

Министерство внутренних дел Российской Федерации

**Федеральное государственное казенное
образовательное учреждение высшего образования
«Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова»**

**АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ
В СОВРЕМЕННЫХ УСЛОВИЯХ**

Сборник статей

**Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2020**

УДК 351.745.7
ББК 32.84
А-43

Редакционная коллегия:

Д.Ф. Флоря (председатель),
Д.В. Кураков (заместитель председателя),
Р.А. Белевский, С.В. Екимцев,
И.М. Смирнов (ответственный секретарь)

А-43 **Актуальные вопросы осуществления оперативно-розыскной деятельности органов внутренних дел в современных условиях : сборник статей / редкол.: Д.Ф. Флоря [и др.]. – Орловский юридический институт МВД России имени В.В. Лукьянова, 2020. – 80, [1] с. – 22 экз. – Текст : непосредственный.**

Сборник составлен по материалам научно-представительских мероприятий: круглого стола «Особенности и проблемы проведения отдельных оперативно-розыскных мероприятий при раскрытии и расследовании преступлений», круглого стола «Актуальные вопросы борьбы с похищением автотранспортных средств».

Материалы публикуются в авторской редакции.

УДК 351.745.7
ББК 32.84

© ОрЮОИ МВД России имени В.В. Лукьянова, 2020

ОГЛАВЛЕНИЕ

<i>Бражников Д.А.</i> НЕКОТОРЫЕ АСПЕКТЫ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СОЦИАЛЬНЫХ СЕТЯХ.....	4
<i>Бычков В.В.</i> ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ И ДОКАЗЫВАНИЮ ПРИ РАССЛЕДОВАНИИ «ЭКСТРЕМИСТСКОГО ХУЛИГАНСТВА» (п. «б» п. 1 ст. 213 УК РФ).....	8
<i>Велиев Я.П.</i> К ВОПРОСУ О ПРЕДУПРЕЖДЕНИИ МОШЕННИЧЕСТВ В СФЕРЕ АВТОКРЕДИТОВАНИЯ.....	13
<i>Екимцев С.В., Филатьева И.В.</i> ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ.....	19
<i>Косарев К.В.</i> НЕКОТОРЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ «МОБИЛЬНЫХ» МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ ОСУЖДЕННЫМИ В ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЯХ	23
<i>Малышев С.Я., Миняшева Г.И.</i> РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ (НЕГЛАСНОСТИ): ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ.....	29
<i>Михайлова Л.В.</i> СИСТЕМНО-СТРУКТУРНЫЙ АНАЛИЗ ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ НА ОБЪЕКТАХ ВОДНОГО ТРАНСПОРТА.....	36
<i>Морозова Н.В., Малащенко П.К.</i> ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ СЛЕДОВАТЕЛЕМ ПРЕДЕЛОВ ДОКАЗЫВАНИЯ	42
<i>Поддубный И.В.</i> ОТДЕЛЬНЫЕ ВОПРОСЫ РАСКРЫТИЯ ХИЩЕНИЙ С БАНКОВСКИХ КАРТ ГРАЖДАН, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ	47
<i>Смирнов И.М., Мирошкин Э.А.</i> ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ, ОБЕСПЕЧИВАЮЩИЕ БЕЗОПАСНОСТЬ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ	53
<i>Чаплыгина В.Н., Волкова В.Р.</i> ОСОБЕННОСТИ РАССЛЕДОВАНИЯ СЕРИЙНЫХ УБИЙСТВ	58
<i>Шеметов А.К.</i> НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЕ ПРЕСТУПЛЕНИЙ НЕСОВЕРШЕННОЛЕТНИХ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИКОВ	62
<i>Шляхова В.В.</i> НЕКОТОРЫЕ ВОПРОСЫ ПРОВЕДЕНИЯ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКИ ПО СООБЩЕНИЮ О ПРЕСТУПЛЕНИИ, ПРЕДУСМОТРЕННОМУ СТ. 186 УК РФ	68
<i>Яппаров Р.М.</i> ВЫЯВЛЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ	73

НЕКОТОРЫЕ АСПЕКТЫ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В СОЦИАЛЬНЫХ СЕТЯХ

*Бражников Дмитрий Анатольевич,
кандидат юридических наук, доцент,
доцент кафедры цифровой криминалистики*

*Московский государственный технический
университет имени Н.Э. Баумана
105005, Москва, 2-я Бауманская ул., 5*

В статье рассмотрены некоторые вопросы раскрытия преступлений, совершаемых в социальных сетях. Приводятся основные способы совершения преступлений, совершаемых с использованием сети Интернет.

Ключевые слова: раскрытие, Интернет, социальные сети, мессенджеры, компьютерные преступления.

На современном этапе развития общества наблюдается негативный рост преступлений совершаемых в социальных сетях и как раз их постоянный мониторинг, может помочь органам предварительного следствия и дознания, установить личность преступника и в последствии доказать его виновность.

Социальная сеть (англ. social network) – это часть информационного пространства телекоммуникационной сети Интернет (интерактивная платформа со множеством пользователей, онлайн-сервис или веб-сайт), предназначенная для построения, отражения и организации социальных связей и взаимоотношений в сети Интернет [1].

Первые предположения о появлении социальных сетей появились в 1837 году, когда русский писатель, философ и общественный деятель XIX века Владимир Одоевский в своем незаконченном утопическом романе «4338-й год» предсказал появление современных блогов и Интернета в целом. В нём сказано, что «между знакомыми домами устроены магнетические телеграфы, посредством которых живущие на далёком расстоянии разговаривают друг с другом», а также о «домашних газетах», издающихся «во многих домах, особенно между теми, которые имеют большие знакомства»: этими газетами «заменяется обыкновенная переписка», в них «помещаются обыкновенно извещение о здоровье или болезни хозяев и другие домашние новости, потом разные мысли, замечания, небольшие изобретения, а также и приглашения, когда же бывает зов на обед, то и le menu».

Популярность в сети Интернет социальные сети начали завоёвывать в 1995 году, с появлением американского портала Classmates.com. Проект оказался весьма успешным, что в последующие несколько лет спровоцировало появление не одного десятка аналогичных сервисов. Но официальным началом «бума» социальных сетей принято считать социальные сети принято считать запущены LinkedIn, MySpace и Facebook. В русскоязычном сегменте Интернета социальные сети стали набирать популярность с 2006 года, когда в России появились

первые собственные социальные сети – Одноклассники и ВКонтакте, имевшие сайты на русском языке (у Facebook русская версия сайта появилась только в 2008 году).

В последствии стали создаваться социальные сети в рамках отдельных стран, к примеру мессенджер с элементами социальной сети WeChat в Китайской Народной Республике. На данный момент существует всего 9 социальных сетей (не учитывая Instagram), у которых количество индивидуальных пользователей превышает 100 млн.

В 2010 году было создано приложение для обмена фотоизображениями и видеозаписями с элементами социальной сети «Instagram». На данный момент эта социальная сеть является одним из самых популярных мобильных приложений и насчитывает более 1 миллиарда активных пользователей, кто пользуется приложением минимум 1 раз в месяц.

Согласно пункту 1.1 Правил сайта «ВКонтакте», социальная сеть – это информация, размещенная на сайте в сети Интернет по определенному адресу и доступная пользователю через сайт, мобильную версию сайта, приложения и иные ресурсы, представляющая собой результат интеллектуальной деятельности в форме программы для ЭВМ [2].

Гражданский кодекс Российской Федерации в статье 1261 раскрывает содержание понятия «программа для ЭВМ» [3]. Согласно данной статье, программа для ЭВМ – это представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Соответственно и сама социальная сеть представлена в объективной форме совокупностью данных и команд, и создаваемых аудиовизуальных отображений, предназначенных для функционирования ЭВМ и мобильных устройств в целях получения определенного результата в виде организации функционала социальной сети.

Исходя из проведенного анализа судебной практики за последние несколько лет, можно выделить составы преступлений, предусмотренных Уголовным кодексом Российской Федерации, которые чаще остальных совершаются при помощи социальных сетей. Одними из самых распространенных преступлений являются преступления против общественной безопасности, основ конституционного строя и безопасности государства, а именно: публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (статья 205.2), публичные призывы к осуществлению экстремистской деятельности (статья 280), возбуждение ненависти, либо вражды, а равно унижение человеческого достоинства (статья 282).

Довольно часто с использованием социальных сетей совершаются такие преступления, как клевета (статья 128.1), мошенничество (статья 159), незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (статья 228.1),

незаконные изготовление и оборот порнографических материалов или предметов (статья 242).

По мере компьютеризации населения, роста доступности средств массовых коммуникаций наблюдается рост количества преступлений, совершаемых в отношении неприкосновенности частной жизни (статья 137), тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 138).

В рассматриваемую группу попадают также преступления, предусмотренные статьями 272 и 273 Уголовного кодекса Российской Федерации (неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ) [4].

Помимо вышеперечисленных преступлений, в последнее время получили распространение статьи 110 и 110.1 Уголовного кодекса Российской Федерации (доведение до самоубийства; склонение к совершению самоубийства или содействие совершению самоубийства). Реже совершаются следующие преступления: организация занятия проституцией (статья 241); организация деятельности экстремистской организации (статья 282.2); организация незаконного вооруженного формирования или участие в нем (статья 208); организация преступного сообщества (преступной организации) или участие в нем (ней) (статья 210).

Так, приговором Октябрьского районного суда г. Рязани от 28 сентября 2017 года был осужден В.А. Кротов по части 2 статьи 210 Уголовного кодекса Российской Федерации, который был организатором распространения наркотических средств по региону, для чего использовал сеть «ВКонтакте» [5].

Говоря о способах совершения преступлений, стоит заметить, что их разнообразие ограничивается функционалом социальной сети и зависит от механизма совершения преступления. Чаще других среди способов совершения преступлений исследуемой группы встречается распространение изображений. Изображение гражданина представляет собой его индивидуальный облик, запечатленный в какой-либо объективной форме, в частности в произведении изобразительного искусства, на фотографии или в видеозаписи. Причем под изображением гражданина следует понимать внешний облик гражданина, включающий в себя не только лицо, но и внешний вид гражданина в целом. Изображения могут содержать элементы, порочащие честь и достоинство личности, экстремистского, порнографического и иного характера. Так, согласно приговору Гагаринского районного суда города Севастополь гр. «А» был привлечен к уголовной ответственности по части 1 статьи 137 Уголовного кодекса Российской Федерации. Используя сайт «ВКонтакте», он отправил нескольким пользователям изображения потерпевшей в обнаженном виде, а также совершающей действия сексуального характера [6]. Данными действиями было нарушено право потерпевшей на неприкосновенность частной жизни.

Среди способов можно выделить также распространение видео- и аудиозаписей. Аудиозаписи позволяют фиксировать любую информацию, которая может быть выражена в звуковой форме. Особое значение аудиозаписей с точки зрения их содержания состоит в возможности с их помощью фиксировать разговоры, предшествующие и сопровождающие действия (бездействие), и иные ком-

поненты так называемого «звукового ряда» (выкрики, возгласы, музыка, иные сопутствующие звуки и шумы).

Использование видеозаписи позволяет точно зафиксировать и сохранить значительную часть информации о произошедшем действии. С помощью аудио и видеозаписей возможно фиксирование не только самого результата действий (бездействия), но и собственно, информации о том, как это действие протекало во времени, а также обстановки, в которой происходило действие (бездействия), и иные обстоятельства, сопровождавшие действие (бездействия) и предшествовавшие ему, наличие которых может поставить под сомнение его законность. С помощью аудио- и видеозаписей информация фиксируется в динамике. При исследовании записей существует большая вероятность восстановить события, именно в том виде и в той последовательности, в которой они имели место в действительности, настолько, насколько позволяют их зафиксировать технические средства.

Согласно приговору Калужского областного суда Е.И. Зинов был привлечен к уголовной ответственности по части 1 статьи 282 Уголовного кодекса Российской Федерации. Данным гражданином были размещены на своей странице во «ВКонтакте», видео- и аудиозаписи экстремистского характера, содержание которых оскорбляет Государственный флаг Российской Федерации и День воинской славы России – 9 мая [7].

Третьим самым распространенным способом совершения преступлений с использованием социальных сетей является распространение текстов на персональной странице и в сообществах. Так, приговором Хасавюртского городского суда от 6 мая 2015 года, по части 2 статьи 128.1 был осужден Р.А. Асакаев. «ВКонтакте» был распространен текст, содержащий сведения, порочащие честь и достоинство потерпевшей [8].

На данный момент социальные сети не используются в полной мере для выявления и раскрытия преступлений, потому что это довольно новый метод и еще отсутствуют методические рекомендации и полноценные научные исследования в этой сфере.

1. Социальная сеть [Электронный ресурс] // Википедия [2017–2017]. URL: <http://ru.wikipedia.org/?oldid=85548865> (дата обращения: 17.04.2020).

2. Правила пользования сайтом Вконтакте [Электронный ресурс]. URL: <https://vk.com/terms> (дата обращения: 20.03.2020).

3. Гражданский кодекс Российской Федерации [Электронный ресурс]: от 26 января 1996 г. № 14-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

4. Уголовный кодекс Российской Федерации [Электронный ресурс]: от 13 июня 1996 г. № 63-ФЗ: в ред. от 23 апреля 2019 г. Доступ из справ.-правовой системы «КонсультантПлюс».

5. Приговор Октябрьского районного суда г. Рязани по уголовному делу № 1-229/2017 по обвинению Кротова В.А. по ч. 2 ст. 210 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». URL: <http://sudact.ru/regular/doc/STfEbGVF4GU9> (дата обращения: 20.03.2020).

6. Приговор Гагаринского районного суда г. Севастополя по уголовному делу № 1-183/2016 по обвинению ФИО1 по ч. 1 ст. 137 УК РФ. 2016 год [Электронный ресурс] // Справочная система «СудАкт». URL: <http://sudact.ru/regular/doc/1N5srs50gto9> (дата обращения: 20.03.2020).

7. Приговор Калужского областного суда по уголовному делу № 2-14/2017 по обвинению Любшина И.В. по ч. 1 ст. 282 УК РФ. 2017 год [Электронный ресурс] // Справочная система «СудАкт». URL: <http://sudact.ru/regular/doc/z1JyiOCqwZmJ> (дата обращения: 20.03.2020).

8. Приговор Хасавюртского городского суда по уголовному делу № 1-96/2015 по обвинению Асакаева Р.А. по ч. 2 ст. 128.1 УК РФ. 2015 год [Электронный ресурс] // Справочная система «СудАкт». URL: <http://sudact.ru/regular/doc/KWaHTTfQfcLw> (дата обращения: 20.03.2020).

**ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ
И ДОКАЗЫВАНИЮ ПРИ РАССЛЕДОВАНИИ
«ЭКСТРЕМИСТСКОГО ХУЛИГАНСТВА»
(п. «б» п. 1 ст. 213 УК РФ)**

*Бычков Василий Васильевич,
кандидат юридических наук, доцент,
декан факультета повышения квалификации*

*Московская академия Следственного комитета Российской Федерации
125080, г. Москва, ул. Врубеля, д. 12*

В статье рассматриваются особенности определения предмета доказывания при расследовании хулиганства, совершенного по экстремистским мотивам. Сформулирована структура обстоятельств, подлежащих доказыванию, по уголовным делам данного вида.

Ключевые слова: *хулиганство, экстремизм, преступления экстремистской направленности, предмет доказывания; обстоятельства, подлежащие доказыванию.*

Последние 10 лет в Российской Федерации на фоне стабильного снижения преступности неуклонно растет количество преступлений экстремистской направленности [1, с. 60–71], в том числе и хулиганство по экстремистским мотивам, предусмотренного пунктом «б» части 1 статьи 213 Уголовного кодекса Российской Федерации [2].

При расследовании хулиганства по экстремистским мотивам, подлежат установлению и доказыванию обстоятельства [3, с. 138–145]:

- 1) по факту совершения уголовно наказуемого хулиганства:
 - нарушался ли общественный порядок;
 - было ли грубое нарушение общественного порядка, выражающее явное неуважение к обществу;

- в чем выражалось грубое нарушение общественного порядка;
- какие обстоятельства свидетельствовали о явном неуважении виновного к обществу;

2) по факту совершения хулиганства по экстремистским мотивам [4]:

- было ли грубое нарушение общественного порядка именно по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы;

- в чем выражалась политическая ненависть или вражда, партийная принадлежность потерпевшего;

- в чем выражалась идеологическая ненависть или вражда, идеологическая направленность потерпевшего;

- в чем выражалась расовая ненависть или вражда, раса потерпевшего;

- в чем выражалась национальная ненависть или вражда, национальность потерпевшего;

- в чем выражалась религиозная ненависть или вражда, религия или атеизм потерпевшего;

- в чем выражалась ненависть или вражда в отношении какой-либо социальной группы, вид данной социальной группы;

- место совершения хулиганства по экстремистским мотивам;

- время совершения хулиганства по экстремистским мотивам;

- способы совершения хулиганства по экстремистским мотивам;

- интенсивность совершения хулиганства по экстремистским мотивам;

- продолжительность совершения хулиганства по экстремистским мотивам;

- не сопровождалось ли хулиганство по экстремистским мотивам совершением других преступлений, каких именно;

- каковы причины совершения хулиганства по экстремистским мотивам;

- каковы обстоятельства, способствовавшие совершению хулиганства по экстремистским мотивам;

- имеются ли смягчающие и отягчающие обстоятельства совершения хулиганства по экстремистским мотивам;

3) в отношении лица, совершившего хулиганство по экстремистским мотивам [5]:

- установочные данные виновного (возраст, национальность, раса, религиозное исповедание, места регистрации и фактического проживания, внешность, особые приметы);

- возраст несовершеннолетнего (число, месяц и год рождения);

- понимал ли, что совершает противоправное действие, а именно хулиганство;

- понимал ли, что совершает хулиганство по экстремистским мотивам;

- каковы причины возникновения у него экстремистских мотивов;

- каких целей он хотел достичь при совершении хулиганства по экстремистским мотивам;

- не совершал ли он подобных действий ранее;

- не был ли привлечен ранее к административной ответственности за мелкое хулиганство;

- условия жизни и воспитания несовершеннолетнего, уровень психического развития и иные особенности его личности;

- влияние на несовершеннолетнего старших по возрасту лиц.

- не состоит ли на учете в полиции;

- его воспитание и взаимоотношения в семье и учебном заведении;

- мог ли в полной мере осознавать фактический характер и общественную опасность своих действий либо руководить ими (при наличии данных, свидетельствующих об отставании в психическом развитии, не связанном с психическим расстройством);

- наличие или отсутствие у несовершеннолетнего заболевания, препятствующего его содержанию и обучению в специальном учебно-воспитательном учреждении закрытого типа – для рассмотрения судом вопроса о возможности освобождения несовершеннолетнего от наказания и направлении его в указанное учреждение;

4) в отношении лица, потерпевшего от хулиганства по экстремистским мотивам [6, с. 36–41]:

- личность потерпевшего (партийная принадлежность, идеологическая направленность, раса, национальность, религиозное исповедание или атеизм, вид его социальной группы);

- не спровоцировал ли хулиганские действия;

- подвергался ли ранее подобному преступному воздействию, когда, где, при каких обстоятельствах;

5) по факту причинения вреда от хулиганства по экстремистским мотивам;

- какой вред причинен от хулиганских действий (физический, материальный, моральный);

- при причинении физического вреда: какова степень тяжести, факты обращения в медицинские учреждения, период лечения;

- при причинении материального вреда: какое имущество повреждено или уничтожено, его стоимость;

- при причинении морального вреда – в чем выражается;

6) при совершении хулиганства по экстремистским мотивам группой лиц по предварительному сговору:

- имел ли место сговор соучастников до начала действий, непосредственно направленных на совершение рассматриваемых преступлений;

- когда и где состоялся сговор;

- состоялась ли договоренность о распределении ролей в целях осуществления преступного умысла;

- какие конкретно действия совершены каждым исполнителем и другими соучастниками преступления;

- пособники преступной группы;

7) при совершении хулиганства по экстремистским мотивам организованной группой:

а) по факту создания организованной преступной группы:

- время и место создания группы;
 - инициатор создания группы;
 - создатели и руководители группы;
 - участники группы и наиболее ее активные члены;
 - время вступления каждого члена в группу и продолжительность участия в ее преступной деятельности;
 - характер и методы поддержания в группе дисциплины;
 - порядок вхождения в группу и выхода из группы;
 - пособники;
 - мотивы пособничества;
 - предварительная договоренность объединившихся в группу лиц совершать преступления, связанные с незаконным оборотом контрафактной продукции;
 - материально-техническое обеспечение группы;
- б) по руководству группой:
- кто из ее членов группы обладает качествами, присущими лидеру (организаторские способности, более высокий интеллектуальный уровень и др.);
 - кто из членов группы имеет опыт преступной деятельности;
 - кто принимал решения, связанные с:
- планированием деятельности группы и осуществлением отдельных преступных операций;
- руководством действиями участников группы при конкретных преступлениях;
- распределением доходов от преступной деятельности;
- в) по участию в группе:
- время и место вступления в группу каждого ее члена;
 - мотивы вхождения в группу каждого из ее участников;
 - в чем конкретно состояли действия каждого участника группы;
- г) по структуре группы:
- состав и характеристика ее участников (возраст, социальное положение, судимости, образ жизни, особые пристрастия и т.п.);
 - иерархия (руководители, активные и второстепенные участники);
 - наличие определенной дисциплины;
 - психологический микроклимат в группе (соперничество, иные конфликтные ситуации; нахождение между собой в родственных, дружеских, приятельских, интимных отношениях);
- д) по организованности и устойчивости группы:
- наличие лидера;
 - наличие иерархии;
 - наличие дисциплины;
 - объединение общим умыслом на совершение рассматриваемых преступлений;
 - планирование всей преступной деятельности группы и отдельных преступных операций;
 - распределение ролей участников группы в ходе всей преступной деятельности группы, а также при совершении конкретных преступлений;

- тщательная подготовка к совершению отдельных преступных операций;
- особо продуманные способы сокрытия преступлений;
- наличие в группе высококачественных и дорогостоящих технических средств и оборудования;
- длительность существования группы;
- стабильность состава группы;
- тесная взаимосвязь между членами группы и согласованность их действий;
- постоянство форм и методов преступной деятельности;
- количество совершенных преступлений;
- «обучение» членов группы, не имеющих преступного опыта;
- совместное проведение досуга;
- наличие «общака»;
- наличие коррупционных связей (в органах власти, в том числе и в правоохранительных органах, а также в средствах массовой информации);
- е) по цели создания преступной группы:
 - где, когда, какие деяния, связанные с хулиганством по экстремистским мотивам, осуществлялись;
 - способы осуществления этих деяний;

7) при совершении хулиганства по экстремистским мотивам, связанного с сопротивлением представителю власти либо иному лицу, исполняющему обязанности по охране общественного порядка или пресекающему нарушение общественного порядка [7, с. 32–41]:

- кому оказано сопротивление: если представителю власти: принадлежность к государственной организации, должностное положение; если иному лицу, исполняющему обязанности по охране общественного порядка или пресекающему нарушение общественного порядка: кем и на основе чего возложены данные обязанности;
- когда, где и при каких обстоятельствах оказано сопротивление;
- в чем выражалось сопротивление;
- какие последствия от оказанного сопротивления;
- какой вред причинен в результате сопротивления.

Таким образом, правильное определение предмета доказывания по любому расследуемому преступлению, в частности, экстремистского характера, имеет большое методическое значение. Оно помогает определить точное направление поиска доказательств, способствует четкому планированию расследования и обеспечивает требуемую законом всесторонность исследования обстоятельств расследуемого деяния.

1. Бычков В.В. Динамика российского терроризма и экстремизма в XXI веке // Расследование преступлений: проблемы и пути их решения. 2018. № 3 (21).

2. Багмет А.М., Бычков В.В. Расследование хулиганства по экстремистским мотивам, совершенного несовершеннолетними и в отношении несовершеннолетних: методические рекомендации. М.: Академия СК России, 2016. 78 с.

3. Бычков В.В. Предмет доказывания по уголовным делам о преступлениях экстремистской направленности // Библиотека криминалиста. 2013. № 4 (9).

4. Багмет А.М., Бычков В.В., Зеленков Ю.М. Расследование преступлений, связанных с экстремистской и террористической деятельностью: учебник. М.: ЮНИТИ-ДАНА, 2019. 719 с.

