МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ПРОТИВОДЕЙСТВИЮ ОТДЕЛЬНЫМ ВИДАМ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ ИНТЕРНЕТ)

Учебно-методическое пособие

КАЗАНЬ
КЮИ МВД России
2018

УДК
Д 11

Одобрено редакционно-издательским советом
Казанского юридического института МВД России

Рецензенты:

- кандидат юридических наук Родичев М.Л. (Санкт-Петербургский ун-тет МВД России;
- Костюнин В.А. (УНК МВД по РТ).

Д 11 Организация деятельности органов внутренних дел по противодействию отдельным видам преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть Интернет): учебное пособие / авт.-сост. И.М. Усманов, Е.П. Шляхтин. – Казань: КЮИ МВД России, 2018. – 169 с.
ISBN

В учебном пособии на основе системного и комплексного подхода проведен анализ практики противодействия оперативных и иных подразделений полиции территориальных и других органов МВД России наиболее часто совершаемых преступлений с использованием информационно-телекоммуникационных сетей таких как: бесконтактный сбыт наркотических средств и психоактивных веществ, а также мошенничества в сети Интернет. Деятельность правоохранителей исследована с учетом использования преступниками новых, так называемых, «бесконтактных» способов общения, где расчеты за сделку происходят посредством различных электронных платежных систем, сети Интернет и сотовой связи. Показан алгоритм действий сотрудников ОВД по получению первичной информации и документированию преступной деятельности преступников.

Пособие предназначено для профессорско-преподавательского состава, адъюнктов, курсантов и слушателей юридических вузов МВД России, а также практических сотрудников органов внутренних дел.

УДК
ББК

ISBN

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Несмотря на кардинальные изменения в законодательстве в области борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных сетей, проблема, связанная с противодействием данным видам преступлений, остается одной из наиболее значимых. Предпринимаемые правоохранительными органами всевозможные меры, к сожалению, не приносят ожидаемого результата. Компьютеры и телекоммуникационные системы, глобальная сеть Интернет, ставшие неотъемлемыми атрибутами жизнедеятельности современного человека, сформировали новую разновидность экономической преступности. Интернет используется преступными группами уже не только как вспомогательное средство, но и как место, и основное средство совершения традиционных преступлений, в сферах мошенничества, распространения наркотиков, экстремистских материалов и т.д.

В «Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» отмечается, что «основной угрозой в области международной информационной безопасности является использование информационных и коммуникационных технологий для совершения преступлений»[1].

Среди основных направлений государственной политики в области противодействия преступности в сфере использования информационных и коммуникационных технологий такие, как «совершенствование механизма обмена информацией о методиках расследования и судебной практике рассмотрения дел о преступлениях в сфере использования информационных и коммуникационных технологий».

Этому новому виду преступности необходимо противопоставить действенные меры, в число которых входят и меры по организации

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (утв. Президентом РФ 24 июля 2013 г., № Пр-1753) // СПС «Консультант Плюс».

деятельности органов внутренних дел. Однако органы внутренних дел не всегда успевают реагировать на вызовы современной преступности. Поэтому новые реально опасные деяния, совершаемые с использованием современных технологий, нередко остаются вне сферы деятельности правоохранительных органов, а в отношении уже криминализированных деяний возникают существенные проблемы в сферах их раскрытия, документирования и привлечения виновных к ответственности.

В условиях новых стремительно изменяющихся реалий в России необходимы системное и последовательное исследование интернет-преступности как в целом, так и отдельных наиболее распространенных ее видов, разработка эффективных мер борьбы и предупреждения преступлений в глобальной сети Интернет. Однако недостаток комплексных исследований Интернет-преступности в России, ее высокая латентность, как и отсутствие официальной статистки, приводят к неэффективности мер предупреждения, которые к тому же нередко носят фрагментарный и противоречивый характер, предопределяя трудности в противодействии и борьбе с данным видом общественно опасных деяний.

I. ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (ВКЛЮЧАЯ СЕТЬ ИНТЕРНЕТ)

Исторически понимание сферы телекоммуникаций связано с изобретением телеграфа (1774 г.)[1], радио (1895 г.), телевидения (1923 г.) и первого компьютера (1937–1943 гг.)[2]. Современные взгляды на сферу телекоммуникаций сопряжены с массовой информатизацией. Глобализация и стремительное развитие информационного пространства создают предпосылки для серьезного воздействия на многие элементы государственности и национальные правовые системы, в том числе структуру и форму современной преступности. Возросла угроза использования информационного пространства для совершения общественноопасных посягательств.

Современное информационное пространство завлекает пользователей своей относительной анонимностью, простотой размещения и большой продолжительностью хранения публикуемых сведений, постоянно находящихся в свободном пользовании для неограниченного круга лиц. На сегодняшний день более 55 % населения Российской Федерации пользуется Интернетом, причем в крупных городах это число возрастает до 75 % их жителей[3]. Анализ статистических данных преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий, указывает на возрастание количества преступлений. Если в 2017 году было зарегистрировано всего 90587 преступлений такого рода, то только за январь-август 2018 г. их число возросло до 107980 (прирост составил 94,4 %), при

[1] Кузнецов П.У. Информационные основания права. Екатеринбург, 2005. С. 9.
[2]Козырев А.А. Информатика: учебник для вузов. СПб., 2002. С. 22.
[3] Ларина Е., Овчинский В. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М.: Книжный мир, 2014. С. 7-8.

этом озабоченность вызывает их низкая раскрываемость (20424 преступлений в 2017 г. и 28329 в 2018 г.)[1].

Анализ юридической и специальной литературы позволяет сделать вывод, что на сегодняшний день нет единой классификации преступлений, которая бы охватывала весь диапазон преступных деяний в сфере информационно-телекоммуникационных технологий.

Так, Уголовный кодекс РФ[2] насчитывает шесть составов, предусматривающих ответственность за совершение преступлений с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 1 ст. 171.2; п. «б» ч. 3 ст. 242; п. «г» ч. 2 ст. 242.1; п. «г» ч. 2 ст. 242.2, ч. 2 ст. 280, ч. 1 ст. 282 УК РФ), а также четыре состава, предусматривающие ответственность за совершение преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 1 ст. 185.3; ч. 2 ст. 205.2; ч. 2 ст. 280.1; п. «б» ч. 2 ст. 228.1 УК РФ).

В отдельную группу выделяются преступления в сфере компьютерной информации – деяния, ответственность за которые предусмотрена главой 28 УК РФ. Основным критерием отграничения выступает понятие «компьютерной информации». «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[3]. Иными словами, к «преступлениям в сфере компьютерной информации» относятся только те противоправные деяния, которые предусмотрены ст. 272, 273, 274 УК РФ, объектом охраны которых выступает компьютерная информация, а иные деяния, совершаемые с

[1] Статистические данные ГИАЦ МВД РФ «Состояние преступности в России за период 2017 г., а также за 8 месяцев 2018 года». URL: https://мвд.рф/reports/item/14468708/ (дата обращения: 20.09.2018).
[2] Здесь и далее см.: Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : в ред. от 12.11.2018 // СПС «Консультант Плюс». Далее – УК РФ.
[3] ст. 272. УК РФ.

использованием информационно-телекоммуникационных технологий, данными статьями не охватываются.

Среди иных преступлений, которые могут быть совершены с использованием информационно-телекоммуникационных технологий, но не содержат квалифицирующего признака, можно выделить такие, как легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174, 174.1 УК РФ), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), нарушение авторских и смежных прав (ст. 146 УК РФ), причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 165 УК РФ), торговля людьми (ст. 127.1 УК РФ), клевета (ст. 128.1 УК РФ), нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), преступления против семьи и несовершеннолетних (глава 20 УК РФ).

В отдельную группу следует выделить преступления, в которых использование информационно-телекоммуникационных технологий выступает неотъемлемым признаком объективной стороны основного состава. К данной группе относятся: мошенничество с использованием платежных карт (ст. 159.3 УК РФ), мошенничество с использованием компьютерной информации (ст. 159.6 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ).

В Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований Федерального закона от 27.07.2006 № 149-ФЗ «Об информации,

информационных технологиях и о защите информации»[1], и иных нормативных правовых актов Российской Федерации в области связи.

Согласно ст. 2 данного Федерального закона информационно-телекоммуникационная сеть – это «технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники».

В вышеназванном Федеральном законе понятия «электронное сообщение», «электронный документ» характеризуются как информация, обращающаяся в информационно-телекоммуникационных сетях, но при этом не используется и не раскрывается понятие электронных сетей, входящее в состав некоторых преступлений[2]. Таким образом, можно сделать вывод, что электронная сеть и информационно-телекоммуникационная сеть – совпадающие по содержанию понятия, признаки вычислительной сети.

Информационная сеть представляет собой систему вычислительных средств или терминалов, с помощью данных средств происходит обработка информации и подготовка ее передачи пользователю. Передача информации обеспечивается совокупностью правил, регламентирующих формат и процедуры обмена информацией между пользователями, или, другими словами, коммутационным оборудованием, программным обеспечением и технологическими протоколами. Отсюда следует, что неотъемлемым признаком преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, будет являться возникновение следовой информации в этих сетях. Как только преступник подключает компьютер к сети, он становится ее частью – рабочей станцией. Следы остаются на

---

[1] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ : в ред. от 19.07.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

[2]Ковлагина Д.А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом РФ / Д.А. Ковлагина // Молодой ученый. 2016. № 16. С. 249-251. URL https://moluch.ru/archive/120/33286/ (дата обращения: 04.06.2018).

серверах, где находятся электронные почтовые ящики; размещается «вредоносная» информация на «транзитных» носителях – серверах, через которые устанавливалось подключение и осуществлялась работа в сети.

На сегодняшний день в отечественных источниках нет единого мнения по поводу терминологии для описания преступности в сфере использования информационно-телекоммуникационных технологий. Ряд авторов отдают предпочтение термину «киберпреступность», другие считают более корректным употребление термина «преступления в сфере компьютерной информации»[1].

Так, Оксфордский толковый словарь определяет «киберпреступность» (на англ. – «cybercrime») как «преступную деятельность, которая осуществляется с помощью компьютеров или Интернета»[2], словарь М. Макмиллана понимает «киберпреступление» как «преступление, совершенное с использованием Интернета», например, кража персональной информации либо заражение чужого компьютера вредоносными программами[3].

Нет единства по данному вопросу и в научном мире. Тропина Т.Л. понимает киберпреступление как «виновно совершенное общественно опасное уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством иных устройств доступа к моделируемому с помощью компьютера

[1]Завидов Б.Д. Сфера высоких технологий как мошенничество и как спорные объекты интеллектуальной собственности, находящиеся вне правового поля (фрикерство, хакерство и радиопиратство): подготовлено для системы «КонсультантПлюс» // СПС «КонсультантПлюс».

[2] Oxford dictionaries language matters. URL: http://www.oxforddictionaries.com (дата обращения: 02.05.2018).

[3] Macmillan dictionary. URL: http://www.macmillandictionary.com (дата обращения: 02.05.2018).

информационному пространству»[1]. Чекунов И.Г. предлагает рассматривать киберпреступность в качестве «самостоятельного вида преступности, определяемого на основе обнаружения обязательного присутствия в преступлениях таких признаков объективной стороны, как средство или орудие, в качестве которых выступает вредоносная программа или программно-техническое средство, подключенное к компьютерной сети или сотовому оператору связи»[2].

Использование исследователями рядом понятий «компьютерная преступность» и «преступления в сфере компьютерной информации», возможно, обусловлено наличием в УК РФ главы 28, предусматривающей ответственность за преступления в сфере компьютерной информации.

В свою очередь, мы согласны с мнением Т.Л. Тропиной и зарубежных исследователей[3], что криминологическое понятие «киберпреступности» шире в своем содержании понятия «компьютерная преступность» и является более предпочтительным для описания всей преступности в IT-сфере. Соотношение данных понятий представляется нам как соотношение общего и частного: киберпреступность включает в себя всю преступность, совершаемую с использованием информационного пространства, информационно-телекоммуникационных технологий, устройств и глобальных сетей.

Сафонов О.М. для описания преступлений, совершаемых в сфере использования информационно-телекоммуникационных технологий, предлагает использовать понятие «преступления, совершаемые с

---

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток, 2005. С. 64.

[2]Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности:дис. … канд. юрид. наук. М., 2013. 235с.

[3]Aghatise E.J. Cybercrime definition.Computer Crime Research Center. URL: http:// www.crime-research.org/articles/joseph06 (дата обращения: 02.05.2018).

использованием компьютерных технологий»[1], выделяя в качестве критерия отнесения деяния к «совершаемому с использованием компьютерных технологий» применение злоумышленником высокотехнологичных приспособлений.

По нашему мнению, использование формулировки «преступления, совершаемые с использованием компьютерных технологий» в качестве обобщенного понятия будет неверным, так как не все современные технологии, используемые в преступных целях, им охватываются. Например, использование био-, нано- и лазерных технологий.

Таким образом, можно сделать вывод, что понятия «преступления, совершаемые с использованием компьютерных технологий» и «преступления в сфере компьютерной информации» поуже понятия «преступления в сфере использования информационно-телекоммуникационных технологий».

Под «преступлениями, совершаемыми в сфере использования информационно-телекоммуникационных технологий» следует понимать виновные общественно опасные деяния, причиняющие ущерб общественным отношениям, связанным с безопасностью охраняемой законом информации, соблюдением установленного законом порядка оборота и использования информационно-телекоммуникационных технологий.

Следует подчеркнуть, что перечень преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, весьма значителен, и прогнозы по дальнейшей информатизации общества указывают на то, что он будет все более расширяться.

[1] Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис. … канд. юрид. наук. М, 2015. С. 36–37.

II. ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО ВЫЯВЛЕНИЮ И РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С БЕСКОНТАКТНЫМ СБЫТОМ НАРКОТИЧЕСКИХ СРЕДСТВ.

2.1. Характеристика бесконтактного способа сбыта наркотиков

Сегодня уже ни у кого нет сомнений, что в современном мире проблемы наркотизации и наркопреступности затрагивают все уровни безопасности общества – от здоровья конкретного индивидуума до безопасности и социального благополучия всего человеческого сообщества.

Анализ сложившейся на сегодняшний день ситуации в России свидетельствует о сохранении негативных тенденций в сфере незаконного оборота и незаконного потребления наркотических средств и психотропных веществ, что представляет серьезную угрозу здоровью населения, экономике страны, правопорядку, а также национальной безопасности государства.

По данным МВД России, за последние пять лет правоохранительными органами было выявлено более 950 тыс. преступлений. Из них 506 тыс. связаны со сбытом наркотиков, около 53,7 тыс. совершены участниками организованных преступных формирований либо в их составе[1]. За последние пять лет к уголовной и административной ответственности привлечено 1 млн 200 тыс. человек, пресечена деятельность 26 тыс. организованных преступных групп и преступных сообществ. Однако, по мнению большинства как российских, так и международных экспертов, эти цифры не отражают реальную криминогенную обстановку. Они считают, что выявляется не более 10-15 процентов таких преступлений.

Это связано с тем, что усиливается организованность преступной среды, а преступления и правонарушения в этой сфере приобрели массовый характер. При этом сотрудники специализированных оперативных подразделений полиции отмечают опасную тенденцию стремительного и

[1] Харченко С.В. Организация оперативно-розыскной деятельности территориальных органов ВМД России на районном уровне по борьбе с незаконным оборотом наркотических средств и психотропных веществ: монография. М.: Академия управления МВД России, 2017. С. 60.

неуклонного роста преступного «профессионализма» и организованности сбытчиков наркотиков.

Наряду с этим в Российской Федерации происходит интенсивная структурная перестройка нелегального рынка наркотиков. Во-первых, синтетические наркотики вытесняют ранее традиционные марихуану, опий и героин. Во-вторых, меняются схемы сбыта наркотиков. В преступную деятельность втягиваются лица с высоким уровнем образования и наличием специальных знаний, которые используют эти знания не только для производства синтетических наркотиков в подпольных лабораториях, но и для организации незаконных схем их сбыта. Будучи хорошо осведомленными о методах работы правоохранительных органов и, в частности, о тактике проведения оперативно-розыскных мероприятий, наркосбытчики прекрасно понимают, какому риску они подвергаются, когда общаются непосредственно с покупателями. В связи с этим с их стороны все чаще преобладает в организации сбыта наркотиков так называемый бесконтактный способ, т.е. с передачей их через системы тайников, а расчеты за сделку происходят посредством различных электронных платежных систем, сети Интернет и сотовой связи. Так, с 2008 года на территории Российской Федерации все большую популярность начал набирать бесконтактный способ сбыта наркотических средств. Для таких целей использовались средства сотовой телефонной связи, обеспечивавшие обмен информацией о времени, месте и способе сбыта наркотиков путем голосовых переговоров и коротких сообщений (СМС). Подобная система связи наркодиллеров между собой и с потребителями сравнительно быстро была изучена правоохранительными органами и взята под контроль. Кроме того, специальные службы МВД совместно с сотовыми операторами получали возможность оперативно устанавливать абонента, его местонахождение и легко контролировали информационный обмен.

С развитием информационно-телекомуникационных систем проникновением глобальной сети Интернет в повседневную жизнь граждан

эволюционировал механизм совершения преступлений в сфере незаконного оборота наркотических средств, психотропных веществ и прекурсоров к ним[1]. Новые тенденции в организации сбыта наркотиков бесконтактным способом стали отмечаться в 2011-2012 годах, когда вместо мобильной сотовой телефонной связи лица, осуществляющие сбыт наркотических средств, и, в первую очередь, новых видов психоактивных веществ, стали использовать возможности сети Интернет.

В 2013-2014 годах доступность технических средств, дешевизна пользования сетью Интернет, возможность конспирации стали толчком для наркосбытчиков к распространению теневого бизнеса с использованием возможностей специальных интернет-программ. В настоящее время преступники используют в своей деятельности такие интернет-программы обмена информацией как «Skype», «Brosix», «Jabber», «ICQ» и ряд других, позволяющих мгновенно обмениваться сообщениями (в т.ч. фото и видео изображениями) о намерениях и условиях сбыта (приобретения) наркотиков, местах тайниковых закладок и прочей информацией.

К преступлениям, связанным с НОН, относятся незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их аналогов без цели сбыта (ст. 228 УК РФ); незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов (ст. 228.1 УК РФ); нарушения правил оборота наркотических средств или психотропных веществ (ст. 228.2 УК РФ); незаконные приобретение, хранение или перевозка прекурсоров наркотических средств или психотропных веществ (ст. 228.3 УК РФ); незаконные производство, сбыт или пересылка прекурсоров наркотических средств или психотропных веществ (ст. 228.4 УК РФ); хищение или вымогательство наркотических средств или психотропных веществ (ст. 229 УК РФ); контрабанда наркотических средств, психотропных веществ, их прекурсоров или аналогов (ст. 229.1 УК РФ); склонение к

[1] Далее – НОН.

потреблению наркотических средств или психотропных веществ (ст. 230 УК РФ); незаконное культивирование растений, содержащих наркотические средства или психотропные вещества (ст. 231 УК РФ); организация либо содержание притонов для потребления наркотических средств или психотропных веществ (ст. 232 УК РФ); незаконная выдача либо подделка рецептов или иных документов, дающих право на получение наркотических средств или психотропных веществ (ст. 233 УК РФ); незаконный оборот сильнодействующих или ядовитых веществ в целях сбыта (ст. 234 УК РФ); незаконный оборот новых потенциально опасных психоактивных веществ (ст. 234.1 УК РФ).

Приобретение наркотических средств состоит из трех этапов: 1) поиск средств для приобретения наркотиков; 2) поиск источника приобретения и 3) договор со сбытчиком или через посредников о цене и количестве приобретаемого наркотика. Поиск средств для приобретения наркотиков в большинстве случаев сопряжен с совершением имущественных преступлений. Источниками приобретения выступают наркоманы и сбытчики.

Под хранением следует понимать любые умышленные действия, связанные с нахождением наркотических средств во владении виновного (при себе, в помещении, тайнике и других местах). При задержании наркоманов наркотики обнаруживают в личных вещах, различных предметах одежды. Тайники можно обнаружить в самых неожиданных местах жилища: люстрах, шторах, гардинах, мебели, бытовой технике, телефонных аппаратах, аптечках с лекарствами и др.

Изготовление наркотических средств в кустарных условиях нередко сопровождается специфическим запахом. В местах изготовления, помимо самих наркотических средств, можно обнаружить: химические реагенты, части растений (мак, конопля, эфедра и др.) и предметы со следами наркотика (весы, разновесы, сито, мясорубку, пресс, посуду, мешочки,

тампоны и иные приспособления). Возможно наличие наркотических средств и их компонентов на одежде и других вещах лиц, их изготавливающих.

Незаконный сбыт наркотических средств — это любые способы их распространения (продажа, обмен, дарение, уплата долга, дача взаймы, введение инъекций другому лицу и т. п.). Обстоятельствами, указывающими на причастность задержанного лица к сбыту наркотиков, являются длительное нахождение в районе известном как место концентрации лиц, допускающих немедицинское употребление наркотиков, при этом удаленном от его постоянного места проживания; обнаружение большого количества наркотического средства расфасованного на разовые дозы; несоответствие показаний относительно места, времени, источника приобретения наркотиков и фактического места и времени задержания и др.

Организованность наркобизнеса проявляется в системе заготовки и первичной переработки наркотиков, отработке способов и каналов их перевозки, мест хранения и сбыта. За каждый этап отвечают конкретные лица. Можно выделить следующие категории лиц, причастных к НОН: 1) организаторы преступных групп и сообществ; 2) заготовители (изготовители); 3) расхитители; 4) перевозчики; 5) пособники; 6) сбытчики (оптовые, перекупщики, розничные); 7) содержатели притонов; 8) покупатели (потребители). Но даже при наличии такой классификации одно и тоже лицо может относиться к одной или нескольким категориями в зависимости от характера своих преступных действий. Например, оптовая реализация наркотических средств осуществляется лицами, производящими наркотики, либо перекупщиками, к которым, в частности, можно отнести торговцев фруктами из среднеазиатских и закавказских регионов. Участники каждого звена системы, как правило, не знают друг друга, что позволяет достигать определенной степени безопасности для конкретного лица и высокой степени конспиративности преступной деятельности. Таким образом, разрыв одного звена не всегда может повлечь за собой крах всей преступной цепочки или группы. Несомненно, что наиболее большой

является доля лиц, связанных с незаконным оборотом наркотиков, состоит из потребителей и розничных сбытчиков наркотиков. Розничных сбытчиков наркотиков условно можно разделить еще на две группы:

1. Лица, действующие самостоятельно. Это, как правило наркоманы, сбывающие наркотические средства ради получения денежных средств, необходимых для приобретения очередной мелкооптовой партии наркотиков, около половины которой идет на собственное потребление, оставшаяся часть, соответственно, сбывается. И лица, не потребляющие наркотики, приобретающие их мелкими партиями и самостоятельно осуществляющие их сбыт.

2. Члены организованных преступных группировок. Каждой категории указанных лиц присущи определенные поведенческие признаки. По этим признакам в практической деятельности и осуществляется выявление лиц, представляющих оперативный интерес с точки зрения причастности к незаконному обороту наркотиков. Например, одним из ярких проявлений поведенческих признаков в рассматриваемой среде является наличие специфического жаргона. Употребление сленга как для обозначения наркотиков, так и для характеристики определенных действий, позволяет лицам, связанным с незаконным оборотом наркотиков, по малейшей оплошности выявить в своих рядах «чужака». Помимо этого, для успешной борьбы с преступлениями, связанными с НОН, оперативным работникам полиции необходимо знать виды наркотиков, признаки их изготовления и способы употребления.

Ранее преобладающей тактической схемой раскрытия квалифицированных составов преступлений, связанных с НОН, являлась схема «от лица – к преступлению», в настоящее время с появлением «бесконтактного» способа сбыта возможна схема «от преступления – к лицу». Это объясняется как элементами оперативно-розыскной характеристики рассматриваемых деяний, так и тем, что основными источниками получения информации о них являются лица конфиденциально

содействующие, сотрудники правоохранительных органов, материалы уголовных дел. Зная поведенческие признаки лиц, допускающих немедицинское употребление наркотиков, не представляет особой сложности раскрыть преступление, связанное с приобретением и хранением наркотического средства путем личного сыска в местах их концентрации. Иначе обстоит дело с раскрытием преступлений, связанных с распространением наркотиков. Без проведения комплекса оперативно-розыскных мероприятий и оперативных комбинаций в большинстве случаев не обойтись. Важнейшее значение в этой ситуации приобретает документирование преступных действий проверяемых и разрабатываемых. Документирование может осуществляться в рамках как проверочных материалов, так и дел оперативного учета.

При выявлении преступлений, связанных с бесконтактным способом сбыта наркотических средств, прежде всего, необходимо установить механизм совершения сделки, всю цепочку от «поставщика» до «потребителя».

Примерная структура бесконтактной группы и распределения ролей выглядит следующим образом:

- «Закладчик» – низшая ступень иерархии. Набираются из числа посетителей интернет-форумов (например, legalrc.biz), имеющих хорошую репутацию. При вербовке в качестве залога за полученные для распространения наркотики вносит на счет «работодателя» от трех до пяти тысяч рублей либо отравляет ему свои фотографии с пятью документами на свое имя. Как показывают результаты проведенных ОРМ, он получает заработную плату примерно в размере 300 рублей за каждую «закладку». При должном исполнении своих обязанностей статус может быть повышен.
- «Оптовый закладчик» – лицо, выбираемое из числа положительно зарекомендовавших себя «закладчиков». Как правило, получает от оператора адреса с закладками небольших партий наркотических

средств[1] и (или) психотропных веществ[2] (до 100 граммов). Также занимается фасовкой наркотиков и делает более мелкие «закладки» для «закладчиков», сообщает адреса «оператору». Кроме того, получает от «оператора» заработную плату, как правило, в процентах от суммы, вырученной с продажи наркотиков.

- «Оператор» – лицо, осуществляющее связь между «складами», «закладчиками» и потребителями наркотиков. Занимается рекламой магазина на интернет-форумах. Получает от «закладчиков» адреса с «кладами», которые передает потребителям после подтверждения оплаты наркотиков. Указывает «закладчикам» и «кладовщикам» количественную и качественную потребность в «закладках». В своей деятельности активно используют интернет программы «Skype», «ICQ» и т.п.

- «Финансовый директор, менеджер» – ежедневно получает отчет, в т.ч. «финансовый» – от «операторов» о продажах, указывает им на какие электронные счета переводить денежные средства. Консультирует по финансовым вопросам. Занимается регистрацией «Qiwi-кошельков», номера которых ежедневно пересылает «оператору» для перевода на них денежных средств от потребителей НС и ПВ.

- «Хакер» – консультирует «операторов» и «кладовщиков» по техническим вопросам. Составляет инструкции для безопасного пользования Интернетом, средствами мобильной связи, безопасного общения через интернет-программы «Brosix», «Skype», и «ICQ». Выдает логины и пароли для указанных программ через интернет-сервис безопасного обмена данными (URL: http:// privnote.com). Помогает «операторам» и «кладовщикам» настраивать оргтехнику, используемую в работе.

- «Курьер» – лицо, осуществляющее транспортные услуги по перевозке крупных партий наркотиков, чаще на своем транспорте, но может

[1] Далее – НС.
[2] Далее – ПВ.

пользоваться услугами общественного транспорта (такси, автобус или железнодорожные поезда дальнего и пригородного сообщения).

- «Кладовщик» – лицо, которое занимается хранением крупных партий наркотиков от 1 кг и выше. Получает партии НС и (или) ПВ с помощью служб доставки, почтовых отправлений, «курьеров». Также имеет фиксированную заработную плату, (выплачивается «финансовым директором») как правило, от 100 000 рублей в месяц.
- «Старший, саппорт» – осуществляет координацию всех нижних звеньев, при должном выполнении своих обязанностей продвигает их на более высокую должность, решает вопрос повышения заработной платы.

Практика оперативно-розыскной деятельности[1] специализированных оперативных подразделений полиции по линии борьбы с незаконным оборотом наркотиков показывает, что, как правило, основными участниками вышеуказанных схем продажи НС и ПВ являются молодые люди в возрасте от 18 до 25 лет, зачастую студенты либо не имеющие другой работы и источников дохода. Продавцами наркотиков часто становятся их потребители из числа активных участников интернет-сообществ, зарекомендовавших себя частыми покупками, подробными отзывами в Интернете о качестве «товара», соблюдением установленных правил приобретения и конспирации. Выявленные в ходе оперативно-розыскных мероприятий подразделениями по контролю за оборотом наркотиков[2] преступные группы наркосбытчиков отличаются разнообразной организационной структурой и имеют все признаки так называемой сетевой преступной организации.

Соответственно определенную сложность в выявлении и документировании преступной деятельности при бесконтактном сбыте НС и ПВ составляет еще и неизвестность при получении первоначальных оперативных данных сведений об отдельных структурных звеньев

[1] Далее – ОРД.
[2] Далее – УНК.

вышеуказанных организованных преступных относительно друг к другу, в том числе и в отношении вышестоящих в их иерархии. В последнее время специализированные оперативные подразделения по линии противодействия незаконному обороту наркотиков сталкиваются с тем, что рядовые участники схем продажи находятся в одном населенном пункте одного из субъектов Российской Федерации, а их руководители в другом того же или другого субъекта Российской Федерации, при этом знают друг друга лишь по «никнеймам»[1].

Подводя промежуточный итог, необходимо отметить, что бесконтактный способ сбытанаркотиков требует со стороны правоохранительных органов дальнейшего совершенствования организации работы по изобличению преступной деятельности наркодельцов, прежде всего, с помощью сил, средств и методов оперативно-розыскной деятельности, выработке новых оперативно-розыскных методик и привлечению виновных лиц к ответственности, установленной российским законодательством.

2.2. Зарубежный опыт противодействия незаконному обороту наркотиков и психотропных веществ (их аналогов)

Для всего международного сообщества проблема распространения наркотиков является не менее актуальной, чем для России. В связи с этим разрабатывается и внедряется в практику широкий комплекс экономических, социальных, организационных, медицинских и правовых мер. Наркомания – явление социальное, и поэтому бороться с ней необходимо, прежде всего, социально-экономическими методами. Вместе с тем существенное значение имеют и меры сугубо юридического характера, поскольку они создают соответствующую правовую базу для применения иных мер[2].

[1]«Никнейм», или «ник» (англ. nickname – кличка, прозвище), также сетевое имя – псевдоним, используемый пользователем в Интернете (в блогах, чатах на форумах).
[2]Аманбаев А.М. Международное сотрудничество в области противодействия незаконному обороту наркотиков: современное состояние и перспективы // Российский следователь. 2011. № 8. С. 89.

Первым международным договором, затронувшим этот вопрос, стала Гаагская конвенция 1912 г. Затем был принят ряд международно-правовых актов по борьбе с незаконным оборотом наркотических средств, в том числе Конвенция о запрещении незаконной торговли наркотическими средствами 1936 г. [1].

С образованием Организации Объединенных Наций разработана и принята Единая конвенция о наркотических средствах 1961 г. В качестве главного постулата Единой конвенции служит необходимость получения разрешения на импорт и экспорт наркотических средств, а также система оценок этой деятельности и статистических отчетов по ней. В качестве глобального наблюдателя стал функционировать один основной орган – Международный комитет по контролю над наркотиками. Его уникальность в том, что, существуя в рамках ООН, комитет по статусу является независимым.

Конвенция 1961 г. регламентирует, прежде всего, использование наркотических средств медицинскими и научными учреждениями, предусматривает их сотрудничество и контроль за культивированием растений, служащих основанием для изготовления наркотических средств, и производством наркотических препаратов. К Конвенции прилагаются Списки I, II, III, IV, в которых указаны наркотические средства и препараты, используемые для их изготовления.

В Протоколе 1972 г. о поправках к Конвенции 1961 г. содержатся поправки и уточнения ко всем четырем спискам наркосредств, включая новые вещества.

Конвенция о психотропных веществах 1971 г. устанавливает международную систему контроля на такие вещества, как галлюциногены, симпатомиметические средства амфетаминного типа, барбитураты, а также

[1] Корнева В.И. Правовое регулирование международного сотрудничества РФ в сфере противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов // Сборник научных трудов аспирантов и соискателей-юристов. Нижний Новгород: Нижегородский университет, 2005. С. 286.

снотворные, транквилизирующие и анальгезирующие средства. Некоторые из этих веществ вообще запрещены к использованию, другие выдаются лишь по рецептам. В Конвенции зафиксированы положения, согласно которым рецепты должны выписываться в строгом соответствии с медицинской практикой, этикетки препаратов снабжаться указаниями об их употреблении и необходимыми предостережениями. Конвенция предусматривает меры против злоупотребления наркотиками и указывает на необходимость лечения, реабилитации и социальной реинтеграции наркоманов[1].

Конвенция о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 г. (далее - Конвенция 1988 г.) принята специальной конференцией ООН в декабре 1988 г. и вступила в силу в ноябре 1990 г.[2] Основным побудительным мотивом ее принятия явилась необходимость укрепления и дополнения мер, предусмотренных двумя предыдущими Конвенциями ООН. Цель – уменьшение масштабов незаконного оборота наркотиков, т.к. он представляет собой международную преступную деятельность, пресечение которой требует первоочередного внимания. При этом основной упор сделан на повышение эффективности юридических средств международного сотрудничества.

