопасности и противодействия коррупции, т.е. к экономическим мошенничествам.

Преступления экономической направленности, относящиеся к перечню преступлений без дополнительных условий – ч.ч. 5, 6, 7 ст. 159 УК РФ.

Все остальные мошенничества (ст. 159 – ст. 159.6 УК РФ) относятся к экономическим только при наличии следующих условий:

К преступлениям экономической направленности относятся деяния, квалифицированные статьями УК РФ при выполнении одного из дополнительных условий, перечисленных в пп. "а", "б", "в", "д" и "ж":

а) преступление совершено лицами:

должностными, материально ответственными и иными, выполняющими на предприятиях, в учреждениях и организациях независимо от форм собственности и организационно-правовых форм организационно-распорядительные или административно-хозяйственные функции в процессе осуществления ими производственно-хозяйственной или финансовой деятельности;

не наделенными указанными полномочиями, но имеющими доступ к предмету преступного посягательства для выполнения трудовых обязанностей по роду деятельности или службы;

выполняющими обязанности по охране имущества или объекта, в котором оно хранится, без материальной ответственности;

б) преступление совершено лицами (за исключением лиц, указанных в п. "а") в процессе осуществления ими производственно-хозяйственной или финансовой деятельности либо под видом ее осуществления:

в отношении юридических или физических лиц, осуществляющих предпринимательскую деятельность независимо от формы собственности и организационно-правовой формы, официально зарегистрированных в качестве предпринимателей, а также объединений (граждан, юридических лиц), не являющихся юридическими лицами;

в отношении участников бюджетного процесса;

выявленное при проведении бухгалтерских документальных ревизий либо проверок контролирующих и надзорных органов;

в) преступление, предусмотренное ст. 159, 159.1, 159.2, 159.3, 159.5, 159.6 УК РФ, совершено физическими лицами с целью завладения имуществом граждан для осуществления производственно-хозяйственной и финансовой деятельности, а также под видом ее осуществления (например, финансовые пирамиды);

д) преступления, предусмотренные ст. 159, 159.1, 159.2, 159.3, 159.5 УК РФ, совершенные неустановленными лицами с использованием подложных документов при осуществлении финансово-хозяйственной деятельности предприятий, выявленные при проведении документально-бухгалтерских ревизий с установлением движения денежных средств, материальных ценностей и т.д.;

ж) преступления, связанные с освоением бюджетных средств, совершенные в ходе осуществления экономической, финансовой и производственно-хозяйственной деятельности участниками бюджетного процесса, в том числе получателями бюджетных средств (орган государственной власти (государственный орган), орган управления государственным внебюджетным фондом, орган местного самоуправления, орган местной администрации, находящееся в ведении главного распорядителя (распорядителя) бюджетных средств казенное учреждение, имеющие право на принятие и (или) исполнение бюджетных обязательств от имени публично-правового образования за счет средств соответствующего бюджета).

Преступление, предусмотренное ст. 159, 159.1, 159.2, 159.3, 159.4 и 159.5 УК РФ, относится к налоговым преступлениям, если оно совершено путем незаконного возмещения НДС, НДФЛ либо выявлено при раскрытии преступлений, предусмотренных ст. 194, 198, 199, 199.1, 199.2, 327.1 УК РФ.

Преступление, предусмотренное ст. 210 УК РФ, относится к числу преступлений экономической направленности, если преступное сообщество было создано в целях совершения преступлений в кредитно-финансовой сфере и такие деяния являются основным видом его деятельности.

Таким образом, при отсутствии указанных выше условий мошенничество является преступлением общеуголовной направленности, за исключением ч.ч. 5, 6, 7 ст. 159 УК РФ, подлежащее обязательному оперативному сопровождению подразделениями экономической безопасности и противодействия коррупции.

Подводя итог, необходимо отметить, что в данном параграфе было дано понятие и основные признаки мошенничества, рассмотрены особенности квалификации ст. ст. 159 – 159.6 УК РФ. Кроме того, с помощью анализа совместного указания Генеральной прокуратуры России № 853/11, МВД России № 5 от 25.12.2018 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» нами разграничены вышеуказанные преступления на общеуголовные и экономические мошенничества.

§2. Оперативная обстановка и способы совершения мошенничеств общеуголовной направленности

В процессе деятельности органов внутренних дел по общим либо отдельным направлениям, а также при оценке результатов их работы в целом либо по линии отдельных служб одним из наиболее часто используемых является понятие оперативной обстановки.

На сегодняшний день существует много различных толкований данного понятия, во-первых, по причине отсутствия единого юридического определения понятия "оперативная обстановка", а также неоднозначностью его трактования представителями науки и практическими работниками.

Так, В.Д. Малков в своих работах связывает понятие оперативной обстановки с изменениями социально-демографических характеристик населения, структурой и динамикой преступности, а также субъектным составом деяний.¹⁹ Г.А. Туманов вкладывает в содержание понятия не только вышеперечисленные признаки, он говорит об оперативной обстановке как совокупности факторов и условий внешней среды, в которую входят климатические, экономико-географические, социально-демографические и многие другие аспекты.²⁰ По нашему мнению, наиболее полно понятие оперативной обстановки представлено Г.Г. Зуйковым, которое он отождествляет с информационным содержанием деятельности органов внутренних дел, отражающим во внешнем управлении состояние преступности, общественного порядка и условий внешней среды.²¹

В теории оперативно-розыскной деятельности под оперативной обстановкой понимается совокупность взаимосвязанных и взаимодействующих внешних и внутренних по отношению к субъекту управления в системах МВД и территориальных органах условий (факторов), определяющих состояние правопорядка на обслуживаемой территории, анализ и оценка информационной модели которых является основой целенаправленных воздействий аппаратов управления на систему подчиненных органов и подразделений внутренних дел субъекта РФ при решении задач правоохраны.²²

Таким образом, к внешним условиям принято относить состояние преступности, социально-экономические, демографические, географические и другие факторы, а к внутренним – силы и средства, а также результаты деятельности органов внутренних дел.

¹⁹ Малков В.Д. Планирование в управлении органами внутренних дел. М., 1976. С. 55.

²⁰ Туманов Г.А. Организация управления в сфере общественного порядка. М., 1972. С. 87

²¹ Зуйков Г.Г. Основы научной организации управления и труда в органах внутренних дел. М., 1974. С. 45 - 46, 111 - 112.

²² Иванов Н.Н., Чиркова Л.В. Аналитическая деятельность в управлении органами и подразделениями внутренних дел. Уч. пос. М., 2005.

В настоящее время оперативная обстановка, связанная с раскрытием и предупреждением мошенничеств общеуголовной направленности, продолжает оставаться сложной.

Нами выделены следующие характерные признаки современного мошенничества:

- в его структуре преобладают преступные действия, посягающие на личную собственность граждан;
- способы совершения обмана достаточно разнообразны и чрезвычайно изменчивы;
- высокий уровень групповых мошеннических посягательств (до 50%), высокий уровень их организованности;
- межрегиональный и международный характер действий мошенников, раздел сфер преступного влияния, постепенное преобразование мошеннических групп в структурные звенья организованных преступных сообществ;
- отличный по социально-демографическим, уголовно-правовым, нравственно-психологическим характеристикам от среднестатистического корыстного преступника портрет мошенника, усиление «интеллектуализации» данной криминальной среды за счет привлечения новых участников²³;
- виктимное, порой неправомерное поведение части потерпевших;
- высокая латентность данного вида преступления.

²³Горбанев В.М. Оперативно-розыскная характеристика мошенничеств, связанных с использованием средств сотовой связи // Общество и право. 2016. № 4 (58). С. 137—141.

Таблица №1. Мошенничества ст. ст. 159-159.6 УК РФ.

	2014	2015	2016	2017	2018
Зарегистрировано	160214	200598	208926	222772	215036
Раскрыто преступлений	62045	59683	54773	56178	57418
Раскрываемость (%)	38,7	29,7	26,2	25,2	28,3
Выявлено лиц, совершивших преступления	39267	39953	35376	36527	37018

Согласно данных анализа состояния преступности, предоставленных ФКУ ГИАЦ МВД России²⁴ в отношении мошенничеств, квалифицируемых по ст. 159-159.6 УК РФ, с 2014 года по 2017 год наблюдается рост зарегистрированных мошенничеств, при этом резкое увеличение преступлений данной категории приходится на 2015 год, что связано с активной распространенностью, так называемых, дистанционных мошенничеств. В 2018 году можно наблюдать спад показателей зарегистрированных мошенничеств общеуголовной направленности. Данное явление можно связать с высокой латентностью данных преступлений, а также с введением в уголовное законодательство России федеральным законом от 28.04.2018 года особо квалифицированного состава преступления кражи п. «г», ч. 3, ст. 158 УК РФ, а именно кража с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 настоящего Кодекса).²⁵ До этого времени, согласно практике оперативных подразделений уголовного розыска, большинство хищений с банковских карт,

²⁴ Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2019. – Режим доступа: <https://мвд.рф/reports/item/12460100/>. - Дата доступа: 17.04.2019.

²⁵ О внесении изменений в Уголовный кодекс Российской Федерации от 28 апреля 2018 г. № 111-ФЗ : в ред. от 28.04.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 02.05.2019)

квалифицировались по ст.159.6 УК РФ в виду неоднозначной судебной практики по делам об общеуголовных мошенничествах.

Так, отделом дознания УМВД России по г. Кирову было возбуждено уголовное дело №*** по ч.2 ст. 159.6 УК РФ в отношении неустановленного лица, которое 30.10.2018 года около 13:30 час, находясь в неустановленном месте, получив неправомерный доступ к счету банковской карты «ВТБ» №**** гр. Муравьева С.А., совершило хищение денежных средств на сумму 27249 рублей. В процессе предварительного расследования данное деяние было переквалифицировано по п. «г» ч.3 ст. 158 УК РФ в виду неустановления вмешательства программных и/или программно-аппаратных средств на средства вычислительной техники, компьютеры, информационно-телекоммуникационные сети²⁶.

Чтобы описать более полную картину оперативной обстановки общеуголовных мошенничеств необходимо выявить динамику раскрываемости указанных преступлений. Так, согласно приведенным данным можно сказать, что с 2014 года по 2017 год наблюдается тенденция снижения раскрываемости мошенничеств, что связано с внедрением преступниками новых способов совершения мошенничеств, таких как мошенничество с использованием платежных карт, в телекоммуникационной сети Интернет и др. Необходимо заметить, что в данный период оперативными подразделениями полиции не были выработаны четкие алгоритмы работы с дистанционными мошенничествами, наблюдалось недостаточное методическое обеспечение по данному направлению, а также нехватка специалистов, обеспечивающих оперативное прикрытие по линии мошенничеств.

В конце 2017 года приказом МВД России №899²⁷ были поставлены следующие задачи по обеспечению эффективной борьбы с мошенничествами:

- разработать проект приказа МВД России о порядке рассмотрения заявлений (сообщений) о дистанционных мошенничествах;
- подготовить предложения о дополнении статистической отчётности сведениями, касающимися учёта мошенничеств;
- ФГКУ "ВНИИ МВД России" разработать рекомендации об особенностях квалификации мошеннических действий по статьям 159¹ - 159³, 159⁵, 159⁶ УК РФ и отграничения их от деяний, подлежащих квалификации по статье 159 УК РФ;
- выработать и направить в территориальные органы МВД России на окружном, межрегиональном и региональном уровнях единый алгоритм действий сотрудников дежурных частей, оперативных подразделений, участковых уполномоченных полиции, следователей и дознавателей при получении заявлений (сообщений) о дистанционном мошенничестве и мошенничестве, совершенном в общественных местах и жилом секторе;
- принять меры по повышению информированности населения о способах совершения мошенничеств и методах защиты от них;
- проработать вопрос о заключении в течение 2018 года соглашений с подразделениями ПАО Сбербанк, другими кредитно-финансовыми организациями, территориальными органами ФНС России и Росреестра, МФЦ, органами социальной защиты населения, расположенными на территориях субъектов РФ, способствующих повышению оперативности обмена документами и информацией и другие меры.

Статистические сведения, приведенные ранее, показывают, что не только количество мошенничеств, регистрируемых правоохранительными

²⁷ Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 24.10.2017 № 3 км : приказ МВД России от 29.11.2017 № 899 // СТРАС «Юрист» (дата обращения: 30.04.2019).

органами становится меньше, но и их раскрываемость начинает нормализоваться благодаря приобретенным знаниям и навыкам борьбы с указанными преступными посягательствами на собственность граждан. Также необходимо заметить, что при всех вводимых мерах, направленных на выявление и раскрытие общеуголовных мошенничеств, доля раскрытых преступлений год от года остается низкой и не превышает 30% от регистрируемых в отчетном периоде. Данное положение дел свидетельствует о технической сложности совершения мошенничеств, возможности быстро сокрыть следы преступления, а также в острой необходимости введения наиболее кардинальных мер по их предупреждению и раскрытию.

Мошенничества общеуголовной направленности характеризуются множественностью способов их совершения, которые можно разделить на две группы – дистанционные (бесконтактные) мошенничества и «контактные» мошенничества.

Анализ оперативной обстановки в сфере борьбы с мошенническими посягательствами свидетельствует о том, что использование преступниками достижений технического прогресса (IP-телефония, зарубежные интернет-ресурсы, динамические IP-адреса, «Skype» и др. с созданием своеобразных диспетчерских пунктов, зашифрованных схем передачи информации, позволяющих им исключить визуальные контакты с потерпевшими), электронных платежных систем, средств мобильной связи значительно снижает для них риск быть задержанными в момент совершения преступления, в связи с чем наиболее организованные группы мошенников в основном переходят на бесконтактный способ совершения преступлений.

В свою очередь под дистанционными мошенничествами согласно письму МВД России «Об организации работы по противодействию отдельным видам мошенничеств» понимается хищение чужого имущества или приобретение права на чужое имущество путем обмана или

злоупотребления доверием, совершенное посредством телефонной связи и (или) телекоммуникационной сети Интернет²⁸.

Исходя из данного определения, можно сделать вывод, что дистанционные мошенничества общеуголовной направленности совершаются с использованием сети Интернет, а также мобильной связи.

Рассмотри самые распространенные способы совершения данных преступлений.

Мошенничества в Интернете.

1. Достаточно быстро во всемирную сеть переместились наиболее простые виды мошенничества: обман покупателей при продаже авиабилетов или создание поддельных сайтов Интернет-магазинов, с целью получения предоплаты за товар без последующей его поставки клиенту. Широко распространение получило мошенничество в социальных сетях и на бесплатных сайтах частных объявлений о продаже. Объявления о возможности приумножения средств граждан публикуют и недобросовестные брокеры.

Согласно проведенному анализу всех поступивших заявлений о дистанционных мошенничествах в УМВД России по г. Кирову за период с сентября - январь 2018 года: около 60% преступлений совершается посредством электронных торговых площадок.

Электронная торговая площадка – программно-аппаратный комплекс организационных, информационных и технических решений, обеспечивающих взаимодействие продавца и покупателя через электронные каналы связи (электронные аукционы, интернет - магазины и т.д.²⁹).

В настоящее время данная сфера имеет недостаточное правовое регулирование, в связи с чем преступники в наибольшей степени стали использовать возможности телекоммуникационной сети Интернет.

²⁸ Об организации работы по противодействию отдельным видам мошенничеств : письмо МВД России от 13.07.2015 №1/5562 // СТРАС «Юрист» (дата обращения: 30.04.2019).

²⁹ Электронная торговая площадка: Википедия. URL:https://ru.wikipedia.org/wiki/Электронная_торговая_площадка (дата обращения: 03.05.2019).

Во-первых, мошенники создают «сайты-однодневки», копии известных интернет-магазинов по продаже различных товаров с целью обмана добросовестных покупателей. При этом продавцу не требуется получать разрешение на создание подобного рода торговой площадки.

