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
2024

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
2024

УДК 351.745.7
ББК 67.99(2)94
А43

А43 **Актуальные вопросы осуществления оперативно-разыскной деятельности органов внутренних дел :** сборник научных статей / редкол.: Д.Ф. Флоря [и др.]. – Орел : ОрЮИ МВД России имени В.В. Лукьянова, 2024. – 112 с.
ISBN 978-5-88872-367-8

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 978-5-88872-367-8

Содержание

Венидиктов М.И.

ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ЭТНИЧЕСКОЙ, ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ В УСЛОВИЯХ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Преступления экстремистской направленности имеют повышенную латентность, а приготовление к их совершению – зачастую неочевидно для окружающих. Растет количество незаконных вооруженных формирований и преступных организаций экстремистской направленности, вербовка и незаконная деятельность которых все чаще осуществляется в сфере высоких технологий (дистанционно). Отдельную опасность представляют скрытые (так называемые «дремлющие») ячейки экстремистских организаций и движений, имеющих транснациональный характер, действующие на территории Российской Федерации. Изучение данной проблематики включает в себя множество вопросов, которые необходимо разрешить. В статье комплексно рассматриваются вопросы предупреждения и раскрытия преступлений экстремистской направленности

Стоит отметить, что в соответствии с действующей Стратегией национальной безопасности Российской Федерации до 2025 года, утвержденной Указом Президента от 2 июля 2021 г. № 400, противодействие экстремистским и террористическим угрозам являются приоритетным направлением правоохранительной деятельности правоохранительных органов Российской Федерации. Методы и способы осуществления экстремистской и террористической деятельности постоянно совершенствуются и требуют инновационных подходов к осуществлению противодействия этим угрозам.

С нашей точки зрения, разработка оперативно-разыскных мер противодействия преступлений экстремистской направленности крайне важная задача в борьбе с этой глобальной угрозой. Заметим, что экстремизм крайне отрицательно воздействует на Российскую Федерацию. Констатируя этот факт, хочется привести в пример выступление на совместном заседании коллегии МВД Министра внутренних дел Российской Федерации Владимира Александровича Колокольцева, который заявил: «В условиях проведения специальной военной операции на территории Украины активизировались элементы транснациональной организованной преступности, в частности связанной с экстремизмом, терроризмом, нелегальной миграцией, торговлей оружием и людьми» [5]. Заметим, что с нашей точки зрения эффективным инструментом профилактики преступлений и правонарушений,

совершаемых в области экстремизма в России, является проведение межведомственных оперативно-профилактических мероприятий по противодействию экстремистской деятельности. Несмотря на усилия правительств и международного сообщества, религиозный экстремизм продолжает оставаться значительной проблемой, требующей комплексного подхода и постоянного мониторинга.

Под противодействием преступлениям нами понимается осуществляемая в соответствии с законом деятельность оперативных подразделений государственных органов, направленная на профилактику, предупреждение, выявление и раскрытие преступлений, посредством использования оперативно-разыскных сил и средств. Предупреждение преступлений – это система мер, предпринимаемых государством, обществом, гражданами, направленная на противодействие процессам детерминации преступности в целях реализации уголовной политики, недопущения совершения преступлений, а также вовлечения в совершение преступлений новых лиц [1, с. 1–6].

С нашей точки зрения, для совершенствования механизма противодействия в рассматриваемой области необходимо усовершенствование координации и обмена информацией между различными службами и ведомствами. Интересным видится усиление сотрудничества с международными партнерами для обмена информацией и опытом по предупреждению, выявлению и раскрытию преступлений экстремистской направленности, повышение квалификации сотрудников по вопросам противодействия экстремизму, совершенствование механизмов координации между правоохранительными органами, общественными объединениями, активизация работы по просвещению и информированию общественности о природе и угрозах религиозного экстремизма.

По нашему мнению, эффективной мерой противодействия в данном случае будет выступать своевременная оснащённость оперативных подразделений техническими средствами, высокий уровень обучения и инструктирования личного состава, а также грамотное и умелое руководство со стороны наставников (способами тут будут выступать мониторинг подозрительных ресурсов, страниц пользователей и организаций). Недостаточная укомплектованность оперативных подразделений полиции служит предпосылкой того, что на оставшихся сотрудников возлагается большой объём работы, в процессе которого могут не усматриваться сообщения или информация того, или иного вида. Министр внутренних дел на расширенном заседании коллегии МВД заявил, что некомплектность личного состава в рядах органов внутренних дел составляет более 100 тысяч сотрудников [2], что напрямую может являться следствием повышения крими-

ногенной обстановки на обслуживаемой территории. Как итог это может повлиять на то, что преступления, связанные с экстремизмом, не удаётся предотвратить на стадии подготовки, а только на стадии совершения объективной стороны либо уже по факту совершённого деяния. Нехватка кадров объясняется сложностью работы, осуществляемой органами внутренних дел, недостатком выделяемых средств для потребностей ведомства. Решением данного вопроса может служить повышение престижности службы в полиции в целом, а в рядах оперативных подразделений в частности.

По мнению А.Ю. Климова, предупреждение преступлений экстремисткой направленности – это деятельность общих или специальных субъектов профилактики, направленная на нейтрализацию и устранение факторов, влияющих на становление и развитие причин преступлений экстремистской направленности [3, с. 1–4].

С точки зрения оперативно-разыскной деятельности как науки, «оперативно-разыскная профилактика преступлений» – это основанная на законах и урегулированная ведомственными нормативными актами научно обоснованная деятельность, проводимая оперативными подразделениями, заключающаяся в комплексном применении гласных и негласных оперативно-разыскных мероприятий с целью выявления и устранения причин преступлений и условий, им способствующих, установления лиц, от которых можно ожидать совершения преступлений, и оказания на них предупредительно-профилактического воздействия с целью недопущения с их стороны совершения преступлений, а также обеспечения безопасности граждан, которые подлежат защите от преступных посягательств [4, с. 1–7]. С нашей точки зрения, профилактика и предупреждение – тождественные понятия, и мы абсолютно согласны с определением, которое отразили Б.В. Борин и Я.Г. Ищук, в контексте рассматриваемой нами темы.

К основным методам, применяемым оперативными подразделениями органов внутренних дел Российской Федерации для профилактики экстремизма, можно отнести:

Во-первых, анализ оперативной обстановки в подконтрольном районе. В рамках данного метода оперативные сотрудники ОВД РФ осуществляют сбор, накопление, систематизацию, хранение, исследование и анализ информации о деятельности лиц и группировок, склонных к осуществлению религиозной экстремистской деятельности. В ходе осуществления этого направления устанавливаются места сбора экстремистски настроенных элементов.

Во-вторых, изучение социально-этнических параметров, включая выявление межэтнических связей, аспектов религиозности, в том числе нетрадиционной для Российской Федерации, и мотивационных

предпосылок поведения, представляется важным элементом предупреждения данного рода преступности.

В-третьих, мониторинг ресурсов сети «Интернет» на предмет распространения религиозных экстремистских материалов и принятие соответствующих решений. Ограничение доступа к Интернет-ресурсам осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), однако в соответствии с п. 5.1 Алгоритма [6] взаимодействия заинтересованных органов при выявлении противоправного контента в сети «Интернет», «веб-зеркала» Интернет-сайтов, содержащих экстремистские материалы, вносятся в Единый реестр на основании официальных писем от органов МВД России, ФСБ России и прокуратуры, содержащих сведения о распространении на страницах сайтов в сети «Интернет» материалов, ранее признанных в судебном порядке экстремистскими.

В-четвертых, проведение комплексной работы по выявлению источников финансирования религиозной экстремистской деятельности. Для отработки этого направления оперативные подразделения органов внутренних дел Российской Федерации взаимодействуют с Федеральной службой по финансовому мониторингу, которая, согласно ч. 5 п. 17 Положения о Росфинмониторинге [7], имеет полномочия направлять информацию в правоохранительные органы при наличии достаточных оснований полагать, что операция (сделка) связана с финансированием терроризма, в том числе и по запросу оперативных сотрудников органов внутренних дел Российской Федерации.

Заметим, что важной проблемой является недостаточная информированность общественности об экстремизме и его последствиях. Недостаточное понимание обществом природы и угроз, связанных с экстремизмом, может привести к недооценке опасности и неправильному реагированию на подобные ситуации. В этой связи необходимо активизировать работу по просвещению и информированию общественности о признаках и последствиях экстремизма.

Таким образом, для выявления и раскрытия преступных деяний экстремистской направленности сотрудникам оперативных подразделений необходимо иметь координацию и планирование совместных оперативно-разыскных мероприятий и процессуальных действий, осуществлять оперативное управление по получению и обработке оперативно значимой информации, необходимой для противодействия преступлениям экстремистской направленности.

---

1. Тузов Л.Л. Проблемы профилактики экстремизма в среде несовершеннолетних и молодежи [Электронный ресурс]. URL:

https://cyberleninka.ru/article/n/problemy-profilaktiki-ekstremizma-v-srede-nesovershennoletnih-i-molodezhi/viewer. С. 1–6.

2. Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации [Электронный ресурс]. URL: https://mvdmedia.ru/news.

3. Климов А.Ю. Предупреждение преступлений экстремистакой направленности [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/preduprezhdenie-prestupleniy-ekstremistskoy-napravlennosti/viewer. С. 1–4.

4. Борин Б.В., Ищук Я.Г. Понятие оперативно-розыскной профилактики преступлений [Электронный ресурс] // Пробелы в российском законодательстве. 2018. С. 1–7. URL: https://cyberleninka.ru/article/n/ponyatie-operativno-rozysknoy-profilaktiki-prestupleniy/viewer.

5. Совместное заседание коллегии МВД [Электронный ресурс]. URL: https://tass.ru/obschestvo/17436681.

6. Алгоритм (порядок) взаимодействия заинтересованных органов при выявлении противоправного контента в сети «Интернет» [Электронный ресурс] / Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. URL: https://14.rkn.gov.ru/directions/p1941/p27622.

7. Вопросы Федеральной службы по финансовому мониторингу [Электронный ресурс]: Указ Президента Рос. Федерации от 13 июня 2012 г. № 808 // Собр. законодательства Рос. Федерации. 2020. № 13, ст. 3175.

Сведения об авторе

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

Московский университет МВД России имени В.Я. Кикотя.

117997, Российская Федерация, г. Москва, ул. Академика Волгина, д. 12.

Ключевые слова: экстремизм, сеть-интернет, информационно-телекоммуникационные технологии, противоправная деятельность, противодействие преступлениям.

Вихляев А.А.

ОПЕРАТИВНО-РАЗЫСКНОЕ ПРОТИВОДЕЙСТВИЕ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ РЕЛИГИОЗНЫХ ОБЪЕДИНЕНИЙ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В настоящей статье автором дается краткая оперативно-разыскная характеристика экстремистской деятельности религиозных объединений, совершаемой посредством использования информационно-телекоммуникационных технологий. Проведенный анализ позволяет сформулировать вектор развития оперативно-разыскного противодействия экстремистским угрозам в информационно-телекоммуникационных сетях.

Экстремизм в религиозной сфере выступает одной из наиболее опасных форм экстремистской деятельности в условиях современных реалий. Все чаще религиозно-экстремистская идеология является частью более сложных общественно опасных деяний, характеризующихся высокой степенью деструкции и вовлеченности. Радикально-религиозные взгляды и воззрения могут использоваться в качестве катализатора для продвижения политических и идеологических радикальных идей и действий экстремистского и террористического характера.

Нередко свобода совести и вероисповедания эксплуатируются экстремистскими организациями и террористическими группировками для вербовки своих последователей, осуществления их «идейной обработки» и мотивирования на совершение преступлений экстремисткой и террористической направленности. Религиозные объединения вовлекаются в криминальные схемы, направленные не только на непосредственное осуществление экстремистских действий и террористических актов, но и для оказания помощи и финансирования экстремистских организаций, преступных сообществ и террористических группировок локального и транснационального характера.

Экстремистская деятельность может осуществляться как религиозными объединениями, легально функционирующими на территории Российской Федерации, и имеющими статус религиозных организаций, так и отдельными религиозными группами, которые не имеют официальной регистрации в соответствии с действующим законодательством, а отдельные их представители могут привлекаться на добровольной основе для реализации потребностей таких групп.

Действующей редакцией Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [1] религиозные объединения освобождены от уведомления федеральных органов исполнительной власти о своих бенефициарах и аффилированных лицах, с которыми они осуществляют непосредственное взаимодействие, что расширяет возможности для их теневого использования в различных сферах экстремистской деятельности.

Таким образом, религиозные объединения становятся наиболее вероятными субъектами осуществления различных видов и форм экстремистской деятельности, ее пропаганды и поддержки.

В современных условиях информационно-телекоммуникационные технологии все чаще применяются в экстремистской деятельности: для создания, передачи и распространения материалов экстремистского содержания, осуществления непосредственного взаимодействия со своими последователями, вербовки и координации деятельности новых и действующих сторонников, осуществления финансовой и иной поддержки экстремистских организаций и террористических группировок [2; с. 63]. Информационно-телекоммуникационные технологии активно применяются и для финансирования деятельности запрещенных экстремистских организаций – в данном случае речь можно вести о незаконных операциях с криптовалютами и иными цифровыми финансовыми активами – например, организации транснациональных пунктов обналичивания, обмена криптовалют и незаконный криптомиксинг, основными целями которых, прежде всего, являются отмывание (легализация) доходов, полученных преступным путем и создание криминальных криптовалютных рынков, использование виртуальных фондов для отмывания доходов, полученных преступным путем, и пр.

К информационно-телекоммуникационным технологиям принято относить компьютерное оборудование, программное обеспечение, телефонные линии, сотовую связь, электронную почту, сотовые и спутниковые технологии, сети беспроводной и кабельной связи, мультимедийные средства, информационно-телекоммуникационную сеть Интернет.

Наиболее распространенными сферами коммуникаций, применяемых для осуществления экстремистской деятельности со стороны религиозных объединений, принято выделять общедоступную информационно-телекоммуникационную сеть Интернет, пиринговые сети, «глубинный Интернет», IIP и I2P-соединения.

Посредством информационно-телекоммуникационной сети Интернет, осуществляется не только распространение информации о де-

ятельности религиозных объединений или групп, но и производится непосредственная коммуникация с действующими и возможными последователями.

Взаимодействие с последователями и их вербовка могут осуществляться как целенаправленно, путем активного взаимодействия администраторов и модераторов ресурсов религиозных объединений (например, путем отправления сообщений на личную страницу пользователя, общением на страницах форумов и в групповых чатах или социальных сетях), так и путем пассивного размещения информации, побуждающей пользователей информационно-телекоммуникационных сетей, самостоятельно переходить на ресурсы, содержащие экстремистский контент (например, размещение гиперссылок на сайты или форумы экстремистских сообществ, расположенных в общем доступе в сети Интернет).

Другой сферой, представляющей оперативный интерес, является применение пиринговых сетей для осуществления коммуницирования между различными пользователями современных информационно-телекоммуникационных технологий. Так, применение программных клиентов в пиринговых сетях, позволяет использовать возможности анонимной передачи информации между пользователями или участниками различных групп, функционирующих в оверлейной компьютерной сети. Например, применение программного обеспечения по типу BitTorrent, RetroShare, Soulseek, EiskaltDC++, ApexDC++, Fopnu и пр. дает возможности участникам контекстных групп взаимодействовать между собой в условиях высокой степени конфиденциальности напрямую, т.е. самостоятельно осуществлять отбор, изучение, передачу, загрузку, обработку и передачу информации экстремистского содержания – от текстовых файлов до видеоизображений и программного обеспечения.

Посредством обозначенного программного обеспечения, находящего в свободном доступе в сети Интернет для загрузки, создается возможность передавать абсолютно любые материалы радикально-религиозного, экстремистского и террористического содержания между пользователями в сети напрямую.

Использование возможностей глубинного Интернета – системы Даркнет, – допуск в которую осуществляется посредством специальных браузеров, находящихся в свободном доступе – так называемых «луковых маршрутизаторов» (например Tor) и иных клиентов – также представляет дополнительную опасность в сфере противодействия экстремистской деятельности религиозных объединений.

Используя данные клиенты, загрузка и распространение которых свободно осуществляется в Сети, одни пользователи могут взаи-

модействовать с другими, не опасаясь при этом слежки или сбора их персональных данных. В некоторых случаях пользователи полагаются на сеть, когда им нужно быстро скрыть или выполнить секретную работу, что может быть использовано для осуществления экстремистской деятельности.

В рамках реализации оперативно-разыскных мер по противодействию экстремистской деятельности религиозных объединений в информационно-телекоммуникационных сетях, большое внимание должно уделяться оперативно-разыскной разведке цифрового пространства, и, в частности, его оперативно-разыскному мониторингу [3; с. 52].

