



Министерство внутренних дел Российской Федерации

**Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова**

АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Сборник научных статей

**Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2023**

Министерство внутренних дел Российской Федерации

**Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова**

**АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ
ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

Сборник научных статей

**Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2023**

УДК 351.745.7
ББК 67.99(2).94
А43

Редакционная коллегия:

кандидат юридических наук, доцент Д.Ф. Флоря (председатель);
С.В. Екимцев (заместитель председателя);
кандидат исторических наук И.М. Смирнов, А.Г. Лисицын;
кандидат юридических наук Д.В. Кураков (ответственный секретарь)

А43 Актуальные вопросы осуществления оперативно-разыск-
ной деятельности органов внутренних дел : сборник научных ста-
тей / редкол.: Д.Ф. Флоря [и др.]. – Орловский юридический инсти-
тут МВД России имени В.В. Лукьянова. – ОрЮИ МВД России имени
В.В. Лукьянова, 2023. – 93 с.
ISBN 978-5-88872-320-3

В сборник включены материалы Всероссийского круглого стола «Актуальные проблемы теории и практики оперативно-разыскной деятельности» и другие научные статьи по обозначенной тематике.

Материалы публикуются в авторской редакции.

УДК 351.745.7
ББК 67.99(2).94

ISBN 978-5-88872-320-3

© ОрЮИ МВД России имени В.В. Лукьянова, 2023

Содержание

Батоев В.Б.

О некоторых вопросах противодействия незаконному обороту специальных технических средств, предназначенных для негласного получения информации 5

Белевский Р.А.

Проблема обеспечения конфиденциальности в области интернета вещей .. 8

Венидиктов М.И., Гущина С.В.

Некоторые особенности оперативно-розыскной характеристики дистанционного мошенничества с использованием сети интернет и средств связи..... 12

Екимцев С.В.

Квалифицированные виды мошенничества и их характеристика 21

Ефремова О.М., Чикина П.В.

Криминалистическое исследование мессенджеров whatsapp и viber с целью получения информации ориентирующего характера для производства экспертиз 27

Гришин Д.А.

Раскрытие преступления как задача уголовного судопроизводства 31

Журбенко А.М., Озеров И.Н.

Некоторые проблемы расследования доведения до самоубийства посредством сети интернет 34

Климачков А.В., Горшкова В.С.

К вопросу об использовании СЭД ИСОД МВД России при проведении ОРМ «исследование предметов и документов»..... 41

Крысина Т.Е., Смирнов И.М.

Актуальные проблемы раскрытия преступлений в сфере интеллектуальной собственности..... 46

Кураков Д.В., Некрасов М.А.

Особенности организации раскрытия и расследования преступлений «по горячим следам»..... 49

Лисицын А.Г.

К вопросу об оперативно-розыскной характеристики краж и угонов транспортных средств..... 53

Малик В.И.

Краткий обзор всемирного доклада о наркотиках за 2023 год управления по наркотикам и преступности ООН..... 58

Митряев И.С.

Проблемы защиты персональных данных на современном этапе 62

Поддубный И.В.

Отдельные аспекты деятельности подразделений уголовного розыска по раскрытию убийств..... 66

Рощупкина А.В.

Совершенствование деятельности оперативных подразделений ОВД
по раскрытию взяточничества 71

Смирнов И.М.

«Скамминг» как новый вид современного интернет-мошенничества 75

Сущенко С.А.

Использование результатов специальных следственных мероприятий
в уголовно-процессуальном доказывании зарубежных стран..... 79

Чаплыгина В.Н., Батуева А.Б.

Особенности производства следственных действий, проводимых
на последующем и заключительном этапах расследования преступлений,
совершенных несовершеннолетними, в силу их вовлечения в них..... 84

Батоев В.Б.

О НЕКОТОРЫХ ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ НЕГЛАСНОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Аннотация. В современных условиях интенсивного развития информационных технологий и всеобщей цифровизации общественной жизни продолжают вызывать тревогу и озабоченность действия криминалитета, связанные с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации. На всех уровнях организации правоохранительной деятельности пристальное внимание уделяется вопросам совершенствования противодействия данному негативному социальному явлению. В работе представлены официальные статистические сведения, недостатки различного характера, устранение которых предлагается рассматривать направлениями совершенствования искомого направления деятельности.

Протекающие бурные технологические процессы в условиях четвертой промышленной революции придали цифровой информации, методам ее добывания, обработки, хранения и передачи качественно иное значение. Развитие современного общества в сложившихся условиях информатизации неразрывно связало процессы организации общественных процессов с информацией, где ключевая роль отведена вопросам ее оборота в цифровом пространстве.

На этом фоне на всех уровнях организации правоохранительной деятельности с иной остротой стали восприниматься аспекты обеспечения информационной безопасности как граждан, так и общества в целом в виду постоянно совершенствующихся методов и средств совершения противоправных деяний в цифровой среде. Об этом свидетельствует практика, примеры которой явно указывают на сложившуюся напряженную ситуацию по линии нарушений прав граждан в сфере частной жизни посредством использования и применения технических средств, целью создания которых является получение различной информации на негласных началах. Не смотря на то, что основным предназначением подобных устройств является обеспечение безопасности от преступных посягательств, последние нашли активное применение при решении криминальных задач, что обусловило функционирование незаконного оборота специальных технических средств, предназначенных для негласного получения информации.

Вопросам противодействия незаконному обороту специальных технических средств, а также их использованию в криминальных целях посвящен целый ряд научных трудов. Изучение юридической литературы

показывает, что к числу основных проблем противодействия данному негативному социальному явлению относится следующее:

- отсутствие разъяснений законодательно закрепленного определения термина «специальные технические средства, предназначенные для негласного получения информации» [1; 2, с. 34-35; 3];
- проблемы определения умысла на использование специальных технических средств в целях негласного получения информации [4, с. 10-12];
- неоднозначное понимание сути действий в рамках объективной стороны данного состава преступления и оснований, исключающих преступность деяния [5; 6, с. 195];
- несоответствие меры наказания за совершение рассматриваемого вида преступлений [7, с. 276-277; 8, с. 97], а также категории преступления [9, с. 111];
- проблемы, связанные с проведением радиотехнической экспертизы [10].

С учетом изложенных проблем, устранение которых, мы, безусловно, предлагаем рассматривать в качестве направления совершенствования правоохранительной деятельности, обозначим современную ситуацию, сложившуюся в сфере незаконного оборота специальных технических средств, предназначенных для негласного получения информации, которая наглядно продемонстрирована в представленной ниже таблице.

Таблица 1. Сведения о состоянии преступности в сфере незаконного оборота специальных технических средств, предназначенных для негласного получения информации

Федеральный округ	Количество преступлений, зарегистрированных в отчетном периоде (2021 год / 2022 год / 6 месяцев 2023 года)	Выявлено лиц, совершивших преступления (2021 год / 2022 год / 6 месяцев 2023 года)
ЦФО	43/53/19	29/42/12
СЗФО	6/4/5	4/4/4
СКФО	10/8/1	10/8/1
ЮФО	16/19/9	13/14/1
ПФО	32/36/12	24/28/14
УФО	21/8/6	19/7/3
СФО	16/18/7	21/15/3
ДФО	9/19/8	12/20/7
Всего по России	164/169/71	137/141/59

Представленные данные в таблице свидетельствуют о росте числа зарегистрированных преступлений в сфере незаконного оборота специальных технических средств, предназначенных для негласного получения информации. При этом с учетом из данных, представленных в таблице, виден

рост числа выявленных лиц, причастных к рассматриваемому виду преступлений.

Подводя итоги, отметим, что должная организация процесса противодействия указанному виду противоправной деятельности в современных условиях информатизации имеет важное значение. Правоохранительным органам следует обратить пристальное внимание на вопросы совершенствования данного направления деятельности, с учетом предложенных выше направлений. Полагаем, что представленные в работе официальные статистические данные о состоянии преступности в искомой сфере имеют практическое значение и будут востребованы при проведении научных исследований.

-
1. Афанасьев Е.В. Актуальные проблемы расследования незаконного оборота специальных технических средств, предназначенных для негласного получения информации // Криминалистика и судебно-экспертная деятельность: теория и практика: материалы V Всероссийской научно-практической конференции, 2017. С. 15-18.
 2. Афанасьев Е.В. Некоторые аспекты в расследовании преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации // Криминалистика: актуальные вопросы теории и практики: сборник материалов Международной научно-практической конференции / ответственный редактор В.В. Осяк, 2019. С. 34-39.
 3. Афанасьев Е.В. Актуальные вопросы оперативно-розыскного противодействия незаконному обороту специальных технических средств, предназначенных для негласного получения информации // Актуальные проблемы криминалистики и судебной экспертизы: материалы международной научно-практической конференции, 2020. С. 8-10.
 4. Земцова А.В. К вопросу о перспективах совершенствования механизма противодействия незаконному обороту специальных технических средств, предназначенных для негласного получения информации // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. 2018. № 4 (48). С. 9-16.
 5. Кегадуев М.З., Далакян Г.А., Николинкин С.А. Проблемы противодействия незаконному обороту специальных технических средств, предназначенных для негласного получения информации // Инновационные аспекты развития науки и техники: сборник избранных статей II Международной научно-практической конференции, 2020. С. 137-143.
 6. Марков Е.А. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации: проблемы квалификации // Научный Альманах ассоциации France-Kazakhstan. 2022. № 3. С. 188-198.

7. Полуянова Е.В., Ковалев С.Д., Курысев К.Н. Нормативное правовое регулирование незаконного оборота специальных технических средств, предназначенных для негласного получения информации // Актуальные проблемы публичного права: сборник научных трудов IV Международной научно-практической конференции. Владимир, 2023. С. 268-277.
8. Полуянова Е.В. Отдельные вопросы нормативного правового регулирования незаконного оборота специальных технических средств, предназначенных для негласного получения информации, в Российской Федерации // Вестник Владимирского юридического института. 2022. № 4 (65). С. 93-98.
9. Решняк М.Г. Современные проблемы уголовной ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации // Пробелы в российском законодательстве. 2019. № 6. С. 109-112.
10. Ржанникова С.С. О возможностях радиотехнической экспертизы в раскрытии и расследовании некоторых преступлений // Научный дайджест Восточно-Сибирского института МВД России. 2019. № 3 (3). С. 172-177.

СВЕДЕНИЯ ОБ АВТОРЕ

Батоев Владимир Батоевич. Кандидат юридических наук, доцент. Старший научный сотрудник.

ФКУ НПО «Специальная техника и связь» МВД России.

111024, г. Москва, ул. Пруд Ключики, д. 2.

Ключевые слова: незаконный оборот, специальные технические средства, негласное получение, информация.

Белевский Р.А.

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ В ОБЛАСТИ ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. Статья рассматривает проблему обеспечения конфиденциальности в интернете вещей. В статье обсуждаются факторы, влияющие на конфиденциальность, а также предлагаются решения для ее обеспечения, такие как шифрование данных, улучшение безопасности продуктов IoT и повышение осведомленности пользователей.

Интернет вещей (IoT) представляет собой сеть физических объектов, подключенных к интернету, которые могут обмениваться данными между собой. Однако, так как эти объекты могут содержать личную информацию:

геолокационные данные, информацию о здоровье и т.д., возникает риск нарушения конфиденциальности.

Термин «Интернет вещей» определен как динамическая глобальная сетевая инфраструктура с возможностью самонастройки на основе стандартных и совместимых протоколов связи, где физические и виртуальные «вещи» имеют идентификаторы, физические атрибуты, используют интеллектуальные интерфейсы и интегрируются в информационную сеть.

Интернет вещей является быстроразвивающейся областью, которая становится все более распространенной в нашей жизни. Однако с этим возникает риск нарушения конфиденциальности, так как объекты IoT могут содержать личную информацию. Проблема обеспечения конфиденциальности в IoT может быть вызвана несколькими факторами, такими как хакерские атаки, уязвимости системы и недостаточная осведомленность пользователей. В этой статье мы рассмотрим эти факторы и предложим решения для обеспечения конфиденциальности в IoT, такие как шифрование данных, улучшение безопасности продуктов IoT и повышение осведомленности пользователей.

В течение последнего десятилетия Интернет вещей проникал в нашу жизнь тихо и постепенно, прежде всего благодаря наличию систем беспроводной связи (например RFID, Wi-Fi, 4G, IEEE 802.15.x), которые все чаще используются в качестве движущей силы для развития технологии интеллектуального контроля и управления приложениями.

Концепция IoT включает в себя множество различных технологий, услуг, стандартов и воспринимается как краеугольный камень на рынке информационно-коммуникационных технологий (ИКТ) по крайней мере на ближайшие десять лет.

В сфере интернета вещей (IoT) персональные данные могут появляться в разных местах, особенно когда пользователь попадает в зону действия датчиков. Например, биометрические данные могут быть записаны и обработаны при использовании датчиков. В таких случаях, при помощи дополнительных признаков, идентифицируемое лицо может быть точно определено. Но не все записанные данные имеют прямую связь с личностью. Например, «умный» детектор движения, установленный во входной зоне торгового центра и передающий измеренную информацию о движении в центр обработки данных, который контролирует и открывает входные двери в часы работы, не обрабатывает никаких персональных данных.

Кроме того, персональные данные могут возникать при использовании мобильных приложений IoT. В будущем многие из этих приложений будут иметь функции распознавания пользователей, так как приложение IoT или связанная с ним услуга должна предоставляться на личной основе и, соответственно, требовать личной аутентификации. Например, для использования интеллектуальных весов, может потребоваться создание учетной записи пользователя, чтобы данные измерений можно было синхрони-

зировать с облаком поставщика услуги. Для осуществления бесконтактных платежей со смартфона с использованием технологии NFC, необходима аутентификация в фоновом режиме с использованием личных данных.

Чтобы сохранить информационное самоопределение и конфиденциальность в IoT, необходимо разрабатывать и внедрять общие подходы к обработке и хранению данных на всех уровнях. Важно повышать уровень безопасности продуктов IoT, использовать шифрование данных и улучшать осведомленность пользователей. Внедрение этих мер позволит создать более безопасную и защищенную среду IoT в будущем. Однако необходимо отметить, что обеспечение конфиденциальности в Интернете вещей является сложной задачей, требующей комплексного подхода и использования передовых технологий. Ответственность за защиту персональных данных в Интернете вещей лежит на производителях устройств, разработчиках программного обеспечения и провайдерах услуг связи, а также на самих пользователях, которые должны быть внимательны при использовании устройств и сервисов IoT.

Вот несколько примеров нарушения конфиденциальности в области интернета вещей:

1. Утечка персональных данных через несанкционированный доступ к умным устройствам. Например, в 2019 году было сообщено, что компания Ring (производитель умных дверных звонков) допустила утечку данных пользователей, которые были доступны через интернет.

2. Нарушение конфиденциальности здоровья пациента через утечку данных из медицинских устройств IoT. Например, в 2020 году было сообщено, что компания Philips допустила утечку медицинских данных пациентов через уязвимости в своих устройствах IoT.

3. Отслеживание личной жизни через утечку данных из умных домов и умных гаджетов. Например, в 2021 году было сообщено, что приложение Xiaomi допустило утечку данных пользователей, которые были доступны через умные камеры в домах.

4. Нарушение конфиденциальности в бизнесе через утечку данных из умных устройств в офисах и на производстве. Например, в 2018 году было сообщено, что компания Tesla допустила утечку конфиденциальных данных своих производственных процессов через умные устройства в своих заводах.

Проблема обеспечения конфиденциальности в IoT может быть вызвана несколькими факторами:

Во-первых, объекты IoT могут быть подвержены хакерским атакам, что может привести к утечке личной информации.

Во-вторых, производители IoT могут не уделять достаточного внимания безопасности и конфиденциальности при разработке продуктов, что может привести к уязвимостям в системе.

В-третьих, сам пользователь может не понимать, как защищать свою личную информацию, оставляя ее уязвимой для злоумышленников.

Одним из способов решения этой проблемы является использование шифрования для защиты данных, передаваемых между объектами IoT. Шифрование данных может предотвратить их попадание в руки злоумышленников и обеспечить конфиденциальность передачи.

Кроме того, важно, чтобы производители IoT уделяли больше внимания безопасности и конфиденциальности при разработке своих продуктов. Это может включать в себя использование безопасных протоколов передачи данных, регулярное обновление программного обеспечения и аудит системы на наличие уязвимостей.

Наконец, пользователи IoT должны быть более осведомлены о том, как защищать свою личную информацию. Это может включать в себя использование сильных паролей и двухфакторной аутентификации, а также ограничение доступа к личной информации.

В заключение можно сказать, что обеспечение конфиденциальности является критически важным вопросом в области интернета вещей. Несмотря на то, что многие продукты IoT были разработаны с учетом безопасности и конфиденциальности, эта область продолжает оставаться уязвимой для кибератак и других угроз. Чтобы обеспечить конфиденциальность в IoT, необходимо сделать шаги в направлении улучшения безопасности продуктов, использования шифрования данных и повышения осведомленности пользователей. Все эти меры будут способствовать созданию более безопасного и защищенного интернета вещей в будущем.

СВЕДЕНИЯ ОБ АВТОРЕ

Белевский Роман Александрович. Кандидат юридических наук. Старший преподаватель кафедры информационных технологий в деятельности органов внутренних дел.

Орловский юридический институт МВД России имени В.В. Лукьянова

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: интернет вещей, конфиденциальность, безопасность, шифрование, уязвимости, осведомленность пользователей.

НЕКОТОРЫЕ ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ И СРЕДСТВ СВЯЗИ

Аннотация. В настоящей статье рассмотрены некоторые особенности оперативно-розыскной характеристики. Описана уголовно-правовая характеристика преступлений, относящихся в рамках данной статьи к дистанционному мошенничеству. Рассмотрены актуальные способы совершения дистанционного мошенничества и выявлены основные проблемы совершения описанного противоправного деяния.

Для того чтобы выделить оперативно-розыскную характеристику (далее – ОРХ) дистанционного мошенничества необходимо понять, что в неё входит, так как на настоящий момент не сформировано единое толкование данному понятию. По мнению В.Д. Ларичева, ОРХ является научно разработанная система обобщенных данных о наиболее типичных оперативно значимых признаках преступлений [1]. По мнению Р.В. Кондрашечкина и А.А. Никонорова, ОРХ преступлений должна различаться друг от друга в силу рассмотрения отдельных видов преступлений [2]. По мнению А.М. Абрамова и И.А. Климова, в содержание ОРХ должны входить характеристики с позиций иных отраслей знаний, например, таких как криминалистическая, уголовно-правовая, уголовно-процессуальная, криминологическая, социологическая, экономическая и другие [3]. Стоит заметить, что мы абсолютно согласны с мнением А.М. Абрамова и И.А. Климова, но, по нашему мнению, в ОХР необходимо включить оперативную обстановку оперативно-розыскные признаки преступной активности, то есть ОРХ – это совокупность уголовно-правовой, уголовно-процессуальной, криминалистической, криминологической и оперативной характеристик.

Заметим, для того чтобы грамотно отразить ОРХ и квалифицировать противоправное деяние необходимо выделить уголовно-правовые элементы состава дистанционного мошенничества. Дистанционное мошенничество включает в себя составы преступлений, регулируемых ст. 159, 159.3, 159.6 Уголовного кодекса Российской Федерации. Уголовно-правовая характеристика заключается в выделении состава преступления, который состоит из объективных и субъективных признаков. Рассмотрим данные элементы в рамках нормы ст. 159.6 Уголовного кодекса Российской Федерации.

Квалифицирующие признаки [4]:

– совершенное группой лиц по предварительному сговору, а равно с причинение значительного ущерба;

- совершенное лицом с использованием своего служебного положения, а равно в крупном размере;
- совершенное организованной группой либо в особо крупном размере или повлекшее лишение права гражданина на жилое помещение;
- сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние повлекло причинение значительного ущерба;
- сопряженное с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние совершено в крупном размере.

По нашему мнению, следует разграничить составы преступлений в соответствии с постановлением Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [5]. Рассмотрим, как необходимо квалифицировать действия злоумышленников в зависимости от приведенных ситуаций.

В случае, когда потерпевший в ходе Интернет смс-сообщения или телефонного разговора сообщает преступнику значимую информацию по банковскому счету например, номер банковской карты, срок действия, CVV-код, содержание смс-сообщений банка с кодами подтверждающие действия по карте и злоумышленник использует полученную информацию для доступа к счету потерпевшего (например, путем входа в приложение «Сбербанк Онлайн», «ВТБ», «Тинькофф», «Р2Р») и похищает денежные средства, находящиеся на счете потерпевшего, то есть преступник похищает их самостоятельно. Данное преступное посягательство следует квалифицировать по п. «г», ч. 3, ст. 158 УК РФ, в соответствии с п. 21 Постановлением Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», а именно: «В тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным, такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети» [5].

В случае, когда сам потерпевший переводит электронные денежные средства через устройства самообслуживания либо в качестве предоплаты за приобретаемый товар, услугу путем использования фишингового сайта, либо в качестве взятки за «непривлечение близкого к ответственности», либо за «ошибочно» полученный перевод, который не числится в переводах, либо по просьбе преступника переводит денежные средства для «пополнения счета на карте» или «баланса телефона», либо по просьбе друга по переписке в социальной сети (в данном случае страницу друга потерпевшего в социальной сети взламывают для того чтобы войти в доверие).

Такие действия следует квалифицировать по ст. 153.3 Уголовного кодекса Российской Федерации, то есть мошенничество с использованием электронных средств платежа, и в зависимости от суммы причиненного ущерба будет соответствующая часть данной статьи.

В данном случае обязательным условием совершения данного преступного деяния будет являться перевод денежных средств непосредственно самим потерпевшим злоумышленнику. Данная квалификация основывается на п. 2 Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [5] и на Федеральном законе от 27.06.2011 № 161-ФЗ «О национальной платежной системе» [6], где указывается понятие электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. Ключевой фразой в данном определении является «позволяющие клиенту оператора», то есть злоумышленник путем обмана потерпевшего получает его денежные средства.

Необходимо заметить, что 29.06.2021 были реализованы изменения в Пленуме Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», данные изменения затронули вопросы квалификации преступных посягательств. В настоящий момент в случае если злоумышленник получил доступ к конфиденциально информации о персональных данных владельца карты или непосредственный доступ к данным платежной карты переданной под воздействием обмана, либо он осуществил при помощи похищенных данных осуществил обналичивание электронных денежных средств через специальные банкоматы, поддерживающих функцию «Pay touch» («Apple Pay», «Android Pay»), то данные действия квалифицируются как кража (п. «г» ч. 3 ст. 158 УК РФ), в предыдущей версии Пленума Верховного Суда Российской Федерации данные действия расценивались по ст. 159.3 Уголовного кодекса Российской Федерации.

В случаях, когда злоумышленник целенаправленно воздействует на программное обеспечение электронных устройств в целях незаконного завладения чужим имуществом, то данные действия квалифицируются по ст. 159.6 УК РФ, если данные действия совершены посредством создания, использования и распространения вредоносных компьютерных программ, то требуется дополнительная квалификация по ст. 272, 273 или 274.1 УК РФ.

В случаях создания поддельных благотворительных сайтов, интернет-магазинов и распространение другой ложной информации в сети «Интернет», то квалифицируется данное деяние по ст. 159 УК РФ.

Безусловно, необходимо рассмотреть криминалистическую характеристику. Типовую криминалистическую характеристику преступлений можно определить, как систему данных о криминалистически значимых признаках преступлений конкретного вида или группы, отражающих закономерные связи между этими признаками, и служащую построению типовых версий, которые берутся за основу при планировании расследований преступлений данного вида или группы [7].

Рассмотрим все элементы криминалистической характеристики дистанционного мошенничества совершенного при помощи сети интернет и средств связи. Непосредственным предметом преступного посягательства данного преступления является денежные средства в безналичной форме. Большинство дистанционных мошенничеств осуществляется при помощи сети «Интернет» и средств связи. Взломы страниц в социальных сетях или получение доступа злоумышленников к данным банковской карты/счета в большинстве случаев возникает не из-за каких-либо технических недостатков, а из-за цифровой неграмотности населения. Под цифровой неграмотностью населения следует понимать знания, умения, навыки при обращении с информационно-телекоммуникационными технологиями, а также навыки поиска, анализа информации в сетевом пространстве (сеть «Интернет»). Из-за недостаточной осведомленности граждан о возможных действиях злоумышленников в информационном пространстве, данная категория лиц подпадает в список потенциальных «жертв», так как преступникам будет легко убедить человека в совершении тех или иных действий, которые приведут к похищению их денежных средств.

