Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Республиканская
научно-практическая заочная конференция
(с международным участием)
(Минск, 2 июня 2025 г.)

Тезисы докладов

Минск
Академия МВД
2025

УДК 343.985.8
ББК 67.408
А43

ISBN 978-985-576-482-4

УДК 341.225.5

Анянова Е.С.

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ СУДОХОДСТВА

В отечественном судоходстве обороты такого масштаба, который требует обеспечения кибербезопасности и автоматизации труда, пока недосягаемы, а вот в зарубежной практике встречаются интересные примеры работы с большими объемами грузооборота, приведшие к киберпреступлениям.

Кибербезопасность – это концепция безопасности, используемая для защиты киберсреды, организации и пользователя.

С 2017 г. кибербезопасности морской отрасли уделяется особое внимание на международном уровне с помощью таких документов, как руководства и рекомендации. Однако обязательных требований не существует.

За последние годы увеличилось количество сообщений о кибернападениях на морскую отрасль.

Например, нападение NotPetya на компанию Maersk в 2017 г. привело к убыткам в размере около 300 млн долларов.

В 2022 г. компания Sea-Invest, один из крупнейших бельгийских портовых терминалов, прекратила все операции из-за хакерской атаки.

В 2022 г. сингапурская судостроительная компания Sembcorp Marine подверглась атаке неавторизованного пользователя, который получил доступ к ИТ-сети через стороннее программное обеспечение. В декабре 2022 г. атаке подверглась ИТ-система сингапурской морской компании Voyager Worldwide.

Веб-сайт и внутренняя компьютерная система порта Лиссабона были нарушены в декабре 2022 г. и не работали в течение нескольких дней после кибератаки.

Норвежское классификационное общество судоходства Det Norske Veritas (DNV) подверглось атаке вымогателей в 2023 г. Международная морская организация (ИМО) также подвергалась атакам в 2020 и 2023 гг. Порт Лос-Анджелеса постоянно подвергается атакам программы вымогателя, вредоносных программ и фишинговых атак.

Документальная часть международного права, посвященная кибербезопасности в судоходстве, содержит в себе лишь отдельные документы: Руководящие принципы ИМО по управлению киберрисками на море 2017 г.; международные или отраслевые стандарты и передовую практику (например, Система кибербезопасности 2.0 Национального института стандартов и технологий, стандарт ISO/IEC 27001 для систем управления

информационной безопасностью); Резолюция MSC.428(98), принятая Комитетом по безопасности на море 16 июня 2017 г.; Международный кодекс по охране судов и портовых средств (далее – Кодекс ОСПС) и др.

Усиление мер кибербезопасности предполагает управление киберрисками. Должна обеспечиваться защита от несанкционированного доступа.

Предлагается разработать новые руководящие принципы кибербезопасности для морского пространства при участии ИМО. Иногда предлагаются поправки к Кодексу ОСПС, которые усовершенствуют меры по вопросам борьбы с киберпреступностью.

В целях содействия управлению кибербезопасностью было внесено предложение о назначении ответственного за кибербезопасность (CySO). Такая должность введена, например, в порту Роттердама и др.

В настоящее время морская индустрия становится все более уязвимой для киберугроз.

Для обеспечения киберустойчивости судов и портовых сооружений требуются дополнительные меры кибербезопасности.

УДК 343.985.8

А.В. Афанасенко, Б.В. Ковалик

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Развитие технологий в последние годы проявилось в широком распространении и совершенствовании беспилотных летательных аппаратов (БЛА), которые из специализированного решения для ограниченного круга задач превратились в универсальный инструмент, активно применяемый в различных сферах. Динамика мирового рынка БЛА, характеризующегося стабильным ростом, обусловлена высокой эффективностью, снижением себестоимости и повсеместной доступностью данного технического средства. Первоначально сформировавшись в военной отрасли, использование БЛА постепенно распространилось на гражданскую. Вместе с тем в деятельности силовых структур БЛА находят особенно значимое и перспективное применение благодаря своей мобильности, скрытности и способности оперативно передавать информацию.

Решение задач мониторинга оперативной обстановки, обеспечения общественной безопасности и противодействия отдельным видам

преступлений обусловливает необходимость внедрения современных технических средств в деятельность правоохранительных органов. Республика Беларусь, следуя глобальному вектору цифровизации, приняла меры правового регулирования эксплуатации БЛА. Указ Президента Республики Беларусь от 25 сентября 2023 г. № 297 установил порядок государственного учета и использования гражданских БЛА, предусматривая, что ввоз, хранение, производство и эксплуатация таких устройств допускаются организациями и индивидуальными предпринимателями при наличии соответствующего разрешения. Физическим лицам, напротив, установлено ограничение на данные действия. Дополнительно предусмотрено создание системы учета БЛА, что направлено на усиление контроля и предотвращение их неправомерного применения.

В практике Министерства внутренних дел Республики Беларусь БЛА уже используются при охране общественного порядка на массовых мероприятиях, фиксации правонарушений в сфере дорожного движения, а также в ходе поисково-спасательных мероприятий. Особое значение приобретает применение БЛА в рамках оперативно-розыскной деятельности (ОРД). Учитывая характер ОРД, БЛА становятся важным инструментом, позволяющим конфиденциально и оперативно получать необходимую информацию и принимать соответствующие решения.

Заимствование и адаптация данной технологии в ОРД не является новшеством, а представляет собой закономерный этап развития практики внедрения технических решений из смежных отраслей. ОРД традиционно характеризуется высокой восприимчивостью к инновациям, включая аудио- и видеозаписывающее оборудование, навигационные и информационные технологии, которые первоначально применялись в гражданских или военных сферах. Применение БЛА логично продолжает данный подход: адаптированные как средства негласного получения информации, они могут эффективно использоваться при решении задач ОРД.

Перспективность использования БЛА в ОРД подтверждается также с экономической точки зрения: при относительно невысоких затратах на эксплуатацию и обучение персонала, они обеспечивают охват значительных территорий, снижают риски для сотрудников и позволяют оперативно получать необходимую информацию.

Полагаем, что БЛА, как современное техническое средство, существенно расширяют потенциал реализации задач ОРД органов внутренних дел. Нормативное закрепление данных задач должно стать важным направлением развития правоохранительной системы. При этом в дальнейшем необходимо обеспечить не только расширение сфер примене-

ния БЛА, но и детальную регламентацию порядка эксплуатации в соответствии с действующим законодательством об ОРД, с учетом особенностей конкретных оперативно-розыскных мероприятий.

УДК 343

А.И. Басова, Р.В. Глубоковских

О ЗНАЧЕНИИ ВЗАИМОДЕЙСТВИЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И ОРГАНОВ УГОЛОВНО-ИСПОЛНИТЕЛЬНОЙ СИСТЕМЫ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ

С каждым годом преступность приобретает сложный формат. Возникает проблематика поиска путей раскрытия отдельных видов преступлений. Без полноценного использования всех сил и средств предстает невозможным решение задач по борьбе с преступностью. В связи с этим вопрос о взаимодействии между органами внутренних дел и органами уголовно-исполнительной системы для данной проблемы актуален как никогда.

В качестве рассмотрения взаимодействия оперативных подразделений ведомств особое положение занимает взаимодействие Федеральной службы исполнения наказаний (ФСИН) России и Министерства внутренних дел Российской Федерации (далее – МВД России). Стоит отметить, что раскрытие преступлений при взаимодействии данных ведомств становится более эффективным и результативным.

Одним из факторов положительного прогресса в деятельности по раскрытию преступлений является развитие взаимодействия оперативных подразделений ФСИН России, а также непосредственных руководителей с оперативными подразделениями МВД России и их руководителями.

Для раскрытия киберпреступлений, а именно телефонных мошенничеств, которые были совершены непосредственно в местах режима следственных изоляторов (СИЗО), эффективным представляется обмен информацией и передача различных форм и методик по раскрытию, а также взаимодействие сотрудников оперативных подразделений МВД России и ФСИН России.

Чаще всего в качестве взаимодействия подразумевают порядок связей следователя и органа дознания, регламентируемый нормативно-правовыми актами, который обеспечивает их взаимообеспечивающую деятельность.

Рассматривая данную проблематику, необходимо выделить следующие формы взаимодействия правоохранительных органов. К ним относятся: оперативный обмен информацией при раскрытии пенитенциарных преступлений; совместное планирование деятельности по пресечению, выявлению, расследованию и раскрытию преступления, совершенного лицом, отбывающим наказание в местах лишения свободы; оперативное обеспечение проведения следственных действий и оперативно-разыскных мероприятий по запросам ведомств.

Стоит отметить, что взаимодействие между подразделениями ведомств может осуществляться в процессе выявления, расследования и раскрытия определенных преступлений. Оно представляет собой совместное осуществление конкретных следственных действий, а также оперативно-разыскных мероприятий.

В качестве субъектов взаимодействия при раскрытии пенитенциарного преступления могут быть как отдельные сотрудники оперативных подразделений МВД России, так и сотрудники оперативных подразделений ФСИН России.

Полноценное раскрытие пенитенциарного преступления возможно лишь при согласованной и тесной связи между ведомствами. Поскольку сотрудники МВД России не обладают достаточной информацией и конкретных лицах и их связях в помещениях закрытого типа СИЗО.

Следует отметить, что сотрудники оперативных подразделений ФСИН России имеют огромный массив информации об осужденных, среде их нахождения, а также о лицах, занимающих высшее положение в иерархии их авторитетного круга, конфликтах между каждым членом группировки.

Данный аспект важно учитывать при организации раскрытия пенитенциарных преступлений, акцентируя внимание на те оперативные подразделения, которые располагают большим массивом информации о личностях и их связях. Тем самым это позволит эффективно и быстро раскрыть преступление.

В качестве главных форм и методов взаимодействия данных ведомств стоит отнести следующее: организационное обеспечение (инструктаж сотрудников МВД России конкретным оперативным сотрудником учреждения закрытого типа СИЗО, располагающим оперативно значимой информацией, а также его содействие в проведении оперативно-разыскных мероприятий; оперативно-информационное обеспечение деятельности оперативных сотрудников МВД России (возможность предоставления права на доступ к базе данных учреждения, ознакомление с учетами, справками и карточками).

При раскрытии пенитенциарного телефонного мошенничества сотрудниками территориальных органов МВД России при взаимодей-

ствии с оперативными сотрудниками ФСИН России должны использоваться все формы взаимодействия.

В зависимости от конкретного преступления субъектами избирается определенная форма взаимодействия, учитывая каждую особенность совершенного преступления.

Таким образом, взаимодействие ведомств ФСИН России и МВД России, а также их оперативных подразделений имеет очень важное значение для эффективной борьбы с преступностью. Поскольку совместная, упорядоченная, целенаправленная деятельность данных субъектов оперативно-розыскной деятельности позволяет объединить их усилия в борьбе с преступностью и достичь при этом наиболее эффективного результата.

УДК 343.8

А.В. Батюков

ОБЩАЯ ХАРАКТЕРИСТИКА И ПРОБЛЕМНЫЕ АСПЕКТЫ БЕЗВЕСТНОГО ИСЧЕЗНОВЕНИЯ ЛИЦ ДЛЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Ежегодно в Республике Беларусь пропадает без вести значительное количество граждан. Розыск пропавших граждан остается одним из наиболее приоритетных вопросов, вызывающих серьезную обеспокоенность в обществе. Бесспорно, суть решения проблемы исчезновения граждан также находится в социальных и экономических сферах жизни общества, однако не последнее место в разрешении данной проблемы играет эффективность выявления и раскрытия фактов совершенных преступлений в отношении исчезнувших лиц сотрудниками оперативных подразделений органов внутренних дел (ОВД).

В сложившейся практике под понятием «без вести пропавшее лицо» подразумевается лицо, о местонахождении которого нет достоверной информации, которое пропало неожиданно, при неизвестных обстоятельствах, без видимых причин. Ситуации, когда близкие не знают, где находится человек, бывают различными и не всегда носят криминальный характер. Лицо может быть задержано правоохранительными органами, иногда люди решают «начать новую жизнь» и уезжают, не сообщив родственникам о своих намерениях, несовершеннолетние сбегают в поисках приключений, пожилые люди и лица с различными психическими заболеваниями могут внезапно забыть о себе сведения и уехать в незнакомое место, в летний и осенний сезоны люди могут заблудиться

в лесах и др. Однако под безвестное исчезновение преступники могут замаскировать и умышленные убийства.

Установление обстоятельств безвестного исчезновения имеет большое значение в обеспечении эффективной охраны личности от преступных посягательств и является гарантией соблюдения конституционных прав и свобод граждан. Следовательно, розыск лиц, пропавших без вести, является приоритетной задачей правоохранительных органов.

По данным информационного центра Министерства внутренних дел Республики Беларусь, в последние годы в стране наблюдается снижение результативности розыска лиц, пропавших без вести. Так, в 2019–2024 гг. ежегодно в розыске в среднем находились свыше 2 000 лиц, пропавших без вести, включая лиц, вновь объявленных в розыск и продолжающих в нем оставаться с прошлых лет. В 2019 и 2020 гг. доля найденных лиц составила 75 %, в 2021 г. – 78 %, в 2022 г. – 75 %, в 2023 г. – 73 %, в 2024 г. –71 %. Несмотря на то что число ежегодно объявляемых в розыск лиц, пропавших без вести, а также сообщений и заявлений по данным фактам имеет тенденцию к уменьшению, общее число разыскиваемых лиц возрастает.

Значительный вклад в разработку теоретических основ рассматриваемой нами проблемы внесли Т.Н. Алешкина, В.М. Атмажитов, Р.С. Белкин, П.Е. Букейханов, Н.И. Вытовтова, В.К. Гавло, Д.А. Гринева, Л.Я. Драпкин, Ю.П. Дубягин, Е.Г. Килессо, Е.Ф. Коновалов, А.В. Котяжов, В.А. Лукашов, А.М. Ларин, А.С. Мальцев, Г.Н. Мудьюгина, В.О. Петросян, В.П. Цильвик.

Вместе с тем работы указанных выше ученых были выполнены в советский период, подготовлены на основе российского законодательства, не затрагивают вопросов раскрытия и выявления преступлений, совершенных в отношении лиц, пропавших без вести, и в настоящее время не отвечают потребностям современной практики, как следствие, не в полной мере позволяют использовать полученные результаты в целях эффективного розыска без вести пропавших лиц.

Это позволяет говорить о том, что вопросы розыскной деятельности, особенности выявления и раскрытия указанных фактов, другие аспекты данной проблемы требуют дополнительного исследования.

В Республике Беларусь диссертационных и монографических исследований, затрагивающих оперативно-розыскные аспекты розыска лиц, пропавших без вести, не проводилось. Среди отечественных ученых вопросы выявления и раскрытия преступлений, совершенных в отношении лиц, пропавших без вести, в своей диссертации рассматривал А.В. Саленик (1994 г.), предложивший примерный перечень проверочных действий сотрудников ОВД при поступлении сообщений о безвестных исчезновениях,

однако изменение законодательства, а также совершенствование информационных систем требуют пересмотра предложенного алгоритма.

Эффективность выявления подобных случаев во многом зависит от уровня и согласованности планируемых оперативно-розыскных мероприятий и процессуальных действий, которые должны согласовываться с тактическими целями и задачами, и предусматривать использование научно-технических средств и методов. В процессе розыска перед оперативными подразделениями ОВД стоит задача определения наличия либо отсутствия криминального характера исчезновения лица. Для решения этой задачи следует изучать обстоятельства, предшествующие исчезновению, саму ситуацию исчезновения как таковую, а также полную информацию о личности пропавшего (социальный статус, характер деятельности, психологические особенности и др.).

Таким образом, современное состояние розыска без вести пропавших лиц свидетельствует о том, что борьба с данным явлением должна рассматриваться как актуальная государственная задача, направленная на защиту прав и свобод граждан. Основная роль в установлении и розыске без вести пропавших лиц принадлежит оперативным подразделениям ОВД, однако в их работе сохраняется целый ряд неустраненных проблем. В частности, остаются нерешенными до настоящего времени вопросы соответствующей правовой регламентации розыска, проведения всего комплекса оперативно-розыскных мероприятий и целостная система их осуществления. Знание механизма совершения подобных убийств, способов его совершения и маскировки, мест сокрытия трупов, а также признаков, указывающих на совершаемое преступление в отношении лица, пропавшего без вести, будет содействовать повышению эффективности работы правоохранительных органов.

УДК 363.985.8

А.В. Башан, А.Н. Тукало

О РАЗРАБОТКЕ НОВОЙ РЕДАКЦИИ МОДЕЛЬНОГО ЗАКОНА «ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ» ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

С целью совершенствования и унификации оперативно-розыскного законодательства на территории государств – участников Содружества Независимых Государств (СНГ) на основании абзаца третьего п. 46

Устава Академии МВД Республики Беларусь от 25 июля 2022 г. № 190 и письма Генерального секретаря – руководителя Секретариата Совета Межпарламентской Ассамблеи государств – участников СНГ от 18 января 2024 г. № И-2024-0054/01-16 с целью подготовки проекта новой редакции модельного закона «Об оперативно-розыскной деятельности» была создана рабочая группа (А.В. Башан, А.Н. Тукало, А.О. Мартынов, О.Н. Шуляковский, П.А. Кайбелев).

Законопроект разработан с учетом современных тенденций в сфере оперативно-розыскной деятельности (ОРД), опыта правового регулирования общественных отношений в данной области государств – участников СНГ, практики применения действующего Закона Республики Беларусь «Об оперативно-розыскной деятельности» и направлен на совершенствование новой редакции модельного закона «Об оперативно-розыскной деятельности» государств – участников СНГ.

Новая редакция модельного закона состоит из 11 глав, включающих в себя 74 статьи. При его подготовке в адрес рабочей группы из компетентных органов государств – участников СНГ поступили замечания и предложения, ряд из которых были учтены частично, отдельные полностью нашли отражение в новой редакции данного закона.

В гл. 1, включающей общие положения, содержатся основные термины, используемые в законопроекте, и их определения, регламентируются задачи и принципы ОРД, закрепляются гарантии соблюдения прав, свобод и законных интересов граждан, прав и законных интересов организаций.

Законопроектом вводятся такие новые основные термины и их определения, как «внедренное (внедряемое) лицо», «дело оперативного учета», «лицо, оказывающее содействие на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность», «материалы оперативно-розыскной деятельности», «оперативно-розыскное мероприятие». Необходимость их введения обусловлена тем, что ранее они были регламентированы в нормативных правовых актах органов, осуществляющих ОРД, и имели различия в их трактовке.

Предлагается рассматривать определения оперативно-розыскных мероприятий (ОРМ) в отдельных статьях (ст. 21–34 Проекта), а не в ст. 1, как это указано в действующей редакции модельного закона «Об оперативно-розыскной деятельности» государств – участников СНГ.

В ст. 3 законопроекта на органы, осуществляющие ОРД, возлагаются дополнительные задачи (по установлению личности погибшего (умершего), граждан, которые не могут сообщить о себе сведения; установлению имущества, подлежащего аресту в уголовном процессе;

обеспечению безопасности участников уголовного процесса, лиц, оказывающих (оказывавших) содействие на конфиденциальной основе органам, осуществляющим ОРД, и других лиц в соответствии с национальным законодательством; сбору сведений о допуске отдельных лиц к государственным секретам и видам деятельности). Ст. 5–9 определяют и раскрывают содержание принципов ОРД (принципы законности, уважения и соблюдения прав и свобод и законных интересов граждан, прав и законных интересов организаций, а также конспирации, гласного и негласного проведения ОРМ).

Ст. 10, 11 определяют права и обязанности граждан и организаций в связи с осуществлением ОРД. Впервые регламентирован порядок привлечения к участию в ОРД в качестве специалиста гражданина, обладающего специальными знаниями в науке, технике, искусстве, ремесле и иных сферах деятельности.

В гл. 2 перечислены органы, осуществляющие ОРД, определены их обязанности и права, порядок взаимодействия.

В гл. 3 определен исчерпывающий перечень и содержание 14 ОРМ, основания и общие условия их проведения, порядок фиксации результатов ОРМ. В данной главе также определено понятие «дело оперативного учета», регламентированы основания для заведения, прекращения дел оперативного учета и сроки их ведения.

В ст. 18 приведен исчерпывающий перечень ОРМ, которые проводятся при осуществлении ОРД. Каждое ОРМ впервые регламентировано самостоятельной статьей, что значительно упрощает восприятие и способствует единообразному применению норм законопроекта (ст. 21–34).

В гл. 4 регламентировано проведение ОРМ в отдельных случаях (случаи, нетерпящие отлагательства; по заявлению гражданина при возникновении угрозы его жизни, здоровью; при сборе сведений и применении мер по обеспечению безопасности) и особенности проведения ОРМ в отношении отдельных категорий лиц.

В гл. 5 регламентированы сроки проведения ОРМ, порядок их исчисления и продления.

В гл. 6 установлены основания и порядок приостановления, возобновления и прекращения проведения ОРМ, проведения ОРМ повторно или более двух раз.

Гл. 7 содержит положения о защите сведений об ОРД; об использовании материалов ОРД, в том числе порядок их предоставления в орган уголовного преследования, суд или другой орган, осуществляющий ОРД.

В ст. 49, 50 детально определен порядок использования и предоставления материалов ОРД, который ранее регламентировался лишь нормативными правовыми актами органов, осуществляющих ОРД.

Гл. 8 включает в себя нормы, регламентирующие правовое положение граждан, оказывающих или оказывавших содействие на конфиденциальной основе органам, осуществляющим ОРД; обеспечение защиты таких лиц, в том числе правовой и социальной. Впервые законопроект дополнен нормами, предусматривающими меры безопасности, применяемые в отношении лиц, конфиденциально содействующих органам, осуществляющим ОРД; устанавливаются поводы, основания и порядок применения этих мер, а также их содержание.

Гл. 9 определяет финансовое и материально-техническое обеспечение ОРД. Гл. 10 регламентирует особенности контроля и прокурорского надзора за ОРД. Гл. 11 включает в себя заключительные положения. Она предусматривает внесение изменений и дополнений в национальное законодательство государств – участников СНГ, которые направлены на согласование их отдельных норм с положениями законопроекта.

При подготовке новой редакции модельного закона были учтены современные тенденции деятельности правоохранительных органов государств – участников СНГ по выявлению, предупреждению, пресечению и раскрытию преступлений, опыт применения национального законодательства, регламентирующего рассматриваемую сферу правоотношений, а также мнения ученых по правовой регламентации отдельных направлений совершенствования оперативно-розыскного законодательства. Окончательное рассмотрение и принятие новой редакции модельного закона государств – участников СНГ «Об оперативно-розыскной деятельности» запланировано на очередном заседании Совета Межпарламентской Ассамблеи государств – участников СНГ осенью 2025 г.

УДК 343.01

П.Л. Боровик

ОСОБЕННОСТИ КРИМИНАЛЬНОГО АНАЛИЗА КРИПТОВАЛЮТНЫХ ТРАНЗАКЦИЙ

Анализ национальной оперативно-следственной и судебной практики свидетельствует о возрастающей роли криптовалют (виртуальных активов, цифровых знаков, токенов, учет которых осуществляется децентрализованными платежными системами в автоматическом режиме)

в преступлениях, совершаемых на территории государств – участников Содружества Независимых Государств. Причины их популярности в криминальной среде обусловлены прежде всего техническими характеристиками таких активов, в числе которых высокая скорость выполнения и необратимость (неотзывность) транзакций, возможность дробления денежных единиц на минимальные доли (вплоть до одной стомиллионной части), относительная анонимность платежей и высокий уровень защиты персональных данных владельцев электронных кошельков. Применение криптовалют злоумышленниками, например, при покупке или продаже запрещенных товаров, контента или услуг, не только существенно снижает вероятность их задержания на месте преступления, но и серьезно затрудняет применение традиционных методов выявления и документирования противоправных действий сотрудниками правоохранительных органов.

В рамках проведенного исследования выявлены четыре основные области использования криптовалют в криминальной деятельности:

приобретение или продажа незаконных товаров, контента или услуг (оружие, наркотические вещества, торговля людьми, детская порнография и др.) в скрытом сегменте сети Интернет («Даркнет»);

легализация («отмывание») доходов, полученных преступным путем;

финансирование террористической и экстремистской деятельности;

хищение криптовалют с цифровых счетов, а также иные преступления против собственности с их использованием.

Отмеченная тенденция вовлечения цифровых активов в противоправную деятельность обусловливает необходимость адаптации правоохранительных органов к новым условиям и поиска эффективных методов противодействия преступлениям подобного рода.

В основе процесса раскрытия преступлений, совершаемых с использованием криптовалют, лежит анализ электронных журналов транзакций, полученных по официальным запросам правоохранительных органов от криптовалютных бирж. Эти журналы обычно представляют собой таблицы формата MS Excel, содержащие данные о депозитах (внесении средств) и выводах (снятии средств) подозреваемых лиц.

Одним из первичных методов анализа журналов транзакций выступает сопоставление временных меток транзакций с датами и временем известных преступлений. Например, если 10 марта 2024 г. было зафиксировано преступление, связанное с вымогательством посредством программы-вымогателя, а 11–14 марта на счет подозреваемого поступили значительные суммы криптовалюты (например, депозит 4207 USDT

от 14 марта 2024 г.), это может свидетельствовать о наличии причинно-следственной связи между криминальным событием и транзакциями подозреваемого.

Другой значимый метод криминального анализа заключается в изучении размеров переводимых сумм и типов используемых криптовалют. Например, мелкие суммы, такие как 0.000396994034900934 MATIC, могут использоваться преступниками в качестве тестовых транзакций для проверки безопасности или работоспособности канала перевода. Напротив, крупные депозиты (например, 69000 KAS или 24167 USDT) могут быть признаком получения значительных доходов от противоправной деятельности.

Отсутствие идентификаторов транзакций в некоторых операциях, особенно связанных с P2P-сервисами, также является важным аналитическим признаком. Например, если в записях журнала транзакций зафиксированы депозиты с указанием типа «P2PDeposit» и отсутствующим хэшем, это может свидетельствовать о попытке преступника минимизировать следы, избегая прямого взаимодействия с официальными криптовалютными кошельками и биржами. Подобная практика распространена при отмывании денежных средств и при проведении операций, связанных с финансированием запрещенных видов деятельности.

Ключевым этапом анализа криптовалютных операций является идентификация владельцев счетов путем использования процедуры Know Your Customer (KYC), предполагающей обязательную проверку персональных данных клиентов криптобирж. Сотрудникам правоохранительных органов могут быть предоставлены сведения о паспортных данных, водительских удостоверениях, адресах проживания, электронных почтах и номерах телефонов подозреваемых лиц. Если по запросу правоохранительных органов криптовалютная биржа предоставляет сведения о том, что подозреваемый (User_id «1234567») совершил транзакции, совпадающие по времени и размеру с доходами от незаконной продажи наркотиков в сети «Даркнет», это позволяет однозначно идентифицировать его личность и собрать доказательную базу для судебного преследования.

Эффективным методом криминального анализа журнала транзакций является отслеживание пути криптовалютных средств после их вывода, осуществляемое с помощью уникальных идентификаторов транзакций. Если в журнале вывода средств указывается хэш транзакции (например, «0x92c4b1f2...»), сотрудники правоохранительных органов могут использовать блокчейн-эксплореры (Etherscan, Blockchain.com) для дальнейшего мониторинга движения активов. Если установлено, что сред-

ства были направлены на криптообменники, связанные с отмыванием денег, или на адреса «даркнет»-площадок, это будет являться прямым доказательством преступного умысла.

Например, наличие в журнале криптовалютной биржи записи о выводе крупных сумм в USDT (стейблкоин) с последующим направлением на нелегальный обменный пункт, не требующий идентификации личности, явно указывает на схему обналичивания преступных доходов и отмывания средств.

Существенное значение имеет экономический аспект криминального анализа криптовалютных транзакций. Так, соотношение суммы комиссий за вывод и общих сумм выведенных средств может указать на логичность или аномальность поведения злоумышленника. Если комиссии явно непропорциональны сумме вывода, это может свидетельствовать о попытках преступника быстро избавиться от компрометирующих средств либо минимизировать риски ареста активов правоохранительными органами.

Кроме того, криминальный анализ способен выявить специфические паттерны поведения подозреваемых, такие как регулярное дробление крупных сумм на более мелкие транзакции («слоение»), что характерно для попыток скрыть источник происхождения денежных средств. Сопоставление размеров депозитов и выводов, а также эквивалентов сумм транзакций в традиционных (фиатных) валютах позволяет более точно определить финансовый масштаб преступной деятельности и потенциальный ущерб, причиненный преступлениями с использованием криптоактивов. В результате такой подход обеспечивает возможность не только установить наличие криминального умысла, но и количественно измерить экономический ущерб, причиненный потерпевшим, а также разработать эффективные меры противодействия и профилактики подобных правонарушений в финансовой сфере.

Таким образом, криминальный анализ криптовалютных транзакций представляет собой комплекс методов и подходов, которые позволяют правоохранительным органам эффективно расследовать преступления с использованием цифровых активов. Сопоставление временных меток операций с датами преступлений, анализ объемов транзакций, идентификация пользователей посредством процедуры KYC, а также отслеживание движения криптоактивов по хэшам транзакций являются мощными инструментами для установления и доказательства причастности лиц к криминальной деятельности.

УДК 343.102:351

А.И. Бородич

ВЗАИМОДЕЙСТВИЕ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, КАК НАПРАВЛЕНИЕ ЭФФЕКТИВНОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ

Органы, осуществляющие оперативно-розыскную деятельность, при выполнении ее задач в пределах своей компетенции взаимодействуют между собой в соответствии с Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» с изменениями и дополнениями и иными актами законодательства. В связи с этим в современных условиях актуальным является изучение проблем, связанных, в частности, с определением организационно-тактических особенностей противодействия преступности, поиска и внедрения адекватных форм и методов оперативно-розыскной деятельности, научно обоснованных подходов к ее организации и тактике. Определим, что состояние противодействия преступности характеризуется тремя субъективно-объективными причинами: умением соответствующих должностных лиц оценивать факторы и определять реальные угрозы; наличием у субъектов противодействия преступности возможностей им реально противодействовать; целесообразным применением имеющихся сил и средств в ходе предупреждения и пресечения выявленных реальных угроз от преступной деятельности.

Общность задач оперативно-розыскной деятельности вызывает у органов, ее осуществляющих, необходимость организации совместных действий, принятие организационных, правовых, оперативных мер по усилению взаимодействия, заключающегося в единстве понимания их сотрудниками задач противодействия преступности, достижении наиболее рационального и эффективного использования сил и средств, обеспечении слаженности в действиях. Такой подход к определению цели взаимодействия заставляет искать методы оценки возможностей взаимодействующих сил и средств, позволяет на научной основе реализовать идею комплексного подхода к их применению. Поэтому, рассматривая взаимодействие как целенаправленный, рассчитанный на объединение усилий заинтересованных органов при различных изменениях обстановки процесс, следует отметить, что оно даст максимальный результат тогда, когда функции, уровни каждого субъекта взаимодействия будут четко определены. Особенно тесным и конструктивным, охватывающим

широкий спектр задач, относящихся к выявлению, предупреждению и пресечению преступной деятельности, должно являться взаимодействие органов внутренних дел, государственной безопасности, пограничной службы, Службы безопасности Президента, Оперативно-аналитического центра при Президенте, органов финансовых расследований Комитета государственного контроля, таможенных органов.

Поэтому, исходя из задач оперативно-розыскной деятельности, органам, ее осуществляющим, в целях повышения качества взаимодействия предлагается: разрабатывать конкретные планы и иные документы, касающиеся взаимодействия, доводить их до исполнителей; организовывать и обеспечивать подготовку сил и средств к предстоящим совместным действиям, оперативно-розыскным мероприятиям; обеспечивать участие своих представителей (органов, подразделений) по установлению, постоянному поддержанию связи с взаимодействующими структурами и периодическому уточнению форм взаимодействия; организовывать и проводить совместные заседания коллегий, оперативно-служебные совещания; создавать совместные рабочие группы для выработки предложений и решения конкретных задач; издавать совместные приказы, распоряжения.

При организации взаимодействия в целях эффективного противодействия преступности, приоритетными направлениями могут являться: рабочие встречи оперативных работников с целью повышения оперативности взаимного информирования, реагирования на организованную преступную деятельность в различных ее сферах; обмен опытом противодействия противоправной деятельности; организация и проведение совместных оперативно-розыскных мероприятий; получение и проверка первичной информации о возможной причастности лиц к преступной деятельности; работа по делам оперативного учета.

При организации взаимодействия межведомственных органов оперативно-розыскной деятельности предлагается прежде всего учитывать особенности, которые влияют на его качество и эффективность и заключаются в следующем: во-первых, взаимодействие должно осуществляться на этапах выработки единого замысла, плана противодействия преступности, в процессе непосредственной реализации замысла и планов вышестоящих структур; во-вторых, взаимодействие, как правило, осуществляется на средних и низших уровнях управления, когда оно объективно требует либо согласования, соподчинения деятельности субъектов, либо установления целесообразного соотношения между какими-либо их действиями; в-третьих, особенность взаимодействия состоит в том, что под контроль руководителей взаимодействующих

структур берутся действия субъектов взаимодействия в процессе их функционирования; в-четвертых, в процессе взаимодействия могут вноситься различные коррективы, связанные со своевременным уточнением действий используемых сил и средств.

В связи с динамично изменяющейся обстановкой взаимодействие предполагает заблаговременную его организацию и постоянное поддержание по нескольким вероятным вариантам развития ситуации. Поэтому на всех уровнях организации взаимодействия, в целях успешного решения стоящих задач, оно должно быть многовариантным. В целях повышения эффективности взаимодействия оно должно рассматриваться в двух аспектах:

во-первых, это: деловая, совместная работа субъектов оперативно-розыскной деятельности по выработке стратегии и тактики противодействия преступности; совместное принятие мер и внесение в установленном порядке предложений об устранении условий, способствующих преступной деятельности; проводимые совещания на различных уровнях, направленные на повышение оперативности взаимного информирования, включение сил, средств и иных возможностей ведомств в планируемые (проводимые) мероприятия; совместная разработка тактики противодействия преступности, с учетом масштабов, усложнения структур и системы отношений в ее среде; активное использование в противодействии преступности возможностей иных государственных органов власти и управления, негосударственных предприятий и иных структур;

во-вторых, это: отношения должностных лиц различных ведомств, возникающие в связи с выполнением ими своих функциональных обязанностей по выявлению, предупреждению и пресечению преступной деятельности на разных стадиях: от получения и оценки исходной информации до планирования, материального, оперативно-технического и силового обеспечения реализации собранных данных.

Создание стабильной, конструктивной и четкой системы согласованных действий, отлаженного механизма взаимного обмена информацией, исключение дублирования в работе является одним из основных направлений повышения эффективности противодействия преступности. В связи с этим, исходя из решаемых задач, можно предложить следующий комплекс основных направлений взаимодействия: определение стратегии противодействия преступности; подготовка на основании тщательного изучения и оценки политической и оперативной обстановки научно обоснованных прогнозов по вопросам обеспечения национальной безопасности; подготовка предложений по совершенствованию деятельности органов, осуществляющих оперативно-розыскную

деятельность; взаимодействие непосредственно в текущей оперативно-розыскной деятельности в вопросах выявления, предупреждения и пресечения преступной деятельности; оказание содействия силами и средствами органам, осуществляющим оперативно-розыскную деятельность; взаимодействие в области подготовки и специализации кадров.

Таким образом, объединение усилий всех заинтересованных органов, осуществляющих оперативно-розыскную деятельность, мобилизация их ресурсов поможет эффективно противодействовать преступности.

УДК 343.985.8

С.Г. Ванагель, Б.В. Ковалик

ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ДИСТАНЦИОННОЙ АНОНИМНОСТИ

Цифровая среда создает беспрецедентные условия для сокрытия противоправной деятельности. Информационно-коммуникационные технологии трансформировали характер преступности, переведя значительную ее часть в дистанционный формат, где ключевым фактором становится анонимность субъекта, что создает определенные затруднения для органов, осуществляющих оперативно-розыскную деятельность. В Республике Беларусь подобные преступления, включая дистанционные хищения, а также действия экстремистского и террористического характера, часто совершаются с использованием SIM-карт и цифровых идентификаторов, исключающих возможность установления личности их пользователей.

Несмотря на наличие правовых норм, регулирующих общественные отношения в сфере электросвязи, существующее законодательство не в полной мере обеспечивает пресечение деятельности лиц, распространяющих средства связи и доступа к различным ресурсам (SIM-карты, учетные записи и т. п.) с заведомо анонимным или подложным оформлением. Проблема обостряется ввиду наличия нелегального оборота SIM-карт, зарегистрированных на подставных лиц, который может обеспечиваться посредством осуществления формально легальной предпринимательской деятельности. Установлены случаи, когда юридические лица заключали сотни договоров на оказание услуг электросвязи в целях обеспечения деятельности транснациональных преступных групп. Проведенный анализ показал, что ряд сотрудников операторов связи, действуя из корыстных побуждений, оформляли договоры с внесением заведомо ложных сведений, что позволило вывести из правового поля значительное количество абонентских номеров. Вследствие этого возникла система теневого оборота SIM-карт, использующихся для регистрации фейковых аккаунтов и отмывания денежных средств через криптовалютные платформы и игорные ресурсы.

Полагаем, что указанная возможность также обусловлена отсутствием четкой правовой регламентации оборота учетных записей, аккаунтов, игровых профилей и иных цифровых идентификаторов, которые не подпадают под понятие «средства платежа», однако активно используются для анонимизации преступной деятельности. Сегодня ответственность за распространение указанных объектов законодательством Республики Беларусь прямо не установлена.

Актуальность данной проблемы подтверждается отсутствием возможности привлечения к ответственности так называемых дропов, дроповодов и посредников, чья деятельность направлена на создание инфраструктуры анонимного доступа к цифровым платформам. Через такие каналы осуществляется регистрация аккаунтов, используемых для распространения экстремистских материалов, управление фишинговыми ресурсами, распространение вредоносного программного обеспечения и иной противоправной активности.

Указанная проблема требует не только теоретического осмысления, но и предложений по совершенствованию законодательства. В частности, целесообразна реализация законодательной инициативы по установлению ответственности за распространение из корыстных побуждений средств связи и иных идентификаторов, способствующих сокрытию личности субъекта. Учитывая различную степень общественной опасности таких деяний, представляется обоснованным введение двухуровневой модели ответственности: административной – за единичные факты оборота, уголовной – в случае систематической либо организованной деятельности.

Дополнительно необходимо обязать операторов электросвязи, криптоплатформы и организаторов игорного бизнеса осуществлять ревизионные мероприятия, направленные на выявление и блокировку анонимных пользователей, а также ресурсов, предлагающих соответствующие услуги. Министерству связи и информатизации, в пределах компетенции, следует ограничивать доступ к сайтам и платформам, рекламирующим распространение «анонимных» SIM-карт и фейковых цифровых идентификаторов и т. п.

Следует отметить, что эффективность противодействия дистанционной анонимности может быть достигнута только при комплексном под-

ходе: нормативном, технологическом и организационном. Закрепление ответственности за предоставление и использование различных инструментов цифровой анонимизации позволит сократить их использование, что должно способствовать прозрачности цифровой среды.

УДК 343.985

В.М. Веремеенко

ЛИБЕРАЛИЗАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК ТОВАРОВ (РАБОТ, УСЛУГ) КАК ОДНА ИЗ ПРЕДПОСЫЛОК СОВЕРШЕНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ

Анализ статистических данных Министерства антимонопольного регулирования и торговли, Национального центра маркетинга и конъюнктуры цен, а также сведений, содержащихся в автоматизированной системе финансовых расчетов Министерства финансов (ГИАС), свидетельствует, что большинство процедур закупок в Республике Беларусь являются неконкурентными.

Так, в 2021 г. было проведено 73 %, в 2022 г. – 72 %, а в 2023 г. – 63 % закупок с применением процедуры из одного источника. В настоящее время в Республике Беларусь продолжается рост количества неконкурентных процедур закупок, а также стоимости заключенных договоров по их результатам (более 70 % от стоимости всех заключенных договоров). Пропорционально увеличению количества процедур закупок из одного источника наблюдается и рост выявляемых тяжких коррупционных преступлений в данной сфере.

Анализ законодательства и статистических данных позволил выделить следующие причины увеличения закупок из одного источника и увеличения стоимости договоров, проводимых по результатам проведения указанного вида процедур закупок.

1. В связи с изменениями и дополнениями в Закон Республики Беларусь от 13 июля 2012 г. № 419-З «О государственных закупках товаров (работ, услуг)» значительно увеличился перечень случаев, позволяющих проводить процедуры из одного источника. В настоящее время увеличена ориентировочная стоимость годовой потребности государственной закупки товаров (работ, услуг) с 300 до 500 базовых величин.

2. До вступления новых изменений и дополнений в Закон Республики Беларусь от 13 июля 2012 г. № 419-З «О государственных закупках товаров (работ, услуг)» в соответствии со ст. 27 в случае признания процедуры государственной закупки, в том числе в отношении отдельных частей (лотов), несостоявшийся заказчик (организатор) был вправе провести процедуру закупки из одного источника только по согласованию с государственным органом (организацией), в подчинении которого он находился либо которому были переданы в управление его акции, или на основании самостоятельно принятого решения после проведения повторной процедуры государственной закупки, которая была признана несостоявшейся.

В настоящее время заказчик (организатор) вправе провести процедуру закупки из одного источника уже после проведения и признания несостоявшейся одной конкурентной процедуры государственной закупки.