Под оперативно-разыскным мониторингом следует понимать комплекс оперативно-разыскных мероприятий, реализуемых сотрудниками оперативных подразделений как индивидуально и в составе подразделений, так и во взаимодействии с другими федеральными органами исполнительной власти, организациями и специалистами, обладающими специальными знаниями в области информационно-телекоммуникационных технологий, и гражданами, на гласной и конфиденциальной основе, для обеспечения контроля за состоянием криминальных процессов в открытой и закрытой сетевой социальной среде.

Мониторинг ориентирован на применение средств и методов оперативно-разыскной деятельности в информационно-телекоммуникационном пространстве, для получения данных о криминальной активности, их последующего сбора, обработки и анализа для решения задач, стоящих перед оперативно-разыскной деятельностью.

Приоритетными направлениями данного мониторинга выступают:

1) изучение сетевых ресурсов, связанных с деятельностью преступных формирований;

2) наблюдение за закрытыми для общего доступа местами сетевого общения криминальной направленности;

3) автоматизированный поиск сетевых ресурсов, содержащих информацию, запрещенную к распространению.

Для реализации оперативно-разыскных задач в процессе мониторинга сотрудники оперативных подразделений могут ориентироваться:

1) на инициативный поиск, который может быть как свободным, так и целеориентированным;

2) опосредованный поиск, реализуемый иными лицами, организациями и подразделениями, с последующим предоставлением информации о рассматриваемом объекте оперативному сотруднику;

3) информационный поиск по имеющейся оперативно-значимой информации, полученной при реализации дел оперативного учета, или в процессе работы по отдельным поручениям органов предварительного расследования по уголовным делам;

4) оперативного внедрения в информационную среду, используемую экстремистской организацией или сообществом.

Информация, получаемая посредством подобного мониторинга, может дать оперативному сотруднику оперативно-значимые сведения об объекте исследования: осуществляет ли религиозная организация свою экстремистскую деятельность открыто, или выступает посредником в экстремистской деятельности иных экстремистских организаций и преступных сообществ; действует ли она латентно, скрывая свою экстремистскую деятельность за иными видами деятельности (общественной, финансово-хозяйственной и пр.).

Используя доступные инструменты, сотрудники оперативных подразделений, могут самостоятельно получить информацию о некоторых финансовых операциях и аффилированных лицах религиозных объединений, выявить контакты представителей религиозных объединений с лицами, подверженными иностранному влиянию, миссионерами, иностранными религиозными организациями и религиозно-политическими группировками экстремистской направленности; провести сопоставление полученных сведений с открытыми информационными ресурсами федеральных органов исполнительной власти – например, реестром организаций и физических лиц, подозреваемых в совершении экстремистской и террористической деятельности, ведением которого занимается Росфинмониторинг, или перечнем общественных объединений и религиозных организаций, иных некоммерческих организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности, который формирует и публикует Министерство юстиции Российской Федерации, открытыми информационными базами и ресурсами ФСБ России и антитеррористического комитета и пр.

Таким образом, оперативно-разыскной мониторинг позволяет оперативным сотрудникам не только инициативно получать, обрабатывать и использовать для решения оперативно-разыскных задач необходимые сведения об объектах изучения, но и посредством комбинирования с открытыми источниками, специальными средствами и методами оперативно-разыскной деятельности, выступать важным элементом оперативно-разыскного противодействия экстремистской деятельности в условиях развития современных информационных технологий.

1. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федер. закон Рос. Федерации от 7 августа 2001 г. № 115-ФЗ.

2. Сундиев И.Ю. Медиаресурсы в экстремистской и террористической деятельности: функциональный анализ. (Res publica) (Общее дело, государство, республика) // Свободная Мысль. 2014. № 4 (1646). С. 55–72.

3. Кузьмин Н.А. Отдельные вопросы использования современных технологий в раскрытии преступлений // Научные труды Российской таможенной академии (Москва, 25 ноября 2022 г.). М.: Российская таможенная академия, 2022. С. 50–55.

Сведения об авторе

Вихляев Александр Александрович. Адъюнкт кафедры оперативно-разыскной деятельности и специальной техники.

Московский университет МВД России имени В.Я. Кикотя.

117437, г. Москва, ул. Академика Волгина, д. 12.

Ключевые слова: религиозные объединения, экстремизм, информационно-телекоммуникационные технологии, оперативно-разыскной мониторинг, оперативно-разыскное противодействие.

Екимцев С.В.

ХАРАКТЕРИСТИКА КВАЛИФИЦИРОВАННЫХ ВИДОВ МОШЕННИЧЕСТВА

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 адап-

тироваться 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 собственности. 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 г. сохраняется тенденция к увеличению количества – на 28,7 % – 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 кратному 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 ноября 2017 г. № 48.

В целях 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 распределить 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 правомочия, 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 однобокой, 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. 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 Орловского 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 [Электронный ресурс]: Федер. закон Рос. Федерации от 29 ноября 2012 г. № 207-ФЗ: в ред. от 3 июля 2016 г. // Собр. законодательства Рос. Федерации. 2012. № 49, ст. 6752.

5. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: в ред. от 24 сентября 2022 г. // 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.

Сведения об авторе

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

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

302027, Российская Федерация, 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.

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

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 уверенны 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 применятся 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 приложениями. В любом случае, даже если у сотрудников не получается получить доступ к текстовому содержанию сообщения и другим фай-

лам, то доступ к метаданным получить удается 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 правоохранительные органы могут осуществить с помощью универсального устройства из-

влечения 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 зако-

нодательства и проблемы правоприменения // Криминалистика: вчера, сегодня, завтра. 2019. № 2 (10). С. 8–14.

Сведения об авторе

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

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

Кизилов А.П.

О НЕКОТОРЫХ ВОПРОСАХ ИЗУЧЕНИЯ БОРЬБЫ С ЭКСТРЕМИЗМОМ, РЕАЛИЗУЕМЫМ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, С ЧАСТНО-НАУЧНЫХ ПОЗИЦИЙ

На сегодняшний день противодействие экстремизму одно из ключевых направлений в развитии современной теории оперативно-разыскной деятельности. Глобальный характер последствий для общества и государства заставляет все чаще совершенствовать методы противодействия данному явлению. Важным аспектом в этом вопросе становится то, что информационно-телекоммуникационных технологии стали неотъемлемой частью жизни любого человека, в том числе и преступников. Изучение данной проблематики включает в себя множество вопросов, которые необходимо разрешить.

В современных условиях Российская Федерация сталкивается с колоссальным давлением как внешних таки внутренних различных сил, направленных на дестабилизацию общественных отношений и направленных на подрыв устоев государственного регулирования. В этой связи экстремистская деятельность становится в один ряд с

наиболее острыми вызовами перед государством и обществом в целом и правоохранительной системой в частности.

Преступления экстремистской направленности несут опасность обществу и государству, так как способствуют дестабилизации обстановки внутри социума; провоцируют межнациональные, межконфессиональные и межрелигиозные конфликты; приводят к проблемам обеспечения территориальной целостности сраны. В современных условиях, когда Российская Федерация проводит специальную военную операцию на территории республики Украина, необходимость обеспечения внутреннего единства страны становится на первый план.

При этом следует отметить, что именно оперативно-разыскные методы, способы и средства являются зачастую чуть ли не единственной возможностью выявления данных фактов преступной деятельности с последующей их легализацией для реализации функции уголовного преследования. Здесь можно согласиться с мнением А.В. Варданяна и О.П. Грибунова, которые отмечали, что раскрытие и расследование преступлений – это сложный процесс, осуществляемый на основе соответствующей уголовно-правовой, процессуальной, оперативно-разыскной и криминалистической информации и знаниях определенных частных закономерностей [2, с. 27].

Информационно-телекоммуникационные технологии активно используются как преступниками, так и правоохранительными органами. В этом единстве заложена одновременно и их внутренняя борьба, поскольку направленность их использования диаметрально противоположна – у преступников – это средство, помогающее реализовывать противоправную деятельность, а у органов правопорядка – средство, способствующее противодействию им.

В то же время развитие информационных технологий и активное использование их людьми заставляют современных исследователей уделять данному обстоятельству всё большее внимание. Существенная часть жизни современного человека связана с коммуникацией с другими членами общества посредством информационно-телекоммуникационных технологий. Человек всё больше их использует для решения своих насущных задач и целей. В контексте данной тенденции не стала исключением и деятельность преступников, которые активно ими пользуются при реализации своих противоправных задач. При этом одним из ключевых признаков сетевой преступности является её организованный характер и высокий уровень внедрения и использования современных информационно-телекоммуникационных технологий [4].

Таким образом, исследование вопросов документирования противоправной деятельности, связанной с совершением преступлений

экстремистской направленности, реализуемой посредством использования информационно-телекоммуникационных технологий является насущным, необходимым и актуальным.

Однако в настоящее время сложилась ситуация, при которой основательных научных исследований, посвящённых данной проблематике крайне мало. Преступления экстремистской направленности, совершаемые с использованием информационно-телекоммуникационных технологий, в последнее время начинают активно рассматриваться в юриспруденции с позиций криминалистики, криминологии и уголовного права. Однако серьёзных и актуальных монографических исследований по рассматриваемой проблематике с позиций оперативно-разыскной науки в настоящее время крайне мало. Однако, следует отметить, что актуальность подобной проблематики не вызывает сомнений у большинства учёных и необходимость тщательного исследования и выработки рекомендаций и положений практического характера констатируется весьма однозначно.

При исследовании рассматриваемой проблематики следует рассмотреть следующие аспекты:

- оперативно-разыскную характеристику и правовое регулирование преступлений, совершаемых по мотивам политической, национальной, религиозной ненависти или вражды с использованием информационно-телекоммуникационных технологий;
- особенности выявления и раскрытия данных преступлений;
- поисковые признаки преступной деятельности в исследуемой сфере;
- факторы, влияющие на состояние оперативной обстановки по рассматриваемой проблематике;
- способы реализации различных оперативно-разыскных мероприятий в процессе выявления, пресечения, профилактики и документирования экстремистских преступлений, совершаемых с пользованием информационно-телекоммуникационных технологий;
- особенности, которые необходимо учитывать при решении вопроса о целесообразности установления конфиденциального сотрудничества отдельных лиц с органами внутренних дел;
- особенности документирования данной разновидности преступной деятельности;
- нормативное правовое обеспечение оперативно-разыскной деятельности по противодействию преступлениям, совершаемым по мотивам политической, национальной, религиозной ненависти или вражды с использованием информационно-телекоммуникационных технологий;

- вопросы документирования преступных действий лиц, занимающихся рассматриваемой преступной деятельностью, по разным направлениям;

- способы и методы совершения рассматриваемых преступлений;

- закономерности противодействия преступлениям, совершаемым по мотивам политической, национальной, религиозной ненависти или вражды с использованием информационно-телекоммуникационных технологий;

- иностранный опыт борьбы с преступлениями экстремистской направленности;

- способы повышения эффективности противодействия экстремизму, реализуемому с использованием информационно-телекоммуникационных технологий.

О необходимости противодействия экстремистской деятельности не раз заявлялось с самых высоких трибун, начиная с Президента России, заканчивая министром внутренних дел Российской Федерации.

План научного исследования в обязательной степени должен включать в себя рассмотрение теоретических аспектов и современного состояния оперативно-разыскного противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных технологий. В рамках чего следует уделить внимание вопросам правового регулирования; оперативно-разыскной характеристики и современного состояния оперативно-разыскного противодействия преступлениям экстремистской направленности. Также следует исследовать организационные и тактические вопросы выявления и документирования преступлений, совершаемых по мотивам политической, национальной, религиозной ненависти или вражды с использованием информационно-телекоммуникационных технологий. При рассмотрении данного блока вопросов следует уделить внимание организационно-управленческим и организационно-тактическим аспектам противодействия данной разновидности преступлений; обеспечения рассматриваемой деятельности негласным аппаратом; взаимодействия подразделений по противодействию экстремизму с иными правоохранительными подразделениями и органами, а также предприятиями, организациями и учреждениями различных форм собственности, при противодействии преступлениям, совершаемым по мотивам политической, национальной, религиозной ненависти или вражды с использованием информационно-телекоммуникационных технологий.

Проблематика исследования информационно-телекоммуникационных технологий, в контексте противодействия экстремизму, требует их рассмотрение с различных позиций. Как средства сокрытия и мас-

кировки следов преступной деятельности; как средства коммуникации и анонимизации личности преступников; как средства реализации преступного умысла и т.д.

При изучении рассматриваемой темы следует рассмотреть вопросы использования биллинга при противодействии данной разновидности преступности. При этом нужно обратить внимание на недопустимость такой распространённой ошибки, когда под данным термином подразумевается сугубо детализация телефонных соединений абонентских номеров операторов сотовой связи. При том, что в действительности это разновидность оперативно-технического мероприятия, реализующегося в рамках оперативно-разыскного мероприятия «снятие информации с технических каналов связи», направленное на выявление связей пользователей и абонентов сетей сотовой связи посредством анализа временных и геолокационных закономерностей телефонных звонков, sms сообщений и интернет соединений, с целью установления закономерностей, способствующих выявлению оперативно-значимой информации.

При исследовании рассматриваемой проблематики не стоит исключительно зацикливаться на рассмотрении экстремистских преступлений сугубо с использованием сети Интернет, дабы не происходило отождествление понятий – информационно-телекоммуникационные технологии и сеть Интернет. Поскольку данная подмена терминологии не может быть уместна, ибо термин информационно-телекоммуникационные технологии существенно шире термина – сеть-интернет. Ввиду вышеизложенного следует обратить внимание и на такие элементы информационно-телекоммуникационных технологий, как телефонная связь, радио-связь и спутниковая связь.

Отдельное внимание при исследовании рассматриваемой проблематики следует уделить рассмотрению вопросов финансирования экстремистской деятельности, посредством использования современных информационно-телекоммуникационных технологий [2].

Особое внимание сотрудников оперативных подразделений, должны вызывать факты размещения в социальных сетях графических изображений с нацистской символикой и атрибутикой, символикой экстремистских организаций [3, с. 67]. При этом следует учитывать положения Федерального закона от 1 марта 2020 г. № 31-ФЗ «О внесении изменений в статью 20.3 КоАП РФ», которые декриминализуют ряд смежных деяний, связанных с демонстрацией экстремистской символики [5].

---

1. Варданян А.В., Грибунов О.П. Современная доктрина методико-криминалистического обеспечения расследования отдельных

видов преступлений // Вестник Восточно-Сибирского института МВД России. 2017. № 2 (81). С. 23–35.

2. Иванов П.И. Оперативно-розыскное сопровождение противодействия финансированию экстремистской деятельности: основные проблемы и пути решения // Труды Академии управления МВД России. 2019. № 4 (52). С. 82–89.

3. Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. Т. 18, № 2. С. 64–71.

4. Тимофеев С.В. О некоторых аспектах привлечения специалиста в ходе изъятия электронных носителей информации при проведении оперативно-розыскных мероприятий // Криминалистика, вчера, сегодня, завтра. 2020. № 1 (13). С. 108–114.

5. О внесении изменения в статью 20.3 Кодекса Российской Федерации об административных правонарушениях [Электронный ресурс]: Федер. закон Рос. Федерации от 1 марта 2020 г. № 31-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

Сведения об авторе

Кизилов Александр Павлович. Кандидат юридических наук, доцент. Доцент кафедры оперативно-разыскной деятельности и специальной техники.

Московский университет МВД России имени В.Я. Кикотя.

117997, Российская Федерация, г. Москва, ул. Академика Волгина, д. 12.

Ключевые слова: экстремизм, информационно-телекоммуникационные технологии, сеть Интернет, противоправная деятельность, противодействие преступлениям.

Климачков А.В., Горшкова В.С.

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

В статье рассматриваются отдельные вопросы использования СЭД ИСОД МВД России при назначении исследований сотрудниками оперативных подразделений полиции в экспертно-криминалистичес-

кую службу органов внутренних дел, при этом раскрываются возможности и ограничения применения вышеуказанного информационного ресурса при осуществлении оперативно-разыскной и экспертной-криминалистической 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-разыскного Закона – право использовать помощь специалистов при организации и проведении оперативно-разыскных 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 г. 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 Перечню 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 г. показал, что сотрудники правоохранительных органов ряда субъектов государства неправильно определяют вид назначаемого экспертного исследования (например, оценочное вместо товароведческое), 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 февраля 2021 г. № 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-разыскного 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, ре-

зультатов 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 (нарочным, 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 нарочным.