Необходимо отметить, что злоумышленник может воздействовать как на саму компьютерную систему, так и на человека путем социальной инженерии. То есть преступник при осуществлении своего замысла определяет путь достижения поставленной цели:

- 1) путем взлома персонального компьютера или иного электронного устройства при помощи специальных знаний и умений в области информационных технологий;
- 2) при помощи методов социальной инженерии.

Рассмотрим осуществление фишинга при помощи электронных писем. В настоящее время мошенники используют специальное техническое обеспечение, которое позволяет злоумышленникам быстро создавать множество поддельных электронных адресов / почт и рассылать необходимые смс-сообщения / спам-письма. В данных письмах содержится ссылка на фишинговый сайт, который предназначен для сбора конфиденциальных данных, выраженных в виде имен пользователей и паролей. Около 50 % фишинговых сайтов используют технологию HTTPS. HTTPS – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Многие электронные почты сами распознают данные сообщения и не дают случайно открыть или перейти к документу направленном зло-

умышленником, система устроена так, что при поступлении такого сообщения оно направляется в специальную папку под названием «Спам». Рассмотрим это на конкретном примере. На электронную почту пришло смс сообщение от имени willdberis-info с адреса электронной почты bouncee@gardentrading.ru. Необходимо отметить, что в настоящее время одним из популярных интернет-магазинов является Wildberries, но их официальный адрес электронной почты совершенно иной sales@wildberries.ru. Таким образом можно утверждать, что после открытия данного прикрепленного файла в электронном сообщении злоумышленник получит данные с электронного устройства, с которого его скачают.

Из-за большого количества данных сообщений даже электронные почты не всегда опознают сообщения-спам, в свою очередь злоумышленники все лучше маскируют данные виды электронных писем, что не всегда удастся выявить вредоносное программное обеспечение, встроенное в сообщения. Около 30 % пользователей открывают фишинговые сайты, а 12 % из них кликают на файлы с вредоносным программным обеспечением или на ссылки, которые позволяют злоумышленнику заполучить конфиденциальные данные.

Следующим рассматриваемым видом фишинга является рассылка текстовых сообщений. Данный вид распространяется только на устройства, поддерживающие сим-карты (на планшет, смартфон, мобильный телефон, электронные часы и другие устройства). Потерпевший получает текстовое сообщение, в котором указываются какие-либо «выгодные» для потерпевшего предложения (например, данными предложениями могут быть выигрыш в лотерею, участие в конкурсе, где большой процент выигрыша, большие скидки на какие-либо услуги и другие) и указывается ссылка, по которой необходимо перейти, чтобы воспользоваться данным предложением. Переходит потерпевший на зеркальный сайт, то есть сайт, который внешне схож с оригинальным, который предназначен для сбора учетных данных для «входа» в систему, но после того, как потерпевший введет свои личные данные, они напрямую окажутся у злоумышленника.

Следует отметить ещё один из способов совершения дистанционного мошенничества путем распространения ссылок на фишинговые сайты через социальные сети в сети «Интернет». Рассмотрим данный способ на наиболее распространённой социальной сети «ВКонтакте». Злоумышленник путем взлома социальной страницы распространяет смс-сообщения всем друзьям, которые имеются у потерпевшего. В данном смс-сообщении указывается какая-то акция или подарок, который получит пользователь, если перейдет по ссылке ниже. При переходе по ссылке возникает новая вкладка, в которой требуется заново ввести свои учетные данные для входа в социальную сеть «ВКонтакте», но этот сайт является фишинговым, то есть при вводе данных, злоумышленник получит доступ к аккаунту потерпевшего и сможет дальше распространять данные сообщения, а также мо-

жет путем обмана пользователей, являющихся «друзьями» данного пользователя одолжить или попросить перевода денежных средств. При этом злоумышленник пытается пародировать манеру письма пользователя, которого взломал, по ранее написанным сообщениям. Диалог злоумышленника обычно начинается со слов: «Привет, у тебя есть займы деньги?», «(обращается по имени к собеседнику), а можно у тебя попросить 900 рублей буквально на один день?», «Привет, выручить можешь? Скинь на карту 2000р до конца недели верну», «У тебя есть 2000 р на несколько часов» и другие подобные фразы. После того как злоумышленник начал переписываться с собеседником он присылает номер карты, а может для «достоверности» и фотографию самой карты, на которой написаны фамилия и имя пользователя, через которого злоумышленник ведет беседу. При переводе денежных средств посредством мобильного приложения «Сбербанк Онлайн» или другого мобильного приложения банка, не указываются контактные данные получателя, только номер карты, то есть злоумышленник делает все возможное чтобы провести анонимно данную операцию. На просьбы со стороны потерпевшего на счет привязанного номера к данной карте, злоумышленник пытается не отвечать и всячески «уваливать». После того как злоумышленник понимает, что настоящий пользователь понял, что его аккаунт взломали он удаляет все следы своего деяния, то есть удаляет свои сообщения из всех диалогов. Проверить из какого места заходил злоумышленник также не получится, так как в большинстве случаев они пользуются VPN, который позволяет обеспечить анонимность данного преступления.

При рассмотрении дистанционного мошенничества необходимо отметить также способы его совершения с использованием мобильных средств связи. Дистанционное мошенничество при помощи использования средств связи может осуществляться различными способами, рассмотрим одни из них:

1) жертве приходит SMS о том, что её родственник совершил какое-либо противоправное деяние, и для того чтобы не привлечь к ответственности, жертве необходимо перевести денежные средства на соответствующий банковский счет;

2) злоумышленник направляет SMS о том, что со знакомым или другом, родственником случилась беда – это может быть ДТП или нападение преступника, и для того чтобы помочь пострадавшему необходимо перевести денежные средства;

3) злоумышленники предлагают оккультные услуги через информационное пространство, то есть мошенник якобы снимет порчу, приворожит любимого и другое;

4) при использовании интернет-сервиса по размещению объявлений о товарах и услугах (например «Авито», «Юла») злоумышленник списывается с владельцем определённого товара и путем обмана назначает личную

встречу и получение товара через посредника. В свою очередь посредник уточняет данные карты продавца, и мошенник присылает смс-уведомление на телефон под ложным номером банка, но при этом продавец не видит разницы в переводе денежных средств. Вследствие чего мошенник и его посредник получают товар бесплатно, а продавец осознает, что его обманули только когда, зайдет проверить денежные средства на карте;

5) на номер жертвы направляется текстовое сообщение о том, что её карта заблокирована, также в данном смс указан контактный номер для уточнения информации. Жертва звонит по указанному номеру, по нему отвечает «специалист», который с помощью психологических приемов получает доступ к электронным денежным средствам жертвы;

6) мошенник, притворяясь работодателем какой-то «престижной» кампании предлагает жертве свободную вакансию с выгодными условиями. Когда жертва едет на собеседование, то её просят купить что-то и заостряют внимание на сохранность чеков, чтобы потом «возместить ущерб», после покупки работодатель (мошенник) звонит уже повторно и просит пополнить баланс номера «проверяющего» под предлогом, что неожиданно закончились денежные средства и после того как он приедет в кампанию, ему все вернут и возместят. Но в большинстве случаев жертва остаётся с купленным дорогостоящим товаром и понимает, что подверглась преступному посягательству;

7) еще одним способом осуществления данных противоправных действий является смс-рассылка, в которой указывается, что жертва выиграла большой приз и для того чтобы узнать все подробности необходимо связаться по указанному в смс сообщении телефону. После того как жертва связывается по номеру её просят перевести незначительное количество денежных средств для оплаты пересылки. По итогу жертва просто переводит электронные денежные средства, но никакого «приза» она не получает.

Данные преступные посягательства могут осуществляться в любое время и в любом месте, в котором имеется доступ к информационно-телекоммуникационным технологиям и выход к сети «Интернет». Изучение личности преступника позволяет правоохранительным органам эффективно осуществлять поиск лица, осуществляющего дистанционное мошенничество, а также предугадать его последующие действия, что позволит сформировать порядок действий необходимых для раскрытия преступления. Следы данного вида преступления остаются непосредственного на информационно-телекоммуникационных технологиях, при помощи которых было осуществлено противоправное деяние. Также они могут содержаться не только на устройствах, при помощи которых злоумышленник осуществил противоправное деяние, но и на компьютерах, ноутбуках, планшетах, смартфонах и других устройствах потерпевшего, через которые осуществлялась связь со злоумышленником. В основном такие следы являются цифровыми.

Для того чтобы правильно выделить криминологическую характеристику дистанционного мошенничества, совершенного при помощи сети интернет и средств связи, необходимо определить, какие элементы в нее входят. Рассмотрим криминологическую характеристику дистанционного мошенничества, но не будем дублировать информацию, которая пересекается с другими вышеприведенными характеристиками. Личность мошенника, использующего информационно-телекоммуникационные технологии, позволяет правоохранным органам в ходе производства расследования по уголовному делу сузить предполагаемый круг преступников, выполнить разработку потенциальных моделей их поведения, предугадать последующие действия и сформировать порядок действий следствия в ход раскрытия преступления и сбора доказательств в целях их предъявления в суде [8]. Особенностью личности преступника, совершающего дистанционное мошенничество является уровень образования, так как лица могут быть специалистами в области информационно-телекоммуникационных технологий, имеющего высшее образование в данной области, так и дилетантом, то есть человеком, который не обладает большим количеством знаний и навыков в информационной сфере, но обладает техническими навыками в работе с электронными устройствами, но всё равно может осуществлять дистанционно мошенничество, а также существуют работники call-центров, которые в свою очередь могут быть не образованными и не иметь высокого интеллекта, так как их работа заключается в психологическом давлении на человека, которому они позвонили.

Преступников, совершающих дистанционное мошенничество можно поделить на две группы:

- злоумышленники знакомы с жертвой, так как работают вместе или сотрудничают;
- злоумышленники не знакомы с жертвой.

Если рассматривать дистанционное мошенничество, совершенное при помощи сети интернет и средств связи, то большинство данных преступлений совершается в отношении лиц не знакомых преступнику. Данные преступники имеют корыстные мотивы, выраженные в:

- жажде накопления денежных средств;
- стремлении данных лиц к благоприятному материальному обеспечению;
- стремлении к разгульной жизни, которая требует материальных затрат;
- личной материальной нужде;
- а также другие мотивы, связанные с получением денежных средств.

Потерпевшими от данных видов дистанционного мошенничества являются лица, которые имеют электронные денежные средства на счетах в банках и имеют доступ к ним путем использования информационно-

телекоммуникационных технологий. Особенностью личности потерпевшего является низкий уровень цифровой грамотности, что позволяет злоумышленникам легко достигнуть поставленной цели.

Причины совершения дистанционного мошенничества заключаются в человеческих потребностях и доступном способе их удовлетворения. Существует иерархия потребностей человека (по-другому её называют стандартом потребления). Потребности играют большую роль в обществе, так как если будут высокие стандарты потребления тот активнее и динамичнее развивается экономика и общество, но также будет сложнее обеспечить доступность удовлетворения стандартных потребностей для многих – тем выше будет уровень неудовлетворенности граждан, что приведет к увеличению корыстных преступлений.

Таким образом, рассмотрение оперативно-разыскной характеристики дистанционного мошенничества совершенного при помощи сети интернет и средств связи необходимо, так как знание характеристики позволит вовремя принять комплекс необходимых мер по раскрытию преступления.

-
1. Ларичев В.Д. Оперативно-розыскная характеристика экономических преступлений: вопросы теории и практики в современных условиях: научный доклад. М., 2008. С. 9-10.
 2. Кондрашечкин Р.В., Никоноров А.А. Содержание оперативно-разыскной характеристики преступлений [Электронный ресурс] // Вестник экономической безопасности. 2020. № 1. URL: <https://cyberleninka.ru/article/n/soderzhanie-operativno-razysknoy-harakteristiki-prestupleniy> (дата обращения: 26.11.2022).
 3. Абрамов А.М., Климов И.А. К вопросу о содержании оперативно-розыскной характеристики вида преступлений // Актуальные вопросы борьбы с преступностью и проблемы ее преподавания: сб. науч. тр. М., 1996. С. 83-84.
 4. Уголовный кодекс Российской Федерации [Электронный ресурс]: от 13.06.1996 № 63-ФЗ: в ред. от 24.09.2022. Доступ из справ.-правовой системы «КонсультантПлюс».
 5. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда Рос. Федерации от 30.11.2017 № 48: в ред. от 29.06.2021. Доступ из справ.-правовой системы «КонсультантПлюс».
 6. О национальной платежной системе [Электронный ресурс]: Федер. закон Рос. Федерации от 27.06.2011 № 161-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
 7. Криминалистика: учебник для вузов / под ред. А.А. Хмырова, В.Д. Зеленского. Краснодар, 1998. С. 30.
 8. Потапова А.В. Мошенничество в сети интернет: криминологическая характеристика и проблемы квалификации [Электронный ресурс] // StudNet.

2020. № 6. URL: <https://cyberleninka.ru/article/n/moshennichestvo-v-seti-internet-kriminologicheskaya-harakteristika-i-problemy-kvalifikatsii>.

СВЕДЕНИЯ ОБ АВТОРАХ

Венидиктов Михаил Игоревич. Кандидат юридических наук. Старший преподаватель кафедры оперативно-разыскной деятельности и специальной техники.

Московский университет МВД России имени В.Я. Кикотя.
117997, г. Москва, ул. Академика Волгина, д. 12.

Гущина Светлана Владимировна. Дознаватель отделения по расследованию общеуголовных преступлений отдела дознания.

УМВД России по Сергиево-Посадскому городскому округу.
141301, Московская область, г. Сергиев Посад, пр. Красной Армии д. 212/2.

Ключевые слова: уголовная характеристика, мошенничество, дистанционная форма, оперативные подразделения.

Екимцев С.В.

КВАЛИФИЦИРОВАННЫЕ ВИДЫ МОШЕННИЧЕСТВА И ИХ ХАРАКТЕРИСТИКА

Аннотация. В статье на основе проведенного анализа обозначены виды мошенничества. Рассмотрены условия, способствующие совершению квалифицированного мошенничества.

Одним из наиболее распространенных преступных деяний, совершаемых с использованием сети интернет, является мошенничество. Можно отметить, что в условиях развития IT-технологий, традиционные способы совершения мошеннических действий постепенно отходят на второй план [1, с. 210-215].

Среди всех преступных посягательств против собственности специфическое место занимает мошенничество. Оно может непосредственно проявляться во всех сферах жизнедеятельности, быстро адаптироваться к изменяющимся условиям рынка. Потерпевшими от совершения мошенничества могут быть обычные граждане, юридические лица, а также общество в целом, что выступает особенностью этого преступного деяния.

«По темпу роста и своим негативным тенденциям мошеннические посягательства значительно опережает другие преступления против соб-

ственности. Высокий уровень латентности мошенничества, значительный имущественный вред, который причиняется гражданам, юридическим лицам и публичным образованиям, постоянно растущие способы совершения этого преступления определяют серьезность сложившейся ситуации» [2, с. 147-151].

В январе–августе 2023 года сохраняется тенденция к увеличению на 28,7 % количества противоправных деяний в сфере информационно-телекоммуникационных технологий. Их удельный вес в числе всех преступных посягательств возрос до 32,9 %, а по тяжким и особо тяжким – до 56,4 %. Больше совершено дистанционных мошенничеств и краж. Раскрываемость киберпреступлений составила 29,9 %, в том числе совершенных с использованием сети Интернет – 28,8 %, расчетных (пластиковых) карт – 35,7 % [3].

Законодатель не оставил без внимания появление новых видов мошеннических проявлений и внес в уголовный закон соответствующие изменения, результатом которых стало появление специальных видов мошенничества [4].

Анализ содержания уголовного закона, позволяет выделить следующие виды мошенничества:

1. Квалифицированные виды мошенничества:

- совершение мошеннических действий группой лиц по предварительному сговору, или с причинением значительного ущерба гражданину;
- совершение мошенничества с использованием служебного положения, или в крупном размере;
- совершение мошеннических действий организованной группой, или в особо крупном размере, или повлекшее лишение права гражданина на жилое помещение;
- совершение мошенничества, сопряженного с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности, если это деяние повлекло причинение значительного, крупного или особо крупного ущерба.

2. Специальные виды мошенничества:

- совершение мошеннических действий в сфере кредитования;
- мошенничество при получении выплат;
- совершение мошеннических действий с использованием платежных карт;
- мошенничество в сфере страхования;
- совершение мошеннических действий в сфере компьютерной информации [5]. Обратимся к краткому анализу указанных видов мошеннических действий, за совершение которых предусмотрена уголовная ответственность.

Условиями, способствующими совершению квалифицированного мошенничества, являются:

1) Непосредственная потребность потерпевшего получить конкретные объекты материального мира (комплектующие, строительные и иные материалы и т.п.), которые он не может получить нигде, кроме как у мошенников;

2) Необходимость потерпевшего к скорейшей продаже определенных объектов (при скором истечении их срока годности, или износа из-за времени пользования);

3) Необходимость потерпевшего увеличить свои сбережения в возможно короткие сроки за счет вложения своего капитала;

4) Специфика регионально-территориальных условий конкретной местности – уровень безработицы, ценовой уровень, среднестатистический доход и т.д. [6, с. 130-134]

Исследуя квалифицированные составы мошенничества, необходимо опираться на положения постановления Пленума Верховного Суда РФ от 30.11.2017 № 48.

Для удобства определения значительного размера правоприменительной практики законодатель в примечании к ст. 158 УК РФ обозначил размер такой ущерба, который не может составлять менее пяти тысяч рублей. При решении вопроса о значительности ущерба в обязательном порядке должно учитываться мнение потерпевшего, его финансовое положение, наличие у него источника дохода, размер этих доходов, наличие иждивенцев на содержании, а также общий доход семьи при ведении совместного хозяйства.

При определении денежного эквивалента размеру ущерба, причиненного в результате совершения мошеннических действий, следует исходить из рыночной стоимости похищенного имущества на момент совершения преступления. Если таким путем установить размер ущерба не представляется возможным, то проводится исследование, по результатам которого устанавливается размер ущерба и оформляется заключение эксперта или специалиста.

Если в результате совершения мошеннических действий и хищения имущества происходит его подмена, то размер причиненного ущерба определяется исходя из стоимости похищенного, а не подменного имущества.

Квалифицированными видами мошенничества являются совершение мошеннических действий в составе: группы лиц по предварительному сговору, или организованной группой с причинением различного по размеру ущерба.

Как справедливо указывается в научной литературе, совершение преступных деяний в составе группировки независимо от степени ее организованности может размыть границы ответственности каждого участвующего в преступлении лица, а с тактической стороны, это позволяет рас-

пределить участникам этой группы обязанности и облегчить совершение преступного деяния [7, с. 12-18].

Выделяются следующие виды участников преступных групп:

1. Инициаторы преступной схемы – лица, которые создают мошеннические схемы преступного характера, и замышляют совершение одного или нескольких преступных деяний для достижения преступной цели. Они распределяют обязанности между участниками, составляют планы, разрабатывают варианты укрытия и сокрытия похищенного или приобретенного имущества и контролируют действия других, непосредственно сами не участвуя в действиях;

2. Основные исполнители – непосредственно совершают мошеннические действия, связанные с хищением или приобретением имущества, имущественных прав или выгоды имущественного содержания. Они взаимодействуют с потерпевшим, поэтому при контакте они используют маскировку, а потом основательно скрываются;

3. «Зиц-председатели» – это номинальные соучастники преступления. Как правило, такие лица обладают «нестабильный социальный статус (бомжи, алкоголики, наркоманы), дают злоумышленникам лишь свои «личности» за определенную плату, необходимую на удовлетворение элементарных нужд (выпить, поесть, поспать и т.д.). Взамен на плату данные личности вступают в преступные схемы в качестве руководителей подставных фирм, организаций и обществ, своим участием облегчая возможность «заметания» следов организаторами и исполнителями мошеннических схем» [8, с. 28].

Другим квалифицированным видом мошенничества является совершение преступных действий лицом с использованием своего служебного положения. Выделение такого способа в отдельный вид мошеннических действий, носящий квалифицированный характер, вполне обоснованно, поскольку такие лица обладают особыми знаниями в конкретном виде деятельности, у них имеются определенные полномочия, что облегчает процесс хищения или присвоения имущества, выгоды имущественного содержания или имущественных прав.

Как обозначается в юридической литературе, этот вид мошеннических действий должным образом нормативно не регламентирован, поскольку присутствует только обозначение субъектов служебного мошенничества, и отсутствуют разъяснения относительно сущности использования служебного положения. Такая позиция законодателя является односторонней, не раскрывающей механизм использования такого положения [9, с. 281-290].

Как справедливо отмечается, исследование этого вида предполагает определение круга субъектов и характера использования их положения (правовыми возможностями, видом полномочий исходя из занимаемой должности) [10, с. 18-23]. Безусловно, наличие у виновного определенных

полномочий облегчает способ совершения преступного деяния, так как у него имеется доступ к официальным документам, компьютерной сети и др. Такой способ совершения мошенничества может быть характерен и для специальных видов мошенничества (при получении выплат; в сфере страхования и др.) [11, с. 78-80].

Полагаем, что важным критерием, на которой необходимо обращать внимание в правоприменительной практике, это сущность и способ использования служебного положения для совершения мошеннических действий и достижения преступной цели.

Последним видом квалифицированного мошенничества является совершение мошеннических действий, сопряженных с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности. Его особенность состоит в том, что может сложиться впечатление, что это гражданско-правовые отношения, в которых исполнитель договора является добросовестным контрагентом, имеющим хорошую платежеспособность, но по каким-то обстоятельствам он не может исполнить свою часть договора.

Наличие умысла на неисполнение договорных обязательств носит скрытый характер. Здесь отличием мошеннических действий от гражданско-правовых обязательств является корыстный умысел у исполнителя. Для установления умысла важно выяснить способ совершения мошеннических действий (он может быть простым или сложным).

Для простого способа характерно то, что преступные деяния мошеннического характера совершаются в пределах одного региона. При сложных способах этого вида мошенничества преступная деятельность осуществляется в «одном или нескольких регионах, или же может осуществляться за пределами РФ. Выбор способа совершения преступления зависит от вида предпринимательской деятельности, осуществляемой преступником» [12, с. 96-108].

Таким образом, законодатель предусматривает две группы видов мошеннических действий: квалифицированные и специальные виды мошенничества [13, с. 202]. Каждый из этих видов включает в себя подвиды, которые имеют свою специфику, способ совершения преступного деяния, обладают повышенной степенью общественной опасности, и предусматривают определенные негативные последствия для потерпевших. Понимание сущности этих видов помогает сотрудникам оперативных подразделений правильно квалифицировать содеянное, обозначить перечень обстоятельств, которые необходимо задокументировать, для последующего осуществления предварительного расследования и привлечения виновного к ответственности, а также возмещения имущественного вреда потерпевшему.

1. Смирнов И.М. Оперативно-розыскная характеристика новых способов совершения мошеннических действий в сети // Научный вестник Орлов-

- ского юридического института МВД России имени В.В. Лукьянова. 2022. № 2 (91). С. 210-215.
2. Камышов Д.А. Понятие и признаки мошенничества в российском уголовном законодательстве // Пробелы в российском законодательстве. 2012. № 2. С. 147-151.
3. Состояние преступности в России за январь–август 2023 года [Электронный ресурс]. URL: <https://мвд.рф> (дата обращения: 22.09.2023).
4. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федер. закон Рос. Федерации от 29.11.2012 № 207-ФЗ: в ред. от 03.07.2016 // Собр. законодательства Рос. Федерации. 2012. № 49, ст. 6752.
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: в ред. от 24.09.2022 // Собр. законодательства Рос. Федерации. 1996. № 25, ст. 2954.
6. Екимцев С.В. Оперативно-розыскная характеристика мошенничества и его видов // Алтайский юридический вестник. 2020. № 4 (32). С. 130-134.
7. Арутюнян Д.А., Рябова К.В. О современных тенденциях оптимизации досудебного производства в целях обеспечения доступа граждан к правосудию // Научный портал МВД России. 2016. № 1. С. 12-18.
8. Пупцева А.В. Особенности раскрытия и расследования преступлений против собственности: учебное пособие. Волгоград: ВА МВД России, 2016. С. 28.
9. Гончаров Д.Ю., Гончарова С.Г. Квалификация мошенничества, совершенного с использованием служебного положения // Вестник Воронежского государственного университета. 2016. № 3. С. 281-290.
10. Иногамова-Хегай Л.В. Служебные преступления как единичные деяния и как множественность преступлений // Общество и право. 2017. № 1(59). С. 18-23.
11. Баранчикова М.В. Использование служебного положения как способ совершения специальных видов мошенничества // Закон и право. 2018. № 10. С. 78-80.
12. Залескина А.Н. Способы совершения мошенничества, сопряженного с преднамеренным неисполнением договорных обязательств в сфере предпринимательской деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2019. № 1-2. С. 96-108.
13. Уголовный процесс: учебник для вузов / А.Н. Артамонов, А.М. Баранов, А.С. Бахта [и др.]; под ред. Б.Б. Булатова, А.М. Баранова. 2-е издание, переработанное и дополненное. М.: ЮРАЙТ, 2010. 606 с.