3. Постановлением Совета Министров Республики Беларусь от 12 марта 2024 г. № 169 значительно расширен список случаев, когда заказчик (организатор) вправе провести процедуру закупки из одного источника. Указанная процедура закупки может применяться до 11 марта 2026 г. для закупки услуг по разработке градостроительных паспортов земельных участков; для приобретения товаров (работ, услуг) при строительстве объектов, включенных в инвестиционные программы областей и г. Минска, у государственных унитарных предприятий, объединений, организаций, акции (доли в уставных фондах) которых находятся в собственности Республики Беларусь и (или) ее административно-территориальных единиц и т. д.

4. Отдельными нормативными правовыми актами определяются конкретные производители, у которых обязательно приобретение товаров (работ, услуг). Например, с 30 сентября 2023 г. в качестве специальных и служебных легковых автомобилей, которые не требуют дооснащения путем монтажа специального оборудования, необходимо закупать автомобили, произведенные СЗАО «БЕЛДЖИ». Указанные автомобили могут приобретаться как у производителя, так и у официального представителя с применением процедуры закупки из одного источника. Данное правило было установлено Указом Президента Республики Беларусь от 26 июня 2023 г. № 191 «Об упорядочении приобретения и использования транспортных средств».

5. В настоящее время принято большое количество локальных нормативных правовых актов, действие которых распространяется на определенные сферы деятельности, содержащие указания на приобретение того или иного товара у конкретного производителя. Такие нормативные правовые акты, как правило, имеют ограничительный гриф «Для служебного пользования». Процедура закупки в данном случае также проводится из одного источника.

Таким образом, либерализация законодательства в сфере государственных закупок товаров (работ, услуг) обусловлена политической и экономической ситуацией и связана с защитой интересов национальных производителей. Вместе с тем рассмотренные выше причины увеличения закупок из одного источника и увеличения стоимости договоров, проводимых по результатам проведения указанного вида процедур закупок, являются предпосылками увеличения количества коррупционных преступлений. В этой связи оперативным подразделениям органов внутренних дел следует уделять особое внимание таким видам процедур закупок, проводить подробный их анализ с целью недопущения совершения коррупционных преступлений и причинения ущерба экономическим интересам страны.

УДК 342.9

С.Е. Вородюхин, К.К. Крупенникова

ПРАВОВОЕ АНТИКОРРУПЦИОННОЕ ВОСПИТАНИЕ СОТРУДНИКОВ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СИСТЕМЕ ПРОФИЛАКТИКИ КОРРУПЦИИ

Антикоррупционное поведение как система сознательно применяемых сотрудниками и работниками органов внутренних дел методов и приемов профессиональных действий формируется как результат целенаправленного и систематического воспитательного, морально-психологического и иного воздействия на сотрудников и работников в целях закрепления и развития в них психологических детерминант антикоррупционного поведения.

Антикоррупционное воспитание – комплексное воздействие на личность, направленное на формирование антикоррупционно значимых качеств личности. Целью антикоррупционного воспитания является передача ценностных установок и развитие способностей, необходимых для последующего формирования гражданской позиции относительно коррупции.

Основные задачи антикоррупционного воспитания включают в себя:

формирование негативного отношения к коррупции. Через обучение и пропаганду необходимо донести до людей, что коррупция негативно влияет на общество, экономику и политическую систему;

развитие чувства справедливости и ответственности. Важно воспитывать у граждан понимание того, что каждый человек несет ответственность за свои действия и должен действовать в соответствии с законом и моральными нормами;

привитие навыков противодействия коррупции. Граждане должны быть осведомлены о своих правах и обязанностях, а также знать, как действовать в случае столкновения с коррупцией;

формирование этических принципов. Антикоррупционное воспитание направлено на развитие у граждан честности, порядочности, уважения к закону и общественным интересам;

повышение общественного контроля. Важной задачей антикоррупционного воспитания является стимулирование граждан к активному участию в общественной жизни, контроле за деятельностью государственных структур и борьбе с коррупцией.

Для преодоления коррупции в России необходимо принять, на наш взгляд, следующие меры:

усилить контроль со стороны надзорных органов за исполнением законов и должностных обязанностей всеми государственными служащими (значимость указанной меры определяется сущностью самого назначения контроля). Ведь именно контроль со стороны надзорных органов позволяет выявить недобросовестных сотрудников и в определенной степени служит неким сдерживающим фактором;

существенно увеличить заработную плату государственным служащим (причины, связанные с недостаточно высоким уровнем денежного довольствия, всегда признавались ключевыми коррупционными детерминантами). На фоне современных темпов инфляционных процессов недостаток финансового стимулирования сотрудников ощущается особо остро. Если государственный служащий будет получать заработную плату, позволяющую удовлетворить все потребности, то не будет необходимости получения денежных средств преступным путем, так как каждый будет дорожить своей должностью и репутацией;

создать должность федерального омбудсмена по борьбе с коррупцией (на указанное лицо будет возлагаться функция контроля соблюдения справедливости и интересов определенных граждан в деятельности органов исполнительной власти и должностных лиц, т. е. в его обязанности должно входить выявление излишних бюрократических процедур, анализ правовых актов, подготовка предложений по улучшению антикоррупционного законодательства и работа с общественностью. Учреждение должности омбудсмена по борьбе с коррупцией – шаг на пути к развитию гражданского общества);

обеспечить объективное освещение в средствах массовой информации мероприятий государства и общественных организаций по про-

филактике и борьбе с коррупцией (данная мера позволит обеспечить эффективное взаимодействие с обществом. Во-первых, широкое освещение антикоррупционных мероприятий позволит повысить уровень сознательности граждан и обеспечит снижение уровня бытовой коррупции. Во-вторых, обеспечивается повышение уровня доверия граждан к деятельности государственных органов и желание участия в выработке отдельных предложений по совершенствованию мер. Ключом к борьбе с коррупцией является транспарентность. Чем больше информации становится общедоступной, тем более эффективно неправительственные организации и средства массовой информации могут «изобличать и позорить» коррупционную практику, и тем самым способствовать ее искоренению).

В настоящее время государство проводит активную антикоррупционную политику и принимает законодательные меры, направленные на формирование нетерпимого отношения к коррупционному поведению в обществе.

В рамках антикоррупционной политики России антикоррупционное воспитание обусловлено необходимостью создания эффективной системы профилактики коррупционных правонарушений и изменения общественного менталитета в отношении коррупции.

Таким образом, антикоррупционная направленность правового воспитания сотрудников и работников органов внутренних дел основана на повышении в обществе в целом позитивного отношения к праву, его соблюдению, повышении уровня правовых знаний, в том числе о коррупционных формах поведения и мерах по их предотвращению.

УДК 81’35

Ю.А. Воронцова, К.В. Дорожинская

РАЗЫСКНОЙ ИЛИ РОЗЫСКНОЙ: К ПРОБЛЕМЕ ВЫБОРА

В правовой коммуникации использование государственного языка Российской Федерации, основополагающим стандартом которого являются кодифицированные формы языка, обязательно.

В настоящее время изменилась орфографическая норма написания слова «*разыскной*» (закрепленная современная норма через «а»), которое перестало быть исключением. Однако в официальных документах используется два варианта написания: через «а» и «о», такой орфографический разнобой в правописании (*розыскной* или *разыскной*) вызывает затруднения. Обратимся к проблеме выбора варианта написания терминологической единицы *разыскной*.

Для лучшего понимания сути вопроса укажем, что ведущим принципом орфографии в русском языке является морфологический, согласно которому сохраняется одинаковое написание морфем, несмотря на различное их произношение. На этом положении основано правило проверки безударной гласной в корне, т. е. в результате изменения грамматической формы, подбора однокоренного слова безударная гласная должна стать ударной. Поэтому для написания слова «*розыскной*» ориентиром ошибочно становится проверочное слово «*розыск*».

Строгая рекомендация учитывать ударение при выборе букв «а» и «о» в приставках *раз- (рас-) / роз- (рос-)* и в безударной позиции писать приставки *раз- (рас-)* с буквой «а»: *разыскной, расписной*, а под ударением – приставки *роз- (рос-): розыск, роспись* содержится в утвержденном в качестве общеобязательного свода правил русского правописания (1956 г.). Аналогичное требование в отношении написания приставок *раз- (рас-) / роз- (рос-)* находим в «Русском орфографическом словаре» (под редакцией В.В. Лопатина, О.Е. Ивановой, 1999 г.); в полном академическом справочнике «Правила русской орфографии и пунктуации (под редакцией В.В. Лопатина, 2006 г., 2009 г.); в «Грамматическом словаре русского языка: Словоизменение» А.А. Зализняка (2008 г.) и др. Как видим, в грамматиках, словарях и справочниках учитывается и фиксируется существующая практика письма, ориентированная на нормативный (единственно возможный) вариант написания слова «*разыскной*» с буквой «а» в приставке *раз-* в безударной позиции.

Однако по неизвестным причинам отдельные словари и справочники, изданные в период с 1960 по 1980 г., например, «Словарь трудностей русского языка» (под редакцией Д.Э. Розенталя, М.А. Теленковой, 1981 г.) и другие, рекомендуют писать слово «*розыскной*» с буквой «о» в безударной позиции, т. е. причисляют написание данного слова к исключению из правила правописания приставок *раз- (рас-) / роз- (рос-).*

В настоящее время это неоправданное и непредусмотренное правилами исключение устранено. В соответствии с действующими «Правилами русской орфографии и пунктуации» нормативным считается написание слова «*разыскной*» с буквой «а»: *оперативно-разыскные мероприятия, разыскные документы, разыскная служба, разыскная собака* и т. д., а вариант написания слова «*розыскной*» с буквой «о» относится к устаревшим.

Отметим, что в юридической сфере функционируют варианты написания: *розыскной* и *разыскной*. Например, написание слова «*розыскной*» с буквой «о» используется в Федеральном законе Российской Федерации

от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; в приказе МВД России от 27 сентября 2013 г. № 776 «Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд»; в Федеральном законе Российской Федерации от 1 июля 2021 г. № 252-ФЗ «О внесении изменения в статью 8 Федерального закона «Об оперативно-розыскной деятельности»; в наименованиях направленности образовательных программ; в учебной и научной литературе и т. д. Написание слова «*розыскной*» обусловлено тем, что при составлении текста Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», в котором закрепляется написание термина «*оперативно-розыскной*» с буквой «о», авторы опирались на словари и справочники, в которых слово «*розыскной*» имело статус «исключение». Поэтому все последующие законодательные тексты используют вариант написания, зафиксированный в исходном документе. Это же обстоятельство определило выбор варианта написания слова «*розыскной*» с буквой «о» в процессуальных документах, например, <…> *это установлено по результатам <…> оперативно-розыскной деятельности, протоколах следственных действий <…>* (Апелляционное определение Верховного Суда Российской Федерации по делу № 224-АПУ 19-1 от 21 ноября 2019 г.). В подобных текстах нарушение орфографической нормы спровоцировано специфическими особенностями институциональной коммуникации, написание слов полностью соответствует законодательным текстам. В результате орфографическая ошибка в слове «*розыскной*» с буквой «о» тиражируется и приобретает санкционированный характер.

В современных официальных документах написание соответствует актуальной орфографической норме, т. е. *разыскной* – с буквой «а». Например, Указ Президента Российской Федерации от 27 мая 2007 г. № 663 «О начальнике Оперативного-разыскного бюро № 10 Министерства внутренних дел Российской Федерации»; *сотрудник полиции проводит оперативно-разыскные мероприятия* (ст. 12 Федерального закона Российской Федерации от 7 февраля 2011 г. № 3-ФЗ «О полиции»), но проводит их, обязательно, в соответствии с Федеральным законом Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Вот такое разногласие в написании слова «*разыскной*» создает основание для споров, поскольку, по сути, закон о полиции ссылается на несуществующий с юридической точки зрения нормативный правовой акт. Данное обстоятельство хотя и кажется несущественным, но при этом вызывает некоторые сложности, в том числе для сотрудников полиции. По этой причине еще в 2007 г. на заседании

Совета Федерации Российской Федерации Ю. Горбунов (заместитель директора Федеральной службы безопасности) инициировал замену буквы «о» на «а» в Федеральном законе «Об оперативно-розыскной деятельности» (газета «Известия», 31 января 2007 г.).

Кодифицированное написание слова «*разыскной*» используется в средствах массовой информации, например, *руководитель главного управления экономической безопасности и противодействия коррупции <…> до этого возглавлял 10-е оперативно-разыскное бюро (ОРБ)…* (газета «Коммерсантъ», № 116 (4657), 29 июня 2011 г.).

Соответствуют современной орфографической норме наименование кафедр в образовательных организациях системы МВД России, например, *кафедра оперативно-разыскной деятельности* (Белгородский юридический институт МВД России имени И.Д. Путилина); *кафедра оперативно-разыскной деятельности в органах внутренних дел* (Санкт-Петербургский университет МВД России); *кафедра криминалистики и оперативно-разыскной деятельности* (Ростовский юридический институт МВД России) и др.

Отметим, что трудности, связанные с правописанием слова «*разыскной*», детерминированы объективными причинами, к числу которых относится сфера использования – правовая. Обратим внимание на то, что правовая коммуникация имеет институциональный характер, поэтому главным ориентиром для использования языковых средств становится законодательный текст, который в лингвистическом отношении является авторитетным источником и полностью должен соответствовать нормам грамматики, стилистики, лексики, орфографии и пунктуации, поэтому отступление от орфографических стандартов недопустимо.

Подчеркнем, что нормативное написание слова «*разыскной*» с буквой «а» закреплено в словарях и справочниках, отражающих современную практику письма. Вариант написания слова «*розыскной*» с буквой «о» сохраняется только в исторических документах, к числу которых относятся законодательные тексты, принятые до 2000 г.

Таким образом, правовая сфера вносит диссонанс между орфографическим правилом и его применением на практике. Правописание в современном русском литературном языке регулируется орфографическими, а не правовыми нормами. Написание слова «*розыскной*» не регламентировано и дезориентирует авторов текстов. Учитывая вышеизложенное, считаем необходимым унифицировать написание слова «*разыскной*» во всех официальных текстах с учетом требований современной орфографической нормы.

УДК 343.811-055.2

Р.В. Глубоковских

ПРОБЛЕМНЫЕ ВОПРОСЫ ОСУЩЕСТВЛЕНИЯ РОЗЫСКА ОСУЖДЕННЫХ ПОДРАЗДЕЛЕНИЯМИ ФСИН РОССИИ

Розыскная работа (деятельность) правоохранительных органов Российской Федерации является составной частью оперативно-розыскной деятельности (ОРД). Задачи по розыску лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, указанные в ст. 2 Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ «Об ОРД») являются общими для всех субъектов ОРД.

Касаемо понятия «розыскная работа», нами ранее была предложена следующая ее дефиниция – самостоятельное направление оперативно-розыскной деятельности, осуществляемой уполномоченными оперативными (розыскными) подразделениями органов внутренних дел с привлечением имеющихся сил, средств и методов, установленных законодательными и ведомственными нормативными актами, в целях установления местонахождения определенных категорий лиц, объявленных в розыск, с целью обеспечения возможности применения к ним предусмотренных законом мер, а также деятельность по идентификации неустановленных трупов и лиц, не способных сообщить сведения о себе.

Основаниями для проведения оперативно-розыскных мероприятий (ОРМ), указанными в подп. 3 п. 2 ч. 1 ст. 7 ФЗ «Об ОРД» являются ставшие известными органам, осуществляющим ОРД, сведения о лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания.

Ст. 13 ФЗ «Об ОРД» оперативные подразделения органов внутренних дел и Федеральной службы исполнения наказаний (ФСИН) наделены правом осуществлять ОРД, и что примечательно в полном объеме, в отличие от оперативного подразделения органа внешней разведки Министерства обороны Российской Федерации, которое имеет право проводить ОРМ только в целях обеспечения безопасности указанного органа внешней разведки и других ограниченных случаях.

Однако нормативно-урегулированная, на первый взгляд, розыскная работа оперативных подразделений ФСИН не является полной и эффективной в части проведения ОРМ, ограничивающих конституционные права граждан в целях установления местонахождения разыскиваемых объектов. Иными словами, оперативные подразделения ФСИН законодательно лишены возможности проведения таких ОРМ, как «прослушивание телефонных переговоров» («ПТП»), «снятие информации с технических каналов связи» («СИТКС»), «получение компьютерной информации» и иных, связанных с негласным проникновением в жилище.

ОРД при исполнении наказаний, не связанных с изоляцией осужденных от общества, предусмотрена ч. 3 ст. 18.1 Уголовно-исполнительного кодекса Российской Федерации и осуществляется оперативными подразделениями уголовно-исполнительной системы самостоятельно и во взаимодействии с оперативными подразделениями иных государственных органов, а также иными государственными органами в пределах их компетенции.

Так, при поступлении материалов на объявление в розыск осужденных у оперативных подразделений появляются полные основания для проведения ОРМ по их розыску (подп. 3 п. 2 ч. 1 ст. 7 ФЗ «Об ОРД»).

Условия проведения отдельных ОРМ, предусмотренные ч. 2 и ч. 4 ст. 8 ФЗ «Об ОРД», значительно сокращают возможности применения оперативно-розыскного инструментария оперативных подразделений ФСИН.

Так, проведение ОРМ, которые ограничивают конституционные права человека и гражданина, осуществляемые на основании судебного решения, допускается по противоправным деяниям, по которым производство предварительного следствия обязательно. В случае осуществления розыска осужденного уже имеется обвинительный приговор суда и о следственном процессе речи не идет.

Кроме того, ОРМ «ПТП» допускается только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях. Такой категории как осужденные в ФЗ «Об ОРД» вовсе не упоминается.

Приведем яркий пример из практики розыскной работы оперативного подразделения ФСИН России по Калининградской области, который является типовым при розыске осужденных за преступления средней тяжести и выше.

Осужденный в 2024 г. за незаконный оборот наркотических средств (преступление средней тяжести) к принудительным работам, ранее судимый «ДВС» находился в федеральном розыске и активно скрывался от органов ФСИН. Проведение оперативно-поисковых мероприятий и несанкционируемых ОРМ подтвердило наличие мобильного телефона у разыскиваемого. Отработка связей фигуранта и выставление засад в местах возможного появления положительных результатов не дали. Сотрудники ФСИН неоднократно созванивались и общались с разыски-

ваемым, склоняя его к самостоятельному прибытию в органы ФСИН. Впоследствии УФСБ России по Калининградской области выявлена и пресечена противоправная деятельность «ДВС». В ходе проведенного комплекса ОРМ установлено, что подозреваемый, действуя по заданию неустановленного лица в интересах Украины, намеревался осуществить поджог электропитающего оборудования базовой станции сотовой связи. По указанному факту следственным отделом УФСБ России по Калининградской области возбуждено уголовное дело по ч. 3 ст. 30, п. «а» ч. 2 ст. 281 «Диверсия» Уголовного кодекса Российской Федерации.

Безусловно, своевременное задержание разыскиваемых осужденных, имеющих в пользовании средства связи, крайне необходимо в том числе и для предупреждения совершения последними иных преступлений.

Проведенный нами опрос и интервьюирование действующих оперативных сотрудников ФСИН показывают, что проблема розыска осужденных и невозможность проведения эффективных ОРМ является крайне острой и по сути не позволяет реализовать задачи по их розыску при наличии тактических возможностей достижения желаемого результата (98 % опрошенных), 100 % опрошенных высказываются за внесение изменений в оперативно-розыскное законодательство в части проведения ОРМ, ограничивающих конституционные права человека и гражданина в целях розыска осужденных. По мнению руководителей территориальных органов ФСИН, 70 % находящихся в розыске осужденных могут быть обнаружены путем проведения ОРМ «ПТП» и «СИТКС» при наличии к тому законных оснований.

Учитывая заинтересованность автора данной публикации в разрешении проблем розыскной работы в органах внутренних дел, считаем необходимым скорректировать норму оперативно-розыскного закона, касающуюся условий проведения ОРМ, ограничивающих права человека и гражданина.

В настоящее время, учитывая общие интересы органов внутренних дел и ФСИН в розыске скрывшихся лиц различных категорий, нам видится возможность общего обсуждения и внесения предложений по гармонизации оперативно-розыскного законодательства в части внесения изменений в ст. 8 ФЗ «Об ОРД».

Таким образом, предлагаем внести изменения в ч. 4 ст. 8 ФЗ «Об ОРД» и изложить ее в следующей редакции: «Прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых, обвиняемых или объявленных в розыск осужденных в (за) совершении (-е) преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях и (или) местонахождении лиц, объявленных в розыск.»

УДК 343.985

Д.В. Гриб

ПРОТИВОДЕЙСТВИЕ ЛЕГАЛИЗАЦИИ СРЕДСТВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ: УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ

Проблема легализации денежных средств характерна большинству форм организованной преступности, так как является необходимым условием ее функционирования. Эта проблема имеет особую значимость, поскольку ее масштабы и распространенность нарушают организацию экономической деятельности государства. В связи с чем противодействие легализации средств и иного имущества, полученных преступным путем, является одной из важнейших задач оперативно-розыскной деятельности при документировании преступлений в сфере экономики.

Правовую основу противодействия легализации доходов, полученных преступным путем, составляют: Закон Республики Беларусь от 30 июня 2014 г. № 165-З «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения», Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», постановление Правления Национального банка Республики Беларусь от 24 декабря 2014 г. № 818 «О внутреннем контроле при осуществлении банковских операций».

Проанализировав правовую основу легализации доходов, полученных преступным путем, целесообразно указать, что к государственным мерам по их предотвращению относят: внутренний контроль и особой контроль. Механизм работы которой заключается в применении расширенных мер контроля при осуществлении финансовых операций с высокой степенью риска, связанного с рассматриваемым видом преступления, а также идентификации таких лиц. К таковым мерам относят идентификацию и верификацию клиентов банка, осуществляющих финансовые операции, мониторинг их деятельности в процессе обслуживания, выявление, документальное фиксирование финансовой операции, подлежащей особому контролю, и передачу соответствующих сведений в орган финансового мониторинга, а также «замораживание» средств и (или) блокирование финансовых операций. Исходя из этого следует отметить, что в рассматриваемых нормативных правовых актах указана организация системы внутреннего контроля в сфере предотвра-

щения легализации доходов, полученных преступным путем, а также основные направления, по которым она реализовывается.

Следует также указать, что законодатель предусмотрел уголовную ответственность по ст. 235 Уголовного кодекса Республики Беларусь (далее – УК) (легализация («отмывание») средств, полученных преступным путем). Согласно ст. 235 УК под легализацией («отмыванием») денежных средств понимают совершение финансовых операций со средствами, полученными заведомо преступным путем, для придания правомерного вида владению, пользованию и (или) распоряжению указанными средствами в целях утаивания или искажения происхождения, местонахождения, размещения, движения или действительной принадлежности указанных средств.

Кроме того, изучение правоприменительной деятельности показало, что легализация средств, полученных преступным путем, выявляется в ходе расследования таких предикатных преступлений, как: мошенничество (ст. 209 УК), хищение путем злоупотребления служебными полномочиями (ст. 210 УК), уклонение от уплаты сумм налогов, сборов (ст. 243 УК), получение взятки (ст. 430 УК) и др.

Как правило, распределение средств от преступных доходов осуществляется путем приобретения имущества, офисов, автомобилей и квартир, либо средства направляются по различным сферам экономической деятельности, используя при этом услуги банкиров, брокеров, бухгалтеров, юристов, с целью приобретения акций, облигаций, криптовалюты. В последующем, после их реализации, указанные финансовые активы приобретают практически легальный статус.

В этой связи следует указать, что существуют определенные сложности процесса доказывания преступной деятельности разрабатываемых лиц, так как преступники используют в своей деятельности новые средства и методы легализации доходов (например, перевод фиатных средств в криптовалюту).

В преступные схемы по отмыванию денег также вовлекаются международные группы, которые создают в определенных странах «офшорные» организации, с которыми отсутствует международное сотрудничество в сфере обмена информацией.

Таким образом, сотрудникам оперативных подразделений необходимо обладать специальными познаниями в выявлении и раскрытии рассматриваемого вида преступления, в целях должной отработки организационно-тактических приемов документирования преступной деятельности разрабатываемого лица, а также выявление особенностей проведения оперативно-розыскных мероприятий.

УДК 343.985

Д.В. Гриб, Н.В. Черницкий

ПРИНЦИП КОНСПИРАЦИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

Принципы оперативно-розыскной деятельности (ОРД) представляют собой ключевые руководящие концепции, сформированные практикой оперативной работы и зафиксированные в соответствующих нормативных актах, регулирующих указанную сферу. Данные принципы отражают политическую, экономическую и социальную динамику современного общества, а также моральные и юридические взгляды граждан на сущность, цели и задачи деятельности сотрудников оперативных подразделений. Это важно для обеспечения законности и правопорядка в деятельности органов внутренних дел Республики Беларусь.

Новый этап развития Республики Беларусь после распада Советского Союза привел к переоценке прежней юридической основы и отказу от устаревших подходов, включая сферу правоохранительной деятельности. Возникла потребность в правовом регулировании ОРД, результатом которой стало принятие Верховным Советом Республики Беларусь 12 ноября 1992 г. Закона Республики Беларусь «Об оперативно-розыскной деятельности» № 1932-XII (далее – Закон «Об ОРД»).

В соответствии с Законом «Об ОРД» данная деятельность осуществляется на принципах законности, соблюдения прав, свобод и законных интересов граждан, прав и законных интересов организаций, конспирации, проведения оперативно-розыскных мероприятий (ОРМ) гласно и негласно.

Кроме того, изучив существующую практику, социальное положение, уровень преступности, исторические аспекты и международную нормативно-правовую базу, мы приходим к выводу, что необходима модернизация правового регулирования принципов ОРД в Республике Беларусь.

Исходя из вышеизложенного, следует отметить, что необходимо внести изменения и дополнения в действующие принципы ОРД. Это позволит детально регламентировать правовые нормы, которыми руководствуются сотрудники оперативных подразделений органов внутренних дел при выполнении поставленных задач, а также это поможет устранить имеющиеся недостатки в формулировках самих принципов.

Более подробной регламентации требует формулировка в содержание принципа ОРД конспирация. В научной литературе принято считать, что данный принцип обеспечивается системой оперативных, ре-

жимных, административно-правовых, воспитательных и других мер, направленных на закрытие доступа посторонним лицам к информации об ОРД и зашифровкой (маскировкой) самой деятельности. Так, рассматриваемую систему мер следует отразить в содержании действующего принципа конспирации в Законе «Об ОРД», изложив ее в следующей интерпретации: «Конспирация поддерживается системой оперативных, режимных, административно-правовых, воспитательных и других мер, направленных на закрытие доступа посторонним лицам к информации об ОРД и ее зашифровкой, обеспечивается органами, осуществляющими ОРД, и иными государственными органами».

Меры, которыми поддерживается указанный принцип, представляют собой своевременное реагирование на факты и события незаконного получения и распространения, в том числе, использования сведений, касающихся тактики и организации осуществления ОРД, укрепления и поддержания порядка защиты этих сведений оперативными подразделениями органов внутренних дел и их сотрудниками, осуществление надзора и контроля, разработка методических и других рекомендаций об использовании защиты информации об ОРД руководителями органов, осуществляющих ОРД, привлечении лиц, по вине которых наступили негативные последствия, поддержания конспирации к предусмотренной законодательством ответственности, а также проведении инструктажей и других собраний по тематике соблюдения режима секретности.

Совершенствование положения принципа ОРД конспирация способствует адаптации к современным условиям, повышения эффективности работы правоохранительных органов, осуществляющих ОРД, и соблюдения прав граждан. Указанные изменения должны проводиться с учетом зарубежного опыта в законодательстве, обеспечивая баланс между интересами государства и правами личности.

УДК 343.985

А.А. Гулюк

CRIMINT (КРИМИНАЛЬНАЯ РАЗВЕДКА) – СОВРЕМЕННЫЙ ИНСТРУМЕНТ ДЕАНОНИМИЗАЦИИ ЗЛОУМЫШЛЕННИКА В ЦИФРОВОМ ПРОСТРАНСТВЕ

Анализ криминогенной ситуации показывает, что актуальной проблемой как для Республики Беларусь, так и для всего мира остаются преступления, совершаемые с использованием сети Интернет.

Стремительная цифровизация всех сфер жизнедеятельности государства и общества, развитие электронной торговли, банковских продуктов и услуг, рост безналичных расчетов в экономике спровоцировали новые вызовы и угрозы.

Ежедневные инциденты в сфере киберпреступности во всем мире показали, что угрозы кибербезопасности стали опасными и гораздо серьезнее. Злоумышленники становятся намного организованнее, а векторы атак – более совершенными, постоянно используются новые методы и инструменты.

Адаптация к специфике киберпространства требует от сотрудников оперативных подразделений органов внутренних дел (ОВД) непрерывного улучшения методов и технологий для эффективного обнаружения и мониторинга киберпреступников в онлайн-среде. Важным аспектом является сотрудничество с провайдерами интернет-услуг и другими заинтересованными сторонами для обмена информацией и разработки совместных стратегий борьбы с киберпреступностью.

В современном информационном обществе, где совершение преступлений в виртуальном пространстве становится все более распространенным, сотрудникам оперативных подразделений ОВД необходимо активно использовать разные методы по установлению злоумышленников, в том числе эффективно могут применяться методы открытого и условно-открытого исследования информации (CRIMINT).

CRIMINT – это сбор и последующий анализ преступных идентификаторов преступной деятельности в киберпространстве из различных источников, который позволяет распознать действия злоумышленников на ранних этапах и оперативно реагировать на киберпреступления и киберугрозы.

Значительный рост киберпреступности подчеркивает важность эффективного мониторинга и анализа данных, доступных в сети Интернет.

CRIMINT предоставляет сотрудникам возможность получать ценную информацию из открытых, условно-открытых и закрытых источников, таких как социальные медиа, «слитые» базы данных, форумы и другие онлайн-ресурсы хакерской и кардерской направленности. Это способствует не только выявлению и раскрытию преступлений, совершенных в сети Интернет, но и преступлений, совершенных по линии иных подразделений ОВД.

Использование CRIMINT в современной деятельности сотрудников оперативных подразделений ОВД становится неотъемлемым компонентом в борьбе с преступностью и обеспечением цифровой безопасности общества и позволяет собирать информацию не только о киберпреступниках, но и о потенциальных угрозах, стратегиях антигосударственных формирований и других аспектах, влияющих на национальную

безопасность. Совокупность использования CRIMINT и методов оперативно-розыскной деятельности (ОРД) значительно улучшит результативность работы сотрудников оперативных подразделений ОВД. ОРД позволяет дополнить CRIMINT информацией из ведомственных учетов и баз данных, расширяя объем доступной информации. Кроме того, оперативные данные способны подтверждать или корректировать результаты CRIMINT, усиливая достоверность полученной информации. Применение методов ОРД в совокупности с CRIMINT дает возможность создания более полного и точного образа исследуемого объекта, что, в свою очередь, повышает эффективность аналитических процессов и оперативных действий в целом.

Часто сотрудники оперативных подразделений ОВД обладают лишь малой частью информации о личности преступника из-за чего затруднительно установить его личность в ходе проведения первоначальных оперативно-розыскных мероприятий. Как правило, имеется лишь id, username, никнейм, электронная почта, на которую был зарегистрирован аккаунт злоумышленника или фишинговый ресурс.

Для эффективного противодействия киберпреступности в интернете необходимо укрепление аналитической работы, включающей в себя контроль за более широким спектром интернет-ресурсов и платформ хакерской и кардерской направленности, как в Clearnet, так и в DarkNet, которые могут использоваться киберпреступниками для распространения идей, вербовки, планирования и совершения преступлений. Это может быть достигнуто путем увеличения числа специалистов в области противодействия киберпреступности и внедрения новых технологий. Например, применение программного обеспечения для автоматического анализа комментариев в telegram-каналах и на других интернет-платформах значительно облегчает работу сотрудников, позволяя быстро идентифицировать пользователей, распространяющих новые схемы преступлений, а также анализировать частоту и площадки их активности для последующей фиксации и обработки информации оперативными сотрудниками.

Для решения данного вопроса можно воспользоваться также методами CRIMINT, которые не требуют специальных навыков, такими как специализированные telegram-боты или интернет-ресурсы. Специализированные telegram-боты позволяют автоматизированно взаимодействовать с пользователями с использованием интерфейса мессенджера и могут предоставлять оперативно значимую информацию.

В качестве примера можно привести специализированные telegram-боты мессенджера Telegram: @funstat_chat_bot, @eyeofbeholder_bot, @user_stats_bot, которые используют информацию открытых

источников и могут предоставить информацию о смене пользователем своего никнейма или username, интересы пользователя в мессенджере, оставленные в открытых группах, чатах, каналах пользователем комментарии, показать список групп, на которые подписан пользователь, а также функции по контролю за пользователем (смена имени, комментарии, вступление в группы в режиме 24/7).

Еще одним решением является использование специализированных интернет-ресурсов, например https://himerasearch.com, osint.industries/ или https://tgstat.ru/, которые позволяют установить принадлежность владельца электронной почты, телеграмм-аккаунта, установить человека по фотографии, предоставить перечень групп, на которые подписано проверяемое лицо в мессенджерах и социальных сетях, установить, на каких сайтах и сервисах зарегистрирован пользователь.

Исходя из собранной информации, сотрудники оперативных подразделений ОВД могут ограничить область поиска или даже получить данные, которые с использованием ресурсов ОВД и оперативно-розыскных возможностей позволят установить личность и местонахождение разыскиваемого объекта.

Таким образом, процесс обнаружения и фиксации информации о преступлениях, совершенных киберпреступником, требует от сотрудников оперативных подразделений ОВД практических знаний в сфере информационных технологий, навыков использования специализированного оборудования и программного обеспечения, необходимого для обнаружения и фиксации оперативно значимой информации, а также обеспечения ее сохранности и неизменности. Сочетание методов CRIMINT и ОРД позволит повысить эффективность деятельности сотрудников оперативных подразделений ОВД при выявлении и раскрытии преступлений.

УДК 343

В.Д. Гущина, Р.В. Глубоковских

ИСПОЛЬЗОВАНИЕ ДРОНОВ И ДРУГИХ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ДЛЯ НАБЛЮДЕНИЯ И СБОРА ИНФОРМАЦИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Дроны и сходные беспилотные летательные аппараты на данный момент являются достаточно распространенным оборудованием. С их помощью можно проводить наблюдение, собирать информацию об объектах и реализовывать иные действия. Это ведет к значимости дронов для многих

сфер деятельности человека, оперативно-розыскная деятельность (ОРД) не стала исключением. На данный момент правоохранительные органы недостаточно используют указанную технологию, что уменьшает эффективность проведения ОРД. Исходя из этого, актуально поднимать подобную тему, а также предоставлять практические рекомендации.

Первоначально требуется доказать, что дроны положительно влияют на проведение ОРД. Один из видов ОРД – это наблюдение, в его рамках дроны увеличивают эффективность мероприятия, так как, во-первых, позволяют осуществить меру максимально быстро. Причина заключается в высокой скорости полета дрона, которая значительно превышает скорость движения человека. Сравнивая оперативность достижения необходимой точки между разным оборудованием, вновь указываем на преимущество дрона, так как он перемещается по воздушному пространству, следовательно, препятствия для его движения минимальны.

Последний пункт требует выделения второй причины – дрон способен осуществить визуальное наблюдение за объектом там, где это было бы невозможно для оперативных работников. Примером является частная и (или) огороженная территория. Для того чтобы незаметно проникнуть на нее, сотрудникам придется реализовать сложные манипуляции, в некоторых случаях это в целом будет невозможно.

В-третьих, перемещение дрона по воздушному пространству однозначно ликвидирует проблему труднодоступных и труднопроходимых мест. Такое устройство беспрепятственно позволит осуществлять наблюдение, реализовать действие скрыто, что крайне значимо для получения наиболее ценных сведений.

В-четвертых, дроны могут быть оснащены различным оборудованием, которое упрощает процесс наблюдения. Так, например, тепловые датчики позволят максимально оперативно идентифицировать лицо, появившееся на определенной территории. Это ведет к тому, что наблюдение за местом становится максимально эффективным. Более того, современные дроны могут быть оснащены камерами, распознающими лица. В результате процесс идентификации определенного гражданина в рамках наблюдения за объектом происходит с максимальной точностью и скоростью. Необходимо согласиться, что камеры видеонаблюдения тоже могут иметь функцию распознавания лиц, однако оператор дрона в каждой ситуации может выбрать такой ракурс, который будет наиболее значим, – камера видеонаблюдения в большинстве случаев стационарна, следовательно, результативность не всегда является максимальной.

В рамках процесса сбора информации дроны позволяют получить аналогичные преимущества, как и при ОРД вида наблюдение – беспилотный летательный аппарат наиболее оперативно позволяет изучить местность, идентифицировать личность на объекте, при этом не возникнет проблем с препятствиями и сложностью ландшафта. Однако сбор информации является крайне широким понятием, потому выгода от использования дронов здесь больше. Так, например, собирая сведения о территории или местности с помощью беспилотного летательного аппарата, оператор получает ценные сведения, позволяющие оперативным работникам с минимальным ущербом провести иную ОРД. Скорость и простота перемещения, доступные лишь летательным устройствам, позволяют максимально быстро достичь точки, получив максимально оперативные и полные сведения о нужном объекте или лице.

Представленные аргументы позволяют однозначно констатировать, что дроны и сходные беспилотные летательные устройства должны применяться в рамках ОРД. Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ (ред. от 29 декабря 2022 г.) «Об оперативно-розыскной деятельности» не имеет ограничений по применению дронов, следовательно, вопрос правового регулирования является относительно решенным.

При этом проблемными являются иные аспекты. Во-первых, лишь незначительное количество территориальных подразделений Министерства внутренних дел Российской Федерации (далее – МВД России) имеют в распоряжении даже один дрон. Это ведет к объективной материальной невозможности использования подобного оборудования. Во-вторых, частое отсутствие нужных кадров. Даже если подразделению был выделен дрон, не всегда в его рамках есть служащий, умеющий результативно использовать его на практике.

Практические решения данных проблем, на наш взгляд, следующие. Требуется сформировать распоряжение, в рамках которого каждое территориальное подразделение МВД России получит минимум один дрон в пользование. Предлагаем сформировать некую классификацию подразделений, исходя из численности населения, которое входит в его юрисдикцию. Такая группировка позволит определить, какое количество беспилотных летательных аппаратов должно получить каждое подразделение. Далее, после определения значения, рекомендуем обязать каждое подразделение направить минимум двух сотрудников (на одну единицу техники), которые пройдут курсы по управлению дронами, уже реализуемые МВД России. При этом пропорцию два сотрудника на одну единицу техники в обязательном порядке необходимо сохранять, следовательно, нужно контролировать возможный отток кадров.

В заключение констатируем, что дроны и сходные беспилотные летательные аппараты позволяют значительно улучшить проведение ОРД вида наблюдение, сбор информации, а также иные. Несмотря на этот факт, на данный момент подобное оборудование не является активно используемым в ОРД. Ключевые причины ситуации были выявлены, их можно решить путем применения предложенных практических рекомендаций. По этой причине их требуется изучить на аспект использования.

УДК 343.3

М.С. Дзырук, А.Ю. Медведева

ОПЕРАТИВНО-РОЗЫСКНОЕ МЕРОПРИЯТИЕ «НАВЕДЕНИЕ СПРАВОК» – ПРЕДЛОЖЕНИЯ ПО РАСШИРЕНИЮ ЕГО ВОЗМОЖНОСТЕЙ

Сегодня невозможно представить современное общество без передовых технологий, функционирующих на рубеже научных разработок. Технологии и техника, отвечающие на вопросы, чем и как достигается результат деятельности человека, играют существенную роль и оказывают сильное влияние на различные стороны общества и государства. Одной из таких сторон является безопасность государства и всех его составных элементов.

Безопасность во всех ее проявлениях должна обеспечивать такое состояние, при котором государство, человек и его интересы будут чувствовать себя вне угроз. Так, функции по обеспечению вышеуказанного состояния возлагаются, в том числе, на оперативно-розыскные подразделения. При выполнении задач оперативно-розыскной деятельности (ОРД) оперативные сотрудники уполномочены проводить различные оперативно-розыскные мероприятия (ОРМ), закрепленные в Федеральном законе Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

В условиях современной вовлеченности людей в информационную среду (социальные сети, получение услуг посредством интернет-трафика и т. д.) можно говорить, что практически любой человек оставляет, как фон своей повседневной деятельности, различные цифровые следы. В настоящее время российским законодательством предусмотрена возможность получения характеризующей информации, в том числе из баз данных, в рамках проведения ОРМ «Наведение справок». Процесс получения информации понятен и подразумевает наличие у оперативника первичной информации, для пополнения и проверки которой он

с помощью оформления запросов и доступа, к имеющимся в оперативно-розыскном органе баз данных, истребует специфическую или общеуголовную информацию. В данном процессе возможно решение изначальных целей, поставленных оперативником, но при этом, при описанном подходе, информацию оперативник может получить только в отношении гражданина Российской Федерации или иного лица, когда они либо привлекались к какой-то ответственности, или являлись получателями особо учитываемых услуг (лицензирование гражданского оружия, получение водительского удостоверения и т. п.), либо стояли на учете в каком-либо органе.