5. Бычков В.В. Противодействие преступлениям экстремистской направленности: курс лекций. М.: Юрлитинформ, 2013. 256 с.

6. Бычков В.В. Преступления экстремистской направленности: понятие, классификация, общие объективные и субъективные признаки, квалифицированные составы // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22).

7. Бычков В.В. Особенности производства отдельных следственных действий при расследовании преступлений экстремистского характера // Воронежские криминалистические чтения. 2018. № 3 (20).

К ВОПРОСУ О ПРЕДУПРЕЖДЕНИИ МОШЕННИЧЕСТВ В СФЕРЕ АВТОКРЕДИТОВАНИЯ

*Велиев Яков Павлович,
старший преподаватель кафедры
оперативно-разыскной деятельности органов внутренних дел*

*Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации
680020, г. Хабаровск, пер. Казарменный, д. 15*

В статье рассматриваются наиболее распространённые способы совершения мошеннических действий при получении кредита на покупку автотранспортного средства. Особое внимание уделяется механизму совершения данных преступлений. Предлагаются меры по предупреждению мошенничества совершаемого в сфере кредитования сделок купли-продажи автотранспортных средств.

Ключевые слова: *автотранспорт, кредит, мошенничество, договор купли-продажи, подделка, финансово-кредитное учреждение.*

На современном этапе развития потребительского рынка в России большая роль отводится кредитованию населения. В большинстве случаев при покупке дорогостоящего товара, люди обращаются в финансовые учреждения за предоставлением кредита. Как правило, таким товаром может являться недвижимое имущество, либо транспортное средство. В банковском секторе данным сферам кредитования проявляется повышенная заинтересованность. В каждом крупном финансовом учреждении созданы отделы, специализирующие на предоставлении ипотечного кредита на покупку недвижимости и на приобретение транспортного средства.

Автокредитование является видом потребительского кредитования целевой направленности и подразумевает конкретные требования к залому и определенные каналы продаж. Автокредит – особая форма потребительского кредита, при которой происходит авансированное движение ссужаемой стоимости приобретаемого транспортного средства от банка к заемщику на условиях возвратности, срочности, платности и дифференцированности с обеспечением в форме залога приобретаемого и зарегистрированного в установленном законом порядке транспортного средства [8]. В настоящее время автокредит является одним из распространённых кредитных продуктов, занимая важное место на отечественном рынке потребительского кредитования.

По данным Национального бюро кредитных историй и аналитического агентства «Автостат», в 2017 году России было выдано около 1 460 тыс. единиц автокредитов, в 2018 – 1 634,2 тыс. единиц, в 2019 составил 1 593,1 тыс. единиц. В 2019 году самое большое количество выданных автокредитов в регионах Российской Федерации было отмечено в Москве (75,2 тыс. шт.), Московской области (57,5 тыс. шт.), Санкт-Петербурге (57,2 тыс. шт.), а также Республиках Татарстан (48 тыс. шт.) и Башкортостан (42,5 тыс. шт.) [9].

Важно отметить, что уменьшение количества сделок на рынке не означает снижение уровня мошенничества в рассматриваемой сфере. Напротив, в период кризисов мошенники, по общему правилу, активизируются, а ряды их пополняются за счет неустойчивых граждан, у которых в благополучные годы больше мотивов к законопослушному поведению, и наоборот. Кроме того, факты мошенничества вскрываются постепенно, а факт обнаружения мошенничества не влечет моментальное решение проблемы, поэтому банки вынуждены разбираться с мошенничествами, совершенными как в текущий период, так и в предыдущие годы, в том числе и тогда, когда автокредитование было на пике.

В связи с наличием крупного сегмента на потребительском рынке, такого как кредитование на покупку автотранспортного средства, увеличивается и уровень преступных посягательств (мошеннических действий) в данной сфере.

Продажа автомобиля, находящегося в залоге у финансового учреждения, является одним из основных способов совершения мошеннических действий при купле-продаже автотранспортных средств. Автомобили приобретаются по программе автокредитования по подложным документам другого лица, и после одобрение кредита банка, автомобиль реализуется в течение месяца, до первого срока выплаты. Затем банк начинает обращаться к владельцу с требованием о выплате кредита, и при невозможности выплаты кредита обращается в суд. В дальнейшем суд выносит решение о возврате автотранспортного средства в банк, в связи с чем лицо, которое приобрело у преступников кредитный автомобиль по подложному ПТС, либо по дубликату ПТС (настоящий находится в банке до погашения задолженности), лишается автомобиля в пользу финансово-кредитного учреждения. В последующем потерпевший обращается в правоохранительные органы с заявлением о мошенничестве [3].

По мнению О.И. Ганченко, мошенничество, совершенное в сфере кредитования покупки транспортного средства, можно рассматривать, как умышленное и неумышленное. В случае неумышленного мошенничества в данной области предлагается считать, как «тривиальное неумение заемщика адекватно оце-

нить собственную платежеспособность». Неправильно рассчитав свои финансовые возможности, заемщик начинает задерживать платежи и однажды понимает, что не в состоянии погасить образовавшуюся задолженность [8, с. 7].

Предлагается сделать основной акцент на умышленное мошенничество, когда кредит оформляется с целью дальнейшей перепродажи автотранспортного средства и неуплаты денежной суммы по кредитному договору.

При анализе уголовных дел по факту мошеннических посягательств в финансово-кредитной сфере можно выделить следующие приемы хищения денежных средств:

- предоставление поддельных (ложных) документов. В их число, как правило, входят справка 2-НДФЛ, копия трудовой книжки и документы, удостоверяющие личность, заверяются все это фиктивными печатями, либо печатями предприятий, давно прекративших свою деятельность;

- оформление кредита на подставных лиц, которым за предоставление своих реальных данных банку, обещано денежное вознаграждение в случае успешной сделки. Как правило, в преступный сговор вступают лица из неблагополучной социальной среды.

В дальнейшем приобретенный нелегальным способом автомобиль легализуются различными способами:

- машина ставится на учет в ГИБДД и тут же снимается с учета, осуществляется продажа по генеральной доверенности или по копии паспорта бывшего владельца. Здесь следует отметить, что в автосалонах или на автомобильных рынках распространена практика перепродажи автомобиля по копии паспорта бывшего владельца, где не нужна доверенность или присутствие собственника. Перекупщики представляются лицами, имеющими к владельцу непосредственное отношение, показывают рукописный договор о получении автомобиля;

- в паспорт технического средства (далее ПТС) вписывается новый собственник, зачастую с помощью сотрудника автосалона и после чего автомобиль ставится на учет в ГИБДД и тут же снимается с него, для дальнейшей продажи третьему лицу;

- после постановки на учет ПТС сдается в банк, выдавший кредит на покупку автомобиля, и заемщик идет в ГИБДД, где пишет заявление об утере ПТС, ему выдается копия, он снимает машину с учета и продает [3].

Примером рассматриваемого мошенничества является уголовное дело в отношении гр. Родина Е.М. по части 4 статьи 159.1, части 4 статьи 174.1 Уголовного кодекса Российской Федерации (далее – УК РФ), который организовал хищение денежных средств у кредитных финансовых учреждений. Родин Е.М. оформлял поддельные документы, необходимые для получения в банках кредитов, представлял эти поддельные документы и обеспечивал явку иных участников преступной группы в банки для оформления кредитов. Родин Е.М. организовал преступные группы, у которых были строго распределены роли: первая группа занималась оформлением поддельных документов для кредитно-финансовых учреждений, вторая группа по поддельным документам непосредственно получала денежные средства и автотранспортные средства из автосалонов, третья группа оформляла на указанные автомашины право собственности в органах Государственной инспекции безопасности дорожного движения (далее

ГИБДД), после чего реализовывала сторонним лицам посредством оформления сделок купли-продажи автотранспортных средств [5].

Таким образом, организованная преступная группа занималась хищением денежных средств у банков под видом получения кредитов на покупку автомобилей, и последующей легализацией похищенных у банков денег путем совершения гражданско-правовых сделок купли-продажи автомобилей и последующей их регистрации в органах ГИБДД, на первый взгляд носящих законный характер, но в действительности имеющих цель придать видимость правомерности владения, пользования и распоряжением отдельными видами автотранспортных средств.

Рассмотрим следующую преступную схему, которая применяется преступными группами, в состав которых входят должностные лица финансово-кредитной организации, занимающиеся оформлением кредитных договоров и выдачей денежных средств. В том числе и сотрудники автосалонов, занимающихся кредитованием сделок купли-продажи автомобилей.

Примером мошенничества с использованием должностного положения сотрудников банка при выдаче кредитного продукта является уголовное дело в отношении гр. Хазовой О.Н. и сотрудников автосалона, которые используя свое должностное положение, оформили кредит на покупку автотранспортного средства в салоне по поддельным документам (паспорт гражданина Российской Федерации, 2-НДФЛ, копия трудовой книжки). Впоследствии данное транспортное средство было реализовано сторонним лицам, которые не были осведомлены о незаконном приобретении автомобиля [6].

Таким образом, проводя анализ уголовных дел, возбужденных по факту мошеннических посягательств в области автокредитования, можно выделить следующие криминогенные факторы:

- неэффективная организационная работа финансово-кредитных учреждений в сфере автокредитования;
- некачественная работа подразделений экономической безопасности, осуществляющих проверку документов (2-НДФЛ, копия документа, удостоверяющего личность, водительское удостоверение и т.д.), предоставляемых в банк для получения кредита;
- невозможность полноценного и беспрепятственного доступа правоохранительных органов к информационным массивам финансово-кредитных учреждений, составляющим коммерческую и банковскую тайну о лицах, получающих кредитный продукт;
- отсутствие должной работы с увольняемыми сотрудниками финансово-кредитных учреждений, которые могут иметь информацию, составляющую банковскую тайну;
- неэффективное взаимодействие между сотрудниками банка, занимающимися экономической безопасностью и правоохранительными органами в области предупреждения и выявления мошенничеств при получении кредитных денежных средств (финансово-кредитные учреждения не обеспечиваются информацией о негативно характеризующихся лицах и об утраченных или украденных паспортах граждан и т.д.);

- отсутствие первичных сведений в ГИБДД об автотранспортных средствах, приобретенных в кредит (только после того, как лицо определенное время не исполняет обязательства по кредитному договору, по судебному решению выносится запрет на переоформление транспортного средства), за исключением автомобилей, приобретенных по договору лизинга;

- несовершенство технических средств, способствующих предупреждению завладения кредитными средствами в части определения подделки документов, а также отсутствие централизованной компьютерной связи между всеми банками и правоохранительными органами, которая способствовала бы обеспечению современной информацией банков о возможности мошеннических действий в сфере кредитования [4, с. 23];

- недостатки в работе правоохранительных органов по выявлению лиц, занимающихся мошенническими действиями в сфере автокредитования (выявление и постановка на учет лиц, занимающихся подделкой документов, печатей, бланков, создающих фиктивные предприятия, ранее совершавших данные преступления).

Вышеуказанные недостатки не являются исчерпывающими, в каждой конкретной оперативной ситуации, сложившейся в результате предупреждения, пресечения, выявления и раскрытия мошеннических посягательств в сфере автокредитования, могут быть установлены иные причины, послужившие возникновению данного преступного деяния.

Одной из наиболее важных задач, стоящих перед оперативными подразделениями, занимающимися борьбой с мошенническими посягательствами в сфере автокредитования, является предупреждение данного преступления.

В юридической литературе существует достаточно много мнений о предупреждении преступлений. Так, В.Н. Кудрявцев и В.Е. Эминов считают, что предупреждение преступности – это система взаимосвязанных элементов, интегрированных в процессе этой деятельности и ее результатов [7]. По мнению Г.А. Аванесова, предупреждение преступлений – многоуровневая система мер воздействия на криминогенные объекты с целью их ограничения, устранения или нейтрализации, осуществляемых государственными органами, должностными лицами, гражданами и общественными формированиями. Под криминогенными объектами понимаются негативные социальные процессы их взаимосвязь и явления, взаимодействие которых порождает и обуславливает преступность [1]. В.Н. Бурлаков пишет: «предупреждение преступности» есть деятельность государства и общества направленная против преступности с целью удержания ее на социально терпимом уровне посредством устранения или нейтрализации порождающих ее причин» [2].

Рассмотрев вышеизложенные мнения, можно сделать вывод, что предупреждение мошенничеств в сфере автокредитования – это система комплексных, взаимосвязанных между собой мер правоохранительных органов и финансово-кредитных учреждений, направленных на устранение причин и условий, способствующих совершению противоправных деяний.

Предлагается следующие меры по предупреждению преступлений в сфере автокредитования:

- создание информационной базы данных заемщиков, между всеми финансово-кредитными учреждениями с правом доступа правоохранительных органов (при соблюдении Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»);

- обмен информацией между банками, создание кредитных бюро, анализ мошеннических схем с целью их предотвращения в будущем;

- обмен сведениями между правоохранительными органами и подразделениями экономической безопасности банков, в части лиц, обосновано подозреваемых в мошеннических схемах, и иной значимой информации, необходимой для решения вопросов, возникающих в ходе проведения оперативно-розыскных мероприятий;

- контроль со стороны финансово-кредитных учреждений за выдачей кредитов на покупку автомобилей, в том числе с заключением сделок с автосалонами;

- предоставление сведений сотрудникам ГИБДД, занимающимся регистрацией автомобилей, с целью предупреждения оформления сделок купли-продажи автотранспортных средств, приобретенных в кредит, находящихся, по сути, в залоге у банка;

- создание информационных площадок по обсуждению проблем, связанных с борьбой в сфере мошенничеств с автокредитами, с привлечением научных, практических работников правоохранительных органов и сотрудников финансово-кредитных учреждений.

Предлагаемые меры в настоящий момент имеют правовые и технические барьеры, однако взаимодействие между финансово-кредитными учреждениями и правоохранительными органами с целью предупреждения мошеннических посягательств в области кредитования является основополагающим.

1. Аванесов Г.А. Криминология: учебник 2-е изд, перераб. и доп. М., 1984. 500 с.

2. Бурлаков В.Н. Криминология: учебное пособие. Изд-во Питер, 2013. 304 с.

3. Велиев Я.П. Способы совершения мошенничеств при купле-продаже автотранспорта и первоначальные действия сотрудников полиции ОВД по раскрытию данных преступлений // Вестник Дальневосточного юридического института МВД России. 2019. № 2 (47). С. 122.

4. Ганченко О.И. Предупреждение мошенничества в сфере кредитования покупки транспортных средств: учебное пособие. М.: ДГСК МВД России, 2011. 49 с.

5. Дело № 1-145/2019 от 3 июля 2019 г. [Электронный ресурс] // Архив Можайского городского суда Московской области. URL: <https://sudact.ru> (дата обращения: 03.03.2020).

6. Дело № 1-465/2019 от 30 августа 2019 г. [Электронный ресурс] // Архив Индустриального районного суда г. Ижевска (Удмуртская Республика). URL: <https://sudact.ru> (дата обращения: 12.03.2020).

7. Кудрявцев В.В., Эминов В.Е. Криминология. М.: Юрист, 1997. 512 с.

8. Леонова И.В. Рынок автокредитования как элемент экономического развития // Инновационная экономика: материалы V Междунар. науч. конф. (г. Казань, май 2018 г.). Казань: Молодой ученый, 2018. С. 1–7. URL: <https://moluch.ru/conf/econ/archive/295/14198> (дата обращения: 04.03.2020).

9. Статистические данные аналитического агентства «АВТОСТАТ» [Электронный ресурс]. URL: <https://www.autostat.ru> (дата обращения: 02.03.2020).

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

*Екимцев Сергей Валерьевич,
старший преподаватель кафедры
оперативно-розыскной деятельности ОВД;*

*Филатьева Ирина Владимировна,
курсант 302 учебной группы
факультета подготовки следователей*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027, г. Орел, ул. Игнатова, д. 2*

В настоящей статье рассматривается деятельность оперативных подразделений органов внутренних дел и использование их результатов в уголовном судопроизводстве, а так же правовые проблемы, возникающие для сведений приобщение к уголовному делу.

Ключевые слова: *результаты оперативно-розыскной деятельности, оперативные подразделения, оперативно-розыскная деятельность, оперативно-розыскные мероприятия, доказательства.*

В последнее время законодатель более подробно прописал познавательную деятельность, которая находится вне уголовного производства, но имеет определенную связь с установлением правонарушения. В целом, теория доказательных правил в главах 10 и 11 Уголовно-процессуального кодекса Российской Федерации является важной частью процессуальной науки.

Доказательства являются неотъемлемой частью уголовного процесса, без которого невозможно решить дело и добиться справедливости. Понятие и сущность превращения результатов частной детективной, административной и оперативно-розыскной деятельности в доказательства уголовного судопроизводства, а также их использование при предварительном расследовании преступлений требует серьезного научного исследования и соответствующего законодательного регулирования в Уголовно-процессуальном кодексе Российской Федерации. Принимая это во внимание можно говорить о том, что тема, выбранная

для конференции, важна и актуальна для теории уголовного судопроизводства, законодательства и практики расследования преступлений.

Рассматривая подробно такое понятие как «доказательство» необходимо провести его сопоставление с таким явлением как использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве.

Оперативно-розыскная деятельность – это самостоятельная правоприменительная деятельность, которая осуществляется специально уполномоченными на то органами самостоятельно и с применением ими определенных правовых средств для выполнения задач и достижения целей, поставленных перед ними. Согласно Федеральному закону от 12 августа 1995 г. № 144 ФЗ «Об оперативно-розыскной деятельности», оперативно-розыскная деятельность – деятельность, осуществляемая гласно или негласно уполномоченными на то органами в соответствии с ФЗ, выполняющими оперативно-розыскные мероприятия в пределах данной им компетенции в целях защиты прав и законных интересов граждан, обеспечения безопасности государства и общества от противоправных посягательств.

Проблема использования результатов оперативно-розыскной деятельности в доказательстве уголовного процесса является одной из наиболее актуальных в современном уголовном судопроизводстве. Консенсус по этому вопросу отсутствует ни в процессуальной доктрине, ни в правоприменительной практике.

Учитывая данный вопрос, необходимо отметить, что имеются определённые различия между оперативно-розыскной деятельностью и уголовно-процессуальной правом. Юридическая практика говорит о том, что нельзя приравнивать результаты ОРД и доказательства, этот же факт закреплён в Уголовно-процессуальном кодексе Российской Федерации.

Е.А. Доля отмечает, что несоответствие ОРД и результатов доказывания обусловлено различием в его правовой природе, что объективно определяет цель и допустимые пределы его использования [1].

Первоначально результаты ОРД нельзя признать соответствующими нормам процессуальных доказательств, так как их получение происходит не надлежащим образом. Часть 1 статьи 86 Уголовно-процессуального кодекса Российской Федерации содержит в себе перечень субъектов, которые имеют право на сбор доказательств, и он является исчерпывающий. В этом перечне нет такого субъекта как оперативный сотрудник. Но есть один момент, сотрудники полиции, которые имеют право осуществлять оперативно-розыскные мероприятия, а так же руководители данных лиц имеют право предоставлять предметы, документы которые в последующем будут включены в уголовное дело как вещественное доказательство.

Процесс доказательства включает в себя несколько шагов. Первый это сбор, потом проверка и последний оценка доказательств. После прохождения всех этих стадий, доказательства используются для расследования преступлений. Если рассматривать первый этап процесса доказывания, то речь идет о первичном производстве следственных действий. При проведении оперативно-розыскной деятельности будут рассмотрены доказательства и результаты, полученные сотрудниками в соответствии с Федеральным законом «Об ОРД» сведе-

ний о преступлении и лицах которые скрываются от следственных или судебных органов (статья 5, статья 36.1 Уголовного кодекса Российской Федерации).

Сам по себе результат ОРД не является доказательством. Он не может быть использован непосредственно для доказательства преступления в целом и лица, совершившего преступление в частности, так как процедура их получения отличается от процедуры получения доказательств в уголовном процессе [2]. Например, бывают случаи, когда лицо оказывает конфиденциальную помощь органам, осуществляющим ОРД, в процессе производства ОРМ, при условии личного соблюдения обстоятельств, доказанных в уголовном деле. Сведения, полученная оперативным сотрудником, информация об этом лице и его участии в инциденте, должны быть переданы следователям, которые будут проводить в отношении этого человека допрос, для того чтобы установить обстоятельства, связанные с этим делом. В этом случае доказательством является не информация, полученная полицией, а показания, записанные во время допроса.

Для того чтобы материалы которые были получены в процессе ОРД преобразовались в доказательства они должны пройти несколько стадий. Для представления непроизводственной информации в уголовный процесс необходимо провести расследование, чтобы субъект процессуальной деятельности мог узнать о фактах и обстоятельствах, связанных с делом, и в той или иной форме соответствовать Уголовно-процессуальному кодексу. Чтобы выступать, как доказательства результаты ОРД должны содержать: сведения, важные для определения обстоятельств, требующих доказательства; сведения о происхождении предполагаемого доказательства или предмета, который может стать доказательством, а также данные, позволяющие проверить процессуальные условия доказательства, сформированного на его основе.

Конституция Российской Федерации гласит, что результаты оперативно-розыскной деятельности не являются доказательствами, а имеют силу только как информация об источниках этих фактов и могут быть доказаны только после соответствующего процессуального оформления, в порядке установленном УПК РФ. Опять же только при том условии, если эти сведения получены в соответствии с требованиями Федерального закона № 144 «Об оперативно-розыскной деятельности».

Конечно, роль оперативных сотрудников и их результаты очень важны. Этот факт проявляется во взаимодействии с другими органами при проведении предварительного расследования.

Объектом обжалования адвокатами определенных действий все чаще становятся законность и обоснованность установления сотрудниками оперативно-розыскных подразделений делопроизводства, а значит, законность и обоснованность возбуждения уголовных дел по данным, полученным при оперативно-розыском мероприятии. В данном случае есть определенные ошибки, которые в частности касаются правовой природы:

1) оперативно-розыскная деятельность осуществляется без оснований, указанных в подпунктах 1-6 пункта 2 статьи 7 Федерального закона «Об оперативно-розыскной деятельности»;

2) сотрудники оперативных подразделений имеют право проводить ОРМ только с дачи согласия на это определенного лица. Многие по своей ошибке получают согласие от должностных лиц, которые не имеют полномочий на это;

3) правильное оформление документов и иных процессуальных актов является одной из главных составляющих при выполнении ОРД. Исходя из этого многие уполномоченные сотрудники, заполняя и составляя процессуальные документы, делают это неправильно, и «уходят» от действующего законодательства (в большинстве случаев это происходит из-за неграмотности самих оперативных сотрудников);

4) несвоевременное уведомление суда в случае крайней необходимости;

5) многие сотрудники используют в своей деятельности ОРМ которые строго не определены статьёй 6 ФЗ «Об ОРД». А, как нам известно, инструментарий, которым владеет оперативный сотрудник, является исчерпывающим и строго регламентирован законодательством;

6) несоответствие проведения ОРМ в отношении определенных категорий преступлений. Например, оперативным сотрудникам необходимо при прослушивании телефонных переговоров учитывать, что данное ОРМ проводится только по преступлениям тяжким и особо тяжким. Ссылаясь на данный факт, многие адвокаты подают в суд и обжалуют действия оперуполномоченных;

7) несоответствие между фактическим содержанием ОРМ и его описанием в соответствующем акте (протоколе).

В большинстве случаев все эти ошибки случаются по вине оперуполномоченных лиц, осуществляющих оперативно-розыскную деятельность в пределах своих полномочий. Для того чтобы предотвратить их, необходимо повышать правовой уровень грамотности сотрудников и периодически проводить проверки правильности выполнения ими своих профессиональных навыков.

Таким образом, результаты оперативно-розыскной деятельности не могут выступать как доказательство. Этот факт объясняется правовой природой этих результатов, а также их нельзя отождествлять с доказательствами, предусмотренными УПК РФ. Важно повысить качество доказательной базы. В то же время для оперативно-розыскного органа важно соблюдать порядок представления результатов ОРД. Если имеются достаточные данные, свидетельствующие о наличии признаков преступления, лицо, осуществляющее ОРД, представляет результаты ОРМ в орган, ответственный за уголовное расследование, а именно – следователю, дознавателю, суду для приобщения их к делу.

1. Доля Е.А. Результатам оперативно-розыскной деятельности нельзя придавать статус доказательств в уголовном процессе // Рос. юстиция. 2007. № 6. С. 39.