СВЕДЕНИЯ ОБ АВТОРЕ

Екимцев Сергей Валерьевич. Старший преподаватель кафедры оперативно-розыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, д. 2.

Ключевые слова: виды мошенничества, квалифицированное мошенничество, способы и условия мошенничества, персональные данные, уголовный розыск, интегрированный банк данных, вредоносные программы.

Ефремова О.М., Чикина П.В.

КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ МЕССЕНДЖЕРОВ WHATSAPP И VIBER С ЦЕЛЮ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ОРИЕНТИРУЮЩЕГО ХАРАКТЕРА ДЛЯ ПРОИЗВОДСТВА ЭКСПЕРТИЗ

Аннотация. В данной статье рассматриваются способы получения данных уполномоченными лицами из программ мгновенного обмена сообщениями, для использования полученной информации в качестве материала для соответствующих экспертиз. Отмечается, что сообщения, обмениваемые в мессенджерах при помощи программ мгновенного обмена, таких как WhatsApp, Telegram, Viber и других, давно используются в качестве доказательств в уголовных делах. Для этого такую информацию необходимо изъять в соответствии с нормами уголовно-процессуального законодательства.

В эпоху всемирной цифровизации инновационные технологии не могут обойти ни одного человека. В наше время любая сфера жизнедеятельности подвержена влиянию различных новшеств в сфере информационных технологий, в особенности затрагивается такая важная область человеческих интересов, как коммуникация друг с другом [1]. Благодаря передовым технологиям у людей появилась возможность общаться друг с другом и передавать различного рода информацию, исключая личный контакт, находясь в разных точках не только определенного региона, но и, более того, земного шара.

Почти каждый человек является обладателем не просто мобильного телефона, а смартфона, оснащенного разнообразными функциями и приложениями, поэтому с большой вероятностью каждый хотя бы один раз сталкивался с мессенджерами. Безусловно, такого рода приложения стали неотъемлемой частью нашей жизни [2]. Мы используем их не только для общения с близкими, но и для работы, что значительно упрощает, и в то же время играет огромную роль в трудовой деятельности, так как таким образом можно передавать и информацию ограниченного пользования. Однако

можем ли мы быть уверены наверняка, что все отправленные нами сообщения и содержащиеся в них данные останутся конфиденциальными и посторонние лица в любой момент не смогут установить к ним доступ.

Стоит отметить, что получение доступа к данным пользователей осуществляется не беспрепятственно. В каждом мессенджере существует свой особый способ шифрования, в каких-то приложениях его взломать легче, в каких-то сложнее. В зависимости от сложности шифрования информации сотрудник, делает выбор в пользу более эффективного метода получения данных.

Специализированные службы способны получать доступ не только к сообщениям, но и к личным данным пользователей, используя при этом многообразие способов и методик. Одним из самых распространенных и понятных простому обывателю является установка так называемой «прослушки», то есть подключение сессии на подконтрольном оборудовании [3]. В случае если устройство, из которого необходимо изъять информацию, находится непосредственно у сотрудника правоохранительных органов, то просмотр интересующей информации можно произвести посредством простого прочтения с последующим производством снимков экрана – «скриншотов», тем самым информация будет фиксироваться на полученных кадрах и в последующем изыматься с устройства лица, которому оно принадлежит [4].

Но существует и ряд других инструментов, которые используются специальными службами в случае, когда доступ к устройству невозможен физически, либо осложнен технически.

Один из таких способов – «взлом задним ходом». Что подразумевает под собой данный метод? В том случае, если правоохранительные органы захотят получить доступ к какой-то конкретной учетной записи в каком-либо мессенджере, например WhatsApp, то они могут использовать слабые места, а также любые другие ошибки операционной системы или приложения непосредственно. Но данный метод может представляться достаточно затруднительным в силу того, что разработчики постоянно совершенствуют систему защиты и шифрования серверов, тем самым устраняя возможные уязвимости.

Второй способ – это сбор метаданных. Чтобы понять, что представляет собой этот способ, необходимо понимать, что в себя включает понятие «метаданные». Метаданные – это дополнительная информация о содержимом файла или объекта, например дата создания и место хранения текстового документа, аннотация текста и другие. Данная информация может иметь огромное значение для сотрудников спецслужб, так как такие данные как время отправки сообщения, частота соединения с определенными контактами играет не меньшую роль, чем смысловое содержание текста отправленного СМС, поскольку на основании этого можно сделать вывод об активности абонента.

Третий способ – судебный приказ. Этот способ подразумевает под собой получение данных в судебном порядке. Безусловно, изъятие и просмотр переписок и другой личной информации затрагивают конституционные права человека. Несмотря на то, что правоохранительные органы имеют полномочия на осуществление подобного рода деятельности, а обычные граждане – нет, бывают ситуации, когда, лицо отказывается предоставлять запрашиваемые у него данные, в силу разных причин. В этом случае применяется данный способ получения интересующей информации [5].

Стоит отметить, что вне зависимости от способа шифрования любой мессенджер может быть подвергнут прослушиванию со стороны правоохранительных органов. Тем не менее, разработчики такого рода приложений постоянно усовершенствуют их, что делает невозможным прочтение сообщений даже администраторами этих приложений. В любом случае, даже если у сотрудников не получается получить доступ к текстовому содержанию сообщения и другим файлам, то доступ к метаданным получить удастся почти в любом случае, что немаловажно, как мы говорили ранее. Так как используя данные о времени отправки сообщения, IP-адреса отправителя и получателя уже можно сделать определенные выводы и использовать полученную информацию для раскрытия преступления [6].

Помимо предоставления пользователю возможности базового обмена сообщениями, мессенджеры собирают множество данных о людях, их использующих, начиная от личной информации и заканчивая местоположением, фото- и видеозаписями. Более того, они могут использовать определенные алгоритмы, определяющие интересы пользователя [7]. Например, вы заинтересованы в покупке бассейна и неоднократно просматриваете различные сайты с интересующим вас товаром, в последующем вам будет предложена соответствующая реклама. А для того, чтобы получить доступ к контактам мессенджер запрашивает разрешение на использование адресной книги устройства, по такому же принципу запрашивается разрешение на отслеживание геопозиции.

Таким образом, правоохранительные органы могут получить из мессенджера огромный объем информации, которая может оказать помощь в расследовании преступления даже в том случае, когда содержание переписки установить не получилось, либо не предоставляется возможным [8].

Немаловажным является правильное изъятие подобной информации в соответствии с законодательством. Чаще всего данные из мессенджеров сотрудники правоохранительных органов получают при непосредственном и гласном изъятии электронных носителей с их последующим осмотром и проведением экспертизы в случае необходимости [9]. Проведение подобных мероприятий без решения суда, ограничиваясь лишь постановлением о проведении ОРМ, и соответствующим протоколом не противоречит позиции Конституционного суда РФ.

На этапе доследственной проверки следователи или дознаватели обычно изымают электронный носитель информации при проведении осмотра места происшествия. Безусловно, возможны и другие случаи:

- владелец добровольно предоставляет устройство при проведении опроса (в порядке ст. 144 УПК РФ);
- изъятие при задержании лица (в порядке ст. 91, 92 УПК РФ);
- производство выемки (ст. 183 УПК РФ).

Если владелец смартфона или иного устройства отказывается представить его для ознакомления с его содержимым, то извлечение электронной информации из памяти устройства правоохранные органы могут осуществить с помощью универсального устройства извлечения судебной информации (UFED – Universal Forensic Extraction Device). Однако чтобы такая информация могла быть признана допустимой в суде, необходимо ее изъять и оформить в соответствии с уголовно-процессуальным законодательством [10].

-
1. Григорьев В.Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство // Академическая мысль. 2019. № 3 (8). С. 57-61.
 2. Ефремова О.М. Процессуальные механизмы получения следователем информации об электронных сообщениях при расследовании уголовных дел // Вестник Академии Следственного комитета Российской Федерации. 2020. №1. С. 78-82.
 3. Клевцов К.К., Васюков В.Ф. Получение электронной информации уголовным делам в рамках международного сотрудничества // Вестник Санкт-Петербургского университета. Право. 2021. Т. 12. № 1. С. 36-51.
 4. Воронин М.И. Недопустимая допустимость электронных доказательств. Судебная практика и пробелы в УПК // Уголовный процесс. 2020. № 10. С. 47.
 5. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров [Электронный ресурс]// Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). URL: <https://cyberleninka.ru> (дата обращения: 18.10.2023).
 6. Зазулин А.И. Получение следователем информации, содержащейся в сообщениях, передаваемых посредством электронной почты и мессенджеров: проблемы процессуального регулирования // Российский следователь. 2018. № 5. С. 17.
 7. Зазулин А.И. Использование цифровой информации в доказывании по уголовным делам. М.: Юрлитинформ, 2019. 168 с.
 8. Поддубный И.В., Флоря Д.Ф. Некоторые особенности раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 2 (95). С. 259–266.

9. Ефремова О.М. Особенности производства осмотра компьютерной информации следователем в уголовном судопроизводстве // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2020. № 1 (82). С. 51-56.
10. Васюков В.Ф. Особенности изъятия электронных носителей информации при производстве следственных действий: новеллы законодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2 (10). С. 8-14.

СВЕДЕНИЯ ОБ АВТОРАХ

Ефремова Ольга Михайловна. Кандидат юридических наук. Преподаватель кафедры криминалистики и предварительного расследования в ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, д. 2.

Чикина Полина Владимировна. Курсант факультета подготовки следователей.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, д. 2.

Ключевые слова: мессенджер, информационные технологии, цифровизация, мобильные приложения, цифровой след, абонент, абонентское устройство.

Гришин Д.А.

РАСКРЫТИЕ ПРЕСТУПЛЕНИЯ КАК ЗАДАЧА УГОЛОВНОГО СУДОПРОИЗВОДСТВА

Аннотация. В статье рассматривается термин «раскрытие преступления» и его нормативное закрепление. Автор обращает внимание на отсутствие в Уголовно-процессуальном кодексе Российской Федерации закрепления соответствующей деятельности. Делается вывод, что законодателю необходимо обеспечить нормативное закрепление раскрытия преступления в качестве цели уголовного судопроизводства.

Термин «раскрытие преступления» широко используется в оперативно-розыскной деятельности. Согласно ст. 2 Федерального закона от 12.08.1995

№ 144-ФЗ «Об оперативно-розыскной деятельности» одной из задач оперативно-розыскной деятельности является раскрытие преступлений.

Однако нам представляется не понятной позиция законодателя, в результате которой сложилась парадоксальная ситуация. Во-первых, словосочетание «раскрытие преступления» в УПК РФ практически отсутствует. Оно используется лишь в ст. 317.1, 317.5, 317.6, 317.7, объединенных в главе 40.1 УПК РФ, регулирующей особый порядок принятия судебного решения при заключении досудебного соглашения о сотрудничестве. Во-вторых, текст указанных норм, а именно словосочетание «раскрытие и расследование преступления» позволяет резюмировать, что законодатель разводит эти понятия, фактически заявляя, что расследование не предполагает раскрытия преступления. При этом, исходя из используемых формулировок, раскрытие преступления не подразумевает изобличения и уголовного преследования других соучастников преступления, розыска имущества, добытого в результате преступления.

В научной литературе раскрытие преступления – это «деятельность, возникающая по факту совершения неочевидного преступления и направленная на установление лица, подлежащего привлечению в качестве обвиняемого, а равно деятельность в ходе расследования очевидного преступления, направленная на установление местонахождения подозреваемого или обвиняемого, его розыск, доставление к лицу, производящему расследование» [1, с. 45].

Существуют различные точки зрения относительно соотношения понятий раскрытие и расследование преступлений. Одни авторы относят первое исключительно к сфере оперативно-розыскной деятельности, а второе – к уголовному судопроизводству [2; 3, с. 14], другие выделяют различные аспекты данного явления, обозначая среди них и уголовно-процессуальный [4, с. 39], третьи рассматривают раскрытие как составную часть расследования, что на наш взгляд, представляется абсолютно верным.

В рамках рассматриваемой проблематики будет уместным вспомнить ст. 2 УПК РСФСР, согласно которой задачами советского уголовного судопроизводства являлись быстрое и полное раскрытие преступлений, изобличение виновных. На наш взгляд, подобный подход максимально точно отражал сущность активности властных субъектов уголовного судопроизводства.

Важным представляется не столько определение рассматриваемых категорий и их соотношения, а сколько выявление приоритетов уголовного судопроизводства, правильное понимание его предназначения. Отрицание необходимости раскрытия преступления в ходе производства по уголовному делу, ориентации на решение этой задачи как следователя, так и дознавателя, безусловно, ошибочно.

Здесь мы исходим из элементарных логических рассуждений, которые состоят в следующем:

1. Невозможно обеспечить защиту прав и законных интересов лиц и организаций, потерпевших от преступлений не раскрыв его, установив виновных, обнаружив похищенное имущество.

2. Показателем эффективности деятельности органов предварительного расследования является количество уголовных дел, направленных в суд, что возможно только после установления всех обстоятельств содеянного и самое главное, – лица его совершившего.

3. К обстоятельствам, подлежащим доказыванию, относятся и такие как виновность лица в совершении преступления, форма его вины и мотивы, характеристики его личности. Чтобы доказать указанные обстоятельства требуется установление причастных к совершению общественно опасного деяния лиц, то есть раскрытие преступления.

В завершении целесообразно резюмировать, что законодателю необходимо обеспечить нормативное закрепление раскрытия преступления в качестве цели уголовного судопроизводства, поставив во главу угла потерпевшего, обратив усилия правоохранительных органов на защиту его личности, восстановление правового статуса, нарушенного в результате преступной деятельности, компенсацию причиненного ему ущерба. Интенсификация деятельности в указанных направлениях вовсе не предполагает необходимости нарушения прав, свобод и законных интересов личности в ходе уголовного судопроизводства.

1. Ахмадуллин А.С. Понятия «раскрытие преступления», «выявление преступления», «очевидное и неочевидное преступления», используемые при формировании официальной правовой статистики // Законность. 2017. № 9 (995). С. 45.

2. Хамизов В.Л. Соотношение понятий «раскрытие преступлений», «раскрытие преступлений по горячим следам» и «расследование преступлений» // Вестник Московского университета МВД России. 2019. № 7. С. 246-250.

3. Судницын А.Б. Задачи предварительного расследования: автореф. дис. ... канд. юрид. наук. Омск, 2011. 26 с.

4. Ку克林 В.И. Раскрытие преступлений и его соотношение с расследованием // Известия Московского государственного индустриального университета. 2011. № 2 (15). С. 39-41.

СВЕДЕНИЯ ОБ АВТОРЕ

Гришин Дмитрий Алексеевич. Кандидат юридических наук, доцент. Старший преподаватель кафедры уголовного процесса и криминалистики.

Академия права и управления Федеральной службы исполнения наказаний.

390000, г. Рязань, ул. Сенная, 1.

Ключевые слова: уголовный процесс, раскрытие преступления, расследование преступления, правовой статус, потерпевший.

Журбенко А.М., Озеров И.Н.

НЕКОТОРЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ ДОВЕДЕНИЯ ДО САМОУБИЙСТВА ПОСРЕДСТВОМ СЕТИ ИНТЕРНЕТ

Аннотация. В статье рассмотрены некоторые проблемные аспекты расследования доведения до самоубийства посредством сети интернет. Рассматривались различные следственные действия, оперативно-розыскные мероприятия и судебные экспертизы, способствующие эффективному расследованию преступлений данной категории.

Актуальность и значимость темы исследования обусловлена развитием и внедрением в повседневную жизнь современных технологий. Их использование значительно облегчает бытность: возможность заказать товар или услугу, общаться с родными и близкими, оплатить счета, найти нового собеседника и т.д.

Вместе с этим, подобная динамика развития порождает благоприятную среду для криминальных элементов. Общение через сеть приобретает совсем другие оттенки, когда человек задумывается, а действительно ли его собеседник тот за кого себя выдает.

С 2016 года на территории Российской Федерации и стран СНГ возросло количество самоубийств несовершеннолетних. Данное явление связали с появлением в информационно-телекоммуникационной сети Интернет (далее – сети Интернет) свыше двух тысяч групп, пропагандирующих суицид. Как правило, они являлись закрытыми и создавались преимущественно в социальной сети «ВКонтакте», в названиях которых пропагандировалась тема причинения себе смерти: «Синий кит», «Море китов», «Тихий дом», «Храм смерти», «Разбуди меня в 4:20», «f57», «f58» и другие аналогично заполненные по контенту сообщества, в которых пропагандируется совершение акта самоубийства, романтизм нанесения себе увечий.

В связи с этим в Уголовный кодекс Российской Федерации внесены изменения в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей, несовершеннолетних к суицидальному поведению (введены ч. 2 ст. 110, ст. 110.1 и 110.2) [1].

Мотив лиц, которые доводят других до самоубийства, определить тяжело. Одно известно точно – склонение производится целенаправленно. Наиболее встречающимся сейчас является кураторство в специализированных группах в социальных сетях. Информация проверяется с осмотра места нахождения трупа. В момент проведения следственного действия, следователь уже разрабатывает пять версий произошедшего, которые при нахождении следов сменяют друг друга:

1. Было совершено убийство;
2. Убийство, замаскированное под самоубийство;
3. Несчастный случай;
4. «Чистое» самоубийство;
5. Доведение до самоубийства.

В любом случае, при поступлении сообщения о суициде, до момента возбуждения уголовного дела, перед следователем стоит задача собрать как можно больше информации о жертве и обстоятельства произошедшего. Такая информация может быть получена путем опросов родственников и педагогов, а также учеников и друзей [2].

При подготовке к осмотру места происшествия, действия следователя должны максимально дать понятие о характере произошедшего, потому одним из важнейших этапов будет обеспечение надлежащей охраны места, где все произошло и присутствие лиц, которые в дальнейшем смогут предоставить информацию, интересующую следствие. Формируется следственно-оперативная группа, которая наилучшим образом обеспечит качественную работу, согласно ст. 178 УПК РФ, приглашается судебно-медицинский эксперт (врач) и специалист-криминалист. В ходе осмотра места происшествия будут устанавливаться признаки состава преступления, а именно ч. 2 ст. 110.2 УК РФ, появится необходимость в оперативной фиксации и изъятия информации с электронных носителей жертвы (мобильный телефон, планшет, ноутбук и т.д.). Именно быстрота совершаемых действий будет иметь особое значение, ведь после достижения кураторами поставленной цели, в 90 % случаев переписки, звонки и любые иные следы взаимодействия с погибшим будут удаляться. Жертвы сами предоставляют злоумышленникам пароли и логины от своих аккаунтов в социальных сетях, так как это является одним из условий «игры».

Согласно подп. 4, 10 п. 10 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» и п. 2 ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» в целях предупреждения, выявления и раскрытия преступлений направляется запрос о предоставлении сведений о конкретном пользователе, интересующем следствие [3], а значит, если пострадавший был зарегистрирован в социальной сети «Вконтакте» или «Одноклассники», то учредители будут содействовать следствию. Уполномоченное лицо может направить соответ-

ствующий документ в ходе производства расследования, электронная переписка может быть предоставлена по судебному решению.

Следователь производит анализ социальных сетей потерпевшего и на основании результатов, подготавливает ходатайство, чтобы получить санкции от судебного органа. При этом, было бы уместно детально рассмотреть и страницы злоумышленника, чтобы картина происходящего складывалась сразу с двух сторон. Помимо этого, подготавливается отдельное ходатайство о производстве выемки. Получить судебное разрешение – не самое сложное в нашем деле. Наибольшее количество времени занимает сам процесс выемки, так как ходатайство необходимо представить в организацию, осуществляющую управление социальной сетью (например, «ВКонтакте» и «Одноклассники» обслуживаются ООО «В контакте» со штаб-квартирой в г. Санкт-Петербурге. Далее подготавливается оборудование и технические средства. При этом на практике обычно изъятие осуществляется сотрудниками оперативных подразделений по следственному поручению [4].

При этом получение информации из иностранных социальных сетей, даже при наличии ходатайства, занимает в разы больше времени, что грозит утратой криминалистически значимой информации. Об этом, в своих трудах отмечает Харисова «Отдельной проблемой является невозможность или сложность получения экстерриториальных данных, информации, хранящейся на серверах иностранных государств и находящейся вне юрисдикции следственных органов» [5].

Обыск – также несет в себе большое значение для расследования преступлений данной категории. Более разумным будет проведение данного следственного действия на раннем этапе расследования, чтобы снизить риск изменения или утраты информации, имеющую значение для криминалистов.

Наряду с вышеизложенным, на первоначальном этапе расследования различных преступлений [6], имеет значение и установление личности преступника, который склонял несовершеннолетнего к совершению суицида. В этом поможет детальное изучение страницы, с которой жертва имела контакт, а также привлечение специализированных оперативных подразделений.

Отметим важности рассмотрения вопроса кибербуллинга. Кибербуллинг – агрессивное поведение в адрес определенного человека, выражающееся в травле, угрозах и унижении личного достоинства. Столкнувшись с этим, морально неокрепшие подростки, испытывают подавленность, пугливость и разочарование. Они теряют уверенность в себе и зачастую пытаются найти способы изолирования от своих друзей и близких. Развитие информационных технологий размывает границы личной и общественной жизни, увеличивая незащищенность человека [7, с. 208].

Люди сами выкладывают в сеть события своей повседневной жизни и свою внешность. Злоумышленники используют полученные данные в своих корыстных целях [8, с. 134].

При производстве осмотра предметов и документов (например, компьютера, телефона, личного дневника и т.п.), следователь должен обратить внимание на наличие запугиваний и унижений.

Осмотр места происшествия – неотложное следственное действие, позволяющее понять картину происходящего. Давайте разделим данное явление на этапы его проведения, а именно: подготовительный, основной и заключительный.

Подготовительный – представляет собой анализ. Следователь обязан выстроить модель криминального деяния, определить стратегию проведения следственных действий и грамотно распределить функции каждого участника следственной оперативной группы, иначе говоря, организовать ее работу. В протоколе осмотра места происшествия отражаются следующие особенности:

- рисунки, надписи, эмблемы, найденные рядом с трупом, либо с местом совершения суицида. Изображения мог нанести либо сам пострадавший, либо находящиеся рядом лица. Не стоит забывать и о смысле найденных узоров, так как они могут отсылать либо на определенное течение группы смерти, либо выражать эмоции погибшего, а также иметь в себе зашифрованные подтексты;

- вещи самого потерпевшего, которые были с ним во время совершения суицида;

- содержимое карманов: записки, личные документы, смартфон, иные вещи, которые имели особое значение для несовершеннолетнего. Телефон проверяется на наличие последних звонков, сообщений, заметок, фотографий и видеозаписей;

- телесные повреждения в области запястий, предплечья и иных местах. Данные раны, могут быть признаком выполнения подростком заданий «игры», нанесения себе увечий и нахождения в депрессивном состоянии [9].

Обратим внимание на проведение осмотра места жительства несовершеннолетнего:

- в протоколе осмотра фиксируются жилищно-бытовые условия проживания;

- производится детальный осмотр личной комнаты подростка, либо комнаты, где погибший проводил больше всего времени;

- в осматриваемом помещении особое внимание уделяется наличию электронных носителей информации, которыми пользовался потерпевший. Изъятию подлежат и рукописные носители данных (личные дневники, ежедневники, предсмертная записка, литература и др.);

- отдельному осмотру подлежат средства фото- и видеофиксации, так как на различных этапах «игры» кураторы требуют от несовершеннолетних отчет о выполнении заданий.