Конвенция 1988 г. учитывает различные аспекты проблемы и, в частности, те из них, которые не предусмотрены или недостаточно полно отражены предыдущими документами (например, сокращение спроса).

Одним из наиболее важных положений этой конвенции является установление контроля за веществами, часто используемыми при изготовлении наркотических средств и психотропных веществ.

Стороны, подписавшие Конвенцию 1988 г., должны предоставлять друг другу самую широкую юридическую помощь (ст. 5 и 6). Согласно Конвенции стороны устанавливают друг с другом различные деловые связи,

[1] Аманбаев А.М. Указ. соч. С.92.

[2] Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (заключена в г. Вене 20.12.1988) // Сборник международных договоров СССР и Российской Федерации. Вып. XLVII. М., 1991. С. 133 – 157.

сотрудничают в расследовании правонарушений, подготовке соответствующих кадров (ст. 9), обмениваются информацией о транзите (ст. 10), осуществляют меры по проведению контролируемых поставок (ст. 11), создают систему мониторинга международной торговли веществами по таблицам № 1 и 2 (ст. 12)[1].

Россия участвует в данных Конвенциях и в силу международных обязательств (хотя и со значительным опозданием) стала создавать свою правовую базу, регламентирующую оборот наркотических средств и психотропных веществ на территории Российской Федерации[2].

Актуальным становится изучение и освоение приемлемого международного опыта законодательного регулирования борьбы с наркотизмом, так как проблема наркотизма – проблема мирового масштаба, а в каждом государстве существуют различные национальные меры борьбы с этим явлением[3].

К государствам, наиболее терпимо относящимся к незаконному потреблению и связанному с ним обороту, относятся Германия, Голландия, Италия, Испания, Швейцария.

Однако законодательство указанных стран дифференцирует виды ответственности в зависимости от вида наркотического средства или психотропного вещества. Для них характерно достаточно суровое наказание за изготовление и распространение «жестких» (ЛСД, героин, кокаин, опиум т.д.) наркотиков, менее суровые меры за действия с «мягкими» наркотиками (марихуана, гашиш и т.д.).

Так, например, в Германии, согласно нормам комплексного Закона об обороте наркотических средств от 28 июля 1981 г. (с изменениями и дополнениями) предусмотрена уголовная ответственность за ряд деяний,

---

[1] Аманбаев А.М. Указ. соч. С.99.

[2] О наркотических средствах и психотропных веществах: Федеральный закон РФ от 08.01.1998 № 3-ФЗ : в ред. от 29.12.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

[3] Преступление и наказание в Англии, США, Франции, ФРГ, Японии: Общая часть уголовного права / Власов И.С. и др. М.: Зерцало, 2013. С. 46.

классифицированных в зависимости от их степени общественной опасности[1]. В частности, уголовно наказуемы незаконное производство наркотиков (в том числе в крупных размерах, представляющих опасность для здоровья или жизни людей, либо членами преступных объединений, либо с целью сбыта); сбыт наркотиков; ввоз и хранение наркотиков в крупных размерах и др. За хранение наркотиков предусматривается лишение свободы на срок от 1 года до 4 лет или штраф[2]. Если же виновный хранил наркотики в крупных размерах, он может быть лишен свободы на срок от 1 года до 15 лет[3]. Определенный интерес представляют нормы, направленные на смягчение наказания и даже отказ от него в отношении лиц, совершивших правонарушения, не представляющие значительной опасности для общества, если при этом имеется возможность избавить указанных лиц от физической наркотической зависимости. Суть их в том, что суд может не назначать наказание, если виновный хранит наркотики в небольшом количестве и только для личного потребления, либо отложить исполнение наказания на срок до 2 лет, если за совершенное преступление предусматривается лишение свободы на срок до 2 лет[4].

Испанское законодательство наиболее показательно в сфере дифференциации ответственности за совершение незаконных действий с различными видами наркотиков.

После введения в Испании в 1985 г. голландской модели (легальное потребление наркотиков в немедицинских целях) количество только зарегистрированных наркоманов увеличилось с 200 тыс. до 1,5 млн, а страна превратилась в перевалочную базу наркотиков со всего мира. Это

---

[1] Клименко Т.М. Проблемы противодействия наркопреступности, наркотизму и наркомании в Российской Федерации (вопросы теории и практики): дис. ... д-ра юрид. наук. Волгоград, 2008. URL: http://www.google.ru/url?sa=t&rct=j&q (дата обращения: 17.12.2014).

[2] Клименко Т.М. Ответственность за незаконный оборот наркотиков по российскому и европейскому законодательству: Тольятти: ТГУ, 2010. URL: http://edu.tltsu.ru/sites/sites_content/site1238/html/media6 (дата обращения: 18.12.2017).

[3] Там же.

[4] Там же.

существенным образом повлияло на размеры наказаний. В настоящее время испанское законодательство наказывает деяния с «мягкими наркотиками» сроком до 17 лет 4 месяцев (вместо 6-ти лет ранее) лишения свободы, а за тяжелые до 23 лет 4 месяцев (вместо 12 лет ранее)[1].

К странам с наиболее жестким законодательством, направленным на борьбу с незаконным оборотом наркотиков и предусматривающим суровые меры наказания вплоть до смертной казни, относятся Франция, Китай, Иран, Пакистан, Таиланд, Малайзия, Нигерия и др.

Франция, являющаяся одной из основных стран-производителей маковой соломы, осуществляет эффективный контроль над производством на основе введенных систем лицензирования и уголовных наказаний, ограничивающих масштабы утечки и незаконного использования не только данного, но и иных видов наркотиков[2].

В соответствии со ст. 222-41 УК Франции наркотическими средствами признаются вещества и растения, указанные в ст. Л.627 Кодекса здравоохранения Франции.

Отличительными особенностями французского законодательства являются:

- установление уголовной ответственности не только за преступления (ст. 222-34 УК и 222-35 УК), но и проступки (ст.ст. 222-36 УК по 222-40 УК), связанные с незаконной торговлей наркотиками;

- указание в каждой норме периода надежности, то есть срока, после которого возможно уменьшение или смягчение наказания (в ст. 222-34 УК период надежности – от 18 до 22 лет, в остальных случаях – период надежности составляет половину срока наказания (ст. 131-23 УК);

- установление аналогичных пределов наказаний как за оконченное преступление, так и за покушение на преступление;

---

[1] Рыжиченков В.И. Преступления, совершаемые в сфере незаконного оборота наркотиков (Теория и практика): дис. ... канд. юрид. наук. М., 2009. С. 123.

[2] Уголовный кодекс Франции / перевод с фр. и предисл. Н.Е. Крыловой; науч. ред. Л.В. Головко, Н.Е. Крыловой. СПб.: Юридический центр Пресс, 2002.

- привлечение к уголовной ответственности не только физических, но и юридических лиц; назначение физическим и юридическим лицам наряду с основными видами наказаний дополнительного наказания.

К видам дополнительных наказаний, общих для физических и юридических лиц, относятся:

- конфискация установок, оборудования и всего имущества, служившего, непосредственно или косвенно, для совершения преступного деяния, а также любой его продукт, какому бы лицу они ни принадлежали и в каком бы месте они ни находились, если владелец не мог не знать об их происхождении или незаконном использовании (ч. 1 ст. 222-49 УК);

- конфискация всего или части имущества осужденного, какой бы характер оно ни носило, мебели или недвижимого имущества, делимого или неделимого (ч. 2. ст. 222-49 УК).

Если же в питейном заведении, ресторане, любом другом заведении, открытом для публики или используемом публикой, владельцем или с его соучастием были совершены уголовно наказуемые незаконные операции с наркотиками (ст. 222-50 УК), то:

а) владелец питейного заведения или ресторана окончательно (ч. 1. ст. 222-50 УК) или на срок не более пяти лет лишается лицензии (ст. 222-51 УК);

б) владелец заведения, открытого для публики или используемого публикой, должен закрыть его окончательно или на срок не более пяти лет (ч. 2. ст. 222-50 УК).

Для физических лиц дополнительные наказания состоят в запрещении проживать в определенных местах, т.е. запрещение появления в местах, определенных судом.

Кроме того, оно включает меры по наблюдениям за поведением и содействию по социальному обустройству.

Перечень запрещенных мест, а также меры по наблюдению и содействию могут быть изменены судьей по исполнению наказаний в условиях, установленных Уголовно-процессуальным кодексом Франции.

Срок запрещения проживания не может превышать десять лет в случае осуждения за преступления (ст. 222-34 УК и 222-35 УК) и пять лет в случае осуждения за проступки (ст. 222-36–222-39 УК); срок запрещения покидать территорию Франции не может превышать пять лет, если субъектом преступного деяния является гражданин Франции (ст. 131-30 УК).

Если преступление или проступок совершили иностранные граждане, то суд, в дополнение к основному наказанию, выносит решение о запрещении этим лицам находиться на территории Франции окончательно или на срок не более десяти лет, в зависимости от тяжести содеянного, после отбытия основного наказания (ст. 222-47 УК).

В качестве отягчающих обстоятельств признано совершение преступления организованной бандой[1]. Как видим, у французского законодательства свой, характерный только для него подход в установлении форм и признаков соучастия. Под организованной бандой понимается любая сформированная группа или любой сговор с целью подготовки одного или нескольких конкретных действий, одного или нескольких преступных деяний[2]. Как уже отмечалось выше, если субъектом преступного деяния является физическое лицо, то обязательными признаками служат вменяемость и возраст на момент совершения преступления (совершеннолетие)[3]. К несовершеннолетним, признанным виновными в их преступных деяниях, применяются меры защиты, помощи, меры по осуществлению надзора и принудительные меры воспитательного характера в условиях, определенных специальным законом[4]. Этот закон определяет условия, при которых могут назначаться наказания несовершеннолетним старше тринадцати лет[5].

---

[1] Уголовный кодекс Франции / перевод с фр. и предисл. Н.Е. Крыловой; науч. ред. Л.В. Головко, Н.Е. Крыловой. СПб.: Юридический центр Пресс, 2002.
[2] Статья 132-71. Уголовный кодекс Франции / Научн. ред. Л.В. Головко, Н.Е. Крыловой. - СПб.: Юридический центр Пресс, 2002.
[3] УК Франции. Ст. 121-4. Часть 1.
[4] УК Франции. Ст. 122-8. Часть 1.
[5] УК Франции. Ст. 122-8. Часть 1.

Независимая британская общественная организация «GlobalDrugSurvey» в апреле этого года опубликовала отчет, результаты которого поражают. Так, по данным опроса, в Соединенном королевстве 22 % респондентов признались, что покупали наркотики в Интернете, чуть меньше таких людей в Ирландии (20,5 %) и Дании (19,8 %).

Анализ правового регулирования противодействия незаконному обороту наркотиков в различных странах показывает, что уголовное законодательство подавляющего большинства стран мира ориентируется на международные правовые акты. Вместе с тем правовое законодательство и исполнительная система воздействий и наказаний разных государств в области антинаркотического законодательства специфичны, что обусловлено не только национальными особенностями стран, но и криминогенной ситуацией в этой сфере.

2.3. Задачи, функции и организация деятельности подразделений органов внутренних дел, обеспечивающих документирование преступных действий сбытчиков наркотических средств

Сбыт наркотических средств, как правило, – разноплановый, многоэтапный, многоэпизодный процесс, требующий познания характерных ситуаций и определения необходимых мер по организации и тактике оперативного документирования.

Целенаправленность исследования требует определить суть самой организации.

Организацию оперативного документирования в сфере НОН можно рассматривать в двух аспектах:

1. Организация системы подразделений с их задачами, функциями, кадровым, оперативно-техническим и иным обеспечением, обязанностями по взаимодействию и др.

2. Организация работы при подготовке к решению конкретных задач, к действиям в характерной или конкретной ситуации с определением цели, быстрым планированием, распределением отдельных конкретных

обязанностей, подготовкой средств документирования, обеспечением контроля за выполнением обязанностей.

Организация работы по раскрытию преступлений, связанных со сбытом наркотических средств, требует преемственности оперативно-розыскных и иных мероприятий при оперативной проверке и оперативной разработке отдельных категорий указанных лиц. Так, выявление и постановка на учет, оперативная проверка и разработка лиц, совершающих преступления, связанные с незаконным оборотом наркотических средств, могут принести успех лишь при концентрации сведений, поступающих из различных подразделений территориальных и других органов МВД России[1], так и других заинтересованных государственных, правоохранительных, контролирующих и иных ведомств, а также органов местной власти, объединения их усилий по изобличению лиц, активно занимающихся этой преступной деятельностью. При этом активное участие всех служб ОВД должно осуществляться на всех этапах оперативной проверки конкретных лиц. Так, например, аппараты уголовного розыска, иные оперативные подразделения полиции[2] располагают значительными возможностями по выявлению и проверке лиц, занимающихся незаконными операциями (изготовлением, приобретением, сбытом, хранением наркотических средств). В отношении лиц, занимающихся перевозкой наркотических средств, важными сведениями располагают органы внутренних дел на транспорте. При поступлении осужденных лиц в учреждения мест лишения свободы важными источниками получения информации обо всех совершенных ранее ими преступлениях и иных фактах, имеющих значение для борьбы с преступлениями, связанными с незаконным оборотом наркотических средств, а также совершенными на почве наркомании, располагают оперативные подразделения Федеральной службы исполнения наказания.

---

[1] Далее – орган(ы) внутренних дел и (или) ОВД.

[2] Основы оперативно-розыскной деятельности органов внутренних дел Российской Федерации: учебное пособие / авт. - сост. Е.П. Шляхтин, И.М. Усманов. Казань. КЮИ МВД России, 2017. С. 110-111.

Как показывает практика, наибольшими возможностями в борьбе с преступлениями, связанными с незаконным оборотом наркотиков, располагают оперативные подразделения полиции, прежде всего, специализирующие на выявлении и раскрытии вышеуказанных преступлений.

К оперативным подразделениям органов внутренних дел, правомочным осуществлять оперативно-розыскную деятельность и документирование преступных действий сбытчиков наркотических средств, в полном объеме, установленном Федеральным законом «Об оперативно-розыскной деятельности», относятся подразделения по борьбе с незаконным оборотом наркотиков (Главное управление, управления, региональные отделы, отделения, группы). Всемерную помощь им оказывают иные оперативные подразделения полиции, как например, уголовного розыска, экономической безопасности и противодействия коррупции, по борьбе с преступными посягательствами на грузы органов внутренних дел на транспорте, по борьбе с преступлениями в сфере высоких технологий и др.

Именно на подразделения органов внутренних дел, осуществляющих оперативно-розыскную деятельность в полном объеме, установленном Федеральным законом «Об оперативно-розыскной деятельности»[1], в качестве возложена основная задача предупреждения и раскрытия преступлений, в том числе, связанных с НОН. В их распоряжении имеются негласный аппарат и другие оперативно-розыскные силы, средства и методы, позволяющие вести успешную борьбу с замаскированными, тайно подготавливаемыми преступлениями.

В процессе документирования преступной деятельности изготовителей и сбытчиков наркотических средств могут принимать участие работники различных служб и подразделений ОВД. Так, при использовании специальной и криминалистической техники в документировании участвуют

[1] Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ : ред. от 06.07.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

подразделения специальных технических мероприятий и в качестве специалистов – работники экспертно-криминалистических учреждений. Участковые уполномоченные полиции по поручению руководства органов внутренних дел или оперативных работников могут проводить опросы граждан, располагающих информацией о незаконной деятельности с наркотическими веществами; наводить справки; обследовать помещения, здания, сооружения, участки местности и т.д. Подобные мероприятия проводят и работники других служб ОВД. Оперативную разработку и документирование отдельной категории изготовителей и распространителей могут и обязаны вести работники всех оперативных подразделений полиции.

Ведомственными приказами МВД России определены общие задачи и основные направления деятельности оперативных подразделений полиции, предусматривается комплексное использование в решении названной проблемы сил и средств всех служб и подразделений ОВД.

Конкретные задачи по борьбе с незаконным оборотом наркотиков определены всем службам и подразделениям органов внутренних дел, в части касающейся их деятельности.

2.4. Взаимодействие оперативных аппаратов органов внутренних дел при документировании преступной деятельности сбытчиков наркотических средств бесконтактным способом

Важную роль в борьбе правоохранительных органов с незаконным оборотом наркотических средств приобретают вопросы взаимодействия. Взаимодействие оперативных подразделений полиции при документировании преступной деятельности сбытчиков наркотических средств, на наш взгляд, необходимо представить в трех уровнях.

Первый уровень – это взаимодействие между различными службами (подразделениями) органов внутренних дел и различными (по территориальности и (или) ведомственной принадлежности) оперативными аппаратами. Вопросы данного взаимодействия регулируются ведомственными нормативными актами.

Высокая результативность в раскрытии преступлений в современный период может быть достигнута путем комплексного использования всех сил и средств органов внутренних дел на основе постоянного совершенствования организации, форм и методов взаимодействия служб и подразделений органов внутренних дел при раскрытии преступлений[1].

Комплексное участие сил различных служб в раскрытии преступлений, связанных с НОН, и необходимость их взаимодействия объясняются целым рядом обстоятельств. Службы и подразделения органов внутренних дел, несмотря на различия в компетенции, формах и методах осуществления оперативно-розыскной деятельности, действуют в одном и том же регионе, внутри которого сложились определенные устойчивые экономические и социальные связи. Актуальность проблемы противодействия распространения наркотических средств многократно возрастает в регионах, в которых, благодаря климатическим условиям произрастают наркотикосодержащие культуры; имеются границы с сопредельными государствами, через которые осуществляются поставки наркотических средств, и т.д. Существует взаимосвязь между городом и прилегающими сельскими районами; между объектами народного хозяйства, занимающимися переработкой наркотикосодержащего сырья, и его поставщиками; между зарубежными наркодельцами и перевозчиками (туристы, «челноки» и т.п.). Это влияние взаимообусловленных обстоятельств внутри региона на преступность, естественно, требует учета при организации мер по борьбе с преступлениями, связанными с НОН, привлечения всех служб к их предотвращению и раскрытию.

Необходимость взаимодействия между службами органов внутренних дел объясняется тем, что они осуществляют деятельность в одной отрасли государственной деятельности – в борьбе с преступностью. Действительно,

[1] Гребельский Д.В., Атмажитов В.М., Ильичев В.А. Изучение эффективности организации взаимодействия аппаратов уголовного розыска с другими службами в раскрытии преступлений / Д.В. Гребельский, В.М. Атмажитов, В.А. Ильичев // Совершенствование управления раскрытием и расследованием преступлений: сб. научн. трудов. М.: Академия МВД СССР, 1981. С. 138.

перед различными службами и подразделениями органов внутренних дел стоят одни и те же задачи, только способы их решения определяются в зависимости от компетенции различными методами, силами, средствами. Несмотря на общую цель борьбы с преступностью, в том числе с преступлениями, связанными с НОН, каждая из служб органов внутренних дел имеет свою компетенцию. Организация взаимодействия должна в полной мере учитывать полномочия и компетенцию каждого субъекта, а также специфику сил, средств, применяемых им для решения общих задач борьбы с преступностью. Исходя из компетенции и общих задач органов внутренних дел, важным звеном организации обеспечения успешной борьбы с преступностью, связанной с НОН, является определение рациональной структуры аппаратов, ее осуществляющих, а также четких организационно-тактических основ взаимодействия.

В основу организационного построения системы служб и подразделений, осуществляющих борьбу с незаконным распространением наркотиков, положен принцип функциональной специализации, проявляющей себя в той или иной мере в зависимости от управленческого уровня специализированного подразделения.

Исходя из общих задач и соображений специализации, вопросы борьбы с распространением наркотических средств распределены между службами.

Основными задачами взаимодействия подразделений и служб органов внутренних дел в расследовании и раскрытии преступлений являются:

- обеспечение неотложных следственных действий и оперативно-розыскных мероприятий при совершении преступлений;

- всестороннее и объективное расследование преступлений, своевременное изобличение и привлечение к уголовной ответственности лиц, их совершивших, розыск скрывшихся преступников; возмещение материального ущерба;

- самостоятельность следователя в принятии решений в соответствии с Уголовно-процессуальным кодексом РФ (далее – УПК РФ)[1];

- самостоятельность сотрудников оперативных подразделений в выборе средств и методов оперативно-розыскной деятельности в рамках законодательства;

- согласованность планирования следственных действий и оперативно-розыскных мероприятий;

- непрерывность взаимодействия в организаторской деятельности, расследовании и раскрытии преступлений до принятия решений по уголовному делу.

Основными принципами взаимодействия являются: соблюдение законности, конституционных прав и свобод граждан; комплексное использование сил и средств органов внутренних дел; персональная ответственность руководителей подразделений за проведение и результаты следственных действий и оперативно-розыскных мероприятий.

Выявление и ликвидация организованных преступных групп, занимающихся наркобизнесом, входит в число основных задач, возложенных на специализированные оперативные аппараты органов внутренних дел, осуществляющие борьбу с организованной преступностью.

Второй уровень взаимодействия можно определить как взаимодействие между оперативными аппаратами органов внутренних дел (далее – ОВД), решающими вопросы документирования преступной деятельности, связанной со сбытом наркотических средств, и подразделениями различных министерств и ведомств, принимающих участие в борьбе с НОН. Вопросы данного взаимодействия регламентируются межведомственными нормативными актами. Так, например, в процессе взаимодействия оперативных аппаратов органов внутренних дел и Федеральной службы

[1] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : ред. от 12.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

безопасности России (далее –ФСБ) их совместные и согласованные усилия направляются на решение ряда задач, в том числе и задач борьбы с НОН.

Взаимодействие оперативных подразделений ОВД и ФСБ организуется по следующим основным направлениям:

- совместное проведение операций по выявлению, предупреждению, пресечению и раскрытию тяжких и особо тяжких преступлений, обезвреживанию межрегиональных и международных преступных группировок;

- использование оперативно-розыскных сил, средств и методов, а также возможностей и каналов НЦБ Интерпола в Российской Федерации, деловых связей с органами безопасности, спецслужбами и правоохранительными органами иностранных государств;

- обмен оперативно-розыскной, криминалистической и иной оперативно значимой информацией о готовящихся, совершаемых или совершенных преступлениях и причастных к ним лицах;

- обмен опытом оперативно-розыскной деятельности, профессиональной подготовки сотрудников оперативных подразделений, проведение совместных учений, тренировок и иных служебных занятий.

Взаимодействие осуществляется путем:

- систематического обмена оперативно-розыскной информацией, представляющей интерес для партнера;

- информационного, организационно-технического, иного содействия оперативно-розыскным мероприятиям, проводимых одной из сторон;

- осуществления согласованных мер в рамках совместных операций по борьбе с преступностью;

- выполнения поручений следователей по уголовным делам и запросов по делам оперативного учета;

- принятия мер по охране мест происшествий, установлению свидетелей; совместного (согласованного) проведения мероприятий в рамках межведомственных следственно-оперативных групп;

- реализация иных мер, диктуемых конкретной оперативной ситуацией.

В процессе осуществления взаимодействия оперативных аппаратов ОВД и ФСБ, в том числе при документировании преступных действий, связанных с НОН, могут осуществляться совместные операции. Под операциями понимаются объединенные общими целями и задачами комплексные совместные или согласованные оперативно-розыскные мероприятия оперативных подразделений ОВД и ФСБ. Операции заранее планируются. Планы подготовки и проведения операций могут быть разовыми и типовыми.

Разовые планы операций в каждом отдельном случае разрабатываются с учетом особенностей конкретной криминогенной и оперативной ситуации и действуют только в пределах, определенных в решении о проведении операции.

Типовые планы задействуются при повторяющихся ситуациях с конкретизацией целей и задач, исполнителей и сроков проведения операций.

Направленность и ход каждой операции конкретизируются с учетом поступающей информации, промежуточных результатов, изменений оперативной обстановки, поведения проверяемых или разрабатываемых лиц.

Время, формы и способы реализации информации, полученной в результате оперативно-розыскной деятельности, определяются по согласованию сторон в зависимости от конкретных результатов операции, характера и содержания полученных данных, их достаточности для введения в уголовный процесс, необходимости проведения дополнительных оперативно-розыскных мероприятий или первоначальных следственных действий. Порядок предоставления результатов оперативно-розыскной деятельности оперативных подразделений полиции регламентируется межведомственным нормативным актом[1].

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю или в суд : приказ МВД РФ, Минобороны РФ, ФСБ РФ, ФСО РФ, Федеральной таможенной службы, СВР РФ, ФСИН, Федеральной службы РФ по контролю за оборотом наркотиков и

Подразделения органов внутренних дел осуществляют скоординированные с подразделениями ФСБ, Федеральной таможенной службы и другими заинтересованными ведомствами, мероприятия направленные на выявление и ликвидацию каналов и источников нелегального проникновения наркотических средств в Россию из-за рубежа, разоблачение преступных групп наркодельцов с межрегиональными и транснациональными связями. Обеспечивают надежное оперативное прикрытие финансовых и коммерческих структур, имеющих контакты с фирмами стран – производителей наркотиков, международных транспортных узлов, а также аэропортов, приморских городов, приграничных и пограничных районов. Активизируют разведывательно-поисковую деятельность в среде этнических группировок, вовлеченных в наркобизнес.

Взаимодействие структурных подразделений СВР России и МВД России происходит на основе информации о каналах и способах заброски на территорию Российской Федерации наркотиков. Структурные подразделения СВР России при получении соответствующих сведений немедленно информируют соответствующие структурные подразделения МВД России о криминальных группировках, а также о лицах, намеревающихся осуществить доставку наркотических средств, и используемых при этом ухищрениях.

Третий уровень взаимодействия – это сотрудничество заинтересованных министерств и ведомств различных государств. В данном случае вопросы взаимодействия регулируются межправительственными и межведомственными (межгосударственными) соглашениями[1].

Следственного комитета России от 27 сентября 2013 г. №776/703/509/507/1820/42/535/398/68 // СТРАС «Юрист» (дата обращения: 25.11.2018).

[1] См., например: Единая конвенция о наркотических средствах 1961 года с поправками, внесенными в нее в соответствии с Протоколом 1972 года о поправках к Единой конвенции о наркотических средствах 1961 года (Заключена в г. Нью-Йорке 30.03.1961); Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (заключена в г. Вене 20.12.1988); Конвенция о психотропных веществах (заключена в г. Вене 21.02.1971) и др. // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

Ратифицировав в 1990 г. Конвенцию ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ, Российская Федерация прочно встала на путь сотрудничества с другими странами в этой области международных отношений. В целях дальнейшего развития и совершенствования договорно-правовой базы такого сотрудничества заключены межправительственные и межведомственные соглашения, посвященные борьбе с незаконным оборотом наркотиков, более чем с 40 государствами[1].

В числе государств, подписавших соглашение с Россией на межправительственном уровне, стали Аргентина, Бразилия, Великобритания, Германия, Греция, Испания, Италия, Канада, Китай, Колумбия, Куба, Мальта, Мексика, США, Турция, Узбекистан, Финляндия, Франция, Чили. В стадии соглашения находятся проекты таких договоров с некоторыми другими странами[2].

МВД России заключены межведомственные соглашения с антинаркотическими службами Австрии, Болгарии, Вьетнама, Венгрии, Германии, Индии, Италии, Канады, Кипра, Македонии, Монголии, Польши, Румынии, Словакии, Турции, Франции, Швейцарии, Швеции, а также со странами – участницами Содружества Независимых Государств (далее – СНГ): Арменией, Белоруссией, Грузией, Молдовой, Туркменией, Таджикистаном, Украиной. Из государств Балтии соглашение подписано только с МВД Латвии.

Подводя итог, можно сказать, что вопросы подготовки кадров требуют дальнейшего совершенствования. Существует необходимость обучения сотрудников оперативных подразделений полиции, прежде всего,

---

[1] Гаврилов В.Г., Диденко В.И. Методика организации и проведения контролируемых поставок наркотических средств и психотропных веществ: учебно-методическое пособие / В.Г. Гаврилов, В.И. Диденко. Белгород: БЮИ МВД России им. И.Д. Путилина, 2003. С.87.

[2] См., например: Об утверждении межведомственного распределения обязанностей по обеспечению участия Российской Федерации в международных организациях системы ООН: постановление Правительства РФ от 03.06.2003 г. № 323 : в ред. от 29.11.2018 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

специализирующихся на противодействие незаконному обороту наркотиков, организации работы по документированию бесконтактного сбыта наркотических средств и психотропных веществ.

Для эффективной работы по документированию необходима разработка единых бланков для документирования противоправных действий при бесконтактном сбыте наркотиков. Более детальной проработки требуют вопросы взаимодействия подразделений, осуществляющих борьбу с незаконным оборотом наркотиков не только внутри МВД России, но и с иными субъектами противодействия преступности в сфере незаконного оборота наркотических средств, психотропных веществ и их прекурсоров.

Вопросы обмена информацией требуют дальнейшего совершенствования и разработки нормативной базы, совместных нормативных актов по организации взаимодействия.

Вопросы обеспечения техническими средствами для более эффективного документирования представляются, несомненно, достаточно актуальными. Для документирования признаков преступной деятельности сбытчиков наркотиков целесообразно применение аудио- и видеотехники; материалы, собранные при помощи технических средств, в том числе, во время проведения таких оперативно-розыскных мероприятий, как «Обследование помещений, зданий, сооружений, участков местности и транспортных средств», «Контроль почтовых отправлений, телеграфных и иных сообщений», «Прослушивание телефонных переговоров», «Снятие информации с технических каналов связи», «Оперативное внедрение», «Контролируемая поставка», «Оперативный эксперимент» и «Получение компьютерной информации», после их надлежащего процессуального оформления, могут быть использованы в качестве доказательств.

Несмотря на детальную регламентацию деятельности различных подразделений ОВД и заинтересованных ведомств, занимающихся борьбой с незаконным оборотом наркотических средств, вместе с тем необходимо обратить внимание на нескоординированность их действий. Следует

отметить отсутствие согласованных планов по противодействию незаконному обороту наркотиков как на уровне отделов внутренних дел и соответствующих подразделений других ведомств, так и на уровне министерств и ведомств. Созданная межведомственные государственные и общественные организации по противодействию злоупотреблению наркотическими средствами и их незаконному обороту не решают всех организационных, финансовых, технических и других вопросов, возникающих в процессе деятельности правоохранительных органов. Одними из актуальных задач , стоящих перед МВД России и другими ведомствами, призванными вести борьбу с незаконным оборотом наркотиков, являются подготовка и комплектование служб ими квалифицированных кадров.

2.5. Особенности следственных действий на различных этапах расследования преступлений, связанных с бесконтактным сбытом наркотических средств

Как указано во многих трудах теоретиков-криминалистов, любую методику расследования можно представить как систему последовательных этапов, что, по мнению И.А. Бастрыкина, является «одним из принципов методики расследования»[1]. Чаще всего выделяются такие этапы, как первоначальный, последующий и заключительный этапы расследования. Но существуют и сложные и многоэпизодные преступления, в которых может выделяться еще и подготовительный этап, характеризующийся тем, что для принятия решения о возбуждении или отказе в возбуждении уголовного дела имеет место деятельность следователя по пополнению недостающего первичного материала. В то же время этот этап является лишь подготовкой к началу расследования и, с точки зрения уголовно-процессуального законодательства, не является в сущности этапом самого расследования.

Каждый из этапов расследования имеет свои специфические

[1] Бастрыкин И.А. Криминалистика: учебник. Том II / под. общ. ред. А.И. Бастрыкина. - М.: Экзамен, 2014. С. 224.

особенности в объеме и методах данной криминалистической деятельности, поэтому для успешного расследования преступлений вырабатываются приемы и способы следственных действий, характерные именно для конкретного этапа. Соответственно, при любом расследовании выделяются особенности производства на первоначальном, последующем и подготовительном этапах.

Для первоначального этапа характерны выявление устанавливающих или уличающих преступника фактов, установленных на основании возможных первичных следственных версий; разработка плана расследования на основании первичной информации или иных данных, что были получены при производстве подготовительного этапа расследования. В основу фактических данных ложится информация, собираемая путем следственных действий, которые нужно провести на первоначальном этапе расследования за относительно ограниченный срок, исходя из специфичных задач (выявление всех признаков преступления, выявление и задержание виновных по горячим следам). Все или часть этих действий могут быть и неотложными. К указанным мероприятиям могут относиться обыск, осмотр места происшествия, допросы свидетелей и подозреваемого, проведение судебных медицинских и судебных химических экспертиз. Фактическим окончанием первоначального этапа расследования считается момент предъявления обвинения лицу.

Как правило, возбуждение уголовного дела осуществляется на основании предварительной проверки, поводом для которой могли послужить сведения о единичном эпизоде сбыта наркотических средств с использованием телекоммуникационных сетей, совершенном одним из членов преступной группировки. На указанном этапе следователю поступают материалы, отражающие результаты оперативно-розыскных мероприятий на основании которых он возбуждает уголовное дело по ст. 228.1 УК РФ, а квалификация преступления по п. «б» ч. 2 указанной статьи производится, если в ходе проведения оперативных действий уже выявлен факт

осуществления преступления бесконтактным способом.

Шебалин А.В. утверждает, что постановление о возбуждении уголовного дела в отношении неустановленного лица выносится в связи с рядом причин:

1. На практике не редки случаи, когда анкетные данные могут оказаться неверными, из-за ошибки в фамилии или неверного указания отчества.