2. Макаров А.В., Фирсов О.В. Особенности использования результатов оперативно-розыскной деятельности в процессе доказывания по уголовным делам // Рос. следователь. 2012. № 8.

НЕКОТОРЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ «МОБИЛЬНЫХ» МОШЕННИЧЕСТВ, СОВЕРШАЕМЫХ ОСУЖДЕННЫМИ В ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

*Косарев Кирилл Викторович,
начальник 2-го отдела Управления уголовного розыска
УМВД России по Орловской области*

302004, г. Орел, ул. Русанова, д. 43а

В статье рассматриваются вопросы раскрытия хищений с использованием средств сотовой связи, совершаемых осужденными в исправительных учреждениях. Автором приводятся способы осуществления преступного замысла фигурантами для обмана абонентов сотовой связи.

Ключевые слова: *мошенничество, осужденный, денежные средства, перевод денежных средств, мобильные телефоны.*

В настоящее время беспроводная связь, подвижная связь, системы так называемой «сотовой» связи распространились по всему миру. Услугами средств мобильной связи пользуется подавляющее число населения планеты. В настоящее время в мире насчитывается около 4 млрд абонентов (абонент – пользователь услуг телефонной связи, с которым заключен договор об оказании услуг телефонной связи при выделении для этих целей абонентского номера или уникального кода идентификации) [1], а в России около 250 млн, что почти вдвое превышает численность населения страны.

Беспроводная связь именуется «сотовой», так как территория ее обслуживания (город, район, область, государство, континент) представляет собой разное сочетание базовых станций, каждая из которых охватывает сегмент под углом около 120°, что в совокупности и напоминает строение пчелиных шестиугольных сот.

В соответствии с законодательством Российской Федерации такая связь имеет наименование подвижной связи, но вместе с тем в настоящее время активно используются такие ее названия как «мобильная связь» или, как уже отмечалось выше, «сотовая связь». В настоящем исследовании мы будем использовать указанные выше термины.

Необходимо отметить, что специфика пребывания лиц в местах лишения свободы предопределила крайне высокую степень востребованности услуг сотовой связи в исправительных учреждениях уголовно-исполнительной системы.

Несмотря на режимные ограничения средства мобильной связи имеют практически неограниченное хождение в исправительных учреждениях. Практика показала, что, несмотря на усилия администраций исправительных учреждений, и оперативных подразделений, ограничить использование средств сотовой связи в местах лишения свободы режимно-заградительными, оперативно-поисковыми и дисциплинарными мерами не удается до настоящего времени.

Способы доставки мобильных телефонов и комплектующих довольно разнообразны, их проносят сотрудники исправительного учреждения, лица, прибывающие на свидания, сотрудники правоохранительных органов, адвокаты; пересылают в посылках, бандеролях передачах; перебрасывают через основное заграждение. Существуют менее традиционные способы доставки средств связи (сбрасывание с квадрокоптеров, пронос при помощи кошек, которые проживают на территории исправительного учреждения и т.д.). Выяснить, каким способом мобильные телефоны попадают в исправительное учреждение, выявить каналы поступления средств связи остается трудной задачей для представителей администрации исправительного учреждения. Осужденные (заклученные) очень редко сообщают информацию о том, как они получают телефонные аппараты, кто их им передает. Это вызвано тем, что с точки зрения «тюремной этики» совершение преступления не осуждается другими осужденными, а иногда и приветствуется. А рассказ о способе получения телефона, указание на тех, кто их проносит (на тюремном жаргоне – «сдать дорогу») жестоко карается другими осужденными. Так как по этим «дорогам» в исправительное учреждение попадают не только телефоны, но и продукты питания, денежные средства, наркотики и иные предметы, необходимые для «нормальной» жизнедеятельности осужденных.

С помощью мобильных телефонов производится координация и управление незаконным оборотом наркотических средств, в том числе поставки наркотиков в исправительные учреждения, осуществляется давления на свидетелей, готовятся и реализуются мероприятия по противодействию следствию, организуется противоправная деятельность подельников, находящихся на свободе и многие другие противоправные действия.

Отмечается лавинообразное увеличение вала фактов так называемого «телефонного или мобильного мошенничества», при которых задействуются средства телекоммуникаций, находящиеся на территории исправительного учреждения и задействуемые для мошеннических действий.

Данный вид правонарушений возник вскоре после массового распространения мобильных телефонов. Преступления совершаются, как правило, в соответствии с несколькими устоявшимися схемами, изменяются только некоторые детали. Схемы совершения мошенничеств осужденными с использованием мобильного телефона в местах лишения свободы устоялись и зачастую являются типовыми [1, с. 7].

Происшествие с близким человеком. Мошенник звонит на мобильные или городские абонентские номера легитимным пользователям сотовых сетей в порядке возрастания или убывания номеров. В случае ответа абонента он представляется родственником или знакомым и, в зависимости от ситуации, с различной степенью эмоциональности сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (совершение ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений).

После этого телефон передается якобы сотруднику полиции, который уверенно сообщает, что он может решить проблему, не регистрируя преступление или путем прекращения действий по возбуждению уголовного дела за вознаграждение. Сумма в зависимости от ситуации, эмоционального состояния и образовательного уровня потерпевшего может составлять от 10 до 500 тысяч рублей.

В функционировании схемы может задействоваться несколько человек. Звонящий может находиться как в исправительном учреждении, так и на свободе, соединяясь с лицом, содержащимся в исправительной колонии посредством конференцсвязи.

Если жертва преступления поверила преступникам, то предлагается привезти указанную сумму. При этом звонящий называет адрес, куда нужно подъехать с деньгами, или узнает адрес потерпевшего. В большинстве случаев мошенники предлагают снять недостающую сумму в банке и сопровождают потерпевшего. Как правило, мошенники оказывают на него давление, стремятся ограничить время на принятие решения, не дать опомниться или усомниться в правдивости ситуации, поэтому ими навязывается непрерывный разговор с потерпевшим непосредственно до момента получения денег. Для передачи им денежных средств преступники могут изобрести и иные, более оригинальные мотивы [2, с. 60].

В марте 2018 г. сотрудниками МВД России проверялась информация о том, что в Московской области действует организованная преступная группа, которая совершает мошеннические действия, используя средства мобильной связи. Проведенными оперативно-розыскными мероприятиями установлено, что данная группа имеет признаки преступного сообщества с четким распределением ролей, наличием «общака» и внешних криминальных связей, координация деятельности данной группы осуществляется неустановленным гражданином, который отбывает наказание в исправительной колонии.

Противоправные действия реализовывались по следующей схеме: один из участников группы осуществлял звонки на прямые мобильные телефоны граждан и беседовал с ними на общие темы, пытаясь установить доверительные отношения. Беседа продолжалась до тех пор, пока потенциальные потерпевшие не признавали в нем кого-то из своих знакомых. Затем на правах старого знакомого участник группы просил одолжить ему денежные средства на различные нужды (лечение ребенка, взятка на поступление в образовательную организацию, покупка квартиры/машины). Но основная цель запрашиваемых денежных средств – попытка решения проблем с правоохранительными органами. Средний размер долга мог составлять до 200 тысяч рублей.

Деньги мошенники обещали вернуть в максимально короткие сроки (через неделю). Поскольку в настоящее время собеседник был занят либо находился в отъезде, денежные средства потерпевшими переводились посредством платежной системы «Вестерн Юнион» в один из банков г. Раменское Московской области. Денежные средства получали другие члены преступной группы и передавали сестре ее лидера. Она положила деньги на сберегательную книжку, оформленную на ее подлинные регистрационные данные, и периодически переводила некоторые суммы в одну из исправительных колоний для нужд содержащихся там осужденных.

В ходе комплексного использования сил, форм и методов оперативно-розыскной деятельности все участники преступной группы были установлены, противоправная деятельность была задокументирована, а также собраны исчерпывающие доказательства причастности участников группы к совершению данных преступлений.

По данному факту возбуждено уголовное дело по признакам состава преступления, предусмотренного частью 4 статьи 159 Уголовного кодекса Российской Федерации. Впоследствии пятеро членов преступной группы задержаны и допрошены в качестве подозреваемых, в том числе и лидер и организатор группы, отбывающий наказание в одной из исправительных колоний, который осуществлял звонки потерпевшим, планировал действия подельников и давал сообщникам указания о получении и хранении денежных средств. В процессе оперативно-розыскных мероприятий и следственных действий изъято 580 тысяч рублей. В ходе допросов подозреваемые признали свою вину полностью и сообщили информацию о лицах, причастных к совершению данных преступлений. Установлены и процессуально закреплены более 50 эпизодов противоправной деятельности участников группы, проведены необходимые следственные действия. Лица, виновные в совершении указанных преступлений, привлечены к уголовной ответственности [3, с. 715].

Победа в лотерее. В связи с проведением всевозможных рекламных акций, лотерей и розыгрышей мошенники часто используют их для прикрытия противоправной деятельности. Мошенники реализуют следующую схему: рассылают на мобильные телефоны граждан SMS о выигрыше ценного приза. Это может быть телефон, ноутбук или автомобиль. При этом доводится информация о том, что для получения приза необходимо в ближайшее время перезвонить по указанному контактному номеру.

Перезвонившему лицу отвечает сотрудник «призового отдела» и объясняет условия акции, устанавливает с ним доверительные отношения, убеждая в легитимности акции, и доводит алгоритм дальнейших действий. При этом выигрыш приза выступает не только в роли приманки, но является поводом затребовать перечисления крупных денежных средств.

Для уточнения всех деталей потенциальному потерпевшему могут предложить посетить определенный сайт и ознакомиться с условиями акции, а также позвонить по одному из указанных телефонных номеров.

Во время разговора мошенники сообщают о том, что надо выполнить необходимые формальности, к примеру: получить восьмизначный код, дающий право на получение приза, уплатить госпошину, для чего необходимо посредством платежных терминалов перечислить на счет мобильного телефона гражданина сумму, составляющую 1 % от стоимости выигрыша; под руководством специалиста информационно-справочной службы набрать определенную комбинацию цифр и символов якобы для проверки получения «кода регистрации». При этом злоумышленники уверяют, что денежные средства, потраченные на прохождение стандартной процедуры регистрации, остаются на счете абонента и могут быть использованы по его усмотрению. Возможно также перечисление денежных средств на указанный злоумышленниками электронный кошелек.

В 2017 году осужденный П., отбывающий наказание в исправительном учреждении УФСИН России по Самарской области, подобным способом получил сумму денег в размере 7564 рублей.

Сообщение из банка. В связи с бурным ростом количества и качества услуг дистанционного банковского обслуживания граждан произошел лавинообразный рост владельцев банковских карт, которые в свою очередь активно ис-

пользуются в различных сферах общественной жизни (при оплате услуг, покупках, в поездках и т.д.). Для удобства пользователей банки подключают пользователям карт услугу так называемого «мобильного банка», позволяющую контролировать операции, совершаемые посредством банковской карты в режиме реального времени, привязывая банковскую карту к абонентскому номеру ее владельца. Злоумышленники рассылают на мобильные телефоны граждан SMS о том, что их банковская карта заблокирована либо приостановлена, либо о том, что ими успешно осуществлен перевод, которого на самом деле не было. Для уточнения информации потенциальному потерпевшему предлагается перезвонить по указанному телефону службы безопасности. В случае если гражданин перезванивает по указанному в сообщении телефонному номеру, мнимый сотрудник службы безопасности банка выяснит, в каком банке им была оформлена карта, его данные, а затем предложит подойти к ближайшему банкомату и под его руководством разблокировать карту путем набора комбинации цифр, который в свою очередь является кодом мобильного перевода в системе электронных платежей. При этом денежные средства со счета жертвы переводятся на счет злоумышленника или его сообщников.

В апреле 2017 г. в одну из исправительных колоний УФСИН России по Самарской области для отбывания наказания был направлен мужчина, который в 2015 г., отбывая наказание за преступления в сфере незаконного оборота наркотиков, совершил ряд «телефонных» мошенничеств. Осужденный наугад набирал номер телефона и отправлял на него сообщение о блокировке банковской карты. Когда абонент перезванивал мошеннику, последний представлялся сотрудником банка, рассказывал о, якобы, случившейся хакерской атаке и убеждал свою жертву зарегистрироваться в мобильном банке. Получив таким образом доступ к деньгам на чужих счетах, арестант перевел больше 117 тысяч рублей на карту своей жены и приятелей. Полгода спустя по подобной схеме он обманул еще одного абонента, причинив материальный ущерб в размере 30 тысяч рублей.

Примерно в то же время другой осужденный, отбывающий наказание в исправительной колонии УФСИН России по Курганской области, совершил ряд «мобильных» мошенничеств в отношении граждан, проживающих в Кировской области. В течение полугода осужденный обзванивал абонентов, представлялся сотрудником банка, а затем убеждал перевести деньги с их карт на нужные счета – якобы для большей сохранности денег. Неизвестно сколько человек обзвонил мошенник, но четверо поверили этой формулировке и перевели на счет мошенника-осужденного 230 тысяч рублей.

Осужденный из исправительной колонии Копейска (ГУФСИН России по Челябинской области) действовал тоньше. Он рассылал SMS с текстом: «С вашего счета списана определенная сумма. По вопросу списания просим обратиться по указанному телефону». Когда абоненты перезванивали мошеннику, он представлялся банковским специалистом по безопасности. Дальше в ход шла отработанная «легенда»: в банковской программе произошел сбой, чтобы вернуть деньги, нужно дойти до банкомата и ввести определенную комбинацию цифр. Жертвами мошенника стали 15 человек, которые перевели ему больше 270 тысяч рублей.

Просьба о помощи. Данный вид мошенничества появился одним из первых. Он не позволяет заработать быстро большие суммы денег, но в свою оче-

редь наименее затратен по времени и позволяет сразу обратиться к огромному числу потерпевших. SMS позволяют упростить схему обмана по телефону. При этом используются широко внедряемые компаниями – операторами услуг связи упрощенные схемы перевода денежных средств с одного телефона на другой. Преступники отправляют абонентам на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «папа», «друг» или тому подобные.

В случае согласия оказать помощь родственнику или знакомому жертва преступления пополняет счет мобильного телефона, указанного преступником. Данный вид преступлений характеризуется высоким уровнем латентности ввиду малозначительности ущерба и психологических особенностей потерпевших, не желающих афишировать то, что они поддались на примитивный обман.

Приведем пример. В феврале 2018 г. осужденный В., который отбывал наказание в исправительном учреждении УФСИН России по Московской области, получил в свое распоряжение сотовый телефон, в котором находилась сим-карта с абонентским номером 8-919-***-**-***. С данного номера он отправлял SMS с текстом: «Папа, закинь деньги на этот номер, потом все расскажу». В результате данных мошеннических действий В. завладел денежными средствами в размере 4750 руб.

Ошибочный перевод средств. На мобильный телефон потерпевшего отправляется SMS-сообщения о поступлении через систему электронных платежей денежных средств на его счет. Деньги якобы переводились с задействованием услуги «мобильный перевод» или через терминалы оплаты услуг связи. Сразу после этого потерпевшему поступает звонок или приходит SMS о том, что на его счет ошибочно переведены деньги, деньги просят вернуть обратно тем же «мобильным переводом».

В течение 2017 г. в одной из исправительных колоний УФСИН России по Московской области осужденный К., имея в своем распоряжении мобильный телефон и 15 сим-карт, отправил более 10 000 сообщений с текстом «Поступил платеж 500 руб. Спасибо, что пользуетесь услугами мобильной связи!». После каждого подобного сообщения осужденный отправлял сообщение с текстом «Извините, по ошибке пополнил баланс Вашего мобильного телефона. Переведите на номер 8-900- ***-**-*** 500 руб. Спасибо». В результате подобной мошеннической схемы осужденный смог «заработать» более 70 000 руб.

Набор номера абонента с последующим отключением до соединения. При данном способе мошенничества потенциальная жертва набирает номер, с которого ей звонили, а после этого приходит счет за исходящий звонок, так как у преступника подключен так называемый «корпоративный» тариф, когда владелец сим-карты вправе сам устанавливать стоимость исходящего вызова. Так, в 2014 году осужденный Л., который отбывал наказание в исправительной колонии УФСИН России по Курской области, получил в свое распоряжение сотовый телефон, в котором находилась сим-карта с коммерческим тарифным планом, позволяющим устанавливать цену на входящий звонок абонента. В свободное время осужденный Л. набирал номера абонентов, проживающих в различных регионах России, и до ответа абонента отключался. Некоторые абоненты перезванивали на абонентский номер, с которого звонил осужденный Л. В результате

данных мошеннических действий осужденный Л. обманным путем завладел денежными средствами потерпевших в размере 54 467 руб.

Улучшение работы оператора связи. На мобильный телефон граждан поступают звонки либо направляются SMS от лица сотрудника службы технической поддержки оператора мобильной связи. Обоснованиями этого звонка или SMS могут быть достаточно широкий спектр причин: предложение подключить новую эксклюзивную услугу; перерегистрация во избежание отключения связи из-за технического сбоя; улучшение качества связи; защита от SPAM-рассылки (SPAM – массовая рассылка корреспонденции рекламного характера лицам, не выразившим желания её получать); предложение принять участие в акции от сотового оператора.

На основании изложенного можно сделать вывод, что раскрытие указанной категории преступлений возможно только при тесном взаимодействии должностных лиц органов внутренних дел и уголовно-исполнительной системы. При этом стоит отметить, что для оперативного раскрытия «мобильных» мошенничеств очень важно привлечение специальных подразделений Министерства внутренних дел и Федеральной службы исполнения наказаний, обладающих установленным законом правом и имеющих специальное оборудование для проведения всего спектра процессуальных, следственных, оперативных, технических, тактических и иных мероприятий.

1. О порядке оказания услуг телефонной связи: постановление Правительства Рос. Федерации от 9 декабря 2014 г. № 1342 // Собр. законодательства Рос. Федерации. 2014. № 51, ст. 7431.

РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ (НЕГЛАСНОСТИ): ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ

*Малышев Сергей Яковлевич,
кандидат юридических наук, доцент, доцент кафедры
финансов, денежного обращения и экономической безопасности*

*Уфимский государственный авиационный технический университет
450006, г. Уфа, ул. Карла Маркса, д. 12*

*Миняшева Гульнара Ибрагимовна,
кандидат юридических наук,
доцент кафедры оперативно-разыскной деятельности ОВД*

*Уфимский юридический институт МВД России
450103, Республика Башкортостан, г. Уфа, ул. Муксинова, д. 2*

В статье рассмотрены основные вопросы осуществления режима конфиденциальности информации (негласности) со стороны сотрудников службы безопасности компании и правоохранительных органов при решении ими кон-

кретных задач. Исследована содержательная сторона условий конфиденциальности (негласности), где для объективности и полноты исследования авторы использовали научный метод сравнения с их прямой противоположностью – условиями гласности.

Ключевые слова: *конфиденциальность информации, условия конфиденциальности, негласность, обязательные элементы мероприятия, конспирация.*

Работа с любого рода информацией предполагает ее сбор, анализ, оценку, учет, использование, хранение и уничтожение, которая может осуществляться как в условиях гласности, так и в условиях конфиденциальности (негласности). Работа такого рода с информацией осуществляется путем проведения определенных действий (мероприятий, в том числе оперативно-розыскных мероприятий) со стороны субъекта (руководителя компании, сотрудника службы безопасности или правоохранительных органов). Если мы говорим об условиях гласности, то такие действия (мероприятия, в том числе оперативно-розыскные мероприятия) со стороны субъекта должны носить открытый, гласный характер. А если мы говорим об условиях конфиденциальности (негласности), то такие действия (мероприятия, в том числе оперативно-розыскные мероприятия) со стороны субъекта должны носить закрытый, конфиденциальный (негласный, тайный) характер, которые обеспечиваются путем осуществления режима конфиденциальности информации (негласности). Режим конфиденциальности информации (негласности) осуществляется для обеспечения коммерческой, служебной и иной тайны. Так, в соответствии со статьей 3 Федерального закона «О коммерческой тайне» [1] под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Для объективности и полноты исследования условий конфиденциальности (негласности) нам необходимо использовать научный метод сравнения этих условий с прямой их противоположностью – условиями гласности.

Условия гласности характеризуются следующими двумя существенными признаками, которые определяются их причинно-следственной связью между собой:

- условия, при которых заинтересованный в них субъект сознательно не применяет меры конфиденциальности (негласности) для сохранения в тайне от посторонних третьих лиц содержание (сущность) проводимых и (или) проведенных мероприятий (действий), в том числе и полученный благодаря им результат;
- посторонние третьи лица знают или потенциально могут знать о содержании (сущности) проводимых и (или) проведенных мероприятиях (действиях), а также полученный благодаря им результат.

В связи с этим, справедливо возникают следующие вопросы:

- что включает в себя содержание (сущность) проводимых и (или) проведенных мероприятий (действий), в том числе и полученный благодаря им результат;

– к чему конкретно субъект сознательно не применяет меры конфиденциальности (негласности)?

Для ответа на поставленные вопросы нам необходимо выяснить содержательную сторону действий (мероприятий, в том числе оперативно-розыскных мероприятий) осуществляемых со стороны субъекта как в условиях гласности, так и в условиях конфиденциальности (негласности), их структурное построение, которое для рассматриваемых условий имеет общий и закономерный характер. В этих целях используем структуру обязательных элементов оперативно-розыскного мероприятия, которую предложил профессор В.Г. Бобров, данная структура имеет значение для любого рода мероприятий, действий, имеющих целенаправленный характер, в том числе для обеспечения режима конфиденциальности информации (негласности). Так, среди обязательных элементов оперативно-розыскного мероприятия В.Г. Бобров выделял следующие составные части (элементы):

- функциональная сторона;
- объект;
- оперативно-тактическая задача (цель);
- субъект;
- приемы организационного характера, интегрирующие вышеназванные элементы оперативно-розыскного мероприятия в единую систему действий, направленных на решение оперативно-тактических задач язык [2].

Важно отметить, что в условиях гласности ни к одному из вышеуказанных элементов со стороны сотрудников службы безопасности компании или правоохранительных органов не должны применяться меры конфиденциальности (негласности).

Условия негласности проведения мероприятий по защите конфиденциальности информации (в том числе оперативно-розыскные мероприятия) нельзя рассматривать в отрыве от гласных, так как последние являются прямой противоположностью первых. Однако важно отметить, что указанные условия организации и проведения мероприятий имеют следующее объединяющее их обстоятельство – они являются результатом сознательных волевых усилий сотрудника службы безопасности компании (сотрудника оперативного подразделения правоохранительных органов) с целью создания благоприятных условий организации и проведения мероприятий (гласных или негласных). При осуществлении гласного мероприятия сотрудник службы безопасности (сотрудник оперативного подразделения правоохранительных органов) сознательно не применяет мер негласности для сохранения в тайне содержания проводимого мероприятия (действия). Таким образом, гласное мероприятие, действие (в том числе оперативно-розыскное мероприятие) – это мероприятие (действие), при организации и осуществлении которого сотрудник службы безопасности компании (сотрудник оперативного подразделения правоохранительных органов) сознательно не применяет мер негласности для сохранения его в тайне, и в связи с этим заинтересованным и иным лицам потенциально может стать известно о содержании проводимого или проведенного мероприятия, действия.

Условия конфиденциальности (негласности) характеризуются следующими двумя существенными признаками, которые определяются их причинно-следственной связью между ними:

- условия, при которых заинтересованный в них субъект сознательно и своевременно применяет достаточное количество мер конфиденциальности (негласности) для сохранения в тайне от посторонних третьих лиц содержание (сущность) проводимых и (или) проведенных мероприятий (действий), в том числе и полученный благодаря им результат;

- посторонние третьи лица ни при каких обстоятельствах не должны знать о содержании (сущности) проводимых и (или) проведенных мероприятиях (действиях), а также полученный благодаря им результат, за исключением случаев предусмотренных законодательством Российской Федерации.

Режим конфиденциальности информации (негласности) осуществляется тогда, когда заинтересованный в тайне субъект сознательно и своевременно применяет достаточное количество мер конфиденциальности (негласности) для сохранения в тайне от посторонних третьих лиц содержание (сущность) проводимых и (или) проведенных мероприятий (действий), в том числе и полученный благодаря им результат.

Из вышесказанного можно сделать вывод, что условия гласности, конфиденциальности (негласности) зависят от волевых усилий сотрудников службы безопасности компании, правоохранительных органов и специальных подразделений по сознательному неприменению или применению мер негласности для сохранения в тайне содержание (сущность) проводимых, проведенных мероприятий, действий.