Информация, найденная на компьютерах, фотоаппаратах и так далее, фиксируется путем съемки экрана.

Осмотр страницы несовершеннолетнего в социальных сетях позволяет установить следующие сведения:

- возможные новые преступные эпизоды, совершенные в отношении других несовершеннолетних потерпевших [10];

- факт участия в «играх смерти», а также группах данного депрессивного течения;

- отсутствие заинтересованности и контроля со стороны родителей по отношению к ребенку;

- общение со злоумышленником и иными пользователями, разделяющими взгляды групп смерти;

- наличие фото, видео и текстовых записей на странице, имеющих намеки на совершение суицида, а также сами отчеты перед кураторами;

- место, время и количество проведенных часов в сети;

- технические устройства, используемые для вхождения в сеть.

Осмотр электронных носителей информации (компьютеров, телефонов, флеш-накопителей и т.д.) также оформляется протоколом. Заметим, что данный вид осмотра является наиболее длительным и проводится без присутствия понятых, но с использованием технических средств.

Как мы знаем, существует риск потери информации путем дистанционного удаления переписки и иных следов, поэтому следователю необходимо совместно со специалистом-криминалистом производить снятие информации на месте происшествия (либо по месту жительства подростка) с использованием криминалистического оборудования и программного обеспечения.

При доведении до самоубийства, доказывание умысла виновного лица – не простая задача. Следователь, должен уже иметь опыт проведения допросов, а также обладать психологическими познаниями и навыками изобличения во лжи. Стоит выделить наиболее подходящие экспертизы. Первая – посмертная психолого-психиатрическая экспертиза. Ее производство требует обширные познания эксперта, но при всей своей тяжести, она позволяет установить состояние жертвы до момента совершения суицида. Это значительно облегчает поиск взаимосвязи между жертвой, ее психологическое самоощущением и воздействием, которое оказывалось со стороны преступника. Однако данная процедура требует большой информационный базис, чтобы эксперт мог сделать конкретные выводы.

Мы пришли к выводу, что основной экспертизой является именно компьютерная. Она поможет обнаружить скрытые и удаленные файлы,

установить IP-адреса лиц, совершивших данное преступление, а также владельцев групп смерти [11].

Также, по нашему мнению, подходящей для данного вида преступлений, будет и лингвистическая экспертиза. Также изучению подлежат не только текстовые сообщения, но и голосовые, видеоматериалы. Лингвистическая судебная экспертиза исследует речевое воздействие на жертву, то есть целенаправленное движение информации от одного участника к другому [12, с. 39]. Исследование наличия в текстовой речи лица склонения к самоубийству, проходит через оценку операций с поступками, то есть, с совокупностью разнообразных коммуникативно-правовых действий, в основе которых лежит контролируемый конфликт [13].

Как известно из психологии – человек достаточно внушаемое существо. Та или иная информация формирует его модель поведения и варианты действий. Например, человеку внушают, что его заболевание лечиться лишь таблетками, содержащими психотропное вещество и тем самым индивид постепенно становится наркоманом; человеку предложили за денежное вознаграждение выдать военную тайну и подтолкнули к предательству; человека втянули в группу, где профессионально занимаются кражами и так далее.

Мы понимаем, что лингвисту в руки попадает информация, которая меняла поступки и эмоциональное состояние человека. Потому задачей специалистов данной отрасли является обнаружение признаков того, что жертве сужали и ограничивали свободу выбора. Вовлечение, побуждение, подталкивание и любое иное речевое воздействие, которое носит смысл «не делай то-то», «сделай так». Именно заключение по данной экспертизе будет служить одним из важных элементов доказывания.

Таким образом, подводя итог, отметим, что при расследовании преступлений о доведении до самоубийства необходимо применять обширный спектр различных специальных знаний и навыков. Специалисты, следователь, эксперт-криминалист, судебно-медицинский эксперт – основная группа в делах данной категории. Для получения наибольшего доказательственного базиса, нужно проводить ряд судебных экспертиз: судебно-медицинскую, компьютерную, лингвистическую и т.д. И исходя из информации, полученной в столь разных направлениях, мы сможем восстановить картину произошедшего.

1. Ильин Н.Н. Особенности следственного осмотра по делам о доведении до самоубийства несовершеннолетних с помощью сети интернет. М.: Московская академия Следственного комитета Российской Федерации. 2021. С. 173-178.

2. Озеров И.Н., Сааков Т.А. Некоторые тактические особенности первоначального этапа раскрытия и расследования преступлений, связанных с доведением до самоубийства посредством сети «Интернет» // Юридическая

- наука и практика: Вестник Нижегородской академии МВД России. 2021. № 4 (56). С. 86-88.
3. Сааков Т.А. Судебно-диагностическое исследование демографических характеристик автора: теория и практика: монография / под ред. Е.И. Галяшиной. М.: Юрлентиформ, 2021. С. 48-49.
4. Россинская Е.Р., Сааков Т.А. Проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Криминалистика: вчера, сегодня, завтра. 2020. № 3 (15). С. 101-122.
5. Харисова З.И. Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети «Интернет» // Вестник УЮИ. 2019. № 3 (85). С. 92-98.
6. Сиделев В.В. Актуальные вопросы использования сведений о личности потерпевшего и подозреваемого при расследовании преступлений о похищении и незаконном лишении свободы наркозависимых лиц в связи с их реабилитацией // Российский следователь. 2021. № 4. С. 44-47.
7. Суворова Г.М. Информационная безопасность: учебное пособие для вузов. М.: Юрайт, 2023. 253 с.
8. Психологическая безопасность личности: учебник и практикум для вузов [Электронный ресурс] / А.И. Донцов, Ю.П. Зинченко, О.Ю. Зотова, Е.Б. Перелыгина. М.: Юрайт, 2023. 222 с. (Высшее образование.) // Образовательная платформа Юрайт [сайт]. URL: <https://urait.ru/bcode/517468/p.134> (дата обращения: 16.02.2023).
9. Галяшина Е.И. Использование специальных знаний для диагностики интернет-коммуникации экстремистской направленности в молодежной среде // Предупреждение и расследование преступлений экстремисткой направленности в молодежной среде: материалы Международной научно-практической конференции (Москва, 21 марта 2019 г.). М.: Московская академия Следственного комитета Российской Федерации, 2019. С. 80-83.
10. Кот Е.А. Тактика следственных действий по делам, связанным с побуждением несовершеннолетних в сети интернет к совершению самоубийства // Вестник Сибирского юридического института МВД России. 2021. № 3 (44). С. 178-184.
11. Бесчастнова О.В. Уголовно-правовые противодействие деятельности, направленной на побуждение детей к суицидальному поведению // Гуманитарные исследования. 2017. № 3. С. 177-181.
12. Душкина М.Р. Психология влияния в социальных коммуникациях: психологическое воздействие – методы и технологии: монография. 2-е изд., испр. и доп. М.: Юрайт, 2023. 213 с.
13. Шунейко А.А., Авдеенко И.А. Лингвистическая экспертиза: учебник и практикум для вузов. М.: Юрайт, 2023. 333 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Журбенко Алексей Михайлович. Кандидат экономических наук. Доцент кафедры криминалистики.

Белгородский юридический институт МВД России имени И.Д. Путилина.

308024, г. Белгород, ул. Горького, 56.

Озеров Игорь Николаевич. Кандидат юридических наук, доцент. Заведующий кафедрой судебно-экспертной и оперативно-розыскной деятельности.

Московская академия Следственного комитета Российской Федерации.

125080, г. Москва, ул. Врубеля, 12.

Ключевые слова: самоубийство, сеть «Интернет», расследование.

Климачков А.В., Горшкова В.С.

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ СЭД ИСОД МВД РОССИИ ПРИ ПРОВЕДЕНИИ ОРМ «ИССЛЕДОВАНИЕ ПРЕДМЕТОВ И ДОКУМЕНТОВ»

Аннотация. В статье рассматриваются отдельные вопросы использования СЭД ИСОД МВД России при назначении исследований сотрудниками оперативных подразделений полиции в экспертно-криминалистическую службу органов внутренних дел, при этом раскрываются возможности и ограничения применения вышеуказанного информационного ресурса при осуществлении оперативно-розыскной и экспертной-криминалистической видах деятельности.

Сервис электронного документооборота единой системы информационно-аналитического обеспечения деятельности МВД России (далее – СЭД ИСОД) активно и успешно используется сотрудниками полиции при осуществлении повседневной оперативно-служебной деятельности, что обусловлено высокой скоростью получения документа и обработки содержащейся в нем информации (изучение, корректировка, принятие итогового решения и т.д.) как руководителем структурного подразделения органа внутренних дел (далее – ОВД), так и непосредственным исполнителем [1]. При этом нивелируется либо полностью устраняется негативное влияние на конечные результаты работы (эффективность, результативность) не только объективных факторов – временного (волокита, неоперативность),

территориального (удаленность) характера, но и субъективных – забывчивость, невнимательность, излишняя спешка, отсутствие возможности более внимательного и вдумчивого изучения деталей изложенных фактов и прочее. Вышеуказанные преимущества информационного ресурса используют также сотрудники оперативных подразделений полиции, что позволяет качественно и в установленные нормативными актами сроки выполнять возложенные на них функции правоохранительной направленности.

Сотрудники оперативных подразделений полиции в своей служебной деятельности используют возможности других служб полиции, в том числе экспертно-криминалистических подразделений ОВД (далее – ЭКП ОВД), что в свою очередь закреплено в ст. 6 оперативно-розыскного закона – право использовать помощь специалистов при организации и проведении оперативно-розыскных мероприятий.

При возникновении необходимости в разрешении вопросов научного, технического и иного характера по имеющимся в распоряжении оперуполномоченных ОВД объектам и образцам проводятся исследования предметов и документов, к непосредственному участию в которых привлекаются «сведущие» лица государственных и негосударственных экспертных учреждений. Однако производство экономических, компьютерных, товароведческих, строительно-технических и иных экспертных исследований во вневедомственных организациях в интересах ОВД осуществляется преимущественно на платной основе. Так, в 2022 году израсходовано 268,7 млн рублей бюджетных ассигнований [2] для оплаты услуг специалистов по исследованию объектов. Необходимо отметить, что в ЭКП ОВД имеется возможность разрешения некоторых специальных вопросов в рамках имеющихся экспертных методик согласно Перечня родов (видов) экспертиз [3] путем выделения отдельных или постановкой комплексных задач перед специалистом. К примеру, вопросы об установлении стоимости электробытовых, спортивных, хозяйственных товаров, пушно-меховых и комбинированных изделий решают сотрудники ЭКП ОВД в рамках проведения товароведческих исследований. Кроме того, в рамках реализации мероприятий по совершенствованию методического обеспечения проведения товароведческих экспертиз и исследований ЭКП ОВД началась апробация алгоритма определения стоимости ювелирных изделий из драгоценных металлов и сплавов, в том числе при наличии вставок из драгоценных камней и иных материалов – комплексно решаются вопросы на основе специальных знаний в области физико-химических методов исследования, геммологии и товароведения [4].

Вышеуказанный анализ практики назначения товароведческих исследований во вневедомственные экспертные организации в МВД России за 2022 год показал, что сотрудники правоохранительных органов ряда субъектов государства неправильно определяют вид назначаемого экспертного исследования (например оценочное вместо товароведческого),

проводимого в ЭКП ОВД, либо не разделяют круг задач, разрешение части которых возможно специалистами полиции. В этой связи разработан, внедрен в практическую деятельность и успешно применяется алгоритм назначения экспертных исследований на платной основе в ЭКЦ ГУ МВД России по Алтайскому краю, который нормативно урегулирован приказом ГУ МВД России по Алтайскому краю от 20.02.2021 № 87 «Об утверждении порядка учета платных экспертиз и исследований, назначаемых во вневедомственных экспертных организациях сотрудниками органов и подразделений внутренних дел Алтайского края» и введена автоматизированная система комплексного учета данных «Платные экспертизы». Порядок назначения проведения исследований в интересах ОВД на платной основе предполагает использование СЭД ИСОД: инициатор проведения исследования подготавливает в электронном виде письмо на имя руководителя ЭКП ОВД субъекта Российской Федерации (экспертно-криминалистического центра, управления) с указанием противоправного деяния, номера и даты регистрации заявления, сообщения в ОВД, перечня имеющихся в распоряжении объектов и образцов, необходимых для разрешения специалистом вопросов. После направления адресату – руководителю ЭКП ОВД, в кратчайшие сроки рассматривается исполнителем содержание обращения по поводу возможности производства экспертного исследования и разрешения ряда вопросов в рамках имеющихся экспертных методик. Только при наличии полученного посредством СЭД ИСОД ответа о невозможности проведения исследования в электронном виде инициатор запроса может обратиться в негосударственное экспертное учреждение по данному вопросу, а финансово-экономическое подразделение полиции произведет оплату услуги специалиста.

Внедрено в ежедневную практику полиции направление посредством СЭД ИСОД писем с ЭКП ОВД на имя инициаторов либо начальника территориального ОВД об исполнении экспертных исследований, что обеспечивает оперативность получения материалов и дальнейшее использование результатов при осуществлении оперативно-служебной деятельности, принятие решений в рамках реализации положений оперативно-розыскного и уголовно-процессуального законодательства, в частности при работе по преступлениям в сфере незаконного оборота наркотиков, экстремистского и террористического характера.

Не представляется возможным обойти вниманием также противоправные посягательства о дискредитации действий Вооруженных Сил Российской Федерации при проведении Специальной военной операции, пропагандой нетрадиционных сексуальных отношений и предпочтений, которые непосредственно связаны с размещением информации в сети Интернет. У сотрудников оперативных подразделений полиции возникает необходимость проведения ОРМ «Исследование предметов и документов» с привлечением специалиста ОВД в области лингвистики для интерпретации

сущности и содержания текстов – комментарии пользователей социальных групп, название или подписи изображений, переписка в различных мессенджерах и прочее. При этом в распоряжение сотрудника ЭКП предоставляются скриншоты либо изображения экрана компьютера, сотового телефона, планшета на бумажном носителе, оптические диски с записями видеофайлов, которые содержат подлежащие исследованию объекты.

Однако в практической деятельности сотрудников ЭКП ОВД Алтайского края встречаются случаи назначения лингвистических исследований сотрудниками оперативных подразделений посредством СЭД ИСОД, когда к заданию на проведение исследования прилагается изображение текста в электронном виде. С одной стороны, вышеуказанный информационный ресурс имеет надежную защиту от внешних угроз, внесения изменений при работе с документами сотрудниками ОВД, обеспечивает оперативность проведения специалистом исследования и получения инициатором ответов на поставленные вопросы, но с другой стороны, содержание задания и объектов исследования, результатов проведенного мероприятия доступно для ознакомления иным лицам-пользователям программы со статусом «Администратор» (например, работникам канцелярии ЭКП ОВД). Проведенным анализом норм главы 2 ведомственного акта, регламентирующего деятельность ЭКП ОВД [5], при применении экспертно-криминалистических средств и методов специалистами установлено, что порядок получения задания (наличным, по почте, электронным способом и т.д.) и объектов исследования не установлен, но указан способ направления результатов исследования – направляются в адрес уполномоченного лица либо выдаются наличным.

Вышеуказанные положения, на наш взгляд, не могут использоваться при проведении оперативно-розыскных мероприятий с привлечением СЭД ИСОД, так как создают предпосылки для существенных нарушений прав и свобод граждан, вовлеченных в сферу оперативно-розыскных правоотношений, нарушения принципа конспирации при осуществлении оперативно-розыскной деятельности.

Важно обеспечивать полноту, всесторонность и объективность принятого по материалу решения и обеспечивать наступательность оперативных подразделений в борьбе с преступностью, активно привлекая «сведущих» лиц ЭКП ОВД. При этом оперативно и в кратчайшие сроки предоставлять в распоряжение специалиста задания и некоторые объекты исследования (например изображение текстов), что в силу ряда причин (например территориальная удаленность друг от друга оперативных и экспертно-криминалистических подразделений, необходимость изучения объектов и предоставления их результатов в выходные и праздничные дни, ночное время суток и т.д.) объективно вызывает трудность. Одним из выходов из сложившейся проблемной ситуации является создание на платформе ИСОД специализированного сервиса «Исследование предметов и документов» – для назначения экспертных исследований и получения их результатов, доступ к кото-

рому будет обеспечен только для уполномоченных руководителей экспертно-криминалистического и оперативного подразделений либо лиц, их замещающих. Предложенный вариант решения проблемы не является исчерпывающим, требует более детального изучения, как со стороны ученого сообщества, так и практических сотрудников полиции, анализа правоприменительной и судебной практики.

На основании вышеизложенного, можно заключить, что активное внедрение информационных технологий в деятельность правоохранительных органов позволяет в кратчайшие сроки, объективно и в полном объеме реализовывать возложенные обязанности сотрудникам оперативных и экспертно-криминалистических подразделений, но в тоже время порождает ряд проблем правового, организационного и технического характера. Только взвешенный подход, глубокое осмысление и предложение наиболее рациональных, эффективных вариантов разрешения проблем использования информационных ресурсов позволит достигать высоких результатов в борьбе с преступностью.

1. О мерах по переходу на электронный документооборот: распоряжение МВД России от 07.11.2015 № 1/9112.
2. Об оперативно-розыскной деятельности [Электронный ресурс]: Федер. закон Рос. Федерации от 12.08.1995 № 144-ФЗ: с изм. от 29.12.2022. Доступ из справ.-правовой системы «КонсультантПлюс».
3. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации [Электронный ресурс]: приказ МВД России от 29.06.2005 № 511: с изм. от 30.05.2022. Доступ из справ.-правовой системы «КонсультантПлюс».
4. По вопросу методического обеспечения производства товароведческих экспертиз (Алгоритм определения стоимости ювелирных изделий из драгоценных металлов и сплавов, в том числе из драгоценных камней и других природных и синтезированных материалов, при расследовании противоправных деяний): письмо ЭКЦ МВД России от 13.04.2023 № 37/24-7380.
5. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России [Электронный ресурс]: приказ МВД России от 11.01.2009 № 7: с изм. от 09.03.2023. Доступ из справ.-правовой системы «КонсультантПлюс».

СВЕДЕНИЯ ОБ АВТОРЕ

Климачков Александр Вячеславович. Старший преподаватель кафедры оперативно-розыскной деятельности органов внутренних дел.

Барнаульский юридический институт МВД России.
656038, г. Барнаул, ул. Чкалова, 49.

Горшкова Вера Сергеевна. Начальник организационно-методического отделения Экспертно-криминалистического центра.

Главное управление МВД России по Алтайскому краю.

656015, г. Барнаул, пр. Ленина, 74.

Ключевые слова: оперативно-розыскная деятельность, судебно-экспертная деятельность, специалист, информационный ресурс.

Крысина Т.Е., Смирнов И.М.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Аннотация. В статье рассматриваются основные аспекты оперативно-розыскной характеристики преступлений в сфере интеллектуальной собственности, а также меры, принимаемые субъектами оперативно-розыскной деятельности по их предупреждению, выявлению и раскрытию.

Одним из актуальных вопросов выявления и раскрытия преступлений в сфере интеллектуальной собственности является получение информации в процессе поиска и обнаружения фактов совершения преступлений в сфере интеллектуальной собственности в сети интернет.

С целью получения информации о противоправном посягательстве на интеллектуальную собственность необходимо осуществлять следующие меры:

- работа в местах возможной реализации контрафактной продукции;
- система контроля персональных ключей защиты;
- мониторинг сети интернет.

Как отмечают отдельные авторы, более строго чем приостановление деятельности интернет-сайтов в настоящее время правоохранительным органам РФ влиять на провайдеров в целом, позволяет нормативная база.

Информацию о сайтах, на которых распространяется продукция, которая защищена авторским правом, как отмечалось выше, можно получить, используя поисковые системы. Для этого лишь необходимо задать корректно запрос. Например, задавая в запросе названия фильмов, которые демонстрируются на данный момент в кинотеатрах или будут демонстрироваться в будущем и добавляя фразу «скачать», также нужно ограничить запрос такой функцией, как страницы из РФ. Не стоит обращать внимание на домен верхнего уровня иерархического адресного пространства сети Интернет, созданный на основе кодирования названий стран в соответствии с международными стандартами, для обслуживания адресного пространства сегмента сети интернет определенного государства, так как,

например, сайт может иметь домен верхнего уровня «RU» (Россия), но физически находиться на территории Украины [1, с. 61].

С целью выявления фактов незаконного воспроизведения, распространения и тиражирования объектов интеллектуальной собственности или незаконного производства, экспорта, импорта, хранения или реализации объектов интеллектуальной собственности необходимо проводить осмотры производственных мощностей организаций и предприятий, которые производят, воспроизводят, распространяют ли тиражируют объекты интеллектуальной собственности, экспортируют, импортируют, хранят или реализуют их.

Для выявления преступлений в интеллектуальной собственности, необходимо провести контролируемую поставку или контрольную закупку контрафактной продукции, результаты их проведения впоследствии могут существенно повлиять на ход расследования.

Задачами проведения контролируемой поставки в сфере борьбы с оборотом контрафактной продукции могут быть:

- установление производителей контрафактной продукции;
- установление каналов транспортировки и хранения контрафактной продукции;
- установление отправителей и получателей предметов поставки;
- установление пунктов хранения, фальсификации защитных элементов продукции;
- установление лиц, причастных к совершению преступления;
- выяснение системы организации сбыта контрафактной продукции;
- установление сети пунктов оптовой и розничной торговли контрафактной продукции;
- установление коррумпированных лиц таможенной службы, которые способствуют перемещению контрафактной продукции;
- обеспечение доказательств преступной деятельности и другие.

В отдельных случаях проводится контрольная закупка товаров, предметов у физических и юридических лиц, независимо от форм собственности, с целью выявления и документирования фактов распространения контрафактной продукции.

Порядок проведения контрольной закупки такой:

- после получения фальсифицированной продукции и товарного чека у сотрудников торговой точки получить свидетельство о государственной регистрации предприятия, накладные на получение товара;
- обеспечить меры сохранности кассового аппарата, имеющейся наличной выручки и фальсифицированной продукции до прибытия следственно-оперативной группы.

Для решения вопросов относительно открытия уголовного производства о преступлениях,

предусмотренных ст. 146, 147, 180 УК РФ, в материалах должны содержаться данные:

- о юридических (физических) лицах, которым принадлежат права интеллектуальной собственности;
- расчет размера причиненного противоправными действиями ущерба;
- предварительное исследование специалиста (эксперта), которое бы подтвердило наличие признаков контрафактности [2, с. 82].

Еще одна из научных и практических проблем – взаимодействие и координация между ОВД и иными субъектами.

Не вдаваясь в теоретическую дискуссию о разграничении взаимодействия и координации, считаем, что основная разница между ними заключается в том, что в отличие от взаимодействия, координация обязательно предполагает субъекта, наделенного координационно-властными полномочиями в отношении других участников совместной (общей) деятельности, то есть взаимодействия.

Завершая рассмотрение вопросов взаимодействия оперативных подразделений ОВД с другими субъектами по противодействию преступлениям, связанным с нарушением прав интеллектуальной собственности, предлагаем определить ее как регламентированную правовыми актами систему общих и согласованных по времени, месту и мерам действий нескольких органов (служб, подразделений), один из которых может быть наделен координационно-властными полномочиями по решению как общих для всех ее участников, так и специальных, задач.

Для выявления указанных преступлений необходимо знать порядок обращения объектов интеллектуальной собственности, их изготовления и регистрации и способы их подделки и распространения в торговой сети и в глобальной сети Интернет [3, с. 107].

Сотрудники оперативных и следственных подразделений должны уметь проводить проверку отдельного производственного и торгового предприятий [4, с. 189-190]. Действенными мерами выявления и документирования преступлений в сфере интеллектуальной собственности являются контролируемое снабжение и контрольная закупка.

1. Кожушкова В.А., Бормотова Л.В. Проблемы использования видеоконференцсвязи в уголовном процессе и перспективы развития // Интерна-ука. 2022. № 4-4 (227). С. 61.

2. Гольяпина И.Ю., Сазанова Н.В. Проблемы привлечения к ответственности за незаконное использование средств индивидуализации товаров (работ, услуг) // Защита интеллектуальной собственности в деятельности бизнеса и государства: сборник докладов III Международной научно-практической межвузовской площадки. СПб.: Российская академия народ-

ного хозяйства и государственной службы при Президенте Российской Федерации, Северо-Западный институт управления, 2021. С. 28.