Во-вторых, стали распространены такие Интернет-сайты как «Авито», «Юла», «ЕВAУ», где договор купли-продажи осуществляется между частными лицами. То есть любой желающий может выложить объявление о продаже товара, находящейся в его собственности, при этом оплата и пересылка производится по договоренности между продавцом и покупателем. Наибольшее количество преступлений приходится на российский интернет – сайт «Авито», в отличие от международной торговой площадки «ЕВAУ», где гарантом каждой сделки является данная организация, использующая электронную платежную систему PayPal при осуществлении каждой сделки. Таким образом, необходимо перенять международный опыт и ввести нормы, которые заставят такого рода электронные торговые площадки выступать гарантами при осуществлении купли продажи, используя безопасные системы оплаты.

Кроме того, необходимо усовершенствовать российское законодательство в области электронной торговли с целью минимизировать возможность использования преступниками интернет - пространства для совершения преступлений, в частности мошенничеств.

В условиях стремительного роста числа безналичных платежей зафиксированы случаи создания сайтов фальшивых кредитных организаций, платежных систем, которые похищают реквизиты платежных карт граждан. Злоумышленники просят ввести конфиденциальную информацию: номер карты, срок действия, имя держателя, а также ПИН-код и CVC-код, указанный на обратной стороне карты.

Совершение дистанционных хищений в большинстве случаев происходит через Интернет в условиях полной анонимности данных. Как правило, в распоряжении злоумышленников есть специальное программное

обеспечение, позволяющее им скрывать своё подлинное местонахождение. Помимо этого они активно используют абонентские номера сотовой связи, банковские карты, зарегистрированные на несуществующих либо на других лиц. Все это препятствует идентификации личности подозреваемых.

При организации противодействия мошенничеству необходимо помнить, что дальнейшая глобализация информационного пространства, развитие электронных платёжных систем и рынка цифровых продуктов - неизбежный процесс.

Мошенничества с банковскими картами.

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

2. Сообщение «Ваша банковская карта заблокирована».

Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда жертва звонит по указанному телефону, её сообщают о том, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации. На самом деле злоумышленникам нужен номер карты жертвы и ПИН-код. Как только потерпевший их сообщает, преступники получают возможность управлять счетом.

3. Начиная с 2014 года в Российской Федерации ежегодно возрастает число хищений денег со счетов клиентов банков, которые можно условно разделить на два типа:

Первый - осуществленные посредством методов социальной инженерии, для использования которых, как правило, не требуется специальных знаний и технических средств.

Второй – посредством тайного (или как принято говорить несанкционированного) заражения смартфона или компьютера жертвы вредоносным программным обеспечением, которое затем тайно собирает

информацию о подключенных услугах дистанционного банковского обслуживания и по команде злоумышленника списывает денежные средства.

3.1. Пример социальной инженерии: гр. А разместила объявление на интернет-сайте «Авито» о продаже туалетного столика. Гр. Янопулов В. А. путем обмана, под предлогом приобретения товара, получил доступ к персональным данным счета банковской карты «Сбербанк Онлайн» и завладел денежными средствами гр. А. в сумме 14000 рублей, причинив последней значительный материальный ущерб³⁰.

3.2. Пример хищений денежных средств со счетов с использованием вредоносных программ: в смартфон или компьютер жертвы тайно устанавливаются вредоносное программное обеспечение (далее – ПО). Вредоносная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в СМС или ММС сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты. Одним из признаков наличия вредоносных программ на мобильном телефоне является направление «пустых» СМС или ММС сообщений на телефоны, имеющихся в контактах устройства. При открытии адресатом такого СМС или ММС сообщения, происходит дальнейшее заражение вирусом телефонов, получившее данное сообщение.

Это могут быть троянские программы, которые не размножаются и не рассылаются сами, они ничего не уничтожают. Задача троянской программы - обеспечить злоумышленнику доступ к устройству жертвы и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений.

³⁰ Дело № 1-826/2017// Архив Ленинского районного суда г. Кирова. - 2017. – Режим доступа: https://sudact.ru/regular/doc/IB1TbNuvL3xE/?regular-txt=авито®ular-case_doc=®ular-lawchunkinfo=®ular-doc_type=1008®ular-date_from=01.01.2015®ular-date_to=03.05.2019®ular-workflow_stage=®ular-area=1003®ular-judge=&_=1556891539938&snippet_pos=428#snippet. Дата доступа: 03.05.2019.

Если к смартфону подключена услуга «Мобильный банк», то сведения о доступе в «Личный кабинет» становятся известны преступнику. Тайно входя в чужие личные кабинеты он может перечислять денежные средства сотен потерпевших на свои счета, а затем обналичивать.

Преступность в информационной и телекоммуникационной сфере не коррелируется с общей динамикой преступности в России, показывающей снижение ее уровня. И если в 2013 году было зарегистрировано 11 104 подобных преступлений, то уже в 2017 году зарегистрировано 90587 преступлений, а в 2018 году – 174674 преступлений. Семнадцатикратный рост обусловлен не только несовершенством статистического учета, связанного с необходимостью разграничения преступлений, совершенных с использованием информационных и телекоммуникационных технологий, от преступлений, совершенных непосредственно в информационной и телекоммуникационной среде, но и доступностью программных средств, позволяющих совершать киберпреступления даже слабо подготовленным пользователям.

Телефонное мошенничество получило развитие с начала 2000-х годов, когда сотовый телефон стал массовым и доступным. В настоящее время, когда широко используются мобильные телефоны и личный номер может быть у всех, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества растут с каждым годом.

Чаще всего в сети телефонных мошенников попадают пожилые или доверчивые люди. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

Основные схемы телефонного мошенничества:

- Обман по телефону: родственник попал в беду, требование выкупа. Звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Это может быть ДТП, хранение оружия или наркотиков,

нанесение тяжких телесных повреждений и даже убийство. Далее он заявляет, что для решения вопроса необходима определенная сумма денег, которую необходимо перечислить на счет банковской карты или электронного кошелька.

В организации обмана по телефону с требованием выкупа могут участвовать несколько преступников. Звонящий может находиться как в исправительно-трудовом учреждении, так и на свободе. Набирая телефонные номера наугад, мошенник произносит заготовленную фразу, а далее действует по обстоятельствам.

– Телефонный номер-грабитель.

Развитие технологий и сервисов мобильной связи упрощает схемы мошенничества. Приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной - помощь другу, изменение тарифов связи, проблемы со связью или с Вашей банковской картой и так далее. После того как потерпевший перезванивает, долго держат на линии. В результате оказывается, что со счёта списаны крупные суммы.

Существуют сервисы с платным звонком. Чаще всего это развлекательные сервисы, в которых услуги оказываются по телефону, и дополнительно взимается плата за сам звонок. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

– Телефонные вирусы.

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения перейдите по ссылке...». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Мошенники используют специальные программы, которые позволяют автоматически генерировать тысячи таких сообщений. Сразу после перевода денег на фальшивый счёт они снимаются с телефона.

– Продажа поддельных и нелицензированных биологически активных добавок (БАДов).

В недобросовестной рекламе, попадающей даже в телевизионные средства массовой информации, БАДы позиционируются как высокоэффективные средства для лечения практически всех заболеваний. Естественным образом, любая торговля «панацеей» - это преступный обман. К тому же БАДы, как правило, стоят немалых денег, а попадают на эту удочку обычно малообеспеченные граждане, пенсионеры и инвалиды. Некоторые средства, продаваемые таким образом, могут быть не только бесполезны, но и вредны для здоровья.

– В дополнение к описанной схеме в последнее время появилась относительно новый вид подобного мошенничества: злоумышленники звонят людям, ранее пострадавшим от продавцов БАДов и обращавшимся с заявлениями в полицию, и предлагают компенсацию. Представляясь по телефону сотрудниками следствия, прокуратуры, суда, судебными приставами они сообщают будущей жертве о том, что преступники, ранее продавшие БАДы, арестованы, осуждены и в установленном порядке проводится процедура возмещения ущерба. Но для этого необходимо оплатить пошлину (налог, услуги инкассации и т.п.). Предлагают в терминале оплаты перевести деньги на какой-либо счет.

Подобные способы совершения преступлений повышают безопасность преступной деятельности и увеличивают стремление расширить географию преступлений, создавая организованные группы.

Ко второй группе мошенничеств общеуголовной направленности относят «контактные» способы совершения преступлений. В связи с тем, что нормативные акты не дают определения «контактных» мошенничеств, выведем данное понятие исходя из данного выше определения

«дистанционных мошенничеств». Таки образом, под «контактными» мошенничествами следует понимать хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, при котором происходит непосредственный контакт между злоумышленником и потерпевшим лицом.

К группе контактных мошенничеств отнесем следующие распространенные способы совершения мошенничеств:

Во-первых, мошенники могут представиться сотрудниками различных коммунальных служб и сообщить, что прибыли для осуществления срочной или плановой проверки газового, отопительного и электрооборудования, водопровода и т.д.

Во-вторых, Хищение денег под видом снятия порчи. Так, например, ... 2017 года гр. Вишнякова Е.А., путем обмана, под предлогом исцеления сына гр. М., завладела денежными средствами последней в сумме 74 500 рублей³¹.

3. Мошенничества под видом денежной реформы.

4. Хищения денег, совершенные под видом продажи предметов.

В нескольких аптеках Чувашии зарегистрированы факты мошенничества. В присутствии фармацевта посетительница продавала специальные адаптеры для проверки подлинности денег. Покупателем выступал мужчина. Затем парочка уходила – он за деньгами, она за дополнительной партией товара. Посредником в их дальнейшем общении невольно оказывался работник аптеки. Продавец электронных устройств просила фармацевта передать покупателю адаптеры, затем тот приходил, забирал их и оставлял деньги. Потом с новым товаром возвращалась женщина. Вся схема была рассчитана на то, что в определенный момент аптекарь, уже уверенная, что ее не обманут, расплачивалась за адаптеры своими деньгами. Естественно, после этого ни мужчина, ни женщина уже не

³¹ Дело № 1-0745/2017// Архив Ленинского районного суда г. Кирова. - 2017. – Режим доступа: https://sudact.ru/regular/doc/vxOwebYBrPV/?regular-txt=порчи®ular-case_doc=®ular-lawchunkinfo=®ular-doc_type=1008®ular-area=1003®ular-court=Ленинский+районный+суд+г.+Кирова+%28Кировская+область%29®ular-judge=&_=1556887297169&snippet_pos=1326#snippet. Дата доступа: 03.05.2019.

приходили. Например, 23 января 2012 года на территории города Бирска Республики Башкортостан за совершение серии мошеннических действий задержана преступная группа, в состав которой входили 39-летний мужчина и 32-летняя женщина, проживающие в городе Уфа³².

5. Мошенничества, совершенные под видом покупки золотых изделий. Мужчина заходил в ювелирные салоны, выбирал несколько схожих золотых изделий, и забирал их якобы не надолго, чтобы посоветоваться с друзьями. В залог он оставлял не традиционные российские рубли, а денежные банкноты Бразилии. Подвох оказался в том, что курс заморских банкнот примерно в 2 раза ниже того, каким его представил покупатель³³.

6. Хищения, совершенные под видом выплаты компенсации.

7. Хищения, совершенные под видом ремонта квартир.

8. Мошенничества, совершенные под видом страховщиков. Преступники заключали с пенсионерами «липовые» договоры страхования и забирали деньги.

Подводя итог, необходимо отметить, что мошенничества общеуголовной направленности на современном этапе развития обладают некоторыми особенностями: межрегиональный и международный характер, высокий уровень организованности, высокая латентность, зачастую виктимное поведение потерпевших, множество способов обмана и др. Кроме того, необходимо отметить серьезные недостатки в статистическом учете ФКУ ГИАЦ МВД России, так как в виду ограниченности данных, нельзя с точностью оценить картину преступности по линии общеуголовных мошенничеств, а в виду этого сложно построить эффективную борьбу с указанными преступлениями.

³² Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2019. – Режим доступа: <https://21.mvd.rf/news/item/500876/>. - Дата доступа: 03.05.2019.

³³ Дело № 1-228/2015// Архив Канашского районного суда Чувашской Республики. - 2015. – Режим доступа: https://sudact.ru/regular/doc/BGWcyBF61l5R/?regular-txt=+бразилии®ular-case_doc=®ular-lawchunkinfo=®ular-doc_type=®ular-date_from=01.01.2015®ular-date_to=01.05.2018®ular-workflow_stage=®ular#snippet. Дата доступа: 03.05.2019

Необходимо отметить, что мошенничества в настоящее время подразделяются на дистанционные и контактные, в свою очередь, охватывая множество различных способов их совершения.

§3. Особенности личности мошенника и способов совершения преступлений

Деятельность оперативных подразделений ОВД по предупреждению и раскрытию мошенничеств, прежде всего, предполагает знание оперативными сотрудниками способов их совершения, приемов, предпринимаемых преступниками на различных стадиях противоправной деятельности, особенностей противодействия правоохранительным органам и т.п. Все это составляет оперативно-розыскную характеристику (далее - ОРХ) данных преступлений. Практическая значимость исследования элементов, составляющих характеристику мошенничества, определяется тем, что эффективная борьба с ним, как, впрочем, и с любым другим видом преступлений, невозможна без изучения действий преступников³⁴.

Рассматривая современное состояние обозначенных преступлений, стоит отметить, что, несмотря на относительно небольшой удельный вес в общей структуре преступлений корыстной направленности (около 10,7%)³⁵, общественную опасность мошенничества нельзя недооценивать. Особенно если это касается мошенничеств, совершаемых организованными преступными группами, с разделением ролей и вовлечением в преступную деятельность представителей предприятий и организаций, сотрудников правоохранительных органов.

По нашему мнению, в целях эффективного противодействия мошенничеству, в первую очередь, необходимо уделять внимание указанным категориям лиц, совершающим мошенничества, и непосредственно характеристике личности преступника.

³⁴ Ермолович Д. В., Широких С. В. Некоторые поисковые социально-психологические признаки личности мошенника // Юридическая Россия. – № 5 (47). – С. 36-38.

³⁵ Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2019. – Режим доступа: <https://мвд.рф/reports/item/12460100/>. - Дата доступа: 17.04.2019.

Вопросы характеристики личности преступника постоянно находятся в центре внимания среди научных деятелей.

В то же время в указанных отраслях права отсутствуют единое определение и исчерпывающий перечень составных элементов (признаков) «оперативно-розыскной характеристики личности преступника». Например, Ю.В. Александров отмечает, что личность преступника – это совокупность социально-психологических свойств человека, которые при определенных ситуативных обстоятельствах являются причиной совершения преступления.³⁶

Рассматривая оперативно-розыскную характеристику лиц, совершающих мошенничество, Б.В. Петухов выделяет основные признаки и разрабатывает классификацию информации о преступнике по трем категориям:

- информация анатомо-физиологического характера (возраст, пол, этнический тип, конституция тела, действенно-функциональные признаки, наличие болезней);
- информация психологического характера (тип характера, мотивация и мотивы, психическое состояние, умственные способности, характер языка, манера поведения, моральные ценности и т.п.);
- информация социального характера (семейное положение, социальный статус, отношения с родными, образование, судимость, роль в преступной группе и т.п.). Таким образом, первая и вторая категории представляют информацию о личности преступника, а третья несет дополнительную информацию, характеризующую не только преступника, но и его окружение, социальные формации, в которых он находится³⁷.

Достаточно интересно мнение О.Ю. Зуева, который определил, что оперативно-розыскная характеристика лиц, совершающих преступления, это

³⁶ Александров Ю. В., Гель А. П., Семаков Г. С. Криминология: курс лекций. – Киев: МАУП, 2002. – С. 295.

³⁷ Петухов Б. В., Лунин Н. Н. К вопросу о понятии мошенничества // Юрист. – 2004. – № 3 – С. 12-16.

совокупность уголовно-правовых, криминалистических и криминологических данных относительно признаков лиц, которые имеют значение для эффективного противодействия указанному виду преступлений.