Условия конфиденциальности (негласности) по своей природе являются неоднородными, так как при осуществлении режима конфиденциальности информации меры по ее охране со стороны заинтересованных субъектов могут применяться лишь к отдельным указанным выше обязательным структурным элементам проводимых мероприятий, действий (в том числе оперативно-розыскных мероприятий). В качестве примера обратимся к правовым положениям Федерального закона «Об оперативно-розыскной деятельности» [3], где определено, что оперативно-розыскная деятельность является видом деятельности, осуществляемая гласно и негласно и в соответствии с конституционными принципами, один из которых является принцип конспирации.

В связи с этим, справедливо возникает вопрос о соотношении понятий «негласность» и «конспирация» между собой при обеспечении режима конфиденциальности информации. Изначально можно предположить, что содержание данных понятий зависит от качественной характеристики существующей системной связи между применяемыми мерами конфиденциальности (негласности) к защите информации о сущности проводимых мероприятий, действий (в том числе оперативно-розыскных мероприятий) и конечным результатом применения таких мер, т. е. скрытность, негласность, тайна в отношении обязательных структурных элементов указанных мероприятий, действий (субъекта, объекта, функциональной стороны, оперативно-тактической задачи (цели), приемов организационного характера). Иначе говоря, вопрос здесь необходимо поставить следующим образом: при обеспечении режима конфиденциальности информа-

ции (негласности) какие обязательные структурные элементы мероприятия, действия (в том числе оперативно-розыскного мероприятия) должны сохраняться в тайне от посторонних третьих лиц?

Необходимо отметить, что при осуществлении конфиденциальных (негласных) мероприятий, действий (в том числе оперативно-розыскных мероприятий) их субъект может сознательно и своевременно применить достаточное количество мер конфиденциальности (негласности) для сохранения в тайне от посторонних третьих лиц как всего содержания проводимых и (или) проведенных мероприятий (действий), так и лишь их сущностной стороны, в том числе и полученный благодаря им результат. Поясним высказанное нами положение следующим образом.

При организации и проведении мероприятий, действий (в том числе оперативно-розыскных мероприятий) сотрудник службы безопасности компании или правоохранительных органов создает определенное информационное поле, которое в условиях конфиденциальности (негласности) должно быть закрыто и недоступно для посторонних лиц. Если указанные мероприятия, действия проводятся на конспиративной основе, то данное информационное поле закрывается полностью от посторонних лиц, при этом применяются меры конфиденциальности (негласности) для зашифровки (легендирования) всех указанных выше обязательных структурных элементов проводимого мероприятия, действия. Легендирование применяется для зашифровки личности субъекта проводимого мероприятия (оперативно-розыскного мероприятия), которое «автоматически» приводит к зашифровке всех обязательных структурных элементов данного мероприятия, действия. Легендирование – это обязательное условие для проведения мероприятия, действия (оперативно-розыскного мероприятия) на конспиративной основе в обстоятельствах, когда такие мероприятия, действия с нашей стороны непосредственно воспринимаются посторонними третьими лицами. Если такого непосредственного восприятия со стороны посторонних третьих лиц отсутствует, то конспирация может быть осуществлена без применения легендирования личности субъекта мероприятия, действия (оперативно-розыскного мероприятия), так как сами условия проведения мероприятия способствуют зашифровке личности указанного субъекта. Сотрудники службы безопасности компании в своей практической деятельности при осуществлении конкурентной разведки или борьбы с промышленным шпионажем, а также при применении мер по охране конфиденциальности информации в целях обеспечения коммерческой тайны должны знать и на практике применять методы ведения конфиденциальной (негласной) работы.

Таким образом, при конспирации сам факт проведения сотрудниками службы безопасности компании или правоохранительных органов конфиденциального (негласного) мероприятия, действия (оперативно-розыскного мероприятия) не должен стать известным посторонним третьим лицам. Меры по охране конфиденциальности информации (негласности) при проведении мероприятий (оперативно-розыскных мероприятий) на конспиративной основе применяются для зашифровки всех обязательных структурных элементов указанных мероприятий, действий (см. схему № 1).

Схема № 1
Условия конфиденциальности (негласности) проведения
мероприятия, действия на конспиративной основе



Однако в практической деятельности сотрудников службы безопасности компании и правоохранительных органов при осуществлении ими мероприятий, действий, в том числе оперативно-розыскных мероприятий в условиях конфиденциальности (негласности) могут складываться и иного рода обстоятельства, когда указанные мероприятия, действия проводятся не на конспиративной основе. В этом случае сотрудником службы безопасности или правоохранительных органов применяются меры по охране конфиденциальности информации (негласности) для закрытия от посторонних третьих лиц сведений, характеризующих только лишь сущность проводимого мероприятия, действия. Информация о субъекте и объекте проводимого мероприятия, действия, в том числе оперативно-розыскного мероприятия, при этом не скрывается от посторонних третьих лиц и если последние предпримут со своей стороны какие-либо волевые усилия с тем, чтобы узнать интересующую их информацию о субъекте и объекте этих мероприятий, действий, то она им станет известна.

Когда сотрудник службы безопасности компании или оперативный сотрудник применяет меры конфиденциальности (негласности) для зашифровки только сущности проводимого мероприятия, действия, в том числе негласного оперативно-розыскного мероприятия, т.е. зашифровывается функциональная сторона, оперативно-тактическая задача (цель), приемы организационного характера осуществляемого мероприятия, но не применяются меры конфиденциальности (негласности) для зашифровки личности субъекта и не скрывается объект его оперативного интереса, то в этой ситуации мероприятие, действие (оперативно-розыскное мероприятие) проводится не на конспиративной основе (см. схему № 2).

Схема № 2
Условия конфиденциальности (негласности) проведения
мероприятия, действия не на конспиративной основе



В указанной ситуации режим конфиденциальности информации распространяется лишь на сущностную сторону проводимого конфиденциального (не-

гласного) мероприятия, действия, в том числе оперативно-розыскного мероприятия. Такая форма конфиденциальности (негласности) в оперативно-розыскной деятельности ОВД существует, например, при работе оперативного сотрудника с задержанными (арестованными) в условиях изолятора временного содержания, где бетонные стены и установленный режим деятельности изолятора сохраняют в тайне сущность проводимых негласных оперативно-розыскных мероприятий, однако известны их субъект и объект, в отношении которых они проводятся. Кроме того, в оперативно-розыскной практике нередко возникают ситуации, когда при опросе очевидцев на месте преступления отдельные лица просят сотрудника оперативного подразделения отойти в сторонку и сообщают ему оперативно значимую информацию, или сотрудник сам предлагает этому лицу провести негласный его опрос, при этом посторонние лица знают, кто субъект негласного мероприятия и кто является объектом его оперативного интереса, даже могут знать, какое мероприятие проводится, однако суть этого мероприятия сохраняется в тайне.

Потенциальные оппоненты могут возразить, что рассмотренные нами примеры из оперативно-розыскной практики ОВД осуществления негласных оперативно-розыскных мероприятий, проводимых не на конспиративной основе, являются по своей сути гласными. Для аргументации ошибочности таких суждений со стороны оппонентов и утверждения своей научной позиции нам необходимо использовать один из наиболее распространенных методов научного познания – метод сравнения. В данном случае сравним практику органов предварительного расследования с оперативно-розыскной деятельностью ОВД в части, рассматривающей их правовую регламентацию вопроса негласности. Так, в статье 310 Уголовного кодекса Российской Федерации («Разглашение данных предварительного расследования») говорится, что разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия следователя или лица, производящего дознание, несет уголовную ответственность. Таким образом, данной статьей определяются условия «тайны следствия», которые по сути своей являются условиями конфиденциальности (негласности). Этот вывод подтверждает и статья 161 Уголовно-процессуального кодекса Российской Федерации («Недопустимость разглашения данных предварительного расследования»), где определено, что данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя, дознавателя и в том объеме, в каком они признаются возможным. В этом случае следует обратить внимание на понятие «гласность», антонимом которого является понятие «негласность». Следовательно, прежде чем придать гласности результаты следственного действия, первоначально органы предварительного расследования должны создать условия негласности. Однако в рассматриваемой нами ситуации нельзя говорить, что органы предварительного расследования осуществляют свою деятельность на конспиративной основе, т.к. должностные лица не применяют мер негласности для зашифровки своей личности как субъекта следственного действия, а также не скрывается личность объекта его интереса.

Если такая форма негласности существует в практике органов предварительного расследования, которая, в свою очередь, имеет нормативную правовую регламентацию, то почему аналогичная форма не может осуществляться в опе-

ративно-розыскной практике органов внутренних дел и в служебной деятельности сотрудников службы безопасности компании?

Исходя из вышесказанного, можно сделать вывод, что режим конфиденциальности информации (негласности) в различных условиях складывающейся обстановки может быть применен в отношении всего содержания проводимого мероприятия, действия, в том числе оперативно-розыскного мероприятия, где зашифровке подвергаются все обязательные структурные элементы данного мероприятия, действия и тогда мы имеем право говорить о конспирации, а также лишь в отношении отдельных обязательных структурных элементов указанных мероприятий, действий, которые характеризуют их сущностную сторону. Важно отметить, что конспирация – это всегда конфиденциальность (негласность), а конфиденциальность (негласность) – это не всегда конспирация. Содержание понятия «конфиденциальность (негласность)» шире содержательной стороны понятия «конспирация».

Таким образом, сотрудники службы безопасности компании и правоохранительных органов в условиях конфиденциальности (негласности) могут проводить в целях решения стоящих перед ними задач, следующие виды мероприятий, действий, в том числе оперативно-розыскных мероприятий, осуществляемые: на конспиративной основе и не на конспиративной основе.

1. О коммерческой тайне [Электронный ресурс]: Федер. закон Рос. Федерации от 29 июля 2004 г. № 98-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Бобров В.Г. Понятие оперативно-розыскного мероприятия. Основания и условия проведения оперативно-розыскных мероприятий: лекция. М.: Академия управления МВД России, 2003. С. 10.

3. Об оперативно-розыскной деятельности [Электронный ресурс]: Федер. закон Рос. Федерации от 19 августа 1995 г. № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

СИСТЕМНО-СТРУКТУРНЫЙ АНАЛИЗ ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ НА ОБЪЕКТАХ ВОДНОГО ТРАНСПОРТА

*Михайлова Лариса Васильевна,
кандидат юридических наук, доцент,
доцент кафедры оперативно-розыскной деятельности в ОВД*

*Дальневосточный юридический институт
Министерства внутренних дел Российской Федерации
680020, г. Хабаровск, пер. Казарменный, д. 15*

В настоящей статье исследуются философские, криминалистические, оперативно-розыскные аспекты системного подхода по определению структурных элементов оперативно-розыскного обеспечения раскрытия и расследо-

вания транснациональной преступной деятельности на объектах водного транспорта. Рассматриваются условия функционирования объектов водного транспорта, формулируется позиция определяющая структуру транснациональной преступной деятельности на объектах водного транспорта.

Ключевые слова: *система, структура, транснациональная преступная деятельность, объекты водного транспорта, обстановка, оперативно-розыскное обеспечение раскрытия и расследования.*

Роль водного транспорта в экономики Российской Федерации довольно велика. Территория страны омывается водами 14 морей и трех океанов, испещрена многочисленными реками и озерами многие из которых являются судоходными [12]. Это говорит об огромном природном богатстве нашей страны в водных ресурсах и дальнейшем развитии «водной» составляющей в экономики страны. В этой связи востребовано постоянное изучение и устранение негативных факторов, тормозящих его развитие, минимизации криминализации объектов водного транспорта. Экономическая привлекательность водного транспорта, активизировала, и изменили действия транснациональной преступности на данных объектах. Развитие тактических основ оперативно-розыскной практики в настоящее время отстает от усовершенствующейся преступной деятельности. Данные обстоятельства наиболее выражены при осуществлении оперативно-розыскного обеспечения раскрытия и расследования преступлений, совершаемых транснациональными преступными сообществами. Создавшееся положение требует научного осмысления данной проблемы, в том числе и с позиций системного подхода в оперативно-розыскной науке.

Исторически методология каждой науки определялась системным анализом, системным подходом, общая теория систем, а системное понимание мира стало неотъемлемой частью научного мышления. При этом роли систематизации в исследовании придается двоякий подход, связанный с тем, что систематизации применяется лишь как решение одного из этапов научного исследования, либо с помощью нее решается научная задача, приводящая к конечному продукту. Наиболее широко основные научно-исследовательские возможности систематизации выражаются в содействии движению науки или отрасли техники со ступени эмпирического накопления знаний, на уровень теоретического синтеза, системного подхода. Такой подход возможен лишь при условии теоретического осмысления многообразия фактов [4, с. 73].

В общенаучной и специальной литературе представлены различные подходы к категории «система» [1, с. 170–178; 2, с. 5; 5, с. 54–56; 7, с. 12; 10, с. 89–96; 13, с. 23–27]. При этом всеми исследователями отмечается некоторая двойственность данного понятия; во-первых, обозначение объективно существующих феноменов, а во-вторых, метод их изучения и представления, т.е. как субъективная модель реальности. Обобщая точки зрения, изложенные в научных исследованиях к типовым признакам можно отнести:

– совокупность отдельных организованных элементов, обладающая целостностью в своих границах и выступающая по отношению к окружающей среде и иным системам как единое целое;

- определенную структуру;
- наличие характерных отличительных свойств (общность в этих отличиях, только когда они в системе);
- элементы в системе превосходят сумму возможностей составляющих её элементов;
- иерархичность, где каждый элемент может быть как частью системы, так и рассматриваться как сама система. При этом сама система может рассматриваться как элемент некоторой суперсистемы.

Таким образом, можно предположить, что комплекс развивающихся научных положений о системном подходе в оперативно-розыскной деятельности, приобретает общенаучное значение в теории ОРД и не может быть отнесен к какому-либо одному из ее разделов.

В то же время, именно системно-структурный анализ, на наш взгляд, позволяет с наибольшей эффективностью исследовать сложные явления, (к ним, несомненно, следует отнести транснациональную преступную деятельность на объектах водного транспорта) в качестве систем, состоящих из комплекса взаимосвязанных элементов, предполагая, в том числе, и изучение их взаимосвязей.

Центральным по отношению к системному подходу, является понятие «систематизация». Использование в разные времена и в различных контекстах в оперативно-розыскной науке указанного понятия, или других близких понятий («структурно-содержательные элементы», «структурно-содержательные признаки», «сущностные элементы») еще не говорит о существовании и использовании системного подхода в оперативно-розыскной деятельности. В оперативно-розыскной науке, систематизация наиболее часто применялась И.А. Климовым и Г.К. Синиловым, так, в исследованиях посвященных оперативно-розыскной методике, они приходят к выводу, что содержательными элементами методики будет системность и комплексность применения специальных сил, средств и методов в единстве их взаимосвязи с оперативно-розыскной характеристикой преступлений, при применении системы оперативно-розыскных мероприятий [6, с. 11–14].

Оперативно-розыскная наука, как и любая другая, наука активно применяет системные исследования и системный подход с учетом специфики изучаемых ею явлений, конкретных объектов и возможностями своего категориального аппарата. Наиболее используемым инструментом системных исследований, является системно-структурный анализ, под которым предлагаем понимать научный метод познания, представляющий собой последовательность действий по установлению и изучению особенностей строения системы, образующих ее структурных уровней и элементов, а также совокупности существенных системных связей между уровнями и образующими их элементами.

В контексте нашей работы, представляет интерес подход, основанный на наличии существенных связей системного характера между преступлением и его выявлением, раскрытием и расследованием.

Нами обосновывается следующая позиция:

- преступная деятельность и деятельность по выявлению и раскрытию преступлений, рассматриваются не как автономные системы, а как взаимосвязанные системы, образующие симметричные структуры;

- в генезисе и развитии преступной деятельности, ее субъект, побуждаемый мотивом, ставит цели и достигает их путем решения задач, воздействуя на исходные состояния объектов водного транспорта, с помощью средств и действий в определенных условиях;

- закономерность связи возможна только путем действий и движений оперативных подразделений, осуществляющих оперативно-розыскную деятельность по выявлению и раскрытию преступлений.

В современных условиях, процесс оперативно-розыскного обеспечения раскрытия и расследования преступлений, в том числе транснациональных, совершаемых на объектах водного транспорта, как правило, осуществляется в достаточно сложных, а нередко чрезвычайных условиях, ситуациях тактического риска (наглядный пример, расследование подобной преступной деятельности при нападении пиратов на суда плавающие под Российским флагом в открытом море, данные преступления чаще всего носят трансграничный характер, они не могут быть ограничены географическими рамками одной страны, в результате чего, возникает проблема противоречия между нормами уголовного права, конвенцией по морскому праву, и полное отсутствие регламентации организации ОРД при столкновении в территориальном море двух юрисдикций: государства берега и государства флага).

Транснациональная преступная деятельность на объектах водного транспорта имеет определенные особенности. Ее отличает глобальный характер, преступления затрагивают интересы более чем одной страны, разрушительное влияние и воздействие на экономическую систему государств, только групповой характер, активное использование новейших технических средств, многообразием преступных деяний (например, нарушение иммиграционных законов, коррупция, торговля оружием или наркотиками, мошенничество, контрабанда и др.).

Эффективность работы по оперативно-розыскному обеспечению раскрытия и расследования транснациональной преступной деятельности на объектах водного транспорта, зависит от четкой ее организации, где важнейшими элементами, являются изучение и оценка оперативной обстановки. Рассматриваемую обстановку объектов водного транспорта отличает ряд факторов – высокая степень автономности, экстерриториальность, круглосуточный характер работы, быстроменяющийся контингент пассажиров, сосредоточие огромного количества постоянно меняющихся разнообразных материальных ценностей и т.д. [9, с. 97–103].

При изучении и классификации данных условий (факторов), оказывающих влияние на оперативную обстановку на объектах водного транспорта, мы исходили из следующих предпосылок.

Во-первых, учитывая специфику работы объектов водного транспорта, наличие в их составе помимо судов, целой инфраструктуры, обеспечивающей потребности юридических лиц и граждан в перевозках (внутренних и международных), можно утверждать, что оперативные сотрудники должны обладать значительным объемом знаний об указанных факторах, для обеспечения правильной расстановки сил и средств, эффективно противостоять преступности на указанных объектах.

Во-вторых, с течением времени многие из действующих факторов качественно изменяются, одни исчезают, другие появляются, или вновь заявляют о себе прежние, порой более активно.

В-третьих, выделить в полной мере степень влияния конкретного фактора (обстоятельства) в некоторых случаях трудно, так как действуют они комплексно и неодинаково в разные периоды.

Результаты проведенного исследования, а также анализ позиций авторов работ смежного характера [3, с. 6–17; 11, с. 8–9] позволяют предложить следующую классификацию условий, определяющих оперативную обстановку на объектах водного транспорта по степени влияния:

- 1) основные и вспомогательные;
- 2) устойчивые и сезонные.

Условия первой группы охватывают обстоятельства, сохраняющие устойчивую тенденцию влияния на формирование объективных и субъективных предпосылок к совершению преступлений. Основные – круглосуточный цикл работы объектов водного транспорта, сосредоточение на относительно малых территориях значительного количества материальных ценностей, концентрация больших людских потоков, значительная протяженность маршрутов водного транспорта. Вспомогательные – специфическая технология обработки и перевозки различных грузов, географически-территориальное расположение речного и морского бассейна.

Условия второй группы включают обстоятельства, влияющие на временные проявления динамики преступлений. Устойчивые – характеризующие совокупное долговременное воздействие (например, фактор недостаточной информированности лиц, соприкасающихся с объектами водного транспорта), и сезонные – циклически возникающие колебания интенсивности пассажирских и грузовых речных и морских перевозок [8, с. 78–86].

Любое изменение выше перечисленных условий, приводит к изменению оперативной обстановки. Злоумышленники используют данные обстоятельства для активизации преступной деятельности. Перечислены лишь некоторые характеристики обстановки, указывающие на то, что на объектах водного транспорта в части противодействия преступной деятельности транснациональных преступных сообществ очень важна их систематизация, для подготовки логически и системно выдержанных рекомендаций по оперативно-розыскному обеспечению раскрытия и расследования преступлений совершаемых транснациональными преступными сообществами на объектах водного транспорта.

С учетом изложенного, под структурой транснациональной преступной деятельности на объектах водного транспорта, можно понимать совокупность условий и обстоятельств, создаваемых сочетанием элементов состоящих из факторов обстановки, действием лиц совершающих преступления, в том числе в организованной форме, а также действиями оперативных сотрудников по раскрытию транснациональной преступной деятельности.

Таким образом, в качестве элементов структуры транснациональной преступной деятельности на объектах водного транспорта полагаем возможным рассматривать:

- лиц, вовлеченных в транснациональную преступную деятельность и составляющих ее преступлений;
- способы совершения преступлений, совершаемых транснациональными преступными сообществами на объектах водного транспорта;
- обстановка, в которой осуществляется транснациональная преступная деятельность и составляющие ее преступления;
- оперативные подразделения, осуществляющие оперативно-розыскное обеспечение раскрытия и расследования транснациональной преступной деятельности.

Завершая рассмотрение вышеназванных положений, позволим себе сделать следующие выводы:

Системно-структурный анализ, позволяет с наибольшей эффективностью исследовать транснациональную преступную деятельность на объектах водного транспорта в качестве системы, состоящей из комплекса структурных уровней и элементов, а также совокупности системных связей, существующих между ними.

К числу приоритетных направлений использования подобного научно-исследовательского подхода, следует отнести: системно-структурный анализ транснациональной преступной деятельности на объектах водного транспорта; выделение составляющих ее видов преступлений; формирование ее оперативно-розыскной характеристики и др.

1. Агошкова Е. Б., Ахлибининский Б. В. Эволюция понятия системы // Вопросы философии. 1998. № 7. С. 170–178.

2. Воскобойников А. Э. Системные исследования: базовые понятия, принципы и методология // Знание. Понимание. Умение. 2013. № 6. С. 5–7.

3. Гетман Н. И., Степаненко Ю. В. Организация борьбы с преступлениями на пассажирском железнодорожном транспорте: практ. пособие. М.: Экзамен, 2003. 127 с.

4. Давыдов В.О. Методика расследования транснациональной преступности экстремистского характера: дис. ... д-ра юрид. наук. Тула., 2018.

5. Ивахненко А.Г. Системный анализ: учебное пособие для студентов вузов. Курск: Курский гос. технический ун-т, 2008. 134 с.

6. Климов И.А., Синилов Г.К. Предмет, система, методология, история и перспективы развития теории оперативно-розыскной деятельности: курс лекций по оперативно-розыскной деятельности. Вып. 1. М.: ЮИ МВД РФ, 1995. 24 с.

7. Костырев В.М. Проблемы системного и формально-логического анализа права: автореф. дис. ... канд. юрид. наук. Уфа, 2002. 24 с.

8. Михайлова Л.В. Обстановка совершения хищений на объектах морского транспорта как элемент оперативно-розыскной характеристики // Проблемы и перспективы развития государства и права в XXI веке: мат-лы VI Международной научно-практической конференции. Улан-Удэ: Изд-во ВСГУТУ, 2015. С. 97–103.

9. Михайлова Л.В. Организация оперативно-розыскной деятельности оперативных подразделений по раскрытию преступлений на объектах морского транспорта (по мат. УТ МВД России по ДФО) // Актуальные проблемы опера-

тивно-розыскной и административной деятельности органов внутренних дел. 2015. № 1. С. 78–86.

10. Ображиев К.В. Системный подход в юриспруденции: теоретико-методологические основы // Вестник Ленинградского государственного университета им. А.С. Пушкина. 2012. № 1. С. 89–96.

11. Омелин В.Н., Мотин С.Г., Бедринский А.А. Организация и тактика выявления раскрытия экономических преступлений на объектах воздушного транспорта: учеб. пособие. М.: ВНИИ, 2007.

12. Савченко В.А. Преступления, совершаемые на водном транспорте России [Электронный ресурс] // Pro-Sud-123.ru: юридический сетевой электронный научный журнал. 2016. № 1 (55).

13. Шагиахметов М.Р. Основы системного мировоззрения: системно-онтологическое обоснование. М.: Товарищество науч. изд. КМК, 2009. 263 с.

ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ СЛЕДОВАТЕЛЕМ ПРЕДЕЛОВ ДОКАЗЫВАНИЯ

*Морозова Наталия Владимировна
кандидат юридических наук,
старший преподаватель кафедры криминалистики
и предварительного расследования в ОВД;*

*Малашенко Полина Константиновна,
курсант 301 учебной группы
факультета подготовки следователей*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027, г. Орел, ул. Игнатова, д. 2*

Статья содержит анализ теоретических аспектов процесса доказывания через определение его пределов.

Ключевые слова: *процесс доказывания, пределы доказывания, предмет доказывания, субъекты доказывания.*

Общеизвестно, что «пределы доказывания» – понятие, обозначающее крайне важный институт, центральный для всей теории доказывания в уголовном судопроизводстве. Несмотря на такую важность, определения пределов доказывания в Уголовно-процессуальном кодексе Российской Федерации не предусмотрено, в связи с чем очень часто в теории права возникают споры, касающиеся трактовки данного понятия [1].

Самостоятельно институт пределов доказывания стал выделяться только после принятия Уголовно-процессуального кодекса СССР в 1960 году, в котором подробно расписывались отдельные положения по теории доказывания и доказательствам. До этого момента теории не считали необходимым выделе-

ние пределов в отдельную категорию, отождествляя тему с категорией «предмет доказывания». Вместе с тем, после принятия нового УПК СССР отдельного определения «пределов доказывания» все также не давалось, но правоведы стали обращать больше внимания на рассматриваемую тематику и заговорили о необходимости выделения рассматриваемого института в отдельную категорию.

Уже после принятия УПК РФ в научном юридическом сообществе были сформулированы отдельные положения, касавшиеся пределов доказывания, однако, единства правоведы так и не достигли: полемика о сущности института «пределы доказывания» в рамках уголовного судопроизводства продолжают и по сей день.

Категория «пределов доказывания» является сложной, многоаспектной правовой конструкцией, которая включает в себя большое количество разноплановых составляющих. В научной литературе можно встретить различные определения пределов доказывания. В настоящее время общепризнанным считается понятие, данное П.С. Элькинд, согласно которому к пределам доказывания относится объём доказательств, обеспечивающих полное, всестороннее и объективное установление всех компонентов предмета доказывания по каждому конкретному уголовному делу [2; с. 109].

Однако далеко не все теоретики согласны с позицией П.С. Элькинд. На наш взгляд, определение, представленное ученым, является не слишком удачным, поскольку не передает сути исследуемой категории. Согласно словарю С.И. Ожегова, под пределами следует понимать границы, того или иного явления, процесса или физического объекта [3, с. 375]. Выходит, что с филологической точки зрения «пределами доказывания» никак не может быть совокупность доказательств, которая раскрывает полную юридическую картину произошедшего. Указанное определение более подходит именно институту «предмета доказывания», поскольку он непосредственно раскрывает обстоятельства, подлежащие доказыванию. В свою очередь, «пределы доказывания» должны служить именно границами, окончательными точками, за пределы которых не должна выходить уголовно-процессуальная деятельность по конкретному делу.

Теоретический аспект проблемы обусловлен также тем, что пределы процессуального доказывания в нашей юридической литературе исследовались гораздо меньше, чем предмет доказывания. С учетом анализа научной литературы, можно отметить попытки смешения предмета и пределов процессуального доказывания, что, безусловно, не может признаваться оправданным. Ведь при всей своей близости эти понятия не равнозначны друг другу – если предмет доказывания отвечает на вопрос: что подлежит познанию, то пределы доказывания, скорее, указывают глубину, оптимальные границы познания и обоснования этого предмета.

С этой точки зрения, пределы доказывания являются формой, то есть внешним выражением процесса, а предмет доказывания – содержанием, то есть внутренней составляющей. Предположим, что предмет доказывания – это прямая, состоящая из множества точек, которыми являются различного рода обстоятельства, имеющие значение для дела. Однако прочертить прямую полностью не представляется возможным, так же, как и найти все доказательства, подтверждающие все значимые для уголовного дела обстоятельства. Несмотря на это,

для успешной работы вся прямая не нужна: достаточно одной лишь её части, имеющей границы, – отрезка. Пределы доказывания являются своего рода отрезком на прямой предмета доказывания, так как они обозначают ту количественную и качественную доказательную базу, без которой, с одной стороны, нельзя достоверно установить наличие или отсутствие факта, а с другой стороны, выход за пределы которой влечёт к избыточности материалов уголовного дела и затягиванию процессуальных сроков.

Определение пределов доказывания для следователей при производстве предварительного следствия являются одной из основных задач на первоначальном и последующем этапах, так как именно эта категория указывает вектор движения, отдельные массивы информации, на которые следует обращать внимание, а которые следует оставлять без акцента, ввиду их незначительности для конкретного уголовного дела. Таким образом, можно говорить о том, что на этапе предварительного расследования именно следователь является субъектом, определяющим пределы доказывания.

При этом крайне важно соблюдение принципа достаточности доказательств, закрепленного в части 1 статьи 88 Уголовно-процессуального кодекса Российской Федерации. В специальной юридической литературе зачастую к субъектам, влияющим на определение пределов доказывания, могут быть отнесены: защитник, прокурор, руководитель следственного органа, подозреваемый, обвиняемый. Именно данные участники уголовного судопроизводства могут путем заявления ходатайств или дачи поручений о направлении предварительного следствия влиять и изменять пределы доказывания, тем самым оказывая содействие в их установлении [1].

Однако следует признать, что пределы доказывания и достаточность доказательств – категории абстрактные и оценочные, они определяются в зависимости от индивидуальных обстоятельств каждого дела. Тем не менее, пределы доказывания – категория идеальная, отражающая тот объем доказательств, который необходим и достаточен для установления каждого обстоятельства предмета доказывания, поэтому дальнейшее собирание доказательств по достижении данного предела будет терять свой познавательный смысл [4, с. 56].

Сложность установления пределов доказывания по уголовным делам обуславливается особенностями данного института. Среди них:

1) Отсутствие универсальности. Не существует одинаковых пределов доказывания для абсолютно каждого уголовного дела. Они будут отличаться, в зависимости от самого состава расследуемого преступления, круга участников, складывающихся тактических ситуаций и многого другого. Рассмотрим данное утверждение на примере.

В ситуации, когда обвиняемый полностью признает свою вину и в деле имеется информация о 20 очевидцах совершенного общественно опасного деяния, следует ли привлекать к допросу всех 20 человек? Однозначного и универсального ответа даже для таких ограниченных условий дать невозможно. С одной стороны, принципы всесторонности и объективности указывают на необходимость допроса всех очевидцев. Но, например, если более 10-12 очевидцев уже говорят об одном и том же, и их информация совпадает с позицией, заявленной в признательных показаниях обвиняемого, вряд ли с точки зрения целесообразно-

сти следует производить допрос оставшихся очевидцев. А если представить, что все 20 очевидцев были на месте происшествия в различные промежутки времени, обладают различными показателями зрения, сообщают отличающуюся информацию? Однозначно будет необходимо допросить каждого, для установления объективной картины на основе соотнесения общего знаменателя всех показаний. В этом случае, следовательно предстоит провести большой объем подготовительной работы, чтобы понять пределы доказывания в конкретном случае.

2) Многоаспектность. Как уже говорилось ранее, пределы доказывания – сложный, разноплановый институт, который включает в себя большое количество различных категорий, обстоятельств и позиций, которые следовательно необходимо учитывать при решении вопроса о самих пределах. В каждом конкретном случае субъект доказывания должен стараться максимально обобщенно воспринимать отдельные аспекты, пытаясь выявить и придать внимание каждой детали, поняв, будет ли она влиять на конечный результат процесса или нет. Так, для процесса доказывания крайне важным будет информация о марке сигарет, которые курит подозреваемый, если на месте совершения преступления будут найдены идентифицируемые окурки, что может послужить косвенным или даже в некоторых случаях, прямым доказательством (при наличии биологических следов на окурке). Но та же самая информация о предпочитаемой марке не будет иметь никакого значения для дела, если преступление, например, было совершено дистанционно или не было найдено каких-либо окурков.

3) Ситуативность. Пределы доказывания могут избираться следователем не только для каждого конкретного расследования по уголовному делу в целом, но и, например, для осуществления отдельных процессуальных действий, действий, которые требуются для принятия процессуального решения. Например, для принятия решения о заключении обвиняемого под стражу, пределами доказывания будет служить круг жизненных обстоятельств, аспектов совершения преступления, которые позволят выявить основания, предусмотренные статьёй 108 Уголовно-процессуального кодекса Российской Федерации. В этом случае, следователь ограничивается выяснением возраста, фактов, свидетельствующих о попытке скрыться, тяжести совершенного преступления и так далее. При этом будет выходить за пределы доказывания для принятия конкретного процессуального решения в данной ситуации, например, информация о количестве судимостей, наличии несовершеннолетних детей, службе в органах внутренних дел, хотя в рамках общего предела доказывания по уголовному делу, в целом, эта информация также должна быть исследована и может повлиять на решение судебного органа в будущем.

4) Условность. Зачастую в отдельных категориях дел можно встречать размытые границы, связанные, например, с событием преступления. Иногда установить точные пределы того или иного явления при расследовании уголовного дела не представляется возможным. В таком случае следует прибегать к размытым формулировкам, не позволяющим точно установить границы, но дающим возможность понять очертания. Так, в некоторых обвинительных заключениях и приговорах суда можно встретить формулировку:

- «в неустановленную следствием дату, но не позднее сентября 2018 года»
- «днем, более точное время следствием не установлено»;

- «в Северном районе г. Орла, более точно место совершения преступления не установлено».

В данном случае четких границ наблюдать нельзя, но можно понимать определенные грани, которые и могут служить частью процесса доказывания. Но также следует заметить, что такое становится возможным лишь в определении составляющих, подробное рассмотрение которых не имеет определяющего значения. Например, не будет особенно важным для предварительного следствия, в районе какого дома по улице Циолковского города Орла были совершены мошеннические действия, связанные с введением в заблуждение потерпевшего при передаче им материальных ценностей, если будет известно, что они происходили в случайно выбранном месте. Но при этом, важным для следствия будет факт совершения хулиганства, например, на борту самолета, совершение отдельных действий, оскорбляющих чувства верующих именно в храме и так далее, поскольку это влияет на квалификацию самого деяния.

4) Влияние на законность окончательного решения.

Следователю крайне важно уметь определять пределы доказывания для принятия конкретных процессуальных решений, ведь только в этом случае, будет обеспечена возможность полноценного сбора доказательств для всестороннего и объективного рассмотрения и установления юридической истины. Неправильное определение данных границ может повлечь за собой признание незаконности решения в целом, и как следствие, невыполнение задач уголовного судопроизводства. Иногда подобная ситуация и вовсе может приводить к принятию противоположных решений последующими инстанциями. Так, приговором Няндомского районного суда Архангельской области от 12 марта 2016 г. по части 4 статьи 111 УК РФ подсудимая была оправдана, поскольку суд признал недоказанность вины в причинении тяжкого вреда здоровью, повлекшего по неосторожности смерть потерпевшего. При этом, органы предварительного следствия, необоснованно сузили пределы доказывания, обратив внимание преимущественно на установление причинно-следственной связи между причинением тяжкого вреда здоровью и смертью потерпевшего [5].

Таким образом, для следователя при проведении предварительного расследования по уголовному делу крайне важно устанавливать пределы доказывания. Вместе с тем, это достаточно многогранная и сложная категория, вызывающая сложности с исследованием. Даже в теоретической среде ученых нет единого мнения о сущности пределов доказывания, однако эта категория обладает своими особенностями, которые необходимо всегда учитывать для вынесения обоснованного процессуального решения на каждом этапе уголовного судопроизводства.

1. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: от 18 декабря 2001 г. № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Зотов Д.В. Пределы доказывания в уголовном судопроизводстве (исследование с позиций разумного формализма) // Журнал российского права. 2016. № 2. С. 105–117.

3. Ожегов С.И. Словарь русского языка / под ред. Н.Ю. Шведовой. М.: Рус. яз., 1989. С. 375.

4. Костенко Р.В. Обеспечение надлежащих пределов доказывания в ходе установления обстоятельств уголовного дела // Библиотека криминалиста. 2017. № 4. С. 55–59.

5. Приговор Няндомского районного суда Архангельской области от 12 марта 2016 г. по части 4 статьи 111 УК РФ № 22-6425/2016 по делу № 1-92/2016 [Электронный ресурс]. URL: <https://sudact.ru> (дата обращения: 20.04.2020).

ОТДЕЛЬНЫЕ ВОПРОСЫ РАСКРЫТИЯ ХИЩЕНИЙ С БАНКОВСКИХ КАРТ ГРАЖДАН, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ

*Поддубный Илья Васильевич,
адъюнкт 1-го курса
кафедры оперативно-разыскной деятельности ОВД*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027, г. Орел, ул. Игнатова, 2.*

В статье рассматриваются проблемы, возникающие при раскрытии хищений с банковских карт граждан, совершаемых с использованием средств сотовой связи. Определяется актуальность данного преступления в современной России, даются определения таким понятиям как социальная инженерия и криптовалюта. Приводятся научные точки зрения по вопросам, связанным с хищениями с банковских карт граждан. Подчеркивается необходимость тесного взаимодействия правоохранительных органов со службами безопасности финансово кредитных учреждений и организациями связи, законодательном регулировании оборота криптовалюты.

Ключевые слова: *банковский карта, раскрытие, хищение, социальная инженерия, криптовалюта.*

На сегодняшний день в Российской Федерации широко используются безналичные способы оплаты среди населения, все более актуальным становится использование банковских карт.

Согласно исследованию, проведенному международной консалтинговой компанией The Boston Consulting Group (BCG), по скорости развития безналичных платежей Россия опережает западные страны: в 2010–2018 годах их число выросло в 30 раз (с 5,8 до 172 в год на человека), этот показатель опережает все европейские страны [1].

Организация денежных расчетов с использованием банковских карт гораздо предпочтительнее платежей наличными деньгами, поскольку достигается значительная экономия на издержках обращения. Во многих зарубежных стра-

нах и в Российской Федерации, количество пользователей платежных карт увеличивается с каждым годом. Согласно данным банка России карточные продукты используют порядка 89 % россиян [2].

В итоге сегодня большинство россиян пользуется как дебетовыми карточками, на которые в основном перечисляется заработная плата, пенсия, или стипендия, так и кредитными картами, причем карты используются не только для получения наличных в банкоматах, но и в качестве платежного средства.

Необходимо констатировать, что с ежегодным ростом пользователей платежных карт также увеличивается количество случаев хищений. Сегодня хищения с банковских карт приобретают катастрофические масштабы, поскольку преступники используют все новые методы преступной деятельности, разрабатывают эффективные схемы обмана, активно используют информационные технологии. Все перечисленное позволяет получить доступ злоумышленникам практически к любой карте. Происходят процессы самоорганизации преступников, создаются организованные группы, которые носят межрегиональный и транснациональный характер, что создает все предпосылки для роста количества незаконных финансовых операций.

Следует отметить, что Банки научились достаточно неплохо защищаться от преступников технически. Чтобы взломать счета и перевести с них деньги требуются специалисты высочайшего уровня. Как правило, их услуги стоят очень дорого, и не факт, что они обойдут охранные системы банка. Поэтому преступники стали использовать самое уязвимое звено между банком и человеком, а именно – последнего.

С этой целью злоумышленники стали активно применять методы социальной инженерии. Социальная инженерия – это совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят человека к необходимому результату. Тем самым социальные инженеры проектируют социальную среду, оказываясь в которой, люди согласно психологическим и физиологическим особенностям выполняют определенные действия. Обратная сторона социальной инженерии – это использование этих приемов и технологий формирования поведения для преступных целей [3]. В данном случае основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам либо побуждение жертвы самостоятельно перевести денежные средства на счет преступника.

Согласно сведениям Банка России, в 2019 году восемь из десяти хищений в России осуществлялись с использованием методов социальной инженерии, когда обманом пытаются узнать у клиентов банков конфиденциальные данные или вынуждают совершить перевод в их пользу. А это значит, что данный вид хищений остается основной угрозой сохранности денежных средств на счетах граждан.

В данном случае уместно привести утверждение заслуженного экономиста Российской Федерации Н.Н. Леонтьевой, которая отмечает, что наибольшая часть хищений со счетов физических лиц совершается через получение киберпреступниками несанкционированного прямого доступа к электронным средствам платежа, либо через побуждение владельцев средств самостоятельно со-

вершить перевод в пользу преступников путем обмана или злоупотребления доверием с использованием методов социальной инженерии [4].

Для примера обратимся к приговору Далматовского районного суда Курганской области № 1-60/2019 от 8 июля 2019 г. по делу № 1-60/2019.

Суд установил, что гр. А. совершил 13 мошенничеств, то есть похитил чужое имущество путем обмана, 7 из которых совершены с причинением значительного ущерба гражданину, а также совершил кражу с банковского счета, с причинением значительного ущерба гражданину.

По одному из эпизодов преступной деятельности А., судом было установлено, что 8 июня 2018 года А., осуществил звонок на мобильный телефон ранее ему не знакомой Потерпевший № 1. В ходе телефонного разговора А., представившись сотрудником службы безопасности банка, сообщил что банковская карта Потерпевший № 1 заблокирована, что для отмены блокировки необходимо подойти к ближайшему банкомату и провести ряд операций по данной карте. Получив отказ от Потерпевший № 1, в связи с отсутствием банкомата в месте ее нахождения, А. сообщил, что для отмены блокировки необходимо сообщить ему, как сотруднику банка, сведения о номере банковской карты, сроке ее действия и CVC коде (то есть, коде проверки карты), а также остатке денежных средств на лицевом счете банковской карты.

Получив эти данные, А., используя платежную систему «ЯНДЕКС МАНИ» и услугу по безналичному переводу денежных средств, осуществил запрос на перевод безналичных денежных средств в размере 7000 рублей с карты принадлежащей Потерпевший №1 на виртуальный счет, виртуальной банковской карты системы «ЯНДЕКС МАНИ», подконтрольный А. Затем А., зная о том, что на телефон Потерпевший № 1 придет смс-сообщение с паролем необходимым для исполнения операции, позвонил последней, и под предлогом отмены блокировки ее банковской карты, предложил сообщить ему, как сотруднику банка, персональный одноразовый пароль.

Получив пароль А. и введя его в платежную систему «Яндекс МАНИ», подтвердил безналичный перевод денежных средств. После чего, получив подтверждение одноразовым паролем, платежная система в автоматизированном режиме провела безналичный перевод денежных средств в сумме 7000 рублей. Таким образом, А. умышленно, из корыстных побуждений, тайно похитил с банковского счета денежные средства в сумме 7000 рублей, принадлежащие Потерпевший № 1, причинив последней значительный материальный ущерб на вышеуказанную сумму, незаконно изъяв денежные средства из владения потерпевшей, и распорядился ими впоследствии по своему усмотрению [5].

Заместитель директора департамента Банка России по информационной безопасности А.М. Сычев в своем интервью «Российской газете» указал, что телефонные звонки из псевдобанков с использованием социальной инженерии (выманивание конфиденциальной информации у жертв. – «РГ») стали основным видом мошенничества с банковскими счетами граждан. В структуре потерянных клиентами и банками денег большая часть – это средства, похищенные с помощью таких обзвонов [6].

Из доклада Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России следует, что объем не-

санкционированных операций с использованием платежных карт в 2018 году вырос на 44 процента, до 1,38 миллиарда рублей, количество таких операций увеличилось почти на треть: преступникам 417 тысяч раз удавалось разными способами получать деньги физлиц [7].

Как справедливо отмечают Р.Р. Гилязов и И.Х. Еркеев, продолжающийся рост преступных посягательств с использованием средств сотовой связи, увеличение числа нераскрытых преступлений, как показывает следственная практика, объясняется не только высокой латентностью подобных преступлений, но, что немаловажно, несовершенством нормативно-правового регулирования в области телекоммуникационных технологий, отсутствием необходимого взаимодействия операторов сотовой связи между собой и правоохранительными органами, недостаточной правовой грамотностью населения [8].

Вышеизложенное свидетельствует о недостаточности принимаемых правоохранительными органами России мер по противодействию указанным преступным проявлениям. В связи с вышеизложенным очевидно, что эффективное раскрытие хищений с банковских карт граждан совершаемые с использованием средств сотовой связи, является одной из приоритетных задач для оперативных подразделений органов внутренних дел. Как справедливо отмечают Н.В. Ерошенков и В.И. Цветов, раскрытие таких преступлений требует от оперативных сотрудников новых тактических подходов и совершенствования практики изобличения преступника [9].

Однако анализ правоприменительной практики по раскрытию хищений с банковских карт граждан, совершаемых с использованием средств сотовой связи показывает, что на сегодняшний день существует ряд проблем, препятствующих эффективному раскрытию преступлений данного вида.

Во-первых, это недостаточный уровень знаний и профессиональной подготовки сотрудников органов внутренних дел в области преступности, совершаемой с использованием информационно-коммуникационных технологий. В частности, распространенной является ситуация, когда сотрудник, входящий в состав дежурной СОГ, не обладают объемом достаточных знаний, необходимых для принятия полноценного заявления и первоначального объяснения от лица пострадавшего от хищения с банковской карты, а также осуществления общих мероприятий по установлению картины произошедшего. В вышеуказанных процессуальных документах сотрудниками не отражаются сведения, которые содержат оперативно-значимую информацию, необходимую для проведения первоочередных ОРМ, направленных на раскрытие преступления, в частности абонентский номер с которого осуществлял диалог злоумышленник, сообщаемые им сведения, реквизиты карты потерпевшего, дата и время операции и т.д., в связи с чем оперуполномоченный получивший на рассмотрение материал проверки вынужден повторно вызывать потерпевшего и дополнительно выяснить обстоятельства произошедшего, что вызывает промедление в осуществлении необходимых ОРМ.

Во-вторых, 3 апреля 2018 г. был подписан приказ МВД России № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» [10], согласно которому приказано обеспечить проведение проверки в порядке, установленном статьей 144 Уголовно-

процессуального кодекса Российской Федерации, сообщения о преступлениях, предусмотренных статьями 158, 159–159.3, 159.5, 159.6 Уголовного кодекса Российской Федерации, совершенных с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, в ходе которой незамедлительно принимать исчерпывающие меры к раскрытию преступлений и установлению лиц, их совершивших; направлять в установленном порядке запросы в кредитные организации, операторам связи, оказывающим услуги связи, в том числе по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет, получать объяснения от заявителя и возможных очевидцев преступления; а также, обеспечить принятие решения о возбуждении уголовного дела в органе внутренних дел Российской Федерации, в который поступило сообщение о преступлении, при наличии достаточных данных, указывающих на признаки указанных преступлений.

Однако одновременно с этим продолжают иметь место случаи необоснованного и многократного направления доследственных материалов проверки из одного территориального подразделения органов внутренних дел в другой, что, в свою очередь, затягивает сроки проверки, приводит к утрате следов преступления и позволяет виновным уйти от уголовной ответственности, нарушает права пострадавших граждан. Получается, что на практике мы имеем материал проверки, по которому не проводились никакие мероприятия, который пересылается месяцами из одного территориального органа в другой и который состоит из одних сопроводительных документов и уведомлений заявителю.

В-третьих, нерешенным остается вопрос информационного обмена с организациями связи, банковскими и иными финансовыми учреждениями. Как справедливо утверждают Н.В. Яджин и В.А. Егоров, продолжительность исполнения запросов организациями и учреждениями увеличивает сроки расследования и затрудняет возможность изобличения преступника [11].

На сегодняшний день существует острая необходимость использования электронного документооборота между территориальными органами и финансово кредитными учреждениями, а также организациями связи. К примеру, в настоящее время информация о движении денежных средств, сведения о номерах счетов, на которые осуществлялись денежные переводы, данные о лицах, их получивших, и т.д., может поступить в ОВД спустя несколько недель или даже месяцев после отправки соответствующего запроса.

За это время у преступников имеется возможность принять меры к сокрытию и уничтожению следов своей противоправной деятельности, изменить средства связи, свое фактическое место проживания и т.д. Также в течение данного времени может быть «утеряна» информация, способствующая установлению преступника, что в итоге приводит к потере доказательств по уголовному делу, например видео- и фотофрагментов с систем фиксации, установленных в отделениях банков и непосредственно в самих банкоматах, которые могли зафиксировать лиц, обналичивающих похищенные денежные средства.