3. Муравьев К.В., Седельников П.В. Назначение и производство судебной экспертизы как вид специальных познаний, применяемый на стадии возбуждения уголовного дела // Вестник Волгоградской академии МВД России. 2014. № 1 (28). С. 102-109.

4. Уголовный процесс: учебник для вузов / А.Н. Артамонов, А.М. Баранов, А.С. Бахта [и др.]; под ред. Б.Б. Булатова, А.М. Баранова. 2-е издание, переработанное и дополненное. М.: ЮРАЙТ, 2010. 606 с.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Крысина Татьяна Евгеньевна. Курсант учебной группы 20040 факультета подготовки следователей.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Смирнов Иван Михайлович. Кандидат исторических наук. Старший преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: преступления в сфере интеллектуальной собственности, интеллектуальной собственности, оперативные подразделения, оперативно-розыскная характеристика, оперативно-розыскные мероприятия.

Кураков Д.В., Некрасов М.А.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ «ПО ГОРЯЧИМ СЛЕДАМ»

Аннотация. В статье рассматриваются вопросы, касающиеся раскрытия и расследования преступлений «по горячим следам», а также взаимодействия следователя с оперативными сотрудниками в процессе расследования.

Одним из важнейших факторов, влияющих на успех при раскрытии и расследовании преступления, является скорость проведения оперативно-розыскных мероприятий и неотложных следственных действий. К сожалению, не всегда возможно провести данный комплекс мероприятий свое-

временно в силу объективных причин, независящих от органов, осуществляющих оперативно-розыскную деятельность и предварительное расследование. Таких причин существует довольно много, одними из них будут являться:

1. Несвоевременное обнаружение собственником пропажи похищенного;
2. Тщательное сокрытие события преступления и его следов преступником;
3. Нежелание лиц, потерпевших от преступного посягательства, своевременно обращаться с заявлением в правоохранительные органы (например, при преступлениях против половой свободы и половой неприкосновенности) и так далее.

В случае, если данные факторы отсутствуют и имеется информация о том, что (или недавно) совершено преступление, то возможно осуществление раскрытия и расследования преступления «по горячим следам». Такой речевой оборот, как «по горячим следам», довольно крепко вошел в лексику и среди практических сотрудников, и в юридической литературе. Для того, чтобы понять почему используется именно эта метафора необходимо обратиться к словарю, в котором приводятся такие синонимы данному выражению как: «без задержки, без промедления, не откладывая, немедленно, сейчас же».

Как считает Р.С. Белкин, раскрытие преступления по горячим следам должно быть осуществлено в срок, не превышающий трое суток с момента поступления сообщения о преступлении или обнаружения его признаков, но не нельзя исключать особо сложные ситуации, когда раскрытие может занять от десяти до пятнадцати суток [1, с. 579]. В таких условиях, когда необходимо максимально быстро принимать меры по выявлению лиц, совершивших преступное посягательство, огромную роль в успешном выполнении данной задачи играют методические рекомендации по планированию, выдвижению версий, а также организации расследования по горячим следам. Стоит отметить, что именно планирование позволяет упорядочить деятельность следователя, что способствует увеличению вероятности успешного раскрытия и расследования преступления.

С.В. Кузьмин определяет планирование расследования преступления следующим образом: «Это сложный повторяющийся динамичный мыслительный процесс, направленный на решение информационно-познавательных и организационно-управленческих задач предварительного следствия в точном соответствии с требованиями закона» [2, с. 59].

Разработанные криминалистические алгоритмы, также известные как программа расследования на первоначальном, последующем и завершающем этапах расследования способствуют оптимизации деятельности следователя при грамотном их применении, поскольку если использовать их не как единый комплекс, элементы которого дополняют друг друга, то по-

являются риски невыполнения задач, связанных с раскрытием и расследованием преступлений.

Важной особенностью процесса раскрытия и расследования преступления по горячим следам является наличие «свежих» следов на месте происшествия, что делает осмотр места происшествия важнейшим следственным действием на данном этапе. Именно в процессе осмотра места происшествия происходит обнаружение и последующие фиксация и изъятие следов, которые в дальнейшем выступят доказательствами по уголовному делу. Представляет особую важность их недавнее образование, поскольку это обеспечивает физическую возможность их фиксации и изъятия. Необходимо уделять внимание не только на обнаруженные следы, но и на саму обстановку места происшествия, чтобы создать наиболее полное представление о механизме совершения преступления и выдвинуть первоначальные версии [3, с. 136].

Следователь, как руководитель дежурной следственно-оперативной группы, получив сообщение о только что совершенном преступлении, исходя из полученных от оперативного дежурного данных о месте происшествия и характере совершенного преступного деяния, должен немедленно принять решение о привлечении необходимых специалистов и служб, а также технико-криминалистических средств.

Оперативные сотрудники играют также немаловажную роль в раскрытии преступлений «по горячим следам», именно поэтому они являются неотъемлемыми участниками дежурной следственно-оперативной группы. По прибытии на место происшествия следователь даёт устное поручение оперативному сотруднику на установление очевидцев происшествия и сбор сведений, которые могут способствовать раскрытию и расследованию. Основным его инструментом в соответствии с Федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» в данном случае будет являться такое оперативно-розыскное мероприятие как опрос. Оперативно-розыскное мероприятие «опрос» по своей сути – это сбор (получение или добывание) фактической информации, значимой для решения конкретных задач оперативно-розыскной деятельности со слов опрашиваемого физического лица, которое реально или вероятно располагает ею [4, с. 139]. Он может проводиться как гласно, так и негласно. В сложившейся обстановке будет проводиться именно гласный опрос, поскольку нет необходимости утаивать цель его проведения. Установление очевидцев не всегда является легкой задачей, ведь преступление могло быть совершено только лишь в присутствии потерпевшего, который, находясь в шокированном состоянии просто не смог запомнить внешность и отдельные черты нападавшего. Сведения, полученные в результате опроса, могут касаться как в целом произошедшего, так и личности преступника, его бросаких примет, одежде, пути, по которому скрылся, что может способствовать скорейшему его установлению и задержанию. В случае, если

данные, полученные в результате опроса, позволяют сделать вывод о местоположении преступника необходимо принимать меры к оцеплению предполагаемого участка, в котором он находится, и задержанию.

Оперативному сотруднику необходимо совершить осмотр прилегающей территории на наличие камер видеонаблюдения для дальнейшего получения информации с них, обойти близлежащие учреждения и организации, а также совершить поквартирный обход [5, с. 16]. Как правило, именно записи с камер видеонаблюдения играют решающую роль в раскрытии преступлений «по горячим следам», поскольку они исключают фактор субъективного восприятия произошедшего очевидцами, но не всегда получается получить доступ к ним сразу же, ведь зачастую сервера, на которых хранятся видеозаписи, находятся в другом городе или в сторонней организации, обеспечивающей видеонаблюдение на данном объекте. Тогда оперативный сотрудник применит наведение справок, для получения значимой для задач оперативно-розыскной деятельности информации. Важно учитывать, что довольно популярным средством гражданско-правовой самозащиты собственности среди граждан стало установление видеокамер на балконах и во дворах в качестве превентивной меры борьбы с правонарушениями, касающимися их автотранспортных средств, поэтому не стоит пренебрегать уточнением данной информации при опросе [6, с. 36].

Таким образом, оперативный сотрудник по факту получения любой информации, значимой для раскрытия и расследования преступления должен сообщить следователю, который уже будет принимать решение о необходимости привлечения дополнительных средств и сил для оцепления отдельных участков местности, выделения сотрудников для осуществления погони и задержания преступника.

1. Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика: учебник / под ред. Р.С. Белкина. М.: НОРМА, 2017.

2. Кузьмин С.В. Содержание планирования расследования преступлений // Правоведение. 2000. № 5.

3. Рогава И.Г., Пятибратов В.А. Проблемы и особенности расследования преступлений по горячим следам [Электронный ресурс] // Международный журнал гуманитарных и естественных наук. 2018. № 6-2. URL: <https://cyberleninka.ru/article/n/problemy-i-osobennosti-rassledovaniya-prestupleniy-po-goryachim-sledam> (дата обращения: 04.10.2022).

4. Колесниченко Н.А. Роль оперативно-розыскного мероприятия «опрос» в деятельности органов внутренних дел // Современное состояние и перспективы развития науки и образования: сборник научных трудов по материалам XXXI Международной научно-практической конференции. Анапа, 2022.

5. Муравьев К.В. Уведомление о подозрении в совершении преступления // Уголовный процесс. 2007. № 11.

6. Муравьев К.В., Писарев А.В., Смирнова И.С., Супрун С.В. Уголовно-процессуальная деятельность органов дознания системы МВД России. М.: ЦОКР МВД России, 2010. 136 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Кураков Денис Владимирович. Кандидат юридических наук. Доцент кафедры оперативно-разыскной деятельности ОВД.

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

Некрасов Михаил Александрович. Слушатель факультета подготовки следователей.

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

Ключевые слова: расследование, раскрытие, орган дознания, следователь, преступление, «по горячим следам».

Лисицын А.Г.

К ВОПРОСУ ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ КРАЖ И УГОНОВ ТРАНСПОРТНЫХ СРЕДСТВ

Аннотация. В настоящее время в нашей стране проблема криминального автобизнеса приобрела особую остроту. Данный вид преступных деяний имеет широкое распространение и является одним из наиболее доходных в преступной среде. Хищения и другие неправомерные завладения автотранспортными средствами относятся к категории преступлений против собственности, пресечение, раскрытие и предупреждение которых представляет собой приоритетное направление в деятельности МВД России.

В теории оперативно-розыскной деятельности оперативно-розыскная характеристика конкретного преступного деяния (группы схожих преступных деяний) рассматривается «как инструмент, обеспечивающий эффективность применения оперативно-розыскных сил, средств и методов в целях противодействия преступности» [1, с. 16].

«Оперативно-розыскная характеристика имеет двойное назначение. С одной стороны, практическое, выражающееся в соответствующих знаниях для правоприменителей. С другой стороны, теоретико-методологичес-

кое, предполагающее информационную основу для ученых. Помимо этого, такая характеристика имеет оперативный аспект, заключающийся в возможности внедрения граждан, оказывающих содействие на конфиденциальной основе, в преступную среду, необходимости зашифровки источников информации и др.» [2, с. 8].

С учетом важности такой характеристики для теории и оперативно-розыскной деятельности, оперативно-розыскная характеристика определяется как, «система признаков информационного содержания, упорядоченных и взаимосвязанных друг с другом, взятых из разных источников (как правило, криминалистической, криминологической, социологической, экономической и других характеристик преступных деяний), носящая динамический характер, предполагающий дополнение или исключение некоторых существенных признаков исходя из вида преступного деяния» [3, с. 89].

Обобщая приведенные суждения, заметим, что оперативно-розыскная характеристика любого вида преступлений представляет собой совокупность сведений, отражающих признаки и элементы преступного деяния, знание которых будет способствовать выбору сотрудниками подразделений уголовного розыска наиболее эффективных методов и средств по выявлению, пресечению и раскрытию этих преступных деяний, розыску лиц, непосредственно их совершивших, а также похищенного имущества.

Оперативно-розыскная характеристика преступлений имеет определенную структуру. Ее основными элементами, по мнению В.Д. Ларичева, являются:

- способы совершения преступного деяния;
- признаки преступного деяния, характеризующие конкретные способы;
- типичный перечень документов, чаще всего подделываемых, исправляемых, незаконно выдаваемых и т.д.;
- перечень предметов, оборудования, механизмов, на которых запечатлены следы преступного деяния;
- перечень лиц, осведомленных о противоправных действиях преступников;
- лица, возможно, причастные к преступному деянию;
- другие сведения, характеризующие преступное деяние [4, с. 124].

К основным способам совершения хищения транспортных средств относятся следующие:

1. Механический способ подразумевает нарушение целостности замка (взлом) посредством поворота личинки отмычкой или вкруткой, отжимание двери или капота посредством применения пневматической подушки, замыкания проводов зажигания двигателя. Этот способ применяется для хищения автомобилей, необорудованных сигнализациями и средствами охраны. Иногда такой способ применяется для хищения двигателя ав-

томобиля, но автомобиль во взломанном состоянии остается на прежнем месте.

2. Нарушение целостности стекла и последующее проникновение в салон автомобиля, затем путем «сверта» сворачивает личинку замка зажигания в направлении запуска двигателя, запускает автомобиль и уезжает в заранее подготовленное место, чтобы его спрятать [5, с. 107].

3. «Испытание терпения: сигнализация «сошла с ума». Этот способ схож с механическим, но он применяется для хищения автомобилей, на которых установлена сигнализация. Сущность этого способа сводится к тому, что преступник заставляют часто срабатывать сигнализацию, чтобы владелец добросовестно посчитал, что произошел сбой системы, и отключил сигнализацию. После чего злоумышленники похищают автомобиль посредством механического способа.

4. Хищение путем использования кодграббера. Этот способ применяется для хищения современных автомобилей, оснащенных хорошей сигнализацией и охранной системой. В основе этого способа находится использование «специальных электронных устройств, с помощью которых происходит деактивация иммобилайзера или охранного комплекса. Это устройство называется кодграббер. «С ним угонщик перехватывает сигнал от брелока, а в нужный момент транслирует его в угоняемый автомобиль, тем самым снимая его с охраны, при этом блокируя дополнительные комплексы защиты, включая спутниковые передатчики, отслеживающие местоположение угнанной машины».

5. Бесключевой доступ. Этот способ предполагает использование штатной системы доступа в автомобиль. «Преступники, работая в паре, с помощью специального усилителя транспондера, транслируют радиосигнал от штатного ключа-метки, находящегося у ничего не подозревающего владельца. Передача сигнала возможна на большие расстояния до находящейся на стоянке автомашины. Получив доступ к управлению, угонщики покидают автостоянку, отгоняя машину в укромное место без привлечения внимания» [6, с. 29].

6. Насильственное завладение транспортным средством путем разбоя или грабежа. Здесь могут применяться различные методы: хищение с помощью эвакуатора, имитация повреждения глушителя, складывания пассажирского зеркала или подкладывание под колеса громко лопающего предмета и др., что приводит к потере бдительности у владельца автомобиля, а затем автомобиль похищается.

Собственнику могут наноситься телесные повреждения либо высказываться угроза их нанесения, после чего его связывают и переносят в другое место, исключая возможность зрительно наблюдать за происходящим. В этот момент автомобиль перегоняется в «отстойник», где находятся приборы, заглушающие сигналы защиты. Затем уничтожаются противугонные устройства [7, с. 90].

Хищение автомобиля с целью последующего его возврата собственнику за денежное вознаграждение.

Хищение автомобилей имеет различные цели: последующая перепродажа автомобиля с перебивкой vin-номера, разборка автомобиля на запчасти с их дальнейшей реализацией на авторынок, получение денежного вознаграждения за возврат транспортного средства собственнику. Распространены кражи заказного характера, когда преступники похищают определенный автомобиль для конкретного клиента [8, с. 19].

Наиболее часто похищаемыми автомобилями являются те, на которые существует спрос на рынке, как на сам автомобиль непосредственно, так и на его комплектующие части. «Таковыми автомобилями являются отечественные – Lada Priora и иностранные – Toyota Camry, Land Cruiser 200, Hyundai Solaris, Ford Focus. Есть и исключения, когда похищают редкие премиальные марки, но это происходит при заказных угонах».

Среди мест, в которых чаще всего совершаются кражи автотранспортных средств, можно отметить:

- парковки, непосредственно прилегающие к жилым домам (чаще всего в ночное время в дни недели с понедельника по четверг);
- стоянки, находящиеся возле торговых центров, магазинов, в местах значительного скопления людей и машин.

Распространенными причинами совершения краж автомобилей являются:

- отсутствие современной сигнализации с системой обратной связи;
- неправильный выбор парковочного места (темное, безлюдное место, где отсутствуют камеры наблюдения, или же камеры системы «Безопасный город»);
- кража редкого автомобиля по заказу конкретного лица (в таких ситуациях действуют профессиональные угонщики, применяющие самые современные технические средства и оборудование) [9, с. 127].

Самыми часто встречающимися в практике способами легализации похищенных автомобилей, являются: сбыт похищенного по поддельным документам; внесение в идентификационные номера изменений для сбыта по поддельным документам автомобилей-двойников; страховые и кредитные мошенничества; вывоз похищенного за пределы РФ и др. Для реализации большинства таких способов преступники сотрудничают на незаконной основе с подразделениями ГИБДД, которые предоставляют информацию о собственнике автомобиля, бланки ПТС, которые должны быть уничтожены и др. [10, с. 72]

Таким образом, оперативно-розыскная характеристика краж и угонов транспортных средств представляет собой совокупность сведений, отражающих признаки и элементы преступного деяния, знание которых будет способствовать выбору сотрудниками подразделений уголовного розыска наиболее эффективных методов и средств по выявлению, пресечению и

раскрытию преступных деяний, розыску лиц, непосредственно их совершивших [11, с. 16]. Самыми распространенными способами совершения хищения и угонов автотранспортных средств являются: механический способ; «испытание терпения: сигнализация «сошла с ума»; хищение путем использования кодграббера; бесключевой доступ; насильственное завладение чужим автомобилем (грабеж или разбой) [12, с. 45]. Для каждого из обозначенных способов характерны свои методы, посредством которых преступники совершают хищение или угон транспортных средств в различных целях (для перепродажи автомобиля посредством перебивки vin-номера автомобиля; для разборки автомобиля и перепродажи его частей; хищение редкого автомобиля для конкретного заказчика и др.).

1. Ларичев В.Д. Оперативно-розыскная характеристика экономических преступлений: понятие и содержание // Оперативник (сыщик). 2007. № 2 (11). С. 15-20 и др.
2. Гаджиев В.Э. Оперативно-розыскное обеспечение уголовного судопроизводства по делам о кражах скота (по материалам Сибирского федерального округа): автореф. дис. ... канд. юрид. наук. Саратов, 2012.
3. Кондратьев М.В. Оперативно-розыскная характеристика преступлений: к описанию понятия // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2012. № 5-1(19). С. 88-90.
4. Ларичев В.Д. Теория и практика борьбы с преступностью в сфере экономики: монография. М.: ВНИИ МВД России, 2009.
5. Хамидуллин Р.С. Некоторые особенности оперативно-розыскного противодействия кражам и угонам автотранспорта // Вестник Уральского юридического института МВД России. 2022. № 3. С. 105–110.
6. Бажко С.И. Способы совершения краж и неправомерного завладения автотранспортными средствами без цели хищения (угонов) и их предотвращение // Молодежь и наука: шаг к успеху: сб. материалов конференции, 2020. С. 28-30.
7. Флоря Д.Ф. Аспекты проведения отдельных следственных действий при необходимости получения информации с мобильных средств связи // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2017. № 1 (70). С. 89-92.
8. Мишуточкин А.Л. Особенности расследования краж автотранспортных средств, совершаемых организованными преступными группами: дис. ... канд. юрид. наук. Омск, 2000.
9. Грибунов О.П. Использование специальных знаний в раскрытии краж автотранспортных средств // Вестник Восточно-Сибирского института МВД России. 2019. № 3 (90). С. 125-132.
10. Кураков Д.В. Преступления, связанные с хищением автотранспортных средств, и пути их раскрытия // Наука и практика. 2016. № 2 (67). С. 70-73.

11. Муравьев К.В. Уведомление о подозрении в совершении преступления // Уголовный процесс. 2007. № 11. С. 16.
12. Муравьев К.В., Писарев А.В., Смирнова И.С., Супрун С.В. Уголовно-процессуальная деятельность органов дознания системы МВД России. М.: ЦОКР МВД России, 2010. 136 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Лисицын Андрей Григорьевич. Старший преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: оперативно-розыскная деятельность, транспортное средство розыск, хищение, угон, преступление.

Малик В.И.

КРАТКИЙ ОБЗОР ВСЕМИРНОГО ДОКЛАДА О НАРКОТИКАХ ЗА 2023 ГОД УПРАВЛЕНИЯ ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ ООН

Аннотация. Во Всемирном докладе УНП ООН о наркотиках за 2023 год предупреждается о сближении кризисов, поскольку незаконные рынки наркотиков продолжают расширяться. Новые оценки числа людей, употребляющих инъекционные наркотики, выше, чем предполагалось ранее, поскольку лечебные услуги и другие меры вмешательства недостаточны, в том числе рекордное количество людей, перемещенных из-за гуманитарных кризисов. «Дешевая и легкая» синтетика меняют рынки наркотиков со смертельными последствиями. Незаконный оборот наркотиков ускоряет разрушение окружающей среды и рост преступности в бассейне Амазонки. Необходимо усилить мониторинг воздействия на общественное здравоохранение на фоне быстрых нормативных изменений и клинических испытаний психоделиков.

Согласно Всемирному докладу о наркотиках за 2023 год [1], опубликованному Управлением ООН по наркотикам и преступности (УНП ООН), сохраняются рекордные объемы незаконных поставок наркотиков и все более гибкие сети их оборота усугубляют пересекающиеся глобальные кризисы и создают проблемы для служб здравоохранения и правоохранительных органов.

По новым данным, глобальная оценка числа людей, употребляющих инъекционные наркотики, в 2021 году составит 13,2 миллиона человек, что на 18 процентов выше, чем предполагалось ранее. В 2021 году во всем мире наркотики употребляли более 296 миллионов человек, что на 23 процента больше, чем за предыдущее десятилетие. Между тем число людей, страдающих зависимостью, вызванными употреблением наркотиков, резко возросло до 39,5 миллионов, что на 45 процентов больше, чем за 10 лет.

В докладе есть специальная глава, посвященная незаконному обороту наркотиков и преступлениям, наносящим ущерб окружающей среде в бассейне Амазонки, а также разделы, посвященные клиническим испытаниям психоделиков и использованию каннабиса в медицинских целях; употребление наркотиков в гуманитарных учреждениях; инновации в сфере лечения наркозависимости и других услуг; наркотики в условиях конфликтов.

Во Всемирном докладе о наркотиках также подчеркивается, как социальное и экономическое неравенство вызывает проблемы, связанные с наркотиками, и само обусловлено ими; разрушение окружающей среды и нарушения прав человека, вызванные незаконной торговлей наркотиками; и растущее доминирование синтетических наркотиков.

Согласно докладу, спрос на лечение расстройств, связанных с употреблением наркотиков, остается в значительной степени неудовлетворенным. В 2021 году только каждый пятый человек, страдающий расстройствами, связанными с наркотиками, проходил лечение от употребления наркотиков, при этом неравенство в доступе к лечению в разных регионах увеличивалось.

Молодежь наиболее уязвима к употреблению наркотиков, а также в некоторых регионах более серьезно страдает от расстройств, связанных с употреблением психоактивных веществ. В Африке, 70 % людей, проходящих лечение, моложе 35 лет [2].

В докладе утверждается, что общественное здравоохранение, профилактика и доступ к лечебным услугам должны быть приоритетными во всем мире, иначе из-за проблем, связанным с наркотиками на «дне» окажется все больше людей. В докладе также подчеркивается необходимость принятия мер правоохрательными органами, чтобы идти в ногу с гибкими моделями криминального бизнеса и распространением дешевых синтетических наркотиков, которые легко вывести на рынок.

Некоторые бедные и уязвимые группы населения, например, проживающие в районе трех границ между Бразилией, Колумбией и Перу, оказались в ловушке в сельских районах с высокой распространенностью преступлений, связанных с наркотиками. Их отдаленное расположение делает для них чрезвычайно трудным получение лечебных услуг, ресурсов или защитой со стороны государства.

Приоритет общественного здравоохранения при регулировании медицинского использования контролируемых наркотиков

Новые исследования по использованию контролируемых наркотиков, таких как психоделики, для лечения психических заболеваний и расстройств, вызванных употреблением психоактивных веществ, показывают многообещающие результаты, в докладе предупреждается, что быстрые темпы развития могут поставить под угрозу усилия по принятию политики, ставящей интересы общественного здравоохранения выше коммерческих интересов. Без хорошо продуманных и адекватно исследованных механизмов доступ к психоделикам для тех, кто нуждается в лечении, может оказаться слишком ограниченным, что может привести к тому, что пациенты обратятся на нелегальные рынки, или, наоборот, психоделики могут быть перенаправлены для немедицинского использования [3].