Принимая во внимание сказанное, можно утверждать, что оперативно-розыскная характеристика мошенников представляет собой совокупность информации, которая содержит уголовно-правовые, криминалистические и криминологически значимые признаки лиц, совершающих мошенничество, на эти признаки и необходимо ориентироваться при противодействии мошенничеству. В теории оперативно-розыскной деятельности, криминологии и криминалистики встречаются различные обобщающие типы лиц-мошенников. Основные из них:

а) случайные мошенники, которые осуществляют мошенничество впервые, под влиянием обстоятельств или других лиц;

б) лица, ранее осужденные за мошенничество, при этом их, в свою очередь, подразделяют на:

– мошенников-рецидивистов, которые осуществляют главным образом мелкое мошенничество;

– мошенников-многократных (закоренелых) рецидивистов;

в) мошенники-гастролеры;

г) мошенники, которые осуществляют длящиеся мошенничества, заключающиеся в длительном получении материальных благ;

д) мошенники-профессионалы, образ жизни которых связан с систематическим совершением преступлений, которые являются для них основным источником получения средств для существования³⁸.

Анализ встречающихся классификаций личности мошенников свидетельствует о том, что в их основу положены устоявшиеся формы, виды и способы совершения рассматриваемых преступлений, которые сегодня, учитывая современные технологии и профессионализм мошенников,

³⁸ Кара М. В. Характеристика лиц, которые совершают мошенничество // Право и Безопасность. – 2018. – № 5 (47) – С. 22-27.

значительно изменились. Что, в свою очередь, существенно отразилось на оперативно-розыскной характеристике личности мошенника.

Рассматривая непосредственно личность мошенника, стоит отметить, что это, прежде всего, «коммерческий» тип преступников. Мошенники совершают преступления без применения насилия, с использованием заведомо ложных сведений. В своем общественном положении мошенники являются профессионалами высокого или среднего уровня, в большинстве случаев хорошо ориентируются в законодательстве – налоговом, банковском; обладают знаниями в области бухгалтерского учета (64,5% мошенников занимали руководящие должности в сферах бухгалтерии и бухгалтерского учета (36,3%), маркетинга (27%), юриспруденции (21,4%)³⁹. Одновременно следует отметить, что мошенники – своего рода элита преступного мира, талантливые артисты, находчивые и изворотливые, быстрые в действиях, нешаблонно мыслящие, имеющие образование (67% из них имеют высшее образование, 27% – неполное высшее и 73% – средний и высокий уровень интеллекта), «религиозные», не злоупотребляют спиртным и наркотиками, отличаются психологической устойчивостью, оптимизмом, конформизмом, самоконтролем, добротой и отзывчивостью, часто имеют глубокие знания в разных сферах человеческой деятельности. Многие из них специалисты в психологии, экономике, информационных технологиях и других отраслях права. Отдельные из них даже осведомлены о методах работы правоохранительных органов⁴⁰.

Анализируя теорию и практику противодействия мошенничеству, приходим к выводу, что в последнее время наблюдается повышение среднего возраста мошенников (с 18 до 24 лет в 2004 г. до 30–35 лет в 2018 г.), а следовательно, их образовательный уровень и профессиональные навыки растут. Вообще по возрастным критериям лица, совершающие

³⁹ Абрамов М.А., Прокопов А.Г. Личность мошенника как основной элемент оперативно-розыскной характеристики.// Вестник Казанского юридического института. – 2015. – № 4(22). – С.73-76.

⁴⁰ Ахмедшин Р. Л. Криминалистическая характеристика личности преступника: автореф. дис. ... д-ра юрид. наук. – Томск, 2016. – С. 20.

мошенничества, распределяются следующим образом: от 14 до 18 лет – 7,1%; от 18 до 25 лет – 22,3%; от 25 до 30 лет – 47,2%; от 30 до 35 лет – 17,5%; от 35 до 45 лет – 13,2%; старше 45 лет – 9,7%. В то же время отметим, что в большинстве случаев (73%) мошенничество совершается мужчинами. Преступное поведение женщин отличается от мужчин масштабом и характером преступлений, способами и средствами их совершения, выбором жертвы преступного посягательства. Результаты изучения эмпирического материала свидетельствуют о том, что женщины совершают мошенничество в большинстве случаев в составе группы, по предварительному сговору, в отношении лиц пожилого возраста, в сфере социального обеспечения граждан, торговли. Вместе с тем установлено, что совершающие мошенничества женщины в 43% случаев, были ранее осуждены за совершение других преступлений против собственности, причем характерным признаком является и то, что 75% мошенничеств совершаются женщинами-цыганками.

Принимая во внимание, что при совершении мошенничества преступник, действуя умышленно, преследует в качестве основной корыстную цель, стоит остановиться на том, что же побудило его совершить преступление, то есть на мотиве. В данном случае уместно привести мнение Ю. М. Антоняна и В. Е. Эминова: «...Мотив наиболее ярко характеризует человека, и личность такова, каковы ее мотивы⁴¹». Выделяют следующие типы корыстных преступников по ведущим мотивам:

- корыстолюбивый;
- утверждающийся;
- дезадаптированный;
- семейный;
- игровой;
- алкогольно-наркотизированный.

⁴¹ Антонян Ю. М., Эминов В. Е. Личность преступника. Криминологическое исследование. — М., 2010. — С. 368.

Проведенное анкетирование сотрудников подразделения уголовного розыска УМВД России по Кировской области позволяет выделить наиболее распространенные условные типы мошенников по ведущим мотивам:

1. Корыстолюбивые — лица (48% мошенников, по мнению опрошенных), которые совершают преступления для достижения своих личных алчных целей, похищенное они накапливают, имеют постоянное место работы, профессиональные знания, навыки и умения, опыт работы.

2. Утверждающиеся — лица (14% мошенников, по мнению опрошенных), которые совершают преступления для самоутверждения. Следует обратить внимание, что самоутверждение их происходит не только в глазах других лиц, то есть соучастников преступления, но и в собственных, в силу того что для некоторых мошенничеств необходимо наличие не только особых знаний, умений, навыков, но и храбрости.

3. Семейные — лица (17% мошенников, по мнению опрошенных), которые совершили преступление для обеспечения нужд своего окружения. Окружением в данном случае следует признавать не только близких родственников, но и иных лиц, состоящих с ними в родстве, свойстве (родственники супруга), а также лиц, жизнь, здоровье и благополучие которых преступникам дороги в силу сложившихся личных отношений. Потребности, ради которых лицо совершает преступление, могут быть весьма разнообразными, от покупки продуктов питания до приобретения элитных вещей, недвижимости. Данный тип мошенника скромный, похищенное тратит не на себя, а на нужды других.

4. Игровые — лица (7% мошенников, по мнению опрошенных), которые обладают низким нравственно-культурным уровнем, обусловленным их индивидуальной психологией. Таким мошенникам присущи игнорирование неприкосновенности чужого имущества, отрицательные антиобщественные черты характера (наглость, дерзость, зависть, эгоизм), а также негативные эмоциональные и волевые качества.

Желание похитить чужое имущество возникает ради развлечения, шалости или игры.

5. Деадаптированные — лица (12% мошенников, по мнению опрошенных), для которых совершение мошенничеств стало основным или единственным источником дохода. К таким, как правило, относят ранее судимых лиц либо мошенников-профессионалов.

6. Алкогольно-наркотизированный тип встречается крайне редко (не более 2% мошенников, по мнению опрошенных).

Вместе с этим необходимо отметить, что лица, совершающие мошенничества, характеризуются умеренностью, уравновешенным темпераментом. Указанное отражается в их преступной деятельности. Так, мошенники тщательно готовятся к совершению преступления, обдумывают каждый свой «шаг», изучают законодательство, выискивая существующие неурегулированные вопросы, чтобы в дальнейшем избежать уголовной ответственности.

Для лиц, совершающих мошенничество в крупных размерах, «профессионально», наряду с материальным обогащением, особенностью также является стремление получить определенный социальный статус, авторитет среди преступного мира, респектабельность. Поэтому высокий материальный достаток и социальная обустроенность не всегда являются той целью, к которой стремятся мошенники. Лица, которые совершают мошенничества, характеризуются наличием высокого социального статуса, поэтому применение к ним такого вида наказания, как лишение свободы, оказывает сдерживающее влияние, потому что, прежде всего, они опасаются потерять именно свой социальный статус, респектабельность и авторитет среди деловых партнеров. Имея достаточно выраженные интеллектуальные и волевые черты характера, многие из них встают на путь профессиональной преступной деятельности, превращая ее в стиль жизни и способ получения основного источника существования.

Для профессиональных мошенников характерно также наличие преступного инструментария, который постоянно обновляется и выступает в роли средств и орудий совершения преступлений, позволяющих таким образом повлиять на поведение потерпевшего, при котором он передаёт имущество (или право на имущество) в пользу мошенника, при этом потерпевший считает такую передачу правомерной.

Таким образом, целенаправленное противодействие мошенничеству невозможно без знания сотрудниками оперативных подразделений ОВД всех элементов, присущих оперативно-розыскной характеристике рассматриваемого вида преступлений. При этом основное место мы отводим характеристике отдельных категорий лиц, совершающих мошенничества, и непосредственно личности преступника. По нашему мнению, знания о личности преступника в структуре оперативно-розыскной характеристики мошенничеств, причинах и механизмах преступного поведения являются основой эффективного предупреждения и раскрытия мошенничества.

Глава 2. ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ДОКУМЕНТИРОВАНИЕ МОШЕННИЧЕСТВ ОБЩЕУГОЛОВНОЙ НАПРАВЛЕННОСТИ

§1. Основные положения выявления мошенничеств общеуголовной направленности

Понятие оперативно-розыскной деятельности неразрывно связано с ее задачами, одной из которых является выявление преступлений.

Выявление преступлений означает добывание информации об их подготовке, совершении и последствиях. Это вызвано тем, что преступник, совершая общественно опасные деяния, с целью избежать наказания практически всегда стремится скрыть сам факт преступления. Исходя из этого, в любом государстве всегда существует определенное число латентных преступлений, выявление которых составляет определенную сложность. К таким наиболее тщательно замаскированным относятся и преступления, связанные с мошенническими посягательствами⁴².

Об уровне латентности мошенничеств можно судить по тому, что, по результатам исследований, реальный его показатель превосходит статистические данные в пять раз. Особенно характерна латентность для мошеннических посягательств на личную собственность граждан. Это обстоятельство обусловлено несколькими факторами. Главный из них — нежелание самих потерпевших обращаться в правоохранительные органы с заявлением о совершенном в отношении них преступлении. Зачастую это объясняется их доверчивостью, неосмотрительностью, беспечностью или алчностью. Выявление фактов мошенничества состоит из нескольких этапов: получение первичных сведений, их проверка и анализ, а также принятие решения по результатам проверки.

Знание оперативными сотрудниками и следователями элементов (признаков) оперативно-розыскной характеристики мошенничества,

⁴² Лабутин А.А. Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. № 12. С. 50—55.

безусловно, будет способствовать повышению их профессиональной квалификации и эффективности борьбы с рассматриваемым видом хищений.

Для предупреждения данных преступлений необходима активная профилактическая работа сотрудниками правоохранительных органов, которым необходимо регулярно выступать в средствах массовой информации, готовить публикации и статьи, размещать видеоматериалы, организовывать встречи с гражданами, в ходе которых пожилым людям рассказывать о механизме совершения данного вида преступлений (главным образом, это телефонные звонки с просьбой помочь попавшему в беду родственнику и перевести деньги через банкомат), напомнить правила поведения в таких ситуациях.

Изучение практики свидетельствует о том, что наиболее эффективными формами привлечения населения к процессу выявления данного вида преступления являются:

- информирование отдельных граждан о совершенных мошенничествах путем индивидуальных бесед с ними;
- ориентирование на выявление мошенничеств лиц, способных оказать такую помощь (работников ДЭЗ, врачей и т.д.);
- информирование населения об обстоятельствах совершения преступления с помощью специальных плакатов и объявлений, а также через СМИ, кабельное телевидение;
- выступления сотрудников ОВД перед гражданами;
- предоставление необходимой информации редакциям газет, радио, телевидения;
- выступления оперативных сотрудников ОВД и следователей в печати, а также по радио и телевидению.

Совершаемые преступления зачастую носят многоэпизодный и межрегиональный характер, совершаются организованными группами, с распределением ролей, с использованием коррумпированных связей. Активно и весьма умело используются при совершении преступлений

банковские документы, кредитные карты, средства связи и оргтехника (компьютеры, принтеры, множительные аппараты и т.п.). Способы мошенничества отличаются крайним разнообразием — от развлекательных манипуляций «наперсточников» до создателей «пирамид». Арсенал мошеннических приемов — разнообразен. Профессиональная ориентация мошенников устойчива.

Таким образом, работа по выявлению общеуголовных мошенничеств выстраивается в зависимости от способа их совершения.

Так, при выявлении дистанционных мошенничеств необходимо проведение следующих оперативно-розыскных и иных мероприятий.

Первоначальным этапом выявления преступлений является поиск первичной информации. Необходимо знать, что имеется ряд причин, подчеркивающих необходимость поиска информации на информационных ресурсах в сети «Интернет» именно в рамках ОРД ОВД, так как одной из причин является то, что электронная информация, содержащая признаки преступления или сведения, позволяющие установить обстоятельства совершенного преступления, затруднительно (а порой и невозможно) обнаружить в рамках гласной процессуальной деятельности. Специфика электронной информации такова, что она может быть уничтожена, прежде чем получит процессуальное закрепление. При этом уничтожение информации легко выполняется не только при физическом контакте с ней преступника, но и на расстоянии, с использованием сети «Интернет».

Кроме этого, своевременное обнаружение и блокирование криминальной информации, создаваемой при помощи аппаратно-программных средств и распространяемой по информационно-телекоммуникационным сетям, позволяет пресечь совершаемые преступления и предупредить новые.

Практика показывает, что в сетевом пространстве существуют ряд объектов, на которые необходимо обратить внимание и на которые осуществляются посягательства, а именно:

- сайты социальных сетей, интернет-магазины, сайты различных банков и т. д.;
- сайты, через которые проходит и распространяется информация, происходит реализация товаров и услуг;
- сайты и форумы сетевого общения криминальных лиц (различные открытые и закрытые форумы).

При этом мошенники применяют следующие методы и технологии при совершении преступлений:

- сокрытие электронной информации о своих действиях:

1) путем передачи (в т. ч. кодирования) электронных посланий. При этом используются компьютеры и электронные записные книжки для хранения следующей информации: номеров банковских счетов, баз данных потенциальных потерпевших, данных связи с сообщниками и т. д.;

2) путем использования неконтролируемых средств электронной связи. Телефоны, факсы, компьютеры применяются и непосредственно при проведении незаконных операций для передачи информации, на какой счет пересылать полученные деньги. С этой целью используются спутниковые телефоны, «клонированные» сотовые телефоны (т. е. сотовые телефоны, идентификационные коды которых, присвоенные законным пользователям, были перехвачены и записаны в сотовые телефоны преступников), телефонные карточки с предварительной оплатой, широкополосные радиочастоты, чат-комнаты в сети «Интернет» с ограниченным доступом;

- отмыwanie доходов от мошеннических действий с помощью электронных переводов. Сеть «Интернет» обладает тремя специфическими свойствами, которые могут способствовать отмыванию денег: свободным доступом, анонимностью отношений между клиентом и финансовым учреждением, высокой скоростью совершения электронных сделок;

- информационное противодействие мероприятиям, проводимым органами внутренних дел.

Для выявления информации, представляющей оперативно-розыскной интерес, в первую очередь используется поиск по информационным ресурсам сети «Интернет» с применением разного рода поисковых систем (Google, Yandex, Rambler и т. п.). Информация, представляющая оперативный интерес, содержится в сетевом пространстве, на криминогенных объектах как в виде следов противоправной деятельности, так и в виде сообщений лиц, осведомленных об обстоятельствах подготовки или совершения преступления, а также в виде ссылок на сетевые сайты и адреса, где могут быть размещены различные запрещенные к распространению сведения.

На данной стадии собираются сведения, поступающие, прежде всего, от источников оперативной информации. Поиск информации может осуществляться и в рамках изучения информации, размещаемой в сети «Интернет». Так, изучение преступной деятельности лиц, занимающихся мошенничеством, показывает, что его особенностью является активный поиск в виде SMS-рассылок (например, информация о том, что родственник или знакомый попал в сложную жизненную ситуацию).