2. В связи с достаточно серьезным уровнем шифровки лиц, занимающихся сбытом наркотических средств, зачастую случается ситуация, когда на момент возбуждения уголовного дела лицо, занимающееся указанным преступным деянием, в действительности может быть не установлено.

3. На основании ст. 133 УПК РФ лицо, подвергнутое незаконному обвинению, имеет право на реабилитацию.

Информация о способе сбыта наркотических средств, об использованных технологиях и информационных ресурсах на момент возбуждения уголовного дела уже должна быть изучена следователем, ибо на основании нее осуществляется разработка типичных следственных версий и первоначальных следственных действий, но есть необходимый перечень следственных действий, которые должны быть включены в план расследования преступлений. К ним относятся допрос подозреваемых, личный обыск и освидетельствование, допрос свидетелей, обыск, задержание подозреваемых и назначение экспертизы.

При расследовании сбыта наркотических средств могут возникать следующие типичные следственные ситуации:

1. При сбыте наркотических средств был задержан закладчик («бегунок»), следователем был установлен канал поступления наркотических средств. В случае возникновения этой ситуации могут и должны быть произведены следующие следственные действия: задержание в порядке статей 91-92 УПК РФ, освидетельствование, допрос и личный обыск

подозреваемого; допрос покупателя наркотических средств, а в случае необходимости и проведение очной ставки. Характерными являются также изъятие образцов для сравнительного исследования; если имеются свидетели, то их допрос; назначение и проведение экспертиз изъятых веществ, материалов, следов, найденных на них: судебно-медицинской, дактилоскопической и иных.

2. При сбыте наркотических средств был задержан закладчик («бегунок»), однако канал поступления наркотических средств установлен не был. Следственные действия не отличаются от тех, что проводятся при расследовании преступлений, которым свойственны ситуации первой группы, только оперативно-розыскные мероприятия направлены на выявление каналов поступления наркотических средств. Перед сотрудниками правоохранительных органов стоят задачи склонения подозреваемого к сотрудничеству, получения от него информации об иных участниках преступной группировки, чья деятельность направлена на бесконтактный сбыт наркотических средств. Особенностью проведения оперативно-розыскных мероприятий на данном этапе является то, что их выполнение должно быть осуществлено в кратчайшие сроки, так как до наркопреступника очень быстро доходит информация о задержании его «соратника», в связи с чем он может прибегнуть к конспирации или вовсе «залечь на дно».

3. Была получена информация о сбыте, но сбытчик не был задержан, канал поступления наркотических средств также не был установлен. В этом случае проводятся следующие следственные действия:

- допрос в качестве свидетеля закупщика наркотических средств;

- опрос проводивших оперативно-розыскные мероприятия оперуполномоченных;

- допрос понятых, участвующих при производстве оперативно-розыскных мероприятий;

- в орган дознания должно быть направлено поручение о проведении

оперативно-розыскных мероприятий в целях установления и задержания сбытчика наркотических средств;

- назначение комплексных химико-фармакологической и физико-технических экспертиз.

Оптимизации проведения следственных действий способствует тесное сотрудничество между следователем, ведущим производство по уголовному делу, и оперативными работниками, которое способствует правильному выбору времени и места проведения следственных действий, вычислению всех фигурантов преступной группы, установлению, изъятию и фиксированию следов, имеющих значение для расследуемого преступления. Все это обеспечивает, если не исключение, то сведение к минимуму возможности избавления преступников от следов преступления и наркотических средств (например, в практике не раз встречались случаи смыва наркотиков в канализацию, глотание «меченых» денежных купюр и т.д.).

Задержание лица, подозреваемого в совершении преступления, на первоначальном этапе является одним из наиболее «богатых» доказательствами следственных действий. Задержание регламентировано ст. 91 УПК РФ, и возможно лишь при наличии хотя бы одного из трех оснований: на лице, подвергаемом задержанию, должны находиться следы преступления, и/или оно должно быть застигнуто в момент или сразу после совершения преступления, и/или на него должны указать свидетели. Отсутствие этих условий порождает незаконность задержании в отношении конкретного лица, но есть исключение, указанное в части 2 рассматриваемой статьи. В случае если есть основания полагать, что конкретное лицо все же причастно к совершению преступления, и если оно не имеет постоянного места жительства, пыталось скрыться либо не установлена его личность, или же если следователем с согласия руководителя следственного органа, а дознавателем – с согласия прокурора было направлено ходатайство в суд об

избрании этой меры пресечения, то указанное лицо может быть задержано по этим исключительным основаниям.

Основная специфика расследования преступлений, связанных со сбытом наркотических средств, заключается в том, что задержание с поличным помогает не только изобличить преступника, но и добыть необходимые для возбуждения уголовного дела наркотические средства, без которых расследование изрядно затрудняется, так как на практике часто невозможно доказать факт совершения наркопреступлений без изъятия наркотического средства у задержанного либо при обыске жилища.

Особенности места задержания сбытчиков наркотических средств связаны с определением информации о местонахождении преступника, о способе совершения преступления, о наличии контрмер со стороны подозреваемого в отношении сотрудников правоохранительных органов. Одним из главных правил задержания наркопреступников является его внезапность для лиц, обоснованно подозреваемых в незаконном обороте наркотиков, и их связей, иначе существует большая доля вероятности, что как конкретное лицо, подозреваемое в совершении преступлении, так и группа, в составе которой он действовал, предпримут попытку скрыть следы своей противоправной деятельности.

Так как задержание является, по сути, самым важным оперативно-следственным действием, то его эффективность зависит от высокого уровня профессионализма лиц, уполномоченных на его совершение: оперуполномоченный оперативного подразделения полиции, проводящий задержание, должен обладать большим объемом информации, «предвидеть» поведение подозреваемого и вовремя пресекать возможные эксцессы.

Необходимо учесть и то, что при проведении задержания оперативному работнику и следователю необходимо установить пути и способы приобретения наркотических средств лицами, их распространяющими, в том числе, рассмотреть вариант, что сами сбытчики, пользующиеся телекоммуникационной сетью для облегчения совершения преступления,

могут приобретать партии наркотиков через сеть Интернет.

У задержанных лиц следует произвести изъятие полученных ими через терминалы оплаты услуг квитанций, свидетельствующих о расчете за распространяемый ими наркотик. В случае если квитанций при подозреваемом не было, информацию, необходимую для следователя, можно получить из терминала. Указанное будет свидетельствовать, что задержанным лицом за наркотик были перечислены денежные средства через электронный терминал на счет банка лица.

При производстве личного обыска и освидетельствования лиц, подозреваемых в совершении преступления, сотруднику правоохранительного органа стоит быть особенно внимательным, учитывая, что сбытчики наркотиков идут на различные ухищрения ради сокрытия следов преступления: как правило, свертки с наркотическими средствами встречаются у задержанных лиц вшитыми в воротники, под заплаты, между швами, поэтому проверка этих мест должна осуществляться наиболее тщательно. Нередки случаи, когда сбытчики могут хранить небольшое количество наркотических средств «на виду», например в кармане сумки, а большая партия спрятана в «тайнике». Это совершается с целью отвлечения внимания полицейских от переносимой крупной партии наркотических средств, маскируя все либо под мелкое административное правонарушение, либо под простой сбыт наркотических средств, без указания на квалифицирующий признак (имеется в виду ч. 3 ст. 228.1 УК РФ «Сбыт наркотических средств в значительном размере»).

Немаловажным является обнаружение при обыске различных записок, схем расположения закладок и т.д., которые могут являться важным доказательством при изобличении лиц, причастных к бесконтактному способу сбыта наркотических средств (могут назначаться почерковедческие экспертизы, дающие основания для выхода на след личностей иных звеньев преступной цепи).

Освидетельствование проводится с обязательным участием врача для

достижения целей установления факта приема задержанным наркотических средств, установления его состояния, особых примет или следов преступления. Также врачебное освидетельствование необходимо для того, чтобы выявить условия содержания лица, предположительно употребляющего наркотические средства (в специализированном медицинском учреждении, изоляторе временного содержания и т.д).

При освидетельствовании также осуществляется смыв с ладоней рук задержанного следов наркотических средств, если есть основания полагать, что указанные вещества побывали в руках подозреваемого. Указанное действие проводится в первые часы после задержания с использованием раствора гексана или спирта. Взятый смыв надлежащим образом упаковывается и направляется на сравнительное исследование. Необходимо учитывать и то, что лица, так или иначе знакомые с производством следственных действий, ухищряются уничтожить данные следы, например, вытирая ладони об одежду, просятся в туалет, где моют руки и т.д.

При производстве следственных действий, направленных на расследование преступлений рассматриваемой группы, объектом поиска будет информация, указывающая на наличие умысла приобретения или сбыт наркотических средств с использованием телекоммуникационных технологий. К такой информации может относиться: переписка сбытчика и потребителя, паспортные данные, номера телефонов, банковских счетов, иная необходимая информация для осуществления платежа, за покупку наркотических средств. Мы выражаем свое согласие с мнением Е.В. Кушпеля и П.Е. Кулешова, которые говорят: «При расследовании преступлений, связанных с незаконным сбытом наркотических средств и психотропных веществ через электронные терминалы оплаты услуг, в качестве неотложных действий необходимо незамедлительно и по возможности одновременно произвести обыски в жилищах участников преступной организации, а также в жилищах лиц, имеющих отношение к деятельности данной

организации…»[1].

«Обычно в рамках производства обыска по месту жительства подозреваемого изымаются наркотические средства, орудия совершения преступления (сим-карты, компьютеры (как правило, изымается только системный блок; мониторы и иная периферия не приобщаются к вещественным доказательствам), оборудование для фасовки наркотических средств, банковские карты, рукописные записи, выраженные на бумаге или ее фрагментах, в том числе и с местом нахождения закладок, фасовочные пакеты, шприцы, чеки и квитанции, указывающие на факт оплаты наркотических средств), а также иное имущество, добытое преступным путем»[2]. По прибытии на место проведения обыска необходимо обеспечить сохранность не только всей компьютерной техники, но также данных и информации, которые она хранит. Во исполнение этого следует придерживаться определенных правил:

- необходимо установить запрет для всех лиц, так или иначе находящихся на объекте обыска, прикасаться к компьютерной технике, несмотря ни на что;

- в случае, если результат манипуляций компьютерной техникой не известен заранее, необходимо установить запрет на его осуществление[3].

Только при соблюдении поставленных условий можно приступить к непосредственному обыску помещения и изъятию компьютерной техники, следуя указанному алгоритму:

1. Изъятию подлежит вся компьютерная техника, которая может являться носителем искомой информации.

---

[1] Кушпель Е.В., Кулешов, П.Е. Особенности методики расследования незаконного сбыта наркотических средств и психотропных веществ, совершенных с использованием высоких технологий // Успехи современной науки и образования. № 7. 2016. С. 29.

[2] Шебалин А. В. Расследование незаконных сбытов наркотических средств, совершенных бесконтактным способом: учебное пособие / А.В. Шебалин. - Барнаул: Барнаульский юридический институт МВД России, 2015. С. 19.

[3] Вехов В. Б. Особенности расследования преступлений, совершаемых с использованием средствэлектронно-вычислительной техники: учебно-методическое пособие. Волгоград: Перемена, 1998. С. 35.

Изъятию подлежит вся компьютерная техника, которая может являться носителем искомой информации.

2. Не стоит просматривать искомую информацию непосредственно в месте ее нахождения, тем более без специалиста.

3. Необходимо по возможности закрыть все программы корректным способом перед тем, как отключить питание компьютера; если же существуют спорные ситуации, то необходимо просто выключить компьютер. Для предотвращения случаев потери информации из оперативной памяти при некорректном выключении компьютера, когда, например, происходит перезагрузка компьютера либо отключается питание без предварительного выхода из программы, на месте должен присутствовать соответствующий специалист.

4. Выключить питание всей компьютерной техники, находящейся в помещении, необходимо наиболее корректным способом.

5. Необходимо установить ключи доступа (пароли, шифры, алгоритмы и т.д.) для снятия средств защиты компьютеров от несанкционированного входа.

6. Необходимо изъять все бумажные носители, на которых могут быть записаны правила пользования компьютерной техникой, ключи к ее разблокировке, пароли и алгоритмы.

7. Запрещено при осмотре места происшествия подносить ближе чем на 1 метр к компьютерной технике источник сильного магнитного напряжения, к которым могут быть отнесены некоторые осветительные приборы и часть следственной аппаратуры.

8. Необходимо выяснить факт получения пользователями указанной аппаратуры услуг лиц, занимающихся обслуживанием компьютеров. Если такой факт подтвердится, то есть необходимость в нахождении таких лиц.

Изъятие компьютерной техники должно проводиться в точном соответствии уголовного процессуального законодательства, а именно необходимо обращать внимание понятых на производимые действия, а также

на их итоги, а в случае необходимости давать разъяснения тем лицам, которые не понимают смысла проводимых действий. Указанные предметы надлежащим образом укомплектовываются для предотвращения возможности разукомплектования или повреждения наиболее важных деталей – носителей информации. При опечатывании необходимо в заднюю часть панели системного блока, в разъем электрического питания, положить лист бумаги.

Что касается проведения следователем допроса, то в зависимости от наличия необходимой информации общей для рассматриваемой группы преступлений является тактика допроса, производимая в форме «свободного рассказа», на что есть две существенные причины. Во-первых, это позволяет установить психологический контакт с подозреваемым, во-вторых, «свободный рассказ» нередко позволяет следователю добыть больше исходной информации, чем он имеет, посредством совершения с подозреваемым вербальных и невербальных действий, которые позволяют отделить ложные показания от истинных.

При допросе обязательно должно быть установлено место нахождения подозреваемого в период совершения действий с электронными системами, а полученные данные должны быть немедленно проверены. Так ряд авторов указывают на необходимость проведения следующих неотложных следственных действий:

- истребовать в компаниях сотовой связи детализацию входящих и исходящих соединений абонентского номера «высшего звена» с указанием базовых станций, обслуживающих абонента в момент соединений, и IMEI-номера телефонного аппарата абонента; данная детализация позволяет установить наличие активности в определенный период времени телефонных переговоров «организационно-управленческого уровня» с «организационно-обеспечивающим уровнем»;

- запросить в компаниях сотовой связи детализацию входящих и исходящих соединений абонентских номеров, находившихся в пользовании

«бегунков», с указанием базовых станций, обслуживающих абонента в момент соединений, и IMEI-номера телефонного аппарата абонента; данные детализации позволят установить наличие активности в определенное время телефонных переговоров «исполнителей», т.е. «бегунков», с «организационно-обеспечивающим уровнем», т.е. «диспетчерами»;

- истребовать в компаниях сотовой связи сведения о поступлении денежных средств на счета номеров абонентов оператора сотовой связи, которыми пользовались члены преступной организации, с отражением даты и суммы пополнения баланса вышеуказанных абонентских номеров[1].

Производство допроса сопровождается рядом особенностей, которые вытекают из следственной ситуации, характерной для того или иного состава преступления. Так, например, при допросе лица, употребляющего наркотические средства, следователю необходимо проявлять спокойствие и сдержанность, так как разговор «на повышенных тонах» может вызвать у подозреваемого агрессию, привести к замкнутости, осложняя установление психологического контакта между подозреваемым и следователем и делая невозможным получение необходимой информации об иных участниках преступного сообщества. Для первого допроса типично получение от подозреваемого ложных данных, поэтому на указанном этапе необходимо проявление следователем высокого уровня профессионализма для изобличения во лжи. Последующая работа основывается на полученной от подозреваемого информации: если она является правдивой, то ее легко можно подтвердить законными следственными действиями, например, очной ставкой, обысками и т.д.

Основной целью проведения обыска является установление лиц, участвующих в преступной группировке, направленной на сбыт наркотических средств, криминальных связей между ними, способов расчета, лиц, потребляющих наркотические средства, и иных имеющих значение для дела обстоятельства.

[1] Кушпель Е.В., Кулешов П.Е. Указ. соч. С. 29.

Для установления фактов, имеющих важное значение по рассматриваемому делу (определение вида и количества наркотического средства – его массы, состояния наркотического опьянения и т.д.), возникает необходимость в проведении ряда экспертиз, к которым относятся судебно-медицинская, комплексная химико-фармакологическая, судебная компьютерная, лингвистическая, дактилоскопическая и другие.

Комплексная химико-фармакологическая экспертиза назначается на основании постановления и сопроводительного письма для выяснения того, является ли изъятое вещество наркотическим средством, психотропным веществом или их аналогом. Производство указанной экспертизы осуществляется экспертом-химиком или экспертом-фармакологом. Перед экспертами ставятся вопросы о природе исследуемого вещества, его массе при поступлении и израсходованной массе для проведения экспертизы.

Судебно-медицинская и судебно-психиатрическая экспертизы проводятся для установления факта заболевания задержанным лицом наркоманией, оценки состояния его психического здоровья и, если такое имеет место быть, состояния его наркотического опьянения.

Судебно-компьютерная экспертиза назначается при возможности наличия конкретной информации в памяти устройства технических средств, предоставленных эксперту, а также наличия в памяти устройства следов работы в Интернете. К этому же типу экспертиз относится проверка сотовых телефонов и сим-карт после получения ранее запрошенных следователем сведений от телефонных операторов о PIN- и PUK-кодах указанной сим-карты, причине блокировки указанного номера. Также следователь может истребовать сведения об абоненте и абонентском номере.

Лингвистическая экспертиза предполагает распознавание экспертами шифра из разговора преступников, если таковой используется для сокрытия состава преступления.

Итак, делая вывод, укажем, что первоначальный этап расследования незаконного сбыта наркотических средств характеризуется следующими

признаками:

1. Основными целями расследования являются изобличение лиц, участвующих в сбыте наркотических средств, каналов и источников поступления наркотиков в обращение, лиц, приобретающих наркотические средства.

2. Первоначальный этап заканчивается с момента предъявление лицу обвинения.

3. Большинство следственных действий, совершаемых на первоначальном этапе, носят неотложный характер.

Типовые следственные ситуации на завершающем этапе в основном связаны с полнотой и качеством положенных в основу обвинения данных, отношением обвиняемого к доказательствам, собранными в процессе расследования, к новым обстоятельствам, полученным в процессе допроса обвиняемого. Например, одной из типовых ситуаций будет признание обвиняемым своей вины при наличии достаточных и достоверных доказательств. Поэтому основным направлением расследования в этом случае будет являться «подготовка и выполнение требований, связанных с окончанием расследования»[1]. Иной же ситуацией будет то, что при наличии достаточных и убедительных доказательств обвиняемый не признает полностью или частично своей вины, тогда дальнейшее расследование идет по пути выяснении и проверки дополнительных обстоятельств с возможностями нового предъявления обвинения или и вовсе прекращения расследования.

На указанном этапе происходит проверка версий, установление деталей события преступления, большое внимание уделяется сбору и фиксации доказательств, направленных на установление связей между членами преступного сообщества, деянием и наступившими последствиями (например, между фактом сбыта наркотических средств и употреблением его несовершеннолетним). Уже выдвигается предположение, что личность лица,

[1] Бастрыкин И.А. Криминалистика: учебник. Том II. М.: Экзамен, 2014. С. 226.

совершившего преступление, известна, поэтому основная задача, стоящая перед следователем, направлена на поиск и анализ свидетельствующей о причастности лица к бесконтактному сбыту наркотических средств доказательственной информации. Поэтому не редки случаи, когда на завершающих этапах для устранения возможных противоречий и восстановления деталей события преступления проводятся дополнительные осмотры места происшествия. Также может проводиться осмотр компьютерной техники и информации.

Этот этап также характеризуется формированием доказательственной информации при предъявлении обвинения. Проведение всех следственных действий направлено на закрепление доказательств, имеющихся в деле, устранение незначительных противоречий, подтверждение одной версии и устранение иных. Также формируются меры по предупреждению и профилактике наркопреступности.

Как правило, все следственные действия необходимо распределять по группам в зависимости от наличия следов, которые были установлены на первоначальном и доследственном этапах.

К первой группе относятся наркотические средства и предметы, непосредственно с ними контактирующие. К указанным следам относятся: выданное закупщиком или изъятое наркотическое средство, обнаруженное при осмотре места происшествия, выемки, задержании, личном обыске обвиняемого, в «закладке»; упаковка наркотического средства, приспособления для употребления наркотиков, тампоны со следами «смыва» наркотических средств, металлизированная бумага, в которую заворачивали указанные вещества и т.д. Для исследования этих предметов и приобщения их к делу в качестве доказательств могут быть проведены такие следственные действия, как:

- назначение физико-технической и судебно-фармакологической экспертиз в случае, если изъятое вещество относится к одному из списков

наркотических веществ, утверждаемых постановлением Правительства РФ[1];

- сдача указанных веществ в камеру хранения на основании вынесения постановления о признании и приобщении их в качестве вещественных доказательств;

- осмотр указанных веществ.

Во вторую группу следов принято включать рукописные записи, к которым относятся: указание места нахождения закладки, номера счетов, кошельков и иные выраженные на бумаге рукописные записи, имеющие значение для дела. Для фиксации данных следов и приобщении их к уголовному делу в качестве доказательств могут осуществляться:

- осмотр указанных следов;

- взятие у конкретного лица образца почерка для проведения сравнительного исследования;

- назначение идентификационной почерковедческой экспертизы, по результатам которой выносится постановление о признании и приобщении к уголовному делу вещественных доказательств.

К третьей группе следов относятся те, что содержат какую-либо компьютерную информацию, имеющую значение для дела: компьютеры, телефоны, сим-карты, ноутбуки и т.д. В ходе исследовании следов третьей группы могут быть проведены следующие следственные действия:

а) осмотр указанных объектов;

б) назначение компьютерной экспертизы на предмет содержащихся в памяти устройства данных, имеющих значение для дела;

в) назначение лингвистической экспертизы в обнаруженной интернет-переписке сведений, которые, как полагает следователь, несут в себе информацию о месте сбыте и возможных участниках преступной деятельности;

---

[1] Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации: постановление Правительства Российской Федерации от 30 июня 1998 г. № 681 // Собрание законодательства РФ. 1998. № 27. Ст. 3198.

г) изъятие из другого альтернативного носителя интернет-переписки задержанного в целях взятия образцов для сравнительного анализа;

д) назначение автороведческой экспертизы в целях выявления факта того, является ли обвиняемое лицо автором сообщений, отправленных под определенным именем («ником»), с использованием определенной программы-коммутатора, такой как «Skype», например;

е) в случае осуществления интернет-подписки с мобильного телефона имеет смысл получение сведений о соединении абонента с указанием базовых станций, чтобы установить место осуществления соединения в порядке ст. 186.1 УПК РФ, а затем, осмотрев полученную распечатку, признать ее вещественным доказательством;

ж) есть необходимость допроса лиц, которые оформили на свое имя средства связи, в число которых входят и сим-карты с мобильными телефонами, а также банковские счета, которыми впоследствии пользовались участники преступного сообщества. Сюда же можно отнести обязанность следователя допросить родственников и иных приближенных к лицам, занимающихся незаконным сбытом наркотических средств, для выявления номеров телефона, которыми они пользовались[1].

К четвертой группе можно отнести следы – фонограммы (записи голосов, отраженные на оптических дисках, которые были получены в ходе проведения оперативно-розыскных мероприятий, таких как «наблюдение», «опрос» и т.д.). Чтобы приобщить к делу указанные следы необходимо провести следующие следственные действия: осмотр и прослушивание фонограмм, записанных на такие материальные носители, как оптические диски; следователем может быть вынесено постановление о приобщении в качестве вещественного доказательства как оптического диска с записью фонограмм, так и бумажного носителя, воплощающего текстовую версию информации, отраженной в виде фонограммы. Органу дознания может быть вынесено поручение следственным органом для необходимости нахождения

[1] Кушпель Е.В., Кулешов П.Е. Указ. соч. С. 30.

лица, которое желало приобрести у обвиняемого наркотические средства, и голос которого записан на фонограмме. Могут быть получены образцы голоса обвиняемого (подозреваемого) для проведения фонографической экспертизы в целях сравнения образца голоса подозреваемого с записью голоса преступника.

В пятую группу включаются следы – результаты оперативно-розыскной деятельности, содержащие номера электронных кошельков и IP-адреса технических средств, используемые преступниками для производства бесконтактного способа сбыта наркотических средств.

Выявление указанных следов характеризуется выполнением определенных оперативно-розыскных мероприятий и следственных действий. Например, когда имеются выявленные оперативным путем сведения об IP-адресах, используемых при незаконном сбыте наркотических средств бесконтактным способом, тогда осуществляется оперативно-розыскное мероприятие «Наведение справок» и направляется запрос в организацию интернет-провайдера на получение сведений об использовавшем этот IP-адрес абоненте, адресе его использования, сайтах, которые посещал абонент в определенный период.

Целесообразно при получении значимой уголовно-процессуальной информации направить в орган дознания отдельное поручение о проведении ОРМ по установлению проживающих в жилище лиц и их занятиях, образе жизни и т.д., а по результатам анализа представленных материалов оперативно-розыскной деятельности провести обыск в жилищах наркосбытчиков и их криминальных, родственных, интимных и иных связей.

Если содержатся сведения об используемых сбытчиками наркотиков электронных кошельках, то в эксплуатирующие платежные системы организации в ходе ОРМ «Наведение справок» направляется запрос, в котором содержится просьба предоставить сведения о произведенных транзакциях по лицевому счету электронного кошелька, а также иных данных, которые могут быть полезны для установления личности владельца.

Если в ответах на этот запрос есть сведения об IP-адресах технических средств, с которых был зарегистрирован указанный кошелек, то аналогичным образом целесообразно направить запрос в организацию интернет-провайдера на получение сведений об абоненте и месте установки оконечного оборудования.

В случае если неизвестно, какому интернет-провайдеру принадлежит IP-адрес, то можно направить в орган дознания поручение о проведении ОРМ по этому поводу. Перед этим следователю целесообразно самостоятельно попытаться установить интернет-провайдера по известному адресу, воспользовавшись таким интернет-ресурсом, как «2ip» (URL: http://2ip.ru/).

Полученные оптические диски и распечатки с транзакциями по лицевым счетам электронных кошельков осматриваются, в них может быть обнаружены данные об оплате штрафов ГИБДД, жилищно-коммунальных услуг, в этом случае в указанные организации направляются запросы, целью которых является установление персональных данных лица, в пользу которого были осуществлены эти платежи. По поводу этих объектов выносятся постановления о признании и приобщении к уголовному делу вещественных доказательств – оптических дисков и распечаток.

Если на оптических дисках и в распечатках с транзакциями по лицевым счетам электронных кошельков содержится информация о снятии денег путем использования банкомата, то в кредитную организацию направляется запрос предоставлении сведений о владельце банковской карты, местонахождении банкоматов, в которых были сняты деньги, записей с видеокамер слежения банкоматов сберегательных банков при выполнении банковских операций по счетам указанной карты и т.п.

После этого в орган дознания направляется поручение о проведении ОРМ, направленных на установление причастности указанного лица к расследуемому преступлению, а также об установлении принадлежности банковских карт определенным банкам. Эту информацию также можно

установить, воспользовавшись интернет-ресурсом «BinDB» (URL: https://www.bindb.com).

Если результаты ОРД указывают на причастность этого лица к совершению преступления, то возможно проведение обыска у него дома, задержание в порядке ст. 91 УПК РФ, допрос подозреваемого и т.п.

Таким образом, типизация и алгоритмизация процесса расследования является одним из условий его эффективности, это в полной мере относится и к расследованию незаконных сбытов наркотических средств, совершенных бесконтактным способом[1].

Подводя итог рассмотрению данного вопроса, можно сделать вывод, что теория расследования бесконтактного сбыта наркотических средств испытывает острую необходимость в развитии новых методологических научно-обоснованных рекомендаций по производству расследования преступлений, квалифицирующихся по п. «б» ч. 2 ст. 228 УК РФ, ибо осуществление сбыта подобным образом дает преступникам неограниченные возможности по сокрытию следов преступления и отмыванию доходов, полученных преступным путем. Кроме того, существует и объективная необходимость в повышении профессионального уровня должностных лиц следственных органов и работников оперативных подразделений полиции.

В настоящее время в Российской Федерации предприняты ряд мер, направленных на законодательное ограничение использования анонимных платежей, так как подобного рода денежные перечисления зачастую используются в сферах распространения наркотиков, детской порнографии и финансирования терроризма. Например, следует отметить принятие российским законодателем Федерального закона от 5 мая 2014 г. № 110-ФЗ «О внесении изменений в отдельные законодательные акты РФ», который предусматривает упрощенную форму идентификации лица при использовании электронных средств платежа для предотвращения

[1] Шебалин А.В. Расследование незаконных сбытов наркотических средств, совершенных бесконтактнымспособом: учебное пособие. Барнаул: Барнаульский юридический институт МВД России, 2015. С. 23-24.

легализации (отмывания) доходов, заведомо добытых преступным путем.

Здесь же следует отметить, что имеется насущная потребность, чтобы в штатах специализированных оперативных подразделениях полиции по контролю за оборотом наркотиков были предусмотрены высочайшего уровня специалисты в области IT-технологий. Которые будут осуществлять мониторинг интернет-пространства в целях пресечения бесконтактного сбыта наркотических средств, анализа состояния наркопреступности в кибер-пространстве, оперативного изобличения лиц, занимающихся рассматриваемым деянием, путем отслеживания подозрительного перемещения денежных средств, выявление международного наркотрафика и др. Возможно и заимствование международной практики по пресечению наркопреступности в информационном пространстве, путем, например, осуществления кибер-атак на интернет-ресурсы, созданные в целях сбыта наркотических средств.

2.6. Тактические основы проведения оперативно-розыскных мероприятий в отношении лиц, причастных к незаконному сбыту наркотиков бесконтактным способом

Первым этапом документирования указанных преступлений является получение оперативно значимой информации в отношении сбытчиков НС и ПВ. Практика показывает, что такой наркобизнес в настоящее время осуществляется во многих регионах Российской Федерации, однако правоохранительным органам о нем становиться известно чаще всего случайно ввиду высокого уровня латентности подобных преступлений.

Наиболее предпочтительной является информация, полученная от конфидентов, отражающая сведения о будущих фигурантах оперативной разработки. Однако на практике чаще всего возможны три пути поступления первичной оперативно-значимой информации:

1) сведения о номерах мобильных телефонов магазинов продажи наркотиков[1], рекламируемых фигурантами (в виде визитных карточек или надписей на стенах зданий, заборах, остановках общественного транспорта, например, «MIX», «SPACE», «Легалка» и т.п.);

2) мониторинг интернет-сайтов и интернет-форумов, созданных для рекламы и продажи наркотиков. В сети Интернет может осуществляться рассылка сообщений на аккаунты в «Skype» с указанием номеров сотовых (мобильных) телефонов, номеров «ICQ» и прочих коммуникационных интернет-программ с приложением инструкции о проведении платежей через электронные системы оплаты;

3) объяснения лиц, задержанных полицейскими по фактам изъятия у них НС и (или) ПВ, в которых указывается источник их приобретения.

Во всех случаях для дальнейшей оперативно-розыскной деятельности необходимо получить информацию об электронном счете (электронном кошельке), на который для приобретения наркотиков должны поступать средства оплаты. Этот счет может сообщить покупатель, задержанный за приобретение и хранение НС и (или) ПВ, или установить его возможно, позвонив на номера мобильных телефонов, указанные в рекламе наркотиков.

После анализа и оценки полученной первичной информации принимается решение о заведении в установленном порядке соответствующего дела оперативного учета[2]. В случаях изъятия НС и (или) ПВ у покупателя и возбуждения уголовного дела в отношении неустановленного лица, сбывшего их, проводится комплекс ОРМ.

В рамках оперативной проверки или оперативной разработки в первую очередь необходимо провести ОРМ «Наведение справок», заключающееся в направлении запроса в «Qiwi Банк»[3]. В нем необходимо запросить имеющуюся информацию о номерах банковских карт, привязанных к

[1] Термин «наркотик», а также любые производные от него слова являются в данном учебном пособии синонимами понятий «НС и (или) ПВ».
[2] Далее – ДОУ.
[3] При проведении указанного ОРМ рекомендуется обратиться в суд с ходатайством на получение разрешения на его проведение.

указанному «Qiwi Кошельку», а также запросить по счету «Qiwi Кошелька» анкетные данные, предоставленные при его регистрации, даты и суммы пополнения установленных счетов терминала оплаты с указанием адресов их местонахождения, переводы средств оплаты на иные счета с указанием номеров, даты, времени и сумм перевода, а также информацию о получении денежных средств (Ф.И.О., дата рождения, вид, номер и дата выдачи документа, удостоверяющего личность, адрес места жительства получателя), телефоны, указанные держателем номера, на которые могут приходить СМС-оповещения о проведенных операциях по счету. Кроме того, может понадобиться информация об адресе электронной почты, IP-адресе, с которого осуществлялась регистрация «Qiwi Кошелька», и IP-адресах, с которых осуществлялись входы на него (электронная система Qiwi Банка такую информацию фиксирует). Вся полученная информация должна быть тщательным образом учтена и проанализирована, т.к. она позволяет в дальнейшем установить, максимальное число участников сбыта наркотиков бесконтактным способом.