Вышеуказанные положения, на наш взгляд, не могут использоваться при проведении оперативно-разыскных мероприятий с привлечением СЭД ИСОД, так как создают предпосылки для существенных нарушений прав и свобод граждан, вовлеченных в сферу оперативно-разыскных правоотношений, нарушения принципа конспирации при осуществлении оперативно-разыскной 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 сложившейся проблемной ситуации является создание на платформе ИСОД специализированного сервиса «Исследование предметов и документов» – для назначения экспертных исследований и получения их результатов, доступ к которому 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 7 ноября 2015 г. № 1/9112.

2. Об оперативно-розыскной деятельности [Электронный ресурс]: Федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ: с изм. от 29 декабря 2022 г. 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 июня 2005 г. № 511: с изм. от 30 мая 2022 г. 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 апреля 2023 г. Исх. №37/24-7380.

5. Об утверждении Наставления по организации экспертно-криминалистической деятельности в системе МВД России [Электронный ресурс]: приказ МВД России от 11 января 2009 г. № 7: с изм. от 9 марта 2023 г. Доступ из справ.-правовой системы «Консультант Плюс».

Сведения об авторах

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

Барнаульский юридический институт МВД России.

656038, Российская Федерация, г. Барнаул, ул. Чкалова, д. 49.

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

Главное управление МВД России по Алтайскому краю.

656015, Российская Федерация, г. Барнаул, пр. Ленина, д. 74.

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

Князьков К.В.

ОСОБЕННОСТИ МЕЖДУНАРОДНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ В ПРОТИВОДЕЙСТВИИ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Особое внимание в статье уделяется международному сотрудничеству и стандартизации процессов кибербезопасности, которые способствуют более быстрому и эффективному обмену данными об угрозах, позволяют своевременно реагировать на инциденты, создают возможности для координации усилий в глобальном масштабе. Итоги проведенного исследования показывают, что успешное противодействие киберугрозам требует комплексного подхода, включающего тесное сотрудничество как на уровне государств и международных организаций, так и частных компаний для обеспечения устойчивой защиты в киберпространстве.

В результате, на основе собранных данных автор приходит к выводу, что применение лучших международных практик и их адаптация к национальным условиям представляются ключевыми для повышения устойчивости киберзащиты в условиях цифровой эпохи.

Первым международным правовым актом в рассматриваемой сфере считается подписанная 23 ноября 2001 г. Конвенция Совета Европы о киберпреступности, или как её еще называют «Будапештская конвенция» [1]. Основной её задачей определена борьба с интернет- и компьютерной преступностью (киберпреступностью). Договор был направлен на выстраивание взаимодействия между странами при расследовании киберпреступлений и преследовании совершивших их лиц. При этом он определял необходимость гармонизации национальных законодательств для эффективного противодействия таким противоправным деяниям как несанкционированный доступ к компьютерным системам, манипуляции с данными, распространение вредоносных программ и кража информации. Конвенцию подписали 68 стран, а именно государства, входящие в Совет Европы, США, Канада, Япония, Тунис, Израиль и другие. Однако, ряд стран, в том числе Россия и Индия, отказались от подписания и ратификации данной конвенции из-за нарушения интересов их национальной безопасности. В частности, указанное соглашение содержало пункты, предоставляющие государствам-участникам право не ставить в известность другие страны о проведении на их территории мероприятий по изобличению киберпреступников. Одновременно с этим проводящим их правоохранительным органам разрешалось иметь полный доступ к ресур-

сам, размещенным в сетях общего пользования того государства, в котором подразумевается поиск преступника.

Важным элементом международного правового регулирования являются стандарты, разработанные «International Organization for Standardization» (ISO) или «Международной организацией по стандартизации». Так, стандарты ISO/IEC 2700X [2] определяют требования к системам управления информационной безопасностью, которые призваны защищать конфиденциальность, целостность и доступность данных. Эти стандарты используются не только частными компаниями, но и государственными учреждениями для создания надежных систем защиты информации.

Одновременно с ISO рекомендации для обеспечения кибербезопасности разрабатывает «Международный союз электросвязи» (МСЭ) [3], деятельность которого направлена на содействие развитию международных стандартов в области информационной безопасности, укрепление сотрудничества между странами при осуществлении борьбы с угрозами киберпространства.

Затрагивая вопрос защиты данных, следует отметить принятие 27 апреля 2016 г. постановления Европейского Союза «General Data Protection Regulation» [4] (GDPR) или «Общий регламент по защите данных», которым были установлены строгие правила обработки и хранения персональных данных, предусмотрены большие штрафы за их нарушение. Этот регламент стал примером для многих стран, стремящихся улучшить свои национальные стандарты защиты данных. Например, в Российской Федерации, несмотря на непринятие стандарта GDPR, с учетом отмеченных международных договоров разработаны федеральные законы от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Выход угроз информационной безопасности на межгосударственный уровень обусловил потребность расширения механизмов сотрудничества стран в вопросах предотвращения и расследования кибератак, создания в этих целях «Computer Emergency Response Team (CERT)» или «Команд реагирования на компьютерные инциденты» [5]. Таких команд в ведущих странах мира существует большое количество. Например, в США это Компьютерная команда экстренной готовности США (US-CERT) и Координационный центр CERT (CERT/CC). В Российской Федерации к наиболее известным относятся BI.ZONE-CERT, Национальный Координационный Центр по Компьютерным Инцидентам (НКЦКИ), KASPERSKY ICS CERT, Financial CERT (ФинЦЕРТ).

Примером продуктивного международного сотрудничества может служить деятельность Европейского центра по борьбе с киберпреступностью или сокращенно «Европола» [6]. Этот центр координирует действия правоохранительных органов стран-членов ЕС по расследованию киберпреступлений, включая атаки на банковские системы, кражу данных и распространение вредоносного программного обеспечения. Сотрудничество между странами ЕС в рамках Европола позволяет оперативно обмениваться информацией о киберугрозах и проводить совместные операции.

Еще одной структурой, созданной для повышения качества взаимодействия между государствами и частным сектором по проблемам кибербезопасности, является «Глобальный форум по борьбе с киберпреступностью», играющий важную роль в координации усилий по предотвращению транснациональных кибератак со стороны фишинговых кампаний, в т.ч. организуемых преступниками из разных стран.

Подобного рода международные инициативы и совместные действия помогают минимизировать риски киберугроз и обеспечивают защиту информационных систем на глобальном уровне. Повышению эффективности деятельности соответствующих структур в рассматриваемой сфере также способствует учет и использование уникального опыта каждой заинтересованной страны, основанного на национальных стратегиях, законодательных инициативах и технологических достижениях.

Большим опытом в области кибербезопасности благодаря комплексному подходу и высокоразвитым технологическим возможностям обладают США. В рамках совершенствования американского законодательства разработан закон о кибербезопасности, предусматривающий разработку стандартов безопасности для государственных учреждений и частных компаний, а также обязательное уведомление о киберинцидентах. Принята программа по защите выборов от вмешательства, направленная на предотвращение атак на избирательные системы. Важным элементом американской системы является «Агентство по кибербезопасности и безопасности инфраструктуры (CISA)» [7], созданное в 2018 г. и предназначенное для защиты от кибератак критической инфраструктуры, включая системы водоснабжения, энергетику, здравоохранение и финансовый сектор. Одновременно с этим США активно сотрудничают со своими международными партнёрами, участвуют в совместных операциях против киберпреступников.

Европейским Союзом, как уже говорилось выше, создана своя уникальная стратегия по защите персональных данных и прав граждан в цифровом пространстве «Общий регламент по защите данных» (GDPR) [4], в 2019 г. принят «Регламент по кибербезопасности», ре-

гламентирующий создание единых стандартов безопасности на уровне всего ЕС, предусматривающий обязательную сертификацию продуктов и услуг в сфере информационной безопасности. Для координации действий в сфере кибербезопасности образовано специальное агентство, которое занимается разработкой рекомендаций и стандартов для защиты информационных систем, а также организует учения по кибербезопасности на уровне ЕС, что помогает отрабатывать механизмы реагирования на кибератаки в случае кризисных ситуаций.

Не стоит упускать из виду наших восточных партнеров, прежде всего Китайскую Народную Республику. Реализуемая КНР политика в области кибербезопасности во многом направлена на контроль и управление киберпространством внутри страны, что обусловлено особенностями государственного управления. Важным элементом китайской стратегии является «Закон о кибербезопасности» [8], принятый в 2017 г. Этот законодательный акт регулирует деятельность государственных органов и частных компаний, обязывает их внедрять системы защиты информации и предоставлять данные о кибератаках в государственные структуры. Для усиления киберзащиты Китаем активно развиваются технологии искусственного интеллекта и блокчейн, создана масштабная система мониторинга интернет-активности, известная как «Великий китайский файрвол», позволяющая блокировать доступ к нежелательному контенту и контролировать интернет-активность внутри страны. На международной арене КНР ведет активное сотрудничество с другими странами в рамках инициативы «Один пояс – один путь», в т.ч. по вопросам информационной безопасности. Китайские компании, такие как «Huawei», выходят на главенствующие позиции в создании глобальных систем 5G, формирующие как новые угрозы кибербезопасности, так и дополнительные возможности в решении вопросов по противодействию им.

Большое внимание этим вопросам уделяется и в нашей стране. Как отмечалось выше, Российская Федерация, избравшая путь защиты национальных интересов, осуществила разработку собственной стратегии в области информационной безопасности. В 2016 г. принята «Доктрина информационной безопасности Российской Федерации» [9]. В данном документе определены приоритетные направления в области защиты информационных систем и технологий, предусмотрены меры по противодействию кибершпионажу и вмешательству во внутренние дела страны. Одновременно с этим приняты меры по созданию своих систем защиты, развитию собственных операционных систем и программного обеспечения для снижения зависимости от западных технологий и повышения устойчивости российской инфраструктуры к внешним угрозам. Уделяется внимание и международному сотрудни-

честву в области борьбы с киберпреступностью, например, в рамках «Шанхайской организации сотрудничества» (ШОС) [10].

Помимо государственных структур важную роль в обеспечении информационной безопасности играют и коммерческие структуры. Многие крупные технологические компании, такие как «Microsoft», «Google», «IBM», «Cisco», «Ростелеком», «Лаборатория Касперского» и другие, инвестируют значительные ресурсы в исследования и разработку решений для киберзащиты. Они предлагают широкий спектр продуктов, включая антивирусное программное обеспечение, системы предотвращения вторжений, решения для шифрования данных и защиты облачных сервисов, разрабатывают программные и аппаратные средства для защиты критической инфраструктуры. В ответ на растущие угрозы, такие как атаки на энергосистемы и транспорт, ими предложены системы мониторинга и управления, позволяющие оперативно реагировать на инциденты и минимизировать ущерб.

Частные компании участвуют и в разработке стандартов безопасности и лучших практик. Например, «ISACA» [11] и «ISC» [12] – это ассоциации, которые работают над созданием профессиональных стандартов для специалистов в области информационной безопасности, проводят сертификацию. Подготовленные с их участием стандарты помогают установить единые требования к подготовке специалистов, способствуют повышению уровня информационной безопасности в различных отраслях.

Таким образом, подводя итог проведенному анализу, следует признать, что информация, программное обеспечение и электронные средства в современных условиях являются объектами устремлений не только конкретных хакеров и преступных организаций, использующих их для личного обогащения, но и соответствующих государственных структур, обеспечивающих руководство своих стран сведениями необходимыми для принятия политических решений, а также оказывающих воздействие в необходимых случаях на критическую инфраструктуру других государств для их побуждения к принятию выгодных для своих стран решений. При этом организация совместной работы по выявлению и пресечению трансграничной противоправной деятельности конкретных лиц и преступных организаций, причастных к кибератакам, как правило, не вызывает никаких проблем.

Рассмотрев опыт различных стран, резюмируем, что в настоящее время государства в основном развивают свою стратегию и принимают шаги по борьбе с угрозами в информационном пространстве локально, независимо друг от друга. И на это есть несколько причин, связанных, прежде всего, с необходимостью обеспечения национальной безопасности, конкуренцией между государствами на мировой

арене. В то же время для эффективного противодействия киберугрозам требуется комплексный подход, дальнейшее развитие внутренних технологий и правил, а также международного сотрудничества в области информационной безопасности. Последнее позволит не только обеспечить обмен опытом, но и ускорить разработку единых подходов и новых технологий в рассматриваемой сфере. В связи с этим острым становится вопрос подготовки, подписания и ратификации стандартов, международных соглашений и программ, которые будут устраивать всех стран участников.

---

1. Совет Европы. Конвенция о киберпреступности (Будапештская конвенция) [Электронный ресурс]: от 23 ноября 2001 г. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата обращения: 03.11.2024).

2. ISO/IEC 27001:2013. Информационные технологии – Методы защиты – Системы управления информационной безопасностью – Требования [Электронный ресурс]. URL: https://www.iso.org/isoiec-27001-information-security.html (дата обращения: 03.11.2024).

3. Международный союз электросвязи (МСЭ). Стандарты и рекомендации по кибербезопасности [Электронный ресурс]. URL: https://www.itu.int (дата обращения: 03.11.2024).

4. Европейский Союз. Общий регламент по защите данных (GDPR) [Электронный ресурс]: от 27 апреля 2016 г. URL: https://gdpr.eu/ (дата обращения: 03.11.2024).

5. Компьютерная группа реагирования на чрезвычайные ситуации [Электронный ресурс] // Википедия: URL: https://ru.wikipedia.org/wiki/Компьютерная_группа_реагирования_на_чрезвычайные_ситуации (дата обращения: 03.11.2024).

6. Европол. Европейский центр по борьбе с киберпреступностью (EC3) [Электронный ресурс]. URL: https://www.europol.europa.eu/activities-services/services-support/european-cybercrime-centre-ec3 (дата обращения: 03.11.2024).

7. Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) [Электронный ресурс]. URL: https://www.cisa.gov (дата обращения: 03.11.2024).

8. Закон Китайской Народной Республики о кибербезопасности [Электронный ресурс]: от 1 июня 2017 г. URL: https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017 (дата обращения: 03.11.2024).

9. Российская Федерация. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]: от 5 декабря

2016 г. URL: http://www.scrf.gov.ru/security/information (дата обращения: 03.11.2024).

10. Шанхайская организация сотрудничества. Основные направления сотрудничества в области кибербезопасности [Электронный ресурс]. URL: http://rus.sectsco.org (дата обращения: 03.11.2024).

11. ISACA. Сертификации и профессиональные стандарты для специалистов по информационной безопасности [Электронный ресурс]. URL: https://www.isaca.org (дата обращения: 03.11.2024).

12. ISC. Профессиональные сертификации в области кибербезопасности [Электронный ресурс]. URL: https://www.isc2.org (дата обращения: 03.11.2024).

Сведения об авторе

Князьков Геннадий Вячеславович. Студент магистратуры.

Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации.

119571, Российская Федерация, г. Москва, вн. тер. г. муниципальный округ Тропарево-Никулино, просп. Вернадского, д. 82, стр. 1.

Ключевые слова: информационная безопасность, киберугрозы, кибербезопасность, критическая инфраструктура, международный опыт, международное сотрудничество, частный сектор.

Корниленко А.В.

РАЗЫСКНАЯ РАБОТА РОССИЙСКОЙ ПОЛИЦИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПРОБЛЕМЫ

Деятельность оперативных подразделений органов внутренних дел Российской Федерации по розыску лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания является одной из главных направлений осуществления законности и привлечения указанных лиц к уголовной ответственности. В статье рассматриваются как современное состояние разыскной работы российской полиции, так и существующие объективные проблемы в данной сфере.

Современная ситуация в сфере развития и трансформации преступности характеризуется рядом объективных факторов: ростом организованности, транснациональностью, активным вовлечением несо-

вершеннолетних, использованием информационно-коммуникационных технологий. Несмотря на снижение количества отдельных видов зарегистрированных преступлений, существует устойчивая тенденция роста их тяжких и особо тяжких составов. При этом, по состоянию на сентябрь 2024 г., не раскрытыми остались 632,2 тыс. преступлений, что на 3,6 % больше аналогичного показателя за период с января по сентябрь 2023 г. Из этого количества на тяжкие и особо тяжкие преступления пришлось 32,6 % (в январе–сентябре 2023 г. – 33 %) [1, с. 5].

Одной из наиболее эффективных мер оперативно-разыскного противодействия криминальной угрозе является розыск лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания [2], в целях привлечения их к уголовной ответственности. Под розыском в данном случае понимается деятельность правоохранительных органов, целью которой является установление местонахождения объектов, индивидуально определенные признаки которых известны [3, с. 3].

Нельзя не согласиться, что «осуществление розыска скрывающихся лиц, с одной стороны, – важнейшее условие реализации принципа неотвратимости ответственности за совершенные преступления, пресечения дальнейшей преступной деятельности разыскиваемых, с другой – резерв повышения раскрываемости преступлений прошлых лет» [4, с. 6].