Если мы говорим о людях, которые не подпадают под какую-либо из названных категорий (например, трудовые мигранты, в том числе находящиеся на территории государства нелегально), то значимой информации по ним оперативные сотрудники получить не смогут. В этой связи считаем, что ОРМ «Наведение справок» может быть актуализировано для получения возможности сбора максимально полной информации из открытых источников (использование OSINT и GEOINT). При этом для применения возможностей использования OSINT и GEOINT оперативно-розыскной орган должен располагать программным комплексом отечественной разработки (аналог «Глаз Бога», «Вектор», «Химера»), который может быть использован оперативным сотрудником по согласованию с начальником оперативно-розыскного органа для исключения возможности использования получаемой таким образом информации в личных целях и нарушения прав третьих лиц.

Использование технологий OSINT и GEOINT подразумевает возможность осуществления электронной разведки (оперативного поиска) по открытым источникам информации (социальные сети, номера телефонов, аккаунты, обращения и т. д.). Доступ к данной информации часто невозможен, в рамках стандартного проведения ОРМ «Наведение справок» в отношении лица, обладающего минимальным количеством цифровых и юридических следов. Стоит отметить, что наиболее актуально использовать OSINT и GEOINT в отношении лиц, проверяемых по подозрению в совершении преступлений против основ конституционного строя и безопасности Российской Федерации (государственная измена, организация экстремистского сообщества, диверсия, шпионаж и т. п.).

Приведем два примера, в которых стандартное проведение ОРМ «Наведение справок» без использования технологий OSINT и GEOINT будет менее информативным:

1) условная ситуация, в которой лицо, подозреваемое в совершении преступления, прибыло с территории Европейского союза, ранее на

территории Российской Федерации не находилось. Объем информации, полученный при ОРМ «Наведение справок», будет заметно меньше, чем при использовании технологий OSINT и GEOINT, которые позволят получить в том числе информацию из открытых источников за время нахождения человека в других государствах;

2) условная ситуация, в которой лицо, подозреваемое в совершении преступления, прибыло как трудовой мигрант официальным путем на территорию Российской Федерации, при том, что с конца 2024 г. по февраль 2025 г. находилось на территории Ближнего Востока, где принимало участие в боевых действиях, как член одной из запрещенных на территории Российской Федерации группировок (ИГ, ХТШ и т. п.). В этом случае также необходимо применить расширенные возможности разведки информации по открытым источникам, которая не будет ограничена регионом пребывания.

Важно отметить, что использование технологий OSINT и GEOINT, а также разработка и использование программного обеспечения позволят своевременно выявлять лиц, представляющих оперативный интерес, основная компрометирующая информация о которых может быть получена только при использовании электронной разведки данных из открытых источников (особенно это касается лиц, прибывших из иностранных государств, что в принципе может свидетельствовать о возможности использования данных технологий как профилактики проявлений терроризма, экстремизма и иных покушений на государственный строй и общественную безопасность Российской Федерации).

УДК 343.985

А.В. Есько, А.В. Яскевич

ТАКТИЧЕСКИЕ КОМБИНАЦИИ В ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

В настоящее время в процессе раскрытия и расследования преступлений сформировался четкий алгоритм, который включает в себя комплекс оперативно-розыскных мероприятий и следственных действий, направленных на всестороннее, полное и объективное проведение предварительного расследования, однако часто определенное количество преступлений остаются нераскрытыми в связи с применением преступниками изощренных способов и методов сокрытия следов их противоправной деятельности. В то же время лица, совершающие преступления, в определенной степени осведомлены о приемах и методах, используемых сотрудниками правоохранительных органов в процессе расследования преступлений. Подобная осведомленность побуждает преступников оказывать противодействие расследованию, а также маскировать следы противоправной деятельности.

Преодолеть подобное противодействие исключительно посредством проведения следственных действий часто затруднительно, в связи с чем представляется необходимым применение тактических комбинаций при организации раскрытия и расследования преступлений.

Тактическая комбинация представляет собой комплексное сочетание тактических приемов и комбинаций, проводимых с целью решения конкретных задач расследования и обусловленных сложившейся следственной ситуацией. Совместное проведение следователем с оперативным сотрудником тактической комбинации создает условия для получения информации, которая может иметь ключевое значение для расследования уголовного дела и выявления новых эпизодов преступной деятельности.

Информация, полученная в результате тактической комбинации, может быть использована для организации планирования следственных действий, определения последовательности их проведения, выбора наиболее эффективной тактики проведения, совершенствования методики расследования и др.

Проведение тактической комбинации в комплексе со следственными действиями и оперативно-розыскными мероприятиями позволяет установить обстоятельства преступления, добыть информацию, которую следственным путем получить было бы невозможно. В случаях когда в процессе расследования преступления установлены лица, причастные к его совершению, но собрать достаточные доказательства их вины не представляется возможным, целесообразно проведение тактических комбинаций с использованием легендирования, дезинформирования и инсценирования.

Легендирование в криминалистике представляет собой тактический прием, основанный на распространении заведомо ложных сведений об отдельных обстоятельствах с целью дезинформирования противодействующей стороны. Использование легендирования в сочетании с оперативно-розыскными мероприятиями и иными организационными мерами образует простую тактическую комбинацию. Применение легенды позволяет сотрудникам правоохранительных органов скрыть истинные цели своей деятельности, а также дезинформирует лиц, противодействующих расследованию.

Следует отметить, что при проведении тактической комбинации с использованием легендирования, дезинформирования и инсценирования определенных событий за лицом, в отношении которого осуществляются данные действия, всегда сохраняется право выбора определенной линии поведения и тактики принятия решений.

Для успешного проведения тактической комбинации следователю и оперативному сотруднику требуется предварительно установить и проанализировать имеющуюся информацию о лице, в отношении которого планируется ее проведение. Совместная работа следователя и оперативного сотрудника при разработке тактической комбинации создает основу для их эффективного взаимодействия в процессе дальнейшего расследования уголовного дела, т. е. обеспечивает его оперативно-розыскное сопровождение.

Дезинформировать значит ввести лицо в заблуждение, используя заведомо ложные сведения. Цель дезинформирования заключается в побуждении человека к принятию ошибочных решений, формируя искаженное представление о степени доказанности его вины, а также собранных по уголовному делу доказательств.

Дезинформирование лица может осуществляться следующими способами: ограничение доступа к достоверной информации; создание искусственной неосведомленности относительно истинного положения вещей; предоставление заведомо ложных сведений, побуждающих к проявлению саморазоблачающей деятельности. Стоит учесть, что применять тактические комбинации с использованием дезинформирования наиболее эффективно в отношении лиц, склонных к даче заведомо ложных показаний.

Достаточно часто одного легендирования для введения в заблуждение противодействующей стороны недостаточно. В таких случаях следует легендирование подкрепить инсценированием, которое представляет собой тактический прием, основанный на искусственном создании обстановки, побуждающей лицо к определенным действиям. Проведение тактической комбинации с использованием легендирования и инсценировки позволяет выявить истинные намерения и причастность лица к совершению преступления. Метод инсценировки широко используется в оперативно-розыскной деятельности при проведении таких оперативно-розыскных мероприятий, как «контролируемая поставка», «оперативный эксперимент» и др.

Таким образом, можно прийти к выводу, что комплексное проведение следственных действий и оперативно-розыскных мероприятий в сочетании с тактическими комбинациями позволит достичь максимальной эффективности в противодействии преступности.

УДК 343.811-055.2

Е.О. Есютина, Р.В. Глубоковских

КИБЕРБЕЗОПАСНОСТЬ ЧЕРЕЗ ПРАКТИКУ: РАЗВИТИЕ НАВЫКОВ РАССЛЕДОВАНИЯ В УСЛОВИЯХ ЦИФРОВЫХ УГРОЗ

Современное общество столкнулось со стремительной трансформацией криминальных угроз, которые, в свою очередь, обусловлены резким развитием цифровых технологий во всех сферах жизнедеятельности человека. Статистические данные, представленные официальным представителем Министерства внутренних дел Российской Федерации Ириной Волк, свидетельствуют о критическом росте доли преступлений, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ). Так, в 2024 г. 40 % от общего числа зарегистрированных в России преступлений были связаны с ИТТ, что на 13,1 % превышает аналогичный показатель 2023 г. Данная тенденция сопровождается увеличением доли на 7,8 % тяжких и особо тяжких составов в структуре киберпреступности, что напрямую повлияло на рост в 4,8 % общего числа указанной категории деяний в годовом исчислении. Стоит также подчеркнуть, что общее снижение уровня преступности на 1,8 % лишь подчеркивает его структурный сдвиг в сторону криминализации цифрового пространства.

Представленная динамика требует переосмысления традиционных подходов к расследованию и доказыванию в рамках уголовного судопроизводства. Рост IT-преступлений коррелирует с усложнением их технической базы: использование криптовалют, анонимизирующих сетей, методов социальной инженерии и вредоносного программного обеспечения формирует принципиально новые вызовы для правоохранительной системы.

Правоохранительные органы нуждаются в более качественных и современных образовательных программах, которые позволят освоить на достаточно высоком уровне навыки по работе с IT-преступлениями. Считаем, что для эффективного осуществления профессиональной деятельности, направленной на раскрытие и расследование преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, сотруднику полиции необходимо обладать комплексом компетенций, интегрирующих технические, криминалистические, правовые и аналитические аспекты.

Основу составляет правовая компетенция, которая подразумевает строгое следование нормам законодательства в сфере противодействия ки-

берпреступности, регламентов получения судебных решений на изъятие данных. Ключевое значение имеет соблюдение процессуальных норм при оформлении доказательственной базы, включая документирование цепочки хранения и защиты цифровых активов для обеспечения ее неизменности и соответствия критериям допустимости в судебном производстве.

Вместе с этим важна аналитическая компетенция, которая представляет собой системный подход к расследованию преступлений: реконструкцию цепочки кибератаки, выявление корреляций в больших массивах данных (с применением методов машинного обучения) и визуализацию результатов. Критическое мышление необходимо для формирования и верификации гипотез на основе косвенных улик, таких как аномалии в сетевом трафике или транзакциях с криптовалютой.

Считаем также необходимым внедрить в учебный процесс курсантов образовательной системы Министерства внутренних дел интерактивную платформу, основанную на разработке деловой игры «Мошенничество, совершенное с использованием социальных сетей», с целью формирования комплексных навыков раскрытия IT-преступлений. Данная инициатива направлена на интеграцию инновационных образовательных технологий, сочетающих элементы визуальной новеллы, квеста и симуляции расследования, что позволяет моделировать реалистичные сценарии киберпреступлений в контролируемой виртуальной среде.

Основой платформы выступает имитация уголовного процесса, где курсанты выполняют роль оперативных сотрудников и следователей, осуществляющих сбор цифровых доказательств, анализ данных (включая IP-адреса, информацию из социальных сетей), взаимодействие с виртуальными свидетелями и подозреваемыми, а также принятие процессуальных решений (вызов на допрос, согласование обысков, формулирование обвинений). Это способствует закреплению знаний в области уголовного права и процесса, оперативно-розыскной деятельности, а также развивает компетенции в области цифровой криминалистики.

Предлагаемая интерактивная образовательная платформа предусматривает детальную имитацию работы с цифровыми данными, что является ключевым элементом формирования профессиональных компетенций курсантов в области раскрытия IT-преступлений. В рамках игрового сценария обучающиеся получают доступ к структурированным массивам информации, представленным в формате таблиц, что соответствует реальным процессам оперативно-розыскной деятельности.

Работа с IP-адресами реализуется через интерактивные модули, где курсанты анализируют таблицы, содержащие данные о сетевых активностях подозреваемых. Например, в ответ на виртуальный запрос к

интернет-провайдеру игрок получает таблицу с IP-адресами, временными метками и географической привязкой. Задача заключается в сопоставлении этих данных с действиями мошенника в социальной сети «ВКонтакте»: установление совпадений времени публикации фишинговых сообщений и активностей на конкретных IP-адресах, определение локации устройства, выявление использования анонимайзеров или VPN-сервисов. Инструменты фильтрации и сортировки позволяют выделять подозрительные паттерны, например, частую смену адресов, что может указывать на попытку сокрытия следов.

Анализ банковских транзакций интегрирован в сюжетную линию через имитацию запросов в финансовые учреждения. Курсанты получают таблицы с детализацией денежных потоков: номера счетов, суммы, даты операций, реквизиты отправителей и получателей. Например, в рамках расследования мошенничества игрок отслеживает переводы с компрометированных счетов потерпевших на счета подставных лиц. Задача включает в себя выявление цепочек транзакций, связывающих фиктивные аккаунты в социальных сетях с реальными банковскими операциями, определение схемы отмывания средств или идентификацию конечных бенефициаров. Для усиления реалистичности в таблицы внедряются типовые аномалии: микроплатежи для проверки карт, повторяющиеся переводы на одни и те же счета, операции в нерабочее время.

Интеграция данных в процессуальный контекст обеспечивается через систему принятия решений. Например, корректное сопоставление IP-адреса с геолокацией позволяет игроку обосновать ходатайство о проведении обыска по месту жительства подозреваемого. Анализ банковских таблиц становится основанием для вызова на допрос владельца счета или блокировки транзакций. Ошибки в интерпретации данных (например, игнорирование временного разрыва между активностью в социальной сети и транзакцией) приводят к сюжетным последствиям: отказу суда в санкции на обыск или утечке доказательств.

Данная платформа не только тренирует технические навыки работы с цифровыми данными, но и формирует понимание их процессуальной значимости. Курсанты учатся преобразовывать сырые данные (IP-адреса, транзакции) в юридически значимые доказательства, аргументировать свои решения в рамках уголовного дела и соблюдать нормы цифровой этики, что критически важно для их будущей профессиональной деятельности в условиях цифровизации преступности.

Таким образом, совершенствование методик расследования, внедрение специализированных образовательных программ для сотрудников правоохранительных органов становятся императивом для противодей-

ствия цифровой преступности. Игнорирование данной проблематики может привести к дальнейшей эскалации угроз, подрывающих доверие граждан к государственным институтам и стабильности правопорядка в условиях технологической революции.

УДК 334.78

В.В. Ефимович

МЕТОДИКА ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ИНТЕГРИРОВАННЫХ СТРУКТУР В ПЕРИОД ТРАНСФОРМАЦИИ ЭКОНОМИКИ

Оценка эффективности интегрированных структур с учетом эффективности интеграции представляет собой сравнительно малоисследованную область, но важную для развития крупных корпоративных структур, поскольку позволяет минимизировать риски, оптимизировать связи между отдельными предприятиями. Кроме того, отдельные элементы данной методики могут быть использованы подразделениями по борьбе с экономическими преступлениями Министерства внутренних дел и подразделениями Департамента финансовых расследований Комитета государственного контроля в оперативно-розыскной деятельности для выявления правонарушений, допускаемых субъектами хозяйствования.

Что касается эффекта интеграции, то отметим, что суть вертикальной и горизонтальной интеграции отличается, поэтому и оценивать их необходимо по-разному.

Оценить эффект масштаба за счет снижения постоянных расходов можно следующим образом:

$$Эм = \sum_{i=1}^{n} (Д_{пост_i} - Д_{пост_0}) \cdot S_i,$$

где n – количество лет, прошедших с момента интеграции; 0 – год перед интеграцией; $Д_{пост}$ – доля постоянных издержек в затратах на производство продукции; S – совокупная себестоимость произведенной продукции однопрофильных предприятий интегрированной структуры.

Помимо экономии на постоянных затратах эффект горизонтальной интеграции может проявиться в маркетинге, совершенствовании управления, специализации на выпуске одного или нескольких видов продукции. Специализация приводит к повышению производительности труда, которая выражается глубиной переработки сырья и может быть оценена как рост выпуска товарной продукции из тонны сырья:

$$Эс = \sum_{i=1}^{n} (ТП_i - ТП_0) \cdot Ос_i,$$

где Эс – эффект специализации; ТП – величина выпуска товарной продукции из тонны сырья; Ос – объем сырья, используемый для производства продукции однопрофильными предприятиями холдинга.

Объединение предприятий в интеграционную структуру позволяет более полно использовать возможности коммерческих служб. В первую очередь это относится к возможности реализации продукции всех объединившихся предприятий одного профиля под брендом, имеющимся у одного из предприятий, чаще всего управляющей компании горизонтально интегрированного объединения.

Оценивать эффект передачи бренда (Эб) предлагаем по формуле:

$$Эб = \sum_{i=1}^{n} К_{рекл_i} \cdot S_{р_i},$$

где $К_{рекл}$ – доля затрат на рекламу в выпуске продукции предприятия-создателя бренда; $S_р$ – себестоимость реализованной продукции предприятий-реципиентов бренда.

Реализация продукции под уже признанным на рынке брендом позволяет интегрированной структуре за счет продукции дочерних предприятий расширять рынки сбыта. Очевидно, что наиболее выгодна эта ситуация в случае, если цены новых рынков выше цен, по которым реализовывается продукция на прежних рынках. Величина эффекта расширения зон поставки (Эп) определяется как количеством продукции, поставляемой на новые, открывшиеся в связи с интеграцией, рынки, так и разницей в ценах новых и прежних рынков.

$$Эп = \sum_{i=1}^{n} \sum_{j=1}^{m} (Цп_{ij} - Цн_{ij}) \cdot Ор_{ij},$$

где m – количество видов продукции, которые после интеграции стали продаваться на новом рынке; Цп, Цн – цена реализации j-ого вида продукции на привычном и новом рынке; Ор – объем реализации j-ого вида продукции на новом рынке в i-м году в натуральном выражении.

Таким образом, совокупный эффект от горизонтальной интеграции может быть рассчитан как сумма эффектов масштаба, специализации, использования бренда и расширения зон поставки:

$$\overline{Э} = Эм + Эс + Эб + Эп.$$

Если горизонтальная интеграция означает объединение предприятия одного профиля, то вертикальная интеграция означает объединение предприятий, осуществляющих последовательные стадии единого цикла производства.

Величину эффекта трансфертных цен (Эц) определяем по формуле:

$$Эц = \sum_{i=1}^{n} \sum_{j=1}^{k} (Цр_{ij} - Цт_{ij}) \cdot Опр_{ij} \cdot Кнал_i,$$

где k – количество видов продукции, передаваемых по трансфертным ценам; Цр, Цт – размер рыночной и трансфертной цены j-ого вида продукции; Опр – объем передачи j-ого вида продукции между предприятиями холдинга в натуральном выражении; Кнал – доля налоговых платежей от выручки и прибыли предприятия, передающего продукцию по трансфертным ценам, в объеме выручки от реализации в i-м году.

Эффект экономии трансакционных издержек может быть определен следующим образом:

$$Эи = \sum_{i=1}^{n} Кпер_i \cdot РР_i \cdot (Ор_{Д_i} / Ор_{Х_i}),$$

где Кпер – доля передаваемой продукции предприятия более низкого уровня передела на более высокий уровень передела в объеме реализации продукции предприятия, передающего продукцию; РР – расходы на реализацию по интегрированной структуре в целом; $ОР_Д$ – объем реализации передающего предприятия; $ОР_Х$ – объем реализации интегрированной структуры в целом.

Эффект совершенствования системы управления качеством может быть определен следующим образом:

$$Эк = \sum_{i=1}^{n} \Delta П_{пп_i} + Овк_i \cdot \Delta Ц_i,$$

где $\Delta П_{пп}$ – изменение размера потерь, связанных с недостаточным качеством промежуточной продукции, млн р.; Овк – объем продукции, производимой из сырья более высокого качества, т; ΔЦ – изменение цены на продукцию, вызванное использованием сырья более высокого качества, млн р./т.

Совокупный эффект вертикальной интеграции определяется как сумма эффектов трансфертных цен, экономии транзакционных издержек и совершенствования системы управления качеством:

$$Э\Big| = Эц + Эи + Эк.$$

Для оценки эффективности интеграции (Эинт) следует сравнить совокупный эффект от интеграции с затратами собственника на его создание и поддержку (Зс):

$$Эинт = \frac{\overline{Э} + Э\Big|}{Зс}.$$

Такой подход позволяет получить комплексную картину экономической обоснованности создания интегрированной структуры, поскольку оценивает окупаемость затрат на создание и поддержание деятельности интегрированной структуры.

УДК 343.91

О.В. Ивушкина

О НЕКОТОРЫХ ВОПРОСАХ СОВЕРШЕНСТВОВАНИЯ ПРОФИЛАКТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Роль профилактики правонарушений, осуществляемой органами внутренних дел, является одним из важных и необходимых направлений в деятельности государства.

Определяя задачи Правительственной комиссии по профилактике правонарушений, министр внутренних дел Российской Федерации В.А. Колокольцев подчеркивает, что они должны быть направлены в первую очередь на выработку решений и координацию организационно-практических мероприятий в рамках государственной системы профилактики правонарушений, направленных на активизацию борьбы с пьянством, алкоголизмом, наркоманией, незаконной миграцией, ресоциализацию лиц, освободившихся из мест лишения свободы, и других мер, направленных на снижение уровня преступности на территории Российской Федерации.

В настоящее время, находясь на самом острие решения социальных проблем, профилактическая деятельность совершенствуется, обогащается опытом.

К основным направлениям дальнейшего повышения эффективности профилактической деятельности, на наш взгляд, следует отнести:

совершенствование системы и методов управления;

развитие правовой основы деятельности профилактического направления;

совершенствование структуры, уточнение функций и обязанностей субъектов профилактики;

наиболее оптимальное решение организационно-штатных вопросов, сбережение профессионального кадрового «ядра» в органах внутренних дел;

укрепление взаимодействия с различными службами органов внутренних дел;

организация взаимодействия граждан с органами государственной власти в целях повышения уровня безопасности жизни и др.

Масштабность и сложность задач, решаемых субъектами профилактики, предъявляют все возрастающие требования к подбору, расстановке и воспитанию кадров. Вместе с тем качественный состав участковых уполномоченных улучшается медленно, присутствует большая текучесть данной категории сотрудников. Так, например, нехватка участковых уполномоченных в полиции за год увеличилась на десятую часть от общего штата и в настоящее время в среднем по субъектам составляет

от 30 % до 45 %. В 39 из 96 территориальных органов не хватает более 20 % сотрудников. В некоторых подразделениях ряда регионов некомплект достигает 40 %. Некомплект аттестованного состава в уголовном розыске составляет 23,9 %, в патрульно-постовой службе – 31,4 %, в подразделениях по контролю за оборотом наркотиков некомплект персонала достиг 24,7 %, в органах предварительного следствия – 22,7 %.

С целью сохранения профессионального кадрового ядра необходимо эффективнее использовать возможности образовательных организаций Министерства внутренних дел Российской Федерации, расширять курсы профессиональной подготовки и переподготовки, повышать качество первоначальной подготовки. Как показывает практика, далеко не каждый сотрудник, получивший специальное образование, и даже имеющий практический опыт, не всегда может успешно проводить профилактические мероприятия.

Решение сложных и ответственных задач по совершенствованию профилактической деятельности невозможно без четкого всестороннего взаимодействия со всеми службами и подразделениями органов внутренних дел, так как требуют комплексного подхода.

Организация эффективной предупредительной деятельности немыслима и без глубокого научного подхода. Необходимо продолжать разрабатывать основополагающие документы в вопросах профилактики правонарушений, методических рекомендаций, внедрение которых должно иметь большое практическое значение, а также осуществлять целый комплекс специальных мер, обеспечивающих перевоспитание правонарушителей (например, таких как психолого-реабилитационных, правоохранительных, политико-правовых, междисциплинарных и иных мер).

Что касается основных превентивных направлений в вопросах совершенствования профилактической деятельности, то, на наш взгляд, они должны заключаться в следующем:

разработка и внедрение адресных профилактических мер, ориентированных на группы риска, с учетом выявленных характеристик личности преступников;

применение современных психокоррекционных методик, направленных на снижение агрессивности, развитие эмоциональной саморегуляции и эмпатии у лиц, склонных к насилию;

организация социальных служб для работы с неблагополучными семьями, молодежью из групп риска, ресоциализация лиц, освобожденных из мест лишения свободы;

изучение влияния новых социальных факторов, исследование воздействия цифровой среды, социальных сетей, информационных технологий;

проведение междисциплинарных исследований, объединение усилий криминологов, психологов, социологов, педагогов для глубокого понимания феномена преступности;

анализ эффективности реализуемых профилактических мер, проведение эмпирических исследований по оценке действенности различных программ профилактики и реабилитации с целью их оптимизации.

Развитие данных превентивных направлений позволит не только углубить теоретические знания о личностных характеристиках преступника, но и повысить эффективность практических мер по дальнейшему предупреждению преступности, что в конечном итоге будет способствовать укреплению общественной безопасности и правопорядка.

Несмотря на то что основы системы профилактики правонарушений, общие правила ее функционирования, основные принципы, направления, виды профилактики правонарушений и формы профилактического воздействия регламентируются Федеральным законом Российской Федерации от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», все же имеются существенные пробелы как в правовой регламентации конкретных профилактических мероприятий, так и в нормативном закреплении и регулировании применяемых профилактических мер. Придавая важное значение вопросам совершенствования профилактической деятельности, в настоящее время введен в действие ряд нормативных актов, регламентирующих профилактическую деятельность. Четкое их выполнение будет, несомненно, способствовать дальнейшему организационному совершенствованию и активизации всех сторон профилактической деятельности органов внутренних дел.

Именно сейчас необходимо возродить и усовершенствовать систему предупреждения и профилактики преступлений, которая способна, на опережение, обеспечить нормальную жизнедеятельность общества, снижая статистические показатели по преступности.

УДК 34.03

Г.А. Казакевич

РЕСПУБЛИКАНСКАЯ СИСТЕМА МОНИТОРИНГА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ КАК ИНСТРУМЕНТ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Развитие республиканской системы мониторинга общественной безопасности берет свое начало с момента вступления в силу Указа

Президента Республики Беларусь от 25 мая 2017 г. № 187 «О республиканской системе мониторинга общественной безопасности» (далее – Указ № 187, система мониторинга, РСМОБ). До этого момента в стране имелось значительное количество разрозненных камер и систем наблюдения, выполнявших лишь обзорную функцию. Использование таких камер и систем для решения задач оперативно-розыскной деятельности было крайне затруднено.

Приоритетными функциями системы мониторинга определены: наблюдение за состоянием общественной безопасности в целях обеспечения общественного порядка, профилактики, выявления (раскрытия) и пресечения правонарушений; расследование преступлений, розыск лиц, их совершивших, и лиц, без вести пропавших; предупреждения и ликвидации чрезвычайных ситуаций, а также оперативное информирование о зафиксированных событиях.

Задача решалась путем построения новых, объединения и модернизации существующих систем видеонаблюдения в единую интегрированную интеллектуальную платформу безопасности. Однако и до подписания Главой государства Указа № 187 в стране принимались нормативные правовые акты (НПА), определяющие подходы к обеспечению общественной безопасности с использованием видеонаблюдения. Одним из первых таких НПА стало Положение о применении систем безопасности и систем видеонаблюдения, утвержденное постановлением Совета Министров Республики Беларусь от 13 декабря 2012 г. № 1135 «Об утверждении Положения о применении систем безопасности и систем видеонаблюдения».

Дальнейшее развитие правовое регулирование порядка внедрения и развития системы видеонаблюдения получило в связи с принятием 28 ноября 2013 г. Указа Президента Республики Беларусь № 527 «О вопросах создания и применения системы видеонаблюдения в интересах обеспечения общественного порядка» (далее – Указ № 527), во многом приуроченное к проведению в 2014 г. в г. Минске чемпионата мира по хоккею.

Согласно Указу № 527 в республике создавалась система видеонаблюдения за состоянием общественной безопасности, состоящая из средств системы видеонаблюдения, каналов связи, используемых для передачи зафиксированной информации, оборудования, используемого для приема, обработки и хранения зафиксированной информации, и иного оборудования, применяемого для обеспечения функционирования системы видеонаблюдения. Указом № 527 также определялись объекты инфраструктуры, используемые при проведении чемпионата мира по хоккею, и общественные места г. Минска, которые до 1 марта 2014 г. подлежали обязательному оборудованию средствами системы видеонаблюдения.

В развитие Указа № 527 Советом Министров Республики Беларусь 30 декабря 2013 г. издано постановление № 1164 «Об утверждении критериев отнесения объектов к числу подлежащих обязательному оборудованию средствами системы видеонаблюдения за состоянием общественной безопасности», которым закреплены параметры отнесения объектов к числу подлежащих в обязательном порядке оборудованию средствами видеонаблюдения (места для проведения массовых мероприятий, места с возможностью единовременного пребывания в них 100 и более человек, гостиницы, общежития, въезды и выезды в г. Минск, административные центры областей и районов; стационарные торговые объекты, зрелищные объекты; объекты транспортной инфраструктуры; учреждения образования и здравоохранения).

Указом № 187 Министерство внутренних дел Республики Беларусь (МВД) определено специально уполномоченным государственным органом, осуществляющим координацию деятельности пользователей, иных организаций и индивидуальных предпринимателей при создании, функционировании и использовании системы мониторинга.

Подключение системы видеонаблюдения, локальных систем видеонаблюдения к системе мониторинга и обмен данными осуществлялось с использованием каналов связи единой республиканской сети передачи данных.

В качестве дополнительного участника правоотношений, связанных с порядком функционирования РСМОБ, вводилось понятие технического оператора системы мониторинга, нормативно закреплялись его права и обязанности, которыми, в том числе являлись создание, развитие и техническая эксплуатация программной платформы системы мониторинга, использование в системе мониторинга программного обеспечения видеоаналитики и т. п.

10 ноября 2017 г. Советом Министров Республики Беларусь издано постановление № 841 «Об утверждении Положения о республиканской системе мониторинга общественной безопасности и порядке подключения к ней».

Основным элементом созданной в соответствии с Указом № 187 системы мониторинга являлась программная платформа – «Система мониторинга общественной безопасности «Кипод», которая включала в себя комплекс программных модулей обработки видеопотоков и данных от системы видеонаблюдения, средства поиска объектов и событий в больших массивах видео, модули видеоаналитики, средства разграничения доступа и информационной безопасности, сервисы уведомлений пользователей.

Однако, несмотря на принятые меры, развитие системы мониторинга осуществлялось явно замедленными темпами. Так, по состоянию на 1 января 2021 г. по республике обязательному оборудованию средствами системы видеонаблюдения подлежало более 10 тыс. объектов, из которых к системе мониторинга был подключен всего 41, или менее 1 % (по состоянию на 1 августа 2022 г. – 66 объектов (в подавляющем большинстве в г. Минске) – 1 130 видеокамер (станции Минского метрополитена, автовокзал «Центральный», Комаровский рынок, пять АЗС «Белоруснефть», пять торговых центров, общественные места столицы).

Для исправления ситуации по инициативе МВД и на основе предложений межведомственной рабочей группы принято решение по созданию принципиально новой модели построения системы, оператором которой определено РУП «Белтелеком». Принятие такого решения нашло свое отражение в Указе Президента Республики Беларусь от 25 февраля 2022 г. № 69 «О развитии республиканской системы мониторинга общественной безопасности» (далее – Указ № 69), в соответствии с которым РСМОБ стала закрытой системой, предусматривающей наличие доступа к ней только государственных органов – пользователей системы мониторинга (пользователями системы мониторинга являются органы прокуратуры, Служба безопасности Президента Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, органы финансовых расследований Комитета государственного контроля, Следственный комитет, органы внутренних дел, органы и подразделения по чрезвычайным ситуациям, органы государственной безопасности, органы пограничной службы, таможенные органы).

В развитие Указа № 69 Советом Министров Республики Беларусь принято постановление № 551 «О реализации Указа Президента Республики Беларусь от 25 февраля 2022 г. № 69», которым утверждено Положение о порядке определения экономически обоснованных затрат стоимости работ (услуг) по содержанию и эксплуатации республиканской системы мониторинга общественной безопасности с учетом рентабельности, установлен ежемесячный размер стоимости работ (услуг) по содержанию РСМОБ, количество подлежащих подключению элементов системы мониторинга, а также порядок осуществления компенсации расходов республиканского бюджета на финансирование таких работ (услуг) организациями и индивидуальными предпринимателями, в собственности, оперативном управлении или хозяйственном ведении которых находятся объекты (места установки), подлежащие оборудованию средствами элементов системы мониторинга.

Создание системы мониторинга осуществляется за счет собственных средств РУП «Белтелеком». МВД осуществляется финансирование расходов на приобретение у оператора работ (услуг) за счет средств республиканского бюджета, ежегодно предусматриваемых МВД на указанные цели.

В общих чертах механизм функционирования системы мониторинга в настоящее время выглядит следующим образом. МВД, как специально уполномоченным государственным органом, формируется перечень объектов (мест установки), который актуализируется министерством по мере необходимости и (или) по предложениям пользователей исходя из специфики выполняемых ими задач. После формирования либо актуализации перечней они направляются оператору, т. е. РУП «Белтелеком», которым начинается работа по оборудованию объектов средствами видеонаблюдения. Собственники объектов (за исключением бюджетных организаций) компенсируют расходы республиканского бюджета на финансирование работ (услуг) по содержанию и эксплуатации системы мониторинга путем перечисления средств в доходы республиканского бюджета.

Внесенные в 2022 г. изменения в действующее законодательство, регулирующие вопросы развития и построения системы мониторинга, уже полностью доказали правильность и своевременность принятого решения по изменению подходов к построению РСМОБ. Начиная со второго полугодия 2022 г. количество видеокамер, подключенных к системе мониторинга, растет быстрыми темпами и по состоянию на 1 января 2025 г. составило 54,1 тыс., что в 50 раз больше, чем такое же число на начало 2022 г. К концу 2027 г. планируется подключение к системе мониторинга 100 тыс. видеокамер.

В рамках выполнения постановления Министерства внутренних дел Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 18 марта 2022 г. № 68/5 «О технических требованиях к программному обеспечению системы видеоаналитики и квалификационных требованиях к поставщику такого программного обеспечения» поступательно развивается и функционал программной платформы системы мониторинга. Помимо распознавания лиц и регистрационных знаков транспортных средств, система отображает установленные видеокамеры РСМОБ на картографической основе, позволяет осуществлять поиск видеокамер по адресам, предоставляет возможность просмотра архива видео и поиска в нем в течение 30 суток, осуществляет построение маршрутов движения распознанных лиц и транспортных средств. В настоящее время функционал системы дополняется новыми возможностями.

Таким образом, избранный вектор развития системы мониторинга доказал свою эффективность. Только в 2024 г. РСМОБ способствовала

выявлению (раскрытию) более 2 000 преступлений, установлению местонахождения около 700 лиц, находившихся в розыске, что более чем в четыре раза превышает аналогичные показатели за 2023 г. История этого важного инструмента борьбы с преступностью динамично развивается и далека от завершения.

УДК 343.985

П.А. Кайбелев

ПРОВЕДЕНИЕ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ ПО ЗАЯВЛЕНИЮ ГРАЖДАНИНА

В соответствии со ст. 38 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон) ряд оперативно-розыскных мероприятий (ОРМ) (наблюдение с использованием средств негласного получения (фиксации) информации и иных средств, установленных в жилище и ином законном владении гражданина, помещении, здании, сооружении, транспортном средстве, на ином объекте и территории организации, за исключением общественных мест, участков местности, а также всех видов общественного транспорта, слуховой контроль, контроль почтовых отправлений, контроль в сетях электросвязи) можно проводить на основании постановления о проведении ОРМ без санкции прокурора или его заместителя.

Несмотря на то что указанные мероприятия, по общим условиям, требуют получения санкции прокурора или его заместителя законодатель, при возникновении угрозы жизни, здоровью и необходимости сохранности имущества граждан, предусмотрел возможность проводить указанные ОРМ без ее получения по заявлению, сообщению гражданина или с его согласия в письменной форме, либо по заявлению его близкого, опекуна или попечителя. Данная мера обусловлена необходимостью экономии времени на организацию проведения ОРМ и в случае совершенного преступления у оперативных сотрудников имеется возможность их проведения сразу после вынесения постановления о проведении ОРМ.

В отличие от указанных выше ситуаций в случаях безвестного исчезновения граждан, а также при возникновении угрозы их жизни и здоровью возможность проведения перечисленных мероприятий исключительно по постановлению о проведении ОРМ не отражает всех потребностей оперативных сотрудников, так как наличие дела оперативного учета как одного из условий их проведения по-прежнему остается, что диктует необходимость принятия определенных мер.

Так, в целях редукции процесса организации проведения ОРМ, перечисленных в ст. 38 Закона, в ситуациях безвестного исчезновения граждан, следует предусмотреть возможность их проведения при соблюдении условий, закрепленных в ст. 38 Закона, без заведения дел оперативного учета.

Следует отметить, что законодателем уже предусмотрены основания, позволяющие проводить ОРМ без заведения дела оперативного учета, среди которых:

поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении;

письменный запрос органа, осуществляющего оперативно-розыскную деятельность, о проведении ОРМ по основаниям, указанным в абзацах втором – девятом части первой ст. 16 Закона;

письменный запрос международной организации, правоохранительного органа, специальной службы иностранного государства в соответствии с международными договорами Республики Беларусь, а также на основе принципа взаимности;

необходимость сбора сведений для принятия решений о допуске граждан к государственным секретам, к работам, связанным с эксплуатацией объектов, представляющих повышенную опасность для жизни и здоровья граждан и окружающей среды, к участию в оперативно-розыскной деятельности, к содействию на конфиденциальной основе органам, осуществляющим оперативно-розыскную деятельность. Среди перечисленных отсутствует основание, закрепленное абзацем седьмым части первой ст. 16 Закона (сведения о гражданине, без вести пропавшем).

Для реализации предложенного решения часть шестую ст. 19 Закона следует дополнить предложением следующего содержания: «Оперативно-розыскные мероприятия, перечисленные в части первой статьи 38 настоящего Закона, проводимые по основанию, предусмотренному абзацем седьмым части первой статьи 16 настоящего Закона, при соблюдении условий, перечисленных в статье 38 настоящего Закона, могут проводиться вне рамок дел оперативного учета». Данное предложение следует включить в конец абзаца.

Очевидно, что на практике возникнет вопрос об определении места хранения результатов оперативно-розыскной деятельности, полученных при проведении ОРМ, в условиях отсутствия соответствующих дел оперативного учета. В этой связи необходимо внести изменения в ведомственный правовой акт, предусматривающие возможность накопления и систематизации материалов оперативно-розыскной деятельности,

полученных в результате проведения ОРМ вне рамок дел оперативного учета, в соответствующем номенклатурном деле. Следовательно, материалы, полученные в ходе ОРМ, проводимых в целях установления обстоятельств безвестного исчезновения лица на стадии возбуждения уголовного дела без заведения дела оперативного учета, предлагается помещать в номенклатурные дела.

Предлагаемые изменения и дополнения правовых актов позволят оптимизировать процесс организации проведения ОРМ в ситуациях возникновения угрозы жизни и здоровью граждан, что, в свою очередь, предоставит возможность оперативным сотрудникам приступать к их проведению сразу же после поступления в органы внутренних дел заявлений или сообщений о безвестных исчезновениях граждан.

УДК 343.985.8

Б.В. Ковалик

ОБ ОТДЕЛЬНЫХ НАПРАВЛЕНИЯХ СОВЕРШЕНСТВОВАНИЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ГУПК»

Тенденции оперативно-розыскной деятельности (ОРД) таковы, что она в большей мере становится наукоемкой и опирается на возможности современных информационных технологий. Эффективность выявления и раскрытия противоправных проявлений, в частности киберпреступлений, часто зависит от того, насколько полно и эффективно будут использованы оперативным сотрудником технические средства, в том числе при решении задач по накоплению и анализу оперативно значимых сведений.

Одним из инструментов, позволяющих решать указанные задачи, является автоматизированная информационная система (АИС) «ГУПК». Посредством подсистемы «Цифровой след» данной АИС производится обобщение и анализ сведений о цифровых следах (идентификаторах), полученных в ходе оперативно-розыскных, поисковых и иных мероприятий, что позволяет в автоматическом режиме устанавливать соответствия между аналогичными идентификаторами по различным эпизодам противоправной деятельности злоумышленников. Указанная АИС показала свою эффективность на практике: в период с 2021 по настоящее время количество раскрытых киберпреступлений прошлых лет возросло практически в семь раз.

С вступлением в силу Указа Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям» рассматриваемая АИС была дополнена разделом «Автоматизированная система обработки инцидентов» (АСОИ), посредством которого организовано взаимодействие между правоохранительными органами, Национальным банком Республики Беларусь и поставщиками платежных услуг по обмену информацией о несанкционированных платежных операциях и попытках их совершения. Благодаря принятию вышеуказанного, а также ряда локальных нормативных актов, правоохранители могут оперативно получать от поставщиков платежных услуг информацию, необходимую для своевременного реагирования на сообщения о преступлениях.

Учитывая динамичность изменения способов совершения киберпреступлений, в целях установления возможных путей совершенствования рассматриваемой АИС, нами был проведен анализ ее текущего функционала, а также проведено анкетирование оперативных сотрудников, непосредственно функционирующих с данной системой.

Рассматривая указанный вопрос с оперативно-розыскных позиций, благоприятным нововведением может стать наличие возможности проверки сведений, полученных в рамках осуществления ОРД до начала ведения уголовного процесса. В настоящий момент регистрация сотрудником криминальной милиции инцидента в АСОИ возможна лишь в случае проведения доследственной проверки либо наличия возбужденного уголовного дела по факту совершения мошенничества с использованием информационно-коммуникационных технологий (ИКТ) и методов социальной инженерии. Таким образом, проверка сведений, полученных оперативно-розыскным путем, но не введенных в уголовный процесс, в настоящее время невозможна, что фактически исключает использование преимуществ, предоставляемых АСОИ, в процессе выявления преступлений. Указанный недостаток присущ и подсистеме «Цифровой след».