Несмотря на то, что фигуранты, как правило, указывают вымышленные анкетные данные при регистрации «Qiwi Кошелька», следует учитывать, что держатель должен правильно указать номер своего мобильного телефона, так как регистрация осуществляется с помощью СМС-сообщений. Также он должен правильно указывать привязанные к своему номеру реквизиты банковских карт. Кроме того, изучение движения средств оплаты по счету позволяет определить как номера других «Qiwi Кошельков», так и реквизиты других банковских карт. В дальнейшем на сайтах «BinDB» (URL: https: // Bindb.com) и «Покупной.рф» (URL: покупной. рф) можно установить по номеру карты ее принадлежность к определенному банку. Запросы в банк о принадлежности банковской карты и движениях денежных средств по ней необходимо проводить с учетом требований федеральных законов от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»[1] и от 12

[1] О банках и банковской деятельности: Федеральный закон РФ от 2 декабря 1990 г. № 395-

августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[1], т.е. по постановлению суда о разрешении проведения ОРМ «Наведение справок».

Для установления фигуранта, владельца «Qiwi Кошелька», необходимо проанализировать возможную оплату им каких-либо иных покупок или услуг. Например, заказ авиабилетов или железнодорожных билетов, покупки в интернет-магазине, услуги провайдера Интернета, сайта знакомств и т.д. В дальнейшем легендированный запрос в компанию, осуществившую какие-либо услуги, позволяет установить анкетные данные фигуранта.

Возможно также, что фигуранты переводят денежные средства на другие мобильные кошельки, привязанные к номерам сотовых телефонов. В таком случае для получения информации о движении денежных средств по счету необходимо проведение ОРМ «Снятие информации с технических каналов связи — СМС» (далее – СИТКС), а также возможно в дальнейшем провести разведывательный опрос (в рамках возбужденного уголовного дела и допрос) сотрудников компании сотовой связи.

Анализ информации, полученной из «Qiwi Банка» и от сотовых операторов связи, о движении средств указанного «Qiwi Кошелька» позволяет установить «оператора» сети сбыта (владельца «Qiwi Кошелька»), «закладчиков» (владельцев других «Qiwi Кошельков», которым перечисляются небольшие суммы оплаты за их услуги), а также вышестоящие звенья сети (владельцев банковских карт, которым регулярно перечисляются более крупные суммы оплаты) с учетом того, что, как правило, многие банковские карты привязываются к номерам мобильных телефонов.

Таким образом, при условии тщательной обработки информации из «Qiwi Банка» оперативный сотрудник должен получить установочные данные фигурантов низового звена сети сбыта наркотиков, а также их:

1) номера мобильных телефонов;

---

1 // Ведомости съезда народных депутатов РСФСР. 1990. № 27. Ст. 357.

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ // Собрание законодательства РФ. 1995. № 33. Ст. 3349. Далее - Закон об ОРД.

2) реквизиты банковских счетов;

3) адреса электронной почты;

4) IP-адреса технических устройств выхода в Интернет.

В дальнейшем необходимо организовать взаимодействие с сотрудниками специальных технических подразделений, в ходе которого:

- направить запросы на установление MAC-адресов используемых компьютеров, IMEI номеров планшетов или мобильных телефонов;

- провести ОРМ СИТКС;

- определить местонахождение абонента, владельца номера IMEI планшета, мобильного телефона, или местонахождение абонента владельца MAC-адреса компьютера, через провайдера сети Интернет (в задании необходимо указывать не только сам номер, но и название сайта и точное время его посещения абонентом);

- провести СИТКС по адресам электронной почты фигурантов (GPRS-СИТКС);

- направить запрос на установление анкетных данных владельцев номеров мобильных телефонов;

- провести СИТКС по номерам мобильных телефонов, в том числе по установлению их IMEI, активность, привязки к базовым станциям;

- поставить на контроль телефонные переговоры фигурантов по выявленным номерам (ОРМ «Прослушивание телефонных переговоров»), а также в целях обеспечения возможности использования в дальнейшем в установленном законом порядке записей телефонных переговоров в определенные сроки, указанные в ст. 5 Закона об ОРД, направить письмо в техническое подразделение о сохранности носителей информации;

- провести СИТКС по СМС и иным сообщениям, направляемых с мобильных телефонов проверяемых или разрабатываемых фигурантов (для обеспечения возможности использования записи переговоров в качестве доказательной базы направить письмо о сохранности носителей информации);

- поставить на оперативный контроль телефонные переговоры и СМС-переписки, ведущиеся с номера, указанного в рекламе сбыта наркотиков.

В дальнейшем при получении установочных данных о фигурантах, местах их проживания целесообразно организовать взаимодействие с сотрудниками поисковых подразделений.

На практике возможна оперативно-розыскная ситуация, при которой не удалось в полном объеме получить установочные данные всех фигурантов, входящих в преступную группу, в том числе, места их проживания, досуга или постоянного времяпровождения. В таких случаях необходимо организовать работу по установлению и анализу возможных видеозаписей момента снятия ими денежных средств с установленных банковских карт в банкоматах. Соответствующий запрос должен быть направлен в службу безопасности банка, выдавшего банковскую карту. При хорошо организованном взаимодействии между оперативными подразделениями полиции и службами безопасности банков подобная информация о снятии фигурантом денежных средств может быть получена очень быстро, в том числе и в рамках конфиденциального содействия и сотрудничества. Полученная видеозапись позволяет получить изображение фигуранта. Кроме того, используя системы «Безопасный город, дом, подъезд» и фиксации административных правонарушений ГИБДД, можно подключиться к видеокамерам, находящимся вблизи данного банкомата. Получив информацию с этих камер о времени снятия средств можно отследить маршрут перемещения фигуранта (возможно, до места жительства или до припаркованного автомобиля).

Получение информации о регистрационном знаке автомобиля фигуранта дает возможность:

1) установить его владельца (самого фигуранта, его родственников, подельников, лица, которому принадлежит автомобиль);

2) с камер видеофиксации ГИБДД (система нарушений ПДЦ «Перехват», федеральная система контроля «Паутина», ЕИТС «Поток»,

КРИС и др.) просмотреть изображение лица, управляющего автомашиной, его пассажиров;

3) по камерам видеофиксации ГИБДД установить маршрут перемещения фигуранта, в т.ч. для встречи с подельниками, для получения партии наркотиков от курьера, к местам закладок наркотиков и др.;

4) по камерам видеофиксации можно установить место парковки автомобиля, а затем и место жительства фигуранта (съемная квартира, квартира знакомых или родственников).

Весь период оперативной проверки или разработки целесообразно осуществлять постоянное взаимодействие с информационными подразделениями и подразделениями оперативно-розыскной информации территориальных и других органов МВД России. Тем самым в ходе соответствующего аналитического поиска можно выявлять и получать дополнительную оперативно значимую информацию.

Для доказывания квалификации преступления, совершенного в составе организованной группой или преступного сообщества (преступной организацией)[1], необходимо задокументировать наличие следующих признаков:

- два или более участника;
- совершение одного или нескольких преступлений;
- объединение участников (факт знакомства, предварительное планирование преступной деятельности, наличие относительно стабильных межличностных связей и т.п.);
- устойчивость (стабильность состава, согласованность действий, длительность существования, тщательность или длительность подготовки преступлений, техническая оснащенность, наличие организатора, распределение функций, постоянство форм и методов и т.д.).

Учитывая специфику предмета доказывания по делам указанной категории, можно выделить два направления сбора доказательственной базы:

[1] Далее – ОГ и ПС.

1) на подтверждение факта организации ОГ и ПС;

2) на доказывание конкретных преступных деяний (контрабанда, приобретение, сбыт и хранение наркотиков), совершенных ОГ и ПС в целом, и каждым из его участников в частности.

В ходе реализации комплекса ОРМ вначале рекомендуется обращать особое внимание на своевременное установление информации о наименее защищенных от разоблачения звеньях ОГ и ПС. К таким звеньям относятся группы непосредственных исполнителей («закладчиков»). Психологически выверенная и продуманная тактика проведения комплекса ОРМ, направленных на установление внутригрупповых противоречий, соперничества в борьбе за власть между отдельными членами ОГ и ПС, позволяет получить оперативно-значимую информацию и о других сторонах функционирования ОПФ, в целом, и его организаторов и руководителей, в частности.

2.7. Документирование и реализация материалов оперативной разработки лиц, причастных к сбыту наркотиков бесконтактным способом

В ходе документирования целесообразно несколько раз провести ОРМ «Проверочная закупка». Во-первых, это позволяет изъять образец сбываемого вещества для установления вида НС и (или) ПВ, а также для обеспечения возможности проведения ОРМ «Сбор образцов для сравнительного исследования» и «Исследование предметов и документов» (сравнительной экспертизы) с другими изымаемыми из тайников наркотиками. Во-вторых, несколько эпизодов сбыта наркотиков будут подтверждать неоднократность совершения преступлений участниками разрабатываемой группы, что позволит в дальнейшем предъявить им обвинение в совершении преступлений в составе ОГ или ПС.

Повторность проведения проверочных закупок ограничена определенными условиями. Так, например, необходимо учитывать, что проведение повторного ОРМ, связанного с очередной проверочной закупкой у одного и того же лица, должно быть обоснованно и мотивированно, в том числе вновь выявленными основаниями и целями с обязательным вынесением нового постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность[1].

Целями повторного ОРМ, в т.ч. и проверочной закупки, могут являться выявление, предупреждение, пресечение и раскрытие организованной преступной деятельности и установление всех ее соучастников, выявление преступных связей участников незаконного оборота наркотических средств, установление каналов поступления наркотиков, выявление места производства при наличии оперативно значимой информации по данным фактам и некоторые иные обстоятельства. Кроме того, это могут быть случаи, когда в результате проведенного ОРМ не были достигнуты цели мероприятия (например, сбытчик наркотического средства не установлен, произошла частичная расшифровка проводимых мероприятий и т.д.).

Для проведения ОРМ «Проверочная закупка» необходимо составить следующие оперативно-служебные документы;

- рапорт оперативного сотрудника о необходимости закупки;
- постановление о проведении проверочной закупки, утвержденное руководителем органа, уполномоченного на осуществление ОРД;
- заявление гражданина о согласии на участие в данном ОРМ;
- личный досмотр лица, выступающего в качестве «покупателя», перед проверочной закупкой;
- досмотр его автотранспортного средства (при наличии);
- протокол пометки и вручения денежных средств закупщику с приложением ксерокопий используемых денег;

[1] О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России: приказ МВД России от 19 июня 2012 г. № 608 // Российская газета. 2012. № 177.

- протокол (акт) вручения аудио-, видеоаппаратуры;
- протокол добровольной выдачи приобретенного наркотического средства;
- протокол выдачи аппаратуры;
- отношение на исследование приобретенного вещества;
- справка об исследовании экспертного подразделения;
- объяснения понятых (незаинтересованных лиц);
- объяснение закупщика;
- справка (акт) о проведении ОРМ;
- рапорт об обнаружении признаков преступления.

Проверочную закупку целесообразно проводить одновременно с прослушиванием телефонных переговоров и скрытым наружным наблюдением, в ходе которых необходимо фиксировать разговор покупателя с диспетчером, а также получение СМС-сообщения о месте закладки. Кроме того, необходимо фиксировать размещения закладок «закладчиком».

В случаях установления мест, используемых для закладок НС и (или) ПВ, силами подразделения, ведущего разработку, или с привлечением поисковых подразделений МВД России необходимо организовать скрытое наружное наблюдение за указанными местами с целью установления визуального контакта с лицом, осуществляющим закладку. В период осуществления наблюдения и установления мест закладок для сбора доказательств необходимо применение фото-, видеозаписи, а также при необходимости и наличии возможности - пометки закладок различными красителями (люминесцентными).

При документировании преступной деятельности фигурантов необходимо помнить, что если проводить задержание фигуранта, приобретающего закладку, то преступные действия сбытчика, сделавшего ее, и (или) лиц, организовавших ее сбыт, могут быть квалифицированы по статье 228.1 УК РФ. В то же время, если проводить задержание лица, осуществившего закладку, то квалифицировать его действия можно по

статьям 30 и 228.1 УК РФ, т.е. покушение на сбыт, в том числе с применением ст. 33 УК РФ, то есть соисполнение при сбыте с основным распространителем, в случае если он будет говорить, что его кто-то попросил осуществить данную закладку.

В случаях сбора всей необходимой информации об участниках сети сбыта наркотиков, в т.ч. сведений о распределении ролей в ней, а также наличия доказательств такой деятельности необходимо переходить к непосредственной реализации оперативной проверки или разработки.

На этом этапе необходимо запланировать задержания фигурантов. Бесконтактная схема продажи наркотиков дает сотрудникам правоохранительных органов определенные преимущества. Так, например, необходимо организовать и проводить одновременные задержания только лиц, которые находятся в непосредственном контакте друг с другом или проживают рядом, так как информация о задержании одного из них быстро станет известна другим фигурантам, и, соответственно, те попытаются скрыться и уничтожить улики. Однако при нерегулярном общении посредством Интернета и на больших расстояниях между участниками одного из звеньев ОГ и ПС информация о задержании одного из участников схемы сбыта НС и ПВ может стать известна другим фигурантам через некоторое время.

На этапе реализации оперативных материалов необходимо обязательно предусмотреть проведение обысков в местах проживания фигурантов для изъятия средств мобильной связи, банковских карт и компьютерной техники, а также иных оперативно-значимых материалов и т.п. Кроме того, обыски должны быть проведены и в местах хранения наркотиков.

После задержания лиц обязательным условием документирования будет являться осуществление аудио-, видеозаписи опроса (оформляется впоследствии соответствующими документами – актом, справкой). Целью проведения данных мероприятий является сбор дополнительных доказательств (при проведении аудиозаписи получают образцы голоса

фигуранта, необходимые впоследствии для проведения фоноскопической экспертизы, а при проведении видеозаписи опроса получают материалы, позволяющие следователю составить наиболее полную картину происходящего).

При проведении опроса задержанных лиц, в том числе и разведывательного характера, необходимо устанавливать:

- сведения, характеризующие личность задержанного;
- сколько раз осуществлялись закладки;
- пути следования, вид транспорта, используемого для перевозки наркотиков;
- какое вознаграждение причиталось за осуществление закладки, от кого и каким образом предполагалось его получить;
- когда осуществлялись аналогичные действия;
- потребляет ли наркотики сам закладчик;
- средства, способы связи и контактов;
- источник приобретения наркотиков;
- когда, кем, где, у кого приобретались наркотики;
- кто производил их расфасовку;
- кому сбываются наркотики, места их сбыта, обстоятельства сбыта, цена продаваемых наркотиков;
- имеются ли постоянные покупатели, объем закупаемого ими «товара», приметы и другие сведения об этих лицах;
- места и способы хранения наркотиков;
- способы расчета с поставщиком, номера банковских счетов, адреса электронных кошельков и т.д.;
- задерживался ли ранее правоохранительными органами и при каких обстоятельствах;
- иные сведения с учетом конкретной ситуации;

- «никнейм» лица (лиц), с которым осуществлялась связь при приобретении наркотических средств;
- точный электронный адрес форума или сайта, через который осуществлялась связь и реализация самого наркотического средства, а также другие вопросы, имеющие значения для документирования преступной деятельности проверяемых (разрабатываемых) фигурантов.

Опросы участников сети сбыта наркотиков бесконтактным способом, как правило, бывают очень результативны. Это обусловлено правдивостью их показаний, связанной с возрастом преступников (20-25 лет), отсутствием у них криминального опыта, неожиданным разоблачением и т.п.

Помимо опросов (допросов) лиц, участвующих в НОН, проводятся осмотры участков местности, где находилась закладка НС и (или) ПВ, либо где производилось задержание названных лиц.

Другим важным направлением по документированию действий фигурантов, осуществляющих вышеуказанный НОН, является производство личного досмотра задержанных лиц с целью изъятия НС и (или) ПВ, принадлежащих им мобильных телефонов и иных предметов, которые могут иметь доказательственное значение для дела, а также иных средств, посредством которых осуществлялся выход в Интернет (в том числе ПЭВМ, ноутбук, смартфон, планшетный компьютер, жесткие диски, CD и DVD диски и др.). В рамках ОРМ «Исследование предметов и документов» направить задание на проведение ОД-И (оперативный досмотр-информации) электронных носителей информации, а именно средств мобильной связи (телефоны, смартфоны и планшетные ПК) и ПЭВМ. Это мероприятие дает возможность получения полной информации, в том числе удаленной (электронной переписки, выхода в сеть Интернет). Необходимо помнить, что при досмотровых мероприятиях, а в последующем при направлении веществ на исследование с постановкой вопроса о проведении обработки предметов упаковки на наличие следов пальцев рук должны быть использованы перчатки для сбора доказательств. При обыске у подозреваемых объектами

поиска и изъятия будут являться НС и (или) ПВ, записные книжки, банковские карты, мобильные телефоны, сим-карты, компьютерная техника с последующим обязательным осмотром и назначением необходимых экспертиз.

После проведения мероприятий по реализации ДОУ в установленном порядке проводится рассекречивание оперативных материалов и их представление в следственные органы[1].

Комплекс дальнейших ОРМ, следственных и иных действий обычно включает в себя допросы свидетелей (в том числе с учетом результатов исследований и экспертиз), очные ставки (особенно, если надо устранить возникшие на предыдущем этапе расследования различные противоречия), следственные эксперименты, новые осмотры и освидетельствования, обыски и выемки, наложение ареста на банковские счета, контроль и запись переговоров и др. В целях координации и организации совместной деятельности оперативных, следственных и иных подразделений территориальных органов МВД России создаются специализированные следственно-оперативные группы[2].

Делая вывод, следует отметить, что работниками специализированных оперативных подразделений по контролю за оборотом наркотиков должно осуществляться оперативное сопровождение всех этапов уголовного и судебного процесса, начиная от стадии возбуждения уголовного дела, расследования, судебного следствия и завершая организацией оперативной разработки фигурантов совместно с оперативными подразделениями ФСИН

---

[1] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю или в суд : приказ МВД РФ, Минобороны РФ, ФСБ РФ, ФСО РФ, Федеральной таможенной службы, СВР РФ, ФСИН, Федеральной службы РФ по контролю за оборотом наркотиков и Следственного комитета России от 27 сентября 2013 г. №776/703/509/507/1820/42/535/398/68 // СТРАС «Юрист» (дата обращения: 11.12.2018).

[2] Об объявлении Инструкции по организации совместной оперативно-служебной деятельности подразделений ОВД РФ при раскрытии преступлений и расследование уголовных дел: приказ МВД России от 29 апреля 2015 г. № 495дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

в местах лишения их свободы, как правило, если фигуранты получили лишение свободы на срок включительно до 10 лет.

III. ДЕЯТЕЛЬНОСТЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО РАСКРЫТИЮ МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ В СЕТИ ИНТЕРНЕТ

3.1. Правовая характеристика мошенничества с использованием сети Интернет

Мошенничество является относительно обособленным феноменом, обладающим рядом специфических признаков. На преобладание экономических факторов в распространении мошенничества обращают внимание, например, И.Я. Фойницкий и многие другие эксперты и ученые. Подчеркивая, что «мошенничество как разновидность имущественного обмана есть преступление цивилизационное, и возрастает в масштабах при значительном развитии экономического оборота»[1], И.Я. Фойницкий указал на тот факт, что распространенность мошенничеств выше в тех странах, которые имеют более высокое промышленно-торговое положение. Современные формы мошенничества, изменяясь на протяжении всего двадцатого века, приобрели собственную специфику. Зачастую они настолько отличаются друг от друга, что влекут за собой необходимость проведения криминалистических исследований отдельных мошеннических схем, распространенных в различных сферах экономической деятельности.

Не удивительно, что сегодня мошенничество может быть сопряжено с совершением преступлений в сфере высоких технологий, поскольку развитие глобальной сети Интернет создает все больше возможностей для ведения полноценной экономической деятельности. Подтверждением сказанного является Письмо Федеральной комиссии по рынку ценных бумаг России от 20 января 2000 г. № ИБ-02/229 «О возможных мошеннических схемах при торговле ценными бумагами с использованием сети Интернет», в котором комиссия акцентировала внимание российских инвесторов на том, что инвестирование денежных средств на фондовых рынках с использованием сети Интернет сопряжено с риском быть вовлеченными в различного рода

[1] Фойницкий И.Я. Мошенничество по русскому праву. С-Пб.: 2014. С. 83.

мошеннические схемы[1].

В реальной действительности правонарушитель несанкционированно вмешивается в процесс надлежащего функционирования обработки данных компьютером таким образом, что это приводит к получению выгоды для себя либо третьих лиц. В иных же случаях посредством сети Интернет осуществляются хорошо известные схемы обмана людей: мошеннические предложения продажи товаров по привлекательно низким ценам; инвестиции в недвижимость в иностранном государстве; предоставление ссуд на условиях, обеспечивающих исключительно высокую норму прибыли; предоплата недостаточно тщательно охарактеризованных товаров; или предложение присоединиться к финансовой пирамиде.

Согласно статистическим данным ГИАЦ МВД России в 2017 году в РФ сотрудниками ОВД выявлено 105087 преступлений экономической направленности, из них 204870 – это мошенничества (по сравнению с аналогичным периодом 2016 года наблюдается увеличение на 6,8%).

Таким образом, доля мошенничества составляет около 26%, (¼ часть всех экономических преступлений). Мошенничество является одним из самых распространенных видов экономических преступлений[2].

Из-за разнообразия мошеннических форм не достигнуто единство мнений среди ученых и практиков по выработке единого понятийного аппарата даже на терминологическом уровне. По меткому замечанию С.В. Петровского, такое состояние в полной мере относится ко всем сферам правового регулирования отношений, возникающих при использовании глобальной сети Интернет, что «отражает отсутствие системного подхода» и «проявляется, в частности, в избыточном терминологическом

[1] Письмо ФКЦБ России № ИБ-02/229 от 20 января 2000 года «О возможных мошеннических схемах при торговле ценными бумагами с использованием сети Интернет» // Вестник Федеральной комиссии по рынку ценных бумаг. 2000. № 1 (38). С. 21-22.

[2] Официальный сайт Министерства внутренних дел Российской Федерации. URL: http://www.mvd.ru/presscenter/statistics/reports (дата обращения: 23.11.2018).

многообразии»[1]. Ограничившись собственным объектом исследования, мы смогли выделить несколько наиболее используемых вариантов наименования изучаемого явления в России: «мошенничество в Интернете», «интернет-мошенничество», «мошенничество в глобальной сети», «сетевое мошенничество»; из за рубежом: «internet-fraud», «internetscams», «on-linefraud (scams)». По сути, все эти понятия обозначают одно и то же явление. Поэтому в данной учебной работе используется понятия «мошенничество в глобальной сети Интернет». По нашему мнению, наиболее полно разграничить интернет-мошенничество со смежными явлениями в состоянии следующая совокупность признаков:

- способ совершения преступления;
- цель и мотив преступления;
- последствия преступления;
- орудие (инструмент) преступления.

Проводя условные параллели с уголовным правом, необходимо сказать, что пользователь действительно не желает, но при этом сознательно допускает возможность ущемления собственных имущественных интересов или же относится к таким последствиям безразлично. Так, небрежное отношение к защите собственных персональных данных либо их невольное разглашение могут привести к тому, что подобными сведениями воспользуется мошенник для совершения юридически значимых действий от имени жертвы в собственных корыстных целях.

Мошенничество в глобальной сети Интернет как явление — это совокупность преступлений, характеризующихся единством способа совершения преступления (использование технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет, для совершения обмана человека или «обмана» компьютерной системы), а также корыстной мотивацией преступной

[1] Петровский С.В. Интернет-услуги в российском праве. М.: Издательский сервис, 2015. С. 8.

деятельности.

Под «обманом» компьютерной системы (автоматизированной системы обработки данных – АСУ) следует понимать получение доступа к процессам автоматической обработки данных одним лицом от имени другого с целью активации алгоритмов действия АСУ, результатами которых являются утрата кем-либо имущества, имущественных прав, причинение имущественного ущерба. Все компьютерные мошенничества основываются на обмане компьютерной системы (АСУ).

Интернет-мошенничество является частью компьютерной преступности. В ее структуре следует выделять преступления в сфере компьютерной информации (глава 28 УК РФ), которые являются общим конструктом, отражающим единый информационно-компьютерный способ совершения компьютерных преступлений. Вместе с тем указанные составы могут применяться самостоятельно. В зависимости от способов использования компьютерной информации в противоправных целях следует выделять еще два структурных блока компьютерной преступности: а) преступления, в которых электронная информация является орудием или средством совершения другого преступления; б) преступления, где компьютеры используются для «визуализации» информации. Мошенничество в глобальной сети Интернет одновременно относится к первой и второй группе компьютерных преступлений. Интернет является инструментом распространения машинно-обрабатываемой информации; компьютер, подключенный к глобальной сети – средством ее «визуализации».

Поскольку Интернет является лишь одним из возможных способов доставки (распространения) компьютерной информации, всю компьютерную преступность нельзя свети к интернет-преступности. Однако интернет-преступность вне компьютерной преступности не существует, что обусловлено технологическими особенностями – Интернет – глобальная компьютерная сеть. Использование Интернета как средства распространения

информации с неизбежностью ведет к распространению мошеннических схем в этой области. Поскольку манипуляция с информацией является сутью преступного обмана.

Интернет объединяет (позволяет совершать) лишь часть мошеннических схем, существующих в действительности. Можно утверждать о наличии двух видов интернет-мошенничества: 1) нетрадиционные компьютерозависимые формы (компьютерное мошенничество), зачастую использующие коммуникационные возможности Интернета, поскольку само преступление (хищение) немыслимо без модификации, копирования компьютерной информации; 2) традиционные компьютеронезависимые» формы мошенничества, использующие возможности Интернет для реализации преступного умысла в целях обогащения.

Система мер предупреждения указанного явления складывается из совокупности трех уровней предупреждения – общего, специального, индивидуального, каждый из которых предусматривает собственные направления предупреждения и конкретные формы реализации.

В области общего предупреждения мошенничества в глобальной сети Интернет основными направлениями являются совершенствование уголовной политики РФ в сфере компьютерной преступности, создание эффективной системы социально-правового контроля над распространением мошенничества в Интернет, криминологическая экспертиза нормативно-правовых актов, посвященных развитию и функционированию сети Интернет в России, международно-правовое регулирование сети Интернет.

Основными формами реализации общего предупреждения указанного вида преступности должны стать: а) разработка и принятие концептуального закона о развитии российского сегмента сети Интернет, включение в указанный закон положения о недопустимости использования информационно-коммуникативных технологий в неправомерных целях; б) разработка и принятие федерального закона о негосударственных субъектах

предупреждения мошенничества и системе мер государственной поддержки такой деятельности; в) устранение разногласий в понимании компьютерного мошенничества путем расширения понятия обмана как способа совершения мошенничества не только в отношении человека, но и автоматизированных компьютерных систем; г) внесение изменений в гражданское законодательство с целью обособления и регламентации процедур заключения сделок, совершаемых в электронной форме; д) принятие мер по совершенствованию правовых основ деятельности электронных платежных систем для выполнения приоритетной задачи – борьбы с анонимностью пользователей и совершаемых ими транзакций.

В области специального предупреждения мошенничества в глобальной сети Интернет основными направлениями являются организационно-техническое предупреждение и виктимологическая профилактика, реализация которых проводится в два этапа: текущий и последующий.

В качестве основных форм специального предупреждения должны выступить: а) разработка и принятие государственной программы по внедрению электронной цифровой подписи в гражданский оборот; б) введение идентификации личности пользователя в случае предоставления ему доступа в Интернет из мест коллективного пользования; в) присвоение каждому пользователю Интернета электронного сертификата (электронного паспорта), содержащего персональную информацию о его владельце; г) создание правовых условий (запрета) в сфере регулирования деятельности интернет-провайдеров, в которых регистрация анонимного ящика электронной почты без заключения письменного договора станет невозможна; д) учреждение всеобъемлющего русскоязычного информационного ресурса.

Рассмотрим вопрос о последствиях интернет-мошенничества. Реализация корыстных целей за чужой счет предполагает следующие последствия преступления:

А) Утрата имущества собственником (владельцем). К примеру,

завладение имуществом осуществляется при дистанционной торговле (мошенничества на интернет-аукционах, доставке товаров из интернет-магазинов).

Б) Утрата права на имущество; при этом «утрата» – довольно спорный термин в сфере современных компьютерных технологий.

Речь, скорее, идет о предоставлении равнозначного права. В результате «фишинга» – хищения идентификационных данных – мошенник получает возможность вывести средства из электронной платежной системы (ЭПС), оплатить ими покупку. При этом законный пользователь, как правило, не теряет возможность пользоваться услугами ЭПС.

В силу неопределенности правового статуса ЭПС и самих «электронных денег» невозможно однозначно определить, является ли пользователь такой системы обладателем имущественных прав по отношению к ЭПС или вкладчиком. «Электронные деньги» существуют только в рамках той системы, которой они эмитированы, и не являются общепринятым платежным средством, обязательным к приему.

В) Причинение имущественного ущерба. В качестве типичной ситуации может рассматриваться одна из разновидностей компьютерного мошенничества – «фрикинг» – неправомерное осуществление доступа в Интернет за счет других пользователей[1].

Таким образом, «фрикинг» отличается от иных форм мошенничества лишь последствиями. В соответствии с разъяснениями Судебной коллегии по уголовным делам Верховного Суда РФ субъективная сторона преступления, предусмотренного ст. 165 УК РФ, характеризуется прямым умыслом на извлечение материальной выгоды за чужой счет. Сознанием виновного должно охватываться причинение имущественного ущерба собственнику или законному владельцу имущественных прав.

Необходимо отметить, что специфическим признаком интернет-

[1] Анохин В.Н. Электронные платежи в обеспечении эффективного функционирования платежной системы: дис. … канд. экон. наук. М., 2015. С. 56.

мошенничества является использование Интернета в противоправных целях. Глобальная компьютерная сеть Интернет (сокр. от «Interconnected Networks» – объединенные сети) представляет собой всемирную систему объединенных компьютерных сетей, построенную на использовании протокола адресации IP и маршрутизации пакетов данных «TCP».

В силу развития техники встает вопрос об устройствах, отличных от компьютерной техники, позволяющих осуществлять доступ в глобальную сеть Интернет. Развитие мобильной телефонии привело к предоставлению целого спектра услуг владельцам мобильных телефонов, на которые телефон в его классическом понимании не рассчитан.

Не является исключением и глобальная сеть Интернет. Технологии предоставления доступа к нему у операторов сотовой связи различны. Мы предлагаем различать протокол подключения «WAP» и технологию «WWW». Протокол «WAP» задействован исключительно в мобильных телефонах и предоставляет доступ лишь к отдельному изолированному сегменту глобальной сети Интернет, ориентированному на потребителей услуг мобильных операторов связи.

Долгое время мобильный телефон не был способен предоставить доступ в «World Wide Web». На это был способен такой класс мобильных устройств, как смартфон. Смартфон – устройство связи, находящееся под управлением операционной системы, обладающей многозадачностью, встроенным программным обеспечением (браузером) с возможностью использования ресурсов и технологических возможностей именно «World Wide Web». Смартфон может быть приравнен по технологическим возможностям к компьютерной системе. Технология, внедренная в мобильные телефоны, позволила осуществлять практически полноценный доступ в Интернет и с этих устройств, что еще больше размыло технологические границы. Поэтому сегодня не представляется возможным абсолютно точно определить все классы устройств, позволяющих осуществлять доступ в «World Wide Web».

Относительно статьи 165 УК РФ необходимо прояснить механизм противоправного использования сети Интернет. На первый взгляд может показаться, что коммуникативные возможности глобальной сети не используются для достижения преступного результата, поскольку преступник посягает на сами отношения по ее правомерному использованию. Однако это верно лишь отчасти, что и способен проиллюстрировать удачно избранный Т.П. Кесареевой термин «вхождение»[1]. При использовании глобальной сети Интернет за чужой счет правонарушитель покушается на материальный носитель веб-сервера провайдера с целью модификации имеющейся на нем информации билинговой системы. В телекоммуникационной сфере билинговая система официально именуется автоматизированной системой расчетов (АСР), способной к учету предоставленных услуг, их тарификации и выставлению счетов для оплаты.

Таким образом, чужие учетные записи предоставляют преступнику возможность причинять имущественный ущерб путем пользования Интернета даже в личных правомерных целях.

Исходя из вышеизложенного, можно утверждать, что спектр криминологического интереса к преступному явлению под названием «мошенничество в глобальной сети Интернет» достаточно широк, поскольку сюда входят и хищения с использованием компьютерных систем, подключенных к глобальной сети Интернет; и причинение имущественного ущерба путем обмана и злоупотребления доверием также с использованием компьютерных систем, подключенных к глобальной сети Интернет; и «традиционные» мошеннические схемы, которые охватываются диспозицией ст. 159 УК РФ, но обязательным элементом в реализации преступного замысла при этом является использование компьютерных систем, подключенных к глобальной сети Интернет.

Можно выделить четыре характерных признака исследуемого явления:

---

[1] Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис… канд. юрид. наук. М., 2016. С.4.

а) использование для совершения преступления компьютерных систем (автоматизированных систем);

б) использование технологических и коммуникационных возможностей Интернета;

в) совершение не только обмана человека, но и «обмана» компьютерной системы;

г) корыстная мотивация преступной деятельности.