Также необходимо особое внимание уделять информации, получаемой в результате мониторинга интернет-сайтов и интернет-форумов. В сети «Интернет» может осуществляться рассылка сообщений на аккаунты по «Skype» с указанием абонентских номеров сотовой связи, приложением инструкции о проведении платежей через электронные системы оплаты.

На стадии выявления сведений, представляющих оперативный интерес, большое значение имеет информационный обмен. Практически все службы и подразделения органов внутренних дел регулярно получают сведения о мошеннических действиях. Также искомую информацию можно добыть при взаимодействии с оперативными подразделениями ФСИН России, в связи с тем, что около 60% мошенничеств с использованием средств сотовой связи

совершается именно осужденными, находящимися в местах лишения свободы⁴³.

В данной ситуации существенное значение приобретает использование возможностей оперативных подразделений органов внутренних дел и уголовно-исполнительной системы (далее – УИС) по выявлению преступлений рассматриваемого вида и документированию фактов преступных действий. При этом возможности оперативных работников уголовно-исполнительной системы в данном аспекте более значимы, так как преступники находятся на территории их оперативного обслуживания – в исправительном учреждении или следственном изоляторе.

Оперативно-розыскная деятельность позволяет использовать не только гласные, но и негласные силы, средства и методы. Причем в деятельности по выявлению мошенничеств изучаемого вида приоритет имеют именно негласные возможности оперативных подразделений УИС.

К особенностям, свидетельствующим о возможности оперативно-розыскного выявления данных преступлений, следует отнести следующие.

Для совершения мошенничества в исправительных учреждениях с использованием мобильного телефона осужденные-мошенники выполняют комплекс подготовительных действий, который включает:

- проработку идеи (ознакомление (целенаправленное) со средствами массовой информации, беседы с лицами, которые совершали аналогичные преступления, хорошо знают работу средств связи) и выбор направления конкретной преступной деятельности (нередко опираясь на опыт ранее совершенных преступлений);

- получение (приобретение) денежных средств, пластиковых карт либо получение согласия родственников, знакомых, которые могут профинансировать затраты на реализацию обозначенной идеи;

⁴³ Кудрявцев А.В., Крюков И.В. Некоторые особенности выявления мошенничеств, совершаемых в учреждениях УИС с использованием средств мобильной связи /Вестник Владимирского юридического института. 2017, № 4(45). - С. 21-24.

- поиск соучастников (лиц, находящихся на свободе, с целью использования их в качестве посредников) и объединение в преступную группу, распределение обязанностей между соучастниками, в том числе по способам получения и передачи денежных средств;

- получение технических средств (мобильных телефонов, sim-карт, зарядных устройств, а также наставлений, инструкций, прайс-листов, в которых излагаются технические возможности конкретных средств связи) является обязательной составляющей подготовки и совершения преступления, так как осуществление подобного рода мошенничества требует наличия мобильного телефона;

- изучение личности предполагаемого потерпевшего;

- определение направлений использования полученных денежных средств⁴⁴.

Кроме того, распространенным способом обмана является телефонное мошенничество. В данном случае преступники используют в целях реализации преступного умысла, а также сокрытия следов преступления множество sim-карт, процедура оформления которых осуществляется вопреки Федеральному закону «О связи»⁴⁵.

Самая распространенная схема приобретения sim-карт выглядит следующим образом: регистрируется фиктивное юридическое лицо, на которое оформляется пакет sim-карт. Далее, эти sim-карты выдаются дилерам на точках, типа выхода из метро, у вокзалов, а те уже занимаются их незаконной реализацией.

⁴⁴ Нуждин А. А. Расследование мошенничества, совершенного осужденными в учреждениях УИС с использованием средств сотовых систем подвижной связи :автореф. дис... канд. юрид. наук. Рязань, 2015. С. 19–22

⁴⁵ О связи : Федеральный закон РФ от 07.07.2003 № 126-ФЗ: в ред. от 27.12.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019).

Ответственность за данные деяния предусмотрена ст. 13.29 КоАП РФ⁴⁶ и влечет наложение административного штрафа на граждан в размере от двух тысяч до пяти тысяч рублей. Данный штраф во много раз меньше, чем сумма денежных средств, получаемая от реализации sim-карт. В связи с чем, считаем необходимым ужесточить меру наказания за заключение договора об оказании услуг подвижной радиотелефонной связи лицом, не имеющим документов, подтверждающих полномочия действовать от имени оператора связи, с целью минимизации теневого рынка sim-карт и, соответственно, предупреждения мошенничеств с использованием средств мобильной связи. С учетом наличия широкого спектра подготовительных действий, связанных с совершением мошенничеств с использованием средств мобильной связи лицами в исправительных учреждениях и следственных изоляторах, у оперативных работников имеется возможность осуществления оперативного поиска оперативно значимой информации в целях выявления сведений о преступной деятельности.

В теории ОРД ОВД существуют различные подходы к определению оперативного поиска. Не вдаваясь в их детальный анализ, подчеркнем, что применение указанной организационно-тактической формы дает оперативным работникам возможность:

- во-первых, выявить информацию о потенциальных правонарушителях с последующей постановкой их на оперативно-профилактический учет для дальнейшего проведения оперативно-розыскных и иных мер, исключающих возможность данных лиц заниматься противоправной деятельностью;
- во-вторых, обеспечить изучение данных лиц, их противоправных замыслов, намерений;
- в-третьих, установить детерминанты возможного преступного поведения правонарушителей с их последующим устранением;

⁴⁶ Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ : в ред. от 01.05.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.05.2019).

– в-четвертых, эффективно применять те или иные тактические приемы, направленные на недопущение преступлений и нарушений режима содержания⁴⁷.

Кроме того, при выявлении лиц, занимающихся бесконтактным мошенничеством, оперативным сотрудникам следует иметь в виду, что таким образом осуществляют преступную деятельность хорошо организованные группы, где прослеживается иерархическая организация, когда все функции участников преступной деятельности четко распределены. При этом соблюдается жесткая дисциплина, продумана система безопасности, имеется контроль за деятельностью лиц, занимающих низшие ступени в подобной организации. Анализируя вышесказанное, необходимо сказать, что получение первичной информации и дальнейшая ее проверка должна предусматривать планирование не только оперативно-розыскных, но и оперативно-технических и оперативно-поисковых мероприятий, что возможно только в рамках ОРД ОВД.

Также необходимо указать на целесообразность создания специализированных групп, состоящих из сотрудников подразделений уголовного розыска, отдела «К» БСТМ МВД России и представителей Роскомнадзора для проведения совместных проверок, в том числе с помощью мониторинга Интренет-ресурсов, направленных на выявление и документирование фактов нарушения законодательства в сфере связи, информационных технологий и массовых коммуникаций.

Необходимо отметить, что выявление лиц, причастных к совершению преступлений такого рода, невозможно без использования специальных познаний. Несомненно, и в дальнейшем, на разных этапах предварительного расследования без таких познаний невозможен сбор и исследование доказательств по уголовному делу.

⁴⁷ Кудрявцев А.В., Крюков И.В. Некоторые особенности выявления мошенничеств, совершаемых в учреждениях УИС с использованием средств мобильной связи / Вестник Владимирского юридического института. 2017, № 4(45), С. 21-24.

Таким образом, необходимо отметить, что выявление фактов мошенничества состоит из нескольких этапов: получение первичных сведений, их проверка и анализ, а также принятие решения по результатам проверки. Для получения первичных сведений в первую очередь используется поиск по информационным ресурсам сети «Интернет» с применением разного рода поисковых систем (Google, Yandex, Rambler и т. п.). Также искомую информацию можно добыть при взаимодействии с оперативными подразделениями ФСИН России, в связи с тем, что около 60% мошенничеств с использованием средств сотовой связи совершается именно осужденными, находящимися в местах лишения свободы.

При выявлении лиц, занимающихся бесконтактным мошенничеством, оперативным сотрудникам следует иметь в виду, что таким образом осуществляют преступную деятельность хорошо организованные группы, где прослеживается иерархическая организация, когда все функции участников преступной деятельности четко распределены.

§2. Документирование мошенничеств общеуголовной направленности на первоначальном этапе раскрытия

Первоначальный этап раскрытия мошенничеств начинается с принятия заявления, сообщения либо обращения граждан сотрудником правоохранительных органов.

Заявления и сообщения о преступлениях, вне зависимости от места и времени совершения преступления, а также полноты содержащихся в них сведений и формы представления подлежат обязательному приему во всех территориальных органах МВД России. Круглосуточный прием заявлений и сообщений о преступлениях осуществляется оперативным дежурным⁴⁸ дежурной части территориального органа МВД России. При

⁴⁸ Согласно пункта 9 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, утвержденной приказом МВД России от 29.08.2014 № 736 (в ред. от

обращении в дежурную часть органа внутренних дел граждан по телефону или лично с заявлением, сообщением о готовящемся, совершаемом или совершенном мошенничестве, оперативный дежурный обязан:

1) Принять и зарегистрировать заявление, сообщение в соответствии с нормативными правовыми актами, регламентирующими порядок приема, регистрации и разрешения в органах внутренних дел Российской Федерации заявлений, сообщений и иной информации о преступлениях и происшествиях⁴⁹.

2) Выяснить у заявителя данные о времени, месте, обстоятельствах и способе совершения мошенничества (под каким предлогом оно совершено), информацию о номерах расчетных счетов, куда были переведены денежные средства и каким способом (через платежный терминал, банкомат, банковским переводом (через оператора банковского учреждения путем составления банковского поручения), электронные платежные системы, с карты на карту и т.д.); об Интернет-ресурсах, с помощью которых было совершено преступление (сайты, социальные сети) и иную информацию, имеющую значение для дальнейшего раскрытия преступления; сведения о предполагаемом преступнике (как представлялся, какие данные о себе сообщил, номера телефонов, электронной почты, паспортные и иные данные); сумму причиненного ущерба, его значительность (с учетом материального положения заявителя); приметах лиц, его совершивших, об очевидцах и о лице, сообщившем о преступлении.

07.11.2018) под оперативным дежурным понимается начальник дежурной части, начальник дежурной смены, старший оперативный дежурный, оперативный дежурный, дежурный, помощник оперативного дежурного // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.05.2019).

⁴⁹ О едином учете преступлений (вместе с «Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о преступлениях», «Положением о едином порядке регистрации уголовных дел и учета преступлений», «Инструкцией о порядке заполнения и представления учетных документов») : приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 (в ред. от 20.02.2014) // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.05.2019).

3) Организовать незамедлительный выезд на место преступления находящихся в оперативном подчинении нарядов, задействованного согласно плана комплексного использования сил и средств органов внутренних дел по обеспечению правопорядка на улицах и в иных общественных местах, а в случае невозможности их направления - сотрудников оперативных подразделений, участкового уполномоченного полиции, для принятия мер к пресечению преступления, задержанию лиц, его совершивших, установлению очевидцев происшествия.

4) С учетом полученной первичной информации, а также исходя из характера совершенного преступления определить состав следственно-оперативной группы⁵⁰ (далее – СОГ), при необходимости обеспечить участие в осмотре места происшествия специалистов-криминалистов и иных специалистов, организовать выезд СОГ и обеспечить сотрудников средствами связи, криминалистической техникой и транспортом для доставления к месту происшествия и обратно.

5) Доложить о совершении мошенничества и принятых мерах неотложного реагирования руководителю (начальнику) органа внутренних дел или лицу, его замещающему, с последующим информированием их о результатах работы СОГ.

6) При необходимости известить другие органы внутренних дел о совершенном мошенничестве, приметах лиц, подозреваемых в его совершении, и других обстоятельствах, имеющих значение для раскрытия преступления.

7) Поддерживать постоянную связь с СОГ, сотрудниками территориального или иного органа МВД России, находящимися на месте происшествия, с целью получения дополнительных данных об обстоятельствах совершения мошенничества, о приметах лиц,

⁵⁰ Об объявлении Инструкции по организации совместной оперативно-служебной деятельности подразделений ОВД РФ при раскрытии преступлений и расследование уголовных дел : приказ МВД России от 29.04.2015 № 495 дсп // СТРАС «Юрист» (дата обращения: 25.05.2019).

подозреваемых в его совершении, и других сведений, необходимых для принятия дополнительных мер по раскрытию преступления.

8) При необходимости, по указанию ответственного от руководства органа внутренних дел, а в случае его отсутствия самостоятельно, с последующим докладом руководителю территориального органа МВД России, организовать проведение неотложных оперативно-розыскных мероприятий по задержанию автотранспорта (план «Перехват»)⁵¹.

9) Докладывать о результатах проведения первоначальных оперативно-розыскных мероприятий и следственных действий руководителю (начальнику) территориального органа МВД России.

10) Обеспечить получение сведений, подлежащих включению в суточную оперативную сводку, особое внимание обратив на информацию о способе совершенного мошенничества, всех известных либо установленных в ходе работы СОГ абонентских номерах, с которых был произведен звонок, номера, на которые перечислялись денежные средства, номера банковских карт (счетов), либо анкетные данные получателей безадресных денежных переводов, с указанием платежной системы (QIWI, Яндекс, WEBMONEY, МОБИ деньги и др.), наименования сайтов, социальных сетей, адресов электронной почты, при помощи которых осуществлялось общение заявителя и виновного лица.

Документирование оперативно-розыскной деятельности на первоначальном этапе раскрытия мошенничеств общеуголовной направленности в первую очередь осуществляется в рамках материала проверки сообщения о преступлении.

После приема заявления (сообщения) о совершенном мошенничестве сотруднику оперативного подразделения необходимо установить обстоятельства его совершения (место, время, способ, приметы лиц,

⁵¹ О мерах по усилению борьбы с преступными посягательствами на автотранспортные средства" (вместе с "Инструкцией по розыску автотранспортных средств") : приказ МВД РФ от 17.02.1994 № 58 (в ред. от 12.09.2000) // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 31.03.2019).

подозреваемых в мошенничестве), данные заявителя, возможных очевидцев. Таким образом, в зависимости от вида совершенного мошенничества оперуполномоченный либо следователь (дознатель), входящий в состав дежурной следственно-оперативной группы получает от заявителя объяснения с учетом обстоятельств совершенного деяния.