В рамках ответов на вопросы при проведении анкетирования рядом сотрудников была высказана необходимость об интеграции подсистемы «Цифровой след» со сходной по функционалу АИС «След», используемой сотрудниками Следственного комитета Республики Беларусь. Полагаем, что это может способствовать повышению эффективности обмена информацией не только между территориальными подразделениями органов внутренних дел, но и различными правоохранительными органами. Сотрудниками практических подразделений также отмечена необходимость внедрения системы оповещения пользователей, при возникновении совпадения идентификаторов по уголовным делам или материалам доследственной проверки.

Две трети респондентов (66,3 %) высказали мнение о наличии необходимости внедрения систем для взаимодействия подразделений криминальной милиции, подобных АСОИ, с иными субъектами. Больше половины опрошенных (56 %), из числа указавших в своих анкетах конкретных субъектов, считают, что повышению эффективности выявления и раскрытия киберпреступлений может способствовать организация оперативного обмена информацией с субъектами, обеспечивающими предоставление услуг электросвязи и надзор за данной деятельностью. Наряду с этим большинство респондентов (69,5 %) указали, что информация от данных субъектов взаимодействия имеет наибольшее значение для выявления и раскрытия мошенничества, совершенного с использованием ИКТ и методов социальной инженерии, доля которых от общего числа всех киберпреступлений в 2024 г. составила 55,5 %.

На актуальность этого вопроса указывает и то, что рядом сотрудников в инициативном порядке были высказаны замечания, касающиеся взаимодействия с организациями, предоставляющими услуги электросвязи. Проблемные вопросы, отмеченные респондентами, – длительность срока ответов на направленные в указанные организации запросы, а также отсутствие возможности получения доступа к технической информации в режиме реального времени, что еще раз подчеркивает необходимость проработки алгоритма оперативного взаимодействия с указанными субъектами.

В данной связи полагаем возможным, что в целях совершенствования функционала АИС «ГУПК» целесообразной является реализация следующих нововведений:

наличие возможности помещения и проверки сведений по всем подсистемам указанной АИС, полученных в ходе осуществления ОРД до начала уголовного процесса;

интеграция сведений, содержащихся в указанной АИС со сходной по функционалу АИС «След», используемой сотрудниками Следственного комитета Республики Беларусь;

внедрение системы оповещений при совпадении внесенных в АИС идентификаторов;

разработка и внедрение в рассматриваемую АИС подсистем, подобных АСОИ, для осуществления взаимодействия подразделений криминальной милиции с иными субъектами (например, организациями, предоставляющими услуги электросвязи).

УДК 004.056.5

Ю.Д. Козленко, Д.В. Шаститко

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ВЫЯВЛЕНИИ И ПРЕСЕЧЕНИИ ФИШИНГА И ТЕЛЕФОННОГО МОШЕННИЧЕСТВА

Современные формы преступности все активнее переходят в цифровую плоскость. Одними из наиболее распространенных видов являются фишинг и телефонное мошенничество, которые характеризуются высокой степенью адаптивности, маскировки и психологического давления на жертв. Рост числа подобных преступлений, а также их социальная опасность обусловливают необходимость изучения и внедрения цифровых технологий для их своевременного выявления и пресечения. По данным Министерства внутренних дел Республики Беларусь, подобные формы мошенничества уже заняли лидирующие позиции среди преступлений в сфере информационно-коммуникационных технологий.

1. Сетевые технологии против фишинга.

Для противодействия фишингу применяются различные технические решения, направленные на блокировку доступа к вредоносным веб-ресурсам. Сетевые антифишинговые фильтры используются на уровне интернет-провайдеров и поисковых систем – они блокируют доступ к известным фишинговым сайтам по черным спискам доменов и URL. В России, например, Роскомнадзор по заявлению Центрального банка и Министерства внутренних дел оперативно вносит фейковые сайты банков в единый реестр запрещенных ресурсов, что позволяет заблокировать их в течение 24 часов. DNS-фильтрация и поведенческий анализ трафика позволяют выявлять новые, еще не внесенные в базы фишинговые ресурсы: в Республике Беларусь оператор A1 реализовал систему автоматического обнаружения вредоносных доменов по признакам подозрительной активности и массовых рассылок.

2. Борьба с телефонным мошенничеством и спуфингом.

Автоматизированные системы блокировки звонков с подменой номера (спуфингом) активно развиваются. В России с 2022 г. действует система контроля межсетевого взаимодействия, внедренная при поддержке Минцифры, которая позволяет блокировать звонки, при которых абонентский номер не соответствует реальному исходному узлу связи.

3. Анализ цифровых следов и криминалистическая экспертиза.

Форензика цифровых следов – один из наиболее значимых инструментов в борьбе с фишингом. Анализ логов, IP-адресов, доменных ре-

гистраций, электронных почтовых адресов проводится в рамках технического сопровождения уголовных дел. Используются сервисы WHOIS, базы RIPE NCC и трассировка маршрутов трафика. Совместные группы Министерства внутренних дел и Следственного комитета Республики Беларусь уже имеют опыт проведения подобных мероприятий при расследовании атак на граждан с целью кражи банковских данных. Это позволяет не только установить факты преступления, но и выйти на организаторов схем за пределами страны.

4. Речевая аналитика и биометрия.

Технологии распознавания речи и голосовой биометрии находят все большее применение в борьбе с телефонным мошенничеством. Банки используют речевую аналитику для выявления типичных фраз, скриптов и голосов, используемых злоумышленниками. В Российской Федерации, например, Сбербанк реализовал систему распознавания мошеннических звонков по голосу и ключевым словам. Такие подходы позволяют формировать базы голосовых отпечатков и автоматизировать выявление повторяющихся злоумышленников.

5. Информационно-аналитические платформы и обмен данными.

Одним из перспективных направлений является создание межведомственных платформ для мониторинга и анализа цифровых угроз. В России с 2021 г. действует Центр мониторинга и реагирования на компьютерные атаки в финансовой сфере (ФинЦЕРТ), который объединяет усилия банков, правоохранительных органов и Федеральной службы безопасности для обмена информацией о новых схемах мошенничества и разработке коллективных мер противодействия. Создание подобного координационного центра в Республике Беларусь позволило бы повысить эффективность превентивных и оперативных мер, а также расширить международное сотрудничество.

Комплексное использование цифровых технологий в практике борьбы с фишингом и телефонным мошенничеством позволяет оперативно выявлять угрозы и минимизировать ущерб. Важным элементом эффективности таких мер является тесное взаимодействие правоохранительных органов, банков, операторов связи и организаций, отвечающих за цифровую инфраструктуру. В перспективе необходимо разработать национальные инструменты автоматического оповещения граждан о попытках мошенничества, создать платформу для сбора, анализа и обмена данными о цифровых угрозах, а также расширять международное сотрудничество с центрами реагирования других стран.

УДК 343.985.8

Н.Ю. Комсюкова, П.С. Милов

ПРОБЛЕМА СООТВЕТСТВИЯ НАИМЕНОВАНИЯ ст. 1 ФЕДЕРАЛЬНОГО ЗАКОНА РОССИЙСКОЙ ФЕДЕРАЦИИ «ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ» ЕЕ СОДЕРЖАНИЮ

Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» содержит одну основную норму, которая определяет «оперативно-розыскную деятельность» (ст. 1). В качестве ключевой категории понятие оперативно-розыскной деятельности должно верно отражать практику оперативно-розыскной работы, охватывая все ее аспекты и избегая искусственных ограничений в ее сфере.

Из представленного в указанном выше законе определения следует понимать, что оперативно-розыскная деятельность осуществляется через проведение оперативно-розыскных мероприятий (ОРМ).

Гл. II данного закона, охватывающая ст. 6–9, подробно описывает порядок проведения ОРМ, определяет их перечень, условия и основания для их реализации, а также устанавливает основы и процедуры судебного рассмотрения материалов, касающихся ограничения конституционных прав граждан при проведении ОРМ и другие важные аспекты. Вместе с тем в тексте вышеназванного закона об оперативно-розыскной деятельности говорится о действиях органов, осуществляющих оперативно-розыскную деятельность (ч. 3 ст. 5, ч. 2 ст. 16). Из изложенного можно сделать вывод, что ОРМ являются только одним из элементов оперативно-розыскной деятельности и не исчерпывают всего содержания оперативно-розыскной деятельности.

При анализе законов «Об оперативно-розыскной деятельности» других государств можно отметить, что в них представлены более четкие и конкретные определения данного понятия, которые, на наш взгляд, являются более емкими.

Так, в Законе Республики Казахстан от 15 сентября 1994 г. № 154-XIII «Об оперативно-розыскной деятельности» сказано, что оперативно-розыскная деятельность осуществляется посредством системы гласных и негласных оперативно-розыскных, организационных и управленческих мероприятий. Из изложенного видно, что оперативно-розыскная деятельность не ограничивается проведением ОРМ.

Учитывая многообразие оперативно-розыскной деятельности и ограниченность определения, предложенного российским законодателем,

считаем целесообразным дополнить ст. 1 упоминанием о том, что оперативно-розыскная деятельность осуществляется не только посредством проведения ОРМ, но и с использованием других законных действий.

Например, к «иным законным действиям» можно отнести действия, о которых, в частности, говорится в тексте российского законодательства об оперативно-розыскной деятельности: создание и использование информационных систем; ведение дел оперативного учета (ч. 1 ст. 10); исполнение поручений дознавателя, следователя о проведении ОРМ (п. 2 ч. 1 ст. 14); изъятие документов, предметов, материалов и сообщений при проведении ОРМ (п. 1 ч. 1 ст. 15); привлечение отдельных лиц к подготовке или проведению ОРМ (ч. 1 ст. 17).

По нашему мнению, оперативно-розыскные действия можно трактовать следующим образом: это предусмотренные законодательством об оперативно-розыскной деятельности ОРМ, а также организационные, управленческие и иные законные действия, обеспечивающие достижение цели и решение задач оперативно-розыскной деятельности.

Вторым спорным моментом в ст. 1 Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» является цель оперативно-розыскной деятельности. Отметим, что отдельной статьи, посвященной цели оперативно-розыскной деятельности, в данном законе не имеется.

Нормативно они определяются в ст. 1 этого закона, согласно которой целью ОРД является защита жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечение безопасности общества и государства от преступных посягательств. С нашей точки зрения, данная формулировка в ст. 1 указанного закона не полностью отражает цель оперативно-розыскной деятельности. Аргументируем наше мнение.

Во-первых, помимо решения задач выявления, предупреждения, пресечения и раскрытия преступлений (ст. 2), Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» допускает проведение ОРМ в ходе так называемой административно-проверочной работы, например, об установлении или о поддержании с лицом отношений сотрудничества при подготовке и проведении ОРМ; о допуске к сведениям, составляющим государственную тайну; о выдаче разрешений на частную детективную и охранную деятельность и др. (ч. 2 ст. 7).

Важно отметить, что объектами ОРМ в данном контексте не являются лица, которые подготавливают, совершают или уже совершили преступления. Цель ограниченного круга проводимых ОРМ заключается в предположительной возможности действий таких лиц, направленных

против государственных, служебных и профессиональных интересов. Это предполагает наличие повышенных требований к проверяемым субъектам.

Во-вторых, ч. 3 ст. 7 вышеуказанного закона допускает проведение ОРМ при наличии соответствующего запроса в области противодействия коррупции, о достоверности и полноте сведений, представляемых лицами, претендующими на замещение определенных в данной норме должностей, соблюдении данными лицами ограничений и запретов, установленных законом. Из изложенного видно, что в этой норме также не идет речь о совершении указанными лицами каких-либо преступных действий.

В-третьих, при формулировании цели оперативно-розыскной деятельности были объединены такие термины, как «защита» и «обеспечение безопасности», что вызывает смешение двух различных, хотя и взаимосвязанных видов деятельности. В ст. 1 термин «защита» относится к индивидууму, тогда как выражение «обеспечение безопасности» применяется к обществу и государству. Оценить данное положение как завершенное представляется затруднительным.

Отмечая многозначность термина «безопасность» и анализируя ряд понятий, существующих в юриспруденции и отражающих многоаспектность этого феномена, А.Ю. Епихин предлагает общее определение безопасности как «конечного состояния», которое «является целью и должно служить результатом защиты» от любого противоправного посягательства.

Далее А.Ю. Епихин рассматривает «защиту» как один из методов обеспечения безопасности в ее различных проявлениях. Следует отметить, что некоторые авторы аргументируют, что термин «безопасность» вполне оправданно употребляется в контексте безопасности личности.

С учетом изложенного считаем целесообразным в рамках текущей формулировки законопроекта уточнить и упростить окончание ст. 1 Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», сформулировав его как «в целях обеспечения безопасности личности, общества и государства». При этом детализация объектов безопасности в отношении конкретных оперативно-розыскных органов должна быть отражена в ведомственных нормативных актах и также обсуждаться в теоретических исследованиях.

Таким образом, можно сказать, что действующая редакция ст. 1 вышеуказанного закона не полностью соответствует сути одного из видов правоохранительной деятельности, описываемой в данной норме.

Представляется, что по сути и назначению оперативно-розыскной деятельности более соответствовала следующая редакция ст. 1 указанного выше закона: «Оперативно-розыскная деятельность – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим законом в пределах их компетенции посредством проведения оперативно-розыскных мероприятий и иных законных действий в целях обеспечения безопасности личности, общества и государства.»

Предлагаемая редакция ст. 1 вышеназванного закона позволит избежать ранее упомянутых противоречий существующего текста и более ясно формулирует понятие, содержание и цели оперативно-розыскной деятельности.

УДК 343.985.8

Я.Ю. Комсюкова, П.С. Милов

СЕТЬ ИНТЕРНЕТ КАК ИСТОЧНИК ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ

В конце XIX в. с появлением радио, телеграфа и телефона был значительно упрощен обмен информацией, что, в свою очередь, способствовало стремительному развитию технологий в области коммуникаций. Уже в XX в. на смену этим изобретениям пришло телевидение, а затем компьютеры и сеть Интернет как способ передачи данных. На этом этапе исследования начали не только способствовать разработке новых информационных технологий, но и провоцировали переосмысление подходов к использованию возможностей интернета в борьбе с преступностью.

Современные технические достижения открывают возможность для взаимодействия людей не только в реальной жизни, но и через новые доступные технологии, такие как смартфоны, ноутбуки и стационарные компьютеры. Сегодня социальные сети, мессенджеры и доски объявлений становятся одними из главных источников получения информации.

В настоящее время можно наблюдать рост объема информации, передаваемой через коммуникационные каналы, что дает сотрудникам оперативных подразделений органов внутренних дел возможность рассматривать сеть Интернет в качестве одного из ключевых источников получения информации.

Информационные ресурсы, размещенные в сети Интернет, представляют собой открытые источники данных, доступ к которым осу-

ществляется через переход по электронной ссылке на определенный онлайн-сервис или веб-сайт.

Основным преимуществом открытых источников в сети Интернет является их доступность, что позволяет сотрудникам оперативных подразделений органов внутренних дел в кратчайшие сроки получать актуальную информацию, необходимую для принятия решений в рамках оперативно-разыскной деятельности. Это включает в себя планирование оперативно-разыскных мероприятий, разработку мер по своевременному предотвращению, пресечению или раскрытию преступлений, а также выявление лиц, причастных к ним, и прогнозирование тенденций развития криминогенных процессов.

Однако использование открытых источников сети Интернет сотрудниками оперативных подразделений органов внутренних дел сопряжено с рядом недостатков:

1. В интернет-ресурсах представлено множество непроверенных и недостоверных данных, поскольку любой пользователь может создавать и размещать информацию.

2. Огромный объем информации, доступной в сети Интернет, затрудняет процесс поиска и отбора необходимых сведений.

3. Для эффективного применения возможностей интернет-ресурсов в качестве источника оперативной информации сотрудники полиции должны обладать профессиональными навыками критического мышления и анализа. Это включает в себя проверку достоверности полученных данных, их источников, а также сравнительный анализ информации с использованием других проверенных ресурсов, включая ведомственные.

В настоящее время в контексте получения оперативной информации о физических лицах особый интерес представляют возможности различных социальных сетей. Согласно статистике, на начало 2023 г. в мире насчитывалось около 4,8 млрд активных пользователей социальных сетей, а к началу 2024 г. это количество возросло до 5,04 млрд.

Преимущество социальных сетей перед другими источниками данных заключается в том, что пользователи регулярно размещают огромное количество информации о себе и своих знакомых. Эти массивы данных могут представлять оперативный интерес для сотрудников органов внутренних дел. На личных страницах пользователей социальные сети содержат общедоступные фотографии и видеозаписи, персональные данные, контактную информацию, а также сведения об увлечениях, хобби, привычках и круге общения данных лиц.

Среди информационных ресурсов, предоставляющих оперативным подразделениям органов внутренних дел возможность поиска и получе-

ния данных из открытых источников в сети Интернет, включая социальные сети, можно выделить следующие онлайн-сервисы:

1. **Search4faces**. Этот сервис предлагает возможность поиска информации о физических лицах по фотографиям посредством технологии обратного поиска изображений. Эффективность его работы достигает 68,8 %, и результатом поиска является ссылка на изображение и профиль найденного человека в социальных сетях. Данный онлайн-сервис может быть особенно полезен для всех субъектов оперативно-розыскной деятельности, поскольку часто сотрудникам полиции необходимо быстро установить личность и местонахождение человека по его фото, будь то правонарушитель, неопознанный труп или другое лицо.

2. **«Глаз Бога»**. Этот сервис позволяет получить информацию как о физических, так и о юридических лицах, включая контактные номера телефонов, фотографии, адреса электронной почты, профили в мессенджерах и социальных сетях, а также данные о государственном регистрационном знаке автомобиля и IP-адресе. Поиск осуществляется через телеграм-бота, который предоставляет возможность находить и получать информацию по следующим критериям: Ф.И.О., номер телефона, аккаунт в социальной сети, адрес проживания или регистрации, фотографии, государственный регистрационный знак или VIN-код автомобиля.

3. **HimeraSearch**. Данный интернет-ресурс позволяет получать широкий спектр информации о конкретном объекте, представляющем оперативный интерес. С помощью указанного сервиса можно получить следующие данные:

о физическом лице по Ф.И.О. (дата рождения, адрес регистрации, номер телефона, место работы, сведения о доходах, имуществе, задолженности и правонарушениях);

о транспортных средствах по государственному регистрационному знаку или VIN (имя, фамилия и номер телефона владельца автомобиля; марка и модель; данные о ДТП, регистрации в ГИБДД и нахождении в розыске);

о юридических лицах по ИНН (данные о владельцах и учредителях, контактные номера телефонов, участие в арбитражных процессах, банкротствах, долговых обязательствах, список сотрудников).

Однако активное использование указанного ресурса в оперативно-разыскной деятельности затруднено из-за доступности его информации только на платной основе.

4. **Поисковая система SEUS** (ПС «СЕУС»). Это веб-приложение предназначено для проведения оперативно-разыскных мероприятий, аналитических исследований и цифровых расследований, а также решения задач, связанных с поиском, мониторингом и анализом информа-

ции, размещенной в открытом доступе социальных сетей и мессенджеров, на которые не влияют настройки приватности.

ПС «СЕУС» предоставляет пользователям следующие функции:

поиск профилей пользователей по различным параметрам, даже по неполным данным;

мониторинг информации без необходимости дополнительной настройки от оператора;

использование фильтров для поиска информации в социальных сетях с помощью лингвистических словарей;

поддержка нескольких языков для поиска;

полное географическое покрытие информационного пространства социальных сетей на территории России, включая небольшие населенные пункты;

экспорт информации в популярные офисные форматы и визуализация результатов на нескольких видах карт;

накопление полученных данных и контента.

Однако и у ПС «СЕУС» также есть недостаток – платный доступ к базе данных.

Согласно проведенному опросу среди сотрудников оперативных подразделений органов внутренних дел, можно отметить, что они активно используют сеть Интернет для получения оперативной информации, а также перечисленные выше сервисы.

Подводя итоги, следует подчеркнуть, что выдающимся преимуществом открытых источников оперативно значимой информации в сети Интернет является их быстродействие, информативность и доступность. Это позволяет сотрудникам оперативных подразделений органов внутренних дел своевременно получать ключевые сведения, необходимые для принятия незамедлительных мер по выявлению, раскрытию и пресечению преступлений, а также оперативно реагировать на любые изменения в криминогенной обстановке. В результате обеспечивается эффективная защита общественной безопасности и интересов граждан и государства.

Поиск и анализ информации в сети Интернет открывают новые источники оперативно-розыскной информации, расширяя возможности ее поиска и повышая уровень профессионализма в выполнении задач оперативно-разыскной деятельности. Как уже было указано, активный поиск в сети Интернет предполагает установление личности преступников, получение дополнительной информации о них, выявление фиктивных аккаунтов, анализ сообщений от лиц, осведомленных о подготовке и совершении преступлений, а также сбор ссылок на сетевые ресурсы, содержащие запрещенные для распространения материалы. Этот пере-

чень можно продолжать, однако конкретика будет зависеть от поиска источников информации в каждом отдельном случае преступления.

УДК 393.985

В.В. Кравец

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ OSINT ДЛЯ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ НА ПРИМЕРЕ ПЛАТФОРМЫ MALTEGO

Современные вызовы, связанные с противодействием преступлениям экстремистской направленности, требуют от правоохранительных органов Республики Беларусь внедрения комплексных и технологически продвинутых методов сбора, анализа и проверки информации. В условиях цифровизации все большее число преступников и радикальных групп задействуют в своей деятельности сетевые ресурсы, социальные сети, мессенджеры и форумы. По данным Генеральной прокуратуры Республики Беларусь, более 70 % преступлений экстремистской направленности совершены в сети Интернет, значительная часть подобных преступлений совершаются злоумышленниками, находящимися вне пределов республики. Подобная «миграция» деструктивных элементов в сети Интернет повышает значимость концепции OSINT (Open Source Intelligence), заключающейся в систематическом исследовании открытых источников в целях выявления, документирования и анализа сведений, способных указать на факты планирования или совершения противоправных действий экстремистского характера. Ценность OSINT состоит в том, что публично доступная информация может быть исследована и использована в качестве доказательств, при условии их надлежащего процессуального оформления в рамках уголовно-процессуального законодательства.

Несмотря на обилие доступных инструментов для открытой разведки, особое место среди них занимает платформа Maltego. Данная платформа представляет собой мощный программный комплекс, ориентированный на структурирование и визуализацию больших массивов данных, получаемых из открытых источников (социальных сетей, веб-сайтов, публичных реестров, форумов, блогов и т. д.). Она позволяет оперативным сотрудникам и аналитикам систематизировать, сопоставлять и интерпретировать разрозненные сведения о лицах, сетевых сообществах и

их инфраструктуре. Применение Maltego в оперативно-розыскной деятельности (ОРД) потенцирует быстроту и глубину анализа, обеспечивая доказательную базу, достаточную для возбуждения уголовного дела или пресечения экстремистских проявлений на ранней стадии.

С технической точки зрения Maltego представляет собой универсальную платформу, включающую так называемые трансформы – специальные модули, которые «преобразуют» исходную сущность (e-mail, имя пользователя, адрес веб-сайта, IP-адрес и т. д.) в набор новых данных. Например, если в ходе проведения оперативно-розыскных мероприятий (ОРМ) было установлено, что подозреваемый распространяет экстремистский контент из аккаунта в социальной сети, то сотрудник может внести в Maltego известные сведения (e-mail, никнейм, номер телефона или даже фрагмент текста) и запустить серию трансформов, связанных с поиском дополняющей информации. Программа автоматически «пройдется» по открытым источникам, поисковым системам, общедоступным базам данных, «социальным графам», попытается выявить, какие еще учетные записи принадлежат данному лицу, с какими группами в сети Интернет он взаимодействует и какова структура его контактов.

Ключевым элементом работы Maltego является возможность наглядной визуализации связей между объектами. Платформа строит граф, на котором каждое «звено» (entity) отражает конкретный фрагмент информации: от имени пользователя или группы до доменных имен и IP-адресов. Линии (edges) показывают взаимосвязи, будь то совпадение телефонного номера, пересечение с другими социальными профилями или упоминания в сети. Такая наглядность крайне важна для оперативного сотрудника, поскольку упрощает понимание структуры экстремистского сообщества, быстро выявляет лидеров, посредников, ответственных за техническое сопровождение сайта или мессенджера, а также лиц, занимающихся финансовой подпиткой.

Например, в ходе ОРМ сотрудникам может стать известно, что некий Telegram-канал распространяет призывы к насилию, направленные на представителей определенной этнической группы. Зная никнейм администратора, оперативный сотрудник вносит в Maltego сущность Alias и связывает ее с Telegram-доменом (t.me). Запуск трансформы, ориентированной на поисковые системы, позволяет выявить, что этот же ник фигурирует на иных платформах, например, в социальных сетях «ВКонтакте», Facebook. Далее Maltego обнаруживает, что администратор указывает одинаковые контактные данные на нескольких ресурсах. Полученный номер телефона, в свою очередь, может преобразоваться в конкретные Ф.И.О., а затем проверяться по базам данных и откры-

тым источникам (доскам объявлений, сайтам резюме, форумам и т. д.). В итоге создается устойчивая цепочка, которая связывает экстремистский Telegram-канал с реальным человеком.

Несмотря на то что Maltego изначально ориентирована на глобальный рынок, ее функционал применим в специфике белорусского сегмента интернета. Программа способна анализировать не только крупные международные платформы (Facebook, Twitter, Telegram), но и локальные ресурсы (форумы, новостные сайты, социальные сети, имеющие аудиторию в Республике Беларусь). Более того, если в ходе проведения ОРМ зафиксированы связи с зарубежными экстремистскими группировками или имеется транзитный сервер за пределами страны, Maltego способствует комплексному анализу всего интернет-трафика, связанного с подозреваемыми. В этом отражается межгосударственный характер экстремистской угрозы, требующей как развитых информационных инструментов, так и правового взаимодействия между государственными органами разных стран.

Для повышения результативности Maltego и аналогичных OSINT-платформ в противодействии экстремизму в Республике Беларусь необходимо дополнительно совершенствовать нормативно-правовую базу. Поскольку технологический прогресс нередко опережает существующие регулятивные нормы, особую актуальность приобретает разработка методических рекомендаций, регламентирующих порядок документирования электронных доказательств и описывающих алгоритмы использования Maltego в ОРД. Одновременно важно внедрять образовательные программы, направленные на формирование у оперативных сотрудников комплексных навыков в сфере OSINT, чтобы обеспечить грамотное и эффективное применение возможностей Maltego на практике.

Таким образом, применение платформы Maltego в ОРД по противодействию преступлениям экстремистской направленности в Республике Беларусь представляется не только актуальным, но и крайне результативным. Возможность оперативно сопоставлять разрозненные фрагменты информации из открытых источников, строить взаимосвязи между профильными аккаунтами, доменными именами и IP-адресами, а также формировать доказательственную базу в цифровом формате позволяет эффективно выявлять и пресекать экстремистские проявления уже на ранних стадиях. Вместе с тем успешная интеграция Maltego в правоприменительную практику требует тщательного соблюдения национального законодательства и процессуальных норм, а также разработки соответствующих методических рекомендаций, отражающих специфику

документирования электронных доказательств. Грамотно выстроенная система подготовки оперативных сотрудников, сочетающая практические навыки использования Maltego с обширными знаниями в области OSINT, существенно повышает качество аналитических решений. Такой комплексный подход, основанный на гармоничном сочетании правовых и технологических инструментов, обеспечивает действенный механизм противодействия экстремистской активности и укрепляет основу национальной безопасности.

УДК 338.2:34

М.А. Кравцова

ЗАРУБЕЖНЫЙ ОПЫТ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В эпоху глобализации построение эффективной экономической системы государства стало еще более сложным, поскольку глобальная экономика стала более взаимосвязанной и взаимозависимой. В этой связи экономическая политика одной страны может оказывать влияние на экономическую ситуацию других стран, а также мировую экономику в целом. Более того, экономическая глобализация приводит к увеличению конкуренции, ускоренному технологическому прогрессу, изменению условий труда и другим сложностям, которые влияют на экономическую систему государства.

В этой ситуации важно изучение зарубежного опыта, поскольку другие страны уже имеют опыт построения своих экономических систем и смогли преодолеть многие сложности. Изучение зарубежного опыта позволяет определить лучшие практики и технологии, которые могут быть использованы для усовершенствования экономической системы своей страны.

Кроме того, анализ зарубежного опыта может помочь в выявлении возможных угроз и рисков, связанных с реализацией определенных экономических мероприятий, и принять меры для их минимизации. Таким образом, изучение зарубежного опыта является важным инструментом для построения эффективной экономической системы государства в условиях глобализации. Считаем, что каждому государству необходимо выстраивать системы экономической безопасности, опираясь не только на внутреннюю ситуацию в стране, но и на опыт других государств.

Хорошим примером для построения эффективной экономики в любом государстве может послужить опыт Китая в данной сфере. Так, в период мирового экономического кризиса, происшедшего в начале второй декады XXI в., экономика Китая, в отличие от многих ведущих, оказалась нетронутой. Более того, она уверенно продолжила свое развитие.

Тем не менее кризис инициировал в Китае активизацию ряда процессов, направленных на преодоление негативных тенденций в развитии национального хозяйства. Реакцией государственного руководства Китайской Народной Республики на мировой финансово-экономический кризис стало принятие антикризисной стратегии.

В качестве первостепенной задачи выхода из кризиса китайским руководством было названо обеспечение устойчивого и сравнительно быстрого развития экономики. Главным условием решения данной задачи было определено расширение внутреннего спроса. Были также выделены основные направления антикризисной экономической стратегии.

Тогда же в качестве приоритетных были определены следующие направления: сельское хозяйство; строительство инфраструктуры; развитие высоких технологий; строительство экономичного жилья; развитие транспортных сетей; повышение доходов жителей сельской местности за счет увеличения норм обязательных закупок зерна по более высоким ценам; сокращение налогов на добавленную стоимость; поощрение технических инноваций и др.

Своевременная переориентация производства на внутреннего потребителя позволила Китаю достичь следующих целей:

сохранить стабильность платежной системы страны;

частично решить социальные проблемы государства;

создать условия для последующего экономического роста.

Еще одним звеном экономической стабильности Китайской Народной Республики является наличие тесных экономических связей с Российской Федерацией. Экономические отношения между данными государствами сложные и неоднозначные. Их развитие за последние годы было связано с качественными сдвигами как в развитии этих двух стран, так и с изменениями международной ситуации.

Анализ существующих подходов к определению экономической безопасности демонстрирует, что одновременно с теоретическим его осмыслением развивались государственные экономические стратегии и формировался механизм государственного управления. В зависимости от географического положения, специфики экономического развития, менталитета населения и ряда других факторов позиции стран в сфере обеспечения национальной и экономической безопасности отличаются.

Таким образом, несмотря на то что ведущие мировые державы имеют достаточно стабильную, защищенную от серьезных внешних угроз экономику, говорить о том, что какая-то определенная модель экономической безопасности является лучшей, нельзя. В рассмотренных ранее примерах четко прослеживаются как сильные, так и слабые стороны экономики. Это обусловлено влиянием ряда как внешних, так и внутренних факторов: геополитическая ситуация в регионе; менталитет общества; обеспеченность природными ресурсами и др.

Однако, основываясь на опыте ведущих экономик мира, Правительство Республики Беларусь может планировать направления развития внутригосударственной политики в экономической сфере, создавая определенные проекты и анализируя реальную возможность их реализации.

По нашему мнению, одной из существенных угроз экономической безопасности является зависимость от экспорта энергоносителей. Представляется, что для минимизации негативных последствий санкционного давления коллективного Запада Республике Беларусь необходимо развивать рынки сбыта энергоносителей и другой продукции в дружественных среднеазиатском и африканском регионах.

Экономические санкции, вводимые странами Европейского союза и США, направлены на то, чтобы вызвать дефицит товаров и услуг в Беларуси, а также перекрыть рынки сбыта отечественной продукции, тем самым подорвав экономическую безопасность государства. Однако оперативное принятие некоторых управленческих решений в области экономики могут и должны подтолкнуть белорусские и российские субъекты хозяйствования к импортозамещению.

УДК 343.98

Д.С. Кудрявцев

ОБ ОСОБЕННОСТЯХ ОПЕРАТИВНЫХ КОМБИНАЦИЙ

О влиянии противодействия на процесс раскрытия и расследования преступлений можно судить не только по статистическим сведениям, отражающим рост отдельных составов, увеличение количества прекращенных и приостановленных уголовных дел, но и по конкретным фактам обеспечения государственной защиты сотрудников правоохранительных и иных органов, осуществляющих борьбу с преступностью. Так, например, на протяжении последних пяти лет в нашей стране приостанавливается практически каждое третье уголовное дело, а по линии борьбы с коррупцией и экономическими преступлениями – каждое пятое.

За три предыдущих года в разы увеличилось число преступлений, предусмотренных ст. 364 и 401 Уголовного кодекса Республики Беларусь (далее – УК). Статистикой стали фиксироваться уголовно наказуемые деяния, предусмотренные ст. 402 и 404 УК, что в предыдущие годы было нехарактерно для отечественной следственной и судебной практики. Остается неизменной наметившаяся еще десять лет назад тенденция увеличения количества уголовных дел, возбужденных за вмешательство в разрешение судебных дел или производство предварительного расследования (ст. 390 УК) и угрозу в отношении судьи или народного заседателя (ст. 389 УК).

Несмотря на то что преступления, предусмотренные вышеуказанными статьями, регистрируются не так часто, достаточно высока их общественная опасность. При этом очевидно, что официальная статистика, отражающая лишь числовой показатель, не отражает объективной ситуации, а свидетельствует о высокой латентности и активности противодействия в целом правоохранительным органам, осуществляющим борьбу с преступностью.

В свою очередь, результативность его преодоления во многом зависит от полноты информации о самом факте противодействия, выступающей основой для планирования, организации и осуществления принимаемых в этих целях мер, одной из которых является проведение оперативных комбинаций.

В научной литературе оперативная комбинация рассматривается в нескольких аспектах: 1) как метод оперативно-розыскной деятельности; 2) как средство (способ) решения задач оперативно-розыскной деятельности; 3) как условие проведения оперативно-розыскного мероприятия; 4) как комплекс действий, направленных на решение конкретной задачи оперативно-розыскной деятельности; 5) как способ осуществления оперативных мероприятий. Вне зависимости от авторского изложения дефиниции, большинство ученых видят основное предназначение оперативных комбинаций в необходимости изменения оперативной обстановки в нужном направлении. Для решения задач противодействия субъектам, осуществляющим оперативно-розыскную деятельность, их предназначение заключается в создании наиболее благоприятных, оптимальных условий для своевременного выявления его признаков, а также оперативного и эффективного преодоления. Такие условия могут быть созданы за счет сочетания оперативно-розыскных и иных мероприятий, методов и сил, тактических приемов оперативно-розыскной деятельности, выработанной легенды действий, использования технических средств.

Что касается оперативных комбинаций, осуществляемых в целях выявления и преодоления противодействия раскрытию преступлений,

то, в отличие от традиционно рассматриваемой в теории оперативно-розыскной деятельности структуры такой тактической категории, включающей оперативную информацию, замысел, легенду, инсценировку, планирование, техническое обеспечение, их самостоятельным элементом выступает также прогнозирование развития оперативной ситуации. Закономерности ее изменения детерминируются:

особенностями личности субъекта противодействия;

убедительностью, реальностью условий, создаваемых для выбора поведения;

мотивированностью субъекта противодействия к активным действиям;

обеспечением конспирации проведения мероприятий.

Совершение лицом конкретных действий в целях противодействия субъектам, осуществляющим оперативно-розыскную деятельность, или отказ от них зависит от ситуации, развитие которой не повлечет его разоблачения. Не опасаясь для себя негативных последствий (задержание, возбуждение дела, привлечение к ответственности и др.), субъект противодействия с большей долей вероятности приступит к реализации своего умысла. В этой связи для более точного прогноза соответствующего поведения и необходимо создание таких условий, нахождение в которых не вызовет у него сомнений в собственной безопасности. При этом должно быть обеспечено соблюдение принципов законности и этичности при побуждении субъекта противодействия к необходимому поведению. Во избежание провокации оперативным подразделениям следует минимизировать совершение активных, целенаправленных действий, избирать в основном пассивные формы поведения.

В то же время для активизации у субъектов противодействия мотивированности к действиям оперативные подразделения фактически не ограничены правовыми и моральными нормами, в связи с чем использование спектра соответствующих мер максимально широко. Для стимулирования мыслительных, психических процессов, воздействия на эмоции достаточно результативно применение таких приемов, как, например, освещение в средствах массовой информации сведений, касающихся отдельных обстоятельств преступления; получение информации, которую субъекты противодействия желают сохранить в тайне, задержание кого-либо из связей последних и др.

Необходимость сохранения в тайне сведений о проведении мероприятий в целях обеспечения успеха рассматриваемых комбинаций обусловливается следующими обстоятельствами:

1) поскольку подготовка, совершение и сокрытие актов противодействия раскрытию преступлений всегда осуществляются в условиях не-

очевидности, то и соответствующие меры по его выявлению и преодолению должны носить конспиративный характер. В противном случае они будут нерезультативны;

2) скрытность работы оперативных подразделений позволяет не допустить публичной оценки полученной в ходе оперативно-розыскных мероприятий информации, необоснованной и преждевременной компрометации лиц, в отношении которых они проводились;

3) в подготовке и проведении отдельных мероприятий нередко участвуют граждане, оказывающие содействие органам внутренних дел на конфиденциальной основе. Сохранение в тайне о них сведений, как правило, является главным условием их привлечения для решения стоящих перед оперативными подразделениями задач. В этой связи утечка любой информации о таких лицах сопряжена с риском угроз не только их жизни и здоровью, но и негативными последствиями ведомственного значения;

4) посредством тайного характера действий обеспечивается защита от несанкционированного доступа к оперативно значимой информации, к сведениям о силах, средствах, методах оперативно-розыскной деятельности, организации и тактике проведения оперативно-розыскных мероприятий, данным, содержащимся в ведомственных информационных системах, базах и банках данных.

Таким образом, оперативные комбинации, осуществляемые в целях преодоления противодействия раскрытию преступлений, характеризуются более широким спектром составляющих элементов. Прогностическая функция таких комбинаций заключается в предвидении направлений изменения оперативной ситуации на основе познания закономерностей поведения субъектов противодействия, основывающегося на психологических особенностях их личности, реальности условий, в которых они находятся, и искусности проведения соответствующих мероприятий.

УДК 343.98

Д.С. Кудрявцев, В.А. Козлов

ПОЛИГРАФ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Анализ практики осуществления в нашей стране оперативно-розыскной деятельности (ОРД) показывает, что проведение практически каждого оперативно-розыскного мероприятия (ОРМ) не обходится без различного рода технических средств, в первую очередь в целях получения (фиксации) оперативно значимой информации. Возможность их использования предусмотрена не только Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон «Об ОРД»), но и обусловлена тактическими соображениями. В одних случаях такие средства выполняют поисково-познавательную функцию, в других – являются неотъемлемым элементом самого ОРМ, определяют его сущность.

Одним из наиболее часто проводимых оперативными подразделениями органов внутренних дел ОРМ является оперативный опрос. Отсутствие нормативных требований по ознакомлению, включая подпись, опрашиваемого лица с его результатами позволяет широко использовать в решении стоящих задач как мессенджеры, позволяющие фиксировать и в последующем анализировать сам разговор, так и приборы, предназначенные для выявления психофизиологических реакций человека. Наиболее распространенным таким средством является полиграф.

Позиция ученых и практических сотрудников правоохранительных органов, в первую очередь тех, кто решает уголовно-процессуальные задачи, к этому техническому средству до сих пор остается неоднозначной. Еще в советский период отдельные авторы видели в нем перспективу, другие – относились к нему весьма скептически. Например, А.Р. Лурия допускал, хоть и в ограниченных пределах, применение полиграфа при раскрытии и расследовании преступлений. Подобной точки зрения придерживались Г.А. Злобин и С.А. Яни, которые считали, что развитие методов исследования психофизиологических состояний человека в конечном итоге послужит научной основой для использования полиграфа в уголовном процессе.

Отстаивание долгое время российскими и белорусскими криминалистами позиции о необходимости придания полиграфу статуса технико-криминалистического средства не позволяло широко использовать его возможности в ином качестве, несмотря на то что его появление связано с потребностями следственной практики в разработке методов изобличения во лжи лиц, совершивших преступления.

В Республике Беларусь изучением возможностей полиграфа в борьбе с преступностью занимались И.И. Басецкий, А.Н. Порубов, О.В. Степанов, В.В. Бачила и другие ученые, которые стали родоначальниками теоретических основ его использования в ОРД.

Правовую основу применения в нашей стране полиграфа составляют Закон «Об ОРД», постановление Министерства внутренних дел Республики Беларусь от 4 ноября 2020 г. № 218 «О порядке проведения опроса с использованием технических средств (полиграфа)» и иные

акты, в соответствии с которыми в отдельных случаях полиграфный опрос допускается проводить в отношении лиц, имеющих некоторые заболевания, находящихся под воздействием определенных препаратов или в состоянии опьянения, а также в других случаях, что запрещено, например, законодательством Российской Федерации.