Таким образом, мошенничество в глобальной сети Интернет как явление – это совокупность преступлений, характеризующихся единством способа совершения преступления (использованием технологических и коммуникационных возможностей компьютерных систем, подключенных к глобальной сети Интернет, для совершения обмана человека или «обмана» компьютерной системы), а также корыстной мотивацией преступной деятельности.

Говоря об уголовно-правовой и криминалистической характеристике мошенничества с использованием сети Интернет необходимо отметить, что определяющим признаком любой формы мошенничества является способ совершения преступления: обман или злоупотребление доверием, являющиеся единственным, исключительным способом совершения данного вида преступлений. В диспозициях некоторых статей также упоминается обман в качестве возможного способа совершения преступления. Среди них выделяют те, которые не являются хищениями (ч. 2 ст. 141, ст. 150, ст. 188, ст. 339 УК РФ); а также группы преступных обманов (например, ст. 176, ч.1 ст. 195, ст. 197 УК РФ), которые, по мнению отдельных ученых, выступают «специальными нормами по отношению к мошенничеству»[1].

С криминалистической точки зрения, интересна идея Е.В. Суслиной, позволяющая выделить мошенничество в самостоятельную группу преступных посягательств, образующих уникальный уголовно-правовой

[1] Суслина Е.В. Ответственность за мошенничество по Уголовному кодексу Российской Федерации: автореф. дисс. … канд. юрид. наук. Екатеринбург, 2014. С 27.

феномен. Однако имеется ряд объективных противоречий, которые не позволяют нам полностью разделить подобную точку зрения. В результате анализа объективных и субъективных признаков мошенничества и смежных составов преступлений в сфере экономики, мы пришли к выводу о необходимости объединения ст. 159, 165 УК РФ и некоторых иных составов, предлагая перейти на новую систему определений обманных имущественных преступлений, заключающуюся в выделении мошенничества «в самостоятельно существующую наряду с хищением уголовно-правовую категорию, родовым понятием для целого ряда обманных имущественных посягательств»[1].

Отметим, что некоторые его формы могут осуществляться непосредственно через Интернет. Так, «фрикинг» – причинение имущественного ущерба путем использования реквизитов чужих учетных записей для доступа в Интернет – невозможен без удаленного воздействия на сервер провайдера посредством той же глобальной сети. Конвенция Совета Европы «О киберпреступности» («Councilof Europe Conventionon Cybercrime») в статье 8 «Мошенничество с использованием компьютерных технологий» раскрывает это понятие следующим образом: «лишение другого лица его собственности путем:

- любого ввода, изменения, удаления или блокирования компьютерных данных;

- любого вмешательства в функционирование компьютерной системы, с мошенническим или бесчестным намерением, неправомерного извлечения экономической выгоды для себя или для иного лица»[2].

Из приведенной нормы неизбежно следует вывод, что компьютерное мошенничество неразрывно связано с противоправными посягательствами на охраняемую законом компьютерную информацию. Отечественная судебная практика предлагает квалифицировать компьютерное мошенничество по

[1]Там же.

[2] The Convention on Cybercrime (ETS) 185 / Council of Europe 2015. – URL: http://www.conventions.coe.int/Treaty/ (дата обращения: 07.11.2018).

статье 159 УК РФ, а также в зависимости от обстоятельств дела по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Аналогично квалифицируется компьютерное мошенничество и в виде причинения имущественного ущерба путем обмана или злоупотребления доверием, ибо незаконный доступ в Интернет, связанный с использованием чужих учетных записей, составляет основную массу таких преступлений.

По мнению некоторых ученых, такая трактовка закона, с точки зрения уголовного права, неоправдана. Тропина Т.Л. отмечает, что компьютерное мошенничество является обманом компьютерной системы, а не человека: «Обман или злоупотребление доверием, предусмотренные в качестве признака объективной стороны мошенничества, с учетом толкования этой статьи Верховным Судом Российской Федерации (добровольная передача имущества потерпевшим), являются обманом или введением в заблуждение физического лица[1]. В случае с так называемым компьютерным мошенничеством потерпевший может ничего не знать о передаче имущества или права на имущество в момент этой передачи, и вообще не желать ее, то есть отсутствует обязательный волевой признак – добровольность»[2]. Тропина Т.Л. предложила криминализировать компьютерное мошенничество путем введения понятия «компьютерного хищения» в статье 159.1 УК РФ в значении «хищения чужого имущества или приобретения права на чужое имущество, совершенного путем ввода, изменения, удаления или блокирования компьютерных данных либо другого вмешательства в

[1] См. п. 12 Постановления Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2008. № 2. С. 3.

[2] Тропина Т.Л. Компьютерное мошенничество: вопросы квалификации и законодательной техники. 2013. URL: http://www.connect.ru/ (дата обращения: 07.11.2018).

функционирование компьютера или компьютерной системы»[1], тем самым предлагая исключить противоречия в понимании компьютерного мошенничества.

Данная трактовка компьютерного мошенничества не учитывает причинение имущественного ущерба путем обмана и злоупотребления доверием, а также не акцентирует внимания на возможности совершения данного преступления посредством Интернета, игнорируя большую общественную опасность удаленного и трансграничного «взлома» компьютерной системы в целях хищения. Однако за счет этого статья 159.1 УК РФ получает более универсальный характер, охватывая все способы вмешательства в работу компьютерной системы в целях совершения хищения. Вполне возможно, что подобную ситуацию можно исправить введением нового квалифицирующего признака: то же деяние, совершенное с использованием удаленного доступа к компьютерной системе, а равно группой лиц по предварительному сговору.

В силу особенностей юридической техники отечественного уголовного законодательства легального определения компьютерного мошенничества в УК РФ нет. Однако несмотря на то, что Российская Федерация не ратифицировала Конвенцию Совета Европы «О киберпреступности», само наличие явления признается. Об этом свидетельствуют как вышеупомянутая практика квалификации, так и тот факт, что отечественные правоохранительные органы РФ ориентируются на кодификатор рабочей группы Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х гг.[2]

В соответствии с ним компьютерные мошенничества классифицированы следующим образом:

- QFC – компьютерные мошенничества, связанные с хищением

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дисс. … к.ю.н. Владивосток, 2016. С. 13.

[2] Мещеряков В.А. Теоретические основы криминалистической классификации преступлений в сфере компьютерной информации // Конфидент. 2016. С. 5.

наличных денег из банкоматов;

- QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств;

- QFG – мошенничества и хищения, связанные с игровыми автоматами;

- QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из них путем манипуляции программами;

- QFP – компьютерные мошенничества и хищения, связанные с платежными средствами;

- QFT – телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

Таким образом, соотношение двух понятий «интернет-мошенничество» и «компьютерное мошенничество» лежит именно в области использования коммуникативных технологий Интернет.

Существуют разные способы совершения мошенничества с использованием сети Интернет:

1. мошенничество в сфере азартных игр.

2. мошенничество в сфере онлайн-аукционов.

3. мошенничество с использованием электронных денег и электронной системы платежей.

4. мошенничество в сети Интернет в сфере предоставления товаров и услуг.

5. мошенничество в сфере интернет-знакомств и др.

Наиболее востребованными сферами, в которых пользователи подвергаются атакам со стороны мошенников, являются электронные деньги и электронные системы платежей, а также сфера товаров и услуг. В связи с этим необходимо подробно рассмотреть способы совершения мошенничества, выделить наиболее важные особенности предварительного расследования в каждом из способов.

Мошенничество с использованием электронных денег и электронной системы платежей.

Директива Европейского парламента и Совета № 2000/46/ЕС от 18 сентября 2000 года определила понятие электронных денег, которые являются «денежной стоимостью, представленной требованием на эмитента, которая:

1) хранится на электронном устройстве;

2) эмитируется по получению средств эмитентом в размере, не менее внесенной в качестве предоплаты денежной суммы;

3) принимается в качестве средства платежа иными институтами»[1].

Таким образом, на наш взгляд, под электронными деньгами понимаются любые платежные средства или системы, которые позволяют произвести платежи посредством информации, хранимой на электронных носителях. Для распоряжения электронными деньгами в Сети необходимо использовать электронные платежные системы («WebMoney», «Яндекс. Деньги» и т.д).

Существуют разные схемы мошенничества в сфере электронных денег: к примеру, на различных сайтах распространяется информация о том, что в системе «WebMoney» обнаружена прореха, которая позволила создать программу, автоматически увеличивающую количество электронных денег в кошельке пользователя. Эту программу можно приобрести за дополнительные электронные деньги, хранящиеся в электронном кошельке доверчивого пользователя, при загрузке программа оказывается «троянским конем», полностью опустошающей интернет-кошелек этого пользователя.

Встречаются более простые схемы мошенничества: в чате или иной форме общения в Интернете один из пользователей сообщает, что работал оператором или иным рабочим в компании «WebMoney», но его уволили, в

[1] Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: Экономика, Изд-е 2-е, перераб. и доп. В 2-х ч. / под ред. С.А. Глотова; Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2015. С. 183.

связи с этим он безвозмездно раскрывает тайну электронной платежной системы о существовании определенных электронных кошельков, позволяющих при перечислении на них электронных денежных средств увеличивать накопления, которые потом возвращаются обратно в кошелек пользователя. В случае, если неопытный интернет-пользователь отправит на указанный в сообщении кошелек деньги, они не возвращаются, а автоматически списываются со счета. Однако существует определенная проблема, возникающая в ходе расследования мошенничества в сфере электронных платежей, так, законодателю необходимо четко определиться с понятием электронных денег, поскольку в настоящее время они остаются вне поля правового регулирования, выполняя роль «реальных» денег в сети Интернет.

Мошенничество в сети Интернет в сфере предоставления товаров и услуг.

Без преувеличения можно сказать, что одна из самых и объемных частей мошенничества в сети Интернет приходится на сферу товаров и услуг. Данный вид мошенничества можно разделить на несколько групп в зависимости от предмета и способа мошенничества.

Примером незаконных услуг, предлагаемых мошенниками, может служить следующая ситуация: на электронный почтовый ящик пользователя приходит сообщение (спам) с предложением о детализации мобильных переговоров (информация о входящих-исходящих с данными владельцев номеров) и расшифровке СМС-сообщений.

Информация о переговорах за последние 2 месяца стоит 80 долларов, перечислить их нужно по электронной платежной системе. В большинстве случаев после получения половины суммы в качестве предоплаты мошенник не выходит на связь, в оставшихся случаях сообщает, что деньги не получены и просит повторить платеж[1].

[1] Ограблен в сетевых переулках. URL: // http://www.ng.ru/society/2008-02-19/10_internet.html (дата обращения: 01.10.2018).

Так, гр-ка К. дала объявление на сайт «Авито» о продаже котят, указав свой электронный ящик, на который пришло письмо от покупателя, желающего приобрести котенка. Покупатель предложил дать гр-ке К. номер своей банковской карты для предварительного перевода денежных средств за купленное животное. Гр-ка К., будучи уверена в искренних намерениях покупателя, дала номер карты. В этот же день с ее счета было снято 50 тысяч рублей путем взлома пароля банковской карты[1]. В ходе предварительного расследования получена справка, что IP-адрес компьютера, с помощью которого осуществлялся взлом пароля, зарегистрирован на гр-на С. в городе Иркутске. Следователем было дано поручение о производстве отдельных следственных действий и оперативно-розыскных мероприятий, направленных на установление лица, совершившего преступление в городе Иркутске. Однако установить лицо не представилось возможным. Также был сделан запрос в банковское учреждение, в котором подтвердилась информация о том, что со счета потерпевшей К. была снята сумма в 50 тысяч рублей, посредствам взлома пароля в онлайн-кабинете.

Мы считаем, что следователю, помимо вышеуказанных мероприятий, необходимо было допросить в качестве специалиста лицо, обладающее специальными знаниями в области программного обеспечения по установлению сетевых и индивидуальных паролей в банковских личных кабинетах, а также представителей банковского учреждения, занимающихся защитой сетевых ресурсов. Эти знания были крайне важны для определения механизма совершения преступления.

Мошенничество в сфере интернет-знакомств.

В сети Интернет имеется большое количество сайтов знакомств. Для регистрации себя в роли потенциальной невесты (жениха) необходимо внести минимальные данные о себе, и достоверность внесенных данных проверить невозможно. Одна из схем мошенничества выглядит следующим образом: на сайте знакомств девушка объявляет, что хочет выйти замуж за

[1] Уголовное дело № 143600066 // Архив Динского СО при ОВД ст. Динской. 2015.

иностранца, рассказывает надежную и достоверную легенду о себе, подтверждая ее фотографиями, а иногда и достоверными паспортными данными. Далее завязывается переписка, жених приглашает невесту в гости, невеста просит деньги взаймы на дорогу и иные возникшие расходы, а через некоторое время сообщает жениху, что возникли новые расходы и просит помочь материально, после получения денежных средств в конечном счете заканчивает переписку.

Необходимо указать, что существует и положительный опыт по разоблачению мошенников в сфере знакомств в сети Интернет. Так, в Йошкар-Оле в 2002 году сотрудники ОВД разоблачили преступную группу мошенников, работавших по стандартной схеме, выманивших деньги у более чем 200 граждан Канады и США. При этом основная переписка с потенциальными жертвами велась молодыми людьми, являющимися организаторами преступной группы. В их квартире была установлена сеть из 3 компьютеров с выходом Интернет, с которых осуществлялась переписка. Только за один месяц преступная группа выманивала около 30 тысяч рублей, используя реальные паспортные данные девушек, при этом изменяя фотографии. Преступники действовали очень осторожно, переведенные иностранцами денежные средства снимали студентки за вознаграждение в 50 долларов[1]. После поступившего в МИД России заявления от гражданина США в город Йошкар-Ола выехали сотрудники подразделения специальных технических мероприятий, которые задержали группу мошенников и вычислили всю цепочку от организаторов до пособников совершенного преступления. В рассматриваемой ситуации в качестве положительного опыта расследования хотелось бы выделить осмотр компьютерной техники и информации, находящейся в памяти компьютера, принадлежащего мошенникам. В ходе предварительного расследования была назначена компьютерно-техническая экспертиза, в результате которой подтвердились

[1] Мошенничество в сфере знакомств в сети Интернет. URL: http://www.phreaking.ru/showpage.php?pageid=54356 (дата обращения: 15.09.2018).

выводы о том, что именно с этого компьютера выходили в Интернет мошенники, а содержание переписки подтвердило и в полной мере раскрыло обстоятельства совершенного преступления.

На основании вышеизложенного мы пришли к выводу, что расследование мошенничества в сети Интернет имеет свои специфические особенности.

Во-первых, лицу, ведущему предварительное расследование, необходимо привлекать к производству отдельных следственных действий компетентного специалиста в области программного обеспечения.

Во-вторых, на законодательном уровне нет четкого урегулирования понятия электронных денежных средств.

В-третьих, несмотря на развитие инновационных технологий, в настоящий момент пока еще не разработаны методики производства экспертиз, объектом которых является Интернет, и которыми исследуется весь сетевой ресурс и описывается механизм следообразования интернет-следов.

Существует компьютерно-техническая экспертиза, в которой исследуется конкретный объект или информация, содержащаяся в компьютере. 98% опрошенных респондентов (активных интернет-пользователей) на вопрос «Смогли бы Вы в повседневной деятельности обойтись без сети Интернет?» ответили категорическим отрицанием, что подчеркивает зависимость нашего общества от глобальной сети, в которой будут развиваться новые, более изощренные способы мошенничества.

3.2. Особенности расследования и раскрытия мошенничества, совершенного с использованием сети Интернет

Криминальная статистика свидетельствует, что преступления в сфере информационных технологий пока составляют незначительную часть в структуре преступности[1]. Однако ущерб, причиняемый ими, по мнению

[1] Состояние преступности в России в 2017 г. URL: www.mvd.ru/presscenter/statistics/reports/show_88233 (дата обращения: 20.11.2018).

ведущих специалистов в этой области, практически не поддается оценке[1]. Используемые злоумышленниками способы маскировки своих действий и противодействия расследованию существенно затрудняют борьбу органов внутренних дел с преступлениями данного вида. Все это и некоторые иные данные свидетельствуют, что подобные преступления имеют высокую латентность и имеют тенденцию к своему росту.

Считаем также необходимым обратить внимание на то, что преступления в сфере компьютерной информации совершаются преимущественно молодыми людьми в возрасте от 17 до 35 лет. Значительная их часть имеет специальное образование (высшее, средне-специальное), связанное со сферой компьютерных технологий, но встречаются и те, кто получил необходимые для совершения преступлений знания иным путем – самостоятельно, от знакомых, и др.

Лица, совершающие данные преступления, могут совершать их в группе, в некоторых случаях лично не встречаясь с соучастниками. Для знакомства и координации своих действий они могут использовать сайты и специальные сетевые форумы, где обсуждаются способы незаконного проникновения в чужие компьютеры и компьютерные системы, маскировки «следов» проникновения и др.[2]

Раскрытие и расследование преступлений в случае использования преступниками «электронных кошельков» имеет свои особенности. Исследование материалов уголовных дел свидетельствует, что преступники при совершении преступлений в сфере интернет-технологий часто используют т.н. «электронные кошельки» платежных систем «Yota», «RBK-money», «Yandex-деньги» и подобные им. Предпочтение злоумышленников использования «электронных кошельков» объясняется тем, что последние, выполняя функции банковского счета, не требуют ни указания персональных данных его владельца, ни его непосредственной идентификации при

[1] Осипенко А.Л. Сетевая компьютерная преступность теория и практика борьбы. М.: МГУ, 2016. С. 42.
[2] Там же.

проведении финансовых операций. Зарегистрировать «электронный кошелек» можно через сеть Интернет, при этом предоставив вымышленные данные о себе, либо вообще указав вместо них случайное сочетание букв и цифр.

Преступниками «электронные кошельки» в основном используются как «промежуточное звено» в цепи перемещения похищаемых денежных средств. После поступления на используемые злоумышленниками «электронные кошельки» денежные средства переводятся далее на другие «электронные кошельки», счета номеров сотовой связи или банковские счета.

При этом целесообразно изучать информацию не только о счетах, на которые перечислялись средства, но и о иных счетах, с которых совершалось перечисление на выявленный «электронный кошелек».

Использование при раскрытии и расследовании преступлений информации об IP-адресе и MAC-адресе.

IP-адрес представляет собой комбинацию цифр (например, 95.139.18.24), которую присваивает пользователю интернет-услуг компания-провайдер, предоставляющая доступ во всемирную сеть. «IP-адрес»[1] может быть статическим (постоянным) или динамическим (временным), но в любом случае он «привязан» к устройству, выходящему в сеть, либо к персональным данным лица, на чье имя заключался договор (при использовании мобильного Интернета). Сведения о том, кому был присвоен «IP-адрес», хранятся у поставщика услуг Интернета (например, компании «Dom.ru», «Сибирьтелеком» и др.) и содержат данные об адресах по которому находился компьютер, с которого был осуществлен выход в сеть, информацию о лице, с которым был заключен договор на предоставление услуг Интернета.

В случае доступа в сеть через проводной Интернет по известному сотрудникам органов внутренних дел IP-адресу компания-провайдер может

[1] Определение местоположения по IP-адресу [Электронный ресурс].URL: www.itpride.net/useful/ip.html (дата обращения: 26.09.2018).

предоставить сведения как о месте расположения компьютера, так и о персональных данных лица, на чье имя заключался договор. Однако необходимо помнить, что подобные сведения могут храниться непродолжительное время. Например, в статье 17 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[1] определяется, что период хранения зависит от технических возможностей провайдеров и может составлять от 1 месяца до нескольких лет. Поэтому необходимо помнить, что промедление может привести к утрате важной информации (Приложение 1).

При использовании преступниками мобильного Интернета (через USB-модем или сотовый телефон) по известному сотрудникам органов внутренних дел IP-адресу компания-провайдер может предоставить сведения лишь о персональных данных лица, на чье имя заключался договор о предоставлении доступа при оформлении сим-карты.

Дополнительные сложности могут возникнуть в ситуации, когда выход в сеть преступниками был осуществлен из т.н. зоны свободного Wi-Fi – участка, где Интернет предоставляется всем желающим бесплатно (территории крупных торговых центров, некоторые кафе). В них каждый может воспользоваться Интернетом с любого портативного устройства (ноутбук, телефон). В этом случае по IP-адресу можно определить лишь сведения о том, например, что доступ был осуществлен из зоны «Wi-Fi» по определенному адресу.

В качестве способа выявления лиц, осуществляющих выход в Интернет в преступных целях через «Wi-Fi» - зоны мы предлагаем следующее:

1. Анализ видеозаписей с прилегающей территории (если таковая ведется) и последующую проверку выявленных лиц. При установлении подозреваемого дальнейшие действия должны быть направлены на доказывание его вины.

2. Сопоставление MAC-адресов изъятого у подозреваемого

[1] О персональных данных : Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ : ред. от 29.07.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 29.11.2018).

электронного устройства с теми, которые были зафиксированы при совершении преступлений. MAC-адрес компьютера (электронного устройства) – серийный номер, аналогичный IMEI-номеру мобильного телефона. Несмотря на то, что и он может быть изменен пользователем в попытке уйти от контроля, существует вероятность выхода компьютера преступника в сеть в нескольких точках доступа с одним MAC-адресом.

Например, если используется ноутбук, который периодически приносят в одну или различные зоны «Wi-Fi», либо с него выходят в сеть, используя проводной Интернет, в различных стационарных точках доступа (квартиры, офисы). В этом случае запрос в компании, предоставляющие доступ в Интернет, на установление IP-адресов (мест, территории), с которых еще был зарегистрирован выход в сеть компьютера с установленным ранее MAC-адресом (серийный номер), может дать ценную информацию.

При раскрытии и расследовании преступлений с использованием преступниками социальных сетей («ВКонтакте», «Одноклассники», «Facebook» и др.), с «персональных страниц» которых они общаются с потерпевшими, вводя последних в заблуждение, целесообразно обращаться к администрации социальных сетей, чтобы установить IP-адрес, с которого происходила регистрация «персональной страницы» и последующие выходы на нее. Это позволит установить компанию-провайдер, услугами которой пользовался злоумышленник. Затем, если информация об IP-адресе будет получена, возможно будет сделать запрос в администрацию компании, предоставившей интернет-услуги, для установления лица, которому по договору был выделен IP-адрес, и дополнительно зафиксированных иных выходов в сеть компьютера с MAC-адресом, фигурировавшем при выявленном подключении.

Особенности раскрытия и расследования преступлений при создании и использовании преступниками интернет-сайтов

В случае создания преступниками вымышленных сайтов, на которых размещается информация о якобы состоявшихся розыгрышах ценных призов

или продаже ходовых товаров по низким ценам, существует возможность направления запроса в компанию, на ресурсе которой был размещен указанный сайт, об IP-данных, используемых при его создании и последующем управлении созданным сайтом. Преступники могут пользоваться «ячейками», выделяемыми администрацией крупных сайтов, для размещения на нем своих небольших по объему страниц мини-сайтов (т.н. хостинг)[1].

Однако, в любом случае злоумышленникам необходимо зарегистрироваться, указав почтовый ящик (E-mail). Данный E-mail они могут использовать неоднократно при создании сайтов, а также для ведения собственной переписки. Вся информация технического и организационного характера от организации, предоставляющей услуги хостинга, будет направляться на данный E-mail, что также в дальнейшем следует учитывать при доказывании вины преступников. Злоумышленники вынуждены будут периодически проверять почту, а также отвечать организатору хостинга по вопросам функционирования страницы своего сайта.

В связи с этим необходимо направлять запросы в компании, на ресурсе которых были размещены указанные сайты, с целью установления IP-адресов и MAC-адресов регистрации сайта; управления им; адреса электронной почты, использовавшегося злоумышленниками.

Зачастую счета абонентских номеров сотовой связи используется преступниками в качестве своеобразной платежной системы при совершении хищений денежных средств. Их выбор объясняется относительной простотой перевода денег, а также возможностью управления счетом телефонного номера через «личный кабинет» в сети Интернет для дальнейшего перечисления похищенных денежных средств.

В случае перечисления преступниками похищенных денежных средств на телефонные номера сотовой связи, необходимо направлять запрос в компанию, предоставляющую услуги связи, для установления, на какие

[1] Обзор хостинг-провайдеров. URL: www.cy-pr.com/hosting (дата обращения: 03.09.2018).

телефонные номера или иные счета были перечислены средства со счета данного телефонного номера, либо кем и где данные средства были сняты (обналичены).

Раскрытие и расследование преступлений с использованием преступниками электронной почты также имеет свои особенности. Так, например, с использованием адреса электронной почты могут совершаться такие преступления, как вымогательство мошенничество угрозы убийством, неправомерный доступ к компьютерной информации и другие.

Операторы электронной почты обычно сохраняют сведения о персональных данных, указанных при регистрации, а также сеансах доступа (авторизациях) пользователей за различный период времени. Кроме того, сохраняется содержимое электронной переписки, если пользователь не удалял свою корреспонденцию самостоятельно.

В настоящее время вышеуказанные сведения о пользователях можно получить только у операторов электронной почты, работающих на территории Российской Федерации, таких как «Mail.ru», «Rambler.ru», «Yandex.ru».

Информацию об адресах электронной почты операторов, расположенных за пределами Российской Федерации, таких как «Google.com», «Gmail.com», необходимо запрашивать путем направления международных следственных поручений или запросов.

Для того чтобы получить сведения о пользователе электронной почты оператора, действующего на территории Российской Федерации, необходимо подготовить запрос в администрацию оператора электронной почты[1].

Для получения сведений об электронной переписке пользователя, который использовал адрес электронной почты, необходимо получить разрешение суда на проведение ОРМ «Контроль почтовых отправлений,

[1]Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств: сб. докладов науч. -практич. семинара. М., 2016. С. 62.

телеграфных и иных сообщений».

При подготовке запросов в администрацию оператора электронной почты необходимо учитывать следующие обстоятельства:

– ООО «Мэйл.Ру» сохраняет сведения о последних 10-15 сеансах доступа пользователя к ящику или за последний период в несколько месяцев;

– в ООО «Мэйл.Ру» необходимо направлять запросы по адресам электронной почты, имена которых заканчиваются на: @mail.ru, @inbox.ru, @list.ru, @bk.ru;

– ООО «Рамблер Интернет Холдинг» и ООО «Яндекс» сохраняют сведения о сеансах доступа пользователя к ящику приблизительно за последние один-два месяца.

При раскрытии преступления, связанного с использованием электронной почты, помимо направления запроса в администрацию оператора, можно получить промежуточную информацию о ресурсах, использованных преступником, путем просмотра свойств письма, пришедшего от злоумышленника.

Свойства письма могут содержать подробную служебную информацию: точное время отправки и доставки сообщения; кодировку; тип сообщения; путь следования письма от сервера отправителя к получателю; протокол, по которому было получено письмо.

Для этого необходимо в присутствии потерпевшего с помощью почтового сервиса зайти на его электронный ящик и открыть письмо, поступившее от преступника. Затем среди вкладок, расположенных в верхней части почтового сервиса, найти вкладку «Еще» или «Подробнее», и в открывшемся окне нажать ссылку «Показать оригинал» или «Служебные заголовки», или «Свойства», или «Исходный текст письма». В открывшихся свойствах письма можно увидеть IP-адрес ресурса, с использованием которого было направлено письмо.

Учитывая вышеизложенное, мы пришли к следующим выводам. Расследование мошенничеств с использованием сети Интернет, таких как

использование преступниками «электронных кошельков»; использование преступниками социальных сетей («ВКонтакте», «Одноклассники», «Facebook» и др.), «персональные страницы»; создание и использование преступниками Интернет-сайтов; использование преступниками электронной почты,имеет ряд особенностей. Каждый вид данных преступлений имеет свои тактику и способы расследования, которые порождают эффективное раскрытие.

Мошенничества в сети интернет, как и другие криминальные деяния в сфере компьютерной информации, предполагаю планомерную работу по данному направлению сотрудников оперативных подразделений. Последовательное и установленное выполнение своих обязанностей сотрудниками оперативного подразделения по различным видам преступлений, связанных с использованием сети Интернет, четкое знание своих полномочий и особенностей расследования данных преступлений и их применение способствуют своевременному раскрытию преступления и привлечению преступников к уголовной ответственности. Своевременное и точное следование алгоритму первоначальных мероприятий при сборе материала по заявлению о мошенничестве, способствует быстрому раскрытию преступлений оперативными подразделениями ОВД.

3.3. Алгоритм первоначального этапа раскрытия мошенничества, совершенного с использованием сети Интернет оперативными подразделениями ОВД

В настоящее время мошенничества в сети Интернет совершаются преимущественно под предлогами реализации различных товаров по сниженным ценам, с большими скидками, с бесплатной доставкой и других выгодных предложений.

В 1998 году в МВД России в составе Бюро специальных технических мероприятий было создано Управление «К» – подразделение, основным направлением деятельности которого является борьба с преступлениями в сфере информационных технологий.

Основные направления работы Управления «К» МВД России:

1. Борьба с преступлениями в сфере компьютерной информации:

• выявление и пресечение фактов неправомерного доступа к компьютерной информации;

• борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

• противодействие мошенническим действиям с использованием возможностей электронных платежных систем;

• борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет:

• выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;

• противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

• противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

Также раскрытием и расследованием данного вида преступлений занимается Федеральная служба безопасности, ГУ МВД России, ГСУ МВД России, УМВД России по субъектам Российской Федерации, подразделения по борьбе с экономическими преступлениями МВД России, подразделения уголовного розыска МВД России.

В виду стремительного развития информационных технологий данное явление порождает новые способы совершения противоправных действий посредством различных аппаратных устройств, таких как сотовые телефоны, персональные компьютеры, планшеты и иные устройства, что, в свою очередь, значительно затрудняет своевременное предотвращение, а также принятие мер к розыску и установлению преступника.

В связи с этим особого внимания требует рассмотрение способов и общего алгоритма действий оперативных сотрудников в различных ситуациях раскрытия и расследования преступлений в сфере компьютерной информации.

Как правило, преступники при совершении подобных правонарушений используют следующие способы:

– злоумышленник на сайте электронных объявлений («Из Рук в Руки», «Авито» и т.п.) разместил объявление о продаже каких-либо товаров по выгодным предложениям, созвонившись с потерпевшим, передал информацию о расчетном счете, на который необходимо перечислить денежные средства за товар, и, получив денежные средства от потерпевшего, обналичил их;

– злоумышленник создал сайт в сети Интернет в виде Интернет-магазина по продаже каких-либо товаров по выгодным предложениям, созвонившись с потерпевшим, передал информацию о расчетном счете, на который необходимо перечислить денежные средства за товар, и, получив денежные средства от потерпевшего, обналичил их;

– злоумышленник создал страницу в социальной сети Интернет, разместил объявление о продаже каких-либо товаров по выгодным предложениям, созвонившись с потерпевшим, передал информацию о расчетном счете, на который необходимо перечислить денежные средства за товар, и, получив денежные средства от потерпевшего, обналичил их.

Исследователь в области оперативно-розыскной деятельности А.Д. Илюшин указывает, что раскрытие и расследование преступлений, совершаемых в сфере предоставления услуг в Интернете, остается довольно сложной задачей[1]. Проблемы, которые в настоящее время возникают при расследовании мошенничества в сети Интернет, связаны с компьютерно-техническим аспектом и, как правило, с одной из сложных типичных

[1] Илюшин Д.А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет: дис. … канд. юрид. наук. Волгоград, 2016. 214 с.

ситуаций, когда подозреваемый неизвестен и информация о нем отсутствует. В данной ситуации следует акцентировать внимание на проведении первоначальных оперативно-розыскных мероприятий и следственных действий с привлечением специалиста. При этом важно использовать методику расследования преступлений, состоящую из таких элементов, как криминалистическая характеристика обстоятельства, подлежащие доказыванию, особенности возбуждения уголовного дела, особенности расследования на первоначальном, последующем и завершающем этапах.

Организация начального этапа расследования зависит от того, какая следственная ситуация сложилась к моменту возбуждения уголовного дела.

На начальном этапе раскрытия преступления организация расследования сводится, в основном, к работе с информацией — к ее восприятию, анализу, переработке, оценке, систематизации, синтезу.

На основе результатов обработки исходной информации оперативными сотрудниками выдвигаются версии, определяются задачи расследования, следователь принимает решения, организует их выполнение и осуществляет контроль за их исполнением всеми участниками процесса.

В результате от оперативных сотрудников следователь получает новую информацию, которая, также, воспринимается, анализируется, перерабатывается, синтезируется, что ведет к постановке новых задач и принятию новых управленческих решений и корректировке прежних.

Постоянно в ходе этого процесса оперативный сотрудник прогнозирует расследование в целом, поведение подозреваемого, обвиняемого, заявителя о компьютерном преступлении в сети Интернет, свидетелей, других участников расследования, а также возможное недобросовестное противодействие со стороны защиты.

Организация расследования осуществляется с использованием программно-целевого метода, метода мысленного моделирования, криминалистического факторного анализа и комплексного подхода.

Учитывая специфику преступлений, совершенных с использованием

сети Интернет, необходимо провести оперативно-розыскные мероприятия[1].

Оперативно-розыскное мероприятие – составная часть оперативно-розыскной деятельности, сведения об организации и тактике которой составляют государственную тайну, представляющую собой совокупность действий специально уполномоченных на то государственных органов и их должностных лиц, осуществляемых с соблюдением регламентированных законом оснований и условий, отвечающую нормам морали и нравственности и непосредственно направленную на достижение целей и разрешение задач оперативно-розыскной деятельности.