Абсолютно очевидно, что на современном этапе развития общества цифровые и информационно-коммуникационные технологии проникли во все сферы развития нашего общества. Данные процессы напрямую коснулись и разыскной работы органов внутренних дел (ОВД), о чем неоднократно говорилось различными авторами. Считаем, что не имеет смысла повторять эти общеизвестные факты, тем более что проблема использования сотрудником полиции современных технологий, как представляется, исходит не от самого сотрудника, а в физической возможности их использования на уровне «район – город» и связанных с ними вопросах организационного характера.

Несмотря на всю очевидную значимость данного вида деятельности, ее научная проработка представляется крайне недостаточной, будучи «заслоненной», как бы в тени других линий оперативной работы уголовного розыска и иных оперативных подразделений. Это связано с распространенным и исторически неверным сложившимся положением дел, когда «розыск» играет вспомогательную функцию и задействуется, когда, как правило, преступнику по каким-либо причинам удалось скрыться (если речь не идет о без вести пропавших).

При этом стоит отметить весомый научный вклад в развитие разыскной и идентификационной деятельности ОВД, внесенный оте-

чественными учеными В.В. Абрамочкиным, В.М. Атмажитовым, Е.В. Буряковым, Г.С. Воропаевым, Д.А. Гриневой, В.Ф. Луговиком, А.В. Парфеновым, В.И. Поповым, А.Е. Чечетиным и др.

В настоящее время разыскные подразделения территориальных органов внутренних дел представлены на уровне района – группой (направлением) сотрудников (один – три человека), на региональном уровне – отделом (отделением), на межрегиональном и окружном – как правило, отделом. На уровне центрального аппарата, в Управлении организации ОРД Главного управления уголовного розыска МВД России существуют два профильных подразделения: отдел организации межгосударственного розыска лиц и отдел организации федерального розыска лиц и идентификационной работы.

В свою очередь розыск в зависимости от субъектов, его осуществляющих, подразделяется на разыскную деятельность следователя и дознавателя, разыскную деятельность сотрудников оперативно-разыскных служб, разыскную деятельность других служб [5, с. 38; 40].

Как справедливо отмечает А. Парфенов, «скрывшись от органов дознания, следствия и суда, уклоняясь от уголовного наказания …, преступники, находясь на нелегальном положении, пребывают в таких условиях, когда их дальнейшее существование неизбежно связано с преступной деятельностью и совершением ими различного рода преступлений» [6, с. 37]. На наш взгляд, именно это обстоятельство и должно учитываться сотрудниками разыскных подразделений в первую очередь при осуществлении розыска. Однако на практике возникает ряд проблем как организационного, так и личностного характера.

При осуществлении надзора органами прокуратуры за исполнением законов при осуществлении ОРД в подразделениях уголовного розыска в общем и разыскных подразделениях, в частности, выявляются такие нарушения как:

нарушение сроков заведения, регистрации и прекращения дел оперативного учета;

нарушение правил ведения дел оперативного учета;

недостаточность оснований проведения оперативно-разыскных мероприятий.

Отдельно стоит отметить такой недостаток, как плохая «наступательность» в ходе осуществления ОРД, все чаще озвучиваемый уполномоченными прокурорами на различных координационных совещаниях.

В процессе организации розыска поднадзорных, не прибывших к месту осуществления административного надзора, либо самовольно оставивших его допускаются упущения, причинами которых явились «недостаточный уровень осведомленности сотрудников полиции о

круге общения поднадзорного в местах лишения свободы (с которыми непосредственно отбывал наказание, состоял в переписке) и по месту пребывания, непроведение в полном объеме специальных мероприятий по установлению наличия банковских счетов (карт) и пенсионных отчислений, проверок на предмет привлечения к административной ответственности» [7, с. 6–7].

Очевидно, что в разыскной работе важнейшим параметром является оперативность, с которой, как раз, не всегда все «гладко». В своей оперативно-служебной деятельности практические сотрудники разыскных подразделений отмечают наличие таких проблем (напрямую влияющих на эффективность розыска), как:

длительность получения оперативно значимой информации о разыскиваемом или его связях от подразделений специальных технических мероприятий;

недостаточность материально-технического, программного, автотранспортного обеспечения;

несовершенство нормативной правовой базы (хотя надо признать, что определенные шаги по ее совершенствованию делаются).

Наконец краеугольной проблемой является кадровое обеспечение. При хроническом затяжном кадровом «голоде» в ОВД, наиболее остро нехватка личного состава ощущается в подразделениях уголовного розыска, и, соответственно, в разыскных подразделениях.

Не секрет, что помимо чисто экономической причины данной проблемы (низкий уровень денежного довольствия) существуют и других причины: высокая загруженность личного состава, несоизмеримое количество «бумажной» работы, частые проверки по различным поводам, наконец, хамское и бездушное отношение руководства к своим подчиненным.

Отток «старых» кадров – опытных разыскников приводит к тому, что молодые, не так давно назначенные сотрудники не знают, как строить тактику разыскных мероприятий, с кем из других оперативных подразделений взаимодействовать в ходе организации розыска. Имеют место случаи, когда молодые разыскники даже не знают, какой объем оперативно-технических мероприятий может осуществляться в интересах инициатора розыска и как правильно оформляются отдельные служебные документы. Высокая служебная загруженность (а зачастую и нежелание) непосредственных начальников структурных подразделений также не позволяет передать соответствующие полезные знания своим подчиненным.

Подводя итог, отметим, что озвучивание автором проблем разыскной работы ОВД имеет своей целью не принизить или уязвить

руководство или рядовой состав разыскных подразделений, а наоборот, дать пищу для размышлений и стимул к дальнейшему развитию.

Считаем разыскную работу одной из важнейших и наиболее трудоемких направлений оперативно-разыскной деятельности, проведение которой требует от личного состава соответствующих профильных подразделений таких личностных качеств как креативность и живость мышления, настойчивость в достижении целей, стрессоустойчивость, твердость характера, многозадачность. Сами сотрудники розыска должны (а по факту и являются) стать своеобразной элитой оперативных подразделений, задачей же руководителей всех уровней является всесторонняя поддержка, забота о личном составе, грамотная реализация своих властных полномочий в столь значимой для государства сфере.

---

1. Состояние преступности в России за январь–сентябрь 2024 года. М.: ГИАЦ МВД России, 2024. 67 с.

2. Об оперативно-розыскной деятельности: Федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ // Собр. законодательства Рос. Федерации. 1995. № 33, ст. 3349.

3. Опыт применения современных технологий в розыскной работе органов внутренних дел: аналитический обзор / В.Н. Омелин, О.А. Королькова, Д.С. Горячев. М.: ВНИИ МВД России, 2021. 26 с.

4. Опыт и перспективы использования органами внутренних дел государств – участников Содружества Независимых Государств возможностей современных технологий в раскрытии преступлений и межгосударственном розыске преступников: аналитический обзор с предложениями / В.С. Овчинский, О.А. Королькова, А.Г. Кузнецов, О.В. Демковец. М.: ВНИИ МВД России, 2023. 46 с.

5. Медведев И.А. Неотложный розыск по уголовным делам: монография. Красноярск: СибЮИ ФСКН России, 2016. 168 с.

6. Парфенов А.В. Правовые основания организации розыскной и идентификационной деятельности органов внутренних дел // Научный портал МВД России. 2018. № 4. С. 37–41.

7. О практике реализации территориальными органами МВД России полномочий по проведению индивидуальной профилактической работы с ранее судимыми лицами: обзор. МВД России, 2024. 8 с.

Сведения об авторе

Корниленко Александр Владимирович. Кандидат политических наук. Старший преподаватель кафедры организации оперативно-разыскной деятельности.

Академия управления МВД России.
125171, Российская Федерация, г. Москва, ул. Зои и Александра Космодемьянских, д. 8.

Ключевые слова: розыск, оперативно-разыскная деятельность, ОРД, оперативно-разыскные мероприятия, ОРМ, проблемы.

Крысина Т.Е., Смирнов И.М.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

В статье рассматриваются основные аспекты оперативно-разыскной характеристики преступлений в сфере интеллектуальной собственности, а также меры, принимаемые субъектами оперативно-разыскной 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 или 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 видео-конференцсвязи в уголовном процессе и перспективы развития // Интернаука. 2022. № 4-4 (227). С. 61.

2. Гольтяпина 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 народного 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, перераб. и доп. М.: ЮРАЙТ, 2010. 606 с.

Сведения об авторах

Крысина Татьяна Евгениевна. Слушатель факультета подготовки следователей.

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

Кураков Д.В.

ОСОБЕННОСТИ ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ «ПО ГОРЯЧИМ СЛЕДАМ»

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-разыскных мероприятий и неотложных следственных действий. К сожалению, не всегда возможно провести данный комплекс мероприятий своевременно в силу объективных причин, независящих от органов, осуществляющих оперативно-разыскную 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 только что (или недавно) совершенном преступлении, 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]. 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].

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 появляются 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].

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-опера-

тивной 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 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в данном случае будет являться такое оперативно-разыскное мероприятие, как опрос. Оперативно-разыскное мероприятие «опрос» по своей сути – это сбор (получение или добывание) фактической информации, значимой для решения конкретных задач оперативно-разыскной деятельности со слов опрашиваемого физического лица, которое реально или вероятно располагает ею [4]. 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 броских приметах, 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-разыскной 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, по-

этому 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. С. 579.

2. Кузьмин С.В. Содержание планирования расследования преступлений // Правоведение. 2000. № 5. С. 59.

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. С. 136. 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, 2022. С. 139.

5. Муравьев К.В. Уведомление о подозрении в совершении преступления // Уголовный процесс. 2007. № 11. С. 16.

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

Сведения об авторе

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

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

Лисицын А.Г.

ОСОБЕННОСТИ ДЕЯТЕЛЬНОСТИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ПО РАСКРЫТИЮ КРАЖ И НЕПРАВОМЕРНОГО ЗАВЛАДЕНИЯ ТРАНСПОРТНЫМ СРЕДСТВОМ

Противодействие преступности продолжает оставаться актуальным направлением деятельности правоохранительных органов и важной задачей, стоящей перед государством, для разрешения которой требуется использование соответствующего комплекса мер социально-экономического, правового, воспитательного и специального характера.

Одним из субъектов, уполномоченных осуществлять противодействие преступности посредством применения специальных правовых мер, являются органы внутренних дел. Такие меры реализуется и посредством осуществления деятельности оперативно-разыскной направленности.

Анализ легального определения понятия «оперативно-разыскная деятельность», закрепленного в Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ «Об оперативно-розыскной деятельности») [1], позволяет выделить основные элементы, присущие этому виду деятельности.

К таким элементам относятся:

1) субъекты, осуществляющие оперативно-разыскную деятельность;

2) оперативно-разыскные мероприятия – основные средства, осуществление которых позволяет достичь цели оперативно-разыскной деятельности. Они могут проводиться гласным и негласным путем;

3) цель оперативно-разыскной деятельности, которая выражена в защите личности, общества и государства от преступных посягательств.

В теории оперативно-разыскной деятельности оперативно-разыскная деятельность существует несколько подходов для определения содержания этого понятия. «В частности, В.П. Легостаев отмечает, что оперативно-разыскная деятельность представляет собой быстрый поиск информации о лицах и фактах, имеющих оперативный интерес, осуществляемый в гласной и негласной» форме, в целях достижения задач поисковой направленности [2].

Другие авторы в содержание этого понятия вкладывают правоохранительную функцию специфического содержания, характерной

чертой которой является разведывательно-поисковый характер. «Специфическое содержание обусловлено в преимущественно негласном характере и направленности на получение информации, с целью ее последующего использования при выявлении, предупреждении, пресечении и раскрытии преступных деяний, выявлении и установлении лиц, их подготавливающих, совершающих или совершивших, а также в розыске лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от отбывания уголовного наказания и без вести пропавших» [3].

По мнению ряда исследователей, «одного законодательного определения недостаточно для уяснения специфики оперативно-разыскной деятельности. Законодательное определение оперативно-разыскной деятельности носит внешний, описательный характер, оно не позволяет полностью раскрыть ее сущность и содержание, не показывает место этого вида деятельности среди иных видов деятельности правоохранительной направленности. Поэтому возникает необходимость в доктринальной трактовке данного понятия» [4].

С учетом приведенных определений можно обозначить сущность оперативно-разыскной деятельности, которая заключается в следующем:

- во-первых, это вид деятельности правоохранительной направленности, проводимый в соответствии с требованиями закона и носящий юридический характер;

- во-вторых, эта деятельность осуществляется специально уполномоченными на то субъектами (оперативными подразделениями: органов внутренних дел; органов ФСБ; федерального органа исполнительной власти в области государственной охраны; таможенных органов; службы внешней разведки; ФСИН), для которых основным содержанием деятельности является борьба с преступными деяниями и правонарушениями;

- в-третьих, способами осуществления этой деятельности являются оперативно-разыскные мероприятия, перечень которых четко определен законодателем и является закрытым;

- в-четвертых, эта деятельность может осуществляться в гласной и негласной форме. Негласность является главным условием ее результативности, поскольку позволяет получать в полном объеме информацию, имеющую интерес для защиты охраняемых интересов;

- в-пятых, для этой деятельности характерно использование специфических сил, средств и методов. «К силам относятся: оперативные аппараты и их должностные лица, которые организуют и осуществляют оперативно-разыскную деятельность, а также граждане, которые могут привлекаться к проведению оперативно-разыскных ме-

роприятий на конфиденциальной основе. Средства оперативно-разыскной деятельности: различные оперативные технические средства (техника) и оперативные учеты. Сюда же относятся и разыскные собаки, помогающие в обнаружении фактического места нахождения разыскиваемых лиц и предметов. Методы оперативно-разыскной деятельности – «это те выработанные практикой оперативно-разыскной деятельности специальные приемы выявления и изучения лиц, занимающихся преступной деятельностью или причастных к совершению преступлений, а также выявления обстоятельств, имеющих значение для раскрытия и предупреждения преступлений» (метод личного сыска, агентурный метод и др.)» [5].

Оперативно-разыскная деятельность является одним из видов деятельности правоохранительной направленности. В теории государства и права понятие «правоохранительная деятельность» рассматривается в аспекте проблем государственной деятельности, связанной с применением права. «При этом правоохранительная деятельность определяется как деятельность компетентных органов по охране норм права от каких бы то ни было нарушений, по защите прав и свобод человека и гражданина, по предупреждению правонарушений и привлечению к юридической ответственности виновных лиц и т.п. Эта деятельность, как отмечается в юридической литературе, отличается тем, что: осуществляется с помощью применения юридических мер воздействия – предусмотренных законом мер государственного принуждения и взыскания; реализуется в установленном законом порядке, с соблюдением определенных процедур; возлагается на специально уполномоченные государственные органы – правоохранительные органы» [6].

Сопоставляя обозначенные понятия, можно заключить, что те характеристики, которые свойственны правоохранительной деятельности, также в целом присущи и деятельности оперативно-разыскного содержания. Оперативно-разыскная деятельность осуществляется уполномоченными государственными органами и реализуется в установленном законом порядке, а в ее задачи, согласно ст. 2 ФЗ «Об оперативно-розыскной деятельности», входит выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих или совершивших. В соответствии со ст. 11 ФЗ «Об оперативно-розыскной деятельности», результаты оперативно-разыскной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий. Они могут служить поводом и основанием для возбуждения уголовного дела, представляться в орган дознания, следователю или в суд, в производстве которого находится уголовное де-

ло, а также использоваться в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального законодательства РФ, регламентирующими собирание, проверку и оценку доказательств. Отсюда логично рассматривать оперативно-разыскную деятельность как специфическую разновидность правоохранительной деятельности, осуществляемой только специально уполномоченными государственными органами (как правило, негласно) в целях защиты законных прав и интересов человека, общества и государства от преступных посягательств.

В теории оперативно-разыскной деятельности вопросы, связанные с понятием и содержанием организации работы по борьбе с криминальным автобизнесом, должным образом не исследованы.

Официальные статистические данные свидетельствуют о снижении количества зарегистрированных краж и неправомерного завладения автомобилем или иным транспортным средством без цели хищения. «Так, за январь–декабрь 2023 года на территории РФ было всего зарегистрировано 6865 краж транспортных средств (-23,6 %), из них 3782 кражи автомобилей (-28,2 %), и 12338 преступлений, связанных с неправомерным завладением автомобилем или иным транспортным средством без цели хищения (-8,6 %)» [7].

В целом оперативно-разыскную деятельность по раскрытию угонов и краж транспортных средств можно определить, как специфический вид деятельности правоохранительной направленности, целями которого являются: установление лиц, причастных к совершению противоправных деяний, предметом посягательства которых являются автотранспортные средства, непосредственное определение фактического места нахождения, угнанного или похищенного транспортного средства, выявление причин и условий, способствующих совершению таких деяний, а также осуществление нейтрализации противодействию со стороны злоумышленников следствию и суду.