Между тем следует отметить, что на сегодняшний день существует положительная практика заключения соглашений с подразделениями ПАО «Сбербанк России» и другими кредитно-финансовыми организациями, а также некоторыми сотовыми операторами такими как ПАО «Мегафон» и ПАО «Вымпел

ком», которые позволяют существенно сократить временные затраты на получение правоохранительными органами необходимой информации, посредством использования систем электронного документооборота и систем удаленного доступа. Однако данное взаимодействие пока носит региональный характер и в некоторых субъектах Российской Федерации отсутствует.

Наличие у правоохранительных органов таких функциональных возможностей информационного обмена позволяет повысить эффективность выявления и раскрытия хищений с банковских счетов граждан.

В-четвертых, в качестве способа легализации денежных средств, полученных преступным путем, все чаще используется конвертация денежных средств в цифровую (виртуальную) валюту, что обусловлено в первую очередь отсутствием возможности контролировать оборот таких денежных средств.

Появление такой виртуальной валюты, как «криптовалюта», постепенно стало изменять процедуру финансовых расчетов, осуществляемых преступниками. В широком научном плане криптовалюта – это цифровые счетные единицы или, иными словами, децентрализованная конвертируемая валюта, основанная на математических принципах, которая защищена с помощью криптографических методов.

В настоящее время несовершенство правового регулирования препятствует органам правопорядка изыскивать и использовать информацию об операциях с виртуальной валютой в целях выявления противоправной деятельности лиц ее использующих. Указанные обстоятельства в своей совокупности служат катализатором процесса перехода финансовой деятельности преступников в виртуальную плоскость.

Приведенный перечень проблем возникающих при раскрытии хищений с банковских карт не является исчерпывающим. Одновременно с этим полагаем, что их оперативное решение позволит повысить эффективность и результативность раскрытия подобного рода преступлений.

1. Калюков Е. ВCG сообщила о «русском чуде» в сфере карточных платежей [Электронный ресурс]. URL: <https://www.rbc.ru/finances> (дата обращения: 20.04.2020).

2. Почему 11 % россиян до сих пор не пользуются банковскими картами? Рассказывают эксперты [Электронный ресурс]. URL: <https://bankstoday.net> (дата обращения: 20.04.2020).

3. Претекстинг [Электронный ресурс]. URL: <https://finuch.ru> (дата обращения: 20.04.2020).

4. Кибермошенники в 2019 г. совершили 115 незаконных операций без согласия физлиц в Ростовской области [Электронный ресурс]. URL: <https://www.interfax-russia.ru> (дата обращения: 30.04.2020).

5. Приговор № 1-60/2019 от 8 июля 2019 г. по делу № 1-60/2019 [Электронный ресурс]. URL: <https://sudact.ru> (дата обращения: 30.04.2020).

6. Телефон недоверия [Электронный ресурс]. URL: <http://www.cbr.ru> (дата обращения: 30.04.2020).

7. Зубков И. Ваша карта бита. Хакеры украли у граждан больше, чем у банков и компаний [Электронный ресурс] // Рос. газ. Столичный выпуск. 2019. 19 февр. № 37 (7795). URL: <https://rg.ru> (дата обращения: 30.04.2020).

8. Гилязов Р.Р., Еркеев И.Х. Методика организации раскрытия и расследования преступлений, связанных с телефонным мошенничеством: методические рекомендации. М.: ДГСК МВД России. 2015. С. 4–5.

9. Ерошенков Н.В., Цветов В.И. Справочные интернет-ресурсы в раскрытии преступлений, связанных с хищением денежных средств с банковских счетов граждан [Электронный ресурс]. URL: <https://cyberleninka.ru> (дата обращения: 12.04.2020).

10. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 3 апреля 2018 г. № 196. URL: <https://43.xn--blaew.xn--plai/Moni/item/13373340> (дата обращения: 30.04.2020).

11. Яджин Н.В., Егоров В.А. Организационно правовое и информационное обеспечение расследования преступлений, совершаемых с использованием средств мобильной связи [Электронный ресурс]. URL: <https://cyberleninka.ru> (дата обращения: 12.04.2020).

ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ, ОБЕСПЕЧИВАЮЩИЕ БЕЗОПАСНОСТЬ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

*Смирнов Иван Михайлович,
преподаватель кафедры оперативно-розыскной деятельности ОВД*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027 г. Орел, ул. Игнатова, д. 2*

*Мирошкин Эдуард Александрович,
начальник управления экономической безопасности
и противодействия коррупции*

*УМВД России по Орловской области
302028 г. Орёл, ул. Тургенева, д. 15/17*

В статье рассмотрены вопросы, связанные с правовой регламентацией и непосредственным проведением оперативно-розыскных мероприятий, целью которых является обеспечение защиты должностных лиц и органов, уполномоченных на осуществление оперативно-розыскной деятельности. Особое внимание уделяется значению некоторых оперативно-розыскных мероприятий для безопасности правоохранительных органов, что, непременно, является важным инструментом повышения эффективности деятельности органов внутренних дел в целом.

***Ключевые слова:** противодействие преступности, оперативно-розыскные мероприятия, оперативно-розыскная деятельность, органы, осуществляющие оперативно-розыскную деятельность, обеспечение безопасности.*

Особенности современного политического и социального устройства Российской Федерации предполагают первостепенную роль личности в складывающихся общественных отношениях. Права и свободы человека и гражданина являются высшей ценностью, а их признание – задача государства. Кроме того, в Основном законе страны – Конституции Российской Федерации провозглашаются и иные ценности, такие как собственность, интересы государственной службы, охрана окружающей среды и многие другие.

В свою очередь, санкции за несоблюдение требований по обеспечению благополучного существования и использования тех или иных охраняемых законом благ содержатся в Уголовном кодексе Российской Федерации в иерархической структуре, соответствующей обозначенным приоритетам.

Государство в данных правоотношениях выступает центральным элементом, наделённым возможностями обеспечения выполнения тех или иных норм закона в принудительном порядке. Здесь мы сталкиваемся с парадоксальной ситуацией, когда обеспечение права одного человека может вызвать необходимость в ограничении прав другого, тем или иным образом препятствующего их реализации, посягающего на интересы защищаемой личности, а также в отношении которого имеются основания предположить его причастность к совершению противоправных деяний в отношении охраняемых законом объектов (личность, общество, государство и др.) [1].

Система защиты прав и свобод личности, охраны иных интересов человека, общества и государства представляет собой сложно структурированный механизм, заключающий в себе два больших блока: законодательный и непосредственно правоприменительный. Система государственных органов, а именно правоохранительных органов построена таким образом, чтобы охватить все сферы общественной жизни.

Следует отметить, что с каждым годом, несмотря на эффективное функционирование правоохранительной системы и количественное снижение уровня преступности, качественные показатели всё же возрастают. Появляются потенциально новые виды преступлений, связанные в большинстве своём с информационными технологиями.

В процессе реализации правоохранительными органами полномочий немаловажно уделить внимание и обеспечению собственной безопасности. Существующие в настоящее время в законодательстве и практической деятельности следственные действия и оперативно-розыскные мероприятия (ОРМ) адаптированы и для целей органов, осуществляющих оперативно-розыскную деятельность (ОРД). В свою очередь такие меры, являясь инструментом достижения целей уголовного судопроизводства и ОРД, выступают способом охраны интересов службы органов, осуществляющих ОРД, а также защиты жизни и здоровья сотрудников, членов их семей от противоправных посягательств, связанных с осуществлением ОРД.

Данный вопрос является весьма актуальным, поскольку нередко становятся известны случаи посягательств на должностных лиц органов, осуществляющих ОРД, в целях воспрепятствования их деятельности, направленной на установление обстоятельств того или иного события, представляющего оперативный интерес. Вместе с тем подвергаются влиянию со стороны преступников и члены семей таких должностных лиц, а также близкие им лица, что осуществляется с той же целью по мотивам осуществления служебной и профессиональной деятельности.

Определим предмет исследования в рамках данной статьи, т.е. органы, которые уполномочены осуществлять ОРД на территории России.

Итак, согласно статье 13 Федерального закона «Об ОРД», к таким органам относятся оперативные подразделения органов внутренних дел Российской Федерации (ОВД РФ), Федеральной службы безопасности (ФСБ), Федерального органа исполнительной власти в области государственной охраны, таможенных органов РФ, службы внешней разведки и Федеральной службы исполнения наказаний (ФСИН) [2].

На перечисленные субъекты распространяется весь спектр прав и обязанностей в части проведения мероприятий в рамках ОРД. Вместе с тем, их правовой статус дополнительно регулируется и конкретизируется федеральным законодательством и подзаконными нормативными правовыми актами по конкретным направлениям деятельности.

Так, например, вопросы обеспечения безопасности данных органов при проведении ОРМ закрепляются в статье 8 Федерального закона «Об ОРД». Наряду с этим соответствующие нормативные правовые акты содержат аналогичное положение применительно к органу, деятельность которого они регламентируют. Обеспечение безопасности содержится в пункте 11 статьи 6 Федерального закона «О внешней разведке», пункте «т» статьи 13 Федерального закона «Об органах ФСБ в РФ», пункте 9 статьи 14 Федерального закона «О государственной охране», части 2 статьи 28 Закона «О государственной границе РФ».

Статья 8 Федерального закона «Об ОРД», содержащая условия проведения ОРМ, закрепляет положение, согласно которому ОРМ, направленные на обеспечение безопасности органов, осуществляющих ОРД, проводятся в соответствии с нормами Федерального закона «Об ОРД» и исключительно в пределах компетенции конкретного органа. Анализ указанного положения позволяет сделать вывод о том, что законодатель не ограничивает правоприменителя в перечне ОРМ. Возможно проведение любых предусмотренных законодательством мероприятий, способствующих обеспечению безопасности органов, осуществляющих ОРД [2].

Вместе с тем, органам, осуществляющим ОРД, предоставляется право сбора необходимых сведений для обеспечения собственной безопасности, что так же регламентируется нормами Федерального закона «Об ОРД».

Обеспечение безопасности органов, осуществляющих ОРД, не является основанием, предполагающим запрет на проведение таких ОРМ, как обследование помещений, зданий, сооружений, участков местности и транспортных средств; контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров; снятие информации с технических кана-

лов связи. Это положение в очередной раз подтверждает то, что для обеспечения безопасности органов, осуществляющих ОРД, возможно проведение любых предусмотренных законом ОРМ [2].

Напротив, проведение указанных мероприятий, а также получение компьютерной информации допускается без судебного решения при условии согласия гражданина в письменной форме. Это повышает оперативность и, соответственно, эффективность принятия мер по обеспечению безопасности [2].

Определим и рассмотрим некоторые ОРМ, практическое значение которых для обеспечения безопасности органов, осуществляющих ОРД, очевидно.

В первую очередь, следует уделить внимание опросу. На наш взгляд, это основополагающее ОРМ, выступающее неформальным поводом для проведения иных мероприятий. Так, в ходе опроса лица об обстоятельствах и лицах, представляющих оперативный интерес, проводимого как в открытой форме, так и с использованием приёмов конспирации, могут быть получены сведения о подготавливаемом покушении на должностных лиц, членов их семей со стороны злоумышленников. Данное ОРМ позволит в целом определить настрой лица, представляющего оперативный интерес и установить степень опасности его для органов ОРД.

Аналогичное значение имеет и наведение справок, наблюдение, отождествление личности. Перечисленные ОРМ позволят установить лицо, определить режим жизни этого лица или нескольких лиц, представляющих угрозу безопасности и принять своевременно меры по защите охраняемых объектов или воспрепятствованию неправомерным действиям с последующими правовыми последствиями в виде задержания лица и решения вопроса о привлечении его к юридической ответственности.

Следующим значимым, по нашему мнению, ОРМ является обследование помещений, зданий, сооружений, участков местности и транспортных средств. Оно представляет собой проникновение и оперативный (непроцессуальный) осмотр указанных и иных объектов в целях обнаружения следов преступной деятельности, орудий совершения преступления, разыскиваемых преступников, а также для решения иных конкретных задач оперативно-розыскной деятельности [3].

Данное ОРМ также имеет значение для обнаружения преступников, орудий совершения преступления или подготавливаемого преступления. Так, к примеру, это ОРМ актуально при обследовании пути следования и мест предполагаемого нахождения сотрудников, осуществляющих ОРД, когда необходимо проверить помещение, участки местности на предмет наличия устройств негласного получения информации, взрывных устройств и т.п.

Для своевременного обнаружения признаков готовящегося покушения на сотрудников правоохранительных органов в целях воспрепятствования деятельности органов, осуществляющих ОРД, могут проводиться прослушивание телефонных переговоров и получение компьютерной информации, снятие информации с технических каналов связи [4].

Ещё одним ОРМ, имеющим очевидное значение для обеспечения безопасности субъектов ОРД, является оперативное внедрение, которое также может быть направлено на получение сведений о настрое преступников в отношении правоохранительных органов и конкретных лиц, в том числе – сотрудников, об

их планам на дальнейшее время. Такое ОРМ проводится путем внедрения в их среду оперативных сотрудников полиции или лиц с ними сотрудничающих на конфиденциальной основе.

Таким образом, наряду с реализацией полномочий, связанных с выполнением функций по охране личности, общества и государства, а также их ценностей и интересов от преступных посягательств, необходимо уделять должное внимание и обеспечению безопасности правоохранительных органов. Нами рассмотрены меры, принимаемые в рамках осуществления оперативно-розыскной деятельности и направленные на защиту субъектов ОРД от посягательств, связанных с осуществлением ими полномочий. Как правило, такие посягательства направлены на воспрепятствование деятельности органов, их дестабилизации в целях продолжения преступной деятельности или мести за уже принятые юридические решения. Проанализировав действующее законодательство, мы пришли к выводу, что для обеспечения безопасности органов, осуществляющих ОРД, возможно проведение всех содержащихся в законе ОРМ. Положение, согласно которому обеспечивается защита органов, содержится в Федеральном законе «Об ОРД» и в нормативных актах, являющихся специальными и регламентирующими деятельность отдельных органов, выступающих субъектами ОРД. Вместе с тем, определено, что наибольшее значение имеют ОРМ, направленные на получение информации о лицах (группах лиц), их образе жизни, планах, интересах, настрое и т.п.

1. Лисицын А.Г. Некоторые вопросы организации контроля за оперативно-розыскной деятельностью органов внутренних дел // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2019. № 2 (79). С. 56–59.

2. Об оперативно-розыскной деятельности [Электронный ресурс]: Федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ: в ред. от 2 августа 2019 г. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Шикунов О.В. Понятие оперативно-розыскного мероприятия «обследование помещений, зданий, сооружений, участков местности и транспортных средств» // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2015. № 4 (36). С. 66–70.

4. Маркушин А.Г. Оперативно-розыскная деятельность [Электронный ресурс]: учебник и практикум для бакалавриата и специалитета. 5-е изд., перераб. и доп. М.: Юрайт, 2019. 342 с. (Высшее образование.) // ЭБС Юрайт [сайт]. URL: <https://urait.ru/bcode/438532> (дата обращения: 25.02.2020).

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ СЕРИЙНЫХ УБИЙСТВ

*Чаплыгина Виктория Николаевна,
кандидат юридических наук, доцент,
доцент кафедры криминалистики и предварительного расследования в ОВД;*

*Волкова Валерия Руслановна,
курсант 301 учебной группы факультета подготовки следователей*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027, г. Орел, ул. Игнатова, д.2*

В статье внимание уделено рассмотрению проблемных аспектов расследования серийных убийств на разных этапах расследования.

Ключевые слова: *убийство, серийное убийство, квалификация, оружие, организованная преступная группа, уголовная ответственность.*

Преступления, посягающие на жизнь человека, жестоко карались во все времена. Чем цивилизованнее становилось общество, тем более непонятными становились причины лишения человека жизни. Поэтому именно со статьи, предусматривающей уголовную ответственность за убийство, начинается Особенная часть Уголовного кодекса Российской Федерации [1]. Различные мотивы движут преступником, когда тот решает лишь другого человека самого ценного, – его жизни. Из наиболее часто встречающихся можно выделить убийства, совершенные из-за мести, желания завладеть имуществом, неприязненных личных отношений и, конечно же, большой процент совершаемых на бытовой почве (зачастую в ходе бытовых ссор).

Но ведь нередко в практике встречаются случаи, когда на счету преступника несколько убийств. В данном случае речь можно вести о серийных убийствах. Ранее действующая редакция Уголовного кодекса Российской Федерации в части 2 статьи 105 предусматривала пункт «н», который позволял отдельно квалифицировать убийства, совершенные неоднократно. В настоящее же время серийные убийства принято квалифицировать по пункту «а» части 2 статьи 105 Уголовного кодекса Российской Федерации, то есть убийство двух и более лиц. Данная норма охватывает лишь количественный критерий, а ведь бывают ситуации, когда лицо убивает 2 или даже 3 лиц, но эти преступления не являются серийными. Чтобы непосредственно говорить о совершении серии преступлений, необходимо, чтобы данные деяния соответствовали ряду определенных критериев. Таковыми являются:

- 1) убийства должны быть совершены одним и тем же лицом или одной и той же группой лиц;
- 2) преступления направлены на один и тот же объект – человеческую жизнь;
- 3) наличие единого мотива преступлений;
- 4) наличие временных интервалов между отдельными убийствами.

Поскольку все данные преступления совершаются одним и тем же субъектом, то и механизм их совершения, орудия преступления, выбор места совершения преступления и сокрытия следов зачастую идентичны.

Криминалистическая характеристика серийных убийств во много определяет методику их расследования. В целом она представляет собой совокупность отдельных процессуальных, оперативных, а также иных сведений по каждому конкретно расследуемому убийству. Именно учет всех этих факторов позволяет определить направления работы по поиску преступника. Криминалистическая характеристика серийных убийств подразделяется на 2 группы:

1) общие признаки, к которым относится характеристика места, времени, механизма совершения преступления, а также данные, характеризующие личность виновного по каждому эпизоду в серии;

2) признаки, которые свойственны лишь отдельным эпизодам из серии, но которые дополняют общие признаки, а соответственно, также имеют значения для раскрытия преступления в целом.

Существует ошибочное мнение, что все серийные убийства относительно идентичны друг другу. Это не так, данный вид преступлений также имеет свою криминалистическую классификацию. Среди самых распространенных критериев классификации можно выделить следующие:

1) количество субъектов, участвующих в убийствах. По данному критерию преступления подразделяются на совершенные убийцей единолично либо совершенные в составе группы лиц (по предварительному сговору, организованной группой);

2) способ их совершения. По данному критерию преступления делятся на: совершенные с применением огнестрельного оружия; с использованием холодного оружия; с применением взрывных устройств; совершенные с использованием различных подручных предметов и средств; для совершения которых использовалось несколько видов оружия.

3) мотив совершения убийств. Данная классификация является наиболее важной для расследования, так как от правильности определения мотива во многом зависит весь процесс расследования серии, поскольку определение мотива позволяет многое сказать о личности преступника. Наиболее часто встречаемыми в практике мотивами и целями совершения серийных убийств являются следующие: серийные убийства на сексуальной почве; по мотивам неприязни (например, «разборки» между несколькими преступными группировками); по мотивам мести (особенно, если преступления совершены по мотивам кровной мести, таким образом, преступник вершит, так называемый самосуд, считает, что возрождает принцип талиона); серийные убийства, совершенные из хулиганских побуждений; совершенные из корыстных побуждений; с целью скрыть другие, ранее совершенные преступления; совершенные по различным религиозным мотивам («ритуальные» убийства); по мотивам расовой или иной ненависти или вражды.

Криминалистическая классификация серийных убийств позволяет их дифференцировать по различным обстоятельствам, и именно по мотиву совершения преступлений и производится их начальное разделение.

Необходимо также отдельно остановиться на личности преступника. Впервые термин «серийный убийца» использовал в своих трудах представитель ФБР Роберт Ресслер [2]. Он достаточно большую часть своей жизни посвятил изучению психотипа, личности серийных убийц. Он предлагал делить их на 2 группы: организованных несоциальных и дезорганизованных асоциальных. Характерными чертами для первой группы преступников являлось: достаточно высокий интеллект, хитрость, расчетливость, выдержка и умение себя контролировать. Данный тип преступников уделяет большое внимание своему внешнему виду, работе над собой, организованные несоциальные серийные убийцы весьма обаятельны, склонны производить приятное впечатление на свое окружение.

Что же касается второй группы, то ее представители отличаются низким интеллектуальным развитием (ниже среднего уровня), зачастую и вовсе умственно отсталые, с выраженными расстройствами психики, неспособностью к общению с людьми и в основном с противоположным полом. В основном это все связано с их тяжелым детством, жестоким обращением к ним со стороны их близких и окружающих.

К сожалению, невозможно в настоящее время вычислить преступника только по его внешнему виду или поведению. Теория Чезаро Ломброзо, в основе которой лежала идея, что преступниками не становятся, а рождаются, не нашла своего научного подтверждения. Хотя во второй половине XIX века его идеи и идеи его единомышленником Ферра и Гарафала имели большую популярность среди населения, но современная наука опровергла версию, что по антропологическим характеристикам можно вычислить прирожденного преступника. Многие серийные убийцы СССР и современной России совсем не производили впечатления людей, связанных с преступным миром. Самый известный серийный убийца советской эпохи Андрей Чикатило был, на первый взгляд, тихим и семейным, работал учителем, никто из его знакомых не мог предположить, кем он является на самом деле.

Именно в связи с высокой опасностью данных преступлений необходимо к организации их расследования подходить очень тщательно, грамотно и скрупулезно. Наиболее целесообразно поручать расследование серийных убийств не одному следователю, а создавать следственную группу с необходимым оперативным сопровождением. Основными направлениями в работе следователь и сотрудников оперативных подразделений являются:

- 1) отработка выдвинутых версий с помощью процессуальных действий и оперативно-розыскных мероприятий;
- 2) проверка конкретно заподозренных лиц, особое внимание уделяется лицам, уже привлекавшимся к уголовной ответственности за подобные преступления;
- 3) тесный контакт следователя и оперативных уполномоченных с их коллегами из других субъектов, с целью обмена информацией, а также имеющимся опытом в расследовании серийных убийств.

Вопрос, связанный с методикой расследования серийных убийств, в своих трудах старались затронуть многие ученые. Так, В.Н. Исаенко склонен считать, что специфика расследования данной категории дел определяется следующими обстоятельствами:

1) минимальным объемом известной информации о личности преступника, а зачастую и вовсе отсутствием данной информации;

2) профессионализмом в действиях преступника, благодаря которому он остается вне поля зрения очевидцев, а также который выражается в минимальном количестве следов на месте преступления или в их полном отсутствии;

3) способностью преступника маскировать убийства под безвестное исчезновение лиц;

4) способностью убийцы избавляться от трупов таким образом, при котором их невозможно или практически невозможно будет найти. Если обнаружить тело все же удастся, то возникают большие проблемы с идентификацией погибшего;

5) разбросом во времени и месте совершения отдельных убийств, что сказывается на том, что сотрудники следственных подразделений не всегда могут выявить между ними связи и обнаружить «серию»;

6) некачественным выполнением необходимых первоначальных следственных действий и оперативных мероприятий;

7) слабыми возможностями экспертных подразделений, которые не позволяют зачастую получить интересующую следствие информацию [3; с. 136].

При разработке методики расследования преступлений данной категории перед учеными и практическими сотрудниками возникают проблемы теоретического характера, без решения которых невозможно разработать рекомендации по конкретным вопросам проведения данной деятельности. В первую очередь необходимо внимательно изучить признаки, указанных в криминалистических характеристиках, которые являются наиболее существенными при выявлении и расследовании серийных убийств.

Но, к сожалению, существуют и проблемные вопросы расследования серийных убийств. Как уже упоминалось ранее, зачастую опыта и профессионализма следователя не хватает, чтобы в отдельных убийствах распознать «серию». Таким образом, получается, что по каждому отдельному эпизоду различные следователи ведут расследования и не всегда приходят к выводу о совершении всех этих преступлений одним лицом. Это приводит к тому, что если настоящий убийца привлекается к уголовной ответственности, то зачастую ему вменяют не все эпизоды, за какие-то отдельные его убийства могут привлечь к ответственности другого человека, к сожалению, от следственной и судебной ошибки никто не застрахован, наглядный тому пример – расследования дела Чикатило. Пока окончательно поняли, что все эпизоды совершил он, расстреляли несколько невиновных лиц. Еще одной проблемой является отсутствие качественной информационно-аналитической базы, отсутствие обмена между различными территориальными подразделениями информацией о личностях преступников и их преступлениях. Существующая в настоящее время система обмена информацией требует качественного преобразования. Еще одним проблемным аспектом при расследовании серийных убийств является не всегда четкая и грамотная координация между субъектами расследования (следственной группой и оперативным сопровождением).