Растущее доминирование синтетических наркотиков

Дешевое, простое и быстрое производство синтетических наркотиков радикально изменило многие незаконные рынки наркотиков. Преступники, производящие метамфетамин – доминирующий в мире нелегально производимый синтетический наркотик – пытаются уклониться от реагирования правоохранительных органов и используя новые пути синтеза, обойти операционные базы неконтролируемых прекурсоров.

Фентанил радикально изменил рынок опиоидов в Северной Америке, что привело к ужасным последствиям. В 2021 году большинство из примерно 90 000 случаев смерти от передозировки опиоидами в Северной Америке были связаны с нелегально изготовленным фентанилом.

Каннабис

Каннабис на сегодняшний день остается наиболее часто употребляемым наркотиком в мире. В 2021 году каннабис употребляли около 219 миллионов человек, или 4 % населения мира. Число людей, употребляющих каннабис, увеличилось на 21 % за последние десять лет. В Америке на севере страны уровень употребления каннабиса остается самым высоким, поскольку в 2021 году его употребляли 17,4 % населения в возрасте от 15 до 64 лет. Каннабис остается основным наркотиком, вызывающим проблемы у большинства людей, проходящих лечение в Африке.

Основной проблемой на глобальном уровне приходится на каннабис, что отчасти объясняется широкой распространенностью его потребления: по оценкам, 41 % случаев расстройств, связанных с употреблением наркотиков, во всем мире связаны с употреблением каннабиса (2019 г.). В 2021 году около 46 % стран заявили, что каннабис является первым веществом, вызывающим такие расстройства, а 34 % – что он является основной причиной обращения за наркологической помощью.

Опиоиды

По оценкам, в 2021 году 60 миллионов человек употребляли опиоиды, что составляет 1,2 % населения мира. Половина из них проживала в

южной или Юго-Западной Азии. Из общего числа людей, употреблявших опиоиды в 2021 году, по оценкам, 31,5 миллиона человек употребляли опиаты, в основном героин. Во всем мире употребление опиоидов в 2021 году оставалось стабильным, после небольшого увеличения в период с 2017-го по 2019 год, около 38 % людей, проходивших лечение от употребления наркотиков в 2021 году, назвали опиоиды основным употребляемым наркотиком. Опиоиды остаются самыми смертоносными наркотиками; на их долю приходится две трети смертей, непосредственно связанных с наркотиками (в основном от передозировок) [4].

В 2022 году площади, занятые под выращивание опийного мака во всем мире, увеличились на 28 %. Производство опиума снизилось на 3 процента, тем не менее сохраняется долгосрочная тенденция к росту. В 2022 году на Афганистан по-прежнему приходилась большая часть (80 %) мирового незаконного производства опиума, балканский маршрут остается основным маршрутом незаконного оборота опиатов, а в 2021 году объем изъятий резко возрос после того, как в 2020 году разразилась пандемия COVID-19. Объемы изъятий фармацевтических опиоидов, которые в долгосрочной перспективе имеют тенденцию к росту, резко возросли в 2021 году.

Две вспышки злоупотребления опиоидами – фентанилом в Северной Америке и трамадолом в Северной и Западной Африке, на Ближнем и Среднем Востоке и в Юго-Западной Азии – продолжают представлять значительный риск для здоровья. В Африке в последние годы наблюдались признаки увеличения немедицинского использования трамадола и причиненного им вреда. В Северной Америке число смертей от передозировки фентанила достигло беспрецедентного уровня во время пандемии COVID-19. Доступ к фармацевтическим опиоидам для обезболивания и паллиативной помощи по-прежнему значительно различается в странах с низким и средним уровнем дохода и странах с высоким уровнем дохода.

1. Всемирный доклад о наркотиках за 2023 год [Электронный ресурс] // Управление по наркотикам и преступности ООН. URL: <https://www.unodc.org/unodc/index.html> (дата обращения: 11.11.2023).

2. Доклад Секретариата по поводу незаконного оборота наркотиков (E/CN.7/2017/5) [Электронный ресурс] // Управление по наркотикам и преступности Организации Объединенных Наций. URL: <https://undocs.org/Home/Mobile?FinalSymbol=E%2FCN.7%2F2017%2F5&Language=E&DeviceType=Desktop&LangRequested=False> (дата обращения: 11.11.2023).

3. Куликов А.В., Шелег О.А. Особенности возбуждения уголовных дел о преступлениях, связанных с незаконным оборотом наркотических средств // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 3 (96). С. 98-105.

4. Единая конвенция о наркотических средствах от 30.03.1961 с поправками, внесенными в нее в соответствии с Протоколом 1972 года // Бюллетень международных договоров. 2000. № 8. С. 15–20.

СВЕДЕНИЯ ОБ АВТОРЕ

Малик Владислав Игоревич. Преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: наркотические средства, незаконный оборот наркотиков, Организация Объединённых Наций, всемирный доклад.

Митряев И.С.

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА СОВРЕМЕННОМ ЭТАПЕ

Аннотация. В данной научной статье рассмотрены основные методы защиты персональных данных в эпоху цифровой трансформации. Анализируются проблемы, связанные с безопасностью данных, а также рассматриваются современные технологии и инструменты для защиты персональных данных. Результаты исследования могут быть использованы для разработки новых подходов к обеспечению безопасности персональных данных в условиях быстрого развития цифровых технологий.

В наше время, когда все больше людей используют цифровые устройства для выполнения различных задач, защита персональных данных становится все более актуальной проблемой. Вместе с тем, цифровая трансформация приводит к созданию новых возможностей для хищения и злоупотребления личными данными. В данной статье мы рассмотрим методы защиты персональных данных в эпоху цифровой трансформации.

Эпоха цифровой трансформации, или Четвертая промышленная революция, – это период в истории человечества, связанный с внедрением новых технологий, которые изменяют способы производства, обмена информацией, общения и взаимодействия людей. Эта эпоха началась в конце XX века и продолжается до сегодняшнего дня.

Основными технологическими инновациями, которые привели к цифровой трансформации, являются компьютеры, Интернет, мобильные устройства, облачные технологии, искусственный интеллект, интернет ве-

щей и блокчейн. Эти технологии изменили не только производственные процессы, но и общество в целом.

Цифровая трансформация повлияла на почти все сферы жизни: от бизнеса и экономики до культуры и образования. Так, например, электронная коммерция изменила способ покупки и продажи товаров и услуг, а социальные сети стали главным средством коммуникации и общения между людьми.

Одним из наиболее значимых аспектов цифровой трансформации является использование больших данных (Big Data), которые представляют собой огромные объемы информации, полученные из различных источников. Обработка и анализ этих данных позволяют получать новые знания и предсказывать поведение пользователей, что может быть использовано в маркетинге, медицине, науке и других областях.

Однако вместе с преимуществами, цифровая трансформация также приводит к ряду проблем, связанных с безопасностью данных. С увеличением объема и важности персональных данных, таких как финансовые данные, медицинские записи и другие, возникает угроза их кражи, потери или неправомерного использования. Это делает вопрос защиты персональных данных более актуальным и важным, чем когда-либо.

Анализ проблемы защиты персональных данных позволяет понять, почему эта проблема стала настолько актуальной в эпоху цифровой трансформации. Одной из основных причин является то, что люди все чаще используют цифровые устройства для выполнения различных задач, таких как банковские операции, покупки, обмен сообщениями и хранение личных данных.

При этом, данные могут быть украдены злоумышленниками, которые могут использовать их для совершения различных видов мошенничества, в том числе для доступа к банковским счетам, кражи личных фотографий или конфиденциальной информации.

Важно отметить, что угрозы для персональных данных могут быть не только с внешних источников, но и изнутри. Например, компании и организации могут собирать и использовать личные данные пользователей для своих целей без их согласия. Это может привести к утечке личной информации и нарушению прав на конфиденциальность.

Одним из наиболее распространенных методов защиты персональных данных является шифрование. Шифрование позволяет скрыть данные, что делает их непонятными и недоступными для злоумышленников. Кроме того, шифрование может быть использовано для защиты данных, хранящихся на устройствах, например, на жестких дисках или USB-накопителях.

Другой метод защиты персональных данных – это использование паролей и аутентификации. Пароли позволяют ограничить доступ к личным данным, а аутентификация позволяет убедиться в том, что только правиль-

ные пользователи имеют доступ к данным. Однако важно использовать надежные пароли, чтобы избежать их взлома.

Третьим методом защиты персональных данных является использование программного обеспечения для защиты от вредоносных программ и хакерских атак. Это может включать в себя использование антивирусных программ, брандмауэров, антишпионского и антифишингового ПО.

Существует несколько методов защиты персональных данных, которые используются в эпоху цифровой трансформации. Рассмотрим наиболее эффективные и распространенные из них.

1. Шифрование данных. Этот метод заключается в переводе читаемого текста в нечитаемый вид, который можно прочитать только с помощью ключа шифрования. Таким образом, при передаче данных через интернет они будут защищены от несанкционированного доступа.

2. Использование паролей и многократной аутентификации. Пароль – это наиболее распространенный способ защиты доступа к персональным данным. Вместе с тем, для большей безопасности может быть использована многократная аутентификация, при которой пользователю необходимо пройти несколько этапов проверки своей личности для получения доступа к данным.

3. Правила доступа. Организации, хранящие персональные данные, должны иметь четкие правила доступа к этим данным. Например, должны быть установлены ограничения на доступ к данным, и только соответствующий персонал должен иметь право просматривать и изменять эти данные.

4. Аудит безопасности. Для эффективной защиты персональных данных необходимо постоянно контролировать и анализировать систему безопасности. Для этого используется аудит безопасности, который позволяет выявлять возможные уязвимости в системе и принимать меры по их устранению.

5. Физическая защита. Для защиты персональных данных необходимо не только электронные методы, но и физическая защита, например, использование замков и системы контроля доступа в зданиях, где хранятся данные.

6. Маскирование данных. Этот метод заключается в изменении или замене некоторых частей персональных данных, чтобы сделать их менее узнаваемыми или идентифицируемыми. Например, номер кредитной карты может быть заменен на последние четыре цифры или на уникальный идентификатор, чтобы сделать его менее уязвимым для взлома.

7. Анонимизация данных. При использовании этого метода персональные данные преобразуются в неличные данные, которые не могут быть идентифицированы с конкретным пользователем. Это позволяет использовать данные для статистических или исследовательских целей без нарушения приватности пользователей.

8. Защита от вредоносных программ. Вредоносные программы, такие как вирусы, трояны или шпионское ПО, могут быть использованы для получения доступа к персональным данным. Для защиты от этих угроз необходимо использовать антивирусное программное обеспечение и другие инструменты для защиты от вредоносных программ.

9. Защита от социальной инженерии. Социальная инженерия – это метод, при котором злоумышленник использует социальную манипуляцию для получения доступа к персональным данным. Для защиты от этого метода можно проводить обучение пользователей, чтобы они знали, как определить и избежать подобных атак.

10. Защита от атак на сетевой уровень. Некоторые злоумышленники могут использовать атаки на сетевой уровень, например, атаку межсетевого экрана или перехват сетевого трафика, чтобы получить доступ к персональным данным. Для защиты от таких атак можно использовать различные методы, такие как использование сетевых экранов, защита от перехвата трафика и т.д.

Все эти методы защиты персональных данных должны применяться в комплексе для максимальной защиты. Важно также понимать, что защита персональных данных – это не статический процесс, а постоянный, который должен постоянно адаптироваться к изменяющимся условиям и угрозам.

Таким образом цифровая трансформация имеет огромный потенциал для развития общества и экономики, но вместе с тем она создает угрозы безопасности персональных данных. В данной статье были рассмотрены основные методы защиты персональных данных в эпоху цифровой трансформации. Рассмотрены современные технологии и инструменты для защиты данных, такие как криптография, аутентификация, авторизация и контроль доступа. Однако эти методы не могут гарантировать абсолютную безопасность данных. Решение проблемы защиты персональных данных требует комплексного подхода и постоянного обновления методов защиты в соответствии с развитием цифровых технологий.

-
1. Сибел Т. Цифровая трансформация. Как выжить и преуспеть в новую эпоху. М.: Манн, Иванов и Фербер, 2021.
 2. Келлехер Дж., Тирни Б. Наука о данных. М.: Альпина паблишер, 2020.
 3. Оганесян Т.Д. Право на защиту персональных данных: исторический аспект и современная концептуализация в эпоху Big Data // Журнал зарубежного законодательства и сравнительного правоведения. 2020. № 2.
 4. Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. 2018. Т. 13. № 5.
 5. Ковлер А.И. Права человека в цифровую эпоху // Бюллетень Европейского суда по правам человека. 2019. № 6.

6. Муравьев К.В., Писарев А.В., Смирнова И.С., Супрун С.В. Уголовно-процессуальная деятельность органов дознания системы МВД России. М.: ЦОКР МВД России, 2010. 136 с.
7. Митряев И.С., Лысенко Е.С., Острякова А.Ф. Технология блокчейн и криптовалюта: инструменты цифровой трансформации // Аграрное и земельное право. 2022. № 4. С. 132-137.
8. Семенов Е.Ю. Совершенствование правовых и организационных аспектов защиты персональных данных в Российской Федерации // Закон и право. 2022. № 1.
9. Линьков В.В., Семенов Е.Ю. Правовые проблемы защиты персональных данных при интеграции Интернета вещей в повседневную жизнь // Закон и право. 2020. № 10.

СВЕДЕНИЯ ОБ АВТОРЕ

Митряев Иван Сергеевич. Преподаватель кафедры информационных технологий в деятельности органов внутренних дел.

Орловский юридический институт МВД России имени В.В. Лукьянова

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: защита персональных данных, цифровая трансформация, безопасность данных, методы защиты, криптография, аутентификация, авторизация, контроль доступа.

Поддубный И.В.

ОТДЕЛЬНЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ УГОЛОВНОГО РОЗЫСКА ПО РАСКРЫТИЮ УБИЙСТВ

Аннотация. Статья посвящена некоторым особенностям деятельности подразделений уголовного розыска по раскрытию убийств. Отмечается, что при раскрытии вышеуказанных преступлений, имеет значение своевременное получение и эффективное использование оперативной информации. На основе изучения оперативной практики автором даются рекомендации, направленные на повышение эффективности раскрытия убийств и изобличения преступников. Отдельно анализируются этапы раскрытия убийств, особенности планирования и система действий по отработке различных версий.

Раскрытие убийств представляет собой осуществление оперативными подразделениями ОВД и аппаратами предварительного следствия в пределах их компетенции оперативно-розыскных мероприятий и следственных действий по обнаружению признаков общественно опасного деяния, установлению лиц, их совершивших, и принятия к ним мер ответственности в соответствии с законом [1, с. 41].

Успешному раскрытию убийств способствует, своевременное оперативно-розыскное сопровождение уголовных дел, которое выражается в деятельности оперативных подразделений органов внутренних дел по созданию оптимальных условий для полного и объективного расследования уголовных дел путем осуществления оперативно-розыскных мероприятий в отношении лиц, предметов и фактов, представляющих оперативный интерес, обеспечению использования их в качестве доказательств по уголовном делу и преодолению противодействия расследования. При этом необходимо сказать о том, что действия оперативных сотрудников различаются в зависимости от стадии расследования уголовного дела. Так особенности действий при поступлении сообщения об убийстве отличается от тактики действий при раскрытии убийства, уголовное дело по которому приостановлено.

Поэтому в настоящей статье будут рассмотрены общие рекомендации, приемы и система действий оперативных сотрудников уголовного розыска на различных этапах расследования указанного преступления.

После получения сообщения об убийстве на место происшествия выезжает следственно-оперативная группа, в которую обязательно входит следователь Следственного комитета России и сотрудники уголовного розыска. По прибытии на место следователь дает поручения о производстве тех или иных действий и совместно с судебно-медицинским экспертом и специалистом-криминалистом приступают к осмотру места происшествия.

Сотрудники уголовного розыска в это же время либо выполняют данные следователем поручения либо, как бывает в большинстве случаев, самостоятельно планируют и осуществляют комплекс первоочередных мероприятий.

В данном случае система мер, осуществляемых оперуполномоченными, может содержать в себе следующие действия:

- принятие мер по задержанию преступника по горячим следам;
- участие в осмотре места происшествия;
- организация и осуществление оперативно-розыскных мероприятий по сбору сведений и фактов, имеющих значение для раскрытия дела.

На основании вышеизложенного, считаем целесообразным более подробно рассмотреть заключительный пункт действий, являющийся на наш взгляд центральным, так как инструментарий оперативно-розыскной деятельности позволяет оперуполномоченному получить большой массив информации о произошедшем.

При принятии решения о производстве оперативно-розыскных мероприятий по сбору сведений и фактов, имеющих значение для раскрытия дела, оперативный сотрудник должен осуществить следующие действия:

- произвести поквартирный обход домов, находящихся в непосредственной близости от места происшествия;
- расширить зону осмотра места происшествия;
- получить записи с камер наружного видеонаблюдения вблизи с местом происшествия;
- установить возможных свидетелей произошедшего и зафиксировать данные ими сведения.

Указанные действия позволяют оперуполномоченному получить сведения о [2, с. 131]:

- личности потерпевшего;
- характере произошедшего;
- обстановке совершения преступления;
- обстоятельствах, предшествовавших убийству;
- соответствии места обнаружения трупа месту причинения повреждений;
- возможном количестве преступников.

По окончании работы на месте происшествия следователь систематизирует полученную информацию и принимает одно из следующих решений:

- о возбуждении уголовного дела по признакам преступления, предусмотренного ст. 105 Уголовного кодекса Российской Федерации;
- о необходимости дополнительной проверки произошедшего в целях уточнения обстоятельств совершения преступления;
- об отказе в возбуждении уголовного дела;

Таким образом, первоначальный этап раскрытия убийства содержит в себе действия, направленные на получение как можно более подробной информации о произошедшем, необходимой для принятия соответствующего процессуального решения. На момент окончания первоначального этапа может сложиться две ситуации, от которых зависит содержание последующего этапа раскрытия преступления:

- лицо, совершившее преступление установлено, но его местонахождение неизвестно;
- лицо, совершившее преступление не установлено.

Также возможна еще одна ситуация, когда лицо, совершившее преступление установлено, но в уголовном деле недостаточно доказательств, подтверждающих его виновность. При данных обстоятельствах оперативно-розыскное сопровождение уголовного дела продолжается, но уже в направлении получения информации в отношении лиц, предметов и фактов, представляющих оперативный интерес, обеспечению использования

их в качестве доказательств по уголовному делу и преодолению противодействия расследования со стороны подозреваемого или обвиняемого.

Убийство является традиционным направлением работы «от преступления – к лицу» [3, с. 14], откуда следует, что дальнейшее раскрытие организуется, основываясь на информации, полученной на месте происшествия.

Как указывалось ранее к такой информации относится:

- личность потерпевшего;
- характер произошедшего;
- обстановка совершения преступления;
- обстоятельства, предшествовавшие убийству;
- соответствие места обнаружения трупа месту причинения повреждений;
- возможное количество преступников.

Исходя из данных сведений, сотрудники уголовного розыска осуществляют планирование дальнейшей деятельности. Важно отметить, что содержание планирования при подобных условиях должно содержать следующие элементы [4, с. 618]:

- формулирование круга обстоятельств, подлежащих установлению в ходе проведения оперативно-розыскных мероприятий;
- анализ и оценка первоначальной информации, полученной в результате их проведения;
- постановка точных вопросов по фактам, которыми интересуются оперативные подразделения;
- определение направлений и системы действий, ведущих к разрешению поставленных вопросов в процессе обозначенных следственных действий и розыскных мероприятий.

Планирование заканчивается составлением плана оперативно-розыскных мероприятий по отработке выдвинутых оперативно-розыскных версий.

Наиболее часто встречающимися версиями об убийствах являются следующие предположения [5, с. 214]:

- убийство, совершенное по найму;
- убийство совершено лицом, ранее судимым за аналогичные преступления против личности;
- убийство совершено лицом из близкого круга убитого;
- убийство совершено лицом, страдающим психическим расстройством.

Каждая из перечисленных оперативно-розыскных версий имеет свои особенности в содержании и тактике оперативно-розыскных мероприятий.

Обязательными действиями по отработке каждой из версий являются следующие действия:

- ориентирование личного состава территориальных и транспортных органов внутренних дел, оперативных подразделений системы исполнения уголовного наказания по обстоятельствам совершенного преступления;
- привлечение общественности к раскрытию преступления;
- назначение судебно-медицинской экспертизы в целях установления причины смерти;
- установление личности жертвы, если она не была установлена ранее;
- изучаются архивные уголовные дела и дела оперативного учета, обстоятельства совершения которых, аналогичны расследуемому преступлению;
- отработка связей потерпевшего и выявление среди них лиц, ранее судимых за совершение преступления против личности, лиц, страдающих психическими расстройствами;
- изучение лиц из окружения потерпевшего, имеющих криминальное прошлое или имеющих связи в криминальном мире;
- при подозрении определенного лица осуществление в отношении него оперативно-технических мероприятий (прослушивания телефонных переговоров, снятия информации с технических каналов связи, получения компьютерной информации);
- в случае убийства лица из огнестрельного оружия назначение баллистической экспертизы в целях установления признаков оружия и их сравнение с результатами других экспертиз, проводимых в рамках других уголовных дел и дел оперативного учета.

Таким образом, подводя итог необходимо отметить, что на современном этапе развития оперативно-розыскной деятельности оперативное сопровождение уголовного дела поделено на два взаимосвязанных этапа: первоначальный и последующий.

Каждый из них имеет собственные задачи, которые могут быть достигнуты эффективным осуществлением оперативно-розыскных мероприятий. Если в ходе первоначального этапа информация о произошедшем собирается в целях принятия соответствующего процессуального решения о возбуждении уголовного дела, то в последующем этапе информация, получаемая оперативными сотрудниками, носит конкретный характер, который подтверждает или опровергает ту или иную версию.

1. Екимцев С.В. Некоторые аспекты деятельности ОВД по раскрытию убийств // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2018. № 3 (76). С. 41-43.

2. Сыпачев А.Ю., Ярошенко С.А. Отдельные аспекты раскрытия умышленных убийств // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 129-134.
3. Попов А.В. Актуальные вопросы организации оперативно-розыскной деятельности по раскрытию убийств, совершаемых по найму // Научные тенденции: Юриспруденция: сборник научных трудов по материалам XI международной научной конференции (Санкт-Петербург, 20 января 2018 г.). Санкт-Петербург: Международная Объединенная Академия Наук, 2018. С. 14-19.
4. Доровин С.А. Раскрытие убийств сотрудниками оперативных подразделений органов внутренних дел // Концепт. 2015. Т. 30. С. 616-620.
5. Уголовный процесс: учебник для вузов / А.Н. Артамонов, А.М. Баранов, А.С. Бахта [и др.]; под ред. Б.Б. Булатова, А.М. Баранова. 2-е издание, переработанное и дополненное. М.: ЮРАЙТ, 2010. 606 с.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Поддубный Илья Васильевич. Кандидат юридических наук. Преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: убийство, раскрытие, планирование, оперативно-розыскные мероприятия.

Рощупкина А.В.

СОВЕРШЕНСТВОВАНИЕ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОВД ПО РАСКРЫТИЮ ВЗЯТОЧНИЧЕСТВА

Аннотация. Статья посвящена некоторым особенностям деятельности подразделений уголовного розыска по раскрытию взяточничества. Отмечается, что при раскрытии вышеуказанных преступлений, имеет значение своевременное получение и эффективное использование оперативной информации. На основе изучения оперативной практики автором даются рекомендации, направленные на повышение эффективности раскрытия взяточничества. Отдельно анализируются этапы раскрытия мошенничества, особенности планирования и система действий по раскрытию преступлений.

Составными частями противодействия коррупции являются выявление, предупреждение, пресечение, раскрытие и расследование коррупционных правонарушений (борьба с коррупцией) [1, с. 4], поскольку уровень распространения этого социально-правового явления стал реально угрожать национальной безопасности страны.

По мнению авторов, существующие в данный момент средства, возможности по раскрытию преступлений коррупционной направленности нуждаются в повышении их эффективности.

Стоит отметить, что по-прежнему достаточно большой процент коррупционных преступлений приходится на правоохранительные органы. Так, коррупция в системе МВД России остаётся на достаточно высоком уровне. Количество жалоб на сотрудников правоохранительных органов уже давно не поддаётся никаким подсчётам. По словам генерального прокурора РФ, больше всего приговоров за коррупцию с января по сентябрь 2021 года было вынесено в отношении полицейских (672 из 898). При этом нельзя сказать, что государство оставляет данную проблему без внимания [2, с. 3].