Произвести подробный опрос потерпевшего с целью выяснения следующих обстоятельств:

- на каком именно интернет-ресурсе потерпевший обнаружил объявление о продаже товара;
- дата и время обнаружения объявления;
- если объявление или интернет-магазин уже отсутствуют, подробное описание, название объявления, наименование сайта (текст, контактные данные продавца, цена товара, доменное имя сайта и т.п.);
- способы связи потерпевшего с преступником (номер телефона, адрес электронной почты и др.);
- дата и время контакта с преступником (телефонные соединения, электронная переписка);
- способ перечисления денежных средств преступнику;
- дата и время перечисления денежных средств.

Если объявление или сайт еще не удалены, необходимо их зафиксировать путем производства моментального снимка экрана (скриншот). Моментальный снимок экрана производится нажатием клавиши клавиатуры «PrintScreen» (расположена рядом с клавишей «F12»). При этом

[1]Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис. … канд. юрид. наук. М., 2016. С. 4

снимок копируется в буфер обмена операционной системы и затем может быть вставлен в любой текстовый документ формата «Word».

Разъяснить потерпевшему о необходимости предоставления платежных документов или их копий, подтверждающих оплату товара.

Разъяснить потерпевшему о необходимости предоставления распечатки (детализации) его звонков за период общения с преступником, которую он может получить по заявлению у оператора связи.

Если общение с преступником осуществлялось посредством электронной почты, иной интернет-переписки, следует разъяснить потерпевшему о необходимости сохранения переписки с преступником для ее предоставления и провести мероприятия по установлению:

- абонентских номеров, использовавшихся преступниками;
- использовался ли злоумышленником при совершении преступления ресурс электронной торговой площадки;
- использовался ли злоумышленником при совершении преступления Интернет-ресурс в виде сайта;
- использовалась ли злоумышленником при совершении преступления страница в социальной сети;
- использовавших преступниками счетов, на которые потерпевшие перечисляли денежные средства.

При получении сведений от операторов электронных платежных систем, банков, операторов сотовой связи проанализировать полученные сведения и принять одно из следующих решений:

– если установлено место совершения преступления, направить материал проверки по территориальности;

– если установлено, что преступление совершено на обслуживаемой территории, принять решение о возбуждении уголовного дела;

– если место совершения установить не представляется возможным, принять решение о возбуждении уголовного дела;

– если отсутствуют основания для возбуждения уголовного дела, отказать в его возбуждении.

Снятие информации с технических каналов связи (с точки зрения расследования мошенничества в сети Интернет) – это регламентированное Законом об ОРД оперативно-розыскное мероприятие, проводимое на основании судебного решения, заключающееся в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами и программным обеспечением работы соответствующих систем и устройств, а также излучаемых ими электромагнитных и других полей.

В тех случаях, когда используемый подозреваемыми в интернет-мошенничестве способ связи совмещен с обычной и/или мобильной телефонной связью, необходимо учитывать требования и говорить не только о снятии информации с технических каналов связи, но и о прослушивании телефонных переговоров.

Таким образом, формируется план расследования по делу в целом, по отдельным эпизодам и обстоятельствам. По мере его выполнения и получения новой информации вносятся коррективы в имеющийся план, и вновь проводится анализ и формулирование дальнейших задач расследования. Наиболее важными оперативно-розыскными мероприятиями на начальном этапе раскрытия преступлений в сети Интернет являются осмотр места происшествия, компьютерного оборудования и информации, обыск и выемка с целью обнаружения, фиксации и изъятия компьютерной информации и компьютерных средств, относящихся к расследуемому событию. Это ключевой момент расследования, поскольку компьютерная информация является предметом посягательства, неправомерный доступ к ней должен быть своевременно процессуально зафиксирован. Тем более что компьютерная информация может быть легко изменена или уничтожена, что

повлечет утрату следов преступления[1].

Если у оперативного сотрудника есть основания полагать, что цифровая информация может являться доказательством по уголовному делу, то она должна изыматься только процессуальными способами, предусмотренными законом: в процессе производства осмотра, обыска, выемки. Выбор конкретного следственного действия зависит от решения следователя, которое, как правило, обусловлено конкретной ситуацией расследования на момент необходимости изъятия цифровой информации.

В бесконфликтной ситуации с собственником или владельцем цифровой информации, когда гражданин или организация потерпели от правонарушения и готовы оказать помощь в установлении истины, целесообразно проводить выемку или осмотр. Такая ситуация чаще всего складывается с организациями, подвергшимися неправомерному доступу к компьютерной информации[2].

В конфликтной ситуации, особенно при расследовании преступлений в сфере экономики, целесообразно проводить обыск, поскольку гражданин и организация могут оказывать явное или скрытое противодействие, вплоть до преграждения доступа и уничтожения информации и ее носителей.

Задачи подготовительной стадии при расследовании преступлений в конфликтной ситуации:

- получить наиболее полное представление о характере деятельности объекта, где могут находиться следы преступления и другие объекты, относящиеся к расследуемому делу, изучить обстановку в организации: отрасль хозяйствования, порядок учета, документооборот, структуру, особенности используемых технологий;

---

[1] Мещеряков В.А. Теоретические основы криминалистической классификации преступлений в сфере компьютерной информации / В.А. Мещеряков // Конфидент. 2014. С. 5.

[2] Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств: сб. докладов науч.-практич. семинара. М., 2016. С. 62.

- изучить коммуникативные и иные тактико-технические характеристики используемой компьютерной техники и программного обеспечения;

- изучить организацию охраны объекта информатизации и конкретной компьютерной информации;

- выяснить служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, а также их прямое или косвенное отношение к ценностям (имуществу), которые стали предметом правонарушения.

Обязательно должен составляться план предстоящего оперативно-розыскного мероприятия, в котором учитываются и тактически обоснованно используются полученные данные об обстановке в заподозренной организации. Именно на основе «разведывательных данных» оперативный сотрудник определяет место, время проведения ОРМ, его участников, материально-техническое обеспечение и др[1].

Техническая подготовка включает обеспечение транспортом, упаковочными материалами, научно-техническими средствами различного назначения, достаточным количеством резервных носителей информации для копирования информации[2].

Целесообразно иметь при себе: портативный компьютер, ноутбук с соединительными кабелями с различными разъемами или с комбинированным разъемом; программное обеспечение для копирования информации на месте производства ОРМ; набор сервисных программ для определения технических характеристик исследуемых компьютеров, исправности отдельных устройств и внешней памяти, а также антивирусные программы; при необходимости копирования небольших фрагментов информации — комплект дискет, чистых компакт-дисков (CD-R или CD-RW) или флеш-накопителей для записи информации.

---

[1] Чернышева В.О. Интернет и преступность // Реагирование на преступность: концепции, закон, практика. М., 2017. С. 144-148.

[2] Там же. С. 62.

Необходимый набор сервисных программ оперативный сотрудник или специалист формирует по своему усмотрению в зависимости от категории расследуемых дел, используемого программного обеспечения и оборудования в данном регионе в данный момент времени.

Как отмечалось выше, место совершения компьютерного преступления, использовавшего глобальную сеть Интернет, не может быть однозначно определенно поэтому поиск и фиксация информации, имеющей значение для уголовного дела, осуществляется на различных объектах[1].

Сбор доказательств при расследовании уголовных дел о мошенничествах, совершенных с использованием сети Интернет, является необходимым условием, для всех уголовных дел. Именно доказательства являются главным элементом в системе доказывания в рамках правового поля.

Так, УПК РФ определяет, что доказывание состоит в собирании, проверке и оценке доказательств с целью установления обстоятельств, которые имеют значение для криминального производства. В процессе доказывания применяются разные способы сбора доказательств. Сторона обвинения осуществляет сбор доказательств путем проведения следственных (розыскных) действий и негласных ОРМ, истребования и получения от органов государственной власти, органов местного самоуправления, предприятий, учреждений и организаций, должностных и физических лиц вещей, документов, ведомостей, выводов экспертов, выводов ревизий и актов проверок, проведения других процессуальных действий, предусмотренных кодексом[2].

Особое внимание среди способов получения доказательств уделяют запросам. Тактически грамотно составленный запрос значительно способствует расследованию мошенничеств, совершенных с использованием

[1] Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. М.: Юрлитинформ, 2012. С. 69.

[2] Дознание в органах внутренних дел: учеб. пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / Ф.К. Зиннуров и др.; под ред. Ф.К. Зиннурова. 2-е изд., перераб. и доп. М.: ЮНИТИ-ДАНА; Закон и право, 2013. С. 176.

сети Интернет, а полученные сведения являются доказательством по делу.

Под тактически грамотно составленным запросом мы подразумеваем своевременно направленный к органам государственной власти, органам местного самоуправления, предприятиям, учреждениям и организациям, должностным и физическим лицам, обладающим информацией, которая представляет интерес для следствия, и имеющим возможность предоставить ее в установленном законом порядке, запрос, в котором отображены все необходимые обстоятельства, подлежащие установлению на момент его направления.

Исходя из технических особенностей процесса передачи информации в сети Интернет, своевременность направления запроса заключается в том, что:

– в кратчайшее время принимается решение о необходимости направления запроса, решается вопрос о том, кому следует его адресовать, определяется перечень необходимых обстоятельств, которые должны быть освещены в ответе на запрос, исходя из чего формулируется перечень вопросов;

– учитывается, что для ответа требуется промежуток времени, зависящий от:

а) объема данных, которые необходимо установить для предоставления полного ответа;

б) наличия и способа хранения запрашиваемой информации;

в) географической локации адресанта;

г) способа передачи запроса-ответа[1].

Установленных законом норм, которые бы прямо определяли право оперативного сотрудника на составление и отправление запроса, нет. Однако ФЗ «О полиции» определяет право сотрудника полиции получать беспрепятственно и бесплатно от предприятий, учреждений и организаций независимо от форм собственности и объединений граждан на письменный

[1] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дисс. … к.ю.н. Владивосток, 2016. С. 13.

запрос сведенья (в том числе и те, что представляют коммерческую и банковскую тайну), необходимые в делах о преступлениях, которые находятся в производстве. На наш взгляд, дальнейшее использование в качестве доказательства информации, полученной в ответ на запрос, следует считать законным и рассматривать такой ответ как документ.

При расследовании уголовного дела о мошенничестве в интернет-аукционе или интернет-магазине составляется запрос к администрации сервиса, в котором указывается:

1) каким образом был(ли) установлен(ы) факт(ы) мошенничества (сообщение от пользователей сервиса, собственный мониторинг, обращение правоохранительных органов и т.д.):

- при сообщении от пользователей:

а) перечень пользователей, от которых поступили жалобы, время их поступления (в том числе регистрационные данные: имя, фамилия, отчество, контактная информация: электронный адрес, номера телефонов и т.п.);

б) краткое изложение сути сообщений о правонарушении (недоброкачественность или несоответствие товара, непоступление товара и т.п.);

в) информация о товаре (лоте), которая является непосредственным объектом конфликтной ситуации (имеющиеся фото, приведенное описание, время выставления на продажу);

г) время, когда было(и) заключено(ы) соглашение(я) продажи (время истечения торгов);

- при самостоятельном выявлении (мониторинге):

а) перечень пользователей, которые были выявлены в качестве пострадавших (в том числе регистрационные данные, контактная информация и т.п.);

б) суть выявленного нарушения;

в) информация о товаре (лоте) (имеющиеся фото, приведенное описание, время выставления на продажу, IP-адрес, с которого был

выставлен лот);

г) время, когда было(и) заключено(ы) соглашение(я) продажи (или время истечения торгов);

д) обстоятельства, которые служили основаниями подозревать в недобросовестном поведении одну из сторон;

2) каким образом осуществляется деятельность интернет-аукциона; в данном случае запрашиваются данные относительно:

а) работы сервиса;

б) регистрации и активации аккаунта на сайте;

в) заключения соглашений покупки-продажи (требования к лотам, информации о них и т.д.);

3) имеющаяся информация относительно деятельности мошенника:

а) о регистрации (точная дата и время), а также способе подтверждения личности;

б) является ли юридическим или физическим лицом (фирма, частный предприниматель и т.д.);

в) товары (лоты) выставленные на продажу;

г) покупателях (победителей торгов), лиц, которые подозреваются в мошенничестве;

д) других участниках торгов по конкретному лоту, который стал непосредственным объектом мошенничества;

е) история посещений сайта (время входа и нахождения, IP-адреса, по которым посещался сайт);

ж) есть ли другие учетные записи, которые принадлежат этому пользователю, если есть, то предоставить по ним вышеприведенную информацию;

з) блокировании учетных записей пользователя, сроках и причинах блокирования;

и) имеющиеся жалобы на учетные записи пользователя (при необходимости – приложить скриншоты);

к) переписку между мошенником и потерпевшим(ми) (при наличии);

л) был ли причинен вред действиями непосредственно интернет-аукциона (интернет-магазина), если да, то какой именно.

Вопрос относительно факта мошенничества на интернет-аукционе или в интернет-магазине может быть подтвержден информацией от службы, которая осуществляла доставку товаров от продавца к покупателю. Через запрос к службе, которая занималась перевозкой товара, можно установить факт получения или неполучения товара стороной и получить информацию относительно характеристик товара (размеры, вес и т.п.).

В запросе следует отметить такие данные, как:

1) дата отправки груза;

2) характеристика груза (вес, размеры, особые требования относительно перевозки и т.п.);

3) кто осуществил отправку (по возможности – фамилия, имя, отчество и информация о документах, которые были предоставлены для подтверждения личности – вид документа, серия, номер и т.п.);

4) из какого адреса и по какому адресу был оформлен перевоз;

5) ведомости о получателе, которые были указаны отправителем;

6) дата прибытия груза на указанный адрес;

7) способ информирования получателя о прибытии груза;

8) дата получения груза (если такой факт имел место);

9) информация о лице получателя (по возможности – фамилия, имя, отчество и информация о документах, которые были предоставлены для подтверждения личности – вид документа, серия, номер и т.п.);

10) наличие документов, которые удостоверяют факт получения (накладная с подписью получателя, журнал о получении и т.п.).

В случае, когда мошенничество совершено способом, предусматривающим деятельность непосредственно на ресурсе (сайт некоторой системы, социальная сеть и т.п.), для получения информации, которая может быть полезна для расследования, необходимо направлять

запрос в администрацию того ресурса, на котором было совершено мошенничество. При этом следует отметить, что в запросе обязательно должен быть указан логин (никнейм) пользователя, информация, которую необходимо получить следователю, а также максимальная конкретизация времени его деятельности на ресурсе, который интересует следствие.

К обязательным элементам, которые должны быть отображены в запросе, относят:

1) регистрационные данные, вносимые пользователем при регистрации на ресурсе;

2) дату, время регистрации и IP-адрес пользователя при регистрации;

3) IP-адрес пользователя в указанный промежуток времени.

Также будет полезной информация, которая может быть предоставлена поставщиками услуги подключения к сети Интернет (провайдерами). Проводя исследование по данному направлению нами решался вопрос относительно возможности установления конкретного лица (фамилии, имени, отчества, места проживания и т.п.) при наличии IP-адреса, с которого было совершено преступление. Известно, что диапазон IP-адресов, которые могут быть использованы для назначения узлами в качестве публичных, является исчерпывающим.

Организации, занимающиеся распределением IP-адресов – это региональные интернет-регистраторы (англ. «Regional Internet Registry»).

На сегодняшний день выделяют пять региональных интернет-регистраторов:

1) American Registry for Internet Numbers;

2) RIPE Network Coordination Centre;

3) Asia-Pacific Network Information Centre;

4) Latin American and Caribbean Internet Addresses Registry;

5) AfricanNetworkInformationCentre.

Статус регионального интернет-регистратора может быть присвоен лишь «ICANN» (Международной некоммерческой организацией

«Корпорация по управлению доменными именами и IP-адресами»). Все указанные региональные интернет-регистраторы оперируют некими объемами ресурсов сети Интернет, которые им делегированы американской некоммерческой организацией «IANA».

Исследовав принцип подчинения и распределения пространства IP-адресов между поставщиками услуги подключения к сети Интернет, мы среди прочего выделили одно криминалистически значащее обстоятельство: для того, чтобы провайдер местного уровня смог предоставлять услуги по подключению к сети Интернет конечному пользователю, он должен быть зарегистрирован у своего регионального интернет-регистратора. Это обстоятельство значительно упрощает поиск провайдера местного уровня, предоставляющего услугу лицу, которое разыскивается.

В частности, изучив сайт «RIPE Network Coordination Centre» (URL:http://www.ripe.net/), мы установили, что на нем можно получить информацию относительно провайдера, который предоставляет услугу подключения к сети Интернет при наличии IP-адреса неустановленного лица. Для этого достаточно воспользоваться поиском в базе данных регионального интернет-регистратора, введя в поисковую строку известный IP-адрес в точечно-десятичной форме и нажав «Поиск». В результате поиска отображается информация об интернет-провайдере местного уровня. Эта информация значительно упрощает поиск поставщика услуги, ведь характеризуется высоким уровнем информативности относительно разыскиваемого объекта. Подразумевается, что использование полученной таким образом информации в качестве доказательств по уголовному делу недопустимо (Приложение 1).

Однако использование ее в качестве ориентирующей существенно ускорит расследование и значительно повысит его качество. С точки зрения доказательной значимости, официальный ответ на запрос, полученный от интернет-регистратора, может быть доказательством. Однако подобный ответ придется ждать долго. Для ускорения необходимых операций можно

применять электронный документооборот: запрос отправляется на официальную электронную почту регионального интернет-регистратора, получение ответа осуществляется также по электронной почте.

Далее рекомендуется обратиться с запросом к провайдеру, информация о котором была получена вышеприведенным образом[1] (Приложение 2).

В запрос включаются вопросы:

1) с какого времени провайдер занимается предоставлением услуги подключения к сети Интернет;

2) какой диапазон публичных IP-адресов арендует провайдер для предоставления своих услуг;

3) входит ли указанный IP-адрес (или несколько) в этот диапазон;

4) каким образом клиентам выдается в аренду публичный IP-адрес;

5) использует ли провайдер локальные IP-адреса, и каким образом они назначаются клиенту при подключении;

6) какую систему аутентификации использует провайдер;

7) кто из пользователей получил в качестве публичного указанный IP-адрес (с учетом отрезков времени).

В запросе следует уточнять данные, представляющие наибольший интерес:

а) фамилию, имя, отчество;

б) дату рождения;

в) адрес проживания;

г) номер, серию паспорта и идентификационный номер (возможно, были получены при заключении договора);

д) информацию относительно способа аутентификации пользователя: логин, MAC-адрес;

е) информацию о количестве подключенных устройств или использовании

[1] Глотов В.С., Шалатов Д.В. Интернет–технологии и электронная торговля: экономика, право, программное обеспечение. Изд-е 2-е, перераб. и доп. В 2-х ч. / под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ. М.: НИЦ «Инженер», 2015. С. 183.

маршрутизаторов (если такой владеет провайдер);

ж) копии документов о предоставлении услуг (в частности, договор с приложениями).

В случае, когда в указанный промежуток времени публичный IP-адрес арендовался несколькими пользователями, необходимо предоставление указанной информации относительно каждого.

В последнее время злоумышленниками для совершения преступлений нередко используются электронные торговые площадки или общедоступные ресурсы, на которых с помощью сети Интернет можно бесплатно поместить объявление о продаже того или иного товара.

Наибольшее распространение получило использование площадки электронных объявлений «Авито». Оператором системы электронных объявлений «Авито» в настоящее время является ООО «КЕХ еКоммерц», поэтому запрос на получение информации необходимо направлять в администрацию данной компании с обязательным указанием номера или точного названия объявления.

В исключительных случаях, если отсутствует информация о номере или названии объявления, при направлении запросов необходимо указывать более подробное описание сути объявления: примерную дату публикации (время обнаружения объявления потерпевшим или свидетелем), точное описание реализуемого товара, контактные данные злоумышленника.

ООО «КЕХ еКоммерц» по запросу предоставляет следующие сведения:

– дата и время размещения объявления;
– IP-адрес, с которого осуществлялось размещение объявления;
– контактная информация лица, разместившего объявление;
– наличие жалоб на автора объявления.

Подводя итог, важно отметить, что эффективное раскрытие преступления зависит от правильного и точного соблюдения алгоритма действий сотрудника оперативного подразделения по конкретному виду мошенничества с использованием сети Интернет, например, установления

источника в сети, информация из которого будет иметь существенное значение в расследовании уголовного дела.

Особое внимание среди способов получения доказательств следует уделить запросам. Тактически грамотно и правильно составленный запрос способствует расследованию мошенничеств, совершенных с использованием сети Интернет, а полученные сведения будут являться значащими доказательствами в раскрытии уголовного дела.

Также, стоит отметить, что при регистрации сайта преступник должен поддерживать связь с хостером или регистратором сайта при помощи кого-либо абонентского номера или адреса электронной почты. Кроме того, злоумышленники при администрировании сайта должны использовать какую-либо точку доступа в сеть Интернет. Учитывая данные обстоятельства, запросив сведения у регистратора сайта или хостера (или хостинг-провайдер), на площадках которого размещен сайт, можно получить первичные сведения о преступнике.

Описанные нами особенности получения информации оперативным сотрудником в ходе расследования мошенничества, совершенного с использованием сети Интернет, позволяют получить информацию:

а) о технической сути совершенного преступления;

б) размере ущерба, а также о том, кому он причинен;

в) технических идентификаторах устройств, с помощью которых осуществлялся доступ к ресурсам сети Интернет при совершении преступления (IP-адрес, MAC-адрес);

г) косвенно (а в некоторых случаях и прямо) получить информацию о лице, которое совершило это преступление.

Таким образом, в большинстве случаев подобные мошенничества по своему характеру и механизму совершения являются однотипными. Средствами и орудиями их совершения могут являться как простейшие мобильные телефоны, так и средства связи с доступом в сеть Интернет. При этом сама сеть Интернет выступает в качестве своеобразной площадки,

на которой мошенники реализуют свой преступный умысел – размещают информацию о псевдопродаже или оказании услуг по низким ценам; сами ищут людей, подавших какое-либо объявление; создают финансовые пирамиды; организуют игорный бизнес и т.п.

Раскрытие таких преступлений не требует от сотрудников ОВД специальных познаний в сфере высоких технологий. Достаточно иметь доступ к сети Интернет в качестве рядового пользователя и следовать определенному алгоритму действий, в основном, состоящему из направления запросов на установление ряда технических параметров, которые в дальнейшем и будут использованы в качестве доказательств при изобличении преступника.

Кроме того, для эффективной борьбы с правонарушениями (преступлениями), совершаемыми в указанной сфере, необходимо четко понимать, что такое информационно-телекоммуникационная сеть, телекоммуникационные системы, компьютерная информация, носители компьютерной информации и т.п.

3.4. Организация и тактика последующих оперативно-розыскных мероприятий при раскрытии мошенничеств, совершенных с использованием сети Интернет

Сущность организации оперативно-розыскной деятельности – это целенаправленная деятельность по созданию оптимальных условий функционирования служб и подразделений, осуществляющих оперативно-разыскное функции; по налаживанию взаимодействия между ними; по направлению их усилий на успешное выполнение задач борьбы с преступностью. При этом следует иметь в виду, что данное понятие имеет как статистические, так и динамические характеристики, включая в себя системное построение оперативных аппаратов ОВД и процесс их функционирования. Отсюда, можно выделить следующие виды организации этой деятельности:

- Изучение и оценка оперативной обстановки.

- Осуществление на этой основе оптимальной расстановки сил и средств.
- Обеспечение взаимодействия.
- Управление, планирование и контроль.
- Координация деятельности оперативных подразделений.

Отправной точкой решения организационных задач должно стать определение общей стратегии оперативно-розыскной деятельности в глобальных компьютерных сетях. Она может быть оборонительной (предусматривать раскрытие наиболее опасных сетевых преступлений без активного влияния на оперативную обстановку в глобальных сетях в целом); наступательной (обеспечивать энергичное противодействие проявляющимися негативным изменениям оперативной обстановки); упреждающей (предполагать постоянное осуществление оперативно-профилактических мероприятий по нейтрализации всех потенциальных угроз). Организация ОРД должна основываться на действиях наступательного характера с тем, чтобы не выпустить ситуацию в глобальных сетях из-под контроля правоохранительных органов.

Опираясь на вышеизложенное, можно выделить два аспекта, имеющих основное значение для совершенствования ОРД в сети Интернет: изучение оперативное обстановки в глобальных сетях; оптимизация взаимодействия в процессе проведения ОРМ.

Одним из основных элементов организации является получение полного и всестороннего представления об оперативной обстановке: о сложившейся ситуации, возможных местах «прорыва» криминальных элементов, об арсенале сил и средств, их способности к недопущению «прорыва» или его своевременной ликвидации. В оперативно-розыскной деятельности под оперативной обстановкой понимается совокупность реально существующих условий, в которых действует конкретный орган внутренних дел. К ним можно отнести социально-экономическую

характеристику территории, состояние преступности, характеристику сил и средств[1].

При анализе и оценке оперативной обстановки на обслуживаемом участке глобальных сетей необходимо изучать сведения, характеризующие:

1. Социально-экономические условия:

- экономическую и технологическую информацию об обслуживаемом участке сетей (основные провайдеры Интернета, механизмы предоставления сетевых услуг, основные параметры каналов передачи данных, используемые схемы подключения и т.д.);
- информацию о пользователях глобальных компьютерных сетей (количество, социальная характеристика);
- данные о наличии подключенных к сетям объектов, представляющих особый интерес для преступников;
- сведения об организациях, специализирующихся в области информационных технологий, образовательных учреждениях, ведущих обучение по специальностям, связанным с вычислительной техникой, и т.д.

2. Состояние преступности:

- характеристику преступности в глобальных компьютерных сетях, ее структурные и динамические показатели, сведения о правонарушениях в глобальных сетях;
- данные о неформальных группах и лицах, представляющих оперативные интерес, характере их деятельности, особенностях поведения, связях;
- сведениях об основных способах совершения сетевых преступлений и условиях, способствующих их совершению;
- адреса мест сетевого общения, конференций и сайтов хакерской тематики.

3. Силы и средства органов внутренних дел:

[1] Осипенко А.Л., Луговик В.Ф., Поправко С.Н. Оперативно-разыскные мероприятия в сети Интернет: учебное пособие. М.: ЦОКР МВД России, 2007. С. 84.

- количественных и качественный состав привлекаемых сотрудников, наличие у них опыта подобной деятельности ранее;
- перечень субъектов, с которыми взаимодействуют оперативные работники, и формы взаимодействия;
- обеспеченность специальными техническими средствами.

Такие сведения должны быть собраны для определения стратегии ОРД на закрепленном участке. Четко отработанная система должна предусматривать организацию постоянного слежения за оперативной обстановкой с целью своевременного обнаружения отклонений от ее обычного состояния, выявления причин этих отклонений и принятия мер для их устранения, а также оптимальной расстановки имеющихся сил и средств.

В силу установленного выше наличия нескольких субъектов ОРД в сети Интернет важное место в организации этой работы занимает обеспечение взаимодействия всех ее участников. Специфика борьбы с сетевыми преступлениями обусловливает необходимость сбора в крайне ограниченные сроки большого объема разнообразных сведений из различных источников, что само по себе возможно только при условии консолидации условий всех субъектов оперативно-розыскной деятельности.

Необходимость во взаимодействии возникает между оперативными подразделениями и иными субъектами при осуществлении совместной деятельности с организациями, не являющимися субъектами оперативно-розыскной деятельности обслуживания; при проведении общих мероприятий с правоохранительными органами.

При организации взаимодействия в области осуществления оперативно-розыскных мероприятий в сети Интернет лежат два концептуальных направления. Во-первых, это слежение за оперативной обстановкой на обслуживаемом участке сетей в интересах данного подразделения. Во-вторых, выявление и использование информационных сигналов, представляющих значение для предупреждения и раскрытия преступлений на других территориях и по другим линиям работы.

Следует выделить приоритетные формы взаимодействия:

1. Формирование единых банков данных оперативной информации.
2. Совместное использование имеющихся сил и средств.
3. Взаимное информирование о результатах деятельности и положительном опыте.
4. Обмен специалистами, программным обеспечением и техникой;
5. Обмен результатами аналитической деятельности, полученными в ходе оперативного обслуживания.
6. Планирование совместных действий, разработка целевых программ и планов совместных мероприятий.
7. Проведение совместных совещаний, семинаров, конференций.
8. Выполнение поручений и заданий на проведение отдельных ОРМ.
9. Совместный анализ оперативной обстановки.

Эффективность оперативно-розыскной деятельности в сети Интернет в существенной степени определяется взаимодействием оперативных подразделений с организациями, заинтересованными в укреплении сетевой безопасности (финансовыми и коммерческими структурами, осуществляющими деятельность в сети Интернет). Наиболее широкие возможности в этом отношении имеют провайдеры доступа. Представители таких организаций обладают глубокими познаниями принципов работы и структуры обслуживаемых объектов. Они могут сообщать о выявленных фактах преступной деятельности, обеспечивать сохранение и предоставление файлов регистрации системных действий, оказывать содействие в проведении отдельных оперативно-розыскных мероприятий. Таким образом, достижение договоренности о взаимодействии с указанными организациями позволяет получать необходимые дополнительные источники оперативной информации в ключевых точках глобальных сетей.

Во взаимодействии на международном уровне могут быть выделены несколько направлений, имеющих приоритетное значение:

1. Обмен оперативной информацией и методиками осуществления оперативно-розыскных мероприятий в сети Интернет.

2. Организация совместного мониторинга сетей, направленного на сбор данных о преступности.

3. Выявление новых форм совершения противоправных деяний, выработка общих мер противодействия им.

4. Образование международных координационных центров с привлечением ведущих специалистов из разных стран.

5. Проведение международных конференций и семинаров по проблемам борьбы с сетевыми преступлениями.

6. Организация горячих линий для согласования действий.

7. Создание международной сигнально-информационной сети.

Совершенствованию оперативно-розыскной тактики в науке оперативно-розыскной деятельности традиционно уделяется особое внимание. Под оперативно-розыскной тактикой понимают совокупность взаимосвязанных, основанных на обобщении опыта, приемов, методов, технических средств и научных рекомендаций, применяемых субъектами ОРД в целях эффективной борьбы с преступностью. Тактика ОРМ в сети Интернет также, в первую очередь, должна опираться на использование опыта оперативных аппаратов.

Оперативно-розыскная тактика в глобальных компьютерных сетях опирается, прежде всего, на комплексное использование ОРМ, исчерпывающий перечень которых дан в ст. 6 Закона об ОРД. Для получения информации о процессах, протекающих в сети Интернет, можно эффективно применять практически весь комплекс указанных мероприятий[1]. Стоит упомянуть, что поводом к возбуждению трети уголовных дел по фактам сетевых преступления послужили результаты ОРМ.

[1] Осипенко А.Л. Оперативно-розыскная деятельность по борьбе с преступностью в глобальных компьютерных сетях: монография Омск: Омская академия МВД России. 2010. 287 с.

В настоящее время оперативные сотрудники связывают использование глобальных сетей в ОРД, главным образом, с одним ОРМ - снятие информации с технических каналов связи. Такой подход необоснованно ограничивает сферу применения оперативно-розыскных возможностей. Компьютерные сети относятся к техническим каналом передачи данных. Вместе с тем специфика современных глобальных сетей допускает не только пассивную регистрацию информации, происходящую при ее снятии с каналов связи, но и осуществление мероприятий, направленных на активный поиск тактически значимых сведений. Следовательно, вполне обоснованным является проведение и иных оперативно-розыскных мероприятий с непосредственным использованием глобальных сетей, таких как опрос, наведение справок, сбор образцов для сравнительного исследования, контроль почтовых отправлений, телеграфных и иных сообщений, оперативный эксперимент и др.

Одним из основных среди указанных мероприятий является снятие информации с технических каналов связи. В зависимости от тактических соображений при его проведении может осуществляться пассивный и активный перехват данных. В случае пассивного перехвата выполняется слежение за передаваемыми по каналу связи сообщениями без вмешательства в их поток. Это позволяет раскрывать содержание сообщений, определять объем и частоту передачи, характер передаваемых данных. При активном перехвате над сообщениями выполняются определенные действия: они могут быть изменены, уничтожены, задержаны, переупорядочены. Решение тактических задач в определенных случаях может потребовать обеспечения блокировки или задержки всех сообщений конкретному адресату. Такие действия, направленные на недопущение получения данным

адресатом криминальной информации, могут предприниматься в порядке ч. 1 ст. 15 Закона об ОРД[1].

Частным случаем таких действий является просмотр электронной корреспонденции на почтовых сетевых серверах и наблюдение за сеансами компьютерной телефонии, осуществляемые в рамках таких ОРМ, как контроль почтовых отправлений, телеграфных и иных сообщений и прослушивание телефонных переговоров.

Основными обстоятельствами, оказывающими влияние на тактику снятия информации в сетях, являются большой объем передаваемых данных, подлежащих анализу; возможность подмены сетевого адреса, снижающая достоверность установления его принадлежности; трудности создания каналов связи между оперативными подразделениями и провайдерами; возможность использования одним субъектом нескольких адресов; отсутствие общего списка пользователей сетей; применение изучаемыми лицами средств криптографической защиты сообщений.