Подводя итог всему вышесказанному, хочется еще раз отметить, что данные преступления представляют наибольшую опасность, покушаясь на высшую

ценность, а именно жизнь человека. Мотивы совершения данного рода преступления у каждого свои, невозможно заранее предугадать, что именно этот человек в будущем станет серийным убийцей. Хотя процент серийных убийств невелик относительно общего количества, совершаемых преступлений, но методика их раскрытия требует постоянного совершенствования. Поскольку прогресс в различных областях не стоит на месте, преступники становятся все более изощренными, именно поэтому следователи при расследовании данной категории уголовных дел должны быть особо внимательными, скрупулезными и не допускать ошибок и промедлений.

Полагаем, что методика расследования конкретной серии убийств должна включать в себя комплекс процессуальных и проверочных действий по выявлению других убийств, которые могли быть совершены установленным обвиняемым (подозреваемым). Наиболее целесообразными вариантами предупреждения данных преступлений являются: назначение виновным максимально строгого наказания с их длительной изоляцией от общества, проведение различных мероприятий разъяснительного характера, а также сокращение в СМИ и сети «Интернет» сцен насилия и жестокость. И тогда, возможно, получится, если не искоренить преступления данной группы, то хотя бы максимально сократить их количество.

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: в ред. от 27 декабря 2019 г. // Собр. законодательства Рос. Федерации. 2001. № 52 (ч. 1), ст. 1.

2. URL: <http://yurpsy.com/files/lica/ressler.htm>.

3. Исаенко В.Н. Проблемы теории и практики расследования серийных убийств: монография. М.: АНО «Юридические программы», 2005. С. 304.

НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЕ ПРЕСТУПЛЕНИЙ НЕСОВЕРШЕННОЛЕТНИХ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИКОВ

*Шеметов Алексей Константинович,
старший преподаватель кафедры криминалистики*

*Екатеринбургский филиал ФГКОУ ВО
«Московская академия Следственного комитета Российской Федерации»
620142, г. Екатеринбург, ул. Щорса, д. 18*

В статье рассмотрены общие направления выявления преступлений несовершеннолетних, связанных с незаконным оборотом наркотиков. Автором предложены рекомендации по организации и проведению проверочной закупки с использованием бесконтактного способа приобретения наркотических средств в сети Интернет. Определены основные трудности, возникающие при подготовке, проведении и оформлении хода и результатов оперативно-розыскного мероприятия.

Ключевые слова: выявление преступлений, проверочная закупка, наркотические средства, сеть Интернет, оперативно-розыскная деятельность.

Большинство уголовных дел о преступлениях несовершеннолетних, связанных с незаконным оборотом наркотических средств, выявляются представителями органов внутренних дел, при задержании подростков и проведении их досмотра. Менее распространенным, к сожалению, является установление фактов такого рода в результате тщательно спланированных и проведенных оперативно-розыскных мероприятий по изобличению организованных мест и способов сбыта запрещенных веществ несовершеннолетним. Несмотря на это, в арсенале органов, осуществляющих ОРД, есть немало средств подобного рода пресекающей деятельности. Самым распространенным средством является проверочная закупка, направленная на задержание непосредственного приобретателя незаконного товара, который даже и не задумывается о внимании со стороны правоохранителей.

Результатом контролируемого приобретения становится протокол личного досмотра лица, приобретшего наркотическое средство или психотропное вещество, в ходе которого происходит изъятие наркотика. Само вещество должно быть при этом надежно упаковано, исключена возможность его повреждения, утраты, несанкционированного доступа к нему, привнесение на его поверхность микрочастиц и посторонних следов. На самой упаковке ставятся отметки о мероприятии, в ходе которого изъято наркотическое вещество, подписи должностного лица, производившего действие и присутствующих при этом участников. В протоколе изымаемый предмет также описывается как можно подробнее.

В последнее время все большую актуальность набирает приобретение наркотических средств в сети Интернет. Торговля запрещенными препаратами и веществами некоторыми сообществами поставлена на профессиональную основу, тщательно и детально планируется и скрывается от правоохранительных органов места размещения товара, каналы его оплаты, получатели платежей. В ряде ситуаций используются профессиональные знания в области программирования и навыки общения в сети. Вполне справедливо такого рода преступная деятельность ориентирована именно на подростков, которые в большей степени представлены во внешней аудитории информационно-коммуникационной сети. Для распространения наркотиков используются социальные сети и мессенджеры, пользующиеся популярностью именно в среде несовершеннолетних. В преступные сети включаются лица, сами являющиеся подростками с целью реализации запрещенного товара среди своих знакомых.

В сети Интернет существуют виртуальные магазины психоактивных средств, где оплата за приобретенный товар осуществляется дистанционно, а его отправка и размещение осуществляется скрыто и заблаговременно до оплаты потребителем. Для расчетов за незаконную деятельность активно используются трудноконтролируемые платежные средства. Яндекс, QIWI-кошельки, оформленные на подставных лиц, даже не догадывающихся об источнике переводов.

Для передачи потребителю товара оборудуются тайники-закладки, о месте расположения которых покупателю сообщается после оплаты. В переписке такого рода указываются точные ориентиры скрытого хранилища, его GPS-метка,

отсылаются фотоизображения маркеров, располагающихся в непосредственной близости и т.п.

Несмотря на достаточно примитивные способы сокрытия собственных действий изобличение даже рядовых участников группы, оборудующих тайник, отправляющих сообщения, мелких оптовиков товара представляет значительную сложность. Установление же куратора, руководящего процессом, в ряде ситуаций вообще становится труднореализуемой задачей.

Ряд интернет-магазинов подобного толка вовсе находится за рубежом, имея на территории Российской Федерации лишь сеть распространителей среднего звена. Многие каналы связи осуществляются с учетом маскировки через коммутацию последовательно располагающихся серверов, значительно затрудняющих установление реального места расположения продавца.

Все это требует долгой и кропотливой работы органов оперативно-розыскной деятельности в тесном контакте со следователем, специалистом, некоторыми организациями, откуда может быть почерпнута нужная информация.

Само наблюдение за сетевыми ресурсами в сети Интернет требует использования особых тактических приемов контроля общения абонентов, грамотного проведения в сети тактических комплексов мероприятий. При этом осуществляется поиск на сетевом ресурсе данных о самом преступном событии, лицах участвующих в нем, а также месте их нахождения. При производстве указанных действий требуется консультативная деятельность с различного рода специалистами в области компьютерной техники, устройства сетей, интернет-провайдерами, мобильными операторами сотовой связи и другими организациями, налаживающими или поддерживающими общение пользователей виртуального пространства.

Контроль за ходом проверочной закупки, осуществляемой посредством сети Интернет отражается в процессуальных документах по общим правилам производства указанного оперативного мероприятия. Особенность ее проведения заключается в том, что оплата, производимая бесконтактным способом, не предполагает непосредственной встречи покупателя и продавца, осуществляется в информационной среде, оставляет специфичные следы реализации.

Проведение проверочной закупки для документирования бесконтактного способа сбыта наркотических средств и психотропных веществ осуществляется в рамках общих тенденций производства этого мероприятия.

Кроме того, отсутствие или недостаточный объем данных о конкретных лицах, участвующих в незаконной сделке, требует организации и проведения дополнительных мероприятия по установлению их персональных данных, технических характеристик, номеров используемых ими средств связи и общения, места их расположения.

В первую очередь путем мониторинга сетевых ресурсов устанавливаются участники, предлагающие сбыт наркотических средств, отдельные интернет-магазины, специализирующиеся на продаже запрещенного продукта. После этого ведется поиск контактов с конкретными продавцами. В ряде ситуаций установление доверительного отношения требует значительного времени, использования кодовых слов и средств общения. Помощь в поисковых действиях назван-

ного рода могут оказывать и молодежные организации, осуществляющие пропаганду здорового образа жизни, активно изобличающие «торговцев смертью».

Далее подвергаются исследованию данные об операциях на электронном счете, активность самого владельца платежного средства, сведения о месте его деятельности, данных о получателях (как промежуточных, так и конечных) отправлений.

Субъектами сбыта подобных средств обычно используются неперсонализированные платежные средства, позволяющие в короткий срок, лишь по номеру мобильного телефона открыть счет, осуществляя при этом дальнейшие транзакции, не констатируя с сотрудниками кредитной организации («Qіwі-Банк», WebMoney, «Яндекс. Деньги», Е-port и др.) [1, с. 95]. Конечным получателем денежных средств чаще становятся лица, за материальное вознаграждение предоставляющие услуги по обналичиванию преступных доходов. Для открытия счетов также могут применяться «серые» SIM-карты, приобретенные номинальными абонентами, а также так называемые абонентские номера – «однодневки», которые распространяются незаконно. Предложенная схема значительно затрудняет установление реального абонента, клиента кредитной организации, продавца наркотического вещества [2, с. 27].

Путем наведения справок истребуется информация о клиенте кредитной организации, на имя которого открыт счет, осуществляется сбор сведений о владельце виртуального кошелька. Для этого в указанные организации направляются запросы, налаживается взаимодействие со структурами, отвечающими за экономическую безопасность названных учреждений.

Имея в распоряжении данные об абонентском номере интересующего лица, IMEI конкретного аппарата связи, которым он пользуется, появляется возможность отследить активность пользователя. При производстве оперативно-розыскных мероприятий устанавливается контроль за устройством сотовой связи, его местонахождением, активностью в сети, абонентами, с которыми он связывается, а также выявляются номера счетов в кредитных учреждениях, которые используются для переводов, их владельцы. Устанавливаются предполагаемые маршруты следования лиц, участвующих в переводах, обналичивании преступных доходов и т.п.

В этих условиях появляется возможность установления действительного получателя преступных средств, степень его активности на рынке запрещенных товаров, клиентскую базу подпольного магазина наркотических средств, географию его действий и т.д. В ходе указанного анализа может стать известно и о других участниках преступной деятельности.

При проведении проверочной закупки посредством бесконтактного способа сбыта наркотиков должны учитываться особенности этой криминальной деятельности.

После обнаружения в телекоммуникационных сетях (на сайтах, форумах) конкретных предложений с указанием наименования и стоимости наркотика производить документирование действий покупателя (оперативного работника) в процессе проведения проверочной закупки, необходимо начинать с момента отправки сообщения покупателем сбытчику о согласии приобрести предлагае-

мое наркотическое средство (фиксация при помощи скриншота на электронном носителе).

После получения положительного ответа от сбытчика прослеживается перенаправления денежных средств через кредитную организацию, количество и место нахождения каждого абонента, включенного в преступную цепь, их местонахождение вплоть до конечного клиента, снимающего реальные денежные средства в платежном терминале.

После получения сообщения от сбытчика о наличии наркотического средства в определенном месте (закладке) факт обнаружения наркотика и конкретный адрес (закладки) фиксируются детально в акте проведения проверочной закупки.

Ход общения между покупателем и продавцом наркотических средств и психотропных веществ фиксируется с использованием компьютерной техники, сохраняется на электронных носителях информации, а позже приобщается к рапорту оперативного сотрудника.

Позже, при расследовании уголовного дела будет подвергаться исследованию и те средства, которые использовались сторонами сделки, а также сотрудниками, осуществляющими контрольную закупку. Поэтому сохранность указанной техники должна быть обеспечена.

В ходе проведения наблюдения фиксируются в хронологическом порядке все действия, связанные с документированием факта сбыта наркотических средств. Для фиксации противоправной деятельности наркосбытчиков применяются специальные технические средства.

Результаты проведенных оперативно-розыскных мероприятий представляются следователю для решения вопроса о возбуждении уголовного дела и использовании в доказывании в соответствии с Инструкцией о порядке представления результатов ОРД органу дознания, следователю, прокурору или в суд. Данные материалы направляются на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, в соответствии со статьёй 11 Федерального закона «Об оперативно-розыскной деятельности» и вышеописанной Инструкцией.

В любой ситуации поступления сведений о содержании противоправной деятельности несовершеннолетнего в сфере оборота наркотических средств требуется использование специальных познаний.

В первую очередь это касается ответа на вопрос об отнесении изъятого вещества к наркотическим, установления его веса и т.д.

В судебно-следственной практике данный вопрос обычно решается путем проведения предварительного исследования.

Юридический статус такого исследования в комментариях не нуждается и часто рассматривался значительным количеством авторов.

Производство предварительных исследований такого рода регулируется практикой их производства в отдельных подразделениях органов внутренних дел.

Результаты исследования оформляются справкой специалиста, которая включается позже в уголовное дело в порядке статьи 144 Уголовно-процессуаль-

ного кодекса Российской Федерации. Унифицированных требований к оформлению такого документа не предусмотрено.

Исследование должно проводиться с использованием методик, достоверно подтверждающих факт наличия (либо отсутствия) наркотического средства. Кроме того, для уголовно-правовой квалификации требуется еще и точное определение массы вещества. Таким образом, специалист должен провести полное исследование поступившего объекта по качеству и количеству, причем в очень короткие сроки. После возбуждения уголовного дела назначается судебная экспертиза, которая и будет иметь доказательственное значение.

И предварительное исследование, и экспертиза решают одни и те же задачи. Анализ практики показывает, что содержание вопросов, поставленных перед экспертом, совпадает.

Между тем исследование наркотиков имеет свои особенности.

Во-первых, для установления качественного состава наркотика используются физико-химические методы, связанные с расхождением определенного количества вещества. Данное обстоятельство необходимо учитывать при направлении на предварительное исследование малых количеств наркотиков.

Во-вторых, исследование наркотиков зачастую проводится с использованием методов, при которых в той или иной степени изменяется первоначальный вид объекта. Так, например, свежесобранные части растений, растворы, мази, различные вещества для количественного определения должны быть высушены до постоянного веса при температуре 110-115 °C [3, с. 42]. В результате при последующем поступлении этих объектов на экспертизу их внешние характеристики при описании могут существенно отличаться от первоначальных, что, безусловно, подстегивает адвокатский интерес. В таких ситуациях при проведении предварительных исследований можно порекомендовать, например, фотографирование объектов перед видоизменением и после этого, а также подробно описывать их состояния и производящиеся над ними манипуляции.

В случае невозможности сохранения целостности первоначальной упаковки необходимо осуществлять переупаковку объекта с отображением данных в исследовании. Раздельная упаковка позволяет следователю в дальнейшем рассматривать первоначальную упаковку и вещество как два разных объекта и принимать по ним соответствующие решения. Такая необходимость, например, возникает при проведении комплексного дактилоскопического и химического исследований.

При поступлении большого количества объектов целесообразно для исследования выделять какой-то один объект, установление принадлежности к наркотику которого будет являться достаточным основанием для возбуждения уголовного дела. При изъятии большой партии наркотика, вес которой не вызывает сомнения, можно ограничиться отбором представительной пробы в присутствии понятых в процессе первоначального осмотра.

Как уже было отмечено, результаты предварительно исследования, проведенного специалистом, будут включены в число оснований принятия процессуального решения о возбуждении уголовного дела или отказа в таковом. Кроме этого учитываются следователем и другая информация, имеющаяся в его распоряжении.

1. Шакирьянов М.М. Особенности проведения оперативно-розыскных мероприятий по выявлению и раскрытию бесконтактного сбыта наркотических средств // Вестник Самарского юридического института. 2019. № 3 (34). С. 92–96.

2. Помелов А.А. Особенности проведения проверочной закупки при документировании бесконтактного способа сбыта наркотических средств // Вестник Барнаульского юридического института МВД России. 2017. № 1 (32). С. 26–29.

3. Косыгина Т.А. Актуальные аспекты применения специальных знаний при расследовании преступлений, связанных с незаконным оборотом наркотиков // Информационная безопасность регионов. 2016. № 3 (24). С. 40–45.

НЕКОТОРЫЕ ВОПРОСЫ ПРОВЕДЕНИЯ ПРЕДВАРИТЕЛЬНОЙ ПРОВЕРКИ ПО СООБЩЕНИЮ О ПРЕСТУПЛЕНИИ, ПРЕДУСМОТРЕННОМУ СТ. 186 УК РФ

*Шляхова Валерия Владимировна,
адъюнкт 1-го курса*

*Орловский юридический институт МВД России имени В.В. Лукьянова
302027, г. Орел, ул. Игнатова, 2*

В настоящей статье рассматриваются особенности выявления преступлений, предусмотренных статьёй 186 Уголовного кодекса Российской Федерации, определяется порядок формирования криминалистически значимой информации при проведении предварительной проверки заявлений (сообщений) о данных преступлениях, являющейся основанием для возбуждения уголовных дел указанной категории.

Ключевые слова: *фальшивомонетничество, поводы и основания для возбуждения уголовных дел, предварительная проверка заявления (сообщения) о преступлении, первоначальные оперативно-розыскные и процессуальные действия, поддельные денежные купюры*

Возбуждению уголовных дел о преступлениях, связанных с изготовлением, хранением, перевозкой или сбытом поддельных денег или ценных бумаг, должна предшествовать тщательная проверка имеющейся первичной информации о преступлении, в результате которой следователь будет обладать достаточными данными, свидетельствующими о наличии или отсутствии закрепленных в уголовно-процессуальном законодательстве поводов и оснований для возбуждения уголовного дела данной категории, а также обстоятельств, исключающих производство по делу.

Источник информации о преступлении, надлежаще оформленный и переданный лицу или органу, уполномоченному принимать решение о возбуждении уголовного дела, называется поводом к возбуждению уголовного дела. В соответствии со статьёй 140 Уголовно-процессуального кодекса Российской Федера-

ции поводами для возбуждения уголовного дела служат: заявление о преступлении, явка с повинной, сообщение о совершенном или готовящемся преступлении, полученное из иных источников, постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании (часть 1); основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления (часть 2) [1].

Поводами для возбуждения уголовных дел указанной категории могут послужить:

1) заявление о преступлении, поданное работником организации в случае обнаружения поддельной денежной купюры в процессе обработки и сортировки денежной наличности, поступившей в учреждения кредитно-банковской системы России, при попытке ее сбыта под предлогом осуществления вклада или обмена денежных средств или внесения их на счет с использованием банкоматов, гражданином, получившим поддельные денежные купюры от известных или неизвестных ему лиц в ходе расчета с ним;

2) явка с повинной лица о совершенном им преступлении, предусмотренном статьёй 186 Уголовного кодекса Российской Федерации;

3) сообщение о совершенном или готовящемся преступлении, полученное из иных источников, чем указанные в статьях 141 и 142 Уголовно-процессуального кодекса Российской Федерации, в соответствии со статьёй 143 Уголовно-процессуального кодекса Российской Федерации принимается лицом, получившим данное сообщение, о чем им составляется рапорт об обнаружении признаков преступления;

4) постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании (поводом для возбуждения уголовных дел о преступлениях, предусмотренных статьёй 186 Уголовного кодекса Российской Федерации, как правило, не является).

Факт совершения преступления, предусмотренного статьёй 186 Уголовного кодекса Российской Федерации, может быть выявлен тремя способами:

- в случае обнаружения поддельных денежных купюр работником организации (сотрудником банка) или гражданином, получившими их в ходе произведенного с ними расчета известными или неизвестными лицами, при пересчете денежной наличности в учреждениях кредитно-банковской системы;

- в случае добровольного сообщения лица о совершенном им преступлении;

- в ходе оперативно-розыскной деятельности.

С целью установления достаточности данных, указывающих на признаки преступления, предусмотренного статьёй 186 Уголовного кодекса Российской Федерации, принятия законного и обоснованного решения о возбуждении или об отказе в возбуждении уголовного дела необходимо провести проверку заявления (сообщения) об изготовлении, хранении, перевозке или сбыте поддельных денег или ценных бумаг. Порядок формирования криминалистически значимой информации при проверке заявлений (сообщений) о преступлениях, предусмотренных статьёй 186 Уголовного кодекса Российской Федерации, будет зависеть

от источника и объема полученной исходной информации о преступлении [5]. При этом криминалистически значимая информация по рассматриваемым преступлениям охватывает сведения о месте, времени и способе совершения преступления, личности преступника, мотивах и целях преступления.

Предварительная проверка сообщения о преступлении включает в себя получение и фиксацию информации о преступлении, осуществление проверочных действий на предмет, имел ли в действительности место факт общественно опасного деяния, на который указано в информации, вынесение решения о возбуждении или отказе в возбуждении уголовного дела [2].

В статье 144 Уголовно-процессуального кодекса Российской Федерации закреплены допустимые действия дознавателя, органа дознания, следователя, руководителя следственного органа при проведении проверки сообщения о преступлении, сроках ее проведения [1]. Данные положения Уголовно-процессуального кодекса Российской Федерации распространяются не только на сообщения о преступлении, но и на другие поводы к возбуждению уголовного дела.

Алгоритм действий при проведении проверки первичной информации о преступлениях, предусмотренных статьёй 186 Уголовного кодекса Российской Федерации, аналогичен порядку формирования криминалистически значимой информации по преступлениям указанной категории и в большей мере зависит от источника и объема полученной информации о преступлении.

В случае обнаружения сомнительных денежных купюр при пересчете денежной наличности в учреждениях кредитно-банковской системы уполномоченные банковские работники осуществляют исследование вышеуказанных купюр на предмет их соответствия подлинным. В случае если в ходе исследования, проводимом специалистами кредитных организаций или иных банковских учреждений, подтверждается факт поддельности денежной купюры, то указанные организации обязаны в течение суток известить об этом территориальный орган внутренних дел. Формой извещения является телефонограмма, факсимильное или письменное сообщение, передаваемые по каналам телефонной или иной связи [3]. После чего на место происшествия незамедлительно направляется следственно-оперативная группа (СОГ).

С целью проверки данного сообщения о преступлении и принятия решения о возбуждении или отказе в возбуждении уголовного дела необходимо выполнить следующие основные мероприятия:

- провести осмотр места происшествия по месту обнаружения поддельной денежной купюры с целью изъятия самой купюры, видео, на котором зафиксирован момент расплombировки инкассаторской сумки и обнаружения поддельной денежной купюры.

Уже на первоначальном этапе необходимо принимать меры к выявлению на денежной купюре следов пальцев рук возможного сбытчика и их изъятию с целью проведения дактилоскопической судебной экспертизы. К сожалению, на практике при изъятии денежной купюры чаще всего не принимаются меры к выявлению следов пальцев рук на ней, что делает практически невозможным дальнейшее проведение дактилоскопической экспертизы и приводит к утрате доказательственной базы по делу.

- опросить работника, обнаружившего поддельную денежную купюру;

- установить место формирования инкассаторской сумки, содержащей поддельную денежную купюру;
- направить изъятую купюру в соответствующий отдел регионального ЭКЦ МВД России для проведения ее исследования.

В ходе предварительной проверки формируется следующий пакет документов: рапорт об обнаружении признаков преступления; сообщение учреждения кредитно-банковской системы России об обнаружении денежных купюр с признаками подделки; документы, предоставляемые сотрудниками банковского учреждения: акт передачи денежных знаков в территориальный орган внутренних дел, справка об исследовании каждого денежного знака с указанием признаков его подделки, копии сопроводительных документов, подтверждающих факт поступления денежной купюры в банковские учреждения; протокол осмотра места происшествия; задание на исследование сомнительной денежной купюры; справка специалиста о проведенном исследовании; объяснение работника, обнаружившего поддельную денежную купюру.

В случае поступления в учреждение кредитно-банковской системы поддельной денежной купюры в инкассаторской сумке из организации, расположенной вне района местонахождения данного учреждения, то в соответствии с пунктом 3 части 1 статьи 145 Уголовно-процессуального кодекса Российской Федерации материал проверки направляется в соответствующий территориальный орган внутренних дел по месту нахождения организации, в которой произошел факт сбыта.

При обнаружении поддельных денежных купюр работником организации (сотрудником банка) или гражданином, получившими их в ходе произведенного с ними расчета известными или неизвестными лицами, имеется некоторая информация о лице, осуществившем сбыт фальшивых купюр. В данной ситуации комплекс мероприятий, проводимых в рамках доследственной проверки, будет несколько отличаться от действий в условиях предыдущей ситуации. Основным направлением деятельности СОГ в сложившейся ситуации является установление личности сбытчика, обнаружение и изъятие следов заподозренного лица на месте происшествия [4].