В этой связи можно отметить, что подобное явление негативно сказывается на раскрытии иных преступлений представляющих серьёзную угрозу для общества и государства. Так, например, происходит усиление влияния преступных групп и сообществ, которые находятся под покровительством коррумпированных сотрудников.

Особая роль отводится ОРД относительно вопросов раскрытия преступлений коррупционной направленности. В этой связи необходимо рассмотреть пути совершенствования основных методов по раскрытию данных преступлений.

Как показывает практика, правоохранительные органы не сильно заинтересованы в приобщении средств массовой информации к их основной деятельности. С одной стороны можно отметить, что специфика работы правоохранительных органов не позволяет в полной мере сделать их работу полностью открытой для общественности. С другой стороны, привлечение граждан к содействию правоохранительным органам может оптимизировать сложный процесс раскрытия преступлений коррупционной направленности. Также подобное взаимодействие сможет оказать положительный эффект на повышение уровня доверия граждан к правоохранительным органам.

Статистика доверия граждан к правоохранительным органам, представленная за прошлый год ВЦИОМ говорит, что чуть больше половины граждан 57 % доверяют правоохранительным органам [3, с. 21]. Остальные относятся к правоохранительным органам скептически, что обусловлено в том числе, встречающимися на практике случаями получения взяток.

Таким образом, сеть Интернет и иные СМИ могут стать непосредственными источниками оперативно-значимой информации. Во многом

преимущество такого способа предоставления информации заключается в анонимности. Нежелание граждан действовать от своего имени, вполне оправданно, т.к. подача жалобы в этом случае может спровоцировать в отношении лица негативные последствия со стороны руководителя организации или лиц, которые имеют отношение к противоправной деятельности. Кроме того сотрудники могут самостоятельно проводить мониторинг сайтов имеющих антикоррупционный характер для последующего выявления и раскрытия преступлений.

Однако нельзя сказать, что данный способ получения информации является основным.

В оперативно-розыскной деятельности, направленной на раскрытие преступлений коррупционной направленности, в частности, получение взятки должностным лицом, особый интерес представляет проведение оперативного эксперимента. Ранее уже говорилось о том, что подобное мероприятие постепенно отходит на второй план. В данном случае это обосновано тем, что зачастую при раскрытии преступлений по ст. 291 УК РФ, происходит проблема определения границ проведения оперативного эксперимента, и сотрудники, которые организовали данное мероприятие, сами становятся подозреваемыми в совершении преступления.

В этой связи требуется рассмотреть возможные пути преодоления имеющихся проблем при производстве данного мероприятия. Сотруднику необходимо уделить внимание при производстве данного мероприятия на умысле разрабатываемого лица. В данном случае указанное лицо должно самостоятельно выразить желание на совершение противоправного деяния в том время как сотрудник не принимает к этому активных действий. Так наиболее уместно проводить оперативный эксперимент не для одного факта получения или дачи взятки, а для подтверждения цепочки лиц причастных к совершению данного преступления. Например, не производить задержание лица, которое получило денежные средства в ходе проведения данного ОРМ, а предоставить ему возможность передать ранее помеченные купюры третьему лицу, которое непосредственно является взяткополучателем и совершает определенные действия за данное вознаграждение.

Однако если речь идет о факте взяточничества со стороны конкретного лица, то оперативный эксперимент, возможно, проводить только в том случае, если должностное лицо самостоятельно выразило желание на совершение указанных противозаконных действий.

На сегодняшний день в целях недопущения возможности трактовать действия сотрудника, как вымогательство взятки, используются средства объективного контроля. Так, в соответствующих помещениях, устанавливаются средства негласного видеонаблюдения и аудио прослушивания.

Стоит отметить, что раскрытие преступлений связанных с получением взятки, равно как и наоборот является достаточно длительный и трудо-

ёмкий процессом, который порой требует от сотрудника не стандартных решений.

В этой связи выделяют отсутствие необходимой подготовки у сотрудников оперативных подразделений, а также опыта в раскрытии подобных преступлений. Следует сказать, как правило, не недостаток квалификации относится не только к сотрудникам оперативных подразделений, но и следствия. Так, встречаются случаи, когда следователь при получении заявления о готовящейся передаче взятки не предпринимает должных мер. В первую очередь причиной этому является отсутствие знаний о том, как необходимо действовать при раскрытии подобных преступлений.

Также необходимо правильно выстроенное взаимодействие оперативных подразделений и следственного органа. Особенно важно такое взаимодействие по вопросам составления доказательственной базы.

Некоторые авторы утверждают, что для раскрытия данных преступлений необходимо декриминализовать статью получения взятки и перевести данное деяние в разряд административных правонарушений. В данном случае такая позиция направлена на повышение раскрываемости фактов получения взятки должностным лицом, что имеет большую общественную опасность по сравнению с предыдущим деянием. Однако стоит заметить, что законодатель на сегодня фактически декриминализовал данную норму, указав на возможность уйти от уголовной ответственности при содействии правоохранительным органам. По нашему мнению данный подход наиболее правильный относительно данных преступлений и не нуждается в преобразовании.

Таким образом, раскрытие преступлений коррупционной направленности, в частности взяточничества, имеет свою специфику. Подобные преступления тщательно скрываются, а соответственно для их выявления требуется своеобразный подход. На сегодняшний день разработаны различные методы, которые способствуют выявлению данного вида преступлений. Однако по-прежнему имеются проблемные стороны, которые требуют корректировки.

1. О противодействии коррупции: Федер. закон Рос. Федерации от 25.12.2008 № 273-ФЗ // Собр. законодательства Рос. Федерации. 2008. № 52, ст. 6228.

2. Полицейских в 2021 году чаще других правоохранителей осуждали за коррупцию [Электронный ресурс]. URL: <https://ria.ru/20211209/korrupsiya-1762876118.html>.

3. Статистика одобрения деятельности общественных институтов, представленная ВЦИОМ 18.04.2022.

4. О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях: постановление Пленума Верховного Суда Рос. Феде-

рации от 09.07.2013 № 24: в ред. от 03.12.2013 // Бюллетень Верховного Суда Рос. Федерации. 2013. № 9.

5. Машков С.А. Раскрытие и расследование фактов взяточничества с использованием результатов оперативно-розыскной деятельности: автореф. дис. ... канд. юрид. наук. Иркутск, 2004. 22 с.

6. Борисов Б.В. Понятие, определение и значение оперативно-розыскной характеристики преступлений экономической направленности // Пробелы в российском законодательстве. 2014. № 1. С. 202-203.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Рощупкина Александра Витальевна. Адъюнкт кафедры оперативно-розыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: мошенничество, раскрытие, планирование, оперативно-розыскные мероприятия.

Смирнов И.М.

«СКАММИНГ» КАК НОВЫЙ ВИД СОВРЕМЕННОГО ИНТЕРНЕТ-МОШЕННИЧЕСТВА

Аннотация. В статье рассматривается в качестве типичного примера стандартная схема шантажа, реализуемого при помощи сети интернет, анализируются способы совершения данного преступления, технические средства и устройства, применяемые для достижения мошенниками преступных целей, принципы их работы с жертвами, способы уклонения от уголовной ответственности. Кроме того, в статье рассмотрены приёмы социальной инженерии, которые мошенники используют для обмана человека и снижения его бдительности.

Стремительное развитие телекоммуникационных возможностей человечества в начале текущего столетия породило и новые способы совершения преступных деяний, особенно преступлений против собственности. В настоящее время одним из самых распространенных преступлений остается мошенничество (ст. 159 УК РФ), представляющее собой, исходя из теории уголовного права, одну из форм хищения, которая осуществляется путем обмана или злоупотребления доверием.

В настоящей статье сделана попытка рассмотреть одну из разновидностей данного противоправного деяния, а именно мошенничество, совершенное с применением сетей связи и информационно-коммуникационных технологий.

В настоящее время существует огромное количество мошеннических схем, реализуемых при помощи сети интернет. В последние годы, с развитием компьютерных технологий, русский язык пополнился новым словом, а именно словом «скам». Данное понятие употребляется по отношению к мошенническим проектам, представляющим собой процесс получения денежных средств преступным путём лицом, или группой лиц, в результате самостоятельного перевода средств жертвой на счёт мошенников.

Практика показывает, что в 90 % случаев «скамеры» (те, кто занимается данным видом мошенничеств) являются несовершеннолетними лицами, либо очень молодого возраста (не превышающего 25 лет). Именно поэтому, в силу несформированности социальных ценностей, несоответствия личных норм морали общественным и неспособности оценить полноту ответственности за содеянное, их действия отличаются особой дерзостью, цинизмом и аморальностью по отношению к жертве преступления. В то же время, к честной работе они проявляют индифферентность.

В настоящее время в сети существует масса ресурсов, на которых мошенники обмениваются информацией о своем незаконном «искусстве», обсуждают полученный преступный опыт, вербуют новичков и преемников. Для обмена информацией скамеры пользуются не обязательно даркнетом. В число подобных площадок, входят не только малоизвестные ресурсы: <https://telegra.ph>, <https://zelenka.guru>, но и общедоступные сайты: <https://dzen.ru>, <https://youtube.com>.

Как утверждал великий китайский стратег и мыслитель Сунь-Цзы в своём произведении «Искусство войны», «если знаешь противника и знаешь себя, сражайся хоть сто раз, опасности не будет; если знаешь себя, а его не знаешь, один раз победишь, другой раз потерпишь поражение; если не знаешь ни себя, ни его, каждый раз, когда будешь сражаться, будешь терпеть поражение» [1, с. 67]. Руководствуясь приведенным подходом, попытаемся подробно разобрать в качестве типичного примера стандартную схему шантажа, реализуемого при помощи сети интернет, в котором анализируем способы совершения данного преступления, технические средства и устройства, применяемые мошенниками для достижения своих преступных целей, принципы их работы с жертвами, способы уклонения от уголовной ответственности.

Самой популярной схемой мошенничества является «Шантаж по интим фото» либо реже «Шантаж изменой». Схема состоит из нескольких пунктов:

- 1) Покупка аккаунта;
- 2) Поиск нужной информации;

- 3) Копирование компромата на жертву;
- 4) Приобретение поддельной страницы;
- 5) Непосредственно шантаж.

Второй популярной схемой является «Шантаж одиноких парней».

В данном случае немного сложнее, потому что требуются знания социальной инженерии.

Разберем по пунктам:

- 1) Создание или покупка готового аккаунта девушки;
- 2) Интимное фото похожей девушки;
- 3) Поиск мужчин и отбор их реальных страниц;
- 4) Беседа для добычи компромата;
- 5) Непосредственно шантаж.

В рассматриваемой сфере мошенничества без анонимности не обойтись, поэтому те люди, которые давно промышляют данным видом деятельности, имеют свой базовый набор для «безопасной» работы:

1) 3G-модем, который покупается у любого человека либо в переходе метро, без оформления документации;

2) SIM-карта, которая приобретается также у любого человека, либо в переходе метро, без оформления документации;

3) Виртуальная машина – VMware или VirtualBox (Виртуальная среда, работающая как настоящий компьютер, но внутри другого компьютера. Проще говоря, приложение, которое имитирует компьютер с полноценной операционной системой и аппаратным обеспечением);

4) Виртуальная частная сеть (так называемый VPN – «virtual private network». Для мошенников грамотный выбор надежного VPN – это гарант счастливой жизни на свободе).

Шифрование трафика, анонимность с отвязкой от регионального положения, отсутствие сохранения логинов и информации о выполненных действиях в сочетании с хорошим VPN, обычно такой набор функционала используется опытными скамерами [2, с. 45].

Для понимания механики процесса необходимо отметить, что:

Во-первых, 3G-модем и SIM-карта – это выход в сеть, их использование необходимо только во время самого шантажа.

Во-вторых, виртуальная среда (так называемая виртуальная машина) позволяет создать на компьютере ещё один компьютер, который будет использовать его ресурсы, но работать изолированно.

В-третьих, VPN скрывает IP и шифрует трафик.

В общем виде поиск жертв можно представить следующим образом. У скамера имеются аккаунты (традиционно около 100 единиц), но ему необходимо зайти на каждый из них и вручную искать потенциальную жертву. Опытные преступники обычно действуют по следующей схеме:

- 1) Открывается блокнот, куда копируются все аккаунты;

2) Оставляется 1 браузер (с которого ранее никуда преступник не заходил, т.е. рабочий);

3) Осуществляется выход из всех остальных браузеров, steam, icq, skype и любых программ, где ведется общение и прочее;

4) Подключается VPN (самый быстрый из имеющихся серверов);

5) Осуществляется вход на сайт «Вконтакте», «Одноклассники» или другой социальной сети и начать поиск компрометирующего материала.

Далее происходит непосредственно поиск и копирование компромата.

В средствах поиска по личным сообщениям вбиваются типичные фразы: «люблю», «любимый», «зая» – это позволяет найти всех бывших либо нынешних парней/девушек. Мошенник видит переписки с людьми, которым предполагаемая жертва это писала. Во вложениях диалога идёт поиск фото, и после того, как фотографии найдены, на флешке создаётся папка под жертву, сначала туда просто сохраняются фото, затем делаются скриншоты, подтверждающие, что эти фото были в данном диалоге. Чаще всего скриншоты делаются в самой беседе и «вложениях», для того чтобы жертва не утверждала в дальнейшем, что это подделка и «фотошоп» и на фото не она. Затем создаётся текстовый документ, куда записывается ссылка на аккаунт жертвы и весь список её друзей. Если в друзьях жертвы родственники, преподаватели или работодатели – они, отмечаются особенно.

Если в пабликах имеется что-то наподобие «Подслушано МГУ» (или иное учебное заведение), это тоже представляет ценность для мошенников и также подлежит сохранению. В конце скамер заходит в настройки приватности и открывает личные сообщения жертвы. На этом этапе советуют покинуть страницу и переходить к следующему этапу, но, если по каким-либо причинам информацию не удалось получить, преступник может перейти к углубленному поиску [3, с. 390].

Для этого открывается список друзей и как правило преступника интересуют первые 5-7 друзей, с которыми предполагаемая жертва общается чаще всего. В основном это могут быть лучшие друзья (в частности подруги), с которыми они возможно обменивались интимными фотографиями для сравнения. Также фотографии могут изыматься из вкладки «избранное».

Помимо этого, в поиске сообщений часто вводят такие слова, как «изменил/изменила», «секс» и прочие подобные фразы, чтобы выйти на диалог, в котором наглядно понятно, что потерпевший гражданин изменяет своему спутнику. Задача состоит в том, чтобы найти в сообщениях какую-либо порочащую жертву информацию, которая негативно окрашивает личность жертвы, что очень выгодно для скамера, ведь для него это составляет ценный компромат.

Как отмечают сами преступники, на проверку 100 аккаунтов уходит примерно 5 часов, вначале это дается сложнее, времени уходит значитель-

но больше. Когда человек набирается опыта, он будет это делать на полном «автомате». В среднем со 100 аккаунтов выходит от 7 жертв, бывают и случаи с 30 жертвами [4].

1. У-цзин. Семь военных канонов Древнего Китая / перевод с китайского и комментарии Ральфа Д. Сойера, 1993; перевод с английского Р.В. Котенко, 1997, 2001. Издательская группа «Евразия», 2001. 448 с.
2. Муравьев К.В., Писарев А.В., Смирнова И.С., Супрун С.В. Уголовно-процессуальная деятельность органов дознания системы МВД России. М.: ЦОКР МВД России, 2010. 136 с.
3. Уголовный процесс: учебник для вузов / А.Н. Артамонов, А.М. Баранов, А.С. Бахта [и др.]; под ред. Б.Б. Булатова, А.М. Баранова. 2-е издание, переработанное и дополненное. М.: ЮРАЙТ, 2010. 606 с.
4. Зарабатываем на шантаже [подробный мануал]. UMBRELLA [Электронный ресурс]. URL: <https://telegra.ph/Zarabatyvaem-na-shantazhe-podrobnyj-manual-10-21>.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Смирнов Иван Михайлович. Кандидат исторических наук. Старший преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: скам, скамминг, интернет-мошенничество, шантаж, оперативное противодействие мошенничеству.

Сущенко С.А.

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ СПЕЦИАЛЬНЫХ СЛЕДСТВЕННЫХ МЕРОПРИЯТИЙ В УГОЛОВНО-ПРОЦЕССУАЛЬНОМ ДОКАЗЫВАНИИ ЗАРУБЕЖНЫХ СТРАН

Аннотация. В статье в сравнительно-правовом аспекте рассматривается современное состояние правового регулирования использования результатов специальных следственных мероприятий в уголовно-процессуальном доказывании зарубежных стран.

Согласно принципу презумпции невиновности, установленному ч. 1 ст. 49 Конституции Российской Федерации [1] и ст. 14 Уголовно-процессу-

ального кодекса Российской Федерации [2], обвиняемый считается невиновным, пока его виновность в совершении преступления не будет доказана в предусмотренном УПК России порядке и установлена вступившим в законную силу приговором суда.

Данный принцип, а также положение, сформулированное в ч. 2 ст. 50 Конституции Российской Федерации, о том, что при осуществлении правосудия не допускается использование доказательств, полученных с нарушением федерального закона, определяют необходимость соблюдения принципа законности, который, в свою очередь, формулирует правило о том, что нарушение норм УПК России судом, прокурором, следователем, органом дознания, начальником подразделения дознания или дознавателем в ходе уголовного судопроизводства влечёт за собой признание недопустимыми полученных таким путём доказательств (ч. 3 ст. 7 УПК России).

Учёными и практическими работниками отмечаются трудности в вопросах определения допустимости доказательств, получаемых на основе результатов оперативно-розыскной деятельности (далее – ОРД). Такая ситуация обусловлена несколькими факторами: различием юридической природы результатов ОРД и доказательств, и субъектов получения таких результатов и доказательств; некорректностью формулировки ст. 89 УПК России, регулирующей использование результатов ОРД в доказывании; рамочным характером правил осуществления оперативно-розыскных мероприятий (далее – ОРМ) в Федеральном законе от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» [3] (далее – Закон об ОРД), затрудняющим оценку законности проведения таких мероприятий и др.

Проблема определения допустимости доказательств, получаемых на основе результатов оперативно-розыскной деятельности, присуща именно отечественному судопроизводству, поскольку уголовно-процессуальное законодательство и судебная практика зарубежных стран допускают использование в качестве доказательств по уголовным делам результатов оперативно-розыскной деятельности (или так называемых «тайных следственных мер») наряду со следственными действиями. Эти меры являются аналогом отечественных оперативно-розыскных мероприятий и в зарубежных странах носят разное название: *covert actions*, *special investigation techniques*, *undercover investigations* и др. В большинстве иностранных государств, многие из которых являются своеобразными законодателями «правовой» моды, все чаще приходят к выводу о диалектическом единстве познавательной направленности предварительного расследования и негласной деятельности полиции по раскрытию преступлений и участия в их дальнейшем расследовании и, как следствие, к постепенному стиранию правовых границ между указанной деятельностью и уголовным процессом.

Данная тенденция выражается в двух основных направлениях развития зарубежного законодательства. Первый путь состоит во введении в национальные уголовно-процессуальные кодексы правовых норм, которые

в России пока ещё рассматриваются как нормы исключительно оперативно-розыскного регулирования.

В Федеративной Республике Германии (далее – ФРГ) правила санкционирования, реализации и использования результатов негласных полицейских мер закреплены непосредственно в нормах уголовно-процессуального закона – Уголовно-процессуальном кодексе ФРГ (Strafprozeßordnung) [4] (далее – УПК ФРГ). Так, ст. § 110a–110с Уголовно-процессуального кодекса ФРГ регулируют институт участия в предварительном расследовании штатных негласных сотрудников полиции; § 100с УПК ФРГ предусматривает «меры, применяемые без ведома лиц, которых они касаются»; при этом речь идёт не только о порядке санкционирования таких мер, но и о правилах их реализации и дальнейшем использовании полученных результатов. Например, ч. 5 § 100с указывается, что информация, полученная в результате применения меры «прослушивание переговоров» внутри жилого помещения «может использоваться, только если интерес в отношении расследования фактических обстоятельств дела или установления места нахождения другого обвиняемого в том же уголовном производстве соразмерен значению доверительных отношений, лежащих в основе запрета». Параграфом 110h регулируется использование иных негласных мер: производство съёмки (кино-, видео-, фото); использование «иных технических средств, предназначенных для наблюдения». Таким образом, в ФРГ при соблюдении правил УПК, а не каких-либо иных подзаконных или ведомственных нормативных актов, результаты негласных мероприятий могут беспрепятственно использоваться в доказывании и принимаются непосредственно как допустимые.

В Уголовно-процессуальном кодексе Франции [5] нет прямого указания на порядок использования результатов негласных полицейских мер расследования, однако положение ст. 427 УПК Франции о свободе оценки доказательств сформировало поддержанную Кассационным судом Франции судебную практику использования в доказывании таких результатов, если соответствующие мероприятия проводились в надлежащем порядке, а те из них, которые ограничивали конституционные права личности, осуществлялись на законном решении следственного судьи или, в определённых случаях – судьи по свободам и задержанию.

В Великобритании п. 1.5 Закона о следственных полномочиях (Regulation of Investigatory Powers Act 2000) [6] прямо предусматривает, что если какие-либо положения кодекса представляются уместными для любого суда или трибунала (if any provision of the code appears relevant to any court or tribunal), результаты, полученные при применении относящихся к этому закону кодексов практики, допускаются как доказательства в уголовном и гражданском судопроизводстве; к данному закону относятся, в частности, кодекс практики о скрытом наблюдении и вмешательстве в частную жизнь [7], регулирующий порядок тайного наблюдения (в том

числе перехват телекоммуникационной информации), включая использование специальных технических средств.

В Китайской народной республике (далее – КНР) отсутствует отдельный закон, регулирующий специальные следственные мероприятия, поэтому китайский законодатель, опираясь на опыт ФРГ и США, закрепил их непосредственно в Уголовно-процессуальном кодексе Китайской Народной Республики [8]. Техничко-следственные мероприятия и тайные следственные действия, аналогичные российским оперативно-розыскным мероприятиям, впервые получили свое законодательное закрепление в нормах УПК КНР в 2012 году. Статья 154 УПК КНР закрепляет, что материалы, собранные при помощи мер технического расследования, могут быть использованы в качестве доказательств в уголовном процессе. Если использование таких доказательств может угрожать личной безопасности сотрудника, проводящего данные мероприятия, или привести к другим серьезным последствиям, необходимо принять защитные меры, чтобы избежать раскрытия применяемых технических мер и личности сотрудника. При необходимости судьи могут проверить полученные таким образом доказательства вне зала суда. Таким образом, результаты данных мероприятий имеют статус полноценного доказательства в уголовном судопроизводстве.

В Уголовно-процессуальном кодексе Эстонии от 12.03.2003 [9] введена вступившая в силу с 01.01.2013 глава 3.1 «Оперативно-розыскные мероприятия», при этом ч. 4 ст. 126.1 УПК этого государства прямо установила, что «информация, полученная путём оперативно-розыскного мероприятия, является доказательством, если при ходатайстве о выдаче разрешения на производство оперативно-розыскного мероприятия, его выдаче и совершении оперативно-розыскного мероприятия соблюдены требования закона» (следует признать, что приведённая формулировка гораздо удачнее положения, сформулированного в ст. 89 УПК России).

Другой путь состоит во введении в уголовно-процессуальный закон не отдельных положений, регулирующих, в сущности, возможность относительно несложного порядка использования результатов тайной полицейской деятельности в доказывании по уголовным делам, а в установлении правового института так называемого тайного (негласного, специального и др.) следствия. По данному пути активно пошли некоторые государства, формирующие после распада СССР национальное уголовно-процессуальное законодательство с учётом современных тенденций стран континентальной правовой семьи. Например, Закон об уголовном судопроизводстве (*Kriminālprocesa likums*) Латвийской Республики [10] содержит институт «специальных следственных действий» (*speciālās izmeklēšanas darbības*); аналогичный правовой институт введён и ст. 232 УПК Республики Казахстан.