Органами внутренних дел нашей страны полиграф стал использоваться с 2001 г. В 2002 г. в структуре главного управления уголовного розыска криминальной милиции Министерства внутренних дел Республики Беларусь создан отдел психолого-технического обеспечения раскрытия преступлений. С 2005 г. аналогичные подразделения, входящие в криминальный блок, стали функционировать в каждой области и в г. Минске. В результате увеличения количества полиграфологов стало возможным более оперативно проводить опросы по различным категориям преступлений, в том числе преступлениям прошлых лет.

Для работы на полиграфе отбираются сотрудники, имеющие соответствующее образование, опыт оперативной работы, положительные характеристики по месту службы, а также прошедшие специальную подготовку, включающую психофизиологический отбор, собеседование, изучение навыков логического мышления, коммуникабельность и организованность.

Как правило, полиграфные опросы проводятся специалистами самостоятельно, но мероприятия по подготовке и составлению тестов, изучению обстоятельств преступления, личности опрашиваемого осуществляются совместно с инициатором, что, в том числе, позволяет подобрать наиболее подходящую методику.

Расширение практики использования полиграфа в борьбе с преступностью подкрепляется многочисленными положительными примерами результативности проведенных с его помощью опросов, позволивших раскрыть отдельные уголовно наказуемые деяния, включая тяжкие и особо тяжкие, серийные и резонансные преступления. С учетом специфики работы этого технического средства, программного обеспечения и методики подготовки и проведения полиграфологом беседы с лицом, представляющим оперативный интерес, сегодня опрос с использованием полиграфа рассматривается как разновидность оперативного опроса, что позволяет использовать полученные результаты в доказывании.

Посредством полиграфных опросов обеспечиваются:

проверка показаний лиц, представляющих оперативный интерес, подозреваемых (обвиняемых), свидетелей, потерпевших;

выявление подозреваемых лиц, причастных к совершению преступлений;

выяснение неизвестных обстоятельств дела;

проверка оперативно-розыскных и следственных версий;

выявление скрываемой опрашиваемыми лицами информации;

преодоление противодействия раскрытию и расследованию преступлений.

Как показывает практика, несмотря на то что результаты полиграфных опросов не являются доказательством по уголовным делам, в судах полиграфологов часто заслушивают как специалистов. Это в полной мере согласуется с тем, что они не отвечают на вопрос, врет человек или нет, не определяют, совершило ли лицо преступление. В пределах профессиональной компетенции полиграфолога – исследование поведения человека и указание на то, есть ли в нем психофизиологические признаки, свидетельствующие о сокрытии значимой информации.

Таким образом, ОРД сегодня является той сферой, где полиграф имеет наибольшие перспективы развития. Отсутствие жестких нормативных требований к порядку использования в целом технических средств, в том числе полиграфа, при проведении ОРМ, возможность применения нетрадиционных приемов и методов получения оперативно значимой информации позволяют внедрять различные методики опросов в отношении широкого круга лиц.

Цель применения полиграфа состоит не в оказании психологического давления на опрашиваемого и выведении его из психического равновесия, а в анализе его физиологических реакций, позволяющих судить о степени осведомленности об обстоятельствах совершенного преступления.

УДК 343

В.В. Лисаускайте

РОЛЬ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЙ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ: СТРАТЕГИЯ УПРАВЛЕНИЯ ООН ПО НАРКОТИКАМ И ПРЕСТУПНОСТИ НА 2021–2025 ГОДЫ

Международные организации являются полноправным участником международных отношений и реализации различных направлений сотрудничества. Они активно участвуют в становлении международного права и развитии его применения. За более чем 100 лет с момента появления первых организационных международных структур (в сравнении с периодом существования мирового сообщества и взаимодействия

в целом) международные организации стали полноправным и общепризнанным субъектом международного права. А борьба с преступностью – одно из направлений деятельности международных организаций, реализация которого позволила сформировать нормативную платформу посредством разработки и принятия конвенций по борьбе с преступностью в той или иной форме; организационный механизм сотрудничества, способствующий своевременно реагировать и предупреждать различные преступные процессы.

Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН) давно осуществляет свою деятельность по активизации международного взаимодействия государств в различных направлениях предупредительной деятельности. Данная международная структура использует различные формы взаимодействия с государствами в целях оказания помощи в борьбе с преступностью. Благодаря такой совместной работе государства-члены устанавливают свои уязвимые места. Так, в контексте борьбы с наркопреступностью последними чаще всего выступают: слабый институциональный потенциал, неразвитое уголовное законодательство, коррупция в правоохранительных структурах, безработица среди молодежи, бедность, социальная неустроенность и др.

Каждый временной период в деятельности УНП ООН характеризуется определенными проблемами в борьбе с преступностью и их решением. В 2020 г. УНП ООН приняла Стратегию своей деятельности на период 2021–2025 гг. Рассмотрим отдельные положения этого документа более подробно.

Стратегия отмечает крайне негативное воздействие пандемии COVID-19 на состояние и распространенность преступности. Обострились проблемы нестабильности, терроризма, обнажилось неравенство. Эксперты отмечают, что именно уязвимые слои населения стали еще более подвержены преступности, как с позиции жертвы, так и самого участия в преступной деятельности. Результатом анализа многолетних статистических данных о преступлениях в динамике стало выделение пяти основных тематических областей работы УНП ООН на обозначенный период.

В качестве последних были определены:

решение проблемы наркотиков и борьба с ней;

предупреждение организованной преступности и борьба с ней;

предупреждение и противодействие коррупции и экономической преступности;

предупреждение терроризма и борьба с ним;

предупреждение преступности и уголовное правосудие.

Относительно каждой указанной области Стратегия определяет цели деятельности УНП ООН в сотрудничестве с государствами, другими международными институтами и партнерами. С одной стороны, мы видим весьма классические направления в механизме борьбы с преступностью. С другой стороны, они представляют собой характерные преступные явления современного общества, которые видоизменяются и становятся более опасными. Борьба с ними имеет важное значение для каждого государства, а взаимодействие с УНП ООН позволяет использовать современные технологии и методики в таком процессе.

Так, в рамках первого направления (наркотики) одной из целей указано повышение роли и наращивание потенциала лаборатории УНП ООН для поддержки программных и политических мер государств-членов по борьбе с незаконным оборотом наркотиков и обеспечению соответствующих медицинских услуг. Поскольку реализация Стратегии подходит к завершению, УНП ООН уже озвучило некоторые результаты ее реализации. Относительно борьбы с незаконным оборотом наркотиков как один из итогов отмечается усиление и расширение поддержки национальных служб судебной экспертизы для выработки политики и программ по вопросам, связанным с наркотиками.

Международное сотрудничество в данном направлении имеет важное значение, поэтому следует отметить различные формы взаимодействия между УНП ООН и международными региональными организациями. Такая совместная работа осуществляется, в том числе, с Шанхайской организацией сотрудничества. Постоянный представитель России в ООН В.А. Небензя в своей речи на заседании Совета Безопасности ООН по положению в Афганистане отметил необходимость такой работы, учитывая серьезные проблемы с производством и распространением наркотиков в этой стране.

В рамках второго направления (организованная преступность) в качестве одного из промежуточных итогов реализации эксперты отмечают повышение эффективности мер по противодействию киберпреступности. Использование интернет-технологий является распространенным средством в преступной деятельности организованного сообщества, что усложняет возможность раскрытия и привлечения к ответственности. Поэтому создание различных механизмов противодействия является одной из приоритетных задач. В качестве подтверждения положительных результатов реализации данного направления Стратегии следует рассматривать подписание в рамках ООН Конвенции Организации Объединенных Наций против киберпреступности. При разработке этого договора за основу был взят проект, разработанный Россией.

Борьба с преступностью представляет собой системный и важный процесс для всего мирового сообщества. От эффективности осуществляемого взаимодействия зависят его результаты. Существующий опыт показывает, что эта деятельность должна проводиться в многоуровневом и многосубъектом формате. Роль УНП ООН в данном процессе весьма значима, а реализация в настоящее время принятой Стратегии свидетельствует о заинтересованности государств всего мирового сообщества в решении обозначенных проблем.

УДК 343.985

Д.В. Лопух, В.В. Якубук

О ПРАВЕ НА ОЗНАКОМЛЕНИЕ СО СВЕДЕНИЯМИ, ПОЛУЧЕННЫМИ В СВЯЗИ С ОСУЩЕСТВЛЕНИЕМ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ, ПРИ ВЫНЕСЕНИИ РЕШЕНИЯ ОБ ОТКАЗЕ В ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА

Решение об отказе в возбуждении уголовного дела является одним из итоговых решений стадии возбуждения уголовного дела. В связи с принятием такого решения процессуальная деятельность по проверке должна быть завершена, приняты необходимые меры по восстановлению нарушенных прав и законных интересов граждан. Одной из таких восстановительных мер выступает право граждан ознакомиться с полученными о них сведениями в связи с осуществлением оперативно-розыскной деятельности. Возникающая при ознакомлении с этими сведениями проблематика рассматривалась белорусскими правоведами: И.И. Бранчелем и А.В. Солтановичем, С.И. Бординовичем, И.А. Шаматульским и Д.В. Ковалевичем, С.Ю. Мельниковым и некоторыми другими. При этом комплексное исследование вопросов вариативности правовых оснований вынесения указанного процессуального решения для ознакомления с такими сведениями, уточнение установленных законодателем границ ознакомления не проводились.

Так, в силу абзаца пятого части второй ст. 10 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон) граждане наделяются правом ознакомления со сведениями, их касающимися, полученными при проведении оперативно-розыскных мероприятий, если в отношении их в возбуждении уголовного дела отказано, или прекращено производство по уголовному

делу, или уголовное преследование прекращено в связи с отсутствием общественно опасного деяния, предусмотренного уголовным законом, или в связи с отсутствием в их деяниях состава преступления, а также при вынесении оправдательного приговора. При этом в научной литературе сложились разные подходы к определению в этом случае правовых оснований процессуального решения об отказе в возбуждении уголовного дела: одними учеными в связи с конструкцией правовой нормы не ограничивается указанное право граждан отдельными правовыми основаниями, другими признается это право только в двух таких случаях (вынесение процессуального решения при наличии обстоятельств, указанных в п. 1 и 2 ч. 1 ст. 29 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК)).

Следует отметить, что всеми правоведами обосновывается предоставление законом этого права реализацией требований ст. 11, части второй ст. 34 Конституции Республики Беларусь, обязывающей государственные органы и должностных лиц осуществить предоставление гражданам возможности ознакомления с материалами, если они затрагивают их законные интересы и права. С целью научного осмысления указанной правовой нормы Закона, выяснения заложенного законодателем в содержании положений Закона их юридического смысла также необходимо руководствоваться принципом системности законодательства, его целостности и согласованности. Так, постановление оправдательного приговора осуществляется как при наличии обстоятельств, предусмотренных п. 1 и 2 ч. 1 ст. 29 УПК, так и в случаях недоказанности участия обвиняемого в совершении преступления. В научной литературе и законодательстве указанные три основания относятся к реабилитирующим, т. е. влекущим необходимость восстановления нарушенных правоохранительной деятельностью прав и законных интересов граждан (например, восстановление на службе, в специальном звании). Другие исключающие возможность судопроизводства обстоятельства (например, отсутствие заявления пострадавшего от преступления лица в определенных законом случаях) не создают таких реабилитирующих правовых последствий. При этом, по нашему мнению, также будет противоречить правилу согласованности законодательства утверждение об указании законодателем в Законе только отдельных правовых оснований для прекращения уголовного преследования с одновременным предоставлением указанного права на ознакомление с такими сведениями всем лицам при прекращении производства по уголовному делу в связи с наличием любых предусмотренных законом обстоятельств. В связи с изложенным системное осмысление правовых норм позволяет, по на-

шему мнению, прийти к выводу о возможности предоставления права ознакомления со сведениями, полученными при проведении оперативно-розыскных мероприятий, при вынесении решения об отказе в возбуждении уголовного дела в отношении определенного лица по всем его деяниям только при наличии реабилитирующих оснований, а не всего спектра правовых обстоятельств, в том числе совместно с реабилитирующими основаниями.

При этом указанными правоведами упоминается также отсутствие единообразия правоприменительной практики в рассматриваемом случае и необходимость подготовки нормативного правового акта, регламентирующего порядок такого ознакомления, в связи с наличием в материалах оперативно-розыскной деятельности охраняемой законом тайны. По нашему мнению, для разрешения данной проблематики также необходимо использовать системное исследование норм законодательства.

Так, в дополненной в 2017 г. ст. 179[1] УПК определено, что лицо в случае вынесения в его отношении решения об отказе в возбуждении уголовного дела вправе знакомиться только с материалами проверки, не содержащими определенные сведения (государственные секреты, иную охраняемую законом тайну). Положения Закона (например, ст. 8) регламентируют сохранение в тайне ряда сведений.

Изложенное приводит к выводу о возникновении при вынесении указанного процессуального решения права ознакомления лиц только с возможными для такого ознакомления сведениями, в том числе не охраняемыми Законом, как в рамках непосредственно уголовного судопроизводства, так и в сфере оперативно-розыскной деятельности. При этом объем такого ознакомления, по нашему мнению, должен соотноситься с рамками вынесенного процессуального решения, подвергаемыми правовой оценке фактами деятельности этих определенных лиц (с учетом временного периода деятельности и других установленных «доследственной» проверкой обстоятельств).

Так, Закон предоставляет право ознакомления только со сведениями, касающимися лиц, в отношении которых принято такое процессуальное решение. Указанное требование непосредственно отсылает к необходимости соотнесения предоставляемых для ознакомления лицу сведений с исследованными фактическими данными его деятельности при принятии процессуального решения, которым дана правовая оценка о наличии реабилитирующих обстоятельств. Принятие процессуального решения только по фактам какой-либо деятельности (незаконного оборота имущества и др.), по нашему мнению, не порождает возникновения рас-

сматриваемого права, в том числе и в случаях какой-либо причастности к этой деятельности определенных лиц. Не приводит к возникновению такого права также и вынесение постановления по фактам безвестного исчезновения лиц в случаях отсутствия какой-либо противоправной деятельности и самих возможных субъектов такой деятельности, а также причастных к такой деятельности лиц. Закон в данном случае не предоставляет право такого ознакомления и другим участникам уголовного процесса (например, заявителю) даже при условии их непосредственной заинтересованности в получении таких сведений для реализации своих прав и законных интересов (например, осуществления обжалования процессуального решения или подготовки гражданского иска).

Таким образом, по результатам настоящего исследования можно сделать вывод о возможности возникновения рассматриваемого права граждан на ознакомление со сведениями оперативно-розыскной деятельности при вынесении решений об отказе в возбуждении уголовного дела по всем их деяниям только при наличии реабилитирующих обстоятельств, в установленных законодательством пределах и с ограничениями такого ознакомления. Результаты исследования могут использоваться для дальнейшего совершенствования законодательства и непосредственно в правоприменительной практике.

УДК 342.9

В.А. Лысенко

ПРЕДОТВРАЩЕНИЕ КОНФЛИКТА ИНТЕРЕСОВ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ КАК ЭЛЕМЕНТ АНТИКОРРУПЦИОННОЙ ПОЛИТИКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Конфликт интересов является многоаспектной теоретико-практической категорией, исследуемой в различных отраслях – социологии, этике, управлении, праве. Как правовая категория конфликт интересов представляет особую значимость, что обусловлено его неоднозначностью и сложностью в юридической науке и законодательной системе.

Многоаспектность и сложность конфликта интересов заключается во взаимосвязи личных интересов сотрудников и их служебными обязанностями, а также последствиями, возникающими в результате подобных конфликтов.

В российской науке комплексные исследования данной категории начали проводиться с 2004 г. Это было связано с закреплением конфликта

интересов в законодательстве о государственной службе. Однако научно-методический подход к предупреждению подобных ситуаций значительно отставал – отсутствовало понимание процедур предотвращения конфликта интересов, типовых случаев, определение подразделений, предупреждающих конфликт интересов.

В ч. 1 ст. 10 Федерального закона Российской Федерации от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции» (далее – ФЗ РФ № 273) содержится понятие «конфликт интересов».

Конфликт интересов – это ситуация, при которой личная заинтересованность (прямая или косвенная) лица, замещающего должность, замещение которой предусматривает обязанность принимать меры по предотвращению и урегулированию конфликта интересов, влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им должностных (служебных) обязанностей (осуществление полномочий).

Обязанность принимать меры по предотвращению конфликта интересов возлагается на государственных служащих (ч. 3 ст. 10 ФЗ РФ № 273).

Кроме того, в указанном законе ничего не говорится о степени влияния личной заинтересованности, о размере возможного дохода, о характере и содержании необъективного и пристрастного исполнения должностных полномочий, что является чрезвычайно важным для квалификации ситуаций конфликта интересов. В связи с этим полагаем целесообразной подготовку специального методического обеспечения порядка оценки личной заинтересованности и квалификации конфликта интересов.

Представляется, что случай, когда личная заинтересованность имеет незначительный характер, не должен квалифицироваться в качестве конфликта интересов. Например, работник государственной корпорации имеет акции завода, входящего в контур ее управления, однако размер этой доли незначителен и не позволяет оказывать сколь-либо ощутимое влияние на решения общего собрания акционеров.

Несмотря на то что перечень способов урегулирования конфликта интересов, установленный в ст. 11 ФЗ РФ № 273, в научной литературе характеризуется как несовершенный, не способствующий полноценной профилактике и предупреждению конфликта интересов, он представляется достаточно полным.

Предупреждение конфликта интересов в системе органов внутренних дел является необходимой задачей, реализация которой обеспечит высокий уровень доверия к сотрудникам правоохранительных органов. Современные механизмы предотвращения конфликта интересов включают в себя меры, обеспечивающие соблюдение этических норм и позволяющие минимизировать риски возникновения подобных случаев. К таким механизмам можем отнести следующие:

регулярное проведение тренингов и семинаров, разъясняющих сотрудникам риски и возможные последствия конфликта интересов;

реализация информационных кампаний (например, выведение на экраны видеороликов о способах предотвращения конфликта интересов);

создание анонимных каналов для сообщений (горячие линии, онлайн-платформы), целью которых будет формирование безопасной среды для информирования об обнаруженных случаях конфликта интересов;

создание механизмов внутреннего контроля для анализа действий сотрудников на предмет конфликтов интересов;

формирование антикоррупционной культуры, где руководитель прививает высокие этические стандарты, а также поддерживает антикоррупционные инициативы;

привлечение независимых аудиторов для выявления возможных конфликтов интересов.

Подводя итоги данного исследования, отметим, что конфликт интересов является проблемой, требующей комплексного подхода к ее предотвращению. Данное явление имеет глубокие исторические корни и продолжает оставаться актуальным в современных условиях. В связи с этим важно формировать прозрачные механизмы контроля, выявляющие и предотвращающие конфликты интересов. Необходимо, чтобы антикоррупционные инициативы не имели формальный характер и активно внедрялись в работу органов внутренних дел.

УДК 343.985.8

А.О. Мартынов, И.О. Анишкевич

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ: ГЕНЕЗИС И СОВРЕМЕННОЕ СОСТОЯНИЕ

Анализ этапов развития информационных технологий свидетельствует о тесной взаимосвязи каждого из них со сферой противодействия преступности. Применение информационных технологий в контексте выявления и раскрытия преступлений имеет свою историческую динамику, которая проявляется через эволюционные этапы их использования для решения задач в данной области.

Развитие и внедрение информационных технологий можно разделить на эволюционные этапы. Начальным этапом принято считать возникновение человеческой речи, ставшей отправной точкой и заложившей основы для кодирования, передачи, хранения и обработки информации. Она же создала постоянную потребность в разработке новых и более эффективных средств коммуникации. Современные информационные технологии, по сути, являются продолжением и развитием тех принципов и функций, которые изначально были реализованы в человеческой речи. Необходимость фиксировать, сохранять и распространять речь привела к созданию письменности, которая, в свою очередь, стала мощным стимулом для развития других технологий. Так, в XV в. получило распространение книгопечатание и, соответственно, появление первых типографий.

Ограничения речи (например, невозможность передавать информацию на большие расстояния или сохранять ее на длительное время) стимулировали изобретение новых средств коммуникации. В этой связи период с конца XIX – начала XX в. связывают с изобретением и распространением средств передачи информации, радио, телеграфа, телефона, что, по мнению ученых, является переломным и кульминационным этапом в контексте развития информационных технологий. В середине XX в. изобретаются и распространяются телевидение и электронно-вычислительные машины, а в конце этого же века появляется World Wide Web или, другими словами, Всемирная паутина. Каждое из этих изобретений можно рассматривать как попытку расширить, улучшить и усовершенствовать возможности, заложенные в человеческой речи.

Глобальная компьютерная сеть Интернет стала важным источником информации, в том числе о лицах и фактах, представляющих оперативный интерес. В современных условиях оперативные сотрудники довольно часто получают необходимые сведения посредством мониторинга сайтов организаций, социальных сетей и интернет-профилей лиц, имеющих отношение к преступной деятельности. В этих условиях использование современных информационных технологий является эффективным инструментом для должностных лиц органов, осуществляющих оперативно-розыскную деятельность (ОРД).

Так, к числу эффективных инструментов поиска и обнаружения информации в сети Интернет следует отнести программные продукты по проведению разведывательно-поисковых мероприятий в открытых источниках, иными словами, использование технологии OSINT (Open Source Intelligence). Наиболее часто указанный поиск осуществляется посредством применения программных продуктов или ботов в мессенджере Telegram. Такие telegram-боты позволяют получить широкий

спектр информации об интересующем правоохранительные органы лице: его приблизительный адрес нахождения и место жительства, полные анкетные данные (фамилия, имя, отчество, дата рождения), место работы, используемый номер мобильного телефона, аккаунты в социальных сетях и многое другое. В качестве примеров телеграм-каналов, которые могут быть использованы для проведения интернет-разведки, можно привести: «Интернет-Розыск | OSINT | Киберрасследования», «OSINT | Форензика», «OSINT Беларусь» и др. В указанных каналах содержатся: большое количество разнообразной информации по рассматриваемой тематике, включая обучающие материалы, статьи, руководства по поиску и анализу информации из открытых источников; обзоры, ссылки, инструкции по использованию различных инструментов для OSINT; информация о новых инструментах, методах, изменениях в политике конфиденциальности различных платформ; анализ конкретных кейсов, разбор техник, используемых в рассматриваемой деятельности; ссылки на полезные сайты, блоги, форумы, базы данных и другие источники информации; советы по защите своей приватности и анонимности в сети, использованию VPN и др.

Значимость метода поиска и обнаружения информации, представляющей оперативный интерес, в сети Интернет заключается в его общедоступности, простоте использования, наличии огромного и постоянно нарастающего объема цифровых данных как источника оперативно значимой информации, глобальном распространении сети Интернет, где человеку все сложнее оставаться невовлеченным в процессы цифровизации общественных отношений и удовлетворять свои потребности традиционным образом.

Следует отметить, что в настоящее время информационные технологии в ОРД активно применяются при создании и использовании автоматизированных информационных систем (АИС) оперативно-розыскного назначения. Их создание и применение обусловлены сложностью системы уголовной регистрации, разнообразием объектов, попадающих в сферу оперативно-розыскной и процессуальной деятельности органов, осуществляющих ОРД, необходимостью повышения управленческих и оперативных возможностей подразделений криминальной милиции. Целями применения АИС в ОРД органов внутренних дел являются обеспечение оперативного сотрудника информацией высокого качества и возможность оперативного пополнения этой информации в ходе осуществления ОРД.

Сегодня в Республике Беларусь для достижения целей ОРД используются различные АИС и автоматизированные банки данных, позволяющие решать широкий спектр задач, среди которых: установление полных анкетных данных лиц, сведений о похищенном имуществе, угнан-

ном транспорте, информация о дорожно-транспортных происшествиях, финансовых операциях, банковских счетах, совершенных и регистрируемых правонарушениях и происшествиях и др.

Активное развитие информационных технологий обусловливает внедрение передовых программных продуктов в повседневность. Не стала исключением деятельность сотрудников оперативных подразделений в части проведения отдельных оперативно-розыскных мероприятий. Так, в настоящее время на рабочих местах оперативных сотрудников установлено специальное программное обеспечение, оснащенное искусственным интеллектом. Данное программное обеспечение значительно расширяет возможности оперативного сотрудника, так как автоматизирует ряд повседневных задач (процесс обработки и анализа больших объемов информации, выявления скрытых связей и закономерностей, мониторинг открытых источников и т. п.), что, безусловно, повышает эффективность ОРД.

Отдельно стоит отметить республиканскую систему мониторинга общественной безопасности, играющую немаловажную роль в деятельности сотрудников оперативных подразделений. Предусмотренная программным интерфейсом возможность идентифицировать лица и различные объекты на видеозаписях, анализировать поведение людей и выявлять противоправные действия способствует повышению эффективности оперативных подразделений в сфере борьбы с преступностью.

Подводя итог изложенному, можно сделать вывод, что внедрение передовых информационных технологий в ОРД предоставило значительные возможности сотрудникам оперативных подразделений для поиска, обработки и анализа различных данных. В современных условиях использование информационных технологий в оперативно-служебной деятельности органов, осуществляющих ОРД, – это не просто техническое обновление, а обусловленная необходимость эффективной борьбы с преступностью.

УДК 343.985.8

А.О. Мартынов, К.А. Ерофеев

НЕКОТОРЫЕ АСПЕКТЫ ВЫЯВЛЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК

Государственные закупки являются важным элементом обеспечения деятельности государственных органов и организаций. Они характеризуются значительными объемами расходования бюджетных средств, что делает данную сферу привлекательной для совершения противоправных

деяний. Выявление преступлений в данной сфере представляет собой комплекс мер, направленных на обнаружение признаков нарушений порядка организации и проведения процедур закупок, а также на установление фактов подготовки, совершения или сокрытия противоправных деяний в указанной сфере. Этот процесс предполагает сбор, анализ и оценку информации, что требует применения комплекса оперативно-розыскных и иных мероприятий.

Процесс выявления преступлений в сфере государственных закупок может осуществляться по различным направлениям. Одно из них связано с получением информации из различных источников о возможных нарушениях. Так, обращения граждан становятся основой для проведения проверок, в рамках которых запрашиваются и анализируются документы, связанные с конкретной процедурой закупки, проводятся опросы участников и иные действия, направленные на подтверждение или опровержение фактов противоправной деятельности.

Следующее направление предполагает самостоятельный поиск информации о признаках преступлений, заключающийся в мониторинге открытых источников (электронных площадок, реестров контрактов и отчетов) с целью обнаружения признаков, указывающих на нарушения. Значительную роль в выявлении преступлений указанной категории играют оперативно-розыскные мероприятия (ОРМ), целью которых является сбор информации о лицах, причастных к противоправной деятельности, анализ их связей, а также документирование конкретных фактов противоправной деятельности.

Важным источником информации для выявления преступлений являются сведения, полученные от лиц, обладающих специальными знаниями о процедурах проведения закупок, включая должностных и уполномоченных представителей, участвующих в подготовке и размещении заказов, членов закупочных и приемочных комиссий, экспертов, ответственных за оценку предложений (определение особенностей проведения отдельных этапов процедур на практике), а также специалистов, обеспечивающих исполнение договоров, организаторов электронных торгов и представителей банков. В ряде случаев эффективным является привлечение специалистов-экономистов и специалистов-бухгалтеров (в части изучения документов, отражающих целесообразность и обоснованность проведения процедуры, а также отражения ее результатов в документах бухгалтерского, финансового или иного учета). Возможно также привлечение специалистов в конкретной области деятельности: специалистов-товароведов (в части оценки качества, подлинности и соответствия товара (работы, услуги) заявленным характеристикам),

специалистов в области строительства или инженерного дела (в части оценки качества выполненных работ) или иных лиц, в зависимости от специфики конкретных процедур государственных закупок.

Получение информации, представляющей оперативный интерес, может быть выражено в различных формах.

Одной из таких форм можно считать проведение оперативного опроса лица, обладающего специальными знаниями, и получение от него консультации о том или ином аспекте организации или проведения процедур государственных закупок, исполнения договора, что в ряде случаев позволит определить признаки, указывающие на противоправную деятельность субъектов, или установить размер причиненного ущерба.

Изучение объектов, полученных в рамках проведения комплекса ОРМ, довольно часто требует наличия определенных компетенций у сотрудников подразделений по борьбе с экономическими преступлениями. Такое изучение направлено на обнаружение и фиксацию следов противоправной деятельности, изъятие предметов и документов, которые в последующем могут стать источниками доказательств. В этой связи в ряде случаев видится целесообразным привлекать специалистов в конкретной области в целях изучения значительного числа различных документов либо когда для их анализа требуются специальные знания (например, в области бухгалтерского учета).

Не менее эффективным способом выявления преступлений в сфере государственных закупок является анализ данных, доступных на специализированных электронных площадках, например, автоматизированной информационной системы «Электронные счет-фактуры» (АИС «ЭСФ») или иные системы, аккумулирующие информацию о проведении операций, связанных с приобретением организаций какого-либо рода товаров. Этот процесс включает в себя детальное изучение сведений о контрагентах, участвующих в последних сделках, с целью выявления подозрительных связей или аномалий в их активности, а также исследование цен заключенных договоров путем сопоставления фактических значений с первоначально заявленными параметрами и среднерыночными показателями.

Сведения, полученные из АИС «ЭСФ», также могут позволить выявить вероятное завышение стоимости предмета государственных закупок при наличии законодательных ограничений на ценообразование для определенных категорий товаров. Такими ограничениями могут выступать предельные максимальные надбавки импортера на реализуемые потребительские товары, выраженные в процентах, или установленные нормативы стоимости материалов, применяемых при строительстве

зданий и сооружений, что служит основой для дальнейшего анализа возможных нарушений.

Таким образом, выявление преступлений в сфере государственных закупок представляет собой многоаспектный процесс, основанный на сведениях, полученных в результате проведения комплекса ОРМ, анализа данных специализированных информационных систем, привлечения специальных знаний участников закупочных процессов или иных лиц и мониторинг рисков и угроз. Только при условии системного подхода возможно не только обнаружение противоправных действий, но и создание условий для их предотвращения, что в конечном итоге будет способствовать обеспечению законности и эффективности расходования бюджетных средств в сфере государственных закупок.

УДК 343.985

В.Ю. Мезяк

СУДЕБНО-БУХГАЛТЕРСКОЕ ИССЛЕДОВАНИЕ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Экономические преступления представляют значительную угрозу для стабильности хозяйственной деятельности и требуют эффективных методов выявления и расследования. В условиях усложнения экономических процессов и роста объемов документооборота правоохранительные органы сталкиваются с необходимостью поиска новых подходов к анализу бухгалтерской документации, которая является ключевым источником доказательств при раскрытии преступлений экономической направленности.

Исследованиями в области криминалистического анализа бухгалтерской документации для выявления экономических преступлений занимались такие ученые, как С.П. Фортинский, Я.В. Орлов, В.Г. Танасевич и др. Их работы посвящены разработке теоретических основ и практических методов анализа учетных данных, включая изучение признаков подлога и расхождений в документообороте. Вместе с тем указанные авторы преимущественно фокусировались на традиционных аспектах анализа первичной документации, тогда как С.П. Голубятников предложил более широкий взгляд, акцентируя внимание на значимости периодической отчетности и сравнительного анализа.

По мнению С.П. Голубятникова, для достоверного установления фактов подлога и выявления скрытых обстоятельств преступной дея-

тельности возможно применение метода расширенной проверки документации и метода расширения круга исследуемых документов.

Метод расширения круга исследуемых документов позволяет выявлять подложные документы, относящиеся к анализируемой хозяйственной операции, при этом ранее не являющиеся объектом изучения; к операциям, однотипным с анализируемой; к материалам периодической отчетности, предоставляемой в вышестоящие организации, и др.

Следует отметить, что С.П. Голубятников впервые в криминалистической литературе обращает внимание на значимость изучения периодической отчетности как важного источника информации при выявлении экономических преступлений. Методологическая основа рассматриваемого подхода базируется на принципе прямого и косвенного отражения хозяйственных операций. Каждая экономическая операция находит: прямое отражение в первичных учетных документах, непосредственно фиксирующих ее содержание и косвенное отражение в сопутствующей документации, косвенно подтверждающей факт совершения операции. Иллюстративно можно привести пример, когда операция по перечислению денежных средств за товары непосредственно документируется платежными поручениями (прямое отражение), тогда как товарно-транспортные накладные служат ее косвенным подтверждением.

Этот метод имеет сходство с предложенным С.П. Фортинским «методом глубокого анализа» при исследовании сомнительных бухгалтерских документов. Однако он более структурирован и доступен для практического применения правоохранительными органами.

Замаскированные хищения, как правило, находят свое отражение в учетных данных, а следы этих преступлений могут быть установлены правоохранительными органами с использованием специальных методов. Экономические преступления могут находить свое отражение в учетных данных в трех основных формах: внутренние противоречия реквизитов отдельных документов; расхождения между содержанием взаимосвязанных документов; отклонение от обычного движения товарно-материальных ценностей и денежных средств. С.П. Голубятниковым также разработан метод сравнительного анализа учетной документации, обладающий признаками общего приема криминалистического исследования. Сущность данного метода заключается в сопоставлении содержательной части совокупности документов, фиксирующих однородные хозяйственные операции, с последующим выявлением статистических отклонений специально рассчитанных параметров. В качестве анализируемых показателей могут выступать: средние весовые характеристики товарных единиц (например, средний вес тарного места), количественные параметры материальных ценностей (размерные показатели штучных товаров), физико-химические свойства сырьевых ресурсов (уровень влажности, плотность) и иные количественно измеримые характеристики, поддающиеся формализации. Указанный подход позволяет выявлять аномалии в документообороте посредством применения статистических методов анализа, что существенно повышает эффективность процессуальной проверки учетных данных при расследовании преступлений экономической направленности. Наиболее эффективен данный метод при выявлении фактов систематических хищений материальных ценностей, замаскированных под легальную хозяйственную деятельность.

Таким образом, можно сделать вывод о том, что в настоящее время заложены основы развития эффективных методов выявления экономических преступлений, такие как расширенная проверка документации и расширение круга исследуемых документов, а изучение периодической отчетности и метод сравнительного анализа позволяют выявлять аномалии в документообороте посредством статистических подходов.

УДК 34.096

С.Ю. Мельников

ЮРИДИЧЕСКАЯ ПРИРОДА ПОСТАНОВЛЕНИЯ И РЕШЕНИЯ О ПРОВЕДЕНИИ ОПЕРАТИВНО-РОЗЫСКНОГО МЕРОПРИЯТИЯ, А ТАКЖЕ ПИСЬМЕННОГО ЗАПРОСА

Частью первой ст. 19 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон) установлено, что оперативно-розыскное мероприятие проводится по постановлению о проведении оперативно-розыскного мероприятия (далее – постановление) или по решению должностного лица органа, осуществляющего оперативно-розыскную деятельность (ОРД), без вынесения постановления (далее – решение) или по письменному запросу органа, осуществляющего ОРД (далее – запрос). В отдельных нормах Закона, а именно части четвертой ст. 34, части первой ст. 35, 36 и 38 и части второй ст. 36, постановление понимается как основание проведения оперативно-розыскного мероприятия. В остальном тексте слово «основание» не применяется к постановлению, а, как и в ст. 19, используется предлог «по». Одновременно ст. 16 Закона закрепляет тринадцать оснований проведения оперативно-розыскных мероприятий. В таком смысле слово «основание» используется в большей части текста Закона. Причем среди оснований, предусмотренных ст. 16, постановления нет.

Такая вариативность использования слова «основание» применительно к оперативно-розыскным мероприятиям в тексте Закона, на наш взгляд, нежелательна, так как может привести к ложным субъективным толкованиям норм, учитывающим интересы не законодателя, а, например, конкретного правоприменителя или правонарушителя. Более того, она недопустима, потому что противоречит таким требованиям нормотворческой техники, как исключение различного толкования предписаний, отсутствие внутренних противоречий, единообразие и однозначность терминологии закона, предусмотренным ст. 28 Закона Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах».

В связи с этим вопрос о природе постановления, решения и запроса получает особую актуальность. Рассмотрим несколько вариантов его решения.

1. Постановление, решение и запрос являются основаниями проведения оперативно-розыскного мероприятия. В подтверждение данного варианта обратим внимание, что в ст. 16 Закона словосочетание «оперативно-розыскные мероприятия» фигурирует в множественном числе, а в нормах, где под основанием понимается постановление, – в единственном или используется название конкретного оперативно-розыскного мероприятия. Другими словами, тринадцать оснований, закрепленных в ст. 16 Закона, являются таковыми для проведения оперативно-розыскных мероприятий вообще. А постановление, решение и запрос – основания для проведения конкретных оперативно-розыскных мероприятий. Однако такая аргументация не выдерживает критики, если учесть, что указанная закономерность не прослеживается во всем тексте Закона. Так, уже в части третьей ст. 19 Закона слово «основания» (в смысле ст. 16) использовано со словосочетанием «оперативно-розыскное мероприятие» (в единственном числе).

2. Постановление, решение и запрос – это основные условия проведения оперативно-розыскных мероприятий. На первый взгляд это логично, так как норма, предусматривающая их, расположена в первой части статьи, называющейся «Общие условия проведения оперативно-розыскного мероприятия». В целом термин «условия проведения оперативно-розыскных мероприятий» имеет очень широкое значение, которое включает в себя все нормы о проведении оперативно-розыскных мероприятий, в том числе основания, предусмотренные ст. 16 Закона. В связи с чем выделение постановления, решения и запроса в качестве основных условий, а значит остальных, в том числе оснований, предусмотренных ст. 16 Закона, – в качестве дополнительных, незначительных, вспомогательных или второстепенных нелогично, так как

основания проведения оперативно-розыскных мероприятий, предусмотренные ст. 16 Закона, имеют первичное значение для принятия решения о проведении оперативно-розыскного мероприятия.

3. Постановление, решение и запрос – это правовые формы решения о проведении оперативно-розыскного мероприятия. Ведь естественно, что проведение оперативно-розыскного мероприятия по постановлению или запросу не исключает факта принятия уполномоченным на то должностным лицом органа, осуществляющего ОРД, решения о проведении оперативно-розыскного мероприятия на основании, предусмотренном ст. 16 Закона. Такой вариант наиболее согласуется с текстом Закона и не создает предпосылок для двойственного толкования оснований проведения оперативно-розыскных мероприятий. А имеющиеся в тексте Закона единичные случаи использования словосочетания «основание проведения оперативно-розыскного мероприятия» применительно к постановлению являются технической ошибкой, требующей корректировки.

Таким образом, мы пришли к выводу, что подход к пониманию юридической природы постановления о проведении оперативно-розыскного мероприятия, решения должностного лица органа, осуществляющего ОРД, без вынесения постановления о проведении оперативно-розыскного мероприятия и письменного запроса органа, осуществляющего ОРД, при котором они представляются как правовые формы решения о проведении оперативно-розыскного мероприятия, наиболее приемлем.

УДК 343.98

М.В. Меркулова

О НЕКОТОРЫХ ТЕХНИЧЕСКИХ ПРОБЛЕМАХ ФИКСАЦИИ И ИЗЪЯТИЯ ЦИФРОВОЙ ИНФОРМАЦИИ В ХОДЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ

В рамках расследования преступлений в сфере компьютерной информации или совершаемых с помощью информационных технологий важнейшее криминалистическое значение приобретает информация, находящаяся на запоминающих устройствах и носителях данных, которая может быть получена в ходе осмотра места происшествия, обыска или выемки. При этом ключевой задачей следователя становится принятие мер к недопущению потери указанной информации.

Интересующая следствие цифровая информация может находиться на различных типах запоминающих устройств – во внешней и внутренней памяти компьютера.

Внешняя память включает в себя цифровые устройства для хранения данных и переноса их на другие аналогичные устройства. Она является энергонезависимой и сохраняет информацию при выключении компьютера. К устройствам внешней памяти относятся: жесткие диски (HDD и SSD) памяти, флеш-карты, DVD- и CD-диски – т. е. носители информации, которые могут быть изъяты в ходе следственного действия и впоследствии приобщены к уголовному делу в качестве вещественных доказательств.

Внутренняя память отвечает за «жизнеобеспечение» и скорость работы устройства; информация здесь хранится как постоянно, так и временно. Устройства внутренней памяти подразделяются на несколько видов: постоянное запоминающее устройство, оперативная память (ОЗУ), кэш-память. Во время работы компьютера ОЗУ сохраняет системные файлы и данные, которые удаляются при перезагрузке или выключении устройства (т. е. при отсутствии внешнего энергоснабжения). Файлы приложений и программ сохраняются только на время их работы, по окончанию их функционирования – удаляются. Данный вид памяти (Random Access Memory) является энергозависимым, поэтому информацию с ОЗУ возможно получить только при работающем компьютере.

Существует несколько способов получения информации из энергозависимой памяти компьютера в виде так называемого слепка (дампа). Один из них заключается в использовании специализированного программного обеспечения, например, DumpIt, Process Explorer или же Belkasoft Live Ram Capturer, которое активно используют криминалисты.

При невозможности изъятия носителей информации возникает необходимость ее копирования, в том числе посредством создания точной копии носителя информации – образа диска (image) – файла, несущего в себе полную копию содержимого и структуры файловой системы и данных, находящихся на жестком диске или в его разделе. Сформировать такие файлы можно посредством как программного, так и аппаратного обеспечения. Так, для работы с жестким диском применяется различное программное обеспечение: Acronis True Image, Paragon Hard Disk Manager, Todo Backup, AOMEI Backupper, R-Drive Image и ряд других. Создание образа флеш-карты можно произвести, например, с помощью программы USB Image Tool. В числе аппаратных средств следует упомянуть компактные дубликаторы (duplicator) и блокираторы записи (bridge), не позволяющие записать что-либо на исследуемый накопитель и используемые для максимально возможного сохранения целостности исследуемых данных.