При получении письменного объяснения от заявителя о *мошенничестве, совершенном в общественных местах и жилом секторе* необходимо выяснить:

- куда направлялся, что делал заявитель до момента встречи с лицом (лицами), подозреваемым(и) в совершении мошенничества;
- в какое время, каком месте и при каких обстоятельствах произошла эта встреча;
- каким образом данное лицо (лица) привлекло(и) внимание заявителя (какая ситуация была смоделирована; что он(и) говорил(и) пострадавшему; какие действия совершали, чтобы привлечь его внимание); зафиксировать подробности состоявшегося разговора, а также особенности разговора и речи (используемые выражения, наличие акцента, дефекты речи) преступника(ов); присутствовал ли кто-либо при этом разговоре;
- при наличии сведений о посещении лицом, подозреваемым в совершении преступления, квартиры или другого помещения - его местонахождение непосредственно в помещении, пути передвижения;
- в чем выражался обман и почему заявитель передал денежные средства или иное имущество; отразить обстоятельства передачи денежных средств или иного имущества, где, в какое время, кому они переданы, в какой сумме, какими купюрами; подробно описать внешность лица, получившего денежные средства (иных лиц, которые были с ним), может ли заявитель его (их) опознать (при возможности опознания – организует направление заявителя в подразделение ЭКЦ ГУ МВД России для составления композиционного портрета предполагаемого преступника, если этого не было сделано ранее сотрудниками органа дознания);

- какие действия подозреваемого(ых) или его (их) слова сформировали располагающее (доверительное) отношение к ним заявителя; какие гарантии или обязательства брали на себя подозреваемые;

- производились ли заявителем какие-либо записи в ходе контакта с подозреваемым, получались ли от последнего вещи, документы, расписки, с целью последующего их изъятия, назначения необходимых судебных экспертиз;

- кто мог быть очевидцем преступления, возможный адрес их нахождения;

- в каком направлении, на каком транспорте скрылись подозреваемые; выяснить модель, цвет, государственный знак автомобиля, внешность водителя, наличие на автомобиле каких-либо опознавательных знаков;

- является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Получение письменного объяснения от заявителя при проверке факта *дистанционного мошенничества, совершенного посредством телефонного звонка.*

Наиболее распространенный способ совершения такого мошенничества заключается в сообщении заявителю посредством телефонного звонка (на стационарный или мобильный телефон) от лица родственника или знакомого (голос звонящего взволнованный, часто очень похож на известный заявителю) о том, что он задержан сотрудниками полиции за совершение того или иного преступления или правонарушения (ДТП, хранение оружия или наркотиков, причинение вреда здоровью), но есть возможность за определенное вознаграждение «решить вопрос». Далее в разговор вступает другое лицо, которое представляется сотрудником правоохранительных органов, сообщает: какую сумму необходимо

перечислить, каким образом и куда. Денежные средства могут быть переданы заявителем курьеру (таксисту), перечислены безадресным переводом, на банковский счет (электронный кошелек) или на лицевой счет абонентского номера телефона. В ходе получения объяснения необходимо выяснить следующие обстоятельства: – дата, время поступления звонка с соответствующим содержанием;

– абонентский номер заявителя, на который был осуществлен звонок (стационарный, мобильный телефон);

– если звонок поступил на сотовый телефон или стационарный телефон с автоматическим определением номера, с какого номера телефона осуществлен звонок;

– дословное содержание разговора, кем представился звонивший, о чем говорил, что предлагал сделать;

– описание голоса звонившего (дефекты речи – хрипота, картавость, шепелявость, заикание), какова была интонация голоса, разговаривал ли он шепотом или обычным тембром; какие особенности, странности в интонации, произношении звуков, в обращении заметил заявитель, использование в разговоре специальных терминов, специфических речевых оборотов; по каким приметам заявитель сможет опознать голос звонившего;

– качество связи (помехи, пропадала слышимость, разговор прерывался, хорошо или плохо был слышен голос и др.); – что именно (по возможности дословно) сам заявитель сообщил неизвестному, представившемуся родственником, а также лицу, представившемуся сотрудником полиции;

– как неизвестный узнал точный адрес места жительства заявителя: последний сам назвал его, либо неизвестный, представившийся сотрудником полиции, уже знал его место жительства;

– как долго по времени длился телефонный разговор с неизвестным (сверить в последующем с данными детализации телефонных переговоров);

– через какой период времени после окончания разговора подъехал звонивший неизвестный к дому заявителя;

– описание голоса неизвестного лица (курьера, таксиста), какие особенности, странности в интонации, произношении звуков, в обращении к нему он заметил; по каким приметам заявитель сможет опознать его голос;

– подробное описание его черт лица, рук, особенностей телосложения, походки, поведения, по которым заявитель сможет его опознать (составить композиционный портрет личности), одежды;

– если передача денег осуществлялась в жилище заявителя, установить: когда неизвестный курьер (таксист) зашел в квартиру, то до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы, задавал ли заявитель ему какие-либо вопросы, интересовался ли судьбой своего родственника, например, путем постановки вопроса, когда родственника «освободят» от уголовной ответственности и пр.;

– сообщал ли заявитель неизвестному точную сумму денег, которую передал ему, для каких целей он передает ему эти деньги;

– судя по поведению неизвестного, был ли тот осведомлен о содержимом переданном ему, о причинах (целях) передачи ему денежных средств;

– пересчитывал ли заявитель, неизвестное лицо на месте передачи деньги;

– как заявитель упаковал деньги;

– звонил ли неизвестный в момент получения денег кому либо, что говорил;

– провожал ли заявитель неизвестного, наблюдал ли за направлением, в котором неизвестный покинул место расположения его дома, передвигался ли неизвестный на автомобиле (какой модели);

– какую сумму денег он хранит дома;

– как часто его посещает родственник, якобы, «попавший в беду», как может охарактеризовать его, характер их взаимоотношений, чем родственник занимается, каков источник дохода родственника, есть ли среди круга общения родственника лица, ранее привлекавшиеся к уголовной ответственности, отбывавшие наказание, в частности, в местах лишения свободы;

– кто из посторонних лиц посещает или посещал в последнее время заявителя (социальный работник, медицинский работник, представитель организации по вопросам пенсионного обеспечения и пр.), его полные анкетные данные, контактные номера телефонов, как может охарактеризовать его, когда последний раз тот посещал заявителя, знаком ли социальный работник (медицинский работник) с его родственником, якобы «попавшем в беду», знает ли социальный работник, где проживает родственник, якобы «попавший в беду», как часто навещает заявителя.

При осуществлении безадресного перевода, необходимо выяснить, на чье имя переводились деньги, полные установочные данные получателя, истребовать у заявителя квитанцию о переводе.

Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты необходимо выяснить:

- абонентский номер телефона или номер банковской карты, с которой переведены денежные средства (дата получения, срок действия, вид платежной системы, банк-эмитент карты, наличие договора банковского счета и документов об оформлении банковской карты), истребовать данные документы, чек или квитанцию о переводе;

- абонентский номер телефона или номер банковской карты, на которую переведены денежные средства;

- размер суммы перевода денежных средств;

- предпринятые заявителем действия после обнаружения факта мошеннических действий;

- является ли ущерб значительным для заявителя.

Получение письменного объяснения от заявителя при проверке факта *дистанционного мошенничества, совершенного с использованием информационно-телекоммуникационной сети Интернет.*

В ходе получения объяснения необходимо установить:

- дату и время обнаружения объявления (получения ссылки на соответствующий Интернет-ресурс), если возможно - найти объявление в Интернете и зафиксировать его адрес (еще раз пройти по интернет-ссылке), сделать снимок экрана, приобщить его к материалам проводимой проверки;
- с использованием какого технического устройства заявитель выходил на сайт с размещенным объявлением (переходил по интернет-ссылке) – стационарного компьютера, мобильного устройства;
- какие характеристики продаваемого товара были указаны в объявлении о продаже;
- какие условия купли-продажи содержались в объявлении (условия о предоплате, оплате товара, сроках и видах его поставки, ответственности сторон);
- какие контактные данные продавца были указаны в объявлении о продаже;
- имелись ли отзывы, комментарии к объявлению о продаже;
- сохранились ли у него данные объявления (№ объявления, ID страницы);
- каким образом, когда (дата, время) заявитель связался с продавцом;
- как продавец представился;
- где, со слов продавца, он находился;
- известно ли ему место нахождения товара;
- отразить подробное содержание разговора с продавцом;
- что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;
- описание голоса продавца, сможет или нет его опознать (по каким приметам);

– когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил на какой счет (№ счета, либо банковской карты, открытые на чье имя) денежные средства в счет оплаты за якобы приобретаемый товар;

– если заявитель осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет», установить место входа потерпевшего в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, wi-fi-роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в этот день заявителю услуги доступа в Интернет);

– дата и место открытия счета (банковской карты), с которой заявитель перечислил денежные средства;

– каким образом известил «продавца товара» о перечислении денежных средств на указанную им банковскую карту (электронный кошелек);

– что именно ему сообщил после подтверждения оплаты (перечисления денег на банковскую карту виновного) «продавец»;

– в какой период времени, куда прибыл для получения (как ему казалось) приобретенного товара;

– когда он осознал, что в отношении него было совершено мошенничество, в результате которого похищены принадлежащие ему денежные средства;

– предпринятые заявителем действия после обнаружения факта мошеннических действий;

– является ли ущерб значительным для заявителя.

Получение письменного объяснения от заявителя при проверке факта *дистанционного мошенничества, совершенного с использованием вредоносного программного обеспечения.*

В ходе опроса необходимо выяснить:

- время, место и обстоятельства хищения денежных средств;
- реквизиты банковской карты, с которой совершено хищение денежных средств, а также подключенной услуги «Мобильный банк» с указанием номеров телефонов, к которым она привязана;
- если услуга подключена самим заявителем, то с какого времени и каким способом (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);
- с какого времени заявитель пользуется абонентским номером, к которому данная услуга подключена, т.к. не исключается перевыпуск номера оператором связи после истечения 6 месяцев неиспользования абонентского номера с оформлением номера на иное лицо;
- модель телефона, подключенного к услуге «Мобильный банк», используемая операционная система в телефоне («Андроид», «IOS» (Apple) или иное);
- наличие установленных антивирусных программ на мобильном устройстве;
- какие мобильные приложения устанавливались в последнее время, способ установки (из официальных источников (сайтов) «AppStore» (Apple), «PlayMarket» (GooglePlay), с сайта банка-имитента банковской карты (банковского продукта, в случае, например, открытия банковского счета без выпуска банковской карты);
- совершались ли операции через мобильное устройство (телефон, планшет) или компьютер, вводились ли иным способом данные карты или хранились сведения о ней в устройствах;
- осуществлялся ли с данного устройства доступ в сеть Интернет, в том числе автоматически (например, при установке графика автоматического обновления приложений, то каких именно приложений и пр.);
- осуществлял ли кто-либо с использованием данных банковской карты (номера, срока действия, данных владельца, CVC/CVV2-кода (три цифры

расположенные на обратной стороне банковской карты)) заявителя покупку товаров, заказ услуг через Интернет;

- поступали ли на мобильное устройство сообщения, содержащие ссылки на Интернет-ресурсы, если да, то когда, от кого, содержание сообщений, осуществлялся ли переход по данным ссылкам, если да, то каков результат (было установлено приложение, установка приложения неожиданно прервалась, мобильное устройство «зависло», потребовалась перезагрузка, приложение «попросило» ввести определенные данные и пр.);

- ремонтировалось ли устройство до или после обнаружения факта хищения, где, кем;

- поступали ли сообщения о снятии денежных средств, их содержание, номер с которого они были отправлены;

- местонахождение мобильного телефона в настоящее время, а также желает ли заявитель добровольно предоставить его для производства компьютерной экспертизы с указанием необходимых паролей;

- обращался ли заявитель в банк, имеются ли у него выписки о движении денежных средств по карте, ответы по обращениям (в случае наличия таковых приобщить их к материалам проводимой проверки);

- является ли ущерб значительным для заявителя.

В ходе проведения ОРМ «Опрос» возможно получение объяснений от свидетелей – очевидцев преступления, родственников заявителя, иных свидетелей, которые располагают какой-либо информацией, имеющей значение для раскрытия преступления. При необходимости во время ОРМ «Отождествление личности» и «Сбор образцов для сравнительного исследования» следует направить их на составление композиционного портрета подозреваемого лица, предъявление фотокартотеки лиц, ранее судимых и состоящих на учете в органах внутренних дел. Объяснения могут быть получены и от лиц, обслуживающих платежные терминалы, работников банков о механизмах перевода денежных средств и др.

После получения объяснения действия сотрудника оперативного подразделения в рамках материала проверки сообщения о преступлении складываются также исходя из характера совершенного мошенничества.

Так при поступлении сообщения о *мошенничестве, совершенном в общественном месте или жилом секторе* сотрудник оперативного подразделения принимает меры по установлению лиц, совершивших преступление, их розыску и доставлению в орган внутренних дел; проверяет по оперативно-справочным, криминалистическим и экспертно-криминалистическим учетам данные, полученные в ходе проверки сообщения о преступлении, оперативно-розыскных мероприятий и первоначальных следственных действий, например, об аналогичных преступлениях, схожих по способу совершения, о лицах, ранее судимых за аналогичные преступления, склонных к их совершению и состоящих на учете по месту жительства и др.

Осуществляет постановку на учет похищенных вещей, имеющих индивидуальные признаки, и объектов экспертно-криминалистических учетов⁵²; оказывает содействие подразделениям охраны общественного порядка в раскрытии преступления; ориентирует лиц, изъявивших согласие оказывать содействие органам, осуществляющим оперативно-розыскную деятельность на безвозмездной основе, об обстоятельствах совершенного преступления и подозреваемых в нем лицах.

В составе СОГ под руководством следователя (дознателя) участвует в осмотре места происшествия: в необходимых случаях организует охрану места происшествия до приезда и в процессе работы СОГ с целью недопущения утраты криминалистически значимой информации и

⁵² Об утверждении Наставления по ведению и использованию централизованных оперативно-справочных, криминалистических и розыскных учетов, формируемых на базе органов внутренних дел Российской Федерации : приказ МВД России, Минюста РФ, МЧС РФ, Минфина РФ, Минобороны РФ, ФСБ РФ, ФСКН РФ, ФСО РФ, СВР России, ФТС РФ, ФМС России, Государственной фельдъегерской службы РФ, СК РФ, Генпрокуратуры РФ от 12.02.2014 № 89 дсп/19 дсп/73 дсп/1 адсп/113 дсп/108 дсп/75 дсп/93 дсп/19 дсп/324 дсп/113 дсп/63 дсп/14/95 дсп // СТРАС «Юрист» (дата обращения: 25.05.2019).

искажения обстановки на месте происшествия; оказывает содействие следователю (дознавателю) и эксперту (специалисту) в установлении и фиксации криминалистически значимой информации на месте происшествия; принимает меры к выявлению свидетелей, установлению обстоятельств преступления в целях принятия незамедлительных мер по информированию нарядов, задействованных в системе единой дислокации, и их ориентированию на поиск и задержание виновных; проводит поквартирный обход, опрос граждан на месте происшествия с целью выяснения обстоятельств происшествия и выявления возможных свидетелей преступления; совместно с участковым уполномоченным полиции, обслуживающим данную территорию, устанавливает места возможного нахождения камер наружного видеонаблюдения (иных средств видео фиксации – на месте происшествия, прилегающей к нему территории, в торговых точках, офисных помещениях, административных зданиях, подъездах жилых домов, автостоянках, банкоматах); о результатах проделанной работы незамедлительно информирует руководителя СОГ.

Сотрудник оперативного подразделения при получении заявления (сообщения) о *дистанционном мошенничестве, совершенном посредством телефонного звонка*, проводит следующие оперативно-розыскные и иные мероприятия. С помощью сайта Федерального агентства связи «Россвязь» по ссылке: (http://www.rossvyaz.ru/activity/num_resurs/registerNum/) или www.kody.su на вкладке «Коды сотовых операторов» и иных сайтах устанавливает принадлежность оператору и региону абонентских номеров, использовавшихся при совершении мошенничества. Далее устанавливает анкетные данные владельца абонентского номера, который использовался при совершении преступления, для чего направляет запрос в соответствующие бюро специальных технических мероприятий органа внутренних дел (далее – БСТМ)⁵³ с указанием необходимости обращения к

⁵³ Например, предоставление сведений об анкетных данных владельцев абонентских номеров операторов связи Кировской области входит в компетенцию БСТМ УМВД

соответствующему оператору сотовой связи за предоставлением сведений о пользователе услуги связи: Ф.И.О. абонента, дата рождения, адрес регистрации, паспортные данные, копия договора об оказании услуг связи, с указанием даты его заключения и расторжения.

Таким образом, оперуполномоченный устанавливает территориальность нахождения виновного лица:

1) Подготавливает постановление о ходатайстве перед судом о получении разрешения на проведение оперативно-розыскного мероприятия «Наведение справок», (ОРМ «Снятие информации с технических каналов связи», ограничивает конституционные права человека и проводится БСТМ только по заданиям в рамках дел оперативного учета) с целью получения информации о соединениях абонентских номеров, используемых при совершении преступления, с указанием местонахождения базовых станций и IMEI телефонных аппаратов, в которых использовались абонентские номера, получение сведений об изменении баланса лицевого счетов абонентских номеров, а также статистики соединений установленных IMEI телефонных аппаратов, с указанием базовых станций.

2) Получает постановление суда и с соответствующим запросом направляет его в БСТМ.