Таким образом, в зарубежных странах теория уголовно-процессуального права не рассматривает различие правовой природы процессуальных доказательств и результатов негласной полицейской деятельности как фактор, определяющий недопустимость прямого использования таких результатов в уголовно-процессуальном доказывании, если они (результаты) получены с соблюдением законодательства и такой подход находит закрепление как в правовых актах, так и в прецедентной судебной практике. Допустимость таких доказательств регулируется правилами, предъявляемыми к другим видам доказательств, что позволяет беспрепятственно использовать результаты негласной полицейской деятельности в доказывании по уголовным делам.

1. Конституция Российской Федерации [Электронный ресурс]: принята всенародным голосованием 12.12.1993: с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. Доступ из справ.-правовой системы «КонсультантПлюс».
2. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: от 18.12.2001 № 174-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
3. Об оперативно-розыскной деятельности [Электронный ресурс]: Федер. закон Рос. Федерации от 12.08.1995 № 144-ФЗ. Доступ из справ.-правовой системы «Консультант Плюс».
4. Уголовно-процессуальный кодекс ФРГ / Strafprozeßordnung [Электронный ресурс] // Официальный сайт Министерства юстиции ФРГ. URL: <http://www.gesetze-im-internet.de/stpo> (дата обращения: 30.04.2023).
5. Code de procédure pénale (CPP) [Электронный ресурс] // Официальный сайт правовой информации Министерства юстиции Франции. URL: <http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154>.
6. Официальный сайт правовой информации правительства Великобритании [Электронный ресурс]. URL: <http://www.legislation.gov.uk/ukpga/2000/23/contents>.
7. Covert Surveillance and Property Interference: Code of Practice. Pursuant to Section 71 of the Regulation of Investigatory Powers Act 2000. London: The Stationery Office, 2014.
8. Портал законов Китая [Электронный ресурс]. URL: <https://ru.chinajusticeobserver.com/law/x/criminal-procedure-law-of-china-20181026> (дата обращения: 21.04.2023).
9. Kriminaalmenetluse seadustik [Электронный ресурс] // Сайт Государственного бюллетеня Эстонской Республики «Riigi Teataja». URL: <https://www.riigiteataja.ee/akt/120052016007>.
10. Latvijas Vēstnesis. 2005. № 74 (3232).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Сущенко Светлана Алексеевна. Кандидат юридических наук. Преподаватель кафедры оперативно-разыскной деятельности ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: уголовный процесс, доказывание, использование результатов ОРД, негласные полицейские меры, специальные следственные мероприятия.

Чаплыгина В.Н., Батуева А.Б.

ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ, ПРОВОДИМЫХ НА ПОСЛЕДУЮЩЕМ И ЗАКЛЮЧИТЕЛЬНОМ ЭТАПАХ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ НЕСОВЕРШЕННОЛЕТНИМИ, В СИЛУ ИХ ВОВЛЕЧЕНИЯ В НИХ

Аннотация. Авторами статьи рассматривается специфика следственных действий, проводимых на различных этапах расследования в рамках уголовного дела, субъектом которого является особый субъект – несовершеннолетний в силу его вовлечения в преступные действия.

Количество преступлений, ежегодно совершаемых в Российской Федерации несовершеннолетними или с их участием, остаётся на стабильно значительном уровне. Данные преступления отличаются определенной степени вовлекаемости несовершеннолетних в совершение преступления из-за их внушаемости и податливости несовершеннолетних к различным проявлениям извне и отсутствия собственного устойчивого жизненного опыта. Данный факт подтверждается тем, что почти половина от всех преступных проявлений, которые были реализованы лицами, не достигшими восемнадцати лет, совершены ими в соучастии (чаще со взрослыми). Статистика неумолимо свидетельствует о том, что среди всех граждан, совершивших преступления за период с 2018-го по 2022 год, доля несовершеннолетних в процентном соотношении составляет не более 5 % [1].

При расследовании преступлений, совершенных несовершеннолетними, существует такая тенденция, что именно на последующем этапе расследования осуществляются наиболее сложные и объёмные следственные и процессуальные действия. Данный этап также подразумевает возможность производства повторных и дополнительных следственных действий по необходимости [2, с. 235; 3, с. 101; 4, с. 49].

При расследовании преступлений, фигурантами которых являются несовершеннолетние, вовлечённые в совершение противоправных деяний, помощью для следователя могут оказаться данные, полученные оперативным путём в ходе проведения оперативно-розыскных мероприятий (ОРМ). В том числе грамотно проведённые комплексы ОРМ в отношении преступника, например, личный сыск, оперативная установка или агентурный метод, могут стать действенным условием для осуществления задержания подозреваемого с поличным. Однако его реализации предшествует некоторый ряд обязательных действий: сбор информации о вовлекателе: привычки, темперамент, образ жизни, круг общения, характер связи с несовершеннолетним; уточнение данных о возможном оказании сопротивления при задержании, а значит, если таковые имеются, поиск средств и методов для его подавления; сбор личного состава правоохранительных органов, участвующих в задержании, для инструктирования и выдачи специальных средств фото- и видеофиксации.

После реализации задержания, производится личный досмотр подозреваемого и места, где он был задержан с целью предотвращения сброса предметов, которые могут быть признаны вещественными доказательствами (личный мобильный телефон с имеющимися контактами, подтверждающими связи с несовершеннолетним, предмет преступления, на котором могли сохраниться следы совместного участия взрослого и подростка в его приобретении и т.п.). Если имеются точные знания о том, что у подростка, склоняемого к совершению преступления, наличествуют предметы, имеющие значение для расследования уголовного дела (свидетельствующие о вовлечении), может быть произведена их выемка с последующим осмотром.

Важное значение на последующем этапе расследования будет иметь допрос совершеннолетнего гражданина, вовлекшего несовершеннолетнего в совершение преступления, в качестве подозреваемого, целью которого будет установление – знал ли он фактический возраст подростка на момент склонения и осознавал ли, что вовлекает в противоправные деяния лицо, не достигшее 18 лет [5, с. 262]. Важно выяснить, когда и при каких обстоятельствах они познакомились, каковы были цели такого знакомства и какой способ вовлечения был выбран для этого.

Доказывание того, какой именно способ был использован, затруднено в связи с тем, что знает об этом обычно ограниченный круг лиц – только вовлекаемый и вовлекатель. Поэтому следователю необходимо прибегать к использованию различных тактик допроса, исходя из сложившейся ситуации (конфликтной или бесконфликтной). Действенными методами оказываются тактики форсированного допроса, предъявления доказательств, в том числе сообщение о факте того, что его соучастники в лице несовершеннолетних, дают изобличающие показания.

В случае отказа давать правдивые показания эффективным методом будет разъяснение лицу последствий, к которым это может привести.

В процессе изобличения лжи возможно использование таких тактик, при которых допрашиваемому предлагается пояснить что-либо о преступном событии в свободной форме, однако не зная, что именно интересно следователю, о чём он осведомлён, а о чём нет, лицо может запутаться в даваемых показаниях и случайно сообщить то, что, по его мнению, не значимо, но по факту является правдой [6, с. 219].

На последующем этапе после произведённых допросов немало важным будет являться производство обыска или выемки по месту жительства вовлекаемого для того, чтобы обнаружить или изъять у него предметы или документы, дающие основания полагать, что он с несовершеннолетним действительно был знаком либо знал о его возрасте, а также факт того, что процесс вовлечения действительно имел место, и в ходе этого подросток совершил противоправное деяние.

Следственная практика свидетельствует о том, что доказательство данного факта – сложный процесс. Но нельзя исключать ситуации, при которых, к примеру, документ, удостоверяющий личность подростка, может быть обнаружен у вовлекаемого дома. В ходе выемки мобильного телефона и осмотра имеющихся в нём переписок также возможен поиск среди смс-сообщений прямых указаний несовершеннолетнего на свой возраст.

В ходе допросов должна сложиться чёткая картина о том, имеется ли ложь в показаниях несовершеннолетнего либо совершеннолетнего лица. В случае возникновения в них существенных противоречий, требующих устранения, необходимо проведения очной ставки между ними. Следователю необходимо решить, целесообразно ли проведение данного следственного действия между подростком, с учётом его психологических особенностей, и совершеннолетним лицом.

Полагаем, что в случаях совершения преступлений несовершеннолетними в силу их вовлечения в них, очная ставка будет целесообразна лишь тогда, когда подросток встал на путь раскаяния, при этом отсутствуют основания для опасений по поводу того, что он в результате отрицательного влияния изменит свои показания, либо, когда следователь точно убежден, что проверить и устранить противоречивые показания иными процессуальными средствами невозможно.

Важно провести следственное действие так, чтобы подросток не чувствовал себя незащищённым, давая показания в присутствии того, кто его вовлекал, то есть обеспечить его надлежащую психологическую подготовку.

Учитывая опыт следственной практики, можно выделить некоторые особенности проведения очных ставок по рассматриваемой нами категории уголовных дел:

- Изучить показания подростка и взрослого, выяснить сущность имеющихся противоречий. У несовершеннолетнего они могут проявляться как в связи с заблуждением, так и благодаря воздействию мнения окружа-

ющих. При подготовке к следственному действию важно проанализировать данный круг общения, степень его влияния на мнение подростка.

- Установить, какие именно факты необходимо проверить, сформулировать вопросы, адресованные участникам, направленные на устранение противоречий, обращение в памяти к спорным моментам.

- Уделить внимание психологической подготовке подростка к следственному действию, объяснить, что со стороны соучастника возможно давление, просьбы отказаться от показаний, угрозы личного характера, которые не должны приводить к изменению показаний или отказу от них.

- Обычно несовершеннолетний допрашивается первым, чтобы в ходе очной ставки минимизировать влияние на него другого участника и каких-либо попыток внушения.

- Необходимость контролирования поведения взрослого, чтобы исключить негативное его воздействие на подростка. Данные действия предотвращаются путём постановки наводящих вопросов.

- Если есть необходимость, обусловленная большим количеством соучастников, то правильным было бы производство нескольких очных ставок. Допускается в виде психологического воздействия на лжеца демонстрация вещественных доказательств, протоколов и др.

- В случае изменения подростком своих показаний, целесообразно узнать этому причину, однако сделать это не на очной ставке, а на следующем допросе, когда взрослый подстрекатель будет отсутствовать.

Так или иначе, очная ставка довольно необходимое следственное действие, способствующее получению новых доказательств по делу. Однако на последующем этапе расследования возможно осуществление и иных следственных действий, среди которых наиболее актуальным является назначение и производство судебных экспертиз [7, с. 124]. Если имеются вещественные доказательства факта вовлечения подростка в совершение преступления, следы, изъятые с места происшествия, а также основания для установления психологического состояния вовлечённого, необходимо вынесение постановления о назначении судебных экспертиз и их последующее проведение.

Мы считаем, что наиболее часто назначаемыми по данным категориям дел экспертизами являются судебно-психиатрическая и судебно-психологическая экспертизы, благодаря которым возможно дать оценку уровню развития подростка, а также его эмоционально-волевой сферы. Возможно определить и его роль в преступлении, в которое он оказался вовлечён. Если несовершеннолетний достиг возраста уголовной ответственности, но имеет задержку в умственном развитии, не связанную с психическим расстройством, то он считается не подлежащим уголовной ответственности. Данные экспертизы необходимо именно для того, чтобы определить указанный факт. Их назначение имеет место быть тогда, когда возникает необходимость квалификации действий совершеннолетнего при во-

влечении. Если будет установлено, что вовлечённый в совершение преступления признан невменяемым, то будет считаться, что деяния взрослого квалифицируются как действия исполнителя по ч. 2 ст. 33 УК РФ.

На практике подавляющее большинство выявляемых форм недостаточности интеллектуального и личностного развития у подростков связано с теми или иными видами психической патологии: психическим и психофизическим инфантилизмом, органическими поражениями головного мозга, олигофренией и др. В связи с этим обычно освидетельствование несовершеннолетних проводится в рамках комплексной судебной психолого-психиатрической экспертизы. При назначении экспертиз следователь должен понимать, какие вопросы он может задать профессиональному психологу и как они должны быть структурированы. Ошибки при назначении экспертиз и при постановке вопросов экспертам часто затрудняют проведение исследований.

Возможно проведение освидетельствования несовершеннолетнего по факту применения по отношению к нему насилия в процессе склонения к совершению преступления, которые могли причинить ему как физические, так и нравственные страдания. В силу чего необходимо с помощью судебно-медицинской экспертизы установить наличие документов о причинении вреда, а значит промедления с её назначением и производством также могут противодействовать эффективному расследованию уголовного дела. Вопросы, направляемые для разрешения эксперту, должны быть заданы по поводу давности причинения повреждения и механизма его образования.

Заключение профессионального психолога о том, что у несовершеннолетнего нет признаков умственной отсталости означает, что он полностью понимает реальный характер и социальные риски своего поведения и может руководить им во время совершения преступления. Следовательно, подлежит уголовной ответственности. Если же отмечаются нарушения психического развития, не связанные с психическими расстройствами, нужно выяснить, мог ли он в полной мере осознавать значение своих действий или произвольное регулирование воли. Основные вопросы следственных органов, в соответствии с этим, следует сформулировать так: способен ли несовершеннолетний осознавать или предвидеть фактический характер своего поведения и его общественную опасность во время совершения противоправного деяния, и если да, то в полной ли мере?

Если несовершеннолетний страдает психическим расстройством, которое не позволяет ему осознать фактический характер и общественную опасность своего поведения или побудить его к общественно опасному поведению, суд может сделать вывод о его невменяемости. Это означает, что несовершеннолетний не несёт уголовной ответственности и ему судом могут быть назначены принудительные меры медицинского характера.

Для решения вопросов эксперту нужно представить не только материалы дела, но и обеспечить обследование самого несовершеннолетнего,

проведение наблюдения за ним, например, во время допроса в качестве обвиняемого, на очной ставке. В этой связи часто возникают проблемы, связанные с назначением психолого-психиатрической экспертизы, заключающиеся в неполноте представляемых на экспертизу материалов.

В процессе расследования преступлений несовершеннолетних, вовлеченных в их совершение, может возникнуть необходимость в проведении и других экспертиз, например, судебно-медицинской для установления возраста. По изученной нами категории уголовных дел такие экспертизы не проводились, хотя в отдельных случаях отсутствовали документы о возрасте подростка.

Для того чтобы следователь мог получить новую доказательственную информацию, в случае её недостаточности по делам о вовлечении несовершеннолетнего в совершение преступного посягательства, им может быть проведена на последующем этапе расследования проверка показаний подростка на месте. В случае реализации следственного действия в отношении данной категории лиц, которые были склонены к совершению преступления взрослыми, требуется учитывать ряд особенностей, которые на сегодняшний день не в полной мере разработаны. Как минимум, проверка показаний на месте необходима и может оказаться полезной потому, что лица, не достигшие 18-летнего возраста, в силу психологических особенностей своего развития склонны к искажению воспринимаемых ими в реальности ситуаций, в том числе, под влиянием давления со стороны совершеннолетних соучастников. Информация о подобных явлениях действительности требует должной проверки.

По делам о вовлечении имеется ряд следственных ситуаций, которые требуют производства проверки показаний на месте с участием несовершеннолетнего. Проверка показаний на месте по делам о вовлечении может помочь уточнить какие конкретно действия, и кто из соучастников осуществлял или мог осуществлять в момент совершения преступления, а также сам факт знания ими отдельных обстоятельств совершённого события, особенно в тех случаях, когда все имеющиеся для этого средства уже исчерпаны. Главной задачей становится установление знания каких-либо фактов о преступлении. Если они подтверждаются, то, как минимум, причастность лица к совершению преступления не нужно исключать.

Часто это видно на примере, когда несовершеннолетний берёт всю вину на себя, исключая причастность взрослого. Следователю достаточно проверить показания подростка на месте, где, в случае его лжи и действительного наличия соучастия, будет выяснено, что многих достаточно очевидных фактов он не знает, хотя должен был, если бы действительно в одиночку реализовывал преступный умысел (часто при стоянии «на шухере»). Так как в силу распределения ролей подростку нередко достаются второстепенные роли или необходимость совершения тех или иных дей-

ствий без должной степени осведомлённости о важных моментах, получается так, что о значимых «мелочах» он может и не догадываться [8, с. 107].

Проверка показаний на месте с участием несовершеннолетнего проводится с некоторыми особенностями, но так или иначе на базе общих криминалистических методик, поэтому, как и везде, предварительная подготовка к следственному действию имеет существенное значение.

Следователь должен: определить цель мероприятия, изучить личность проверяемого лица, оценить предварительно обстановку, на которую предстоит выезд, обозначить начальную точку для проверки, выбрать время, назначить круг иных участников, подготовить технические средства, в том числе транспорт, а также разъяснить сущность следственного действия, права и обязанности всем участвующим лицам.

В отношении несовершеннолетнего этот алгоритм приобретает некоторые изменения и дополнения.

Во-первых, становится важным исследование всех материалов, собранных на предыдущем этапе расследования. Тщательно изучаются протоколы допросов, после необходимо установить, какие обстоятельства необходимо уточнить при проверке показаний на месте и провести дополнительный допрос несовершеннолетнего с учётом данных факторов. Чтобы понимать, какова должна быть последовательность проверки и какие конкретные данные подлежат установлению, требуется обратить внимание и на показания свидетелей. По данным подростком на допросе ориентирам осуществляется его движение в ходе самого следственного действия, поэтому этот момент должен быть чётко уточнён. Отправной точкой является то место, которое несовершеннолетний запомнил больше всех остальных, и опять же, указал на него и его существование.

Необходимо обеспечить присутствие психолога или педагогического сотрудника. Для создания благоприятной подростку обстановки лучше, чтобы ими выступали те лица, которые уже участвовали с ним вместе ранее в следственных действиях. В процессе следственного действия следователь вправе руководить им, тем самым помогая подростку в демонстрации тех или иных фактов, словесно предлагая ему указать на места расположения похищенного, нахождения взрослого соучастника, его самого, повторить совершаемые в момент преступления действия и т.д. [9, с. 40]

Тактика действий будет достаточно эффективна, если при реализации проверки показаний на месте будут осуществлены указанные действия:

1. Дача подростку свободы в процессе демонстрации обстоятельств преступления. Конечно, с учётом принципа безопасности для участников и самого себя. Он также вправе выбирать направление движения всей группы, однако в этом случае должен следовать впереди неё. Важно понимать, что если несовершеннолетний активно пользуется предоставленной ему самостоятельностью, то вполне вероятно, что он действительно осведом-

лён о преступном событии и участвовал в его совершении. Вторжение в его демонстрацию недопустимо, так же, как и постановка наводящих вопросов.

2. Проверка показаний каждого из соучастников, в том числе двоих несовершеннолетних, должна осуществляться в разное время.

3. Позволять комбинировать показ, рассказ, демонстрацию.

4. Придерживаться запланированной последовательности в проводимых на месте проверки действиях.

5. Периодически уточнять и детализировать данные подростком показания или просить пояснять те или иные продемонстрированные действия, особенно в местах, где имелась или имеется концентрация следов преступления. Важно постоянно выяснять и осведомлённость подростка о тех действиях, которые в конкретный момент совершал вовлекатель.

6. Запечатлевать особенности в поведении проверяемого лица. Таким образом оказывается возможным понять, насколько несовершеннолетний уверен в своих действиях и как чётко даёт показания, меняется ли при этом его психическое и эмоциональное состояние.

7. Не исключать возможность обнаружения на месте проверки следов преступления, в связи с чем реализовывать поисковые мероприятия.

8. Соотношение ранее данных показаний и полученных при проверке показаний на месте [10, с.79].

9. Расстановка участников таким образом, чтобы не происходило ущемления действий подростка при демонстрациях и показах, и при этом исключалась возможность срыва следственного действия, например, побегом.

Проверка показаний на месте в рассматриваемой нами категории преступлений необходима, в первую очередь, для того, чтобы установить, действительно ли имело место быть вовлечение несовершеннолетнего в совершение противоправного деяния, а именно, знает ли он место, где произошло событие, и на которое он или его взрослые соучастники указывают, действительно ли принимал участие в реализации преступного умысла или лишь наблюдал действия сообщников со стороны и так далее.

Нами были названы не все следственные действия, производство которых может быть необходимо на последующем этапе расследования рассматриваемого нами вида преступления. Так, возможно производство следственного эксперимента для реконструкции обстановки и производства опытных действий. Также может иметь место быть предъявление преступника для опознания несовершеннолетнему. В данном случае возможно осуществление следственного действия в условиях, исключающих визуальное наблюдение опознаваемого опознающим. Последнее необходимо в случаях, когда подросток опасается данное лицо. Опознающим в ходе данного следственного действия может быть и свидетель.

Заключительный этап расследования должен завершаться передачей уголовного дела прокурору. Однако немаловажное значение для предупреждения совершения новых аналогичных преступлений играет необходимость составления следователем представления об устранении причин и условий совершений данного вида противоправного деяния [11, с. 374]. Обычно оно направляется в компетентные органы, которые могут поспособствовать этому.

Резюмируя сказанное, отметим, что преступления, касающиеся вовлечения несовершеннолетних в совершение противоправных деяний, не являются редким явлением в следственной практике, что является веской причиной говорить о том, что их расследование должно иметь крайне качественный характер, без допущения следственных ошибок. В силу данного положения нужно отметить, что подход к производству предварительного следствия по таким уголовным делам должен быть максимально ответственным, с применением не только общих, но и эффективных частных методик, позволяющих изобличать виновных и привлекать их к уголовной ответственности без испытания сложностей в процессе доказывания на каждом этапе расследования.

-
1. Состояние преступности Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: <https://мвд.рф/reports/6> (дата обращения: 02.10.2023).
 2. Юркова М.А., Чаплыгина В.Н. Особенности и проблемы надления несовершеннолетнего уголовно-процессуальным статусом потерпевшего и пути их решения // Государственная служба и кадры. 2022. № 2. С. 235-237.
 3. Сафронова А.В., Чаплыгина В.Н. Некоторые аспекты реализации прав и законных интересов несовершеннолетних подозреваемых (обвиняемых) в досудебном производстве // Проблемы уголовно-процессуального права и криминалистики: сборник научных статей / редколлегия: Н.В. Морозова [и др.]. Орел, 2021. С. 98-108.
 4. Чаплыгина В.Н. Особенности расследования преступлений с участием несовершеннолетних, связанные с выяснением условий их воспитания // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. 2021. № 1. С. 46-50.
 5. Морозова Н.В., Лазаренко О.Н. Некоторые вопросы проведения допроса несовершеннолетних подозреваемых // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сборник материалов Международной научно-практической конференции, 2018. С. 262-266.
 6. Морозова Н.В. Особенности производства следственных действий с участием несовершеннолетних // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2023. № 1 (94). С. 211-219.

7. Гуковская Н.И., Долгова А.И., Миньковский Г.М. Расследование и судебное разбирательство дел о преступлениях несовершеннолетних. М., 1974. С. 124.
8. Чаплыгина В.Н. Расследование вовлечения несовершеннолетних в совершение преступления: теоретические основы и практические особенности // Личность, право, государство. 2017. № 3. С. 107.
9. Морозова Н.В., Ермакова А.Л. Институт представительства несовершеннолетних на досудебных стадиях уголовного судопроизводства: практические проблемы реализации требований закона // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2020. № 2 (83). С. 39-46.
10. Муравьев К.В., Писарев А.В., Смирнова И.С., Супрун С.В. Уголовно-процессуальная деятельность органов дознания системы МВД России. М.: ЦОКР МВД России, 2010. 136 с.
11. Уголовный процесс: учебник для вузов / А.Н. Артамонов, А.М. Баранов, А.С. Бахта [и др.]; под ред. Б.Б. Булатова, А.М. Баранова. 2-е издание, переработанное и дополненное. М.: ЮРАЙТ, 2010. 606 с.

СВЕДЕНИЯ ОБ АВТОРАХ

Чаплыгина Виктория Николаевна. Кандидат юридических наук, доцент. Начальник кафедры криминалистики и предварительного расследования в ОВД.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Батуева Алтони Батоевна. Курсант факультета подготовки следователей.

Орловский юридический институт МВД России имени В.В. Лукьянова.

302027, г. Орел, ул. Игнатова, 2.

Ключевые слова: следственные действия, расследование преступлений, несовершеннолетний.

Сборник научных статей

**АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ
ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ
ОРГАНОВ ВНУТРЕННИХ ДЕЛ**

Подписано в печать 22.11.2023. Формат 60×90¹/₁₆.
Усл. печ. л. – 5,81. Тираж 20 экз. Заказ № 353.

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