Отметим, что создание образов дисков нередко ассоциируют с клонированием дисков. Хотя оба процесса копируют дисковые данные, между

ними имеется различие. Клонирование диска с операционной системой копирует содержимое и создает загрузочный раздел (т. е. создает точную функциональную копию), а создание образов дисков создает только резервную копию содержимого диска. Во время клонирования диска создается один большой файл (обычно сжатый), который впоследствии используется для восстановления. Наиболее полным программным обеспечением для клонирования является Clonezilla – программа с открытым исходным кодом, которая поддерживает почти все файловые системы, что позволяет клонировать Windows, Linux, Mac OS X и Chrome OS.

При копировании информации с жесткого диска на USB-накопитель в ходе следственного действия может возникнуть проблема, связанная с повреждением файлов при их передаче. Основная причина проблемы – неисправный USB-накопитель (например, в силу наличия в нем поврежденного сектора). Кроме того, к повреждению файлов на USB-накопителе может приводить неправильное копирование или заражение компьютерным вирусом. В связи с этим возникает необходимость определения целостности файлов при их передаче и хранении. Для этого можно, например, просмотреть свойства файла и определить его атрибуты, формируемые системой в зависимости от системного времени, установленного на компьютере. Однако эти атрибуты можно умышленно изменить: установить самостоятельно дату, время, «подогнать» размер файла и т. д. Поэтому оптимальным способом определения целостности полученной информации являются вычисление и сравнение контрольных суммы файлов (хэш-кодов) – значений, рассчитанных для файлов путем применения определенного алгоритма и используемых для проверки целостности данных при их передаче и хранении, а также для сравнения двух наборов данных на неэквивалентность. Этот атрибут подделать практически невозможно.

Контрольная сумма (хэш-сумма) или хэш-код – это строка бит, являющаяся выходным результатом хэш-функции. Хэш-функция (от англ. hash – «мешанина»), или функция свертки – функция, преобразующая массив входных данных произвольного размера в выходную битовую строку определенного (установленного) размера в соответствии с определенным алгоритмом. Она преобразует любой фрагмент данных (текстовый файл, изображение и т. д.) в фиксированную строку чисел и букв. Преобразование, выполняемое хэш-функцией, называется хэшированием.

Подсчет контрольной суммы для файла, располагающегося на определенном носителе, можно выполнить с помощью файлового менеджера Total Commander, но существует и более простое решение подсчета и сравнения хэш-кодов – с помощью приложения Hash Tab. Данная программа представляет собой расширение Проводника Windows, после установки которого при просмотре свойств любого файла в соот-

ветствующем окне появляется новая вкладка «Хэш-суммы файлов». При этом достаточно использовать функцию «Сравнить файл…», указать на сравниваемый файл – и в окне «Сравнение хэша» будет выведен результат совпадения контрольных сумм.

Результат применения алгоритмов хэширования Message Digest Version 5, Secure Hash Algorithm Version 1 и Secure Hash Algorithm Version 2 к документу Word размером 161242 байт и состоящим из одной страницы с графическим изображением и текстом выглядит следующим образом:

MD5: ece11a3d6adae84d89a24d22e99b7319
SHA1: 7893b3c12f30db01abf4d6de12762fae1f37f874
SHA256: ab971590ac4973745ddf6c24b92eec49d732097f39cf6df3903b6436b4511394
SHA512: 9435ba60b560ba664ed16a52bb1335e3786f175653753e925253e36ed3a72435 89a232eb4ec4fb8c5d9924ba6a5dd451de33013239d9b2b3b3200710e39c1b16

Нередко в ходе расследования киберпреступлений возникают ситуации, когда необходимо установить интернет-сайт (платформу), откуда были скачаны определенные файлы, вредоносные программы и т. п. Так, в уголовных делах о мошенничестве в сфере компьютерной информации (ст. 159.6 Уголовного кодекса Российской Федерации) часто фигурируют названия интернет-сайтов (платформ), с которых были скопированы вредоносные программы, использовавшиеся преступниками для совершения хищений. Как правило, в дальнейшем указанные обстоятельства не исследуются должным образом, хотя несложная операция подсчета и сравнения хэш-кодов файлов позволила бы получить дополнительную доказательственную информацию, связанную с использованием конкретного интернет-сайта (платформы) в качестве «поставщика» нелегального контента.

УДК 34

Д.Ф. Минзянова

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Современные технологии играют революционную роль в практике борьбы с преступностью, предоставляя правоохранительным органам новые инструменты и возможности для предотвращения, расследования и реагирования на преступления. Их использование постоянно расширяется и становится все более интегрированным в повседневную работу полиции и других правоохранительных органов.

Основные направления использования современных технологий в борьбе с преступностью:

1. Предотвращение преступлений:

1.1. Системы видеонаблюдения и интеллектуальный анализ видео. Умные камеры с функцией распознавания лиц, анализа поведения и автоматического оповещения о подозрительных событиях помогают предотвращать преступления в общественных местах, на транспорте и в жилых районах.

1.2. Предиктивная аналитика и «горячие точки» преступности. Алгоритмы машинного обучения анализируют исторические данные о преступлениях для прогнозирования места и времени наиболее вероятного совершения преступления. Это позволяет органам внутренних дел более эффективно распределять ресурсы и проводить профилактические мероприятия в «горячих точках».

1.3. Системы оповещения и информирования населения. Мобильные приложения, социальные сети и другие цифровые каналы используются для оперативного оповещения граждан о потенциальных угрозах, совершенных преступлениях, розыске преступников и для предоставления советов по безопасности.

2. Расследование преступлений:

2.1. Цифровая криминалистика. Извлечение, анализ и интерпретация цифровых данных с компьютеров, мобильных телефонов, жестких дисков и других электронных устройств играют ключевую роль в расследовании большинства современных преступлений. Специализированное программное обеспечение и оборудование помогают восстанавливать удаленные данные, анализировать логи, сообщения, геолокацию и другую цифровую информацию.

2.2. Биометрические технологии:

распознавание лиц, которое используется для идентификации подозреваемых по видеозаписям, фотографиям и базам данных;

дактилоскопия (цифровая). Автоматизированные системы идентификации отпечатков пальцев значительно ускоряют процесс идентификации и сравнения отпечатков;

генетическая дактилоскопия. Быстрые и точные методы ДНК-анализа позволяют идентифицировать преступников по биологическим следам, оставленным на месте преступления.

2.3. Анализ больших данных и искусственный интеллект, которые используются для анализа огромных объемов данных из различных

источников (базы данных полиции, социальные сети, открытые источники, данные видеонаблюдения и т. д.) для выявления связей, закономерностей, профилей преступников и раскрытия сложных преступных схем. Сбор и обработка больших объемов персональных данных, особенно биометрических, вызывают опасения по поводу нарушения приватности и злоупотребления информацией.

2.4. Системы геолокации и отслеживания, которые используются для отслеживания передвижений подозреваемых, установления алиби и восстановления хронологии событий.

3. Анализ и прогнозирование преступности:

3.1. Геоинформационные системы и картографирование преступности позволяют визуализировать на карте данные о преступлениях, анализировать пространственные закономерности, выявлять «горячие точки» и оптимизировать маршруты патрулирования.

3.2. Мониторинг открытых источников и социальных сетей позволяет выявлять потенциальные угрозы, отслеживать распространение экстремистских идей, изучать общественное мнение и выявлять преступные группы.

3.3. Статистический анализ и моделирование используются для анализа трендов преступности, прогнозирования будущих преступлений и оценки эффективности различных методов борьбы с преступностью.

Следует отметить, что современные технологии являются мощным инструментом в борьбе с преступностью, но их эффективное и этичное использование требует комплексного подхода, который включает в себя:

инвестиции в развитие технологий и обучение персонала;

разработку четких правовых и этических норм;

международное сотрудничество в борьбе с трансграничной преступностью и киберпреступностью;

открытость и прозрачность в использовании современных технологий правоохранительными органами;

учет интересов и прав граждан при внедрении новых технологий.

Только при таком подходе современные технологии смогут стать надежным союзником в борьбе за безопасность и правопорядок в современном мире. В целях предупреждения дальнейшего развития преступности в сфере информационно-телекоммуникационных технологий органы государственной власти должны осуществлять задачи по предупреждению преступлений в условиях цифровизации общественных отношений.

Таким образом, сотрудники органов внутренних дел имеют возможность осуществлять сбор необходимых оперативно значимых и аналитических сведений о преступлениях и преступниках с использованием

современных технологий с определенными цифровыми (виртуальными) следами, например, изучая историю просмотров (через cookie) и авторизации на различных интернет-ресурсах.

Современные технологии предоставляют мощный инструментарий для борьбы с преступностью, значительно повышая эффективность деятельности правоохранительных органов. Однако для их эффективного и этичного использования необходимо учитывать потенциальные риски и вызовы, разрабатывать четкие правовые и этические нормы, обеспечивать защиту персональных данных и предотвращать злоупотребление. Только при таком подходе современные технологии смогут стать надежным союзником в обеспечении безопасности и правопорядка в современном мире.

УДК 343

А.А. Муратова, Р.В. Глубоковских

ОПЕРАТИВНО-РАЗЫСКНОЕ ВЫЯВЛЕНИЕ, ПРЕСЕЧЕНИЕ И РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ СРЕДИ МОЛОДЕЖИ

В настоящее время интернет играет значимую роль в жизни каждого человека, но у всего хорошего всегда есть свои минусы. Так, перед оперативными сотрудниками органов внутренних дел стоит серьезная задача по пресечению, выявлению и раскрытию преступлений террористической направленности среди молодежи, поскольку именно интернет является источником передачи информации для осуществления террористической деятельности и вербовки.

В современном мире подростки проводят большую часть своей жизни в социальных сетях, просматривают различные видеоролики на разных платформах, в том числе запрещенных в Российской Федерации, прочитывают посты сообществ и закрытых телеграм-каналов. Кроме того, они с легкостью поддаются вербовке, а также, поскольку их сознание недостаточно зрелое, некоторые из них берут пример с преступников и видят в них своих кумиров. На данный момент самым распространенным проявлением подросткового терроризма является «скулшутинг» или «колумбайн» – разбойное нападение на учебные заведения, в основном школы, с целью массового убийства людей. Подростков на данное преступление побуждают высмеивания в школе, шутки и издевательства со стороны сверстников и учителей, из-за чего у них проявляются агрессия и ненависть, тем самым они хотят отомстить за это.

На ранних стадиях проявления агрессии возможно выявить подготавливаемое преступление.

Примером является массовое убийство в Казанской школе 11 мая 2021 г.

Ильназ Галявиев – преступник, совершивший теракт в гимназии, вел телеграм-канал, в котором писал о своих намерениях. Способами выявления со стороны правоохранительных органов может являться мониторинг телеграм-каналов, сообществ в социальной сети «ВКонтакте», а также выявление девиантного поведения ребенка со стороны родителей, кроме того родители должны поинтересоваться целью приобретения оружия. Одним из средств пресечения может выступать сотрудничество с IT-компаниями по блокировке контента террористической и экстремистской направленности.

Дополнительно упомянутому, у Ильназа появились поклонники, которые им восхищались, и в целях пресечения и профилактики преступления поклонников нужно проводить беседы с ними и их родителями, проводить мониторинг социальных сетей и направить интерес подростков на какие-либо молодежные проекты.

Помимо вышеизложенного, в связи с положением в стране, украинские спецслужбы осуществляют вербовку граждан Российской Федерации для осуществления терроризма в нашей стране. Вербовке также может поддаться молодежь, чьи отцы защищают Родину, или же подростки, которые ищут «легкие» деньги. Украинские спецслужбы путем злоупотребления доверием просят подростков совершить преступные деяния за предоставление информации (ложной) про родственников, которые находятся в зоне специальной военной операции или же за деньги. Для решения данной проблемы нужно выявлять и блокировать каналы вербовки, закрытые чаты и сообщества с террористическим содержанием, кроме того проводить анализ финансовых потоков, проверять переводы в запрещенные организации и поступления из них. Огромную помощь в выявлении, пресечении и раскрытии преступлений террористической направленности среди молодежи могут предоставить родители. Они, сообщая в территориальные органы внутренних дел о том, что их ребенку поступило сообщение о просьбе совершить деяние, устрашающее население и создающее опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях дестабилизации деятельности органов власти или международных организаций, помогают выйти на след террористических ячеек.

УДК 343.72

А.А. Олексюк, С.С. Курнавин

ОПЕРАТИВНО-РОЗЫСКНОЕ ОБЕСПЕЧЕНИЕ РАСКРЫТИЯ МОШЕННИЧЕСТВ ОБЩЕУГОЛОВНОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Под оперативно-розыскным обеспечением раскрытия мошенничеств общеуголовной направленности, совершаемых с использованием информационно-телекоммуникационных технологий (ИТТ), в общенаучном смысле следует понимать основанную на законах и подзаконных нормативно-правовых актах, организованную при определенных условиях, с учетом исходных оперативно-розыскных ситуаций, системную и комплексную деятельность оперативных работников по эффективному использованию имеющихся сил, методов и средств оперативно-розыскной деятельности (ОРД).

Общепринято включать в систему оперативно-розыскного обеспечения раскрытия преступлений следующие элементы:

теоретический элемент (правовые и нравственные основы, правовая и социальная защита, а также психологическая характеристика учеников ОРД);

организационный элемент (основания и условия проведения оперативно-розыскных мероприятий (ОРМ), оперативно-розыскное документирование преступной деятельности, агентурная разработка, розыскная работа, использование результатов ОРД в расследовании преступлений, алгоритмизация и программирование хода расследования);

материально-технический элемент (специальные технические средства и специальная техника, в том числе аппаратно-программные комплексы, информационно-поисковые системы, оперативные учеты).

К общим условиям оперативно-розыскного обеспечения относятся:

системное и комплексное использование сил, средств и методов оперативных органов;

самостоятельность оперативного работника и следователя в выборе путей получения информации и принятия решений, разграничение прав и обязанностей указанных субъектов;

своевременный обмен оперативно значимой информацией между оперативными службами, с использованием современных информационных технологий, позволяющих существенно повысить эффективность раскрытия преступлений.

Так, К.К. Горяинов и И.А. Иваньков отмечают, что в ходе применения информационных технологий для раскрытия преступлений возникают следующие проблемы:

в идентификации подлинности источника информации;

сохранности и обеспечении секретности следственной и оперативной информации;

материальном обеспечении внедрения и поддержки современных информационных технологий обмена, хранения и защиты информации.

Поддерживаем мнение ученых. Считаем необходимым отметить, что в целях оптимизации оперативно-розыскного обеспечения раскрытия преступлений необходимо внесение изменений в положения Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – ФЗ «Об ОРД») с учетом развития новых информационных технологий.

Так, в соответствии со ст. 2 ФЗ «Об ОРД» одной из задач оперативно-розыскной деятельности является выявление, предупреждение, пресечение и раскрытие преступлений, а также выявление и установление лиц, их подготавливающих, совершающих и совершивших. Между тем в текст ст. 46 Федерального закона Российской Федерации от 7 июля 2003 г. № 126-ФЗ «О связи» (далее – ФЗ «О связи») были внесены изменения Федерального закона Российской Федерации № 386-ФЗ, согласно которым абз. 9 п. 1 ст. 46 ФЗ «О связи» изложен следующим образом: «оператор связи обязан: прекратить оказание услуг связи при поступлении соответствующего запроса от органа, осуществляющего оперативно-розыскную деятельность… в случае предотвращения и пресечения преступлений с использованием сетей связи и средств связи».

Однако законодатель в положении ФЗ «Об ОРД» не наделил правом орган, осуществляющий ОРД, обращаться с мотивированным запросом о прекращении оказания услуг связи в случае предотвращения и пресечения преступлений.

В условиях отсутствия законодательного регулирования процедуры осуществления такого полномочия применение указанных норм ФЗ «О связи» в практической деятельности правоохранительных органов становится проблематичным, так как действующие положения п. 1 ст. 15 ФЗ «Об ОРД» наделяют правом уполномоченных субъектов при проведении ОРМ прерывать предоставление услуг связи только в случае:

а) возникновения непосредственной угрозы жизни и здоровью лица;

б) угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

Императивность ст. 15 ФЗ «Об ОРД» делает невозможным применение данной нормы в рамках деятельности по пресечению преступлений, посягающих на другие права граждан, в частности, права собственности.

Анализ судебной практики свидетельствует о существовании значительных проблем при необходимости прерывания услуг связи на территории исправительных учреждений в целях пресечения дистанционных хищений.

Считаем необходимым согласиться с мнением Б.П. Смагоринского и А.В. Сычева, которые обозначают, что в настоящее время законодателем предпринимаются шаги по противодействию данному явлению. В частности Федеральным законом Российской Федерации от 9 марта 2021 г. № 44-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории следственных изоляторов и учреждений, исполняющих уголовные наказания в виде лишения свободы» были дополнены положения ст. 82 Уголовно-исполнительного кодекса Российской Федерации, суть которых заключается в том, что в случаях выявления фактов использования осужденными на территории исправительного учреждения абонентских номеров подвижной радиотелефонной связи оказание услуг связи по этим абонентским номерам прекращается оператором связи на основании решения руководителя исправительного учреждения в письменной форме. Однако в указанном выше законе законодатель оставил без внимания субъекты ОРД, что оставляет обозначенную проблему нерешенной.

Учитывая изложенное, отметим, что закрепление в ФЗ «Об ОРД» полномочий правоохранительных органов на обращение с запросами (в интерпретации ст. 46 ФЗ «О связи») поспособствует дальнейшей работе по созданию нормативно-правовой базы, регулирующей порядок оформления, направления и исполнения указанных запросов, а также поспособствует исполнению оперативно-розыскными органами задач, направленных на пресечение хищений, совершаемых с использованием ИТТ.

УДК 159.9:34

Д.А. Пашкевич

РОЛЬ ПСИХОЛОГИЧЕСКОЙ ПОДГОТОВКИ КУРСАНТОВ ДЛЯ РАБОТЫ С ГРАЖДАНАМИ, ОКАЗЫВАЮЩИМИ СОДЕЙСТВИЕ НА КОНФИДЕНЦИАЛЬНОЙ ОСНОВЕ

Психологическая подготовка курсантов в процессе образования представляет собой одну из сторон формирования их профессиональной пози-

ции, раскрывающейся в форме взаимодействия с гражданами. Это взаимодействие предполагает не только передачу информации, но и сложную коммуникацию, где вербальные и невербальные сигналы, управление эмоциями, анализ поведения и преодоление когнитивных искажений становятся основой эффективности взаимодействия, что способствует оперативности в работе с гражданами на конфиденциальной основе. Рассмотрим структуру психологической подготовки в контексте задач, которые необходимо решать при выполнении служебной деятельности.

Структуру психологической подготовки можно представить следующими компонентами:

1. Вербальная и невербальная коммуникация, где вербальная коммуникация подразумевает обучение курсантов формулировать вопросы, использовать в своей речи точные фразы, избегая двусмысленности. Обучение невербальной коммуникации, в свою очередь, предполагает акцент на интерпретации жестов, мимики, тона голоса, дистанции в общении. Наиболее эффективным представляется форма проведения занятий в виде практических занятий с просмотром видеозаписи для анализа невербальных сигналов и последующие выполнения упражнений с акцентом на «язык тела», которые помогут закрепить полученные теоретические знания на практике.

2. Управление мышлением и эмоциями подразумевает под собой когнитивную рефлексию, когда курсанты учатся выявлять и корректировать искажения собственного мышления (например, стереотипы, предвзятость) для принятия более обоснованных и объективных решений в процессе профессиональной деятельности. Можно отметить также обучение эмоциональному контролю посредством освоения техник саморегуляции для сохранения хладнокровия в стрессовых ситуациях. С помощью рассмотрения случаев из практической деятельности, последующим анализом совершенных ошибок, а также выполнением упражнений с дыханием, визуализацией, медитативными практиками становится возможным сформировать навыки, которые позволят эффективно и этично взаимодействовать с гражданами, оказывающими содействие на конфиденциальной основе.

3. Понимание и прогнозирование поведения гражданина, оказывающего содействие на конфиденциальной основе, которые включают в себя: развитие навыка анализа действий собеседника, его реакций, изучение мотивов его поведения, а также его социальных особенностей, с целью достижения взаимодействия, необходимого для выполнения служебных задач.

Таким образом, психологическая подготовка курсантов для работы с гражданами, оказывающими содействие на конфиденциальной основе, – это не просто «дополнительный навык», а системный процесс, направленный на формирование профессионала, способного эффективно выполнять поставленную задачу, в том числе действуя не только по инструкции, но и гибко реагируя на человеческий фактор в зависимости от ситуации. Психологическая подготовка превращает абстрактные знания в практические навыки, которые становятся основой доверия между сотрудником и гражданами, оказывающими содействие на конфиденциальной основе.

УДК 343.985

В.И. Пикта

РЕВЕРС-ИНЖИНИРИНГ ПРОГРАММНЫХ СИСТЕМ КАК ИНСТРУМЕНТ В ПРАКТИКЕ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Современная эпоха цифровизации характеризуется глубоким проникновением технологий во все аспекты общественной жизни, что одновременно создает новые возможности и порождает ранее неизвестные вызовы. Одним из таких вызовов является трансформация преступности, которая все чаще использует цифровые инструменты для достижения противоправных целей. В ответ на эти угрозы правоохранительные органы обращаются к высокотехнологичным методам, среди которых особое место занимает процесс, направленный на разложение сложных программных систем на их базовые компоненты с целью понимания их устройства, функций и взаимодействия с внешней средой. Этот аналитический подход, основанный на глубоком изучении программной логики, становится важным инструментом в противодействии правонарушениям, совершаемым в информационной среде.

По своей природе рассматриваемая технология, известная как реверс-инжиниринг, представляет собой систематическое исследование программных объектов, созданных для выполнения определенных функций, с целью реконструкции их внутренней структуры и принципов действия. В отличие от процесса разработки программ, который начинается с идеи и заканчивается готовым продуктом, этот метод движется в обратном направлении, стремясь от конечного результата вернуться к замыслу создателя. По существу, данный подход представляет собой анализ команд, алгоритмов и взаимосвязей внутри программы в целях выявления, явных или скрытых, выполняемых операций. Такой анализ требует не только глубоких знаний в области вычислительных

наук, но и развитых аналитических навыков, поскольку программы часто защищены сложными механизмами маскировки, такими как шифрование или динамическое изменение структуры. Этот процесс можно сравнить с разборкой сложного устройства, где каждая деталь изучается для понимания ее роли в общей системе.

Данный аналитический подход находит широкое применение в борьбе с преступлениями, совершаемыми с использованием информационно-коммуникационных технологий. Злоумышленники создают сложные системы, предназначенные для выполнения задач, связанных с нарушением конфиденциальности данных, блокировкой доступа к ресурсам или манипуляцией информацией. Разбирая такие системы на их составные элементы, правоохранительные органы получают возможность понять, как они функционируют, какие каналы связи используют и какие ресурсы оказались под угрозой. Например, в ситуациях, когда информационные ресурсы организации подверглись заражению вредоносным программным обеспечением, изучение данного программного инструмента позволяет установить, каким образом он проник в систему и какие действия выполнил.

Следующим логическим шагом в применении реверс-инжиниринга является восстановление хронологии и обстоятельства преступного деяния. В цифровой среде правонарушения оставляют специфические следы, которые проявляются в виде программных артефактов, требующих детального анализа для реконструкции событий. Такой подход позволяет установить источник совершения атаки, задействованные технические приемы и использованные уязвимости. Без понимания внутренней логики программного инструмента правоохранительные органы могут столкнуться с трудностями, особенно в случаях, когда преступление совершается через глобальные сети, где следы быстро растворяются. Полученные в результате анализа данные становятся основой для квалификации действий виновных, позволяя установить их намерения и масштабы причиненного вреда в соответствии с правовыми нормами.

Расширяя область применения, технология выходит за пределы анализа внутренней структуры программ и охватывает изучение их взаимодействия с внешними системами и ресурсами. Программы, используемые в преступных целях, могут быть настроены на выполнение скрытых функций, таких как перехват коммуникаций, манипуляция финансовыми потоками или организация удаленного контроля. Разбирая эти механизмы, представляется возможным выявить не только непосредственные последствия атаки, но и более широкую сеть преступной деятельности, включая организаторов и их посредников. Это приобретает особую значимость в условиях, когда правонарушения совершаются распределенными группами, действующими через сложные цепочки, что затрудняет их обнаружение.

В правоприменительной практике декомпозиция программных систем играет центральную роль в формировании доказательной базы, необходимой для уголовного процесса. Цифровые идентификаторы, полученные в ходе анализа, должны отвечать строгим требованиям, чтобы быть признанными в качестве юридически значимых доказательств. Точное описание функционирования программы, использованной в преступлении, позволяет установить умышленный характер действий виновного и причинно-следственные связи между его действиями и наступившими последствиями. Например, если программа была задействована для несанкционированного вмешательства в информационные ресурсы, ее анализ подтверждает факт нарушения и оценивает нанесенный ущерб. Указанное обстоятельство требует умения переводить технические выводы в юридическую плоскость, обеспечивая их соответствие действующему законодательству.

Однако использование данной технологии сопряжено с рядом аспектов, которые усложняют ее практическое применение. Программы, создаваемые для преступных целей, часто обладают высокой степенью защиты, включая механизмы, которые изменяют их поведение в зависимости от условий или препятствуют анализу. Такие особенности требуют значительных интеллектуальных и временных ресурсов, что может быть затруднительно для правоохранительных органов, работающих в условиях ограниченных возможностей. Указанные обстоятельства подчеркивают необходимость совершенствования технической инфраструктуры и повышения квалификации сотрудников правоохранительных органов в целях эффективного противодействия динамично развивающимся угрозам.

Глобальный характер преступлений в цифровой среде подчеркивает необходимость международного сотрудничества. Правонарушения, совершаемые с использованием программных инструментов, часто охватывают множество юрисдикций, что делает обмен информацией и опытом ключевым фактором успеха. Участие в совместных инициативах, направленных на противодействие киберугрозам, позволило бы интегрировать передовые подходы и повысить эффективность аналитической работы. Создание международных платформ для обмена результатами анализа могло бы ускорить выявление источников угроз и координацию усилий, обеспечивая более оперативное реагирование на глобальные вызовы, особенно в сфере противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий.

В заключение можно отметить, что метод, позволяющий разбирать программные системы для понимания их работы, представляет собой мощный инструмент в борьбе с преступлениями цифровой эпохи. Его успешное применение требует гармоничного сочетания технических инноваций, правовых норм и профессиональной подготовки. Создание условий для эффективного анализа, развитие кадрового потенциала и укрепление международного сотрудничества позволят противостоять современным угрозам, обеспечивая безопасность и стабильность. Эти усилия станут важным шагом к построению системы, в которой технологии поддерживают справедливость и общественное благополучие, отвечая на вызовы стремительно меняющегося мира.

УДК 343.4

С.С. Приёмка

ПРИМЕНЕНИЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМУ

В условиях глобализации и быстрого технологического прогресса понятие экстремизма превратилось в многогранное явление. Экстремизм может проявляться в различных формах, включая политический, религиозный и социальный аспекты, что создает серьезные угрозы для общественной безопасности. В ответ на эти вызовы органы внутренних дел Республики Беларусь стараются внедрять современные технологии, направленные на противодействие экстремистским проявлениям.

С развитием интернета и социальных сетей экстремисты получили мощную платформу для распространения своих идей. Ранее локальные группы могли действовать в рамках отдельных регионов, но сегодня они имеют возможность влиять на аудиторию по всему миру. Это делает задачу противодействия экстремизму гораздо более сложной.

Экстремисты активно используют такие инструменты, как видео, графические материалы и тексты, чтобы привлечь внимание и спровоцировать молодежь. Следовательно, необходимость в мониторинге и анализе информации выросла многократно. Органы внутренних дел Республики Беларусь понимают, что для эффективной борьбы с данными угрозами требуется использование современных технологий, таких как алгоритмы машинного обучения и платформы для анализа больших данных.

Одним из ключевых направлений работы органов внутренних дел Республики Беларусь является анализ больших данных. Этот подход позволяет делать выводы на основе огромного объема информации, что, в свою очередь, помогает в выявлении потенциально опасных ситуаций и лиц.

Аналитические системы, использующие искусственный интеллект, теперь способны обрабатывать не только текстовую информацию, но и изображения и видео. Это дает возможность оперативно реагировать на экстремистские проявления в режиме реального времени. Например, если в социальных сетях появляется видео с пропагандой насилия, система может немедленно уведомить соответствующие службы об этом факте для дальнейшего анализа и принятия мер.

С помощью таких технологий органы внутренних дел способны выявлять не только известных экстремистов, но и анализировать профиль потенциальных участников. Это позволяет заранее принимать меры к предотвращению их деятельности.

Важной составляющей работы по противодействию экстремизму является мониторинг социальных сетей и специализированных интернет-ресурсов. В условиях, когда многие экстремистские идеи распространяются через эти платформы, система мониторинга становится критически важной.

Органы внутренних дел используют программы для отслеживания и анализа разговоров в социальных сетях, а также для выявления ключевых слов и фраз, ассоциирующихся с экстремистской деятельностью. Это позволяет оперативно обнаруживать и реагировать на угрозы, не дожидаясь, когда они перейдут в реальную жизнь.

Использование таких технологий также позволяет обратиться к молодежи на их языке и в тех пространствах, где они проводят больше всего времени. Органы внутренних дел Республики Беларусь разрабатывают специальные информационные кампании, направленные на онлайн-платформы, чтобы обозначить позиции государства и развеять мифы, имеющие отношение к экстремизму.

В последние годы заметно увеличилось использование дронов для мониторинга гражданских массовых мероприятий, где существует вероятность проявления экстремизма. Дроны способны обеспечивать видеонаблюдение на больших расстояниях и в труднодоступных местах, что значительно увеличивает уровень безопасности.

Системы видеонаблюдения, размещенные в общественных местах, также помогают оперативно реагировать на экстремистские действия. Современные технологии разработки видеоаналитики позволяют выявлять подозрительное поведение и быстро отреагировать на ситуацию.

Например, в случае возникновения массовых беспорядков система может немедленно передать информацию о происходящем оператору.

Таким образом, использование дронов и систем видеонаблюдения значительно укрепляет охрану общественного порядка и повышает шансы на быстрое предотвращение экстремистских действий.

Современные технологии неизменно требуют новых законодательных мер, направленных на правовую защиту права граждан и защиту безопасности государства. Органы внутренних дел Республики Беларусь активно работают над изменением и дополнением законодательства, чтобы адаптироваться к новым вызовам.

Использование современных технологий в борьбе с экстремизмом должно происходить в рамках правового поля, чтобы избежать нарушения прав граждан. Необходимо определить четкие границы мониторинга и анализа данных, чтобы обеспечить защиту личной информации и приватности.

Законы, касающиеся интернет-цензуры, защиты данных и урегулирования работы правоохранительных органов в цифровом пространстве, становятся актуальными как никогда. Без соответствующего правового обеспечения применение технологий может привести к эксцессам и негативному отношению со стороны граждан.

В результате такого подхода возможно создание сбалансированной системы, которая будет эффективно бороться с экстремизмом, не нарушая прав человека и обеспечивая безопасность общества.

Таким образом, противодействие экстремизму в Республике Беларусь требует комплексного подхода, основанного на современных технологиях и адекватных законодательных мерах. Применение технологий анализа больших данных, мониторинга интернет-ресурсов, образовательных программ и взаимодействия с международными организациями становится необходимым условием для эффективной борьбы с растущими угрозами.

Важно понимать, что экстремизм – это не только уголовное преступление, но и социальная проблема, требующая профилактических мер. Использование современных инструментов мониторинга и анализа информации позволяет не только реагировать на угрозы, но и предотвращать их развитие на ранних стадиях.

В условиях стремительно меняющегося мира органы внутренних дел Республики Беларусь должны оставаться на передовой борьбы с экстремизмом, сочетая инновации с соблюдением прав граждан.

УДК 343.985.8

А.В. Родевич

НЕКОТОРЫЕ АСПЕКТЫ СУЩНОСТИ РИСКА В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Риск в оперативно-розыскной деятельности (ОРД) является малоизученным явлением. Почему такой важный аспект в экстремальной, связанной с высокой эмоциональной напряженностью работе остается без изучения? Решение этого вопроса связано с пониманием сущности риска в рассматриваемой деятельности.

Проблема риска изучается во многих областях знаний – в экономике, психологии, истории, социологии, политологии, естественных и технических науках, в рамках теории игр и теории принятия решений. Такие риски существуют, но в определенные моменты, например, страховой риск – это предполагаемое негативное событие, на случай наступления которого и производится страхование. Наиболее часто проблема риска возникает при решении практических задач в борьбе с преступностью, в основном в оперативной работе, которая рассматривается как деятельность, связанная с риском во всех ее проявлениях.

В юридическом понимании риск – это возможность наступления событий с отрицательными последствиями в результате определенных решений или действий.

Риск всегда предшествует вероятной опасности, т. е. возможности нанесения вреда, имущественного (материального), физического или морального (духовного) ущерба личности, обществу, государству. Соответственно, опасность – следствие необдуманного риска. Опасность (проблема, угроза) возникает в настоящем, риск всегда существует только в будущем.

Анализ теоретических и практических обобщений показывает, что в зависимости от того, как риски могут влиять на достижение поставленных целей в ОРД, они могли иметь стратегический (перспективный) и тактический (молниеносный) характер. Следует отметить, что неопределенность возможных последствий и вызывает то чувство тревоги, которое сопровождает оперативного сотрудника при осуществлении ОРД. Частота наступления негативных последствий формирует чувство риска в деятельности оперуполномоченного в различных оперативно-розыскных ситуациях. Другими словами, риск – это ожидание проблемы, наступление возможных потерь, которые могут возникнуть в будущем. На практике такое состояние возникает, как правило, из-за того, что опе-

ративные сотрудники располагают минимум информацией, не в полной мере контролируют ситуацию, возможно, ощущают дефицит времени.

Такие ситуации заставляют задуматься, действовать ли в условиях риска, и каковы будут его последствия. Соответственно, оперативный сотрудник принимает решение: проводить оперативно-розыскное мероприятие, осуществить задержание с поличным, дополнительно подготовиться или отказаться от своих решений.

Практическое решение указанных проблем связано с пониманием рисков в ОРД. Так, анализ практики показывает, что риск бывает:

а) по возможности предвидения: прогнозируемый (ситуация риска сведена к четко определенному числу сценариев развития событий, в силу чего оперативник, при наличии достаточного опыта, может дать относительно точный прогноз); частично непрогнозируемый (риск включает в себя сценарные варианты, которые объективно не могут быть учтены);

б) по источникам возникновения: внешний (риск, связанный с объективными факторами: погодными условиями, временем суток, некомплектом личного состава); внутренний (риск, непосредственно зависящий от профессионального, грамотного руководства тактической операцией должностным лицом органа, осуществляющего ОРД, подбора сил и средств, наличия определенного оперативного опыта);

в) по размеру возможного ущерба: допустимый (приемлемый) риск (негативное событие, наступление которого не желает, но допускает оперативный сотрудник: неудачная реализация дела оперативного учета, расшифровка методов ОРД, репутационные издержки и т. п.); критический (риск, на который идет оперативник, в случае неудачи, связан с очевидными негативными последствиями для жизни, здоровья, имущества участников ОРД);

г) по характеру проявления во времени: постоянный (характерен для всего периода проведения оперативно-розыскного мероприятия или тактической операции); временный (риск, носящий перманентный характер, возникающий на отдельных этапах разработки);

д) по субъектам: индивидуальный (проблема может коснуться лично оперативника или лица, оказывающего содействие на конфиденциальной основе); групповой (действия, из-за которых может пострадать оперативное подразделение).

Следует отметить двойственный характер риска в ОРД, несущий в себе как негативные (риски причинения вреда или иных нежелательных последствий), так и позитивные аспекты (возможность реализовать информацию здесь и сейчас, задержать всех фигурантов одномоментно, изъять неожиданно крупную партию запрещенных веществ и т. п.).

При этом ситуации в условиях риска могут возникать на системной основе или внезапно. То, что происходит неожиданно, разрешается, как правило, интуитивно и за счет профессионального опыта сотрудника. Если риск носит постоянный характер, то требуется определение оперативно-розыскной ситуации с анализом действий противоборствующей стороны и установлением конкретных оперативно-розыскных мер. Это решается путем разработки методических рекомендаций и правового регулирования. Отсюда следует, что риск в ОРД – это действия оперативного сотрудника в условиях отсутствия или наличия неэффективных методик изобличения преступника или пробелов в правовом регулировании. Потому что одним опытом и интуицией решить сложные, неожиданно возникшие задачи не всегда представляется возможным. Должны быть продуманы резервные действия.

На основании вышеизложенного становится очевидным, что при возможности наступления риска надо понимать уровень наступления последствий для человека, общества, государства, имущества, окружающей среды и т. д. Поэтому представляется важным разобраться в пределах допустимости риска и устранении недостатков и упущений в работе оперативных сотрудников.

Как измерять риск? Например, на интуиции и личном опыте. Однако личности все разные, соответственно достоверность этих сведений может быть невелика. Традиционно при оценке события или явления рассматриваются количественные и качественные показатели. Так, количественная оценка рисков – это числовые показатели, например в ОРД, количество успешно проведенных операций или оперативно-розыскных мероприятий, комбинаций, в ситуациях риска. Такие количественные показатели снижают либо увеличивают степень риска. Качественная оценка рисков – более интуитивный подход, заключающийся во внутреннем убеждении оперативного сотрудника, которое формируется на количественных показателях, которые уже качественную оценку могут формулировать от «очень низкой» до «очень высокой». Часто недостаток количественных показателей, дефицит времени делают низкими качественные показатели, что влияет на понимание рисков при решении задач ОРД.

Следует отметить, что количественный и качественный подход имеет свои преимущества и недостатки. В основе принятия решений лежит сравнительный анализ, прогнозирование проблемы, возможность изменения оперативно-розыскной ситуации, пути ее решения.

Учитывая изложенное, можно определить признаки риска: неопределенность, направленность на общественно полезные цели, вероятность наступления потери, вреда, наличие выбора в действиях, невозможность решения задач ОРД без риска.

На наш взгляд, риск в ОРД – это вероятность возникновения опасного, неконтролируемого события, наносящего вред или ущерб гражданам, государству (в широком смысле), а также создающего невозможность или затрудняющего решение задач ОРД (в узком смысле). Эта мысль позволяет сделать вывод, что риск в рассматриваемой деятельности, как важный ее признак, нуждается в более глубоком изучении и анализе.

УДК 343.98

О.В. Савчук

О КРИТЕРИЯХ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ ПОДРАЗДЕЛЕНИЙ КРИМИНАЛЬНОЙ МИЛИЦИИ

Оценка работы служб криминальной милиции является одним из направлений совершенствования в целом системы органов внутренних дел (ОВД), позволяет не только своевременно выявить «слабые места» в деятельности того или иного подразделения, но и спрогнозировать на перспективу ее результативность при изменении оперативной обстановки. При этом необходимо учитывать, что территориальные подразделения ОВД работают в различных условиях, характеризующихся природными, экономическими, социальными, демографическими и иными особенностями. Это обусловливает различие в их организационно-штатной численности. Исторически их формирование, как правило, осуществлялось по административно-территориальному принципу: в каждом районе – ОВД.

Исторический анализ практики работы ОВД показывает, что для отдельных служб (участковые инспекторы милиции, подразделения по гражданству и миграции, Государственная автомобильная инспекция) штатная численность определялась нормативно (исходя из численности населения, проживающего на территории обслуживания, из количества зарегистрированного автомототранспорта). При этом оперативные подразделения формировались преимущественно с учетом криминогенной обстановки, исходя из количества регистрируемых уголовно наказуемых деяний, в отдельных случаях – по указанию руководства Министерства внутренних дел.

Первая попытка научного исследования проблемы определения оптимальных штатов ОВД предпринята советскими учеными С.Е. Вициным и В.Н. Золотаревым, которые в 70-х гг. прошлого века на теоретическом

уровне разработали модель определения организационно-штатной численности горрайорганов внутренних дел. В основу расчета ими положены:

численность сотрудников на 10 тыс. населения;

годовая нагрузка на одного оперуполномоченного, выражаемая числом зарегистрированных преступлений по соответствующим линиям работы;

уровень преступности из расчета на 10 тыс. населения;

площадь обслуживаемой территории.

Тем не менее авторам так и не удалось использовать представленный в их же модели уровень преступности, а также сформировать методику расчета штатов каждой службы и ОВД в целом.

В 2014 г. на основе исследований российских ученых В.В. Важенина и С.В. Баженова Министерства внутренних дел Российской Федерации разработана методика определения оптимальной численности сотрудников подразделений уголовного розыска. Для этого предложено выделить основные направления работы, выполняемой данной службой, определить численность сотрудников и сложить полученные показатели. При этом, помимо раскрытия преступлений, работы по материалам проверок и розыска преступников, к основным направлениям деятельности подразделений уголовного розыска отнесены административно-управленческая и непрофильная функции (охрана общественного порядка, конвоирование и т. п.).