В условиях данной ситуации членам СОГ необходимо выполнить комплекс следующих действий:

- провести осмотр места происшествия по месту обнаружения поддельной денежной купюры с целью изъятия самой купюры, видео, на котором зафиксирован момент обнаружения поддельной денежной купюры, иных следов лица, сбывшего поддельную денежную купюру, в случае их обнаружения назначить необходимые судебные экспертизы;
- направить изъятую купюру в соответствующий отдел регионального ЭКЦ МВД России для проведения ее исследования;
- установить и опросить очевидцев произошедшего, при возможности составить фоторобот лица, сбывшего поддельную денежную купюру;
- проверить лиц, ранее судимых за совершение преступлений указанной категории;
- проверить близлежащие торговые и иные учреждения с целью выявления иных фактов сбыта поддельных купюр;

- установить и опросить лицо, сбывшее поддельную денежную купюру.

В ходе предварительной проверки формируется следующий пакет документов: рапорт об обнаружении признаков преступления или заявление лица о совершенном преступлении; протокол осмотра места происшествия; задание на исследование сомнительной денежной купюры; справка специалиста о проведенном исследовании; объяснение лица, обнаружившего поддельную денежную купюру; объяснение лица, передавшего поддельный денежный билет работнику организации (гражданину), и иные документы, собранные в ходе доследственной проверки.

Особенностью ситуации, складывающейся в случае добровольного сообщения лица о совершенном им преступлении, предусмотренном статьёй 186 Уголовного кодекса Российской Федерации, является тот факт, что на момент регистрации такого сообщения у сотрудника, принявшего явку с повинной, отсутствует достоверная информация об изъятии из свободного оборота именно тех поддельных денежных купюр, на которые указывает данное лицо. В связи с этим с целью обнаружения и последующего изъятия поддельных денежных купюр, необходимо установить места их сбыта, основываясь на показаниях лица, написавшего явку с повинной, а также очевидцев произошедшего. После установления и изъятия указанных в явке с повинной поддельных денежных купюр, мероприятия, осуществляемые до возбуждения уголовного дела, в большей степени будут аналогичны рассмотренным выше.

Для решения вопроса о возбуждении уголовного дела по результатам оперативно-розыскной деятельности следователю должны быть представлены: рапорт об обнаружении признаков преступления; постановление о представлении результатов оперативно-розыскной деятельности органу дознания, следователю, или в суд; материалы оперативно-розыскной деятельности; задание на исследование сомнительной денежной купюры; справка специалиста о проведенном исследовании.

Результаты процессуальной и оперативно-розыскной деятельности, проведенной до возбуждения уголовного дела, позволяют следователю сформировать криминалистически значимую информацию о рассматриваемом преступлении и сделать вывод о наличии или отсутствии основания для возбуждения уголовного дела, о чем им в порядке статьи 145 Уголовно-процессуального кодекса Российской Федерации выносится соответствующее мотивированное постановление.

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: в ред. от 4 ноября 2019 г. № 354-ФЗ // Собр. законодательства Рос. Федерации. 2001. № 52 (Ч. 1), ст. 4921; 2019. № 44, ст. 6175.

2. Научно-практический комментарий к Уголовно-процессуальному кодексу Российской Федерации / под общ. ред. В.М. Лебедева; науч. ред. В.П. Божьев. 9-е изд., перераб. и доп. М.: Издательство Юрайт, 2014. 851 с.

3. Тришкина Е.А., Токарева Е.В. особенности возбуждения уголовных дел о фальшивомонетничестве // Актуальные проблемы права и правоприменения: сборник материалов пятой международной научно-практической конференции, 2011. С. 276–281.

4. Шрам О.Р. Оперативно-разыскные и процессуальные действия, проводимые в ходе предварительной проверки сообщений об изготовлении и сбыте поддельных денежных знаков // Вестник УЮИ. 2014. № 3 (65). С. 44–49.

5. Шунк В.Э. Порядок формирования криминалистически значимой информации при проверке заявлений (сообщений) о преступлениях, предусмотренных ст. 186 УК РФ // Вестник Санкт-Петербургского университета МВД России. 2014. № 4. С. 110–113.

ВЫЯВЛЕНИЕ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

*Яппаров Рауф Мидхатович,
кандидат юридических наук, доцент,
доцент кафедры оперативно-разыскной деятельности органов внутренних дел*

*Уфимский юридический институт МВД России
450103, Республика Башкортостан, г. Уфа, ул. Муксинова, д. 2*

В содержании статьи рассматриваются вопросы противоправного использования сети Интернет, информационных систем и компьютерных технологий для получения персональных данных, иной информации конфиденциального характера, а также проблемы выявления компьютерных преступлений, совершаемых с использованием интернет технологий.

Ключевые слова: *пользователь, компьютер, технологии, Интернет, информация, доступ, пароли, коды, вредоносная программа, поиск, файл, вирус, аккаунт, социальный инжиниринг, сайт, данные, ICQ-сообщения, онлайн-банкинг, интернет-аукцион, интернет-нейджер, контакт-лист, фишинг, потребительский, рынок, спам-рассылка, интеллектуальная собственность, защита, криминал, киберпреступность, формы, методы, способы, профилактика.*

В настоящее время компьютеры настолько прочно вошли в нашу жизнь, что с каждым днем все больше и больше людей хранят в них свою «виртуальную собственность». И если многие из них весьма трепетно относятся к таковой в реальном мире, то к сосредоточенным в сложных кибернетических устройствах, каковыми являются персональные ЭВМ, они явно не уделяют должного внимания. Большинство граждан продолжают считать, что никому нет дела до информации, сосредоточенной в их компьютерах, что в файлах нет ничего ценного для злоумышленника, и что все вирусные атаки пройдут мимо. Это далеко не так.

За последние годы интенсивного развития телекоммуникационных технологий, преступные структуры, постоянно изобретая новые вредоносные программы, превратили Интернет в высокодоходное занятие, своеобразный криминальный бизнес [1]. Так, только за период 2015 по 2019 год, по различным оценкам специалистов, преступный доход, построенный на кражах денежных средств граждан посредством сети Интернет, составил сотни миллиардов долларов.

В данной статье мы хотели бы проанализировать наиболее распространенные способы криминального обогащения, совершаемые с использованием интернет технологий и на этой основе определить оптимальные пути выявления компьютерных преступлений. Для этого мы предлагаем проанализировать современное состояние борьбы с компьютерными преступлениями с двух позиций, какая информация, сосредоточенная на компьютерах граждан, представляет интерес для правонарушителей и каким образом происходят непосредственно сами преступления.

Отметим, что в подавляющем большинстве случаев для совершения преступлений используются специализированные вредоносные программы или методы социального инжиниринга [2], либо и то и другое в совокупности. В настоящее время можно выделить 4 группы сведений, которые наиболее часто подвергаются атакам с помощью вредоносных программ:

- доступ к различным финансовым операциям (онлайн-банкингу [3], пластиковым картам, электронным деньгам), интернет-аукционам [4] и т.д.;
- доступ к аккаунтам [5], а также к адресам электронной почты;
- пароли, коды для доступа к интернет-пейджерам [6], сайтам и др.;
- пароли, коды к онлайн-играм.

Цель любой вредоносной программы – это осуществление контроля над действиями пользователя (например, запись последовательности всех нажатых клавиш), либо целенаправленный поиск ключевых данных в файлах или системном реестре. Полученные данные вредоносная программа в итоге передает лицу, намеревающемуся совершить преступление. Согласно общепринятой терминологии их называют программам Trojan-Spy или к Trojan-PSW [7]. «Заразиться» такими программами можно самыми различными путями: при просмотре вредоносного сайта, по почте, в чате, форуме, через интернет-пейджер или иным способом «во время путешествия» в сети Интернет. В качестве примера можно использовать алгоритм действий широко распространенного программного продукта Trojan-PSW.Win32.LdPinch, который занимается кражей паролей к почтовым ящикам, FTP и другой информации [8].

Особое опасение вызывает тот факт, что подобные вредоносные программы начинают сочетать с методами социального инжиниринга. В большинстве случаев преступники одновременно с вредоносными программами вынуждают пользователя сети совершать определенные действия, необходимые для достижения ими преступного умысла. Так, после запуска вредоносной программы может выйти диалоговое сообщение с просьбой заплатить небольшую сумму денег за пользование услугами интернет-провайдера [9]. При этом следует отметить, что сообщение будет составлено по всем правилам социального инжиниринга, то есть:

- пользователю не оставляют времени для размышлений, так как заплатить необходимо быстро, не раздумывая, в день получения письма;
- предлагается заплатить символическую плату – например 1 рубль, что резко увеличивает шансы мошенников;
- для стимулирования действий пользователя злоумышленники могут угрожать – если не заплатишь, провайдер заблокирует тебе доступ к сети Интернет.

При этом чтобы минимизировать подозрения пользователя в истинности намерений, в качестве отправителя указаны данные провайдера. Вполне логично предположить, что провайдер знает адрес электронной почты своего пользователя.

Первый этап работы такой программы – это ввести добросовестного пользователя в заблуждение, не оставить у него сомнений в необходимости ввода данных например своей кредитной карты. Законопослушному пользователю просто не оставляют выбора, и он нажимает кнопку «Оплатить», что приводит к появлению следующего диалогового окна. Естественно, что после заполнения всех полей и нажатия кнопки «Оплатить» никакой оплаты не происходит, а вся информация о вашей кредитной карте отправляется по почте к мошенникам.

Методы социального инжиниринга используются не только в совокупности с вредоносными программами. Красноречивым подтверждением этого является фишинг-атака, направленная на клиентов того или иного банка, использующих для управления своего счета систему онлайн-банкинга [10]. Так, например, в рассылаемых от имени банка фальшивых письмах авторы могут утверждать, что учетная запись клиента заблокирована по той или иной причине, и что для ее разблокирования необходимо ввести учетные данные пользователя и т.д. При этом в содержании письма имеется специальным образом сформированная ссылка, которая создается таким образом, чтобы на экране пользователя она отображалась как реально существующий сетевой адрес сайта банка (на самом же деле ссылка при ее активации приведет на сайт лица, намеревающегося совершить преступление). Введенные данные попадут не в банк, а к преступнику, который получит данные клиента, а вместе с ними и возможность доступа к его счету. Похожим образом рассылаются и письма от имени различных служб поддержки, социальных служб и т.п.

Преступники «охотятся» не только за данными пользователей банковских карт. Их интересуют и такие данные, как списки электронных адресов пользователей компьютеров. Неоценимую помощь в этом хакерам оказывают вредоносные программы, которые, согласно классификации произведенной известной фирмой «Лаборатория Касперского», получили название SpamTool. Эти программы занимаются сканированием файлов данных на компьютере пользователя и ищут там все адреса электронной почты, хранящиеся в операционной системе. Собранные таким образом адреса могут тут же отфильтровываться по заданным критериям (например, удаляются принадлежащие антивирусным компаниям) и отсылаются лицу, намеревающемуся совершить хищение денежных средств.

Существуют и куда более циничные способы проникновения вредоносных программ в компьютеры пользователей сети Интернет. Отмечены случаи, когда преступники предлагают владельцам сайтов купить вредоносные программы. Так, на одном из сайтов всемирной паутины Веб-мастерам предлагалось установить на собственных сайтах эксплойты [11] для дальнейшей автоматической загрузки посетителям вредоносных программ. «Партнерам по бизнесу» авторы предлагали купить вредоносные программы по цене 61\$ за 1000 заражений [12].

Безусловно, основная причина совершения преступлений – это корыстная направленность. В итоге практически любая информация продается либо напрямую используется для материального обогащения. Но получить данные кредит-

ных карт или электронные адреса граждан – это только часть дела, самое сложное – это вывести из платежной системы награбленное.

Способы обналичивания преступно нажитых средств путем использования интернет-технологий также весьма разнообразны. Если результатом проведенной фишинг-атаки стали, например, параметры для доступа к системе онлайн-банкинга или электронному кошельку пользователя, то средства могут быть выведены через цепочку виртуальных электронных обменных пунктов, например, путем перевода одной электронной валюты в другую через электронные платежные системы [13] или приобретения товара непосредственно в интернет-магазине [14]. Этап обналичивания доходов, полученных преступным путем, является самым опасным для преступника, так как приходится указывать какие-либо «свои» идентификационные признаки, например, адрес для доставки товара, номер индивидуального счета/электронного кошелька и т.д.

Изошренность в достижении преступных замыслов толкает мошенников на поиск новых путей решения проблем такого рода. Одним из таких направлений является привлечение людей для получения или передачи денежных средств, которых называют «дропами» [15]. Что же касается украденных адресов электронной почты, то их можно потом продать на «черном» рынке за немалые деньги тем же «спамерам», использующим эти данные в социальных сетях [16].

Другой, представляющий оперативный интерес, криминальный промысел – это учетные записи онлайн-игр, которые приобретают все большую популярность. В процессе таких игр многие пользователи «покупают» себе с помощью электронных денег виртуальное оружие, заклинания, всевозможную защиту и другие атрибуты. Отмечены случаи, когда виртуальные ресурсы продаются вполне за реальные деньги. Стоимость таких программ, ворующих пароли от известных игр, может достигать до \$100 тыс. в месяц [17].

Любой бизнес, расширяясь, постоянно ищет новые области своего применения, не является исключением в данном случае и криминальный в сфере интернет. Через сети Интернет продается все больше товаров и предлагается такое же количество услуг, постоянно появляются новые. Преступность оперативно внедряет в них мошеннические схемы из реального мира. Практически во всех случаях мошенники пытаются склонить «клиента» к добровольной сделке и для этого в подавляющем большинстве случаев используют фиктивное занижение цен. Как правило, в таких схемах для привлечения покупателей ставка делается на значительно более низкие цены по сравнению с существующими на потребительском рынке. Вся аргументация таких цен в подобных интернет-магазинах весьма и весьма сомнительна. Но многие «покупатели» верят этим аргументам: «А почему бы не продавать товар дешевле, если он достался им бесплатно!».

Так, например, один из интернет-магазинов на своем сайте предлагал ноутбуки по приемлемой цене, обосновывая это следующими положениями:

- продажа конфиската (таможенный конфискат);
- продажа товаров, купленных по украденным ранее кредитным картам;
- продажа товара, купленного в кредит через подставных лиц [18].

В подобных случаях при заказе товара «клиента» просят внести предоплату, а иногда и заплатить стоимость товара полностью, после чего телефоны или адреса преступников перестают отвечать, а деньги, безусловно, никто не воз-

вращает. При этом способы злоупотребления доверием покупателя весьма разнообразны. Например, широко распространена доставка купленного в интернет-магазинах товара с помощью курьеров. В этом случае мошенники могут требовать предоплату только за доставку, аргументируя свое требование тем, что курьер часто приходит по адресу, где никто ничего не заказывал, и затраты на курьера приходится покрывать интернет-магазину. В этом случае покупатель оплачивает затраты за доставку, а товар, естественно, не доставляется и др.

Такие интернет-магазины – это далеко не единственные ловушки для обманутых граждан. В качестве очередного примера можно рассмотреть еще один из «проектов» мошенников, когда «клиенту» предлагают вложить определенную сумму денег под очень привлекательный процент [19]. В один момент люди, доверяющие таким «инвестиционным» сайтам, превращаются из «инвесторов» в обманутых вкладчиков.

Способов мошенничества и здесь предостаточно: постоянно обнаруживаются ложные обменные сайты для электронных денег, клиенты которых также лишаются своих средств, периодически появляются интернет-пирамиды (аналог сетевого маркетинга из реального мира), рассылается «спам» о существовании секретных специализированных электронных кошельков, которые удваивают или утраивают полученные суммы и т.д.

Как мы уже сказали ранее, все подобные мошеннические схемы используют менталитет граждан, склонных к легкой наживе [20]. С середины 2006 года в России появились новые вирусные технологии, направленные на вымогательство денег пользователей сети Интернет [21]. Так, появляющийся периодически «информер» выдвигал требование о переводе некому владельцу сайта через СМС-сообщение определенной суммы денег за пользование ресурсами сети, взамен в сообщении гарантировалось восстановление работоспособности неисправного компьютера. Распространялся такой вирус в чатах, на форумах под видом программ, позволяющих получать бесплатную IP-телефонию, бесплатный доступ к сети Интернет, к сотовым коммуникациям, сайтам знакомств и т.д. Достаточно было только «кликнуть» мышкой на появляющийся рекламный баннер, и ты становился очередным «владельцем» вредоносной программы.

Следующие модификации вредоносных программ уже якобы шифровали файлы данных на диске пользователя, не давая ему возможности дешифровать их самостоятельно. Восстановление информации было платным, каталоги с зашифрованными данными содержали файл «readme.txt» со следующим содержанием: «Some files are coded by RSA method. To buy decoder mail: xxxxxxxx@yandex.ru with subject: RSA 5 68251593176899861». Несмотря на сообщение об использовании RSA-алгоритма шифрования, мошенник на самом деле использовал обычное симметричное шифрование, что делало восстановление данных не столь сложным. Эта вредоносная программа сопровождалась сменой алгоритма шифрования и постоянным увеличением его сложности. Сумма выкупа для различных версий варьировалась от 30 до 70 \$. Распространялся вирус с помощью спам-рассылки.

Семейство «программ-вымогателей» активно росло (Daideneg, Schoolboys, Cryzip, MayArchive и др.), ширилась география их применения: подобные вредо-

носные программы были обнаружены в Великобритании, Германии, России и других странах.

К сожалению, мы вынуждены констатировать, что рыночная экономика инициирует появление все новых и новых методов, форм, способов криминального обогащения, совершаемых с использованием интернет технологий, а наличие собственности, денежных средств у граждан, их персональные данные, менталитет и другие факторы определяют вектор ее развития. Почему же в сфере интернет технологий такие преступления, как вымогательство, мошенничество, кража и другие, так популярны среди лиц, их совершающих? Ответ на этот вопрос банален: в надежде восстановить утерянные или испорченные данные, «заработать» не прилагая больших усилий, получить максимум удовольствия при минимуме затрат, пользователи сети согласны выполнить любые условия «доброжелателей». Предрасположенность пользователей сети Интернет к «добровольной» передаче своих персональных данных, халатность и небрежность при работе во всемирной паутине зачастую является инициирующим фактором преступного обогащения злоумышленников и намного осложняет процесс привлечения к ответственности мошенников.

Практика осуществления ОРД по установлению мошенников может идти и по-разному. Например, установлением данных о том, куда были направлены преступниками списанные средства и (или) как он были использованы [22]:

- средства направлены на конкретные банковские счета;
- средства зачислены на лицевые счета абонентов сотовой связи;
- средства поступили на «электронные кошельки» платёжных систем;
- средства перечислены в счёт оплаты товаров (работ, услуг) и др.

Трудности могут возникнуть, если похищенные средства были переведены ещё раз на другой счёт или на счет банка в иностранном государстве. В этом случае с одновременным предоставлением материалов следователю необходимо направить запрос по линии Интерпола. Если же деньги были переведены на территории России и в дальнейшем обналичены, то необходимо проводить оперативно-розыскные мероприятия в отношении лица, обналичившего средства, так как оно и будет причастно к совершённому преступлению.

Учитывая огромную общественную опасность, выраженную латентность, сложность расследования преступлений, совершаемых в сфере телекоммуникационных технологий, каковой является и сеть Интернет, а также имеющийся мировой опыт, особое внимание, на наш взгляд, необходимо уделять вопросам предупреждения мошеннических действий. Для этого необходимо активно информировать население о новых способах, формах и методах криминального обогащения через ресурсы сети Интернет. Правоохранительным органам необходимо постоянно совершенствовать оперативно-розыскную деятельность, направленную на защиту чести и достоинства, жизни и здоровья граждан от преступных посягательств, а для этого разрабатывать эффективные правовые, организационные и технические меры защиты интеллектуальной собственности.

1. Комплексный анализ состояния преступности в Российской Федерации по итогам 2019 года и тенденции ее развития: аналитический обзор. ФГКУ «ВНИИ МВД России», 2020.

2. Социальная инженерия – это метод управления действиями человека без использования технических средств воздействия. Метод основан на использовании психологических особенностей человека, его восприятии окружающей среды и нравственного состояния.

3. С помощью услуги «Онлайн-Банкинг» клиенты Банка могут в режиме реального времени контролировать состояние своих счетов.

4. Интернет-аукцион (он же «онлайновый аукцион») – аукцион, проводящийся посредством интернета. В отличие от обычных аукционов, интернет-аукционы проводятся на расстоянии (дистанционно) и в них можно участвовать не находясь в определённом месте проведения, делая ставки через интернет-сайт или компьютерную программу аукциона.

5. Аккаунт – это учётная запись, где хранится персональная информация пользователя для входа на сайт.

6. Интернет-пейджер, то есть программа для моментального обмена сообщениями, главной функцией которого является вызов заданного пользователя (этот процесс состоит из двух стадий – определения доступности пользователя и установления канала связи).

7. Левин М. Хакинг с самого начала: Методы и секреты. М.: Бук-пресс, 2006. С. 34.

8. FTP (англ. File Transfer Protocol – протокол передачи файлов) – протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам и просматривать содержимое каталогов, загружать файлы с сервера или на сервер, передавать файлы между серверами.

9. Провайдер (англ. Internet Service Provider, ISP, букв. «поставщик Интернет-услуги») – организация, предоставляющая услуги доступа к Интернету и иные связанные с Интернетом услуги.

10. Фёшинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

11. Эксплойт (брешь в безопасности) – это компьютерная программа или скрипт, использующий специфические уязвимости операционной системы, с помощью которых могут быть получены расширенные права доступа.

12. URL: www.iframedollars.biz.

13. Электронные платежные системы – это технологии, позволяющие производить расчеты напрямую между контрагентами с помощью электронной связи.

14. Интернет-магазин (электронный магазин) – это каталог товаров, в котором перечислены свойства (характеристики) каждого товара, имеются фотографии, и, конечно, указана цена. В электронном магазине вы ищете необходимые товары и формируете свой заказ, а так же вводите информацию, необходимую для оплаты, времени и места доставки выбранных товаров. Доставка осуществляется курьером или почтой.

15. URL: <https://zen.yandex.ru/media/anosistema/ia-uvidel-strannuiu-vakansiiu-kto-takie-dropy-i-pochemu-im-tak-mnogo-platiat-5bf61b52cb2c6900aa3f094e>.

16. Спам (англ. spam) — массовая рассылка коммерческой, политической и иной рекламы (информации) или иного вида сообщений лицам, не выразившим желания их получать.

17. URL: https://safe.cnews.ru/news/top/2017-12-19_na_prodazhe_uchetnyh_zapisej_polzovatelej_haker.

18. URL: http://www.securelist.com/ru/images/vlpub/0610_bmw_pic4.png.

19. URL: http://www.securelist.com/ru/images/vlpub/0610_bmw_pic3.png.

20. Менталитет [от лат. mens, mentis – ум и alis – другие] – система своего образа психической жизни людей, принадлежащих к конкретной культуре, качественная совокупность особенностей восприятия и оценки ими окружающего мира, имеющие надситуативный характер, обусловленные экономическими, политическими, историческими обстоятельствами развития данной конкретной общности и проявляющиеся в своеобразной поведенческой активности.

21. Волков Ю.В. Телекоммуникационное право: учебное пособие. Екатеринбург, 2008. С. 17.

22. Определить провайдера можно по специальной поисковой системе в сети Интернет по адресу: www.whois-service.ru. Сначала на интернет-странице сайта в поисковую строку вводится IP-адрес, затем на обновлённой интернет-странице необходимо «кликнуть» IPLookup, ещё раз ввести в поисковую строку тот же IP-адрес, после чего система выдаст ответ о данных провайдера, который предоставил соответствующий адрес. Для европейской части сети действует поисковая система по адресу: WWW.RIPE.NET.

Сборник статей

**АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ
В СОВРЕМЕННЫХ УСЛОВИЯХ**

Свидетельство о государственной аккредитации

Рег. № 2660 от 02.08.2017.

Подписано в печать 28.05.2020. Формат 60х90¹/₁₆.

Усл. печ. л. – 5. Тираж 22 экз. Заказ № 86.

Орловский юридический институт МВД России имени В.В. Лукьянова.
302027, г. Орел, ул. Игнатова, 2.