При получении ответа из БСТМ в зависимости от дальнейшего движения денежных средств по лицевому счету абонентского номера устанавливает место их обналичивания, для чего при перечислении похищенных денежных средств на счет банковской карты подготавливает в соответствии с частью 5 статьи 26 Федерального закона от 02.12.1990

России по Кировской области, которое также имеет возможность предоставить запрашиваемые сведения по абонентским номерам оператора «Вымпелком Билайн», независимо от региональной принадлежности. В случаях необходимости установления владельцев номеров, принадлежащим номерным емкостям иных операторов связи, расположенных за пределами Кировской области, направляется запрос за подписью руководителя территориального органа МВД России на районном уровне в БСТМ территориального органа МВД России по интересующему субъекту Российской Федерации.

№395-1 «О банках и банковской деятельности»⁵⁴ постановление о ходатайстве перед судом о получении разрешения на проведение ОРМ «Наведение справок» в кредитной организации с целью получения сведений о принадлежности и месте открытия банковской карты, об операциях и авторизациях по банковской карте за интересующий период, о наличии подключенной услуги «Мобильный банк» с указанием абонентского номера, об IP-адресах регистрации и проведения операций в системе «Сбербанк Онлайн» по банковской карте за интересующий период. Далее оперуполномоченный получает постановление суда и с соответствующим запросом направляет его в банк-эмитент карты⁵⁵.

Кроме того, в ходе установления первичных обстоятельств совершенного преступления информацию о банковском счете, на который были перечислены похищенные денежные средства, можно получить из платежных документов, предоставленных заявителем, или из выписки о движении денежных средств по счету, которую заявитель лично может получить в банке обслуживания счета.

При подготовке постановлений и запросов необходимо иметь в виду, что номер банковской карты не совпадает с номером расчетного счета, к которому она «привязана». По первым 6-ти цифрам (bin), указанным в номере банковской карты, можно определить, каким кредитным

⁵⁴ О банках и банковской деятельности : Федеральный закон РФ от 02.12.1990 № 395-1 - ФЗ : в ред. от 03.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 04.05.2019).

⁵⁵ Следует отметить, что в ряде регионов осуществляется электронный документооборот с банковскими учреждениями. Так, организовано подключение МВД по Республике Карелия к единому центру обработки запросов ПАО «Сбербанк», что значительно сократило сроки предоставления запрашиваемой информации. В Управлении уголовного розыска МВД по Республике Марий Эл с января 2016 года используется система удаленного доступа «SBERSIGN», обеспечивающая направление запросов по установлению владельцев банковских счетов и движению по счетам в электронном виде, по которым ответы работниками ПАО Сбербанк предоставляются в кратчайшие сроки (от 1 до 7 суток) // Информационное письмо о положительном опыте при раскрытии и расследовании мошенничества, совершенного с использованием средств мобильной связи, подготовленное ГУУР МВД России (исх. № 6/4-5238 от 09.06.2018).

учреждением выдана банковская карта. Данную информацию можно получить, перейдя по ссылке: <https://www.bindb.com/bin-database.html>.

Необходимо учесть, что не всегда похищенные денежные средства перечисляются мошенником на расчетный счет банка, зачастую злоумышленники стали использовать электронные кошельки одной из платежных систем (QIWI, Яндекс, WEBMONEY, МОБИ деньги и др.) В данном случае необходимо подготовить постановление о ходатайстве перед судом о получении разрешения на проведение ОРМ «Наведение справок» с целью получения информации о принадлежности электронного кошелька, IP-адресах его регистрации и использования с указанием времени, а также движении по нему денежных средств, с указанием расчетных счетов и номеров банковских карт получателей в интересующий период. Как только постановление суда будет получено, оно с соответствующим запросом направляется в компанию регистратор электронного кошелька.

В случае, если *мошенничество, совершено с использованием сети Интернет*, проводятся следующие мероприятия:

Во-первых, необходимо установить принадлежность доменного имени⁵⁶, адресов электронной почты, анкетные данные владельца абонентского номера, которые использовались при совершении преступления, для чего направляет запрос в БСТМ с указанием необходимости предоставления сведений о принадлежности конкретного доменного имени, электронного почтового ящика, а также обращения к соответствующему оператору сотовой связи за предоставлением сведений о пользователе услуги связи: Ф.И.О. абонента, дата рождения, адрес регистрации, паспортные данные, копия договора об оказании услуг связи, с указанием даты его заключения и расторжения.

Во-вторых, устанавливается территориальность нахождения виновного лица:

⁵⁶ Домен (доменное имя) – это обозначение символами, предназначенное для адресации сайтов в целях обеспечения доступа к информации, размещенной в сети Интернет, например, qwert.ru.

– В случае использования для совершения дистанционного мошенничества электронных торговых площадок, например, «Avito.ru», направить запрос владельцу данного сайта (ООО «КЕХ ЕКОММЕРЦ») на предоставление сведений об IP-адресе⁵⁷ размещения объявления, с указанием даты и времени, контактных данных, указанных при регистрации на сайте, а также наличие жалоб на данное объявление.

– При использовании социальных сетей направить запрос администратору социальной сети на предоставление сведений об IP-адресах регистрации и использования учетной записи, контактных данных, указанных при регистрации, об учетных записях, зарегистрированных с использованием интересующего абонентского номера (электронного почтового ящика).

– При установлении IP-адреса лица, подозреваемого в совершении преступления, при выходе в сеть Интернет и регистрации на различных ресурсах, запросить у провайдера⁵⁸ следующие сведения: кому предоставлена услуга доступа в сеть Интернет; геолокацию данного лица, т.е. населенный пункт и конкретный адрес точки доступа; копию заключенного договора об оказании услуги; контактные данные лица, с которым заключен договор, а при наличии и копии документов, удостоверяющих его личность. Сведения о принадлежности IP-адреса к оператору информационной системы (провайдеру) можно получить на сайте компании ООО «Регистратор доменных имен РЕГ.РУ», перейдя по ссылкам: <https://www.reg.ru/whois> или <https://www.nic.ru/whois>.

Если общение происходило с использованием абонентского номера или он был указан как контактный, подготавливает постановление о ходатайстве перед судом о получении разрешения на проведение ОРМ

⁵⁷ IP-адрес (сокращение от англ. InternetProtocolAddress) – уникальный идентификатор (адрес) устройства (обычно компьютера), подключённого к локальной сети или Интернету.

⁵⁸ Провайдер (от англ. Internet service provider, сокр. ISP) – организация, предоставляющая услуги доступа к сети Интернет и иные связанные с Интернетом услуги.

«Наведение справок» с целью получения информации о соединениях абонентского номера с указанием местонахождения базовых станций и IMEI телефонного аппарата, в котором использовался абонентский номер, статистики соединений установленного IMEI телефонного аппарата с указанием базовых станций. Получает постановление суда и с соответствующим запросом направляет его в БСТМ.

Сотрудником оперативного подразделения могут быть проведены мероприятия по фиксации голоса подозреваемого лица. Для этого может быть использовано любое техническое средство записи телефонных разговоров, состоящее на балансе органа внутренних дел, в том числе имеющееся в его распоряжении либо заявителя, например, телефон с установленной программой (диктофон) для записи переговоров. При осуществлении звонка подозреваемому лицу предпочтительно использовать абонентский номер (SIM-карту) заявителя, при отсутствии такой возможности – любой другой абонентский номер, в том числе стационарный телефон. При «легендированном» разговоре с подозреваемым лицом необходимо представиться родственником, соседом, по возможности увеличить продолжительность переговоров, не используя резкий стиль разговора, уточнить возможность возврата денежных средств, сослаться на трудное финансовое положение. Ни при каких обстоятельствах не сообщать, что заявитель обратился либо планирует обратиться в полицию, по возможности убедить собеседника в том, что заявитель поверил в предложенный им предлог, с помощью которого были похищены денежные средства, и готов ожидать их возврата. Сотрудник оперативно подразделения докладывает рапортом о проведенных мероприятиях руководителю органа внутренних дел и принимает меры к сохранению полученной аудиозаписи для последующего приобщения к материалам уголовного дела.

Также необходимо установить место обналичивания похищенных денежных средств.

Необходимо отметить, что в случае, если в действиях лиц(а) усматриваются признаки совершения преступления, а также, если задокументировать действия мошенников не представляется возможным в ходе проведения гласных оперативно-розыскных мероприятий и процессуальных действий, то на данном этапе перед сотрудником оперативного подразделения стоит задача о заведении дела оперативного учета⁵⁹. Дело оперативного учета – это специальные накопители информации (папки) для сбора (накопления) и систематизации документов, содержащих данные о лицах и фактах, представляющих оперативный интерес, сведения (материалы), отражающие основания, условия, планы, организацию, тактику и результаты проведения ОРМ в целях решения задач ОРД⁶⁰.

В таком случае последующее документирование преступных действий будет производиться в рамках данного дела.

Подводя итог рассмотрения особенностей документирования общеуголовных мошенничеств на первоначальном этапе раскрытия, необходимо отметить, что данный этап начинается с принятия заявления оперативным дежурным дежурной части территориального органа МВД России и осуществляется, в первую очередь, в рамках материала проверки сообщения о преступлении. Далее в зависимости от вида совершенного мошенничества оперуполномоченный либо следователь (дознатель), входящий в состав дежурной следственно-оперативной группы, получает от заявителя объяснение с учетом обстоятельств совершенного деяния, которое должно максимально полно отражать все нюансы противоправного деяния. Необходимо отметить, что успех документирования мошенничеств общеуголовной направленности во многом зависит от четкого и полного проведения первоначальных мероприятий, таких как: использование имеющихся учетов МВД России, ориентирование лиц, оказывающих конфиденциальное содействие (сотрудничество), подворно-поквартирный

⁵⁹ Далее – ДОУ.

⁶⁰ К.К. Горяинов, В.С. Овчинский, Г.К. Синилов. Теория оперативно-розыскной деятельности: учебник. М: НИЦ ИНФРА-М, 2016. - С. 414.

обход, установление мест возможного нахождения камер наружного видеонаблюдения, ОРМ «Опрос», ОРМ «Наведение справок», ОРМ «Исследование предметов и документов». Именно полнота полученной информации поможет всесторонне оценить обстоятельства преступления и построить правильную линию последующих мероприятий по раскрытию общеуголовных мошенничеств.

§3. Документирование мошенничеств общеуголовной направленности на последующем этапе раскрытия

Рассматривая вопрос о фиксации сведений, полученных в результате ОРД ОВД, следует отметить, что в юридической науке этот вопрос практически не изучен. Лишь в ходе рассмотрения вопросов документирования ОРД, исследователи говорят о том, что фиксация является одним из элементов оперативно-розыскного познания наряду со сбором, изучением и оценкой фактических данных, полученных в ходе оперативно-розыскных мероприятий.⁶¹ Документирование выступает средством познания и составляет информационную основу ОРД, обеспечивая достижение целей и решение её задач. В Федеральном законе «Об оперативно-розыскной деятельности»⁶² термин «документирование» употребляется лишь в названии статьи 10, не упоминаясь в её тексте. Однако по смыслу под документированием в ОРД можно понимать осуществляемый по делам оперативного учета процесс сбора и систематизации сведений, проверки и оценки результатов ОРД, а также принятия на их основе подходящих решений органами, её осуществляющими. В соответствии с содержанием ФЗ об ОРД, выделим несколько групп объектов, при познании которых в ОРД осуществляется документирование.

⁶¹ Молдавский, М. В. Представление результатов оперативно-розыскной деятельности и их реализация в уголовном судопроизводстве [Текст] : дис. ... канд. юрид. наук. – СПб., 2003.

⁶² Об оперативно-розыскной деятельности: Федеральный закон РФ от 12.08.1995 №144-ФЗ : в ред. от 06.07.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.05.2019). Далее – ФЗ об ОРД.

Во-первых, это объекты, связанные с производством по уголовному делу и обстоятельствами, подлежащими доказыванию в уголовном судопроизводстве (ст. 73 Уголовно-процессуального кодекса Российской Федерации), а также установление имущества, подлежащего конфискации.

Во-вторых, - события или действия (бездействия), создающие угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

В-третьих, - лица и обстоятельства, познаваемые в связи с осуществлением ОРД по основаниям, перечисленным в п. 4 - 6 ст. 7 ФЗ об ОРД.

К основным объектам, познаваемым при документировании, относятся события, лица и обстоятельства, устанавливаемые в соответствии с уголовно - процессуальным кодексом в связи с совершением преступлений. В этом плане документирование и в целом оперативно-розыскная деятельность подчинены целям уголовного судопроизводства, установленным уголовно - процессуальным законом. Таким образом, можно сделать вывод, что осуществляемое в рамках ОРД документирование выполняет функцию, способствующую достижению целей уголовного судопроизводства.

Кроме того, одной из основных задач процесса документирования является выявление преступлений и лиц, их совершивших. В ходе осуществления такой деятельности, органы, осуществляющие ОРД, обязаны принимать все меры по пресечению обнаруженных общественно опасных действий, раскрытию совершаемых или готовящихся к совершению преступлений.

Оперативно-розыскное документирование - это процесс, который состоит из следующих взаимосвязанных элементов:

- выявление данных, представляющих оперативный интерес (установление источников информации, определение тактических приемов, средств и инструментария получения информации);

- фиксация полученных данных (оформление полученной информации в целях: обеспечения сохранения информации, дальнейшего использования и обработки информации);
- проверка полученных данных (установление дополнительных источников получения информации, накопление информации, необходимой для решения стоящей задачи, установление на основе накопленной информации ее истинности или ложности);
- систематизация и оценка полученных данных (определение возможности использования (относимости и допустимости) сведений о фактах по конкретному рассматриваемому событию);
- обеспечение использования полученных данных (определение направления использования, определение тактики их использования) и др.

Оперативно – розыскное документирование должно соблюдать ряд требований:

1) соблюдение законности, т.е. документирование должно осуществляться в соответствии с федеральным законом «Об оперативно-розыскной деятельности», ведомственными нормативными актами, а также необходимо установить объективную истину по делу;

2) своевременность документирования преступных действий разрабатываемых 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;

3) Полнота документирования состоит в том, чтобы задокументировать преступные действия каждого из разрабатываемых в полном объеме;

4) Конспирация документирования преступных действий разрабатываемых состоит в том, чтобы все мероприятия по документированию осуществлялись в тайне от разрабатываемых и посторонних граждан.

Последующий этап документирования преступных действий по делам о мошенничествах общеуголовной направленности осуществляется в рамках обеспечения деятельности органов предварительного расследования по возбужденному уголовному делу. Документирование общеуголовных мошенничеств ведется, как правило, в рамках материалов и дел предварительной оперативной проверки с возможностью его перевода в иные ДОУ. На данном этапе возможно проведение оперативно-розыскных мероприятий, ограничивающих конституционные права граждан. Самыми информативными и эффективными, с точки зрения документирования преступных действий общеуголовных мошенников, являются такие оперативно-розыскные мероприятия: прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации и др.

Прослушивание телефонных переговоров – это оперативно-розыскное мероприятие, заключающееся в негласном контроле, аудиозаписи и прослушивании переговоров проверяемых лиц, ведущихся по телефонным линиям связи⁶³. Объектом данного ОРМ может выступать также и односторонняя передача речевой информации одного абонента на автоматическое записывающее устройство другого. К телефонным линиям связи относятся любые сети электросвязи общего пользования, предоставляющие соответствующие услуги населению; ведомственные сети связи, имеющие выход на сети связи общего пользования; выделенные сети связи непроизводственного назначения; сети подвижной радиотелефонной связи, а также системы глобальной подвижной персональной спутниковой связи. В правовом отношении для прослушивания телефонных переговоров не имеют значения технические характеристики используемых каналов связи (проводные линии, радиотелефонные каналы, каналы сотовой, спутниковой

⁶³ Сермягин К.А.. К вопросу о совершенствовании организации проведения оперативно-розыскных мероприятий «прослушивание телефонных переговоров» и «снятие информации с технических каналов связи» / Московский университет МВД России имени В.Я. Кикотя. 2017. N1(32). С. 172-173.