По мнению В.В. Важенина и С.В. Баженова, численность сотрудников зависит от числа зарегистрированных в текущем отчетном периоде (как правило, за год) по линии уголовного розыска преступлений, количества сотрудников, задействованных для их раскрытия, в том числе прошлых лет, а также интенсивности оперативно-розыскной деятельности и региональных условий, в которых соответствующие службы работают.

В белорусском государстве оценка деятельности подразделений криминальной милиции ОВД сегодня проводится в соответствии с приказом Министерства внутренних дел Республики Беларусь от 26 апреля 2024 г. № 48-дсп «Об оценке деятельности органов внутренних дел» (для аппаратов ГУВД Мингорисполкома, УВД облисполкомов), а региональных РУ-РО-ГОВД, ОВД на транспорте, Минского ОВД на воздушном транспорте – на основании соответствующих приказов ГУВД-УВД, где одним из элементов при определении их эффективности работы является выявление (раскрытие) преступлений. В этой связи для соответствующих направлений – уголовный розыск (УР), борьба с экономическими преступлениями (БЭП), наркоконтроль и противодействие торговле людьми (НиПТЛ), противодействие киберпреступности (ПК) разработаны отдельные методики оценки.

С учетом нормативно определенной компетенции подразделений криминальной милиции (выявление, пресечение, раскрытие пре-

ступлений, розыск лиц, их совершивших, скрывающихся от органов, ведущих уголовный процесс, и др.) оценка эффективности работы УР, БЭП, НиПТЛ и ПК складывается преимущественно из цифровых (статистически учтенных) показателей по основным (приоритетным) направлениям этих служб. Причем для каждой из них оценочные показатели (критерии) эффективности работы различны, что обосновывается спецификой решаемых задач.

Например, одними из показателей работы для подразделений ПК являются количество составленных протоколов по ст. 13.3 Кодекса Республики Беларусь об административных правонарушениях (за совершение криптовалютных операций) и число преступлений, выявленных в рамках дел оперативного учета, что нехарактерно для иных оперативных подразделений. В то же время традиционно для службы УР на первом месте стоит раскрытие общеуголовных преступлений, в том числе прошлых лет, розыск преступников и без вести пропавших. Для БЭП результативность определяется числом выявленных лиц, совершивших уголовно наказуемые деяния в сфере экономики.

В свою очередь, общим для всех служб криминальной милиции ОВД, фактически не учитываемым при оценке эффективности их работы, является:

исполнение следственных поручений по уголовным делам;

разрешение материалов проверок в порядке, предусмотренном Уголовно-процессуального кодекса Республики Беларусь;

направление информации в государственные органы (организации) в рамках реализации постановления Совета Министров Республики Беларусь от 23 апреля 2021 г. № 241 «О порядке использования сведений, содержащихся в материалах оперативно-розыскной деятельности».

В этой связи в целях совершенствования подходов к оценке деятельности подразделений криминальной милиции считаем целесообразным для всех служб одним из оценочных показателей определить:

нагрузку на подразделение (сотрудника) по исполненным следственным поручениям;

нагрузку на подразделение (сотрудника) по материалам с решением об отказе в возбуждении уголовного дела, в том числе о прекращении проверки по делам частного обвинения;

количество направленных в государственные органы, организации писем (информации) по результатам проведенных оперативно-розыскных и иных мероприятий с целью принятия соответствующими должностными лицами мер по устранению причин и условий, способствующих совершению преступлений.

УДК 343.01

П.И. Сацук, П.Л. Боровик

АКТУАЛЬНЫЕ ВОПРОСЫ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПЛЕНИЙ В СФЕРЕ НЕЗАКОННОГО ОБОРОТА СРЕДСТВ ПЛАТЕЖА И (ИЛИ) ИНСТРУМЕНТОВ

Актуальность настоящего исследования обусловлена стремительным и непрекращающимся ростом числа мошенничеств и краж, совершаемых в сфере электронных платежей. Традиционные подходы к расследованию имущественных посягательств не всегда применимы к подобным преступлениям, поскольку они могут совершаться дистанционно, в режиме онлайн, с использованием современных технологических решений и сложных схем сокрытия своей деятельности. Разработка криминалистической характеристики данных посягательств позволяет систематизировать информацию об их способах, объектах, а также определить наиболее эффективные пути противодействия подобным преступлениям.

Криминалистическая характеристика рассматриваемой категории преступлений включает в себя ключевые аспекты, необходимые для соответствующей оперативно-розыскной практики:

место и время совершения преступления: часто совпадает с местом физического пребывания преступника при списании денежных средств, но в онлайн-среде данные координаты могут оставаться неизвестными или быть искусственно замаскированными;

способы совершения преступления: от банальной кражи банковской платежной карточки и психологического воздействия на жертву (офлайн) до сложных технических схем (онлайн), где применяется скимминг, фишинг и др.;

объект преступного посягательства: денежные средства на банковском счете, электронные деньги, иные расчетные инструменты;

характеристика личности преступника: уровень технических знаний (от базовых до профессиональных), мотивация (корысть, самоутверждение, хулиганские побуждения), возраст, социальный статус и пр.;

характеристика личности жертвы: возраст (особенно пожилые люди), склонность оставлять в открытом доступе персональные данные, недостаточно высокая финансовая грамотность, доверчивость при общении в сети;

иные аспекты: перечень необходимой преступнику информации (логины, пароли, реквизиты банковских платежных карточек), объекты-но-

сители следов преступления (электронные устройства, камеры банкоматов, технические устройства для скимминга и т. д.), круг возможных свидетелей (сотрудники банков, специалисты в сфере ИТ, работники мобильных операторов и пр.).

Исследование практики показало, что совершение противоправных действий с банковскими платежными карточками и другими платежными инструментами может быть условно разделено на две группы:

1. Офлайн-преступления:

прямое физическое завладение карточкой: кража, ограбление, обман пожилых людей и т. д. При этом жертва сама может неосознанно помочь преступнику, храня пин-код рядом с карточкой или сообщая его третьим лицам;

«дружественное мошенничество»: использование банковской платежной карточки близкими друзьями или родственниками, которые знают пин-код и совершают несанкционированные транзакции;

завладение средствами в торговых точках: кассир повторно проводит оплату или копирует данные карточки клиента;

скимминг в банкоматах: установка считывающего устройства (скиммера) в кардридер и накладки на клавиатуру. Эти действия позволяют получить реквизиты банковской платежной карточки и пин-код.

2. Онлайн-преступления:

фишинг: создание поддельных сайтов банков или известных интернет-магазинов, массовая рассылка писем от имени финансовых организаций, обмен сообщениями в социальных сетях и мессенджерах с целью выманить у жертвы конфиденциальные данные (номер банковской платежной карточки, срок ее действия, CVV-код, одноразовые пароли);

сайты-зеркала: дублирование интерфейса официальных платформ для введения реквизитов, которые, попадая к мошенникам, становятся инструментом для дальнейшего хищения;

использование личных данных держателя банковской платежной карточки (без ее физического похищения): реквизиты могут быть незаконно получены, например, через подкуп сотрудников торговых сетей или АЗС, после чего злоумышленник совершает удаленные платежи или переводы;

незаконные операции держателя: сам владелец карточки совершает покупку или платеж, а затем заявляет, что транзакция была несанкционированной и требует возврата.

Анализ показал, что среди лиц, совершающих преступления с использованием платежных инструментов, преобладают мужчины в возрасте 30 лет и старше, причем значительная доля таких преступлений совершается группой (нередко – организованной). Среди характерных черт:

техническая подготовка: многие преступники владеют компьютерными технологиями, умеют программировать, разрабатывают или используют шпионское программное обеспечение, знают иностранные языки (в первую очередь английский) для доступа к зарубежным ресурсам;

социально-демографические особенности: высокая доля неработающих (или нерегулярно занятых) лиц, имеющих при этом достаточный уровень образования и (или) практических навыков в сфере ИТ;

психологические черты: свободолюбие, эгоцентризм, склонность к анонимности, нежелание контактировать с внешним миром офлайн. При разоблачении многие активно сотрудничают со следствием, так как расценивают это как менее рискованный путь.

Важным направлением для органов внутренних дел становится выявление организованных преступных групп, работающих в удаленном режиме. В таких организованных преступных группах задействованы программисты, «заливщики» (занимающиеся переводом средств), «прозвонщики» (обманом выуживают у жертвы данные банковской платежной карточки), «дропы» (лица, открывающие счета, обналичивающие средства), а также поставщики технической и инфраструктурной поддержки (серверов, SIM-карт и пр.).

С учетом специфики онлайн-среды и технических нюансов преступлений в сфере незаконного оборота средств платежа и (или) инструментов, при расследовании нужно учитывать следующие моменты:

фиксация цифровых следов: логи банковских систем, IP-адреса, история транзакций, данные о местоположении устройств и т. д.;

анализ возможных каналов утечки: проверка кассиров, операторов, посредников, чьи действия могут быть связаны с копированием или распространением реквизитов;

экспертная поддержка: участие специалистов в области ИТ-технологий, криптографии, программирования; при необходимости – проведение компьютерно-технических экспертиз;

оперативное взаимодействие: для более эффективного розыска и задержания преступников необходима скоординированная деятельность банков, мобильных операторов и правоохранительных органов;

международное взаимодействие: поскольку нередко средства выводятся за пределы одной страны, важна отлаженная система международного сотрудничества (поиск цифровых следов, запросы в иностранные банки, взаимодействие с профильными организациями).

Как видим, криминалистическая характеристика преступлений в сфере незаконного оборота средств платежа и (или) инструментов демонстрирует сложный комплекс оперативно-розыскных, технических, психологических и организационных аспектов.

Дальнейшие исследования в этой области должны учитывать постоянно меняющиеся способы незаконного оборота платежных инструментов и средств, обеспечивая тем самым своевременный и эффективный отклик государственных институтов на возникающие угрозы.

УДК 343.13:343.9

Д.А. Симоненко

О ЗАКОНОДАТЕЛЬНОМ РЕГУЛИРОВАНИИ СОДЕЙСТВИЯ ОТДЕЛЬНЫХ ЛИЦ ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, В СОПРЕДЕЛЬНЫХ С РОССИЕЙ ГОСУДАРСТВАХ

Содействие отдельных лиц органам, осуществляющим оперативно-розыскную деятельность (ОРД), выступает одним из основных направлений борьбы с преступностью. Многовековой опыт осуществления этой работы свидетельствует о том, что вне зависимости от исторического периода или географического положения она осуществляется в основном по одним и тем же лекалам. Вместе с тем состоявшийся этап законодательного закрепления в ОРД такового содействия органам правопорядка в различных государствах несколько разграничил существо описываемой деятельности и ее терминологический ряд.

В настоящей публикации мы осуществим попытку сопоставления основных положений в этой части Федерального закона Российской Федерации от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон об ОРД РФ) с аналогичными законами: Законом Республики Казахстан от 15 сентября 1994 г. № 154-XIII «Об оперативно-розыскной деятельности» (далее – Закон об ОРД КР) и Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон об ОРД Беларуси) и на этой основе внесем предложения о совершенствовании российского закона.

Такая последовательность анализа законодательных предписаний избрана с учетом времени принятия нормативных правовых актов.

В Законе об ОРД РФ вопросы содействия отдельных лиц оперативным подразделениям регулируются ст. 17 «Содействие граждан органам, осуществляющим оперативно-розыскную деятельность». Само наименование статьи вызывает вопросы у исследователей, так как обозначена категория «гражданин», что формально-юридически подразумевает наличие гражданства Российской Федерации, при этом в содер-

жании рассматриваемой статьи указывается на возможность заключать контракты с лицами независимо от их гражданской принадлежности. Аналогичное название ст. 51 содержится в Законе об ОРД Беларуси. Закон об ОРД РК содержит иное наименование – ст. 13 рассматриваемого закона «Содействие органам, осуществляющим оперативно-розыскную деятельность». Данный подход представляется более совершенным в сравнении с Законом об ОРД РФ и Законом об ОРД Беларуси.

Здесь следует также отметить, что в модельном законе Содружества Независимых Государств «Об оперативно-розыскной деятельности» (постановление Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 16 ноября 2006 г. № 27-6) (далее – Модельный закон об ОРД) ст. 17 называется «Оказание содействия органам, осуществляющим оперативно-розыскную деятельность» и в своем содержании указывает не на граждан, а на «отдельных лиц». Формулировка наименования статьи, регулирующей оказание содействия органам, осуществляющим ОРД, в Законе об ОРД РК наиболее приближена к модельному законодательству. Модельный закон не имеет императивного характера и призван определить варианты правового регулирования в целях унификации законодательств различных государств и сближения правовых систем. По своей сути это своеобразная норма международного мягкого права, однако цели, преследуемые государствами – участниками Содружества Независимых Государств при формировании модельного законодательства, указывают на наличие в них определенных правовых ориентиров для законодателей. При этом следует отметить, что только Закон об ОРД Беларуси был принят позже, чем Модельный закон об ОРД.

В ч. 1 ст. 17 российского закона представлена *обязанность содействующих лиц сохранять в тайне сведения, ставшие им известными* в ходе подготовки или проведения оперативно-розыскного мероприятия, *и не предоставлять* указанным органам *заведомо ложную информацию*. Аналогичные положения содержатся в Модельном законе об ОРД. В ч. 2 ст. 13 казахского закона представлены подобные формулировки, однако отмечается, что *за разглашение таких сведений и представление заведомо ложной информации они несут ответственность, установленную Законом Республики Казахстан*. Что касается Закона об ОРД Беларуси, такое или похожее предписание в ст. 51 отсутствует. И это представляется оправданным, поскольку в иных законодательных актах государства упоминание о какой-либо ответственности за указанные действия отсутствует.

В ч. 2 ст. 17 Закона об ОРД РФ изложено предписание, создающее органам, осуществляющим ОРД, *возможность заключать контракты*

с совершеннолетними дееспособными лицами независимо от различных перечисленных в законе признаков. Аналогичное по сути положение содержится в ч. 3 ст. 13 Закона об ОРД РК и в части третьей ст. 51 Закона об ОРД Беларуси. Данный подход всецело отвечает задачам ОРД и коррелируется с положениями Модельного закона об ОРД.

Вместе с тем в казахском законе присутствует фраза, согласно которой *форма контракта, условия и сроки его действия определяются ведомственными нормативными актами*, в белорусском, согласно части четвертой ст. 51, порядок заключения контракта, его типовая форма определяются органами, осуществляющими ОРД. Кроме того, в нем *применительно к заключению контракта содержится лишь требование о совершеннолетии* согласившегося на его заключение человека. И это нам представляется оправданным. Поскольку степень дееспособности гражданина (в случае возникновения каких-либо сомнений) устанавливает суд, эта категория в рамках привлечения лица к сотрудничеству (т. е. заключение с ним соответствующего контракта – *Д.С.*) представляется некорректной, и в Законе об ОРД РФ следует использовать не гражданско-правовую терминологию дееспособности, а уголовно-правовую категорию вменяемости.

В ч. 3 ст. 17 Закона об ОРД РФ содержится запрет на заключение контракта с депутатами, судьями, прокурорами, адвокатами, священнослужителями и полномочными представителями официально зарегистрированных религиозных объединений. Аналогичное требование присутствует в части пятой ст. 51 Закона об ОРД Беларуси и Модельном законе об ОРД. Интересно, что в казахском законе такое установление отсутствует. Означает ли это возможность заключения контракта о сотрудничестве (в том числе в негласной форме) с отмеченными лицами, и какова ее аргументация – предмет возможного исследования в перспективе.

Таким образом, анализ норм законодательства об ОРД сопредельных государств (России, Беларуси, Казахстана) позволяет нам сделать некоторые выводы:

1. Исследуемое законодательство в целом имеет общие начала и сходные нормы, при этом детальный анализ института содействия органам, осуществляющим ОРД, позволяет констатировать наличие различных подходов к отдельным правоотношениям в рассматриваемой сфере и указывает на перспективы развития законодательного регулирования предмета исследования.

2. Наименование ст. 17 Закона об ОРД РФ не соответствует его содержанию и нуждается в корректировке по аналогии с Законом об ОРД РК и Модельным законом об ОРД.

3. Требование российского законодателя к содействующим оперативным подразделениям лицам сохранять в тайне сведения, ставшие им известными в ходе подготовки или проведения оперативно-розыскного мероприятия, и не предоставлять указанным органам заведомо ложную информацию, не подкреплено материальными нормами, а потому представляется декларативным. С целью устранения названного недостатка необходимо законодательно закрепить ответственность указанных лиц за отмеченные выше действия.

4. В формулировке ч. 2 ст. 17 Закона об ОРД РФ следует заменить термин «дееспособный» на «вменяемый». Ее следует также дополнить фразой, аналогичной содержащейся в ч. 3 ст. 13 Закона об ОРД РК, о регулировании общих требований, предъявляемых к контракту ведомственными нормативными актами.

5. Наличие в ч. 3 ст. 17 ОРД РФ и части пятой ст. 51 Закона об ОРД Беларуси предписания о невозможности заключения контракта о конфиденциальном содействии с рядом лиц, имеющих особый правовой статус, и их соответствия Модельному закону об ОРД, представляется оправданным и законодательно перспективным в части возможного несоответствия конституционным нормам, при отсутствии такого запрета.

УДК 343.13

В.С. Сороко, А.А. Березко

ПРАВОВЫЕ АСПЕКТЫ ВЗАИМОДЕЙСТВИЯ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, С ГРАЖДАНСКИМ ОБЩЕСТВОМ И СРЕДСТВАМИ МАССОВОЙ ИНФОРМАЦИИ

Оперативно-розыскная деятельность (ОРД) играет огромную роль в обеспечении безопасности государства и общества. Однако ее эффективность во многом зависит от взаимодействия с гражданским обществом и средствами массовой информации (СМИ). Это взаимодействие регулируется законодательством, но на практике возникает ряд проблем, связанных с открытостью, защитой прав граждан и балансом между конфиденциальностью и общественным контролем.

ОРД в белорусском государстве регулируется Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности». Под правовой основой ОРД следует понимать совокупность законодательных и иных нормативных актов, регламентирующих

отношения, возникающие в сфере этой деятельности. Регулирование ОРД основывается на Конституции Республики Беларусь (ст. 28 – право на защиту от незаконного вмешательства в частную жизнь), Законе Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (ст. 5 – принципы законности, уважения прав человека, конспирации), Законе Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации» (ст. 37 – Информация, распространение которой в средствах массовой информации, на интернет-ресурсах, новостных агрегаторах ограничено), Уголовно-процессуальном кодексе Республики Беларусь (регламентирует использование результатов ОРД в уголовном процессе). Основными субъектами ОРД в Республике Беларусь являются органы внутренних дел, органы государственной безопасности, органы пограничной службы, Служба безопасности Президента Республики Беларусь, Оперативно-аналитический центр при Президенте Республики Беларусь, органы финансовых расследований Комитета государственного контроля, таможенные органы, разведывательные службы Вооруженных Сил Республики Беларусь. Эти структуры взаимодействуют с гражданским обществом и СМИ в рамках, установленных законом, но с существенными ограничениями.

Как отмечалось ранее, взаимодействие органов ОРД с гражданским обществом и СМИ имеет ряд проблем, которые требуют поступательного решения. Одной из них является отсутствие должного участия граждан в обеспечении безопасности. Под обеспечением безопасности мы подразумеваем создание условий, при которых люди могут жить, работать и развиваться без угрозы физического, эмоционального или экономического вреда. Привлечение граждан к совместным инициативам, таким как программы по профилактике преступности или участие в общественных советах, позволяет создать более безопасную среду. Можно реализовать совместные программы, направленные на профилактику преступности, например, «Соседский патруль» или «Безопасный район», которые могут значительно повысить уровень безопасности в населенных пунктах и вовлечь граждан в процесс.

Следующим предметом внимания является конфликт между конфиденциальностью и свободой СМИ, манипуляция информацией в СМИ. Ключевую роль играют СМИ в формировании общественного мнения. Однако часто сталкиваются с ограничениями при освещении деятельности силовых структур, например, дела об «экстремизме». А иногда информация, полученная от органов ОРД, может быть искажена или представлена в неверном свете, что приводит к панике или необоснованным обвинениям. Недоработкой является отсутствие четких крите-

риев, какую информацию можно публиковать, а какую – нет, что приводит к самоцензуре или судебным преследованиям. Этот вопрос можно решить путем создания кодекса этики для СМИ. Создание кодекса, регулирующего работу журналистов при освещении тем, связанных с ОРД, поможет избежать манипуляций и недостоверной информации. Такой кодекс может включать в себя рекомендации по проверке фактов и соблюдению баланса между интересами общества и правами граждан. В данном документе можно отразить основные принципы и этические нормы, которые будут определять работу журналистов в этой чувствительной области.

Например, глава о специфике освещения оперативно-розыскной деятельности, в которую могут входить такие статьи, как ответственность за информацию, учет интересов общественности и правоохранительных органов, защита личных данных и конфиденциальности. Следующей главой может являться работа с источниками информации, в которую будут входить статьи про принципы работы с анонимными источниками, этические стандарты при получении информации от правоохранительных органов.

Если говорить конкретнее, то в этот кодекс можно добавить статью «Избежание сенсационности», в которой будет закреплено положение о том, что журналисты не должны использовать сенсационные заголовки или преувеличенные утверждения для привлечения внимания к материалу. Освещение уголовных дел должно основываться на фактах, а не на эмоциональных реакциях. Или статью «Этические стандарты при работе с анонимными источниками». Использование анонимных источников должно быть оправданно и тщательно проверено. Журналисты обязаны удостовериться в достоверности информации, предоставленной такими источниками, прежде чем использовать ее в своих материалах.

Важно также проводить обучение для сотрудников органов ОРД по вопросам эффективного взаимодействия с журналистами. Это поможет избежать недоразумений и повысить качество информации, передаваемой в СМИ. Дополнительно можно ввести «период тишины» по резонансным делам до завершения оперативных мероприятий.

Считаем важным усовершенствовать законодательство, а именно внести изменения в действующий Закон Республики Беларусь «Об оперативно-розыскной деятельности» с указанием пределов взаимодействия со СМИ.

Таким образом, взаимодействие органов ОРД с гражданским обществом и СМИ в Беларуси требует баланса между конфиденциальностью и открытостью. Существующие проблемы – недостаточное взаимодействие гражданского общества и органов ОРД, риск злоупотреблений и

ограничения для СМИ – могут быть решены через усиление общественного контроля, диалог с медиа и законодательные реформы. Это повысит доверие к правоохранительной системе, не снижая эффективности оперативной работы.

УДК 343.985

А.П. Стефаненко

О ВЗАИМОДЕЙСТВИИ ОРГАНОВ, ОСУЩЕСТВЛЯЮЩИХ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ, И СЛЕДОВАТЕЛЕЙ

Проблемы взаимодействия оперативных и следственных органов в процессе противодействия преступности возникали со времен образования и разделения данных органов на отдельные структуры, с присущими им полномочиями.

Взаимодействие органов, осуществляющих оперативно-розыскную деятельность, и следователей в современных условиях представляет собой организованную, совместную деятельность, сочетающую эффективное использование сил и средств с достижением общих целей и задач, а также учитывающую разграничение компетенции взаимодействующих субъектов, направленную на выявление, раскрытие, предупреждение и пресечение преступлений.

К основным составляющим взаимодействия, на наш взгляд, целесообразно отнести следующие: комплексное использование сил и средств органов, осуществляющих оперативно-розыскную деятельность, и следователей; самостоятельность следователя в принятии решений; самостоятельность органов, осуществляющих оперативно-розыскную деятельность, в выборе собственных средств и методов проведения оперативно-розыскных мероприятий; своевременный обмен между следователем и органом, осуществляющим оперативно-розыскную деятельность, информацией, имеющей значение для расследования уголовного дела; планирование и проведение совместных совещаний по вопросам эффективности оперативно-розыскного сопровождения расследования уголовного дела.

Изучение результатов оперативно-служебной деятельности позволяет констатировать, что в ряде случаев оперативные сотрудники, направившие материалы проведенных проверок следователю, после принятия решения о возбуждении уголовного дела, утрачивают инициативу и настойчивость при проведении оперативно-розыскных и иных проверочных мероприятий. В подобных случаях взаимодействие сводится к формальному исполнению поручений следователя, которое часто затягивается.

В отдельных случаях следователи несвоевременно направляют поручения в органы, осуществляющие оперативно-розыскную деятельность, для проведения следственных действий и оперативно-розыскных мероприятий. При этом проведение отдельных оперативно-розыскных мероприятий по конкретному уголовному делу не санкционируется прокурором без наличия соответствующего поручения следователя. В таких случаях видится целесообразным проводить совместные совещания, в ходе которых появляется возможность своевременно планировать производство следственных действий и проведение оперативно-розыскных мероприятий.

Кроме того, на наш взгляд, необходимо учитывать возможное противодействие органам уголовного преследования со стороны подозреваемых, обвиняемых и их связей. Это обстоятельство предполагает более активное осуществление оперативно-розыскного сопровождения уголовного процесса, которое может включать в себя: установление и проверку причастности к совершению преступлений иных лиц; выявление и документирование дополнительных фактов противоправной деятельности; проведение оперативно-розыскных мероприятий в отношении лиц, заключенных под стражу; планирование и проведение дополнительного комплекса оперативно-розыскных мероприятий в отношении связей обвиняемых; предотвращение и пресечение новых преступлений и др.

Совершенствование правового регулирования взаимодействия органов, осуществляющих оперативно-розыскную деятельность, и следователей также играет немаловажную роль в данном процессе. Определение и законодательное закрепление перечня отдельных следственных действий и оперативно-розыскных мероприятий, требующих совместного и безотлагательного проведения, может способствовать более эффективному оперативно-розыскному сопровождению расследования уголовного дела, что напрямую влияет на результативность в оперативно-служебной деятельности. Определение сроков как исполнения поручений следователя, так и их направления в органы, осуществляющие оперативно-розыскную деятельность, влияет на своевременность получения доказательств по делу. Установление согласованной системы предоставления материалов оперативно-розыскной деятельности, содержащих сведения о новых обстоятельствах расследуемого преступления или дополнительных составах преступлений, в следственные органы влияет на полноту и достаточность собранных доказательств.

От данного обстоятельства зависит окончательная квалификация содеянного и вынесение приговора суда.

Видится, что в настоящее время, в виду перманентного изменения социально-правовых условий, влияющих на состояние преступности, подходы к организации взаимодействия правоохранительных органов и органов уголовного преследования требуют дополнительного исследования. Все еще остаются неурегулированными некоторые правовые, организационные и тактические элементы механизма взаимодействия. Уголовно-процессуальное законодательство также не в полной мере регламентирует организацию взаимодействия при раскрытии и расследовании преступлений, имеет некоторые недостатки, требующие пересмотра, внесения изменений и дополнений.

УДК 343.985.7

А.П. Стефаненко, П.С. Гринь

ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКНОГО СОПРОВОЖДЕНИЯ РАССЛЕДОВАНИЯ КОРРУПЦИОННЫХ ПРЕСТУПЛЕНИЙ

На различных этапах развития общества и государства коррупция оказывала негативное влияние на уровень национальной безопасности. Несмотря на то что в настоящее время приняты существенные меры по борьбе с данным антисоциальным явлением, коррупционные риски все еще создают препятствия для эффективного развития государства.

Одной из главных задач правоохранительных и иных государственных органов является противодействие коррупции. Данные органы наделены соответствующими полномочиями, с учетом разграничения их компетенций. При этом высокая результативность их деятельности может быть достигнута путем организации и осуществления эффективного взаимодействия между ними. Рассмотреть такого рода взаимодействие можно на примере совместной работы следователя и органа дознания при расследовании коррупционных преступлений.

Взаимодействие следователя и оперативного сотрудника, как правило, начинается с момента принятия решения о возбуждении уголовного дела. В процессе взаимодействия происходит квалификация содеянного, выдвигаются версии совершения преступления, планируется проведение оперативно-розыскных мероприятий и следственных действий, согласовывается время и последовательность их проведения, подводятся промежуточные итоги по результатам совместной работы. В научной литературе под таким взаимодействием принято понимать оперативно-розыскное сопровождение или обеспечение. При этом полагаем, что отождествлять данные понятия не следует, так как их сущность и содержание разнятся. Так, в рамках оперативно-розыскной деятельности происходит обеспечение уголовного процесса оперативными данными, а также информацией о лицах и событиях, в отношении которых проводится расследование уголовного дела. Кроме того, проводятся оперативно-розыскные и иные проверочные мероприятия, в том числе в рамках направленных поручений следователя и т. д. Таким образом, процесс расследования обеспечивается результатами оперативно-розыскной деятельности, что по своей сути является оперативно-розыскным обеспечением уголовно-процессуальной деятельности.

По нашему мнению, применение данного подхода имеет место в тех случаях, когда до возбуждения уголовного дела оперативная разработка не осуществлялась, а поводом и основанием для возбуждения уголовного дела послужили иные обстоятельства. В свою очередь, когда возбуждению уголовного дела предшествовала оперативная разработка, результаты которой послужили основанием для возбуждения уголовного дела, а также ввиду того, что содержание соответствующего дела оперативного учета может быть значительно шире эпизода, явившегося основанием для возбуждения уголовного дела, целесообразнее использовать термин «оперативно-розыскное сопровождение».

С целью эффективного расследования коррупционного преступления представляется необходимым принимать во внимание вероятность возникновения препятствий со стороны подозреваемых, обвиняемых и их связей, что может потребовать своевременного реагирования на данные обстоятельства. В качестве одного из средств решения указанной задачи может выступать своевременно организованное и эффективно реализованное оперативно-розыскное сопровождение расследования уголовного дела.

По нашему мнению, при осуществлении такой деятельности целесообразно проводить оперативно-розыскные мероприятия, сопровождающие уголовный процесс, задачами которых являются: выявление дополнительных фактов противоправной деятельности; установление иных лиц, причастных к совершению расследуемого преступления; определение размера причиненного ущерба; розыск лиц, скрывшихся от уголовного преследования, и др.

Кроме того, с целью повышения эффективности оперативно-розыскного сопровождения по делам данной категории видится значимым осуществлять работу с лицами, оказывающими содействие на конфиденциальной основе.

Таким образом, в настоящее время вопросы оперативно-розыскного сопровождения расследования коррупционных преступлений остаются актуальными и не всегда разрешенными. При этом в совместной деятельности государственных органов, осуществляющих борьбу с коррупцией, во взаимодействии с иными органами и организациями, участвующими в борьбе с коррупцией, имеются значимые результаты, о чем свидетельствует снижение уровня коррупционной преступности. Однако представляется все еще актуальным совершенствовать способы и методы взаимодействия различных служб и ведомств в борьбе с коррупцией, одним из которых является оперативно-розыскное сопровождение расследования коррупционных преступлений.

УДК 343.98

А.М. Субцельный, К.С. Копач

ПРИМЕНЕНИЕ OSINT-ТЕХНОЛОГИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ И ПУТИ ЕЕ СОВЕРШЕНСТВОВАНИЯ

Современные реалии оперативно-розыскной деятельности (ОРД) требуют применения передовых технологий для поиска, сбора и анализа информации. Одним из самых актуальных направлений в данной сфере является использование технологии OSINT (Open Source Intelligence), которая подразумевает разведку на основе открытых источников. Это позволяет оперативным подразделениям правоохранительных органов получать данные из сети Интернет, социальных сетей и других доступных ресурсов, существенно увеличивая их возможности.

Существуют различные способы классификации методов, используемых OSINT. Наиболее практикоориентированный подход заключается в разделении на «активный» и «пассивный».

К «активным» методам можно отнести такие приемы сбора информации, как: анкетирование, интервьюирование и опрос; перехват бесед; внешнее наблюдение.

Преимущество указанного метода заключается в возможности получения информации высокого уровня достоверности, актуальности и значимости.

«Пассивный» метод, в свою очередь, не подразумевает под собой непосредственного контакта, взаимодействия с лицом. Данный метод

также можно разбить на определенные приемы поиска интересующей информации, к которым относятся:

сбор информации из открытых источников (средства массовой информации, сеть Интернет и т. д.), используя поисковые системы;

пассивное наблюдение с целью мониторинга конкретных свободных источников информации на протяжении определенного периода времени;

использование различных баз данных.

Существует также деление методов OSINT по типу источников информации. В этом случае методы можно классифицировать на методы сбора данных из источников специализированных (базы данных, репозитории, специализированные платформы и сервисы) и общественных (информация, доступная в открытых медиа, социальных сетях, форумах, блогах и других открытых ресурсах).

Стоит отметить, что данные, полученные с помощью OSINT-технологии, играют значимую роль в успешном раскрытии преступлений. Они способствуют более эффективному анализу, планированию и организации оперативной деятельности, в том числе формированию версий, выбору оптимальной тактики проведения оперативно-розыскных мероприятий.

Для этого сотруднику оперативного подразделения необходимо использовать так называемые OSINT-сервисы, перечень которых достаточно широк. Принцип работы этих сервисов основывается на сборе данных определенной направленности. Данная информация может выступать в роли идентификатора, по которому и осуществляется поиск. В этой связи все указанные сервисы объединяет и одновременно разграничивает объект поиска, среди которых, как правило, выделяют сервисы для сбора информации о персональных данных, адресах проживания, фотографиях, номерах телефона, электронной почте, никнеймах, домене.

Перечисленный список сервисов не является исчерпывающим, все больше появляется баз данных в открытых источниках, находящаяся информация в которых может являться предметом интернет-разведки и направлена прежде всего на борьбу с существующей проблемой деанонимизации личности пользователя сети Интернет.

Очевидно, что OSINT-технология востребована и требует активного внедрения при решении оперативно-розыскных задач соответствующей технологической базы и разработки комплекса материально-технических мер в виде программного софта, мобильных приложений, аппаратно-программных комплексов, задействования искусственного интеллекта.

Особую важность приобретает вопрос подготовки соответствующих специалистов, не сосредотачиваясь при этом на получении навыков использования этой технологии ограниченным кругом сотрудников специ-

ализированных оперативных подразделений органов внутренних дел, что требует модернизации современных образовательных программ.

В настоящее время отсутствует детальное регулирование данного метода, нет критериев, по которым информация из открытых источников может быть признана допустимой для использования в качестве доказательств в уголовном процессе.

Таким образом, OSINT-технология является неотъемлемой частью современного подхода к борьбе с преступностью, позволяя значительно расширять возможности в ходе осуществления оперативно-розыскной деятельности. В этой связи для полноценного внедрения данной технологии требуется комплексный подход, включающий в себя создание правового регулирования порядка его осуществления, совершенствование технической составляющей, использование искусственного интеллекта и обеспечение постоянного обучения и развития специалистов.

УДК 343.98

А.В. Трайнель, В.Ю. Мезяк

АНАЛИЗ КРИПТОВАЛЮТНЫХ ТРАНЗАКЦИЙ С ПОМОЩЬЮ ИНСТРУМЕНТА CHAINALYSIS ДЛЯ РАСКРЫТИЯ КИБЕРПРЕСТУПЛЕНИЙ

Современная цифровая экономика характеризуется ростом преступлений, связанных с использованием криптовалют, таких как Bitcoin, Ethereum, Solana и др. Эти преступления включают в себя легализацию преступных доходов, финансирование терроризма, мошенничество, атаки с использованием программ-вымогателей и др.

Ключевой проблемой, сдерживающей эффективное выявление и расследование преступлений данной категории, является децентрализованный характер криптовалют, их относительная анонимность, а также использование технологий анонимизации, таких как криптовалютные миксеры и приватные токены. Указанные факторы затрудняют применение традиционных методов выявления и расследования преступлений и требуют использования специализированных инструментов анализа блокчейн-транзакций.

В данный момент на рынке можно найти большое количество инструментов, помогающих в отслеживании криптовалютных транзакций. Например, Elliptic – программа, которая помогает банкам и биржам проверять, не связаны ли кошельки с преступниками, и показывает, откуда пришли деньги. Crystal Blockchain делает простые графики, чтобы компании могли следить за транзакциями и не нарушать законы. AnChain.AI использует умные алгоритмы, чтобы сразу замечать мошенничество или опасные переводы и связывать кошельки с реальными людьми. Есть еще бесплатные сайты, вроде Etherscan или Blockchain.com, где любой может посмотреть, кто кому отправил деньги, – это удобно для простых проверок. Для инвесторов есть платформы Glassnode, Santiment, которые показывают, что происходит на рынке, например, как много денег переводят крупные игроки. А разработчики могут использовать программные коды, такие как BitcoinJ или Web3.js, чтобы самостоятельно сделать программы для анализа блокчейна, если им нужно что-то особенное.

Одним из наиболее эффективных решений в данной сфере признан программный комплекс Chainalysis, разработанный одноименной американской компанией в 2014 г. Chainalysis предоставляет инструменты для мониторинга, анализа и визуализации криптовалютных транзакций, в том числе транзакций с участием миксеров, бирж и иных сервисов, потенциально задействованных в незаконной деятельности. Программное обеспечение включает в себя модули Reactor и KYT (Know Your Transaction).

Chainalysis – программа, которая помогает следить за движением денег в криптовалютах, таких как биткоин или эфир, чтобы обнаруживать преступников, которые, например, легализуют незаконный доход, совершают мошенничество или финансируют преступные организации. Она анализирует блокчейны – это как открытые книги, где записаны все транзакции: кто, кому и сколько отправил. Поскольку в блокчейне нет имен, а только адреса кошельков, Chainalysis позволяет понять, кто за ними стоит, даже если люди пытаются скрыться.

Программа работает с помощью искусственного интеллекта и умных алгоритмов, которые собирают и разбирают огромные объемы данных. Она замечает, какие кошельки связаны между собой, например, если несколько адресов используются в одной транзакции, Chainalysis считает, что они принадлежат одному человеку. Она просматривает также транзакции по шаблонам: если деньги часто переводятся между одними и теми же адресами, это может быть определенным сигналом.

Главный инструмент данной программы – Reactor, который позволяет ввести адрес кошелька и увидеть, куда ушли деньги, даже если их пытались спрятать через сложные схемы, вроде сервисов, которые смешивают транзакции, чтобы запутать следы.

Вторым инструментом программы Chainalysis является KYT, который следит за транзакциями прямо в момент их совершения. Он про-

веряет, не связаны ли деньги с подозрительными личностями, которые по различным причинам представляют интерес, и, при установлении связей, уведомляет оператора программы. Chainalysis хранит большую базу данных, где собраны адреса, связанные с биржами, хакерами или преступными сайтами, и постоянно добавляет новую информацию, чтобы быть на шаг впереди.

Для того чтобы убедиться в эффективности данного инструмента, мы можем обратиться к реальным делам, в которых правоохранительные органы использовали Chainalysis для расследования преступлений. В марте 2025 г. Федеральное бюро расследований и Министерство юстиции США с помощью Chainalysis изъяли 200 000 USDT, связанных с финансированием террористической организации, что демонстрирует эффективность инструмента. В 2022 г. благодаря Chainalysis были обнаружены $1 млрд в Bitcoin, украденные хакерами из биржи Mt. Gox. В России приговор по делу № 1-134/2019 (Тамбов) подтвердил использование криптовалюты в мошеннической схеме: злоумышленник имитировал платеж через СМС, чтобы похитить BTC у жертвы. Блокчейн-анализ позволил отследить перевод и доказать причастность обвиняемого.

Одной из основных проблем при выявлении и расследовании преступлений, связанных с криптовалютами, является развитие технологии анонимизации, такой как миксеры, перемешивающие транзакции для сокрытия их происхождения, и приватные монеты (например, Zcoin), использующие криптографические протоколы для обеспечения полной анонимности. Эти технологии создают барьеры для традиционного анализа, требуя применения передовых методов обработки данных.

Chainalysis эффективно справляется с вызовами, связанными с технологиями анонимизации, благодаря следующим решениям: использованию методов разборки транзакционных потоков для анализа транзакций через миксеры; применению методов анализа метаданных для выявления активности с использованием приватных монет; поддержке актуальной базы данных по методам анонимизации; внедрению алгоритмов машинного обучения для обнаружения аномалий; сотрудничеству с криптовалютными платформами, предоставляющими сведения о пользователях. Эти подходы позволяют преодолевать барьеры, создаваемые анонимизацией, и повышать результативность расследований.

Таким образом, использование инструмента Chainalysis представляет собой перспективное направление для повышения эффективности выявления и расследования преступлений, связанных с использованием криптовалют. В Республике Беларусь внедрение подобных технологий позволит адаптироваться к вызовам цифровой экономики и укрепить

экономическую безопасность. Для достижения устойчивых результатов необходимо обеспечить техническое оснащение правоохранительных органов, подготовку квалифицированных кадров и развитие международного сотрудничества. Будущие исследования могут быть направлены на создание национальных аналитических платформ, что снизит зависимость от иностранных технологий и повысит автономность в борьбе с киберугрозами.