Представляется, что организация деятельности сотрудников оперативных подразделений должна главным образом быть ориентирована на установление лиц, которые причастны к совершению указанных преступных деяний (непосредственные исполнители, подстрекатели и лица, которые оказывали содействие и помощь при хищении или угоне транспортных средств), их розыск и последующее задержание.

Тактика раскрытия сотрудниками подразделений уголовного розыска краж (угонов) транспортных средств включает в себя совместные действия сотрудников оперативных подразделений, следователя и иных участников следственно-оперативной группы по установлению лица, причастного к совершению этого преступного деяния, выявле-

нию его фактического места нахождения для последующего задержания и проведения необходимых следственных действий, а также обнаружение похищенного (угнанного) автомобиля.

После получения информации о совершении кражи (угона) автомобиля основной тактической задачей является раскрытие кражи (угона) «по горячим следам». Эффективность раскрытия преступного хищения транспортного средства будет зависеть от оперативности начала действий и мероприятий по его раскрытию. Первоначальные действия по раскрытию угона (хищения) автомобиля «по горячим следам» нужно начинать совершать в первые сутки, с того момента, когда был непосредственно совершен угон. Главным фактором, обуславливающим эффективность раскрытия преступных деяний этого вид, выступает временной фактор. На этом этапе проводятся следующие мероприятия и действия: установление механизма совершения преступного деяния; непосредственное задержание угонщика, осуществление розыска автомобиля, установление лица, совершившего преступное деяние и скрывшегося с места происшествия, посредством введения и реализации плана «Перехват»; выявление следов, их фиксация и изъятие, обеспечение сохранности обстановки на месте происшествия; выявление возможных очевидцев происшедшего преступного события, их опрос с целью получения информации, имеющий оперативный и доказательственный интерес.

Принимая участие в раскрытии преступного хищения (неправомерного завладения без цели хищения) транспортного средства, сотрудник подразделения уголовного розыска активно взаимодействует со следователем и иными участниками следственно-оперативной группы, выполняет поручения следователя, проводит оперативно-разыскные мероприятия по сбору информации, представляющей оперативный интерес, устанавливает фактическое место нахождения очевидцев преступного деяния, проводит их опрос, а также предпринимает меры к розыску похищенного автомобиля, выдвигает возможные версии происшедшего, помогает в разработке плана совместных следственных действий и оперативно-разыскных мероприятий, осуществляет информационно-аналитическую работу (работает с учетами, имеющимися в органах внутренних дел), а также осуществляет иные действия в целях раскрытия преступного деяния этого вида.

Подводя итог, отметим, что деятельность сотрудников оперативных подразделений по раскрытию краж и неправомерного завладения транспортным средством представляет собой специфический вид деятельности правоохранительной направленности, осуществляемый уполномоченными на то законом органами, посредством производства оперативно-разыскных мероприятий, использования тактиче-

ских приемов и средств, в целях установления лиц, причастных к совершению таких преступных деяний, их розыска и задержания, обнаружения фактического места нахождения похищенного или угнанного транспортного средства и его последующей передаче законному владельцу. Эффективность такой деятельности зависит от качества проводимых оперативно-разыскных мероприятий, следственных и иных действий, а также от взаимодействия сотрудников оперативных подразделений со следователями, сотрудниками Госавтоинспекции и иными подразделениями органов внутренних дел и других органов.

1. Об оперативно-розыскной деятельности: Федер. закон Рос. Федерации от 12 августа 1995 г. № 144-ФЗ: в ред. от 28 июня 2022 г. // Собр. законодательства Рос. Федерации. 1995. № 33, ст. 3349.

2. Легостаев В.П. ОРД как вид правоохранительной деятельности и ее признаки // Вестник академии знаний. 2013. № 1. С. 195.

3. Кондратьев М.В., Драпезо Р.Г. Об актуальности оперативно-розыскной деятельности на современном этапе развития государства // Вестник Кемеровского государственного университета. 2015. № 2. С. 171–172.

4. Теория оперативно-розыскной деятельности / [О.А. Вагин, К.К. Горяинов, А.В. Земскова и др.]; под редакцией заслуженного деятеля науки Российской Федерации, доктора юридических наук, профессора К.К. Горяинова, заслуженного юриста Российской Федерации, доктора юридических наук В.С. Овчинского. 5-е изд., перераб. М.: Норма: ИНФРА-М, 2021. С. 178.

5. Правовые основы оперативно-розыскной деятельности: учеб. пособие / В.Ю. Алферов, А.И. Гришин, Н.И. Ильин; под общ. ред. В.В. Степанова. 3-е изд., испр. и доп. Саратов: Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2016. С. 12.

6. Тарасов А.М. К вопросу о понятии правоохранительной деятельности и о правоохранительных органах // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2018. № 4 (44). С. 299–300.

7. Состояние преступности в России за январь–декабрь 2023 года [Электронный ресурс]. URL: https://мвд.рф/reports/item/47055751 (дата обращения: 16.04.2024).

Сведения об авторе

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

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

Ключевые слова: раскрытие краж, завладение транспортным средством, раскрытие, следователь, преступление.

Малахаев Д.Д.

ОПЕРАТИВНО-РАЗЫСКНЫЕ МЕРЫ ПО ВЫЯВЛЕНИЮ И РАСКРЫТИЮ ЭКСТРЕМИСТСКИХ ДЕЙСТВИЙ, СОВЕРШАЕМЫХ ИНОСТРАННЫМИ ГРАЖДАНАМИ

В настоящей статье автором дается краткая характеристика оперативно-разыскных мер по выявлению и раскрытию экстремистских действий, совершаемых иностранными гражданами, рассматриваются основные проблемы и делаются предложения по их решению.

Современные условия глобализации и миграционных процессов способствуют увеличению числа преступлений экстремистского характера, совершаемых иностранными гражданами на территории различных государств, в том числе и России. Экстремистская деятельность представляет собой значительную угрозу национальной безопасности, общественному порядку и стабильности, что требует применения эффективных методов выявления и пресечения подобных действий. В этой связи важную роль играет оперативно-разыскная деятельность (ОРД), нацеленная на своевременное обнаружение, предупреждение и раскрытие экстремистских преступлений.

Актуальность темы обусловлена возросшими рисками, связанными с участием иностранных граждан в экстремистских актах, а также недостаточностью существующих правовых механизмов и ресурсов для их пресечения. В условиях постоянного изменения тактик и методов экстремистских групп необходима постоянная адаптация оперативно-разыскных мер и совершенствование правоприменительной практики.

В последние годы опубликовано множество научных работ, посвящённых проблемам борьбы с экстремизмом. Так, в диссертации на тему «Методологические основы раскрытия и расследования преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет» А.В. Кутузов изложил

методологические основы и представлены практические рекомендации относительно повышения результативности раскрытия и расследования преступлений экстремистской направленности, посредством оптимизации и интенсификации процесса получения и использования актуальной уголовно-релевантной информации [1].

И.А. Яцкина в работе «Совершенствование методики расследования преступлений, связанных с пропагандой экстремизма» рассмотрела вопросы разработки комплексных криминалистических рекомендаций для повышения эффективности раскрытия преступлений экстремистской направленности. В работе решены ключевые задачи, включая анализ и систематизацию научных источников, классификацию преступлений, составление профиля преступников, изучение методов их совершения и особенности сбора первичной информации.

Не смотря на достижения ученых других научных отраслей юриспруденции оперативно-разыскная деятельность (ОРД) в современной правовой системе является ключевым инструментом борьбы с преступностью, включая преступления экстремистской направленности, совершаемые иностранными гражданами. Для полного понимания и эффективного применения ОРД необходимо проанализировать её теоретико-правовые основы, правовую регламентацию, а также специфические особенности в контексте экстремистских действий.

Экстремистские действия – это общественно опасные деяния, направленные на разжигание ненависти, вражды по признаку расы, национальности, религии или политических убеждений, а также дестабилизацию государственного строя. Юридическое определение таких действий содержится в ст. 1 Федерального закона № 114-ФЗ «О противодействии экстремистской деятельности» [2].

Под оперативно-разыскными мерами следует понимать комплекс действий, которые проводят оперативные подразделения государственных органов для выявления, предупреждения, пресечения и раскрытия преступлений, а также для розыска лиц, скрывающихся от правосудия.

Правовой режим оперативно-разыскных мероприятий в отношении иностранных граждан в России требует соблюдения международных обязательств страны, а также учета специфики миграционных потоков и трансграничных угроз. Согласно российскому законодательству, иностранные граждане на территории страны подчиняются тем же законам, что и граждане России, однако их действия часто требуют более тщательного контроля с точки зрения угроз национальной безопасности.

Федеральный закон № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства» устанавливает обязанности

органов внутренних дел по учету и контролю иностранных граждан, что служит основой для осуществления оперативно-разыскных мероприятий в отношении потенциальных экстремистов.

ОРД в отношении иностранных граждан также регулируется международными соглашениями о правовой помощи и сотрудничестве, такими как Европейская конвенция о взаимной правовой помощи по уголовным делам и соглашения с Интерполом.

Также важным аспектом является необходимость учета культурных, религиозных и социальных особенностей иностранных граждан, чтобы избежать неправильной интерпретации действий и излишне репрессивных мер. Для этого оперативные сотрудники должны обладать специальными знаниями и проходить дополнительное обучение.

Юридическая квалификация экстремистских действий требует учёта их социальной опасности и специфики. Экстремизм представляет собой серьёзную угрозу для стабильности и благосостояния общества, может привести к насилию, экономическим потерям и разрушению принятых обществом ценностей.

Экстремистские преступления могут носить как индивидуальный характер, например, размещение материалов экстремистского характера в интернете, так и групповую организационную форму, что усложняет их оперативное выявление и пресечение [3].

Для определения экстремистских действий учитываются следующие критерии:

1. Действия связаны с неприятием существующего государственного или общественного порядка и осуществляются в незаконных формах. Экстремистскими будут те действия, которые связаны со стремлением разрушить, опорочить существующие в настоящее время общественные и государственные институты, права, традиции, ценности.

2. Действия носят публичный характер, затрагивают общественно значимые вопросы и адресованы широкому кругу лиц.

При расследовании экстремистских преступлений необходимо использовать на всех стадиях досудебного производства возможности оперативных разработок для выявления скрываемых преступлений, установления всех элементов конспирируемой экстремистской деятельности, субъектов, её осуществляющих, и их ролей.

Раскрытие тщательно скрываемых преступлений экстремистской направленности требует продуктивного взаимодействия органов оперативно-разыскной деятельности и расследования. Для успешного выявления всех участников преступной деятельности и устранения экстремизма важно рассмотреть несколько ключевых проблем.

Первой проблемой является транснациональный характер экстремизма, который осложняется отсутствием единого международного подхода к его определению. В каждой стране существуют свои законы и трактовки экстремистских действий и высказываний. Это приводит к тому, что одно и то же поведение может считаться преступлением в одной юрисдикции и оставаться безнаказанным в другой. Такие расхождения создают трудности в международном сотрудничестве, особенно при совместных расследованиях и обмене информацией.

Правовые различия между странами также играют важную роль. Когда требуется взаимодействие, чтобы передать данные о подозреваемых лицах или проводить международные расследования, различия в законодательствах могут значительно замедлить или даже сделать невозможным процесс обмена информацией и проведения оперативных действий.

Экстремизм, в свою очередь, является питательной средой для терроризма, который представляет собой серьёзную угрозу общественной и государственной безопасности. Для эффективной борьбы с терроризмом необходимо не только сотрудничество на международном уровне, но и усиление правовой базы, которая обеспечит возможность обмена информацией, упрощения экстрадиции и организации совместных расследований и операций.

Активное использование экстремистскими группами интернета для распространения своих идей, привлечения новых участников и координации действий представляет серьёзную проблему.

Современные технологии позволяют экстремистам на качественно ином уровне организовывать процесс расширения своей пособнической базы и совершенствовать методы вербовки новых членов. Например, закрытые группы в мессенджерах, таких как Telegram и WhatsApp, дают возможность экстремистам обмениваться информацией и инструкциями, оставаясь при этом анонимными.

Использование криптовалют усложняет задачу правоохранительных органов по перекрытию каналов финансирования экстремистских группировок. Анонимность криптовалютных транзакций, трансграничность переводов, большая стоимость и доступность делают их привлекательным механизмом для финансирования экстремистской деятельности.

Для предотвращения неправомерного использования криптовалют экстремистскими группами необходимо расширять сотрудничество между правоохранительными органами и криптобиржами, улучшать меры по борьбе с отмыванием денег и обеспечивать большую прозрачность в криптоэкосистеме.

Также включить интернет-ресурсы, предоставляющие возможность скрывать личные данные (такие как VPN и даркнет), в список угроз, которые подлежат блокировке с помощью технических средств противодействия угрозам (ТСПУ). Это позволит ограничить доступ к анонимным сервисам и предотвратить использование виртуальных номеров телефонов для регистрации в мессенджерах и на сайтах.

И разработать систему мониторинга интернет-трафика, которая даст возможность контролировать передачу данных между операторами связи и интернет-провайдерами. Такая система позволит оперативно выявлять подозрительные активности и передавать данные в правоохранительные органы для быстрого реагирования.

1. Кутузов А.В. Методологические основы раскрытия и расследования преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет: автореф. дис. ... канд. юрид. наук. Ростов-на-Дону, 2022. 25 с.

2. О противодействии экстремистской деятельности [Электронный ресурс]: от 25 июля 2002 г. № 114-ФЗ. Доступ из справ.-правовой системы «ГАРАНТ».

3. Карагодин В.Н. Некоторые особенности расследования преступлений экстремистской направленности // Актуальные вопросы профилактики и расследования преступлений экстремистской и террористической направленности: материалы Международной научно-практической конференции (Москва, 9 ноября 2023 г.). М.: Московская академия Следственного комитета Российской Федерации, 2023. С. 82–88.

Сведения об авторе

Малахаев Данила Денисович. Адъюнкт кафедры оперативно-разыскной деятельности и специальной техники.

Московский университет МВД России имени В.Я. Кикотя.

117437, Российская Федерация, г. Москва, ул. Академика Волгина, д. 12.

Ключевые слова: экстремизм, оперативно-разыскные меры, информационно-телекоммуникационные технологии, интернет-ресурсы, трансграничность,

Малик Е.Н., Малик В.И.

БОРЬБА С ВИРТУАЛЬНЫМ НАРКОБИЗНЕСОМ: ЗАЩИТА НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ РОССИИ

В статье раскрывается проблема выявления сетевой наркопреступности, а также обосновано пагубное влияние бесконтактного распространения наркотических средств на духовное здоровье нации. Незаконный сбыт наркотических средств и психотропных веществ, представляет собой одну из злободневных тем современного общества.

Проблема сетевой наркопреступности является одной из главных составляющих общественной и информационной безопасности Российской Федерации. Использование киберпространства и криптовалют для незаконного оборота наркотических веществ создает серьезные проблемы для специалистов в области уголовного правосудия, особенно для правоохранительных органов.

Сеть Интернет выступает коммуникативным полем, поскольку большинство сайтов предусматривает блог для общения пользователей. Стоит взять во внимание, «что наступление новой информационной эры сулит всем «несомненные блага». Однако все понимают, что, как в любом явлении, последствия могут быть как позитивными, так и негативными» [1, с. 27].

Последние достижения в области развития информационно-телекоммуникационных технологий позволили транснациональным организованным группам использовать Интернет как рынок для продажи синтетических наркотиков. Точное количество синтетических наркотиков, продаваемых в Сети, трудно оценить, но количество интернет-магазинов и веб-сайтов, продающих наркотические вещества, неуклонно растет.

Если в 90-х гг. сбыт наркотиков осуществлялся посредством передачи определенных материальных ценностей в руки продавцу (деньги, ювелирные украшения и др.) и взамен потребитель получал на руки товар (в данном случае, наркотик определенного типа), то в настоящее время «большая часть сбытов осуществляется бесконтактным способом, путем безналичного перевода денежных средства и последующего получения наркотика в тайнике (так называемой, закладке)» [2, с. 106].

Интернет становится все более популярным среди отдельных лиц и организованных преступных групп как платформа для незаконного оборота синтетических наркотиков. Приведем некоторые осо-

бенности Глобальной сети, которые используют наркоторговцы при дистанционных способах незаконного оборота наркотиков:

1. С высокой степенью анонимности. Благодаря применению технологий анонимизации, таких как шифрование, VPN, прокси-серверы и другие, преступники избегают обнаружения законом, поскольку затрудняют свое выявление и идентификацию.

2. Мировой охват. Использование Интернета предоставляет преступникам возможность широкого присутствия и доступа к большему числу клиентов. Кроме того, упрощается анонимное общение между продавцом и покупателем, и сокращается необходимость личного взаимодействия [3].