связи и т.д.). Абонентами телефонной связи являются граждане и организации, с которыми заключен договор об оказании услуг телефонной связи с выделением абонентского номера⁶⁴. Прослушивание телефонных переговоров проводится с использованием возможности подразделений специальных технических мероприятий органов, уполномоченных на осуществление оперативно-розыскной деятельности. Прослушивание телефонных переговоров является мероприятием ограниченного применения и в соответствии с ч. 2 ст. 23 Конституции РФ, а также ч. 2 ст. 8 ФЗ об ОРД может осуществляться только на основании судебного решения в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений.

Снятие информации с технических каналов связи – это оперативно-розыскное мероприятие, заключающееся в контроле и перехвате с помощью специальных технических средств текстовой, графической и иной информации, передаваемой проверяемыми лицами по телексным, факсимильным, селекторным, радиорелейным каналам передачи данных, системам персонального радиовызова (пейджинговая связь), а также линиям абонентского телеграфирования, IP-телефонии, электронной почте и иным каналам связи⁶⁵. Снятие информации с технических каналов связи проводится с использованием возможности подразделений специальных технических мероприятий органов, уполномоченных на осуществление оперативно-розыскной деятельности. В соответствии с ч. 4 ст. 6 и ч. 2 ст. 8 ФЗ об ОРД данное мероприятие осуществляется только на основании соответствующего судебного решения с использованием возможности подразделений специальных технических мероприятий органов, уполномоченных на осуществление оперативно-розыскной деятельности.

⁶⁴ Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» / под ред. А.И. Алексеева и В.С. Овчинского. М.: Проспект, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант»

⁶⁵ Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» / под ред. А.И. Алексеева и В.С. Овчинского. М.: Проспект, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант»

В результате проведения ОРМ «Прослушивание телефонных переговоров» органы, осуществляющие оперативно-розыскную деятельность, получают только речевую информацию, передаваемую по телефонным линиям связи, а в результате ОРМ «Снятие информации с технических каналов связи» осуществляется перехват иной информации, передаваемой проверяемыми лицами по телексным, факсимильным, селекторным, радиорелейным каналам передачи данных, системам персонального радиовызова (пейджинговая связь), а также линиям абонентского телеграфирования, IP-телефонии, электронной почте и иным каналам связи. Оперативно-розыскные мероприятия «Прослушивание телефонных переговоров» и «Снятие информации с технических каналов связи» дают возможность получить информацию о возможных соучастниках преступления, выявить неизвестные ранее, а также новые факты мошенничества, получить больше данных о личности мошенника, его местонахождении. Так, с помощью проведения ОРМ «Прослушивание телефонных переговоров», проведенного в рамках ДООУ по факту мошенничества посредством мобильной связи под предлогом «снятия порчи», оперативным сотрудникам удалось установить наличие соучастника преступления, роль которого заключалась во встрече с обманутыми гражданами, передача им «положительно заряженных» предметов, не имеющих материальной ценности (бутылки с водой, мыла, камней и т.д.) в обмен на денежные средства и перевод незаконно полученных средств на установленный расчетный счет. Личность гражданки впоследствии была установлена путем проведения ОРМ «Наведение справок». Полученные данные явились основанием для проведения комплексного оперативно – технического мероприятия «оперативная установка» в отношении гражданки К⁶⁶.

Оперативная установка как один из комплексов оперативно-розыскных мероприятий - это осуществляемые в процессе ОРД ОВД целенаправленное,

⁶⁶ ДООУ №72/18 от 14 марта 2018 года

систематическое визуальное или опосредованное (с использованием оперативно-технических средств) восприятие и фиксация значимых для решения задач оперативно-розыскной деятельности явлений, событий, фактов, процессов. В процессе установки могут выявляться:

- очевидцы преступления;
- непосредственно лица, совершающие преступления, и их участники;
- места сбыта похищенного имущества;
- тайники и места хранения материальных ценностей для дальнейшего обеспечения возмещения материального ущерба лицом;
- данные об образе жизни и криминальных связях подозреваемого лица;
- конспиративные места нелегального сбора организованных преступных формирований.

Еще одним немаловажным мероприятием является ОРМ «Получение компьютерной информации». Одной из предпосылок введения законодателем нового оперативно-розыскного мероприятия – получение компьютерной информации, послужил рост преступлений, в частности, мошенничества в сфере компьютерной информации. Получение оперативно значимой компьютерной информации предполагает обследование информационных объектов сети «Интернет», среди которых основными являются информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих. Это могут быть различные интернет сайты, социальные сети, форумы посвященные пропаганде криминогенной среды. При реализации обследования вышеперечисленных объектов, сотрудниками оперативно - розыскного органа, может быть получена информация, имеющая оперативный интерес. К примеру, различные интернет - ссылки на материалы, запрещенные к распространению предметов ограниченных в гражданском обороте, переписки лиц, которые уже осведомлены о готовящемся преступлении. Особое место занимают сетевые каналы коммуникации, задействованные преступниками для

координации действий с использованием электронной почты различных поисковых систем, ICQ, Skype, WhatsApp, Viber и т.п.

Таким, образом, получение компьютерной информации связано с применением особых способов доступа сотрудниками оперативно-розыскной деятельности к информационным объектам.

К таким способам, относится, во-первых, негласное применение специального программного обеспечения или оборудования, для конспиративного съема данных с компьютерных устройств, во-вторых оперативно-розыскной мониторинг сетевых информационных ресурсов. Данный мониторинг реализуется посредством автоматизированного поиска информации, сотрудниками органа осуществляющий оперативно-розыскную деятельность⁶⁷. В этой связи, можно обозначить, что под получением компьютерной информации следует понимать негласное оперативно - розыскное мероприятие, осуществляемое с использованием возможностей оперативно-технических подразделений.

Зачастую, в рамках проведения доследственной проверки у оперативно-розыскных органов имеется адрес электронной почты, с которой передавалась информация, связанная с совершением мошенничества. Оперативным сотрудникам необходимо получить информацию о лице, которое зарегистрировало данный адрес электронной почты на конкретном сайте в сети «Интернет», а также информацию о том, когда и с какого компьютерного устройства передавалась вышеуказанная информация. Для этого оперативно-розыскным органам необходимо провести такое ОРМ как «Наведение справок», по результатам которой у компаний, владеющих такой информацией, будут истребованы сведения о предполагаемом преступнике. В дальнейшем с помощью ОРМ «Получение компьютерной информации» информация о предполагаемом совершенном преступлении может быть получена с искомого компьютера.

⁶⁷ Баженов С.В. Оперативно-розыскное мероприятие «Получение компьютерной информации» // Научный вестник Омской академии МВД. №2. - С. 32

Кроме того, в настоящее время приобретает распространение положительный опыт направления международных запросов.

Зачастую преступники, совершающие такие преступления находятся за рубежом или имитируют свое присутствие на территории другого государства, чтобы скрыться от правосудия. Этот фактор необходимо учитывать при направлении международных запросов по линии Интерпола.

Раскрытие таких преступлений не требует от сотрудников ОВД специальных познаний в сфере высоких технологий. Достаточно иметь доступ к сети «Интернет» в качестве пользователя и следовать определенному алгоритму действий, в основном, состоящему в направлении запросов на установление ряда технических параметров, по которым в дальнейшем и будет изобличен преступник.

Информационное взаимодействие и направление запросов по линии Интерпола в процессе раскрытия преступлений с применением высоких технологий и сети Интернет осуществляется в соответствии с требованиями приказа МВД РФ от 6 октября 2006 года №786 «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола»⁶⁸. Взаимодействующие органы в процессе раскрытия преступлений направляют запросы по каналам Интерпола в правоохранительные органы иностранных государств - членов Интерпола о следующих преступлениях в области высоких технологий, имеющих международный характер, связанных с:

- 1) неправомерным доступом к компьютерной информации;
- 2) созданием, использованием и распространением вредоносных программ для ЭВМ;
- 3) нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети.

По соответствующим запросам может быть получена информация:

⁶⁸ Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД России от 06.10.2006 №786 // СТРАС «Юрист» (дата обращения: 26.04.2019).

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

Одним из наиболее важных факторов, которые следует учитывать при направлении запросов о предоставлении компьютерной информации в зарубежные государства, является время.

Практика показывает, что если с момента совершения преступления и до направления запроса по каналам Интерпола прошло более 6 месяцев, то получение данных от зарубежных компаний представляется крайне затруднительным, а в ряде случаев невозможным. Связанно это с тем, что законодательство большинства зарубежных государств предусматривает срок хранения компьютерной информации максимум 6 месяцев, в ряде государств сроки хранения не превышают 20 дней. Исходя из этого, крайне важно направить запрос в максимально короткие сроки.

Второй крайне важный критерий это законодательство зарубежных государств в области предоставления информации. Надо учитывать, что зарубежные государства имеют право отказать в предоставлении компьютерной информации. На данный момент в список стран, которые

предоставляют компьютерную информацию только на основании международного следственного поручения входят: США, Украина и Италия. Поэтому подготовка запросов в данные государства без соблюдения этих требований представляется нецелесообразной.

Также, в процессе проверки сообщения и оперативного сопровождения предварительного расследования, следователь (дознатель) вправе давать органу дознания обязательное для исполнения письменное поручение о проведении оперативно - розыскных мероприятий, о производстве отдельных следственных и иных процессуальных действий (пункт 4 части 2 статьи 38, пункт 1.1 части 3 статьи 41, часть 1 статьи 144 УПК РФ). Срок исполнения поручения не должен превышать 10 суток. Поручение о производстве оперативно-розыскных мероприятий исполняется в порядке, предусмотренном Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд⁶⁹. Результаты выполнения поручения о проведении оперативно-розыскных мероприятий могут быть доложены начальнику органа дознания рапортом, после чего приобщаются следователем (дознателем) к материалу проверки. Сообщение о выполнении поручения должно носить конкретный информативный характер. На сегодняшний день процент раскрываемости мошенничеств весьма низок (28,3%)⁷⁰, что вызвано рядом проблем, возникающими перед оперативными подразделениями.

Во-первых, в 90% случаев дистанционные мошенничества совершаются лицами, находящимися в другом регионе, что существенно затрудняет их поиск и своевременное задержание, так как злоумышленники используют следующие приемы, обеспечивающие сокрытие следов их

⁶⁹ Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд : приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 // СТРАС «Юрист» (дата обращения: 26.04.2019).

⁷⁰ Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2018. – Режим доступа: <https://мвд.рф/reports/item/12460100/>. - Дата доступа: 30.09.2018.

преступления: быстрая смена субъектом преступления sim-карт мобильной связи, банковских карт, оформление их с нарушением действующего законодательства на другое имя, постоянная смена места пребывания (мошенники-гастролеры), что сильно затрудняет установление личности и местонахождения мошенника. С целью оперативного задержания преступника необходима организация взаимодействия между территориальными органами и различными организациями, так как после совершения преступления действие sim-карт и движение денежных средств по банковским картам осуществляется в течение 1-3 суток, после чего носители уничтожаются (блокируются) и установить преступника силами и средствами оперативных подразделений не представляется возможным. В связи с чем, необходим оперативный обмен данными с кредитными организациями, операторами сотовой связи, регистраторами доменных имен, транспортными компаниями, и т.д. В настоящее время российским законодательством предусмотрена возможность обмена данными посредством электронного документооборота (Приказ МВД России № 615)⁷¹, но практически эта возможность не реализуется в полном объеме.

В настоящее время, соглашение об электронном документообороте в территориальных органах МВД России налажено только с ПАО «Сбербанк», в связи с большим количеством клиентов у данного коммерческого банка и постоянной необходимостью правоохранительных органов обращаться к этому юридическому лицу за получением информации, необходимой для раскрытия преступлений. Но следует отметить, что общеуголовные (в особенности дистанционные) мошенничества, требуют поддержания связи с огромным количеством организаций, число которых растет с каждым месяцем. Подписание соглашений с каждой из них не представляется возможным, и не является целесообразным, в связи с чем обмен информацией осуществляется только посредством направления запросов

⁷¹ Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации : приказ МВД России от 20.06.2012 № 615 (в ред. от 25.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 12.05.2019).

почтовыми отправлениями. Как правило, оперативно-значимая информация может быть получена только в течение одного-двух месяцев со дня их отправления, что затягивает как процесс предварительной оперативной проверки, так и оперативного сопровождения уголовных дел. В таком случае, считаем необходимым разработать меры, позволяющие эффективно использовать имеющиеся у оперативных подразделений силы и средства, а именно, усовершенствовать систему электронного документооборота с целью обмена данными без процедуры подписания соглашений о сотрудничестве. Кроме того, необходим регулярный анализ совершенных преступлений по способам их совершения, так как злоумышленники за короткий период не станут менять наработанную схему обмана граждан.

Во-вторых, несовершенство централизованных информационно-поисковых систем МВД России, которые не позволяют накапливать и систематизировать информацию о дистанционных мошенниках, а также препятствуют взаимодействию оперативных подразделений различных субъектов поиску злоумышленника при множественности эпизодов противоправного деяния. С целью устранения данной проблемы с 2017 года в Мурманской области внедрена тестовая информационно-поисковая система «дистанционные мошенничества», являющейся аналогом информационно-поисковой системы «СОДЧ», но в настоящее время неизвестно, когда эта системы будет распространена по всем регионам РФ уже в рабочем режиме.

В-третьих, недостаточная разработанность электронных платежных систем, таких как «QIVI- money», платежная система «Вконтакте», которые затрудняют работу по установлению данных о личности мошенников, а также способствуют распространению данного негативного явления.

Таким образом, под документированием понимается осуществляемый по делам оперативного учета процесс сбора и систематизации сведений, проверки и оценки результатов ОРД, а также принятия на их основе подобающих решений органами, её осуществляющими. На последующем этапе раскрытия преступления документирование общеуголовных

мошенничеств ведется, как правило, в рамках материалов и дел предварительной оперативной проверки, а в исключительных случаях по иным делам оперативного учета. На данном этапе возможно проведение оперативно-розыскных мероприятий, ограничивающих конституционные права граждан, а именно: прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации; проведение комплекса оперативно-розыскных мероприятий, например, оперативной установки. Также набирает распространение положительный опыт международного сотрудничества.

ЗАКЛЮЧЕНИЕ

В ходе выполнения выпускной квалификационной работы были проделаны следующие этапы:

- 1) изучена оперативно-розыскная характеристика мошенничеств общеуголовной направленности;
- 2) рассмотрена организация информационного обеспечения оперативно-розыскной деятельности оперативных подразделений полиции по противодействию мошенничествам общеуголовной направленности;
- 3) дана характеристика оперативно-розыскного и иного документирования противоправных фактов, связанных с мошенничествами общеуголовной направленности;
- 4) исследована практика выявления замышляемых и подготавливаемых мошенничеств общеуголовной направленности;
- 5) выработан теоретико-прикладной подход по повышению эффективности тактики проведения оперативно-розыскных мероприятий по установлению лиц, причастных к мошенничествам общеуголовной направленности.

Таким образом, согласно ч.1 ст. 159 УК РФ «Мошенничество - это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием». Являясь формой хищения, мошенничество обладает отличительными признаками: 1) предмет посягательства (имущество либо право на имущество); 2) способ совершения преступления (обман либо злоупотребление доверием); 3) добровольная передача имущества потерпевшим.

Российское уголовное законодательство в Особенной части УК РФ выделяет «специальные виды мошенничества». Так, например, в УК РФ в статье 159.1. «Мошенничество в сфере кредитования», в статье 159.2. «Мошенничество при получении выплат», в статье 159.3. «Мошенничество с использованием платежных карт», в статье 159.5. «Мошенничество в сфере

страхования», в статье 159.6. «Мошенничество в сфере компьютерной информации».