В соответствии с ч. 2 ст. 8 Закона об ОРД названные мероприятия, как ограничивающие конституционные права граждан, должны осуществляться только на основании судебного решения.

Современные глобальные компьютерные сети предоставляют оперативному работнику возможность осуществления поиска информации в сетевом компьютере проверяемого лица. Такой поиск предполагает применение специального программного обеспечения для дистанционного проникновения в компьютер и последующего обследования содержащихся в нем файлов. В данном случае следует говорить об особом виде дистанционного обследования. Хотя основные виды объектов такого оперативного осмотра перечислены в названии мероприятия (помещения, здания, сооружения, участки местности и транспортные средства), специализироваться могут и другие объекты, связанные с преступной

[1] Софронов В.Н. Основы деятельности криминальной милиции по раскрытию мошенничеств: вопросы теории: монография Омск: Омская академия МВД России. 2008. 124 с.

деятельностью, к которым допустимо относить и сетевые компьютеры. Специфика проведения указанного мероприятия связана с поиском мест проникновения в обследуемую систему, преодолением установленных защитных средств, сокрытием следов пребывания. Целесообразно включение в арсенал оперативных служб программных комплексов сканирования сетей с функциями автоматического поиска и анализа уязвимости (например, «Internet Security Scanner», «SATAN»). На компьютер, содержимое которого обследуется, могут устанавливаться и другие специальные средства (программы регистрации активности пользователя, удаленного управления сетью и т.д.), позволяющие просматривать файлы с электронной корреспонденцией; указатели мест, которые пользователь посещал в Интернете; адресную книгу, отражающую связи проверяемого лица. В то же время нельзя забывать, что изучаемый компьютер может использоваться несколькими лицами и проведение обследования в таком виде может нанести ущерб законопослушным гражданам.

Дистанционное обследование компьютера практически невозможно без копирования определенных файлов, направленного на их последующее изучение и сравнение с аналогичными образцами, содержащими признаки преступной деятельности. Такие действия можно считать специфическим видом проведения традиционных оперативно-розыскных мероприятий - сбора образцов для сравнительного исследования и исследования предметов и документов. Закон не дает его перечня собираемых оперативным работником образцов, но и не ограничивает, поэтому вполне допустимо отнести к ним и информационные объекты, передаваемые по глобальной сети Интернет.

Одним из мероприятий, обеспечивающих получение тактически значимой информации, является опрос – специальная беседа, проводимая с гражданами, которым могут быть известны сведения о сетевых преступлениях, причастных к ним лицах, других обстоятельствах, представляющих оперативный интерес. Закон не регламентирует процедуру

опроса, в силу чего вполне допустимо его проведение на основе контакта с определенными лицами с использованием коммуникативных возможностей глобальной сети Интернет.

Новые возможности придает использование глобальных сетей и такому мероприятию как наведение справок, которое в данном случае осуществляется путем непосредственного изучения документов, размещенных в сетевых информационных системах и на сайтах, а также направления по сетям запросов в организации, обладающие интересующими сведениями. Среди таких организаций наиболее значительную помощь способны оказать операторы связи – провайдеры.

Особой формой наведения справок можно считать контент-анализ содержимого информационных сайтов и сетевых конференций криминальной направленности с целью выявления сведений, представляющих оперативный интерес.

В условиях явной недостаточности сил и средств, предназначенных для оперативно-розыскного обслуживания глобальных компьютерных сетей, возможно привлечение к проведению данного мероприятия лиц, оказывающих содействие ОВД.

Одним из наиболее важных мероприятий в плане расширения возможностей при оперативно-розыскном обслуживании глобальных сетей является оперативный эксперимент. Его применение регламентируется нормой, изложенной в ч. 6 ст. 8 Закона об ОРД, в соответствии с которой проведение указанного ОРМ допускается только в целях выявления тяжких преступлений и лиц, их подготавливающих, совершающих и совершивших.

Оперативный эксперимент может проводиться как в отношении конкретных лиц, так и, что особенно важно, для выявления намерений неизвестных лиц путем применения различных «ловушек» и «приманок». Таковыми в глобальных сетях могут быть файлы с названиями, способными вызвать криминальный интерес; «файлы-улики» со скрытой в них

специальной информацией, позволяющей в последующем изобличить преступника; сообщения с дезинформацией в местах сетевого общения.

Изучение положительного опыта дает возможность предложить в качестве эффективных действий при осуществлении оперативного эксперимента в глобальных сетях организацию сетевых конференций криминальной направленности; создание контролируемых сетевых объектов, представляющих интерес для преступников (например, электронных магазинов); образование организаций (например, фирм, разрабатывающих программное обеспечение); использование на обслуживаемых объектах специальных программ, которые позволяют отслеживать действия преступников.

Для выявления мошеннических действий, связанных с функционированием интернет-магазинов, возможно также проведение в них проверочной закупки, являющейся самостоятельным ОРМ. Тактической особенностью проведения этого мероприятия в глобальных сетях служит относительная простота осуществления закупки зашифрованным способом.

Таким образом, грамотное и эффективное проведение оперативными сотрудниками таких оперативно-розыскных мероприятий, как опрос, наведение справок, оперативный эксперимент, сбор образцов для сравнительного исследования, исследование предметов и документов, снятие информации с технических каналов связи, контроль почтовых отправлений, телеграфных и иных сообщений в соответствии с Законом об ОРД, обеспечивает полное и быстрое раскрытие преступлений, связанных с различного рода мошенническими действиями.

ЗАКЛЮЧЕНИЕ

Малоизученность способов оперативного противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей (включая сеть Интернет), и значимость вопросов противодействия их распространению определяют актуальность представленной темы, цели и задачи, научную и практическую значимость данного исследования. Большое значение имеет положительный опыт, как зарубежных стран, так и подразделений по борьбе с незаконным оборотом наркотиков МВД России в субъектах РФ.

Проведенный анализ теоретических источников и обобщение практического опыта оперативных подразделений МВД по РТ позволило нам: во-первых дать общую характеристику преступлений, совершаемых с использованием информационно-телекоммуникационных сетей; во-вторых, определить порядок документирования преступных действий сбытчиков наркотических средств. Данная инструкция может использоваться компетентным подразделениям в целях более эффективного выполнения задач путем использования имеющегося арсенала уголовно-процессуальных и оперативно-розыскных средств и методов, решать основную задачу в борьбе с преступлениями незаконного оборота наркотиков – выявление и изобличение всех участников (членов) организованных групп и преступных сообществ; в третьих, выработать рекомендации по предупреждению и раскрытию мошенничества в глобальной сети Интернет, которые могут способствовать совершенствованию существующих методов и способов борьбы сданным общественно опасным явлением с учетом специфики сферы информационных технологий.

Разработка лиц, совершающих преступления с использованием информационно-телекоммуникационных систем, достаточно сложна, требует детального и длительного документирования фактов их преступной деятельности, значительно количества привлекаемых сил и оперативно-

технических средств. Опыт практической деятельности ОВД свидетельствует что для успешного осуществления этой работы целесообразно закреплять за данной специализацией наиболее квалифицированных и опытных сотрудников уголовного розыска, оперативных подразделений.

С уверенностью можно сказать, что развитие телекоммуникационных технологий, в особенности сети Интернет, с каждым днем привлекает все большее количество людей. Эта сфера становится все более и более привлекательной для участников преступных групп, осуществляющих сбыт наркотиков, и если не обеспечить своевременное и профессиональное противостояние этим проявлениям, вероятность выхода криминальной ситуации из-под контроля крайне велика.

Список рекомендуемых источников

Федеральные законы Российской Федерации

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 февраля 2014 г. №2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
2. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ : ред. от 28.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 28.11.2018).
3. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : ред. от 12.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : ред. от 12.11.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
5. О прокуратуре Российской Федерации: Федеральный закон РФ от 17 января 1992 г. № 2202-1 : ред. от 29.07.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
6. Об оперативно-розыскной деятельности: Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ : ред. от 06.07.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
7. О наркотических средствах и психотропных веществах: Федеральный закон РФ от 8 января 1998 г. № 3-ФЗ : ред. от 29.12.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
8. О противодействии экстремистской деятельности: Федеральный закон РФ от 25 июля 2002 г. № 114-ФЗ : ред. от 23.11.2015 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).
9. О противодействии терроризму: Федеральный закон РФ от 6 марта

2006 г. № 35-ФЗ : ред. от 18.04.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

10. Об информации, информационных технологиях и о защите информации : Федеральный закон РФ от 27 июля 2006 г. № 149-ФЗ : ред. от 19.07.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 29.11.2018).

11. О персональных данных : Федеральный закон РФ от 27 июля 2006 г. № 152-ФЗ : ред. от 31.12.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 29.11.2018).

12. О противодействии коррупции : Федеральный закон РФ от 25 декабря 2008 г. № 273-ФЗ : ред. от 30.10.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

13. О безопасности : Федеральный закон РФ от 28 декабря 2010 г. № 390-ФЗ : ред. от 05.10.2015 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

14. О полиции : Федеральный закон РФ от 7 февраля 2011 г. № 3-ФЗ : ред. от 03.08.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

Нормативные правовые акты Президента Российской Федерации

15. Об утверждении перечня сведений конфиденциального характера : указ Президента РФ от 06 марта 1997 г. № 188 : ред. от 13.07.2015 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

16. О дополнительных мерах по противодействию незаконному обороту наркотических средств, психотропных веществ и их прекурсоров" (вместе с "Положением о Государственном антинаркотическом комитете", "Положением об антинаркотической комиссии в субъекте Российской Федерации") : указ Президента РФ от 18 октября 2007 г. № 1374 : ред. от 11.10.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

17. Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2020 года : указ Президента РФ от 09 июля 2010г. № 690 : в ред. от 23.02.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

18. О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 31 декабря 2015 г. № 683 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

19. О совершенствовании государственного управления в сфере контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров и в сфере миграции : указ Президента РФ от 5 апреля 2016 г. № 156 : ред. от 15.05.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

20. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 5 декабря 2016 № 646 : ред. 05.12.2016 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

21. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

Нормативные правовые акты Правительства Российской Федерации

22. О сертификации средств защиты информации : постановление Правительства РФ от 26 июня 1995 г. № 608 : ред. от 21.04.2010 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

23. Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации : постановление Правительства РФ от 30 июня 1998 г. № 681 : ред. от 22.06.2018 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

24. Об утверждении Правил допуска лиц к работе с наркотическими средствами и психотропными веществами, а также к деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ : постановление Правительства РФ от 6 августа 1998 г. № 892 : ред. от 25.05.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

25. О порядке дальнейшего использования или уничтожения наркотических средств, психотропных веществ и их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, или их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, а также инструментов и оборудования, которые были конфискованы или изъяты из незаконного оборота либо дальнейшее использование которых признано нецелесообразным : постановление Правительства РФ от 18 июня 1999 г. № 647 : ред. от 04.09.2012 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

26. О Типовом регламенте взаимодействия федеральных органов исполнительной власти : постановление Правительства РФ от 19 января 2005 г. № 30 : ред. от 13.06.2018 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

27. О взаимодействии и координации деятельности органов исполнительной власти субъектов Российской Федерации и территориальных органов федеральных органов исполнительной власти : постановление Правительства РФ от 5 декабря 2005 г. № 725 : ред. от 08.12.2008 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

28. Об утверждении Положения о системе межведомственного электронного документооборота: постановление Правительства Российской Федерации от 22 сентября 2009 г. № 754 : ред. от 17.10.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

29. О порядке хранения наркотических средств, психотропных веществ и

их прекурсоров (вместе с "Правилами хранения наркотических средств, психотропных веществ и их прекурсоров") : постановление Правительства РФ от 31 декабря 2009 г. № 1148 : ред. от 10.11.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

30. О представлении сведений о деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ, и регистрации операций, связанных с их оборотом" (вместе с "Правилами представления отчетов о деятельности, связанной с оборотом прекурсоров наркотических средств и психотропных веществ", "Правилами ведения и хранения специальных журналов регистрации операций, связанных с оборотом прекурсоров наркотических средств и психотропных веществ") : постановление Правительства РФ от 09 июня 2010 г. № 419 : ред. от 27.06.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

31. Об утверждении Правил производства, переработки, хранения, реализации, приобретения, использования, перевозки и уничтожения прекурсоров наркотических средств и психотропных веществ : постановление Правительства РФ от 18 августа 2010 г. № 640 : ред. от 27.06.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

32. О порядке установления требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и их прекурсоров, и (или) культивирование наркосодержащих растений : постановление Правительства РФ от 17 декабря 2010 г. № 1035 : ред. от 29.12.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

33. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства РФ от 03 февраля 2012 г. № 79 : ред. от 15.06.2016 // СПС Консультант Плюс. URL:

www.consultant.ru (дата обращения: 25.11.2018).

34. Об утверждении крупного и особо крупного размеров прекурсоров наркотических средств или психотропных веществ, а также крупного и особо крупного размеров для растений, содержащих прекурсоры наркотических средств или психотропных веществ, либо их частей, содержащих прекурсоры наркотических средств или психотропных веществ, для целей статей 228.3, 228.4 и 229.1 Уголовного кодекса Российской Федерации : постановление Правительства РФ от 8 октября 2012 г. № 1020 : ред. от 21.02.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

35. О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено" (вместе с "Правилами создания, формирования и ведения единой автоматизированной информационной системы "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", "Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети "Интернет", распространение которых в Российской Федерации запрещено") : постановление Правительства РФ от 26 октября 2012 г. № 1101 : ред. от 21.03.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

36. Об утверждении государственной программы Российской Федерации "Обеспечение общественного порядка и противодействие преступности" :

постановление Правительства РФ от 15 апреля 2014 г. № 345 : ред. от 31.03.2017 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

37. О дальнейшем развитии единой системы межведомственного электронного взаимодействия : постановление Правительства РФ от 19 ноября 2014 г. № 1222 : ред. от 29.03.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

38. О федеральной государственной информационной системе координации информатизации" (вместе с "Положением о федеральной государственной информационной системе координации информатизации") : постановление Правительства РФ от 14 ноября 2015 г. № 1235 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

Решения судебных инстанций различного уровня

39. Дело «Быков (Bykov) против Российской Федерации» (жалоба № 45413/07) : постановление Европейского суда по правам человека от 10.03.2009 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

40. Дело «Александр Новоселов (Aleksandr Novoselov) против Российской Федерации» (жалоба № 33954/05) : постановление Европейского суда по правам человека от 28.11.2013 // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

41. Об отказе в принятии к рассмотрению жалобы гражданки Юлдашевой Люции Ахматгалеевны как не соответствующей требованиям Федерального конституционного закона «О Конституционном Суде Российской Федерации : определение Конституционного Суда РФ от 05.06.1997 № 72-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

42. По делу о проверке конституционности отдельных положений Федерального закона ″Об оперативно-розыскной деятельности″ по жалобе гражданки И.Г. Черновой : определение Конституционного Суда РФ от

14.07.1998 № 86-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

43. По жалобе граждан М.Б. Никольской и М.И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона "Об оперативно-розыскной деятельности": определение Конституционного Суда РФ от 14.02.1999 № 18-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

44. Об отказе в принятии к рассмотрению жалобы гражданина Барковского Константина Олеговича на нарушение его конституционных прав частью четвертой статьи 127 УПК РСФСР, пунктом 1 части первой статьи 6 и пунктом 3 части первой статьи 7 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от 01.12.1999 № 211-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

45. Об отказе в принятии к рассмотрению жалобы гражданина Идалова Тимура Сайд Магомедовича на нарушение его конституционных прав рядом статей Уголовно-процессуального кодекса РСФСР и частью второй статьи 8 Федерального закона "Об оперативно-розыскной деятельности" : определение Конституционного Суда РФ от 21.12.2000 № 290-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

46. По жалобам гражданина Уразова Сергея Владимировича на нарушение его конституционных прав положениями статей 49, 91, 92, 227, 228, 229, 255 и 355 Уголовно-процессуального кодекса Российской Федерации и статей 6, 8 и 10 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от 11.07.2006 № 268-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

47. Об отказе в принятии к рассмотрению жалобы гражданки Дьячковой Ольги Геннадьевны на нарушение ее конституционных прав пунктами 6 и 14 части первой и частью четвертой статьи 6, пунктом 3 статьи 7, частью второй

статьи 8 Федерального закона ″Об оперативно-розыскной деятельности″, частью второй статьи 7, пунктом 4 части второй статьи 38, статьями 125, 140 и 146 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 16.11.2006 № 454-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

48. Об отказе в принятии к рассмотрению жалобы гражданина Донского Александра Павловича на нарушение его конституционных прав пунктами 4 и 6 части первой и частью третьей статьи 6 Федерального закона ″Об оперативно-розыскной деятельности″ и статьями 13, 89 и 186 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 20.03.2007 № 178-О-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

49. Об отказе в принятии к рассмотрению жалобы гражданина Дахкуряна Сурена Николаевича на нарушение его конституционных прав частями второй и четвертой статьи 8 и частью третьей статьи 11 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от 17.07.2007 № 597-О-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

50. Об отказе в принятии к рассмотрению жалобы гражданина Шкутяка Данилы Ярославовича на нарушение его конституционных прав пунктом 14 части первой статьи 6, частью четвертой статьи 13 Федерального закона ″Об оперативно-розыскной деятельности″ и статьей 89 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 21.10.2008 № 640-О-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

51. Об отказе в принятии к рассмотрению жалобы гражданина Мазы Александра Леонидовича на нарушение его конституционных прав статьями 7 и 8 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от 28.05.2009 № 641-О-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

52. Об отказе в принятии к рассмотрению жалобы гражданина Абдулхамидова Ахмедшапи Гамзатовича на нарушение его конституционных прав положениями статей 8 и 9 Федерального закона ″Об оперативно-розыскной деятельности″, а также статей 7, 29 и 450 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 22.03.2012 № 629-О-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

53. Об отказе в принятии к рассмотрению жалобы гражданина Аносова Игоря Викторовича на нарушение его конституционных прав статьями 74, 75 и 81 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Суда РФ от 11.05.2012 № 814-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

54. Об отказе в принятии к рассмотрению жалобы гражданина Шестиперстова Леонида Федоровича на нарушение его конституционных прав пунктом 14 части первой статьи 6 и частью четвертой статьи 16 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от 17.06.2013 № 941-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

55. Об отказе в принятии к рассмотрению жалобы гражданина Крюкова Виктора Федоровича на нарушение его конституционных прав положениями статьи 6 Федерального закона ″Об оперативно-розыскной деятельности″, статей 30, 158 и 159 Уголовного кодекса Российской Федерации : определение Конституционного Суда РФ от 22.04.2014 № 845-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

56. Об отказе в принятии к рассмотрению жалобы гражданина Демина Олега Евгеньевича на нарушение его конституционных прав частями первой и третьей статьи 159 Уголовного кодекса Российской Федерации, статьями 307—309 Уголовно-процессуального кодекса Российской Федерации, а также частью седьмой статьи 8 Федерального закона ″Об оперативно-розыскной деятельности″ : определение Конституционного Суда РФ от

23.10.2014 № 2400-О // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

57. По делу о проверке конституционности статей 21 и 21.1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина Е.Ю. Горовенко : постановление Конституционного Суда РФ от 23.11.2017 № 32-П // СПС «Консультант Плюс». URL: www.consultant.ru (дата обращения: 25.11.2018).

58. О некоторых вопросах, связанных применением ст.ст.23 и 25 Конституции РФ : постановление Пленума Верховного Суда РФ от 24.12.1993 № 13 : ред. от 06.02.2007 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

59. О некоторых вопросах применения судами Конституции Российской Федерации : постановление Пленума Верховного Суда РФ от 31.10.1995 № 8 : ред. от 03.03.2015 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

60. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ от 15.06.2006 № 14 : ред. от 16.05.2017 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

61. О судебной практике рассмотрения уголовных дел об организации преступного сообщества (преступной организации) или участии в нем (ней): постановление Пленума Верховного Суда РФ от 10.06.2010 № 12 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

62. О судебной практике применения законодательства, регламентирующего особенности уголовной ответственности и наказания несовершеннолетних : постановление Пленума Верховного Суда РФ от 01.02.2011 № 1 : ред. от 29.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

63. О судебной практике по уголовным делам о преступлениях

экстремистской направленности : постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 : ред. от 03.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

64. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 : ред. от 03.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

65. О практике применения судами особого порядка судебного разбирательства уголовных дел при заключении досудебного соглашения о сотрудничестве: постановление Пленума Верховного Суда РФ от 28.06.2012 № 16 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

66. О применении судами законодательства, регламентирующего основания и порядок освобождения от уголовной ответственности : постановление Пленума Верховного Суда РФ от 27.06.2013 № 19 : ред. от 29.11.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

67. О практике применения судами законодательства о мерах пресечения в виде заключения под стражу, домашнего ареста и залога : постановление Пленума Верховного Суда РФ от 19.12.2013 № 41 : ред. от 24.05.2016 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

68. О судебной практике по делам о преступлениях против половой неприкосновенности и половой свободы личности : постановление Пленума Верховного Суда РФ от 04.12.2014 № 16 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

69. О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем : постановление Пленума Верховного Суда РФ от 22.07.2015 № 32 // СПС Консультант Плюс. URL: www.consultant.ru (дата обращения: 25.11.2018).

70. 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: 25.11.2018).

Нормативные правовые акты министерств и ведомств Российской Федерации

71. О деятельности органов внутренних дел по предупреждению преступлений : приказ МВД России от 17 января 2006 г. № 19 : ред. от 28.11.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).

72. Об организации использования экспертно-криминалистических учетов органов внутренних дел Российской Федерации : приказ МВД России от 10 февраля 2006 г. № 70 : ред. от 28.12.2016 // СТРАС «Юрист» (дата обращения: 25.11.2018).

73. Об утверждении Временной инструкции по информационному взаимодействию подразделений органов внутренних дел Российской Федерации и ФМС России с интегрированными банками данных : приказ МВД России от 04 июля 2006 г. № 523дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

74. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД России № 786, Минюста России № 310, ФСБ России № 470, ФСО России № 454, ФСКН России № 333, ФТС России № 971 от 6 октября 2006 г. : ред. от 22.09.2009 // СТРАС «Юрист» (дата обращения: 25.11.2018).

75. О некоторых организационных вопросах и структурном построении территориальных органов МВД России : приказ МВД России от 30 апреля 2011 г. № 333 : в ред. от 11.08.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).

76. Об утверждении перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну

: приказ МВД России от 11 января 2012 г. № 17 : ред. от 12.12.2016 // СТРАС «Юрист» (дата обращения: 25.11.2018).

77. Об основах организации ведомственного контроля за деятельностью органов внутренних дел Российской Федерации: приказ МВД России от 3 февраля 2012 г. № 77 : ред. от 13.02.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).

78. О некоторых вопросах организации оперативно-розыскной деятельности в системе МВД России : приказ МВД России от 19 июня 2012 г. № 608 : ред. от 14.08.2018 // СТРАС «Юрист» (дата обращения: 25.11.2018).

79. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации : приказ МВД России от 06 июля 2012 г. № 678 : ред. от 07.12.2016 // СТРАС «Юрист» (дата обращения: 25.11.2018).

80. Об утверждении требований к оснащению инженерно-техническими средствами охраны объектов и помещений, в которых осуществляются деятельность, связанная с оборотом наркотических средств, психотропных веществ и внесенных в список I перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации, прекурсоров, и (или) культивирование наркосодержащих растений для использования в научных, учебных целях и в экспертной деятельности : приказ МВД России № 855, ФСКН России № 370 от 11 сентября 2012 г. : ред. от 03.12.2015 // СТРАС «Юрист» (дата обращения: 25.11.2018).

81. Об организации планирования в органах внутренних дел Российской Федерации : приказ МВД России от 26 сентября 2012 г. № 890 : ред. от 02.02.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).

82. Об утверждении Инструкции об организации рассмотрения обращений граждан в системе Министерства внутренних дел Российской Федерации : приказ МВД России от 12 сентября 2013 г. № 707 : ред. от 01.12.2016 // СТРАС «Юрист» (дата обращения: 25.11.2018).

83. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности дознавателю, органу дознания, следователю или в суд : приказ МВД РФ, Минобороны РФ, ФСБ РФ, ФСО РФ, Федеральной таможенной службы, СВР РФ, ФСИН, Федеральной службы РФ по контролю за оборотом наркотиков и Следственного комитета России от 27 сентября 2013 г. №776/703/509/507/1820/42/535/398/68 // СТРАС «Юрист» (дата обращения: 11.11.2018).

84. 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 февраля 2014 г. №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: 25.11.2018).

85. 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 г. № 736 : ред. от 07.11.2016 // СТРАС «Юрист» (дата обращения: 25.11.2018).

86. Об утверждении методик выявления злоупотребления алкоголем или токсическими веществами, потребления без назначения врача наркотических средств или психотропных веществ, склонности к совершению суицидальных действий, а также критериев оценки результатов комплексного обследования, направленного на их выявление : приказ МВД России от 25 декабря 2014 г. № 1130дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

87. Об объявлении Инструкции по организации совместной оперативно-

служебной деятельности подразделений ОВД РФ при раскрытии преступлений и расследование уголовных дел : приказ МВД России от 29 апреля 2015 г. № 495дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

88. Об утверждении структуры и системы адресации интегрированной мультисервисной телекоммуникационной сети Министерства внутренних дел Российской Федерации : приказ МВД России от 23 сентября 2015 г. № 926 : ред. 25.08.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).

89. Об организации информационного сопровождения деятельности территориальных органов Министерства внутренних дел Российской Федерации : приказ МВД России от 11 декабря 2015 г. № 1165дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

90. О порядке взаимодействия правоохранительных и иных государственных органов на досудебной стадии уголовного судопроизводства в сфере возмещения ущерба, причиненного государству преступлениями : приказ Генпрокуратуры России № 182, МВД России № 189, МЧС России № 153, ФСБ России № 243, СК России № 33, ФСКН России № 129, ФТС России № 800, ФССП России № 220, Росфинмониторинга № 105 от 29 марта 2016 г. // СТРАС «Юрист» (дата обращения: 25.11.2018).

91. Об утверждении Положения о Главном управлении по контролю за оборотом наркотиков Министерства внутренних дел Российской Федерации : приказ МВД России от 23 апреля 2016 г. № 209 // СТРАС «Юрист» (дата обращения: 25.11.2018).

92. Об утверждении Типового положения о подразделении по контролю за оборотом наркотиков территориального органа Министерства внутренних дел Российской Федерации на региональном уровне : приказ МВД России от 30 апреля 2016 г. № 219 : в ред. 26.05.2018 // СТРАС «Юрист» (дата обращения: 25.11.2018).

93. Об утверждении Наставления по технической эксплуатации средств связи и автоматизации территориальных органов Министерства внутренних дел Российской Федерации : приказ МВД России от 30 ноября 2016 г. № 772

// СТРАС «Юрист» (дата обращения: 25.11.2018).
94. Об организации рассмотрения сообщений об отдельных видах преступлений экономической направленности : приказ МВД России от 1 декабря 2016 г. № 785 // СТРАС «Юрист» (дата обращения: 25.11.2018).
95. О некоторых вопросах подразделений по контролю за оборотом наркотиков территориальных органов МВД России на региональном уровне : приказ МВД России от 6 декабря 2016 г. № 795 : ред. от 06.03.2017 // СТРАС «Юрист» (дата обращения: 25.11.2018).
96. Об организации деятельности в органах внутренних дел Российской Федерации по обеспечению сохранности и учета вещественных доказательств и иных изъятых предметов и документов : приказ МВД России от 30 декабря 2016 г. № 946 // СТРАС «Юрист» (дата обращения: 25.11.2018).
97. Об утверждении Типового положения о подразделении оперативно-разыскной информации территориального органа Министерства внутренних дел Российской Федерации : приказ МВД России от 7 февраля 2017 г. № 45дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).
98. О мерах по обеспечению безопасности и антитеррористической защищенности зданий, сооружений, помещений и иных объектов территориальных органов МВД России : приказ МВД России от 10 февраля 2017 г. № 58дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).
99. Вопросы организации информационно-правового обеспечения деятельности органов внутренних дел Российской Федерации : приказ МВД России от 25 августа 2017 г. № 680 // СТРАС «Юрист» (дата обращения: 25.11.2018).
100. Об утверждении Наставления по организации деятельности подразделений органов внутренних дел Российской Федерации, осуществляющих в пределах компетенции выявление, предупреждение, пресечение и раскрытие преступлений террористического характера, преступлений и правонарушений экстремистской направленности, а также расследование преступлений террористического характера и экстремистской

направленности : приказ МВД России от 3 октября 2017 г. № 759дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

101. Об утверждении Типового положения о подразделении уголовного розыска территориального органа Министерства внутренних дел Российской Федерации на региональном уровне : приказ МВД России от 19 января 2018 г. № 25 // СТРАС «Юрист» (дата обращения: 25.09.2018).

102. Об утверждении Положения об организации и осуществлении розыска и идентификации лиц : приказ МВД России № 117дсп, Минюста России N 40дсп, Минздрава России N 88н, МЧС России N 82дсп, Минобороны России N 114дсп, СК России N 17дсп от 1 марта 2018 г. // СТРАС «Юрист» (дата обращения: 25.11.2018).

103. Об утверждении формы отчета о расходах на осуществление оперативно-розыскной деятельности : приказ МВД России от 24 апреля 2018 г. № 251дсп // СТРАС «Юрист» (дата обращения: 25.11.2018).

Учебная литература

Основная

104. Агарков, А. В. Дефиниции оперативно-розыскных мероприятий: сравнительный анализ и законодательное закрепление : монография / А. В. Агарков ; Федер. служба исполн. наказаний, Владим. юрид. ин-т Федер. службы исполн. наказаний. – Владимир : ВЮИ ФСИН России, 2017.

105. Андреев, Б. В., Пак, П. Н., Хорст, В. П. Расследование преступлений в сфере компьютерной информации / Б.В. Андреев, П.Н. Пак, В.П. Хорст. - М.: Юрлитинформ, 2016.

106. Баженов, С. В. Основы оперативно-розыскной деятельности органов внутренних дел: учебное пособие / С.В. Баженов. - Хабаровск: РИО ДВЮИ МВД РФ, 2014.

107. Делопроизводство и режим секретности в органах внутренних дел : учебно-методическое пособие / авт.-сост.: Е.П. Шляхтин, И.М. Усманов. – 3-

е изд., перераб. и доп. – Казань: КЮИ МВД России, 2017.

108. Документирование результатов оперативно-розыскного мероприятия – «оперативный эксперимент», связанного с коммерческим подкупом и взяточничеством: методические рекомендации / Киселев Н.Н. и др. – Уфа: УЮИ МВД России, 2014.

109. Дознание в органах внутренних дел: учеб. пособие для студентов вузов, обучающихся по специальности «Юриспруденция» / Ф.К. Зиннуров и др.; под ред. Ф.К. Зиннурова. – 2-е изд., перераб. и доп. - М.: ЮНИТИ-ДАНА: Закон и право, 2013.

110. Киселев, Н. Н. Основы организации ОРД ОВД: лекция / Н.Н. Киселев, Р.Р. Насыров. – Уфа: УЮИ МВД России, 2014.

111. Климов, И. А. Оперативно-розыскная деятельность [Электронный ресурс]: учебник/ Климов И.А., Дубоносов Е.С., Тузов Л.Л. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2014.— 383 с.— Режим доступа: http: // www.iprbookshop.ru / 18176.— ЭБС «IPRbooks».

112. Кокурин, Г. А. Правовая регламентация оперативно-технических мероприятий / Г.А. Кокурин // Российский юридический журнал. 2015. № 5 (104). С. 108—111.

113. Корнеев, И. К. Правовые, организационные и тактические основы раскрытия преступлений подразделениями уголовного розыска: монография / И.К. Корнеев, Е.А. Степанов, С.С. Галахов; под общей ред. Ф.Б. Мухаметшина. – Уфа: УЮИ МВД России, 2014.

114. Луговик, В. Ф. Методические рекомендации по изучению основ организации и тактики оперативно-розыскной деятельности органов внутренних дел / В.Ф. Луговик, Е.В. Буряков, С.В. Баженов. – Омск, 2013.

115. Маркушин, А. Г. Оперативно-розыскная деятельность: учебник для вузов / А.Г. Маркушин. – 2-е изд., перераб. и доп. - М.: Юрайт, 2013.

116. Миняшева, Г. И. Основы организации и тактики выявления, предупреждения и раскрытия преступлений оперативными подразделениями ОВД: лекция / Г.И. Миняшева, В.Ф. Габзалилов. – Уфа: УЮИ МВД России,

2013.

117. Образцы процессуальных документов органов дознания: учебно-практ. пособие для студентов, обучающихся по специальности «Юриспруденция» / авт.-сост. Ф.К. Зиннуров и др.; под ред. Ф.К. Зиннурова. – М.: ЮНИТИ-ДАНА: Закон и право, 2013.

118. Оперативно-разыскные ситуации в деятельности оперативных подразделений полиции : практикум. Часть 1: Описание ситуации / под ред. Ю.В. Демченко, К.Ю. Пантюхина. – Барнаул: Барнаульский юридический институт МВД России, 2015.

119. Основы оперативно-розыскной деятельности: учебное пособие / под ред. М.С. Десятова. – Омск : Омская академия МВД России, 2016.