3. Простой доступ к форумам для обмена знаниями и опытом. В сети Интернет существует обилие информации о различных вопросах, включая инструкции по изготовлению наркотиков, способы получения запрещенных веществ-прекурсоров, услуги по распространению и пересылке денежных средств, а также меры конфиденциальности, помогающие избежать выявления со стороны правоохранительных органов.

Роль Интернета в содействии торговле наркотиками обратила на себя внимание после закрытия нескольких веб-сайтов «клирнета» (общедоступного Интернета) и DarkNet, также известных как торговые площадки [4, с. 33]. Синтетические наркотики продаются в социальных сетях, на веб-сайтах клирнета и в даркнете. Онлайн-торговля может оказать значительное влияние на общий оборот наркотиков.

Важно подчеркнуть, что использование онлайн-платформ по продаже синтетических наркотиков в последние годы увеличилось и диверсифицировалось, предоставляя преступникам эффективные возможности для рекламы своей продукции и привлечения клиентов, а также методы эффективного сокрытия своих незаконных операций.

Эти платформы также помогли повысить профессионализм продаж лекарств, продвигая продукты с подробными описаниями, фотографиями, информацией о наличии, акциями и скидками, а также создавая прочную репутацию среди онлайн-клиентов. Онлайн-платформы включают торговые площадки DarkNet, социальные сети, приложения для обмена сообщениями, услуги связи и платежные системы.

КЛИРНЕТ – это общедоступный Интернет, к которому легко получить доступ при обычном подключении к Интернету и с использованием стандартного веб-браузера, включающий, например, Google, онлайн-игры, YouTube, Wikipedia и Netflix. Клирнет содержит ряд веб-сайтов, блогов, форумов и торговых площадок, на которых есть возможность рекламировать различные синтетические наркотики. Такие торговые площадки часто выдают себя за розничных продавцов

большого спектра фармацевтических препаратов и строго регулируемых химических веществ-прекурсоров.

ГЛУБОКАЯ СЕТЬ (DEEP WEB) – общедоступный Интернет, закрытый для поисковых систем, таких как Google, и включает, например, зашифрованные или неиндексируемые веб-сайты, частные базы данных и другой несопряженный контент, такой как медицинские записи, научные базы данных и юридическая документация.

ДАРКНЕТ (DarkNet) – это часть «всемирной паутины», к которой нельзя получить доступ с помощью стандартных веб-браузеров, таких как Internet Explorer, Firefox, Edge или Chrome. Он работает внутри специализированных зашифрованных сетей, обеспечивающих анонимность. «Как и клирнет, даркнет содержит тысячи веб-страниц, но они становятся доступными только при подключении к даркнету» [5, с. 270].

Наркоторговцы используют различные сервисы по доставке сообщений, МЕССЕНДЖЕРЫ, со сквозным шифрованием для рекламы и продажи своей продукции, а также для связи с покупателями с использованием данных геолокации. Мессенджеры также используются подпольными дилерами криптовалют для организации их обмена.

При том, что СОЦИАЛЬНЫЕ МЕДИА, несомненно, расширили возможности для социального взаимодействия, они также используются отдельными лицами и транснациональными организованными преступными группировками для незаконного оборота наркотиков.

Платформы и приложения социальных медиа, таких как Facebook, Instagram (Компания Meta на территории РФ признана экстремистской организацией), Snapchat и других, применялись для обеспечения незаконного оборота наркотиков с использованием изображений и видео. «Серьезную опасность представляют специализированные форумы в социальных сетях, темы которых посвящены употреблению наркотиков. Крупнейшим онлайн-форумом, на котором зарегистрированы интернет-магазины по продаже этого вида наркотиков, является Legal. RC, доступ к которому в Российской Федерации решением Роскомнадзора запрещен». Продавцы часто используют всевозможные эмоджи, хештеги и сленг для рекламы продаваемых ими наркотиков в сообщениях, твитах или именах пользователей в социальных медиа. У людей есть возможность искать различные наркотики и получать подробную информацию о том, где и как их приобрести.

При всем этом исключается личная встреча участников сделки что обеспечивает сложность поиска и привлечения к ответственности всех участников преступной схемы [6, с. 45]. В «экосистеме онлайн-торговли» есть несколько акторов с разными режимами (ролями):

Администраторы: несут ответственность за обеспечение эффективной работы торговой площадки.

Продавцы: поставщики наркотиков, которые продают свою продукцию на рынке. Обычно они делают это, создавая свои собственные странички по продаже [7].

Покупатели: лица, которые покупают рекламируемые наркотики. Покупатели также оставляют отзывы после совершения покупок и участвуют в обсуждениях в различных блогах и форумах.

Дропы: («мулы»; буквально «ишаки») те, кто доставляет наркотики по месту назначения.

В настоящее время на просторах Интернета доступна обширная информация на тему наркотических средств, включая рецептуры, способы изготовления и приобретения. Важно проводить дифференциацию по классификации интернет-ресурсов, связанных с распространением наркотиков [8].

Первая категория: веб-сайты государственных организаций, которые распространяют информацию для обеспечения пользователей обновленными научными открытиями и исследованиями в области незаконного оборота наркотиков.

Вторая категория: ресурсы клубов, сообществ и социальных групп, обычно направленные на образовательные цели, такие как реабилитация после употребления наркотиков и борьба с наркозависимостью.

Третья категория: частные веб-сайты, целью которых является распространение информации о наркотиках, обсуждение побочных эффектов и т.д. Чаще всего контент данных сайтов представляет собой повествование об использовании наркотиков с точки зрения наркозависимых.

Четвертая категория: владельцы сайтов, активно привлекающие внимание общественности, предлагают на продажу как легальные, так и полулегальные наркотики.

При всех вышеперечисленных обстоятельствах гораздо сложнее оперативно провести оперативно-разыскные мероприятия, направленные на выявление и пресечение подпольных каналов поставки наркотиков, а также доказать их сбыт и виновность наркоторговцев. При этом следует учитывать, что «выявление и расследование правонарушений, связанных с использованием ресурсов сети Интернет, в большинстве случаев требует специальных знаний в области сетевых и компьютерных информационных технологий» [9, с. 320].

1. Устинович Е.С. Социальное государство в условиях информационного развития // Социальная политика и социальное партнерство. 2017. № 11.

2. Дудник И.С. Особенности проведения оперативно-розыскных мероприятий при документировании преступлений, связанных с незаконным оборотом наркотических веществ, осуществляемых бесконтактным способом // Право и государство: теория и практика. 2020. № 7 (187). С. 106–109.

3. Полуянов С.А., Филатова В.А. Некоторые вопросы выявления и пресечения сбыта наркотиков бесконтактным способом с использованием сети Интернет // Актуальные проблемы противодействия наркотрафику на современном этапе: сб. мат-в между-нар. науч.-практ. семинара (2–3 апр. 2020 г.). Красноярск: Сибирский юридический институт Министерства внутренних дел Российской Федерации, 2020. С. 26–31.

4. Старченко В. Актуальные проблемы противодействия незаконному обороту наркотических средств с использованием сети Интернет и пути их решения // Российско-азиатский правовой журнал. 2020. № 1. С. 32–35.

5. Малик В.И. Актуальные проблемы противодействия сбыта наркотических средств и психотропных веществ с использованием информационных технологий // Безопасность в современном мире: материалы III Всероссийской научно-практической конференции с международным участием (Волгоград, 17 февраля 2021 г.) / отв. редактор С.А. Бондарева. Часть 2. Волгоград: Волгоградский институт управления – филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», 2021. С. 268–271.

6. Васюков В.Ф. Расследование дел о сбыте наркотиков с использованием мессенджеров и криптовалюты // Уголовный процесс. 2019. № 9 (177). С. 44–49.

7. Овчинникова О.В. Особенности расследования сбыта наркотических средств, совершенных с использованием сети Интернет // Правопорядок: история, теория, практика. 2018. № 1. С. 94–98.

8. Дикарев В.Г., Олимпиев А.Ю. К вопросу о противодействии бесконтактному способу сбыта наркотиков через сеть Интернет // Вестник Московского университета МВД России. 2016. № 8. С. 147–152.

9. Колычева А.Н. Отдельные аспекты судебной компьютерной экспертизы, назначаемой при расследовании преступлений, совер-

шенных с использованием сети Интернет // Вопросы экспертной практики. 2019. № S1. С. 319–324.

Сведения об авторах

Малик Елена Николаевна. Кандидат политических наук, доцент. Сотрудник Академии ФСО России.

Академия ФСО России.

302015, Российская Федерация, г. Орел, ул. Приборостроительная, д. 35.

Малик Владислав Игоревич. Кандидат юридических наук. Преподаватель кафедры оперативно-разыскной деятельности ОВД.

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

Ключевые слова: наркопреступность, виртуальный наркобизнес, информационные технологии, сеть Интернет, расследование преступлений, противодействие наркобизнесу.

Марков А.Ю.

НЕКОТОРЫЕ АСПЕКТЫ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ОТНОШЕНИИ ОСУЖДЕННЫХ ИНОСТРАННЫХ ГРАЖДАН, ОТБЫВАЮЩИХ НАКАЗАНИЕ В ИСПРАВИТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

На основе статистических показателей органов государственной власти, исследований преступности иностранных граждан, полученных эмпирических данных обоснована необходимость совершенствования методов оперативно-разыскной деятельности заинтересованных подразделений учреждений и органов уголовно-исполнительной системы Российской Федерации при работе с осужденными иностранными гражданами.

Анализ статистической отчетности показателей Росстата [1], МВД России [2], ФСИН России [3], Судебного департамента при Верховном Суде Российской Федерации [4] позволяют сделать следующие выводы:

- с 2015-го по 2023 г. произошло значительное снижение количества осужденных, отбывающих наказание в исправительных учреждениях уголовно-исполнительной системы России. Количество осужденных снизилось в исправительных колониях (далее – ИК) общего режима на 60 % – 84699 чел., ИК строгого режима на 51,4 % – 146433 чел., ИК особого режима на 42,2 % –11357 чел., колониях поселениях на 33,5 % – 10487 чел., лечебно-исправительных учреждениях на 72,8 % – 19816 чел., лечебно-профилактических учреждениях на 37,7 % – 4686 чел.

Резкое снижение спецконтингента в ИК общего режима произошло в 2018 г. – 18305 чел. и 2020 г. – 17907 чел., тогда как в ИК строгого режима в 2022 г. – 35428 чел. и 2023 г. – 36910 чел.

- значительная часть иностранных граждан отбывает наказание в исправительных колониях:

в ИК общего режима: 2020 г. – 3722 чел.; 2021 г. – 3006 чел., 2022 г. – 3654 чел., 2023 г. – 3600 чел.;

в ИК строгого режима: 2020 г. – 14710 чел.; 2021 г. – 13826 чел., 2022 г. – 12836 чел., 2023 г. – 14125 чел.;

в ИК особого режима: 2020 г. – 0 чел.; 2021 г. – 0 чел., 2022 г. – 380 чел., 2023 г. – 381 чел.;

- соотношение количества иностранных осужденных, отбывающих наказание в исправительных колониях к списочному составу спецконтингента систематично увеличивается:

в ИК общего режима: 2020 г. – 4,78 %; 2021 г. – 4,35 %, 2022 г. – 5,76 %, 2023 г. – 6,39 %;

в ИК строгого режима: 2020 г. – 6,62 %; 2021 г. – 6,56 %, 2022 г. – 7,31 %, 2023 г. – 10,18 %;

в ИК особого режима: 2020 г. – 0 %; 2021 г. – 0 %, 2022 г. – 1,98 %, 2023 г. – 2,45 %;

- произошло увеличение уровня нарушений (на 1000 чел.) в исправительных учреждениях:

нарушений установленного порядка отбывания наказания:

2015 г. – 1126,9; 2023 г. – 1911,58 (увеличение на 70 %);

злостных нарушений установленного порядка отбывания наказания:

2015 г. – 41,7; 2023 г. – 54,26 (увеличение на 30,2 %);

- миграционные процессы оказывают влияние на криминальную ситуацию в местах лишения свободы в большей степени, путем формирования качественно-количественного состава спецконтингента. Число иностранных граждан стран ближнего зарубежья (СНГ) значительно превалирует в количественном соотношении с гражданами дальнего зарубежья. Осужденные иностранные граждане таких госу-

дарств, как Узбекистан, Таджикистан, Украина, Беларусь, Азербайджан, Киргизия имеют весомое численное преимущество в местах лишения свободы по сравнению с представителями других государств.

Среди осужденных-иностранцев довольно часто встречаются лица с устойчивой криминогенной мотивацией, осознанно идущие на совершение преступления. Данное обстоятельство обусловлено тем, что криминологические портреты осужденного рассматриваемой категории и осужденного рецидивиста совпадают.

Сохраняется тенденция к активизации противоправных действий осужденных, направленных на дестабилизацию деятельности исправительных учреждений, однако если ранее значительное влияние имели «воровские традиции», то в настоящее время иерархично построенная система «воровских понятий» легко разбивается о догмы ислама. Примером тому является принятие в качестве «своих» осужденных по насильственным статьям, если они единой веры в среде иностранных граждан. Стирается кастовый подход к определению места в криминальной иерархии. Данные обстоятельства с одной стороны развенчивают криминальную субкультуру, с другой стороны значительно усложняют работу оперативным подразделениям уголовно-исполнительной системы России, выработанную годами. В настоящее время значительная работа направлена на сохранение «этнического баланса» в исправительных учреждениях.

Криминогенность исправительных учреждений обусловлена рядом детерминант, которые связаны с присутствием осужденных иностранных граждан в структуре спецконтингента. Среди причин возникновения криминальных ситуаций с участием иностранных граждан можно выделить следующие:

- борьба за распределение материальных и культурных благ, а также материальных ценностей между группами осужденных;
- нерешенные правовым путем бытовые конфликты, возникающие на почве геополитической неприязни;
- этнографические различия в культуре и сложность восприятия их другими осужденными;
- отсутствие этноконфликтологического мониторинга.

В настоящее время сформирована устоявшаяся модель оперативной работы в исправительных учреждениях. Данная модель предполагает непосредственное оперативное взаимодействие по установлению нераскрытых эпизодов с целью доказывания обстоятельств по уголовным делам. В исправительных учреждениях оперативная работа строится с учетом тюремной субкультуры и использования принципов криминальной иерархии. Современные тенденции миграционных процессов формируют качественный состав исправительных уч-

реждений. В зависимости от всплесков миграционного прироста меняется структура спецконтингента в пенитенциарных учреждениях. Миграционные процессы влияют на методы оперативной работы с учетом демографических особенностей лиц, в отношении которых она осуществляется. Криминальная субкультура утрачивает свое значение на фоне концентрации иностранных граждан в местах лишения свободы, которые отказываются соблюдать ее принципы. Современная геополитическая ситуация требует пересмотра устоявшихся принципов оперативной работы и учетом тенденций миграционных процессов и их последствий.

---

1. Численность и миграция населения Российской Федерации [Электронный ресурс] // Статистический бюллетень Росстата / Официальный сайт Росстата. URL: https://rosstat.gov.ru/compendium/document/13283 (дата обращения: 10.10.2024).

2. Состояние преступности в России [Электронный ресурс] // Аналитический сборник МВД России / Официальный сайт МВД России. URL: https://мвд.рф/folder/101762 (дата обращения: 10.10.2024).

3. Основные показатели деятельности уголовно-исполнительной системы ФСИН России [Электронный ресурс] // Информационно-аналитический сборник ФКУ НИИИИТ ФСИН России / Официальный сайт ФКУ НИИИТ ФСИН России. URL: https://niiit.fsin.gov.ru/niiit (дата обращения: 10.10.2024).

4. Сводные статистические сведения о состоянии судимости в России [Электронный ресурс] // Отчет Судебного департамента при Верховном Суде Российской Федерации / Официальный сайт Судебного департамента при Верховном Суде Российской Федерации. URL: http://www.cdep.ru/?id=79 (дата обращения: 10.10.2024).

Сведения об авторе

Марков Александр Юрьевич. Преподаватель кафедры организации режима юридического факультета.

Санкт-Петербургский университет Федеральной службы исполнения наказаний.

196602, Российская Федерация, г. Санкт-Петербург, г. Пушкин, ул. Саперная, д. 34, лит. А.

Ключевые слова: миграция, преступления иностранных граждан, криминогенность, пенитенциарные учреждения, безопасность, оперативно-разыскная деятельность.

Поддубный И.В.

ОТДЕЛЬНЫЕ АСПЕКТЫ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ УГОЛОВНОГО РОЗЫСКА ПО РАСКРЫТИЮ УБИЙСТВ

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-разыскных 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-разыскное 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-разыскных мероприятий в отношении лиц, предметов и фактов, представляющих оперативный интерес, обеспечению использования их в качестве доказательств по уголовном делу и преодолению противодействия расследования. 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 поручении 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-разыскных 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-разыскной деятельности позволяет оперуполномоченному получить большой массив информации о произошедшем.