В науке существует следующая классификация мошенничества. Так, мошенничество делится на общеуголовное и экономическое. Общеуголовные мошенничества – категория преступлений, связанная с хищением чужого имущества или приобретением права на чужое имущество путем обмана или злоупотребления доверием, рассмотрение которой подлежит компетенции оперативных подразделений уголовного розыска. Мошенничества общеуголовной направленности на современном этапе развития обладают некоторыми особенностями: межрегиональный и международный характер, высокий уровень организованности, высокая латентность, зачастую виктимное поведение потерпевших, множество способов обмана и др. Кроме того, необходимо отметить серьезные недостатки в статистическом учете ФКУ ГИАЦ МВД России, так как в виду ограниченности данных, нельзя с точностью оценить картину преступности по линии общеуголовных мошенничеств, а в виду этого сложно построить эффективную борьбу с указанными преступлениями. Необходимо отметить, что мошенничества в настоящее время подразделяются на дистанционные и контактные, в свою очередь охватывая множество различных способов их совершения.

Рассматривая непосредственно личность мошенника, стоит отметить, что это, прежде всего, «коммерческий» тип преступников. Мошенники совершают преступления без применения насилия, с использованием заведомо ложных сведений. В своем общественном положении мошенники являются профессионалами высокого или среднего уровня, они талантливые артисты, находчивые и изворотливые, быстрые в действиях, нешаблонно мыслящие, имеющие образование, не злоупотребляют спиртным и наркотиками, отличаются психологической устойчивостью.

Выявление фактов мошенничества состоит из нескольких этапов: получение первичных сведений, их проверка и анализ, а также принятие решения по результатам проверки. Для получения первичных сведений в

первую очередь используется поиск по информационным ресурсам сети «Интернет» с применением разного рода поисковых систем (Google, Yandex, Rambler и т. п.). Также искомую информацию можно добыть при взаимодействии с оперативными подразделениями ФСИН России, в связи с тем, что около 60% мошенничеств с использованием средств сотовой связи совершается именно осужденными, находящимися в местах лишения свободы. При выявлении лиц, занимающихся бесконтактным мошенничеством, оперативным сотрудникам следует иметь в виду, что таким образом осуществляют преступную деятельность хорошо организованные группы, где прослеживается иерархическая организация, когда все функции участников преступной деятельности четко распределены.

Под документированием понимается осуществляемый по делам оперативного учета процесс сбора и систематизации сведений, проверки и оценки результатов ОРД, а также принятия на их основе подходящих решений органами, её осуществляющими.

Процесс документирования общеуголовных мошенничеств на первоначальном этапе раскрытия начинается с принятия заявления оперативным дежурным дежурной части территориального органа МВД России и осуществляется, в первую очередь, в рамках материала проверки сообщения о преступлении. Далее в зависимости от вида совершенного мошенничества оперуполномоченный либо следователь (дознатель), входящий в состав дежурной следственно-оперативной группы, получает от заявителя объяснение с учетом обстоятельств совершенного деяния, которое должно максимально полно отражать все нюансы противоправного деяния. Необходимо отметить, что успех документирования мошенничеств общеуголовной направленности во многом зависит от четкого и полного проведения первоначальных мероприятий, таких как: использование имеющихся учетов МВД России, ориентирование лиц, оказывающих гласное и негласное содействие (сотрудничество), подворно-поквартирный обход, установление мест возможного нахождения камер наружного

видеонаблюдения, ОРМ «Опрос», ОРМ «Наведение справок», ОРМ «Исследование предметов и документов». Именно полнота полученной информации поможет всесторонне оценить обстоятельства преступления и построить правильную линию последующих мероприятий по раскрытию общеуголовных мошенничеств.

На последующем этапе раскрытия преступления документирование общеуголовных мошенничеств ведется, как правило, в рамках дела предварительной оперативной проверки, дела оперативной разработки, а в исключительных случаях оперативно-поискового дела. На данном этапе возможно проведение оперативно-розыскных мероприятий, ограничивающих конституционные права граждан, а именно: прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации; проведение оперативно-технического мероприятия – оперативная установка. Также набирает распространение положительный опыт международного сотрудничества.

В выпускной квалификационной работе обозначена необходимость в усовершенствовании российского законодательства в области электронной торговли с целью минимизировать возможность использования преступниками интернет - пространства для совершения преступлений, в частности мошенничеств. А именно, ввести нормы, которые заставят электронные торговые площадки выступать гарантами при осуществлении купли-продажи, используя безопасные системы оплаты.

Также мы считаем необходимым ужесточить ответственность за совершение правонарушения, предусмотренного ст. 13.29 КоАП РФ «Заклучение договора об оказании услуг подвижной радиотелефонной связи неуполномоченным лицом» с целью минимизации теневого рынка sim-карт и, соответственно, предупреждения мошенничеств с использованием средств мобильной связи. Кроме того, необходимо указать на целесообразность создания специализированных групп, состоящих из сотрудников подразделений уголовного розыска, отдела «К» БСТМ МВД России и

представителей Роскомнадзора для проведения совместных проверок, в том числе с помощью мониторинга Интренет-ресурсов, направленных на выявление и документирование фактов нарушения законодательства в сфере связи, информационных технологий и массовых коммуникаций.

Нами выявлено несовершенство централизованных информационно-поисковых систем МВД России, которые не позволяют накапливать и систематизировать информацию о дистанционных мошенниках, а также препятствуют взаимодействию оперативных подразделений различных субъектов поиска злоумышленника, в виду чего следует провести работу по реализации имеющихся программных обеспечений по всем регионам России.

И в заключение, предлагаем разработать меры, позволяющие эффективно использовать имеющиеся у оперативных подразделений силы и средства, а именно, усовершенствовать систему электронного документооборота с целью обмена данными без процедуры подписания соглашений о сотрудничестве.

Комплексное осуществление вышеперечисленных мер позволит улучшить деятельность подразделений по борьбе с мошенничествами общеуголовной направленности.

Таким образом, поставленная цель исследовательской работы: разработка комплексных научно обоснованных предложений и рекомендаций по совершенствованию организационных и тактических основ оперативно-розыскной деятельности ОВД по выявлению и документированию преступлений, связанных с мошенничествами общеуголовной направленности, по нашему мнению, достигнута.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Законы, нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации от 12 декабря 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 05.02.2014 №2-ФКЗ) 2018 [Электронный ресурс] / СПС «КонсультантПлюс». - Режим доступа: <http://www.consultant.ru> (дата обращения: 12.05.2019).
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ : в ред. от 18.03.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019).
3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: в ред. от 01.04.2019 [Электронный ресурс] / СПС «КонсультантПлюс». - Режим доступа: <http://www.consultant.ru> (дата обращения: 12.05.2019).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: в ред. от 23.04.2019 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 12.05.2019).
5. Об оперативно-розыскной деятельности : Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ : в ред. от 06.07.2016 [Электронный ресурс] / СПС «КонсультантПлюс». - Режим доступа: <http://www.consultant.ru> (дата обращения: 12.05.2019).
6. Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ : в ред. от 03.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019).
7. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : Федеральный закон РФ от 20 августа 2004 г. № 119-ФЗ : в ред. от 07.02.2017 [Электронный ресурс] / СПС «КонсультантПлюс». - Режим доступа: <http://www.consultant.ru> (дата обращения: 20.04.2019).

8. О персональных данных : Федеральный закон РФ от 27 июля 2006 г. №152-ФЗ: в ред. от 31.12.2017 [Электронный ресурс] / СПС «КонсультантПлюс». - Режим доступа: <http://www.consultant.ru> (дата обращения: 20.04.2019).

9. О связи : Федеральный закон РФ от 07 июля 2003 г. № 126-ФЗ: в ред. от 27.12.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 07.04.2019).

10. О банках и банковской деятельности : Федеральный закон РФ от 02.12.1990 № 395-1 : в ред. от 27.12.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 04.05.2019)

11. О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности : указание Генпрокуратуры России № 853/11, МВД России № 5 от 25.12.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 31.03.2019).

12. О едином учете преступлений (вместе с «Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о преступлениях», «Положением о едином порядке регистрации уголовных дел и учета преступлений», «Инструкцией о порядке заполнения и представления учетных документов»): приказ Генпрокуратуры России № 39, МВД России № 1070, МЧС России № 1021, Минюста России № 253, ФСБ России № 780, Минэкономразвития России № 353, ФСКН России № 399 от 29.12.2005 : в ред. от 20.02.2014 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 31.03.2019).

13. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ МВД России от 19 июня 2012 г. № 608: в ред. от 14.08.2018 // СТРАС «Юрист» (дата обращения: 07.04.2019).

14. Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об

административных правонарушениях, о происшествиях: приказ МВД России от 29 августа 2014 № 736: в ред. от 07.11.2018 // СТРАС «Юрист» (дата обращения: 07.04.2019).

15. Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 24.10.2017 № 3 км: приказ МВД России от 29.11.2017 № 899 // СТРАС «Юрист» (дата обращения: 30.04.2019).

16. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд: приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 12.05.2019).

17. Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации : приказ МВД России от 20 июня 2012 г. № 615: в ред. от 25.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 12.05.2019).

18. О деятельности органов внутренних дел по предупреждению преступлений : приказ МВД России от 17 января 2006 г. № 19 : в ред. от 28.11.2017 // СТРАС «Юрист» (дата обращения: 12.05.2019).

19. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола: приказ МВД России от 6 октября 2006 г. №786 // СТРАС «Юрист» (дата обращения: 26.04.2019).

20. О мерах по усилению борьбы с преступными посягательствами на автотранспортные средства» (вместе с "Инструкцией по розыску автотранспортных средств"): приказ МВД РФ от 17 февраля 1994 г. №58: в ред. от 12.09.2000 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 31.03.2019).

21. Об организации работы по противодействию отдельным видам мошенничеств: письмо МВД России от 13 июля 2015 г. № 1/5562 // СТРАС «Юрист» (дата обращения: 30.04.2019).

22. Информационное письмо о положительном опыте при раскрытии и расследовании мошенничества, совершенного с использованием средств мобильной связи, подготовленное ГУУР МВД России (исх. № 6/4-5238 от 09.06.2018).

23. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 07.04.2019).

24. О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 : в ред. от 16.05.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 07.04.2019).

25. Дело № 1-826/2017// Архив Ленинского районного суда г. Кирова. - 2017. – Режим доступа:<https://sudact.ru>. Дата доступа: 03.05.2019.

26. Дело № 1-0745/2017// Архив Ленинского районного суда г. Кирова. - 2017. – Режим доступа: <https://sudact.ru> Дата доступа: 03.05.2019.

27. Дело № 1-228/2015// Архив Канашского районного суда Чувашской Республики. - 2015. – Режим доступа: <https://sudact.ru> Дата доступа: 03.05.2019.

II. Монографии, учебники, учебные пособия

28. Александров Ю. В., Гель А. П., Семаков Г. С. Криминология: курс лекций. – Киев: МАУП, 2002. – 295 с.

29. Ахмедшин Р. Л. Криминалистическая характеристика личности преступника: автореф. дис. ... д-ра юрид. наук. – Томск, 2016. – 20 с.

30. Зиннуров Ф.К. Криминология. Особенная часть: учебник /под общей редакцией Ф.К. Зиннурова. – 2-е изд., перераб. и доп. – Казань: КЮИ МВД России, 2016. – 525с.

31. Малков В.Д. Планирование в управлении органами внутренних дел. М.: Юрид. лит., 1976. - 174 с.

32. Молдавский, М. В. Представление результатов оперативно-розыскной деятельности и их реализация в уголовном судопроизводстве [Текст] :дис. ... канд. юрид. наук. – СПб., 2003. - 186 с.

33. Нуждин А. А. Расследование мошенничества, совершенного осужденными в учреждениях УИС с использованием средств сотовых систем подвижной связи :автореф. дис... канд. юрид. наук. Рязань, 2015. - 22 с.

34. Горяинов К.К., Овчинский В.С. Теория оперативно-розыскной деятельности: Краткие юридические курсы юридических наук / К.К. Горяинов, В.С. Овчинский. – 4-е изд., перераб. и доп. - М.: Норма: ИНФРА-М, 2017. - 190 с.

35. , Сенилов Г.К.. Теория оперативно-розыскной деятельности: учебник./ К.К. Горяинов, В.С. Овчинский, Г.К. Сенилов М: НИЦ ИНФРА-М, 2016. - 712 с.

36. Зуйков Г.Г. Основы научной организации управления и труда в органах внутренних дел. Учебное пособие / Г.Г. Зуйков, А.П. Ипакян, В.Д. Малков, Г.А. Туманов; Под ред.: Зуйков Г.Г. - М.: Юрид. лит., 1974. - 176 с.

37. Иванов Н.Н., Чиркова Л.В. Аналитическая деятельность в управлении органами и подразделениями внутренних дел. Уч. пос. М.: Московский университет МВД России, 2005. – 149 с.

38. Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» / под ред. А.И. Алексеева и В.С. Овчинского. М.: Проспект, 2017 [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант».

39. Туманов Г.А. Организация управления в сфере охраны общественного порядка / Г.А. Туманов - М.: Юрид. лит., 1972. - 232 с.

40. Шляхтин Е.П., Усманов И.М., Минзянова Д.Ф., Рашитов Л.Р. Сборник нормативных актов по оперативно-розыскным дисциплинам / сост. Е.П. Шляхтин, И.М. Усманов, Д.Ф. Минзянова, Л.Р. Рашитов. – Казань: КЮИ МВД России, 2017. – 398 с.

41. Шляхтин Е.П., Усманов И.М. Основы оперативно-розыскной

деятельности органов внутренних дел Российской Федерации: учебное пособие / авт. - сост. Е.П. Шляхтин, И.М. Усманов. – Казань. КЮИ МВД России, 2017. – 88 с.

42. Шляхтин, Е. П. Особенности борьбы с отдельными видами организованной преступности: лекция / Е.П. Шляхтин. – Казань: КЮИ МВД России, 2011. – 42 с. - Режим доступа: \\ Grandserver \ ЭЛЕКТРОННАЯ_БИБЛИОТЕКА \ Эл. библиот. для учебы \ Электронная библиотека КЮИ\ОРД\2011 Шляхтин лекция Орг. преступность.

III. Статьи, научные публикации

43. Абрамов М.А., Прокопов А.Г. Личность мошенника как основной элемент оперативно-розыскной характеристики.// Вестник Казанского юридического института. – 2015. – N 4(22). – С.73-76.

44. Анистратенко А.В. Понятие мошенничества как формы хищения // Вестник ВУиГ. - 2010. - №74. - С.57-65.

45. Антонян Ю. М., Эминов В. Е. Личность преступника. Криминологическое исследование. — М., 2010. — 368 с.

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

47. Гумаров И.А., Саеггараев В.Ф. Некоторые проблемы организации работы оперативных подразделений органов внутренних дел по противодействию мошенничествам общеуголовной направленности // Вестник Казанского юридического института МВД России. 2018. № 2(32). - С. 224-230.

48. Ермолович Д. В., Широких С. В. Некоторые поисковые социально-психологические признаки личности мошенника // Юридическая Россия. – № 5 (47). – С. 36-38.

49. Кара М. В. Характеристика лиц, которые совершают мошенничество // Право и Безопасность. – 2018. – № 5 (47) – С. 22-27.

50. Кудрявцев А.В., Крюков И.В. Некоторые особенности выявления мошенничеств, совершаемых в учреждениях УИС с использованием средств мобильной связи /Вестник Владимирского юридического института. 2017, №4(45), С. 21-24.

51. Лабутин А.А. Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. № 12. С. 50—55.

52. Петухов Б. В., Лунин Н. Н. К вопросу о понятии мошенничества // Юрист. – 2004. – № 3 – С. 12-16.

53. Сермягин К.А.. К вопросу о совершенствовании организации проведения оперативно-разыскных мероприятий «прослушивание телефонных переговоров» и «снятие информации с технических каналов связи» / Московский университет МВД России имени В.Я. Кикотя. 2017. N1(32). С. 172-173.

54. Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2019. – Режим доступа: <https://мвд.рф/reports/item/12460100/>. - Дата доступа: 17.04.2019.

55. Официальный сайт Министерства внутренних дел Российской Федерации // МВД России: [Электронный ресурс]. – 2019. – Режим доступа: <https://21.мвд.рф/news/item/500876/>. - Дата доступа: 03.05.2019.

56. Электронная торговая площадка: Википедия. URL:https://ru.wikipedia.org/wiki/Электронная_торговая_площадка (дата обращения: 03.05.2019).