120. Основы оперативно-разыскной деятельности ОВД: учебник / под ред. З.Л. Шхагапсоева и Н.П. Голяндина. — Краснодар: Краснодарский университет МВД России, 2016.

121. Противодействие органов внутренних дел экстремизму и терроризму: учебное пособие / С.Н. Миронов и др. – Казань: КЮИ МВД России, 2017.

122. Специальная техника органов внутренних дел: учебник: в 2 ч. / под общ. ред. Ю.А. Агафонова. – Краснодар: Краснодарский университет МВД России, 2014.

123. Телепнев, П. Ф. Теоретические и прикладные вопросы использования оперативно-розыскной информации в обеспечении уголовного судопроизводства: диссертация на соискание ученой степени кандидата юридических наук 12.00.12 – криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность / П.Ф. Телепнев. – Санкт-Петербург, 2017.

124. Теория оперативно-розыскной деятельности / под ред. К.К. Горяинова, В.С. Овчинского. – 4-е изд., перераб. – М. : Норма : ИНФРА-М, 2017.

125. Усманов, И. М. Выявление лиц, причастных к экстремистской и

террористической деятельности : учебно-практическое пособие / И.М. Усманов, Е.П. Шляхтин. – Казань: КЮИ МВД России, 2015.

126. Усманов, И. М. Противодействие преступной деятельности организованных преступных групп, связанных с бесконтактным сбытом наркотических средств: учебно-практическое пособие / И.М. Усманов. – Казань: КЮИ МВД России, 2016.

127. Харченко, С. В. Организация оперативно-розыскной деятельности территориальных органов ВМД России на районном уровне по борьбе с незаконным оборотом наркотических средств и психотропных веществ: монография / С.В. Харченко. – М.: Академия управления МВД России, 2017.

128. Шевко, Н. Р., Панченко, В. В., Каримов, А. М. Методические рекомендации по предупреждению, пресечению, раскрытию и расследованию преступлений, совершенных с использованием высоких технологий и коммуникаций / Н.Р. Шевко, В.В. Панченко, А.М. Каримов. - Казань: КЮИ МВД России, 2016.

129. Чечетин, А. Е. Обеспечение прав личности при проведении оперативно-розыскных мероприятий: монография / А.Е. Чечетин. - СПб.: Изд-во СПб. ун-та МВД России, 2016.

Дополнительная

130. Арефьев, А. Ю. Правовые и организационно-тактические особенности оперативно-розыскного предупреждения преступлений в современных условиях (по материалам ЭБиПК) / А.Ю. Арефьев. – Н. Новгород, 2011.

131. Бастрыкин, И. А. Криминалистика : учебник. Том II / Под общ. ред. А.И. Бастрыкина. – М. : Изд-во «Экзамен», 2014.

132. Вагин, О. А. Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (постатейный) / О. А. Вагин, А. П. Исиченко, А. Е. Чечетин. – М., 2009.

133. Вехов, В. Б. Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учебно-методическое пособие / В.Б. Вехов. - Волгоград: Перемена, 1998.

134. Власов И. С. Преступление и наказание в Англии, США, Франции, ФРГ, Японии: Общая часть уголовного права / И.С. Власов и др. – М.: Зерцало,2013.

135. Гаврилов, В. Г., Диденко, В. И. Методика организации и проведения контролируемых поставок наркотических средств и психотропных веществ: учебно-методическое пособие / В.Г. Гаврилов, В.И. Диденко. - Белгород: ЮИ МВД России, 2003.

136. Глотов, В. С., Шалатов, Д. В. Интернет-технологии и электронная торговля: экономика, право, программное обеспечение. – Изд-е 2-е, перераб. и доп. - в 2-х ч. / Под ред. С.А. Глотова / Центр прав человека и защиты прав потребителей РГТЭУ, Кубанский научный Центр социальных исследований «Законодательная инициатива», Краснодарский ин-т (филиал) РГТЭУ.–М.: НИЦ «Инженер», 2015.

137. Гусев, В. А. Права органов, осуществляющих оперативно-розыскную деятельность: проблемы реализации и пути решения: ПРЕПРИНТ / В.А. Гусев. - Хабаровск: Дальневосточный юридический институт МВД России, 2011.

138. Завидов, Б. Д. Сфера высоких технологий как мошенничество и как спорные объекты интеллектуальной собственности, находящиеся вне правового поля (фрикерство, хакерство и радиопиратство): подготовлено для системы «КонсультантПлюс». – Доступ из справ. правовой системы КонсультантПлюс.

139. Козырев, А. А. Информатика: учебник для вузов / А.А. Козырев. - СПб. – 2002.

140. Корнеев, И. К. Информационная безопасность и защита информации / И.К. Корнеев, Е.А. Степанов. – М.: ИНФРА-М, 2010.

141. Ларичев, В. Д. Преступность экономической направленности: монография / В.Д. Ларичев. – М.: Юрлитинформ, 2012.

142. Международный опыт уголовно-правового противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий. - Краснодар: Краснодарский университет МВД России, 2017.

143. Овчинский, С. С. Оперативно-розыскная информация / С.С. Овчинский; под ред. А.С. Овчинского и В.С. Овчинского. – М.: ИНФРА-М, 2000.

144. Оперативно-розыскная деятельность: учебное пособие / С.И. Давыдов и др. - М., 2009.

145. Психология оперативно-розыскной деятельности: учебное пособие / В.Л. Цветков и др. – М.: ЮНИТИ-ДАНА; Закон и право, 2010.

146. Рогов, А. В. Выявление и раскрытие преступлений в сфере нарушений авторских и смежных прав: методические рекомендации / А. В. Рогов. – Н. Новгород, 2010.

147. Софронов, В. Н. Основы деятельности криминальной милиции по раскрытию мошенничеств: вопросы теории: монография / В.Н. Софронов. – Омск: Омская академия МВД России, 2008.

148. Фойницкий, И. Я. Мошенничество по русскому праву / И.Я. Фойницкий. - С-Пб.: 2014.

149. Шебалин, А. В. Расследование незаконных сбытов наркотических средств, совершенных бесконтактным способом : учебное пособие / А.В. Шебалин. – Барнаул : Барнаульский юридический институт МВД России, 2015.

150. Шляхтин, Е. П. Основы оперативно-розыскной деятельности ОВД: курс лекций / Е.П. Шляхтин. – Казань: КЮИ МВД России, 2011.

151. Шляхтин, Е. П. Особенности борьбы с отдельными видами организованной преступности: лекция / Е.П. Шляхтин. – Казань: КЮИ МВД России, 2011.

Статьи, научные публикации

152. Аманбаев А.М. Международное сотрудничество в области противодействия незаконному обороту наркотиков: современное состояние и перспективы // Российский следователь. – 2011. - № 8.

153. Анохин В.Н. Электронные платежи в обеспечении эффективного функционирования платежной системы: дисс… канд.экон.наук. – М., 2015.

154. Гребельский Д. В., Атмажитов В. М., Ильичев В. А. Изучение эффективности организации взаимодействия аппаратов уголовного розыска с другими службами в раскрытии преступлений // Совершенствование управления раскрытием и расследованием преступлений: Сб. научн. трудов. М : Академия МВД СССР, 1981.

155. Гудзь Е.Г. Актуальность проблемы ведения борьбы с преступлениями в сфере высоких технологий // Сб. докладов науч.-практ. семинара “Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств, М., 2016.

156. Илюшин Д.А. «Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет» :дис. канд. юрид. наук : Волгоград, 2016.

157. Кесареева Т. П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: автореф. дис. канд. юрид. наук. – М., 2016.

158. Клименко Т.М. Проблемы противодействия наркопреступности, наркотизму и наркомании в Российской Федерации (вопросы теории и практики):дис... д-ра юрид. наук .-Волгоград, 2008.

159. Клименко Т.М. Ответственность за незаконный оборот наркотиков по российскому и европейскому законодательству: Тольяттинский государственный университет.-Тольятти, 2010. - [Электронный ресурс] – Режим доступа.URL: http://edu.tltsu.ru/sites/sites_content/site1238/html/media6 (дата обращения: 18.12.2017г.).

160. Ковлагина Д. А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом РФ // Молодой ученый. — 2016. — №16. — С. 249-251. - [Электронный ресурс] – Режим доступа.— URL https://moluch.ru/archive/120/33286/

161. Корнева В.И. Правовое регулирование международного сотрудничества РФ в сфере противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов // Сборник научных трудов аспирантов и соискателей-юристов. – Нижний Новгород: Издательство Нижегородского университета, 2005.

162. Кушпель Е.В. Кулешов П.Е. Особенности методики расследования незаконного сбыта наркотических средств и психотропных веществ, совершенных с использованием высоких технологий // Успехи современной науки и образования. № 7. – 2016 г.

163. Ларина Е., Овчинский В. Кибервойны XXI века. Возможности и риски для России или о чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014.

164. Мещеряков В.А. Теоретические основы криминалистической классификации преступлений в сфере компьютерной информации // Конфидент. – 2014. – №4

165. Осипенко А.Л. Сетевая компьютерная преступность теория и практика борьбы: монография. Омск: Омская академия МВД России, 2016. – 183 с.

166. Петровский С. В. Интернет-услуги в российском праве. – М.: Агентство «Издательский сервис», 2015.

167. Рыжиченков В.И. Преступления, совершаемые в сфере незаконного оборота наркотиков (Теория и практика): дис. ... канд. юрид. наук. – М., 2009.

168. Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дис…. канд. юрид. наук. – М, 2015.

169. Суслина Е.В. Ответственность за мошенничество по Уголовному

кодексу Российской Федерации: автореф. дисс. канд. юрид. наук. – Екатеринбург, 2014.

170. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: понятие, состояние, уголовно-правовые меры борьбы: дис…. канд. юрид. наук. – Владивосток, 2005.

171. Тропина Т.Л. «Компьютерное мошенничество»: вопросы квалификации и законодательной техники, [Электронный ресурс] – Режим доступа – URL: http://www.connect.ru/ (дата обращения: 07.12.2017).

172. Чекунов И.Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: дис. … канд. юрид. наук. – М., 2013.

173. Чернышева В.О. Интернет и преступность // Реагирование на преступность: концепции, закон, практика. – М., 2017.

Справочная литература

174. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (заключена в г. Вене 20.12.1988) //Сборник международных договоров СССР и Российской Федерации. Вып. XLVII.- М., 1991.

175. Aghatise E. J. Cybercrime definition. Computer Crime Research Center. – URL: http:// www.crime-research.org/articles/joseph06 (дата обращения: 02.05.2018).

176. Википедия – свободная энциклопедия. – URL: https://ru.wikipedia.org (дата обращения: 02.05.2018).

177. Oxford dictionaries language matters. – URL: http://www.oxforddictionaries.com (дата обращения: 02.05.2018).

178. Macmillan dictionary.URL: http://www.macmillandictionary.com (дата обращения: 02.05.2018).

179. Мошенничество в сфере знакомств в сети Интернет. - URL: http://www.phreaking.ru/showpage.php?pageid=54356 (дата обращения: 15.03.2018).

180. Обзор хостинг-провайдеров.URL : www.cy-pr.com/hosting (дата обращения 03.02.2018).
181. «Ограблен в сетевых переулках» URL: // http:// http://www.ng.ru/society/2008-02-19/10_internet.html (дата обращения: 01.10.2018).
182. Определение местоположения по IP-адресу. [Электронный ресурс]. – Режим доступа: www.itpride.net/useful/ip.html (дата обращения 26.02.2018 г.).
183. Показатели преступности в России. – Официальный сайт Генеральной прокуратуры Российской Федерации. - [Электронный ресурс] – Режим доступа. URL: http://www.crimestat.ru/.
184. Преступность в регионах. – Официальный сайт Генеральной прокуратуры Российской Федерации. - [Электронный ресурс] – Режим доступа. URL: http://www.crimestat.ru/.
185. Статистические данные. – Официальный сайт МВД Российской Федерации. - [Электронный ресурс] – Режим доступа. URL:URL: https://мвд.рф/reports/item/14468708/
186. Уголовный кодекс Франции / перевод с фр. и предисл. Н. Е. Крыловой; науч. ред. Л. В. Головко, Н. Е. Крыловой. - СПб. : Юридический центр Пресс, 2002.
187. Уголовное дело № 143600066 // Архив Динского СО при ОВД ст. Динской.
188. The Convention on Cybercrime (ETS) 185 / Council of Europe 2015. – URL: http://www.conventions.coe.int/Treaty/ (дата обращения: 07.01.2018).

Базы данных, информационно-справочные и поисковые системы.

- http://www.consultant.ru – Правовая система «Консультант Плюс»;
- http://www.constitution.garant.ru – Правовая система «Гарант»;
- http://www.garant.ru – информационно-правовой портал «Гарант»;
- http://www.ksrf.ru/ – Официальный сайт Конституционного суда Российской Федерации;

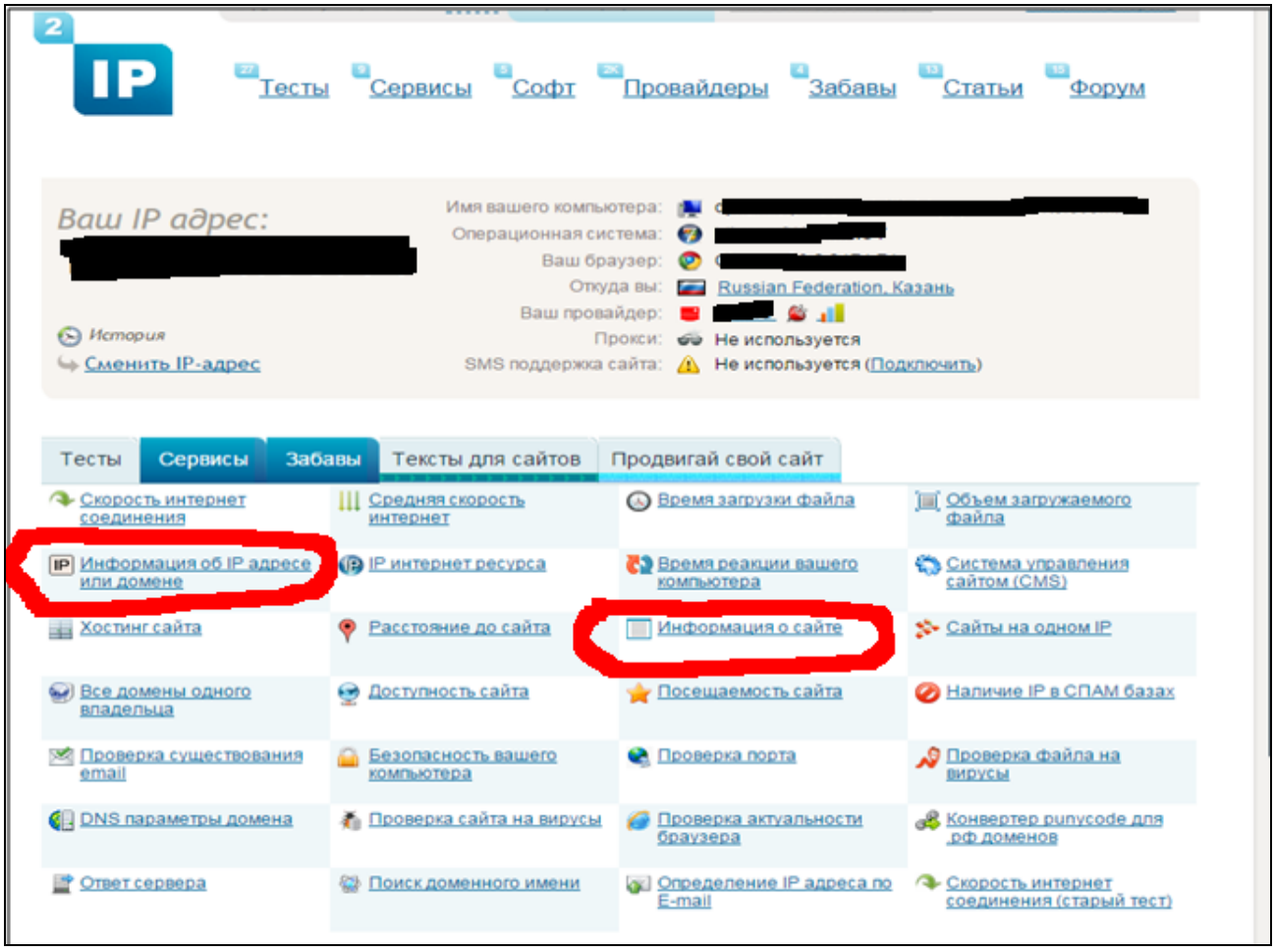
- http://www.supcourt.ru – сайт Верховного Суда Российской Федерации;
- http://www.vsrf.ru. – Официальный сайт Верховного суда РФ.
- http://president.kremlin.ru/ – Официальный сайт Президента России;
- http://www.un.org – Организация Объединенных Наций;
- http://www.gov.ru – Официальный сервер органов государственной власти Российской Федерации;
- http://www.gov.ru/main/ministry/isp-vlast44.html – Официальный сайт Федеральных органов исполнительной власти;
- http://www.gov.ru/main/page7.html – Официальный сайт Федерального собрания РФ;
- http://www.government.ru – Официальный сайт Правительства России;
- http://www.genproc.gov.ru – Официальный сайт Генеральной прокуратуры Российской Федерации;
- http://www.mvd.ru – Официальный сайт Министерства внутренних дел РФ;
- http://guebmvd.ru – сайт Главного управления экономической безопасности и противодействия коррупции МВД России.
- http://www.minjust.ru – Официальный сайт Министерства юстиции РФ;
- http://www.sledcom.ru – Официальный сайт Следственного комитета РФ;
- http://www.gov.ru/main/page10.html – Официальный сайт Судебной власти РФ;
- http://rsl.ru - Российская государственная библиотека;
- http://elibrary.ru - Научная электронная библиотека;
- http://window.edu.ru – Электронная библиотека Федерального портала «Российское образование» «Единое окно»;
- http://www.big-library.info – Большая электронная библиотека;
- http://constitutions.ru – Российский правовой портал;

- http://www.juristlib.ru – Электронная юридическая библиотека «ЮристЛиб»;
- http://www.pravo.ru – ПравоRu;
- http://www.jur-portal.ru – Юридический портал jur-portal.ru;
- http://ur-fak.ru – Юридический портал;
- https://rospravosudie.com/ – крупнейшая база судебной практики в РФ с данными по адвокатам, юристам, судьям и прокурорам.

Приложения 1

1. На сайте www.2ip.ru определяем какому *ХОСТИНГУ* принадлежит данный сайт
   ХОСТИНГ – (англ. hosting) – услуга по предоставлению вычислительной мощности для размещения информации сервере, постоянно находящемся в сети (обычно Интернет), хостингом также называется услуга по размещению оборудования клиента на территории провайдера с обеспечением подключения его к каналам связи с высокой пропускной способностью.

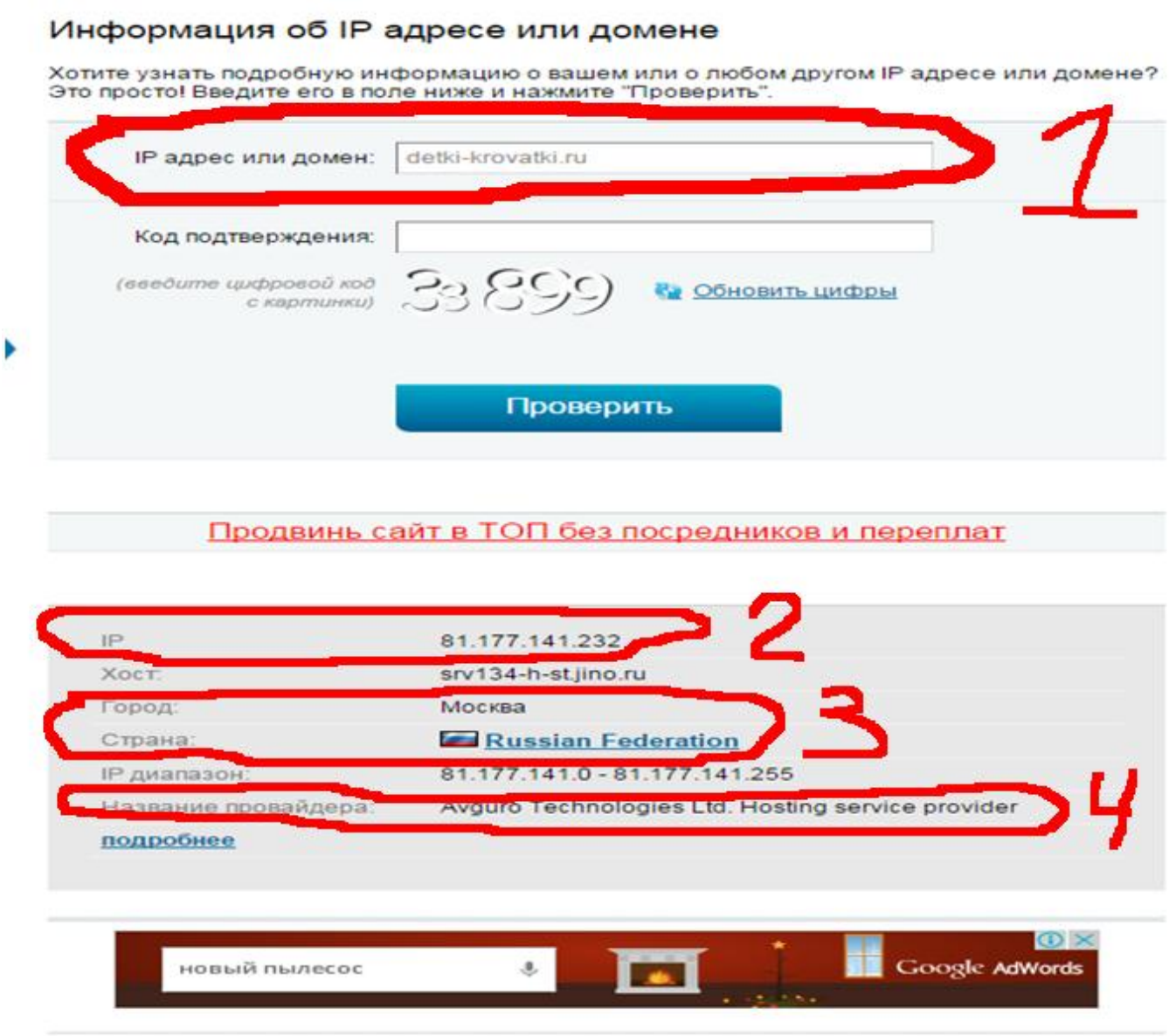
   На странице сайта www.2ip.ru выбираем нужную нам ссылку (в зависимости что нам нужно узнать):
1. «Информацию об IP адресе или домене»
2. «Информацию о сайте»
   Мы выбираем «Информацию о сайте»



   После того как нажали на ссылку: «Информацию о сайте» видим следующее окно, где нам предлагают ввести интересующий нам IP адрес или домен

1. В строке «IP адрес или домен» вводим нужный нам адрес сайта:

www.detki-krovatki.ru.

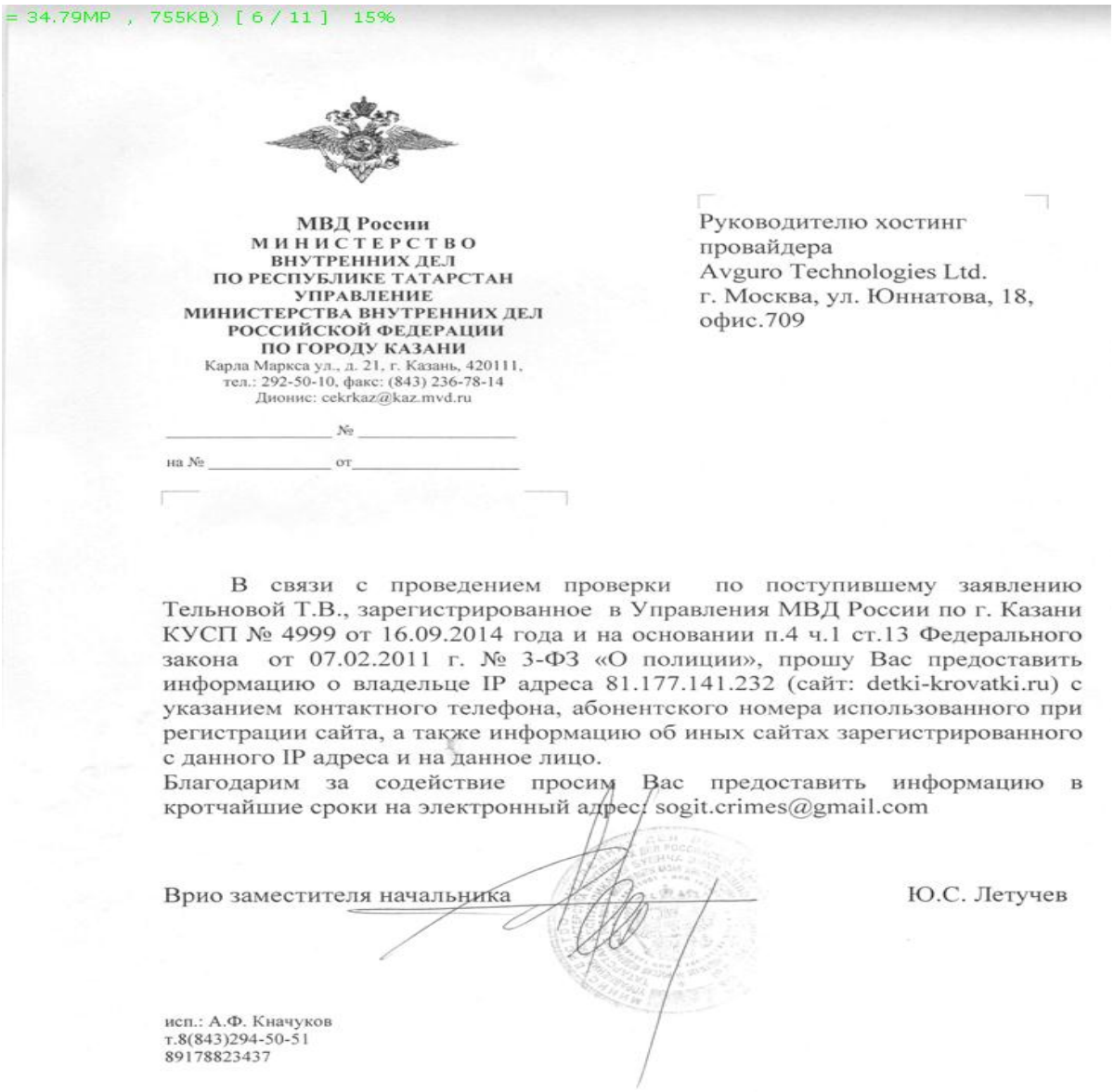


После не долгого ожидания видим результат:

2. IP адрес: **81.177.141.232** принадлежащий сайту www.detki-krovatki.ru.
3. Город и страну, если Хостинг провайдер зарегестрирован на запределами Российской Федерации, то необходимо делать запрос через отдел Интерпола МВД РФ по РТ.
4. Название провайдера: AvgurotechnologiesLtd. Hostingserviceprovider , Хостинг провайдер на котором зарегестрирован сайт www.detki-krovatki.ru.

Приложения 2

После этого готовим запрос для получения информации о владельце IP адреса: **81.177.141.232** (сайт: www.detki-krovatki.ru) по примерному образцу: Образец запроса Хостинг провайдеру:



= 34.79MP , 755KB) [6 / 11] 15%

МВД России
МИНИСТЕРСТВО
ВНУТРЕННИХ ДЕЛ
ПО РЕСПУБЛИКЕ ТАТАРСТАН
УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ГОРОДУ КАЗАНИ
Карла Маркса ул., д. 21, г. Казань, 420111,
тел.: 292-50-10, факс: (843) 236-78-14
Дионис: cekrkaz@kaz.mvd.ru

№ _____

на № _____ от _____

Руководителю хостинг
провайдера
Avguro Technologies Ltd.
г. Москва, ул. Юннатова, 18,
офис.709

В связи с проведением проверки по поступившему заявлению Тельновой Т.В., зарегистрированное в Управления МВД России по г. Казани КУСП № 4999 от 16.09.2014 года и на основании п.4 ч.1 ст.13 Федерального закона от 07.02.2011 г. № 3-ФЗ «О полиции», прошу Вас предоставить информацию о владельце IP адреса 81.177.141.232 (сайт: detki-krovatki.ru) с указанием контактного телефона, абонентского номера использованного при регистрации сайта, а также информацию об иных сайтах зарегистрированного с данного IP адреса и на данное лицо.
Благодарим за содействие просим Вас предоставить информацию в кротчайшие сроки на электронный адрес: sogit.crimes@gmail.com

Врио заместителя начальника Ю.С. Летучев

исп.: А.Ф. Кначуков
т.8(843)294-50-51
89178823437

Ответ от Хостинг провайдера AvgurotechnologiesLtd. Hostingserviceprovider:

avguro

ООО «Авгуро Технолоджис»
ИНН / КПП: 7706641390 / 770201001

127083, Москва, Юннатов ул., д. 18, офис. 709
+7 (495) 797-95-53, +7 (495) 229-30-31
info@avguro.ru / http://www.avguro.ru

Заместителю начальника полиции
управления МВД России по г. Казани
Ю.С. Летучеву
от ООО «Авгуро Технолоджис»

На ваше обращение N Б-9а 038 от 18.09.2014 о предоставлении информации сообщаем:

1 Имеющиеся у нас данные по ресурсу Detki-Krovatki.ru

2 Логин: zeta
Номер договора: 045915261
Время регистрации: 2 ноября 2013 г. 19:14:29

3 Контактный E-mail: mbhor@yandex.ru

4 Юридическое лицо
Наименование: Общество с ограниченной ответственностью «ЗЕТА»
IP при регистрации: 178.204.204.100
Юридический адрес: 420138 г. Казань, ул. Юлиуса Фучика, д.49
ИНН: 1659121190
КПП: 165901001

5

6 Другие доменные имена, размещённые на учётной записи пользователя: kupilkrovat.ru, mfuspeh.ru, economkrovatki.ru, bumkrovatki.ru, krovatuspeh.ru.

7 Последний доступ в контрольную панель для управления ресурсами (вкл. Работу с файлами) осуществлялся клиентом удалённо со следующих IP-адресов (время московское):

06.08.2014 18:32 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:31.0) Gecko/20100101 Firefox/31.0
26.07.2014 22:23 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
11.07.2014 20:54 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
08.07.2014 19:39 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
07.07.2014 09:40 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0
06.07.2014 20:45 92.255.207.148 Mozilla/5.0 (Windows NT 6.3; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0

8 Оплата производилась клиентом самостоятельно, в том числе через расчётный счёт:

Номер документа 7 от 05.11.2013
Сумма 2000,0
Наименование платежа Оплата по счету № 306613405963 от 02 ноября 2013 г., за веб услуги В том числе НДС (18%), 305.08 руб.
Покупатель ООО "ЗЕТА" Р/С 40702810029150000078
ИНН покупателя 1659121190
РС покупателя 30302810900000001006
КПП получателя 165901001
Банк покупателя ОАО "АЛЬФА-БАНК" г МОСКВА
БИК банка покупателя 044525593
КС банка покупателя 30101810200000000593

Генеральный директор Е.Л. Магдесиев
23.09.2014

В ответе от провайдера видим следующую информацию:

Что на самом деле на Хостинге AvgurotechnologiesLtdзарегестрирован данный сайт:

1. Название сайта www.detki-krovatki.ru
2. Логин: Zeta

- Номер договора: 045915261
- Время регистрации: 2 ноября 2013 г. 19:14:29

3. Контактный E-mail: mbhpr@yandex.ru
4. Владельца данного сайта в нашем случае это юридическое лицо: Общество с ограниченной ответственностью «ЗЕТА», так юридический адрес организации: 420138 г. Казань, ул. Юлиуса Фучика, д. 49
   ИНН: 1659121190
   КПП: 165901001
5. IP адрес при регистрации: 178.204.204.100
6. Другие доменные имена, размещенные на учетной записи пользователя: www.kupilkrovat.ru, www.mfuspeh.ru, www.economkrovatki.ru, www.bumkrovatki.ru, www.krovatuspeh.ru.
7. Последний доступ в контрольную панель для управления ресурсами (вкл. Работу с файлами) осуществлялся клиентом удаленно со следующих IP-адресов (время московское):

- Первый вход был осуществлен: 06.07.2014 года в 20:45 IP адрес 92.255.207.148
- Последний вход был осуществлен: 06.08.2014 года в 18:32 IP адрес 92.255.207.148.

Как видим вход разное время был осуществлен с одного и того же IP адреса.

8. В «8» пункте видим каким способом производилась оплата за услуги Хостинг провайдера AvgurotechnologiesLtd,

- Номер Дату оплаты: № 7 от 05.11.2013 года
- Сумму: 2000 рублей
- Наименование платежа: Оплата по счету: № 306613405963 от 02 ноября 2013 года за веб услуги в том числе НДС (18%), 305.08 рублей.
- Покупатель: ООО «ЗЕТА» расчетный счет 40702810029150000078
- Банк в котором открыт счет на организацию ООО «ЗЕТА».