При принятии решении о производстве оперативно-разыскных 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-разыскное 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 уголовном 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 отме-

тить, что содержание планирования при подобных условиях должно содержать следующие элементы [4, с. 618]:

– формулирование круга обстоятельств, подлежащих установлению в ходе проведения оперативно-разыскных 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 разыскных мероприятий.

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

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

– убийство совершено 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-разыскных версий имеет свои особенности в содержании и тактике оперативно-разыскных мероприятий.

Обязательными 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;

– изучение архивных уголовных дел и дел оперативного учета по преступлениям, обстоятельства совершения которых аналогичны расследуемому преступлению;

– отработка связей потерпевшего и выявление среди них лиц, ранее судимых за совершение преступление 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, на современном этапе развития оперативно-разыскной 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-разыскных 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.). СПб.: 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, перераб. и доп. М.: ЮРАЙТ, 2010. 606 с.

Сведения об авторе

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

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

Рощупкина А.В.

ВОЗМОЖНОСТЬ ИСПОЛЬЗОВАНИЯ КРИПТОВАЛЮТЫ В ОТМЫВАНИИ ДЕНЕГ

В статье рассматривается проблема регулирования криптовалюты в аспекте отмывания денег. В частности, производится оценка возможности регулирования субъектов, участвующих в проведении транзакций с участием криптовалюты. Также, описаны схемы, используемые различными странами, в целях контроля компаний, использующих в своей деятельности криптовалюты.

В настоящее время отношение к криптовалюте может быть разным: от полного отрицания ее потенциала и преимуществ до всепоглощающего признания ее как будущего способа освобождения от финансового государственного контроля. Мы не поддерживаем ни одну из радикальных точек зрения относительно криптовалют, рассматривая их как инструмент, у которого есть свои преимущества и недостатки. Однако правоохранительные органы по всему миру выявляют использование криптовалют для совершения различных видов преступлений, в основном связанных с экономической и финансовой сферами, в частности, с отмыванием денег. Вышеупомянутое беспокойство вызывает необходимость глубокого исследования путей и средств использования криптовалют в процессе отмывания денег, что поможет эффективно и своевременно раскрывать данный вид преступности.

Виды виртуальной валюты: закрытая, виртуальные валюты с однонаправленным потоком и виртуальные валюты с двунаправленным потоком.

Фактически, закрытая виртуальная валюта не связана с реальным сектором экономики. Он предназначен для оплаты виртуальных

товаров или услуг, например, виртуальных игр, и не может быть использован вне виртуального сообщества. Все неконвертируемые виртуальные валюты централизованы: согласно определению, они эмитируются центральным администратором, который контролирует систему, устанавливает правила использования виртуальной валюты, ведет централизованный реестр платежей и имеет право изымать валюту из обращения.

Виртуальная валюта с однонаправленным оборотом. Такую валюту можно приобрести по специально установленному курсу, используя «реальную» валюту, однако невозможно обменять ее обратно по тому же курсу. Ее основное назначение – оплата виртуальных товаров и услуг, тем не менее, некоторые из них позволяют оплачивать реальные товары и услуги.

Виртуальные валюты с двунаправленным потоком. Такую валюту можно приобрести по определенному обменному курсу, другими словами, конвертировать ее. Основной целью этого является оплата реальных и виртуальных товаров и услуг. В качестве примера «конвертируемой валюты» можно привести криптовалюту.

В настоящее время самой популярной криптовалютой, которая используется в двунаправленном потоке, является биткоин. Биткоин – это децентрализованная платежная сеть P2P (от человека к человеку), которая обслуживает своих пользователей без центральных органов и агентов. С точки зрения пользователей, биткоин является аналогом наличных денег, но только для Интернета.

Блокчейн автоматически предоставляет одной стороне информацию о том, что другая сторона договора на законных основаниях оплатила товары или услуги. В вышеупомянутой транзакции нет третьей стороны. Система буквально контролируется всеми участниками. Любой человек, участвующий в торговле криптовалютами, имеет такую же возможность контролировать движение криптовалюты. Все подтвержденные транзакции включаются в блокчейн. Транзакция представляет собой перевод средств между биткойн-кошельками, которые включены в блокчейн.

Следует отметить, что правительства разных государств мира придерживаются разного мнения о легализации биткоина внутри своих стран. Например, новый закон, вступивший в силу в Японии, позволяет использовать биткоин в качестве законного платежного средства. Что касается России, то с 1 января 2021 г. вступил в силу Федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте». Документ регулирует отношения в части выпуска, обращения и учета виртуального платежного инструмента, а также деятельность операторов обмена.

Исходя из указанных в Федеральном законе определений, следует разделить два новых понятия.

Цифровые финансовые активы (далее – ЦФА), по сути, представляют собой электронные ценные бумаги, выпущенные по технологии блокчейн.

С этим инструментом можно совершать следующие действия:

1. Проводить операции по покупке и продаже.
2. Обменивать актив.
3. Использовать для залога.

Цифровая валюта – это виртуальные монеты, представленные электронным кодом. Их применяют в качестве платежа, инвестиций или сбережений. Это определение подходит для любых криптоактивов, включая Bitcoin. Виртуальные монеты приравниваются к имуществу. Несмотря на то, что согласно закону, цифровая валюта может использоваться как инструмент расчета, введен запрет биткоина в РФ для оплаты товаров или услуг. Также документ регулирует рекламу. Организациям запрещено упоминать возможность оплаты криптовалютой в объявлениях и маркетинговых кампаниях.

Следует отметить, что неоднозначный подход к криптовалюте в разных странах мира создает дополнительные проблемы для определения правового статуса криптовалюты.

В качестве примера использования криптовалюты для преступной деятельности, можно привести успешное функционирование подпольного веб-сайта «Silk Road». Это был крупнейший вируальный рынок торговли наркотиками. Все транзакции через этот веб-сайт осуществлялись с помощью биткоина, а анонимность пользователям обеспечивалась благодаря функционированию в Даркнете, жизнеспособность которого обеспечивалась с помощью программного обеспечения TOR. «Silk Road» функционировал как своеобразный биткоин-банк, где любой пользователь должен был иметь учетную запись для проведения транзакции через веб-сайт. Биткоин-адреса, которые были привязаны к учетной записи пользователя на веб-сайте, хранились на сервере, который контролировался «Silk Road». Для совершения покупки пользователь отправлял добытый биткоин на биткоин-адрес «Silk Road», который был привязан к его аккаунту на веб-сайте. После осуществления покупки валюта пользователя переводилась в систему условного депонирования на счете до полного завершения транзакции, затем биткоин клиента переводился со счета условного депонирования на биткоин-адрес продавца. Кроме того, для любого покупателя использовался «тумблер», который направлял все платежи с помощью сложной серии квазислучайных поддельных транзакций, что практически исключало возможность привязки платежа к любому

биткоину, который был отправлен с веб-сайта. В настоящее время вышеупомянутый сайт закрыт, а лица, которые им управляли, привлечены к уголовной ответственности.

Подводя итог, следует подчеркнуть, что современные технологии облегчают использование криптовалют, в частности биткоина, для отмывания денег. Раскрытие преступлений, связанных с криптовалютами, сопряжено с различными проблемами. Отсутствие четкого законодательного регулирования порождает вопросы безопасности и усложняет контроль за обращением криптовалют. Определенные особенности криптовалют, такие как быстрые и невозвратные транзакции, анонимность и сложные модели торговли, усложняют раскрытие преступлений, совершаемых с ее использованием.

Во-первых, стоит подчеркнуть, что достаточно сложно установить связь между реальным лицом и счетом виртуальной валюты, поскольку биткойн-адрес и протоколы не требуют идентификации клиента; во-вторых, преступники могут создавать неограниченный объем счета, что объективно делает невозможным контроль всех транзакций; в-третьих, они используют инструменты, которые блокируют возможность отследить определенную активность (анонимайзеры и т.д.).

Таким образом, биткоин позволяет осуществлять различные схемы отмывания денег, которые практически блокируют возможность идентификации преступников. Эта особенность ставит перед правоохранительными органами новые задачи по поиску новых форм и методов расследования случаев отмывания денег. Более того, вышеупомянутые характеристики криптовалюты подталкивают законодателей всего мира к модернизации законодательной системы для борьбы с преступностью в данной сфере.

Сведения об авторе

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

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

302027, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

Ключевые слова: криптовалюта, отмывание денег, цифровая валюта, раскрытие преступлений.

Саркисян Г.Г.

АЛГОРИТМ ВЫЯВЛЕНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (КИБЕРПРЕСТУПЛЕНИЙ)

В статье рассматриваются современные подходы к раскрытию киберпреступлений с использованием алгоритмических методов и технологий. Анализируются преимущества применения алгоритмов машинного обучения, искусственного интеллекта и методов анализа больших данных в оперативно-аналитической деятельности правоохранительных органов. Автор делает вывод о высокой эффективности алгоритмических инструментов, подчеркивая их значимость в противодействии киберпреступности и повышении уровня цифровой безопасности.

Современное развитие информационно-коммуникационных технологий привело к возникновению новых форм преступной деятельности, которые представляют собой серьезную угрозу для безопасности общества. Преступления, совершаемые с использованием ИКТ, охватывают широкий спектр правонарушений – от кражи персональных данных и кибермошенничества до распространения вредоносного программного обеспечения и взлома критически важных информационных систем. Эти правонарушения отличаются высокой степенью латентности и сложностью раскрытия, так как злоумышленники активно применяют средства анонимизации и скрытия следов, такие как виртуальные частные сети (VPN), прокси-серверы и сети Tor.

Для успешного противодействия преступлениям, совершенным с использованием информационно-коммуникационных технологий, правоохранительные органы вынуждены адаптироваться к постоянно меняющимся цифровым условиям. Важным элементом такой адаптации становится разработка и внедрение алгоритмов и методик, которые позволяют эффективно вести расследования и раскрывать правонарушения, учитывая технические особенности преступлений в виртуальной среде [1]. Применение алгоритмов и технологических решений в процессе расследования обеспечивает возможность систематизации и автоматизации ключевых этапов работы, сокращает временные затраты и минимизирует человеческий фактор, что особенно актуально при анализе больших объемов данных.

С учетом данных реалий задача правоохранительных органов по раскрытию преступлений в цифровой среде становится сложной и

требует использования новых методологических подходов [2; 3]. Традиционные методы выявления и раскрытия преступлений зачастую оказываются недостаточно эффективными при работе с киберпреступлениями, что обуславливает необходимость применения специализированных цифровых технологий, таких как аналитические системы больших данных, методы машинного обучения и искусственного интеллекта, а также инструменты открытой разведки (OSINT)[1]. Эти методы позволяют оперативным подразделениям органов внутренних дел Российской Федерации не только собирать и анализировать огромные объемы информации, но и выявлять скрытые взаимосвязи между преступными деяниями и лицами, причастными к ним.

Целью данной статьи является исследование и описание наиболее универсальных подходов и технологий, применяемых для раскрытия преступлений, совершенных с использованием ИКТ, а также анализ их эффективности в условиях цифровой трансформации общества. Такие решения, как правило, наиболее эффективны и удобны в использовании в виде конкретных алгоритмов действий оперативных сотрудников, позволяющих пошагово организовать и осуществить работу по выявлению и раскрытию киберпреступлений.

Разработка алгоритмов для выявления преступной активности лиц и раскрытия киберпреступлений в сети требует интеграции знаний в области кибербезопасности, анализа данных и цифровой оперативно-разыскной деятельности. Алгоритмы позволяют выявлять сведения и цифровые следы, оставляемые злоумышленниками, отслеживать взаимодействия пользователей с подозрительными ресурсами, а также проводить углубленный анализ сетевой активности. Для качественного анализа этих данных применяются технологии предиктивной аналитики, которые помогают выявить скрытые связи между отдельными действиями и паттерны поведения злоумышленников. Включение моделей предиктивной аналитики и алгоритмов машинного обучения в процессы расследования значительно расширяет возможности правоохранительных органов в сборе и интерпретации информации.

В результате анализа теории и имеющейся на сегодняшний день практики предлагаем рассмотреть наиболее универсальный алгоритм выявления и раскрытия преступлений, совершаемых с использованием ИКТ, включающий в себя методики деанонимизации подозреваемых лиц, алгоритмы анализа цифровых следов, особенности применения открытой разведки (OSINT), техники корреляционного анализа для выявления связей между сетевой активностью и действиями подозреваемых лиц, а также инструменты для работы с большими объемами данных.

Алгоритм выявления и раскрытия киберпреступлений:

1. Получение и оценка информации о преступлении:

– оценка исходных данных: уголовно-правовая оценка и характеристика преступления;

– работа с источником поступления информации: сообщение потерпевшего, анонимные источники или обнаружение признаков состава преступления в рамках регулярного мониторинга сети;

– изучение особенностей и признаков, совершенного преступления, сбор исходной информации о преступлении.

2. Сбор и анализ цифровых следов:

– выявление и фиксация информации, которая в последующем может быть передана в следственные органы и использована в качестве доказательств (логи, скриншоты, сохраненные веб-страницы, электронные письма и т.п.);

– сбор информации о методах и технологиях, которые были использованы для совершения преступления (IP-адреса, VPN, TOR и т.п.), а также ресурсах и платформах, на которых действует злоумышленник.

3. Идентификация следов:

– сбор и оценка сведений с помощью инструментов OSINT (например, поиск по социальным сетям, мониторинг общедоступных баз данных);

– установление местоположения (географического положения) злоумышленников, в том числе по результатам анализа по IP-адресов и используемых провайдеров;

– получение другой оперативно значимой информации, которая может обеспечить полноту и достоверность выдвигаемых оперативных версий.

4. Выдвижение гипотез и составление плана:

– выдвижение версий и гипотез, подлежащих проверке, в том числе посредством сопоставления фактов;

– составление плана проведения оперативно-разыскных мероприятий с учетом вариативности полученных или отсутствующих результатов.

5. Использование аналитических инструментов:

На данном этапе вариативность применяемых технологий зависит от имеющихся возможностей и инструментов. На данном этапе могут быть применены, например:

– системы распознавания лиц и голоса (при наличии данных) для идентификации подозреваемых;

– примените программного обеспечения для визуализации схем связей с последующим их анализом;

– средства анализа больших данных, машинного обучения или искусственного интеллекта для прогнозирования действий злоумышленника [4].

6. Взаимодействие с другими органами и организациями:

– получение информации в других подразделений органов внутренних дел и иных государственных органов, в том числе уполномоченных на осуществление оперативно-разыскной деятельности;

– получение информации по результатам взаимодействия с провайдерами интернет-услуг, хостинговыми компаниями, владельцами ресурсов и платформ, которые могут быть связаны с преступлением.

7. Документирование результатов оперативно-разыскной деятельности:

– систематизация всех данных и доказательств для последующего оформления материала с учетом требований работы со сведениями, составляющими государственную тайну;

– оформление материалов с результатами проведенных оперативно-разыскных мероприятий (в том числе графические материалы, схемы связей и т.п.);

– направление в установленном порядке материалов в органы предварительного расследования для принятия процессуального решения (например, о возбуждении уголовного дела).

Важно отметить, что данный алгоритм представляет собой универсальный пошаговый механизм, а работа по конкретному преступлению или поручению может выходить за рамки данного алгоритма или включать только ряд предложенных действий.

Применение алгоритмов в раскрытии киберпреступлений является эффективным инструментом борьбы с современными угрозами в цифровом пространстве [5]. Аналитические методы, такие как машинное обучение, искусственный интеллект и алгоритмы обработки данных, позволяют оперативно выявлять подозрительные действия, анализировать большие массивы информации и предсказывать потенциальные угрозы. Такие технологии улучшают точность и скорость оперативно-разыскной деятельности, обеспечивая более высокий уровень защиты от киберпреступников. Современные алгоритмические подходы становятся неотъемлемой частью стратегий правоохранительных органов, направленных на повышение эффективности работы по выявлению и раскрытию преступлений в сфере ИКТ.

---

1. Саркисян Г.Г. Современное состояние и проблемы информационно-аналитического обеспечения оперативно-розыскной деятельности // Юристъ-Правоведъ. 2019. № 4 (91). С. 214–218.

2. Павличенко Н.В., Тамбовцев А.И. Будущее профессии оперуполномоченный – BigData и аналитика // Труды Академии управления МВД России. 2020. № 2 (54). С. 62–68.

3. Жданов Ю.Н., Овчинский В.С. Полиция будущего. М., 2018. С. 42.

4. Овчинский С.С. К вопросу о прогнозировании индивидуального преступного поведения // Научная информация по вопросам борьбы с преступностью. М., 1972. № 30. С. 74–84.

5. Основы кибербезопасности: учебник / Г.Г. Саркисян, А.В. Бецков, Б.А. Торопов, В.А. Апульцин [и др.]. М.: Академия управления МВД России, 2023. 108 с.

Сведения об авторе

Саркисян Гор Георгиевич. Кандидат юридических наук. Профессор кафедры организации оперативно-разыскной деятельности.

Академия управления МВД России.

125171, Российская Федерация, г. Москва, ул. Зои и Александра Космодемьянских, д. 8.

Ключевые слова: оперативно-разыскная деятельность, оперативно-аналитическая деятельность, органы внутренних дел, органы, уполномоченные на осуществление оперативно-разыскной деятельности, технологии предиктивной аналитики, киберпреступления, информационно-коммуникационные технологии.

Смирнов И.М.

«СКАММИНГ» КАК НОВЫЙ ВИД СОВРЕМЕННОГО ИНТЕРНЕТ-МОШЕННИЧЕСТВА

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]. Руковод-

ствуясь приведенным подходом, попытаемся подробно разобрать в качестве типичного примера стандартную схему шантажа, реализуемого при помощи сети интернет, в котором проанализируем 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 вы-

полненных 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 покидать 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 значительно больше. Когда человек набирается опыта, он делат это 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 / пер. с китайского и комментарии Ральфа Д. Сойера, 1993; пер. с английского Р.В. Котенко, 1997, 2001. Издательская группа «Евразия», 2001. 448 с.

2. Уголовно-процессуальная деятельность органов дознания системы МВД России / К.В. Муравьев, А.В. Писарев, И.С. Смирнова, С.В. Супрун. 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, перераб. и доп. М.: ЮРАЙТ, 2010. 606 с.

4. Зарабатываем на шантаже [подробный мануал]. UMBRELLA [Электронный ресурс]. URL: https://telegra.ph/Zarabatyvaem-na-shantazhepodrobnyj-manual-10-21.

Сведения 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, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

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

Сущенко С.А., Мунх-Учрал Н.Э.

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В МОНГОЛИИ

В настоящей статье рассмотрены некоторые вопросы оперативно-разыскной деятельности Монголии. Раскрыты основные особенности законодательного регулирования оперативно-разыскной деятельности, а также виды, процедура санкционирования, порядок проведения оперативно-разыскных мероприятий и использования их результатов в уголовно-процессуальном доказывании.

Становление и развитие оперативно-разыскной деятельности Монголии тесно связано с российской школой оперативно-разыскной деятельности, поскольку многие монгольские ученые являлись выходцами из российской научной школы [2]. Оперативно-разыскное законодательство Монголии основывается на схожих с российскими правилами негласной деятельности по противодействию преступности, где соблюдение и уважение прав и свобод человека и гражданина являются основополагающим принципом. Однако оно имеет определенную специфику, обусловленную демографическими, территориальными, экономическими и другими особенностями монгольского государства [4].

Правовую основу ОРД Монголии составляют законы и нормативные акты, регламентирующие деятельность органов, осуществляющих оперативно-разыскную деятельность: Конституция Монголии 1992 г., УПК Монголии 1992 г., Закон «О национальной безопасности Монголии» 2001 г., Закон «О Полиции Монголии» 1993 г., Закон «Об оперативно-разыскной деятельности» 1998 г., Закон «Об органе разведки», Закон «О государственной тайне Монголии» и иные нормативные акты, предоставляющие полномочия органам, осуществляющим ОРД, полномочия производить действия и принимать решения, в целях защиты прав и законных интересов граждан.

В соответствии со ст. 2 Закона Монголии «Об оперативно-разыскной деятельности» под оперативно-разыскной деятельностью понимаются такие действия как поиск, сбор и проверка сведений, ин-

формации и доказательств, осуществляемых уполномоченными государственными органами с использованием обычных, специальных и негласных методов и средств в целях защиты национальной безопасности, прав и свобод человека от преступных посягательств.

В настоящее время в Монголии правом осуществлять оперативно-разыскную деятельность наделены Главное разведывательное управление, Служба исполнения наказания, Управление по борьбе с коррупцией и Национальное полицейское агентство Министерства юстиции и внутренних дел.

Криминальная полиция Национального полицейского агентства Монголии является основным подразделением Министерства юстиции и внутренних дел, осуществляющим оперативно-разыскную деятельность. В соответствии со ст. 9.1.3 Закона Монголии «Об оперативно-разыскной деятельности Монголии» полиция должна выявлять, пресекать и идентифицировать лиц, виновных в совершении конкретного преступления, совершенного любыми скрытыми способами, обеспечивать общественную безопасность, безопасность судов и магистратов, обеспечивать безопасность свидетелей, потерпевших и их иждивенцев, предотвращение нападений, а также розыск пропавших без вести или умерших лиц, скрывающихся от правосудия подозреваемых, обвиняемых, подсудимых, осужденных и других лиц, назначенных прокурором или судом, поиск наркотических и токсичных веществ, памятников истории и культуры и других ценностей. Кроме того, полиция занимается поиском утраченного огнестрельного оружия, боеприпасов и других опасных предметов.

В настоящее время в состав криминальной полиции Монголии входят следующие оперативные подразделения:

- уголовный розыск,
- подразделение организационно-аналитического обеспечения оперативно-разыскной деятельности;
- подразделение по борьбе с преступлениями в сфере экономики;
- подразделение по борьбе с киберпреступностью;
- подразделение по борьбе с организованной преступности и торговле людьми;
- подразделение по борьбе с преступлениями против общественной безопасности;
- подразделение по борьбе с тяжкими и особо тяжкими преступлениями;
- подразделение по борьбе с хищениями.

Закон Монголии «Об оперативно-разыскной деятельности» не содержит определения понятия и перечня оперативно-разыскных мероприятий. В соответствии с Законом Монголии «О государственной

тайне» сведения о силах, средствах, методах и источниках информации оперативно-разыскной деятельности, а также о лицах, штатных сотрудниках и тактике проведения оперативно-разыскных мероприятий относятся к сведениям, составляющим государственную тайну. Положения, закрепляющие виды, а также тактику и методы проведения оперативно-разыскных мероприятий, содержатся в Инструкции «Об организации и тактике ОРД полиции Монголии», утвержденной приказом начальника Главного управления полиции Монголии и инструкции службы криминальной полиции. В Законе Монголии «Об оперативно-разыскной деятельности» и в комментарии к УПК Монголии указывается на то, что на стадии дознания и следствия проведение оперативно-разыскных мероприятий, таких как прослушивание телефонных переговоров; контроль почтовых отправлений и телеграфных сообщений; досмотр жилых помещений, зданий, сооружений, местности; досмотр транспортных средств, их грузов и вещей, а также применение специальных технических средств и проведение наблюдения осуществляется с разрешения специально на то уполномоченного прокурора. В случаях, не терпящих отлагательства, данные мероприятия могут быть проведены на основании мотивированного постановления руководителя органа, осуществляющего ОРД с обязательным получением разрешения прокурора в течение 24 часов.

Необходимо отметить, что в последние годы в Монголии правоохранительными органами при проведении опроса начали активно проводиться психофизиологические исследования с применением полиграфа [1]. Правовая регламентация использования результатов полиграфа при расследовании и раскрытии преступлений, содержится в нормах отраслевого законодательства, в частности, в Законе Монголии «О разведывательных органах» (2006) и Законе «О полицейской службе» (в новой редакции 2017 г.).

Основаниями для проведения оперативно-разыскных мероприятий являются:

- невозможность проверить обычным способом достоверность сведений о тайно совершенном или подготавливаемом преступлении;

- лицо, совершившее преступление, не может быть установлено иными методами и средствами;

- по поручению суда, прокурора и следователя провести полную проверку доказательств по уголовному делу;

- на основании обращения гражданина или организации об освобождении заложника или розыске пропавшего без вести лица либо на основании имеющихся сведений;

- на основании запроса иностранного государства или международной организации, подписавшей с Монголией соглашение о правовой помощи по уголовным делам.

Согласно ст. 67 УПК Монголии материалы по уголовному делу, которые были получены при осуществлении оперативно-разыскной деятельности на законном основании, условиях и порядке, могут быть использованы и оценены в качестве доказательства [3]. Также в соответствии с ч. 3 ст. 79 УПК Монголии по уголовному делу фактические данные, полученные при осуществлении оперативно-разыскной деятельности, могут быть оценены в качестве доказательства при условии, что они были проведены с разрешения прокурора и в соответствии с нормами закона. При этом источник получения таких данных должен быть засекреченным. Таким образом, в Монголии законодательно закреплена возможность использования результатов ОРД в уголовном процессе в качестве доказательств. Однако, по мнению монгольских ученых, в Монголии отсутствует должная правовая основа, необходимая для использования результатов оперативно-разыскной деятельности в уголовно-процессуальном доказывании, что приводит к произвольному толкованию правоприменителями норм законодательства [5].

Таким образом, в связи с постоянно происходящим процессом развития страны, изменением характера и структуры преступности существует объективная необходимость совершенствования действующего оперативно-разыскного и уголовно-процессуального законодательства Монголии.

---

1. Баяндорж Цолмон. Практика использования полиграфа в Монголии: проблемные аспекты и пути их решения // Российский девиантологический журнал. 2022. № 2 (4). С. 438–442.

2. Жалинский А.Э., Мяханова А.Н. Сравнительно-правовое исследование УПК Монголии и УПК РФ // Вестник Бурятского госуниверситета. 2011. № 2. С. 255–259.

3. Козловский П.В., Рэнцэндорж Ганболд. Порядок прекращения уголовного дела (уголовного преследования) на реабилитирующих основаниях в Российской Федерации и Монголии // Сибирское юридическое обозрение. 2019. № 16 (3). С. 364–368.

4. Нарангэрэл С. Правовая система Монголии. Улан-Батор; М., 2004. 387 с.

5. Оюунчимэг Тамжидийн. К вопросу об использовании результатов ОРД в уголовном процессе Монголии // Известия Российского государственного педагогического университета им. А.И. Герцена. 2008. № 2. С. 263–267.

Сведения об авторах

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

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

302027, Российская Федерация, г. Орёл, ул. Игнатова, д. 2.

Мунх-Учрал Номин-Эрдэнэ. Слушатель специального курса по подготовке кадров для зарубежных стран.

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

302027, Российская Федерация, г. Орёл, ул. Игнатова, д. 2.

Ключевые слова: оперативно-разыскная деятельность, использование результатов оперативно-разыскной деятельности, сравнительное правоведение.

Тишков С.А.

НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ КРИМИНАЛИСТИЧЕСКИХ УЧЕТОВ В МОНГОЛИИ

В статье рассмотрены некоторые аспекты организации криминалистических учетов Монголии, а также проведен сравнительно-правовой анализ использования отдельных элементов системы криминалистической регистрации в Монголии и Российской Федерации.

Для раскрытия и расследования преступления важное значение имеет использование систем и баз криминалистической информации, аккумулирующих данные о лицах, совершавших преступления, способах преступной деятельности, предметах, которые были использованы при совершении преступления, а также о похищенном имуществе.

Именно для такой цели в правоохранительных органах различных государств внедряется и используется система криминалистической регистрации, объединяющая различные учеты, содержащие информацию о разных группах однородных объектов.

Основными целями криминалистической регистрации являются предупреждение, раскрытие и расследование преступлений, розыск

лиц и похищенного имущества, идентификация лиц и неопознанных трупов.

История и развитие системы криминалистических учетов Монголии начинается в 1928 г. После установления народной власти приказом начальника Управления внутренней охраны Монголии впервые была утверждена должность фотографа в секретном отделе расшифровки. Именно в этом подразделении начали вести учеты по уголовным делам.

С 1940 г. в структуре милиции Монгольской народной республики, появилась новая должность эксперта, функциями которого являлись фотографирование преступников, изъятие следов рук. Считаем важным отметить, что с этого времени эксперты ведут дактилоскопический учет.

12 января 1944 г. была создана первая экспертно-техническая служба, заложившая фундамент формирования системы информационного обеспечения судебно-экспертной деятельности в Монголии [3, с. 30].

В 1950 г. был создан специальный отдел науки и техники при Главном управлении милиции при Министерства внутренних дел с целью создания криминалистических лаборатории, разработки методических материалов и инструкций для сотрудников милиции по ведению различных видов учета (например, учет похищенного имущества, осужденных лиц, гильз и пуль от огнестрельного оружия, дактилоскопическая картотека).

Монголия является унитарным государством, административное-территориальное деление которой включает 21 аймак, каждый из которых подразделяется на сомоны (районы). В соответствии с этим делением гвозможно выделить два уровня организации криминалистических учетов – национальный (федеральный) и областной (на уровне аймака), т.к. на местном уровне (на уровне сомона) учеты не ведутся.

Считаем возможным отметить, что в этом проявляется отличие от Российской Федерации, в которой функционируют три уровня учетов (федеральный, региональный и местный) [1, с. 274].

В настоящее время в соответствии со ст 22.1 Закона Монголии о судебной экспертизе криминалистический учет включает в себя централизованную и специализированную базы данных.

Централизованная база данных Монголии содержит учеты: дактилоскопический, огнестрельного оружия, пуль и гильз, учет данных ДНК биологических объектов, а также учет данных экологических экспертизов. Она ведется в подразделениях Министерства юстиции и внутренних дел областного уровня (на уровне аймака).

К специализированной базе данных относятся учеты поддельных денежных билетов, бланков ценных бумаг, следов обуви, поддельных бланков документов, следов транспортных средств, а также учет черепов неопознанных трупов, лиц, пропавших без вести, неопознанных трупов и иные учеты в области судебно-медицинской экспертизы.

Специализированная база данных ведется на национальном уровне в экспертно-криминалистическом лаборатории при Главном управлении судебной экспертизы Монголии и охватывает регистрацией всю территорию Монголии.

В 1972 г. по приказу начальника Главного управления милиции создали систему картотеки следов рук, оставленных и изъятых на месте преступлений [2, с. 26]. С 1990 г. региональная дактилоскопическая картотека ведется во всех аймаках.

В дальнейшем в целях формирования единой государственной сети дактилоскопических учетов, объединяющих все аймаки, в 2008 г. была создана сеть станций автоматизированной дактилоскопической идентификационной системы (АДИС) «Папилон» и внедрили технологию безкраского дактилоскопиравания с использованием «живого сканера» [2, с. 25].

Таким образом построение системы криминалистической регистрации в Монголии предусматривает два уровня учетов, что отличается от трехуровневой системы в Российской Федерации. Вместе с тем, российской информационные технологии активно применяются при создании централизованного дактилоскопического учета Монголии, что может послужить для дальнейшего развития сотрудничесва правоохранительных органов наших государств.

---

1. Криминалистика: учебник / под ред. В.Д. Зеленского, Г.М. Меретукова. СПб.: Юридический центр-Пресс, 2015. 704 с.

2. Ундрах З. Образование и развитие судебно-экспертных учреждений Монголии // Эксперт-криминалист. 2010. № 1. С. 26–30.

3. Цолмон Б. Сравнительный анализ законодательства России и Монголии, регламентирующего информационное обеспечение судебно-экспертной деятельности // Вестник Московского университета МВД России. 2014. № 6. С. 29–32.

Сведения об авторе

Тишков Сергей Александрович. Кандидат политических наук, доцент. Заместитель начальника кафедры криминалистики и предварительного расследования в ОВД.

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

***Ключевые слова*:** криминалистическая регистрация, «Папилон», дактилоскопирование.

Чаплыгина В.Н.

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

Автором 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 г., 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-разыскных 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 немаловажным будет являться производство обыска или выемки по месту жительства вовлекателя 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 вовлекателя 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 окружающих. 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 постановление 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 вовлечении. 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 освидетельствование 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 преступле-

ния. 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 соответствие 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 совершен-

нолетних 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 действий 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 это 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 осведомлён 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 явля-

ется 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: 02.10.2024).

2. Юркова М.А., Чаплыгина В.Н. Особенности и проблемы наделения 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 судопроиз-

водства: практические проблемы реализации требований закона // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2020. № 2 (83). С. 39–46.

10. Уголовно-процессуальная деятельность органов дознания системы МВД России / К.В. Муравьев, А.В. Писарев, И.С. Смирнова, С.В. Супрун. 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, перераб. и доп. М.: ЮРАЙТ, 2010. 606 с.

Сведения об авторе

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, Российская Федерация, г. Орел, ул. Игнатова, д. 2.

Ключевые слова: следственные действия, расследование преступлений, несовершеннолетний.

Сборник научных статей

АКТУАЛЬНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Подписано в печать 28.11.2024. Формат 60×90 1/16.
Усл. печ. л. – 7. Тираж 20 экз. Заказ № 936.

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