УДК 363.985.8

А.Н. Тукало

НЕКОТОРЫЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНА РЕСПУБЛИКИ БЕЛАРУСЬ «ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ»

В настоящее время Министерством внутренних дел Республики Беларусь (далее – МВД) наряду с иными органами, осуществляющими оперативно-розыскную деятельность (ОРД), проводится работа по подготовке проекта закона по изменению и дополнению действующего Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Проект). В данной публикации принимает участие и кафедра оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь. Планируется внесение следующих дополнений и изменений:

1) дополнения прав органов, осуществляющих ОРД, следующим функционалом:

осуществлять оперативно-розыскной мониторинг, под которым понимается регулярный поиск информации, связанной с состоянием и изменением оперативной обстановки на закрепленных объектах, территории или по линиям работы, анализ и прогнозирование;

создавать и (или) использовать автоматизированные системы взаимодействия с организациями, включая электронный документооборот;

2) изменения и дополнения терминов, используемых в Законе Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон «Об ОРД») и их определений, в том числе определение термина «оперативно-розыскной мониторинг», уточнение термина «материалы оперативно-розыскной деятельности»;

3) дополнения перечня оперативно-розыскных мероприятий (ОРМ) новым видом «оперативный поиск», которое проводится по решению

должностного лица органа, осуществляющего ОРД, путем поиска и анализа информации из баз данных (учетов), информационных систем, хранящейся в общедоступных ресурсах глобальной компьютерной сети Интернет (далее – Интернет) и локальных компьютерных сетях в целях получения информации, имеющей значение для решения задач ОРД;

4) дополнения оснований проведения ОРМ необходимостью сбора сведений для обеспечения безопасности органов, осуществляющих ОРД;

5) обеспечения единого подхода в части регламентации оснований прекращения дел оперативного учета, в том числе заведенных в целях розыска лиц, установления персональных данных гражданина, который погиб (умер) или который в силу состояния здоровья или возраста не может сообщить о себе сведения;

6) совершенствования порядка прерывания соединения в сетях электросвязи при проведении ОРМ «контроль в сетях электросвязи»;

7) совершенствования порядка подготовки и проведения ОРМ при сборе сведений и применении мер по обеспечению безопасности, в том числе:

приведение норм Закона «Об ОРД» в соответствие с положениями Закона Республики Беларусь от 17 июля 2007 г. № 263-З «Об органах внутренних дел Республики Беларусь»;

закрепление в Законе «Об ОРД» психологического сопровождения гражданина, оказывающего или оказывавшего содействие на конфиденциальной основе органу, осуществляющему ОРД, и его близких, в отношении которых применяются меры по обеспечению безопасности.

Частично рассмотрим лишь 1-й и 2-й пункты Проекта. В Проекте предлагается «оперативно-розыскной мониторинг» определять как «функция по обеспечению эффективного контроля за состоянием и изменениями в оперативной обстановке и прогноза ее дальнейшего развития на определенной территории, конкретном объекте или по линии работы, посредством проведения комплекса мероприятий, в виде постоянного поиска информации, связанной с состоянием и изменением оперативной обстановки, анализа такой информации и прогнозирования на ее основе изменений оперативной обстановки с выработкой упреждающих мер, направленных на предупреждение преступлений и решение иных задач, возложенных на правоохранительные органы». Необходимо отметить, что относительно определения деятельности оперативных подразделений по контролю оперативной обстановки на линии работы, объекте или определенной территории в локальных правовых актах МВД до настоящего времени нет единого подхода к используемой терминологии. Данная деятельность определяется как «оперативное обслуживание объекта», «оперативный контроль за закрепленной территори-

ей», «контроль оперативной обстановки», «мониторинг оперативной обстановки» и др.

Следует учитывать, что с развитием информационно-коммуникационных технологий возникла потребность в постоянном мониторинге Интернета. Такой вид деятельности можно осуществлять посредством OSINT (Open Source Intelligence, разведки на основе открытых источников). В данном случае под открытыми источниками понимаются общедоступные ресурсы Интернета (интернет-сообщества, социальные сети и популярные мессенджеры (Viber, WhatsApp, Telegram, Messenger), блоги и форумы, видеохостинги и файлообменные серверы).

Поиск может осуществляться с использованием поисковых систем Google, Yandex, Rambler.ru, Yahoo.com, Bing.com, Duckduck.go и др. Кроме этого для решения задачи по установлению определенной информации могут использоваться поисковые функции целевых форумов, социальных сетей, иных ресурсов. Мониторинг Интернета может осуществляться также с использованием специализированных программных продуктов. Люди все больше времени проводят в социальных сетях, мессенджерах, иных интернет-площадках, оставляя на просторах Интернета и локальных компьютерных сетях, а также попадая в объективы камер видеонаблюдения сведения, которые могут существенно облегчить работу сотрудников правоохранительных органов.

Термин «оперативное обслуживание» появился в теории и практике ОРД в советский период и означал «изучение», «анализ» оперативной обстановки, слежение за ее состоянием, «контроль поведения соответствующих криминогенных контингентов». Такое «обслуживание» считалось «оперативным» ввиду сочетания гласных и негласных методов наблюдения, используемых при этом сил и средств. Однако оперативные подразделения и их сотрудники никогда не относились к сфере обслуживания, поэтому, на наш взгляд, использование термина «мониторинг», означающего «регулярное наблюдение за развитием какого-либо процесса, состояния, явления, их оценивание и прогнозирование», является предпочтительным.

Правовая регламентация осуществления «оперативно-розыскного мониторинга» предполагает: право органов, осуществляющих ОРД, создавать и (или) использовать автоматизированные системы взаимодействия с организациями, включая электронный документооборот; дополнение оснований проведения ОРМ необходимостью сбора сведений для обеспечения безопасности органов, осуществляющих ОРД; проведение по решению должностного лица органа, осуществляющего ОРД, поиска и анализа информации из баз данных (учетов), информационных

систем, в том числе создаваемых и используемых органами, осуществляющими ОРД, хранящейся в общедоступных ресурсах Интернета и локальных компьютерных сетях.

В настоящее время существующие программные продукты, базы данных (учеты) значительно облегчают работу оперативного сотрудника по поиску и анализу данной информации, а также сокращают время на решение повседневных служебных задач. Принципиальным в этом случае является именно результат «оперативного мониторинга», анализ разрозненных сведений из различных источников, а не сама исходная информация, которая может быть получена при проведении различных ОРМ.

УДК 363.985.8

А.Н. Тукало, Д.Г. Ананян

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ МАТЕРИАЛОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ДОКАЗЫВАНИИ ПО УГОЛОВНЫМ ДЕЛАМ

Одним из способов эффективного противодействия общественно опасным деяниям является использование материалов оперативно-розыскной деятельности (далее – материалы ОРД) в раскрытии преступлений, а также при оперативном сопровождении процесса расследования для создания доказательственной базы и изобличения виновных лиц.

Среди ученых имеется много аргументов «за» и «против» использования материалов ОРД в доказывании по уголовным делам, и данный вопрос остается дискуссионным, однако закрепление материалов, полученных в ходе ОРД в качестве источников доказательств, представляется, по нашему мнению, необходимым как для реализации принципов уголовного процесса, так и для успешного достижения его задач. Как отмечает Е.А. Доля, использование материалов ОРД допускается в доказывании уголовных дел только при условии строгого соблюдения процедуры их получения и оформления, поскольку от этого зависит законность и достоверность представленных доказательств.

По мнению С.С. Овчинского, материалы ОРД, собираемые в ходе специальных мероприятий, требуют дополнительной проверки и сопоставления с другими элементами доказательной базы, чтобы избежать нарушения баланса прав сторон в судебном процессе. В своих исследованиях А.С. Винберг подчеркивает, что ввод оперативно-розыскных материалов в качестве доказательств должен проводиться с обязательным

выделением их методологических особенностей, так как процедуры их получения и оформления отличаются от традиционных, что может негативно сказаться на объективности судебного разбирательства, если не предусмотрены дополнительные гарантии. М.С. Десятов в своей работе приходит к выводу, что материалы ОРД могут иметь решающее значение в доказывании состава преступления, однако их допустимость условно и определяется наличием строгого судебного контроля за процедурой их получения, что является залогом соблюдения принципов справедливости и законности в уголовном процессе.

В соответствии со ст. 2 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон) материалы ОРД – оперативно-служебные документы и материальные носители информации, содержащие порядок проведения оперативно-розыскных мероприятий, и сведения, полученные при их проведении, а также иные сведения и документы, полученные при осуществлении оперативно-розыскной деятельности. Направления использования материалов ОРД закреплены в абзацах втором – пятом части первой ст. 49 Закона, среди них – для подготовки и проведения следственных, иных процессуальных действий, доказывания в уголовном процессе.

Согласно ч. 2 ст. 88 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК) одним из источников доказательств являются, в том числе, и материалы ОРД. Исходя из положений нормы, закрепленной в ст. 101 УПК, материалы ОРД могут быть использованы в качестве доказательств. Проанализировав обе нормы, следует отметить то, что положения ст. 88 УПК очевидно называют и закрепляют источники доказательств, именуя материалы ОРД таковыми, когда, напротив, положения ст. 101 УПК закрепляют лишь возможность использования материалов в качестве одного из источников доказательств. Содержание ст. 101 УПК свидетельствует о том, что материалы ОРД могут быть источником доказательств только после их проверки и оценки, произведенной в порядке, установленном УПК. Однако следует отметить, что в УПК установлена процедура проверки и оценки доказательств, а не их источников. Более того, из ст. 101 УПК «выпала» важная составляющая процесса доказывания, присущая правовому режиму формирования доказательств в уголовном процессе, такая как этап их собирания. Вместе с тем именно с порядком собирания доказательств законодатель связывает систему гарантий доброкачественности получаемых доказательств, так как, исходя из абзаца четвертого части первой ст. 14 Закона, предоставление (представление) материалов ОРД органу уголовного преследования и суду есть не что иное, как обязанность органа, осуществляющего ОРД.

Несмотря на специфику такого источника доказательств, предоставленные в соответствии с Законом и ведомственными нормативными актами, регламентирующими порядок предоставления (представления) материалов ОРД, последние должны быть оценены в соответствии с критериями, предусмотренными ст. 105 УПК. Немаловажным критерием оценки доказательств является элемент их допустимости. Материалы ОРД будут ему соответствовать, если: соблюдены цели, задачи, принципы ОРД (ст. 3, 5–9 Закона); оперативно-розыскное мероприятие проведено уполномоченным на то органом – субъектом ОРД (ст. 12 Закона); проведено оперативно-розыскное мероприятие, предусмотренное законом (ст. 18 Закона); орган, осуществляющий ОРД, действовал в пределах своей компетенции, установленной законодательством (ст. 15 Закона); имелись основания для проведения данного оперативно-розыскного мероприятия (ст. 16 Закона); соблюдены условия проведения оперативно-розыскного мероприятия (ст. 19 Закона); соблюден особый порядок проведения оперативно-розыскного мероприятия, требующего получения санкции прокурора (ст. 19, 35–39 Закона); обеспечены гарантии социально-правовой защиты гражданам, содействующим органам, осуществляющим ОРД (ст. 51–54 Закона).

Современное состояние использования материалов ОРД в доказывании по уголовным делам, на наш взгляд, могло бы быть более интенсивным, если бы было усовершенствовано уголовно-процессуальное законодательство Республики Беларусь. Так, относительно доказательственного значения материалов ОРД в ст. 99 УПК закреплено, что источниками доказательств являются протоколы оперативно-розыскных мероприятий о прослушивании и записи переговоров, осуществляемых с использованием технических средств связи, и иных переговоров, составленные в установленном законом порядке и с приложением соответствующей записи прослушивания. Неоднократно обращалось внимание теоретиков и практиков, что неясно из указанной формулировки протоколов о проведении каких оперативно-розыскных мероприятий имеет в виду законодатель (ввиду отсутствия в Законе оперативно-розыскного мероприятия «прослушивание и запись переговоров»). С целью устранения названных противоречий считаем целесообразным внести в УПК следующие изменения и дополнения.

Изменить название ст. 99 УПК на «Протоколы следственных действий, звуко- или видеозаписи хода судебных заседаний, протоколы судебных заседаний». Содержание указанной статьи изложить таким образом: «Источниками доказательств являются составленные в порядке, предусмотренном настоящим Кодексом, протоколы следственных действий, удостоверяющие обстоятельства и факты, установленные при осмотре,

освидетельствовании, выемке, обыске, предъявлении для опознания, проверке показаний на месте, следственном эксперименте, эксгумации; звуко- или видеозапись хода судебного заседания, протокол судебного заседания, отражающие ход судебных действий и их результаты».

Изменить название ст. 101 УПК на «Материалы оперативно-розыскной деятельности» и изложить ее в следующей редакции: «Материалы оперативно-розыскной деятельности являются источниками доказательств при условии, если они получены и предоставлены в соответствии с законодательством Республики Беларусь, проверены и оценены в порядке, установленном настоящим Кодексом».

На наш взгляд, указание в ч. 2 ст. 88 УПК, что материалы ОРД являются источниками доказательств (а, как указано выше, к ним относятся и протоколы оперативно-розыскных мероприятий) и наличие отдельной статьи (ст. 101 УПК) лишает необходимости отдельно прописывать в ст. 99 УПК, что «источниками доказательств являются протоколы оперативно-розыскных мероприятий».

Считаем, что внесение указанных изменений в УПК будет способствовать единообразному пониманию терминологии, используемой в УПК и Законе, а также позволит упорядочить нормы, касающиеся использования материалов ОРД в доказывании по уголовным делам.

УДК 159.9

И.А. Фомина

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ ПРОФАЙЛИНГА В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Профайлинг – технология анализа поведенческих, психологических и социальных характеристик личности с целью выявления потенциально опасных лиц, раскрытия преступлений и их профилактики. В оперативной деятельности профайлинг дает возможность составить профиль преступника и спрогнозировать их деятельность, что позволяет оптимизировать оперативно-розыскные мероприятия (ОРМ).

Стратегии профилирования в рамках раскрытия и расследования преступлений направлены на решение задач по составлению профиля неизвестным преступником – криминальное профилирование, чаще всего используется при расследовании серийных преступлений, террористических актов, а также при киберпреступлениях (для целей составления профиля хакера), на основе анализа способа совершения преступления,

изучения особенностей выбора жертвы и определения «подписи» преступника. Однако это не единственная возможность по использованию рассматриваемой технологии в оперативно-розыскной деятельности. Немаловажным являются возможности профайлинга в рамках поведенческого анализа, когда происходит выявление и прогнозирование действий подозреваемых по невербальным признакам (мимика, жесты, манера речи) при непосредственном наблюдении, а равно в рамках профилактической деятельности, когда выявляются лица, склонные к экстремизму, насилию, мошенничеству, при анализе социальных сетей.

Несмотря на то что профайлинг используется правоохранительными органами, он остается спорным. Критики утверждают, что ему часто не хватает эмпирической проверки. Он, в значительной степени, опирается на субъективную интерпретацию и может способствовать когнитивным искажениям в уголовных расследованиях. Исторически профайлинг основывался на интуиции и опыте, но по мере развития этой области знаний необходимость в более научно обоснованном подходе привела к разработке эмпирических моделей (типологий) поведения преступников, с учетом концепции мотивов и статистического подхода к анализу данных – это позволило объединить знания специалистов-практиков с объективным изучением закономерностей преступлений и связанных с ними результатов. Достижения в области юридической психологии и методологии, основанной на эмпирических данных, продолжают формировать эту сферу, объединяя психологические теории со статистическим анализом для повышения надежности и точности полученных данных.

При составлении психологического портрета преступника используются две основные стратегии-предположения: последовательность в поведении и гомология. Последовательность в поведении – это идея о том, что преступления, совершенные преступником, будут похожи друг на друга. Гомология – это идея о том, что похожие преступления совершаются похожими преступниками. Несмотря на общность технологий профайлинга, применяемых в следственной и оперативной практиках, в рамках оперативно-розыскной деятельности использование сводится в следующие направления:

в розыскной работе: позволяет сузить круг подозреваемых на основе психологических и поведенческих признаков и оказать помощь при задержании;

при оперативном сопровождении уголовных дел: позволяет более тщательно продумать тактику ОРМ, задержания и опросов, спрогнозировать побеги или возможность повторного совершения преступления.

Однако наиболее эффективно рассматриваемая технология может себя проявить в рамках такого направления, как «географический

профайлинг» – метод анализа пространственных закономерностей совершения преступлений с целью определения предполагаемого места жительства или работы преступника, зон его комфорта, а также прогнозирования вероятных мест совершения преступлений в будущем. В оперативно-розыскной деятельности данная технология используется в основном при расследовании серийных преступлений, террористических актов и поиске скрывающихся преступников. В основе данного направления лежат принцип наименьшего усилия (преступник действует в знакомых местах), теория кругового поиска (преступник действует в пределах определенного радиуса) и концепция географической стабильности (преступники редко меняют свои паттерны перемещения), которые позволяют, на основе использования модели Крэсси (анализ «узлов» (дом, работа), «путей» (маршруты) и «краев» (границы зон активности)), модели (формулы) Россмо (математический расчет вероятного места жительства на основе распределения мест преступлений) и геопрофилирования по Кантеру (определение центра активности и радиуса действий преступника), определить все связанные с преступлением места, проанализировать их пространственное расположение (построение карт плотности), определения очага активности и прогнозирование зон риска (выявление районов, где возможны следующие преступления). Конечно, существуют определенные ограничения использования данной технологии. Так, ее использование менее эффективно при прогнозировании «гастролерных» преступников и требует точных пространственных данных, однако преимущества технологии существеннее: позволяет сузить район поиска, спрогнозировать новую преступную активность, эффективна при недостатке доказательств.

Кроме того, в качестве перспективных направлений развития использования технологии профайлинга в оперативно-розыскной деятельности можно выделить:

интеграцию с Big Data (анализ мобильных данных, транзакций, камер наблюдения), позволяющую анализировать огромные массивы информации, выявлять скрытые закономерности и прогнозировать преступную активность, распознавать образы и лица. Например, выявление связей между подозреваемыми через анализ телефонных переговоров, социальных сетей, финансовых активностей; использование графовых баз данных (Neo4j, TigerGraph), которые помогают визуализировать криминальные схемы; обнаружение криптовалютных схем (Blockchain-анализ, Chainalysis); мониторинг социальных сетей и Darknet для выявления угроз, экстремизма, незаконной торговли и сбора данных (NLP-анализ, Scraping, OSINT) и др.;

ИИ-профилирование. Например, анализ потенциально опасных текстов, выявление хакеров по стилю программирования, методам атак; анализ darknet-форумов для поисков сбытчиков оружия, наркотиков, похищенных данных; для обучения; для распознавания лиц; создания фотороботов на основе словесного портрета; нейроинтерфейсы (например, Brainwave-анализ) и др.

В целом следует отметить, что, несмотря на существующие недостатки в использовании технологии профайлинга в оперативно-розыскной деятельности, преимуществ ее применения намного больше.

УДК 343.985 + 341.244.3

Д.Л. Харевич

СОВРЕМЕННОЕ СОДЕРЖАНИЕ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ В КОНТЕКСТЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА

Широкое использование современных технологий в преступной деятельности влечет за собой необходимость применения адекватных средств противодействия ей. К ним относится «электронное наблюдение», представляющее собой один из специальных методов расследования. Институт специальных методов расследования был впервые в полном объеме предусмотрен в Конвенции ООН против транснациональной организованной преступности (г. Нью-Йорк, 15 ноября 2000 г.) и позже использован в Конвенции ООН против коррупции (Нью-Йорк, 31 октября 2003 г.), иных многосторонних международных договорах, например, в Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (Варшава, 16 мая 2005 г.) и других региональных многосторонних международных договорах.

Поскольку их участниками является большинство стран мира, данный институт входит в число глобальных стандартов международного сотрудничества и выступает одним из источников формирования национального законодательства. С учетом этого актуальным является вопрос о его соотношении с понятиями национального права. Как показано ранее, в правовой системе Беларуси, России и ряда других постсоветских государств категорией, наиболее близкой к специальным методам расследования, являются оперативно-розыскные мероприятия (ОРМ) и негласные следственные действия. В то же время их нельзя сопоставлять буквально, поскольку специальные методы расследования выступают

институтом международного права и почти никогда непосредственно не применяются (в большинстве стран используется порядок осуществления соответствующих им процедур, предусмотренный национальным законодательством). С учетом указанных аспектов необходимо говорить не о соответствии отдельных специальных методов расследования тем или иным категориям национального законодательства, а о сопоставлении возможностей получения информации путем применения тех или иных негласных способов. В этой связи в запросе об оказании содействия в соответствии с вышеприведенными международными договорами нужно ссылаться не на отдельные виды специальных методов расследования, а на данный институт в целом, предоставляя возможность исполнителю самостоятельно избирать доступные и целесообразные способы его выполнения.

Несмотря на отмеченные аспекты, раскрытие содержания отдельных видов специальных методов расследования не лишено смысла по ряду причин. Прежде всего это позволяет более предметно запрашивать требуемое содействие у зарубежных партнеров. Во-вторых, такой подход раскрывает потенциал совершенствования законодательства и правоприменительной практики, поскольку содержание отдельных видов специальных методов расследования не является постоянным, адаптируется к изменяющимся видам и способам совершения преступлений. Появляются новые разновидности специальных методов расследования, позволяющие более эффективно выполнять правоохранительные задачи борьбы с противоправными посягательствами.

К электронному наблюдению относят действия правоохранительных органов, связанные с применением специальных технических, электронных и программных средств, направленные на получение криминально значимых сведений о содержании и обстоятельствах действий наблюдаемого лица, передаваемых и хранимых им данных либо истребование таких данных или сведений о них от других лиц, которые их обрабатывают или хранят. Как и иные специальные методы расследования, электронное наблюдение проводится без ведома лица, в отношении которого оно осуществляется. В отличие от них, электронное наблюдение не сопровождается каким-либо воздействием представителя правоохранительного органа (его конфидента) на наблюдаемое лицо.

В документах ООН электронное наблюдение включает в себя использование «подслушивающих устройств или перехвата сообщений», не связанных с физическим внедрением сотрудников правоохранительных органов или других лиц либо непосредственным наблюдением за действиями. Его подразделяют на аудионаблюдение (акустический контроль, audio surveillance), видеонаблюдение (визуальное наблюдение,

visual surveillance), контроль за передвижением (отслеживание местоположения, tracking surveillance), наблюдение за данными (цифровое отслеживание, data surveillance). Развитие форм электронного наблюдения от периода его зарождения идет путем появления новых разновидностей: от ранних способов аудионаблюдения в виде прослушивания переговоров, осуществляемых по проводным каналам связи, до современных форм наблюдения за данными путем перехвата сетевого трафика.

Полагаем, что в правовой системе Республики Беларусь аналогами электронного наблюдения являются:

разновидности ОРМ «наведение справок» о телефонных соединениях, месте совершения вызовов в сети сотовой связи, аппаратных и программных идентификаторах используемых при этом устройств, о месте и обстоятельствах совершения финансовых транзакций и ряде сопутствующих сведений;

«сбор образцов» путем копирования компьютерной информации с сетевых ресурсов и локальных хранилищ данных;

«оперативное отождествление» с применением биометрических и иных технологий для идентификации личности и иных объектов (анализ голоса, распознавание внешности и номерных знаков транспорта);

«оперативный осмотр» информационных систем, информационных ресурсов, компьютерной информации путем удаленного доступа;

«наблюдение» с использованием средств негласного получения (фиксации) информации;

«слуховой контроль»;

«контроль в сетях электросвязи», в том числе установление, получение аппаратных и программных идентификаторов устройств и аккаунтов;

«контроль почтовых отправлений»;

такие способы реализации прав органов, осуществляющих ОРД, как «получение сведений из баз данных (учетов), информационных систем»;

«использование баз данных (учетов), информационных систем, средств негласного получения (фиксации) информации и иных средств» (в том числе получение данных с использованием устройств геопозиционирования, слежения за местонахождением, а также путем автоматизированной обработки больших массивов данных);

следственное действие «прослушивание и запись переговоров».

24 декабря 2024 г. Генеральной Ассамблеей ООН в составе делегаций 193 государств – членов ООН принята Конвенция ООН против киберпреступности. Она восприняла концептуальные подходы, отраженные в предшествующих ей глобальных соглашениях по борьбе с транснациональными преступлениями, а также Конвенция Совета Европы о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.).

Перечень мер по получению сведений компетентными государственными органами в борьбе с преступлениями, совершаемыми с использованием информационно-телекоммуникационных систем, предусмотренных указанной Конвенцией ООН, относятся: распоряжение о предоставлении информации (абонентских или электронных данных), обыск и изъятие хранимых электронных данных (в информационно-коммуникационной системе или на носителе электронных данных), сбор в режиме реального времени данных о трафике, перехват данных о содержании. Данные меры применяются по распоряжению компетентного правоохранительного органа поставщиками услуг, т. е. организациями, которые обеспечивают пользователям возможность обмена информацией посредством использования информационно-коммуникационной системы либо осуществляют обработку или хранение электронных данных от имени такого поставщика коммуникационных услуг или пользователей таких услуг (например, хостинг, кэширование, услуги доступа к сети Интернет).

Рассматривая перечисленные меры в контексте электронного наблюдения, в тексте названной Конвенции ООН явное указание на негласный характер имеется лишь в отношении последних двух мер, хотя остальные также могут проводиться негласно. Как видно, что большинство приведенных мер относятся к такому виду электронного наблюдения, как наблюдение за данными (цифровое отслеживание, data surveillance).

Являются ли меры, приведенные в указанной Конвенции ООН, новациями для белорусского законодательства? С одной стороны, вышеперечисленные оперативно-розыскные действия и ОРМ достаточно полно охватывают предусмотренные ею меры. Среди ОРМ, предусмотренных в законодательстве Республики Беларусь, их аналогами являются: наведение справок, сбор образцов, оперативный осмотр, контроль в сетях электросвязи. Вместе с тем это не исключает совершенствования организационно-правовых форм и способов их реализации, например, путем налаживания каналов прямого доступа компетентных государственных органов к программно-аппаратным средствам поставщиков услуг, создание необходимых информационных систем, программных продуктов, обеспечивающих сходный функционал.

Полагаем, что важное значение приведенной Конвенции ООН для Республики Беларусь заключается не столько в определении направлений совершенствования отечественного законодательства, сколько в обеспечении универсального механизма оказания международного содействия по делам оперативного учета и уголовным делам. Как известно, большинство поставщиков, предоставляющих на территории Республики Беларусь различные услуги хранения и обмена данными,

располагаются за ее пределами (социальные сети, мессенджеры, облачные хранилища, поисковые системы, стриминговые платформы). Отсутствие по ряду причин двусторонних договоров с некоторыми государствами, на территории которых расположены хранилища данных этих поставщиков, затрудняет международное сотрудничество в борьбе с киберпреступлениями. Рассматриваемая Конвенция ООН после присоединения к ней Республики Беларусь может служить правовым основанием для такого сотрудничества, особенно учитывая детальную регламентацию соответствующих процедур в ее тексте.

УДК 343.985.8

Я.А. Хлыстова, Р.В. Глубоковских

АКТУАЛЬНЫЙ ИНСТРУМЕНТАРИЙ OSINT И ПЕРСПЕКТИВЫ ЕГО ПРИМЕНЕНИЯ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

В настоящее время оперативно-розыскная деятельность (ОРД) сталкивается с беспрецедентными вызовами, спровоцированными цифровизацией общества, ростом киберпреступности и усложнением методов противодействия правоохранительным органам. В сложившихся условиях традиционные методы сбора информации часто оказываются недостаточно эффективными, что требует внедрения инновационных технологий, способных обеспечить своевременное выявление и предупреждение преступлений. Одним из ключевых направлений развития ОРД в последние годы стало активное использование технологии открытого сбора информации (OSINT – Open Source Intelligence), позволяющей получать и анализировать данные из общедоступных источников.

OSINT представляет собой методологию сбора, обработки и анализа информации, находящейся в свободном доступе: социальные сети, форумы, блоги, государственные реестры, средства массовой информации, данные геолокации и метаданные цифровых файлов. В отличие от классических оперативно-розыскных мероприятий, OSINT не требует санкционированного доступа к закрытым данным, что значительно снижает временные и ресурсные затраты, а также минимизирует правовые риски.

Современные инструменты OSINT выступают комплексом программных и методических решений, позволяющих качественно собирать, исследовать и визуализировать данные из открытых источников. В зависимости от поставленных задач их можно классифицировать по нескольким ключевым направлениям.

1. Поисковые системы и агрегаторы информации (Google Dorks, Shodan, Censys, SpiderFoot и др.) – технологии, которые позволяют находить скрытые данные, используя специальные поисковые операторы. Одним из ключевых применений этих технологий в ОРД является выявление утечек конфиденциальной информации, включая документы, базы данных и учетные данные.

2. Анализ социальных сетей и цифровых следов (Maltego, Social Links, ExifTool, TinEye и др.) – программное обеспечение для визуализации связей между людьми, организациями и доменами, например, Facebook и Linkedln, может быть полезно в установлении связей между подозреваемыми в преступной деятельности и их социальным окружением.

3. Геоинформационные и временные данные (Google Earth Pro, Sentinel Hub, Hunchly) – программы для анализа спутниковых снимков и исторических данных, использующиеся для изучения географических особенностей местности и выявления закономерностей.

4. Автоматизация и обработка больших данных в OSINT (OSINT Framework, TheHarvester, Palantir Gotham, Recorder Future) – структурированная база инструментов и методов для решения различных задач в сфере OSINT, включая сбор электронных адресов, анализ доменов.

5. Специализированные инструменты для ОРД (DarkOwl, Blockchain Analysis) – технологии, предназначенные для мониторинга и отслеживания даркнет-пространства, криптовалютных транзакций и анализа активности в блокчейн-сетях, помогают выявить подозрительные финансовые операции и скрытые схемы.

Рассмотрев теоретические аспекты применения инструментов OSINT, необходимо привести реальные примеры их использования на практике. Так, благодаря одному из инструментов OSINT, направленному на обнаружение фишинговых и мошеннических схем, в 2023 г. SpiderFoot была выявлена сеть, включающая более 120 фишинговых сайтов, которые имитировали интерфейс Сбербанка, используя общие шаблоны HTML-кода.

В рамках расследования утечки данных клиентов российской телекоммуникационной компании комбинация Google Dorks (filetype:sql “password”) и поиск в RaidForums позволили обнаружить исходный SQL-дамп до его публикации в открытом доступе.

В 2022 г. мониторинг Telegram-каналов экстремистской направленности с использованием инструментов Social Links также позволил выявить координатора вербовочной сети по повторяющимся паттернам времени публикации контента.

В 2021 г. розыск преступника, скрывавшегося от исполнения условного осуждения, был успешно завершен благодаря обнаружению его аккаунта в игре War Thunder, где он использовал электронный адрес,

совпадающий с данными, найденными в скомпрометированной базе почтового сервиса.

Технологии открытого сбора информации играют ключевую роль в современной оперативно-розыскной деятельности, предоставляя правоохранительным органам эффективные инструменты для широкого спектра задач. Внедрение методик OSINT способствует значительному повышению результативности оперативной работы за счет таких факторов, как расширение возможностей сбора информации, автоматизации аналитических процессов, оптимизации временных и ресурсных затрат, повышению качества доказательственной базы.

Однако применение инструментов OSINT в ОРД сопряжено с рядом проблем:

юридические ограничения – необходимость строгого соблюдения норм законодательства, регулирующих вопросы защиты персональных данных;

технические трудности – постоянное совершенствование методов сокрытия информации преступными элементами;

этические дилеммы – риск нарушения права на частную жизнь граждан при массовом сборе данных.

Для оптимальной реализации потенциала методик OSINT необходимо доработать нормативно-правовые базы, регулирующие работу доступными источниками информации, организовать непрерывное обучение оперативных сотрудников новым цифровым технологиям и способам анализа данных и целесообразно развивать международное сотрудничество в области обмена опытом и внедрения лучших практик.

Грамотное использование OSINT-инструментов способно значительно повысить качество оперативно-розыскных мероприятий, поэтому требуется подойти комплексно к устранению выявленных недостатков для создания действенного средства в борьбе с преступностью.

УДК 343.985.8

В.Н. Цынкевич

ОПЕРАТИВНО-РОЗЫСКНАЯ СИТУАЦИЯ: ПОНЯТИЕ, ЗНАЧЕНИЕ И КЛАССИФИКАЦИЯ

Любые действия оперативных подразделений осуществляются в окружающей реальности. Выступая субъектами оперативно-розыскной деятельности (ОРД), оперативные сотрудники решают комплексные задачи по борьбе с преступностью в продиктованных им условиях

и обстоятельствах, которые складываются в определенные временные рамки. Такое положение раскрывается через содержание понятия «оперативно-розыскная ситуация».

Обзор юридической литературы по избранной теме показывает, что оперативно-розыскная ситуация – это «реально существующее на данный момент состояние определенного криминального события, по поводу которого осуществляется ОРМ, условие, в которых оно проявляется, и возможности оперативного работника (или аппарата) принять необходимые меры, формулируемые в виде конкретной задачи»; «складывающаяся по поводу криминального поведения совокупность пространственно-временных и иных факторов, характеризующих ход, процесс ОРД, условия, в которых она осуществляется, и одновременно оказывающих управляющее воздействие на ее организацию и тактику». Большинство ученых рассматривают вышеуказанное понятие с позиции научной категории и элемента оперативно-розыскной тактики.

В криминалистических методиках встречается сходный термин «следственная ситуация», рассматриваемый как «совокупность фактических данных, которые отражают существенные черты события, каким оно представляется на том или ином этапе расследования преступлений»; «сложившаяся динамичная совокупность характеризующих расследование информационных, доказательственных, организационно-технических и тактических факторов, анализ и оценка которых влияют на определение направлений расследования, принятие решений и выбор способов действия»; «совокупность условий, в которых в данный момент осуществляется расследование, то есть та обстановка, в которой протекает процесс доказывания». Некоторые авторы полагают, что «в ходе расследования имущественных общественно опасных деяний, совершенных в условиях неочевидности, оценке подлежит доказательственная и оперативно-розыскная информация, что воедино представляет собой следственно-оперативную ситуацию».

При разработке практических рекомендаций по выявлению и раскрытию отдельных видов преступлений ситуационный подход используется в качестве метода научного познания. Изученная концептуальность его применения в различных областях позволяет выделить гносеологическую сущность, которая заключается в получении заинтересованным субъектом сведений об особенностях ситуации и оказании в случае необходимости на нее воздействия для достижения поставленных целей.

Ситуационный подход позволяет изучить любую систему – сочетание взаимосвязанных между собой элементов. Согласно ему любая организация представляет собой некую открытую структуру, непрерывно взаимодействующую с внешней средой. Для установления причин,

происходящих внутри данной организации, следует изучить складывающиеся обстоятельства извне, а именно, в тех условиях, где она реально существует. Этому способствует применение системного анализа – комплекса средств конструирования и управления системами, основным назначением которого является решение проблемных ситуаций. Как отмечает В.Г. Афанасьев, «системный анализ позволяет расчленить сложную систему на элементы, сложную задачу – на совокупность простых, выразить их количественно, а значит, с большей степенью точности».

Характеризуя аналогичную оперативно-розыскной ситуации категорию, Р.С. Белкин отмечает, что сложный, многокомпонентный состав следственной ситуации, значительное число объективных и субъективных факторов, влияющих на содержание и характер этих компонентов, образуют в своих сочетаниях неисчерпаемое количество вариантов следственных ситуаций, каждая из которых чем-то обязательно отличается от других. Данное мнение разделяет С.И. Давыдов, уточняя, что каждая ситуация представляет собой уникальное событие: вместе с тем многие ситуации признаются на практике минимально различимыми, что дает основание говорить о том, что они являются типичными.

При разработке научно обоснованных рекомендаций по выявлению преступлений, типы оперативно-розыскных ситуаций формируются с двумя условиями: многократной их повторяемости в практической деятельности; наличием общих признаков проявления, например, идентичный способ совершения преступления. В свою очередь, моделирование этих ситуаций эффективно используется, когда оперативный сотрудник испытывает затруднения в принятии тактических решений. Данный метод способствует распознанию незнакомых обстоятельств, сложившихся в реальности, путем их сопоставления с типичными, для которых имеется наиболее оптимальный алгоритм действий.

Как показывает ретроспективный анализ юридической литературы, одним из первых к вопросу классификации оперативно-розыскных ситуаций обращается В.Г. Самойлов. Он разделяет указанные ситуации по различным основаниям, в зависимости от времени их возникновения: начальные, промежуточные и конечные; по возможности достижения желаемого результата: благоприятную и неблагоприятную; по степени повторяемости на практике: типичную и специфическую; по характеру и степени противоборства: бесконфликтную или конфликтную.

Воззрения данного автора представляют научный интерес в теоретическом аспекте, позволяя глубже уяснить смысл этой категории. Вместе с тем для решения практических задач приведенная классификация не в полной мере уместна, поскольку используемые в ее основе критерии носят универсальный характер обобщения информации, не конкретизируют явление. Например, не вызывает сомнений, что ситуации являются благоприятными или неблагоприятными, бесконфликтными или конфликтными, исходя из объективных причин или субъективного восприятия, которое зависит от интеллектуального уровня развития оперативного сотрудника, опыта его работы, индивидуально-психологических и других качеств.

На наш взгляд, прикладную направленность имеет классификация, предложенная С.И. Давыдовым, где выделяются: 1) ситуации, характеризующие степень осведомленности о признаках криминального поведения, в том числе о событии преступления. Например, таковы группы ситуаций, связанные с получением первичных оперативных данных, требующих проверки, с получением неполных данных о преступлении (неизвестны место, время, способ и т. д.); 2) ситуации, характеризующие степень осведомленности о лицах, совершивших или совершающих преступления; 3) ситуации, характеризующие степень осведомленности о лицах, которые могут выступить в качестве свидетелей; 4) ситуации, характеризующие степень осведомленности о ценностях, предметах, которые могут выступить вещественными доказательствами; 5) ситуации, характеризующие степень осведомленности о месте нахождения потерпевшего (трупа); 6) ситуации, характеризующие степень осведомленности о месте, времени совершения готовящегося преступления.

Таким образом, классификация оперативно-розыскных ситуаций в прикладных целях должна формироваться на основе информационного критерия, поскольку находящаяся в распоряжении оперативно-розыскная информация, во-первых, влияет на выбор тактического решения, позволяющего исключить либо минимизировать противодействие со стороны преступников, во-вторых, создает условия для рационального и эффективного распределения имеющихся сил и средств, в-третьих, обеспечивает возможность выполнения различных задач ОРД.

УДК 343.985

А.А. Чехович

ЛИЧНОСТЬ ПОТЕРПЕВШЕГО КАК ЭЛЕМЕНТ ОПЕРАТИВНО-РОЗЫСКНОЙ ХАРАКТЕРИСТИКИ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В условиях стремительного развития информационных технологий и глобализации цифрового пространства несанкционированный до-

ступ к компьютерной информации (НДКИ), предусмотренный ст. 349 Уголовного кодекса Республики Беларусь, представляет собой значительную угрозу информационной безопасности. Данный вид преступления характеризуется большой распространенностью, высокой степенью латентности и сложностью раскрытия, требует системного подхода к анализу его структуры, что обеспечивается разработкой оперативно-розыскной характеристики (ОРХ). ОРХ, как информационная модель, интегрирует данные о различных аспектах преступления, включая предмет посягательства, способы и орудия совершения, а также личности преступника и потерпевшего, для оптимизации оперативно-розыскных мероприятий. Особое внимание в структуре ОРХ НДКИ уделяется личности потерпевшего, которая выступает не только объектом преступного воздействия, но и ключевым элементом, влияющим на раскрытие и предупреждение данного вида преступлений.

Личность потерпевшего в контексте ОРХ НДКИ определяется как совокупность социально-психологических, профессиональных и поведенческих характеристик, которые обусловливают уязвимость индивида или организации к преступным посягательствам. Анализ оперативно-розыскной практики и данных информационного центра Министерства внутренних дел Республики Беларусь (далее – ИЦ МВД) свидетельствует о том, что потерпевшими от НДКИ могут быть как физические лица, использующие средства компьютерной техники в повседневной деятельности, так и юридические лица, применяющие специализированные программные продукты (например, семейства «1С»), для автоматизации хозяйственных процессов. Уязвимость потерпевших во многом связана с недостаточным уровнем цифровой грамотности, проявляющимся в использовании упрощенных паролей, незащищенном хранении идентификационных данных и отсутствии мер шифрования при передаче конфиденциальной информации. Эти факторы создают благоприятные условия для реализации преступного умысла, особенно в случаях, когда преступники применяют методы социальной инженерии или программные средства для подбора паролей по технологии «Брутфорс».

Значимость личности потерпевшего в структуре ОРХ НДКИ обусловлена ее причинно-следственной взаимосвязью с другими элементами, такими как способ и орудия совершения преступления. Например, низкий уровень цифровой грамотности физических лиц, проявляющийся в выборе легко угадываемых паролей или хранении идентификаторов доступа в открытом виде, предопределяет применение преступниками методов фишинга или программного обеспечения технологии «Брутфорс». В отношении юридических лиц уязвимости, связанные с

недостаточной сменой идентификаторов доступа при кадровых изменениях или слабой организацией технических мер защиты, способствуют использованию злоумышленниками программных атак на системы автоматизации, таких как «1С». Установление характеристик личности потерпевшего позволяет прогнозировать вероятные способы совершения НДКИ, что, в свою очередь, ориентирует оперативные подразделения на выбор соответствующих тактических приемов для раскрытия рассматриваемого вида преступления.

Особое значение в анализе личности потерпевшего имеет социально-психологический аспект, связанный с особенностями поведения в цифровой среде. Анализ данных ИЦ МВД показывает, что физические лица с ограниченным количеством социальных контактов в сетях (до 100 друзей или подписчиков) чаще становятся объектами НДКИ, поскольку их аккаунты предполагают доверительное общение, что упрощает реализацию мошеннических схем, таких как рассылка сообщений с просьбами о денежных переводах. Для юридических лиц и индивидуальных предпринимателей уязвимость связана с приоритетами сохранения репутации на рынке, что может приводить к латентности НДКИ, когда организации предпочитают не обращаться в правоохранительные органы, чтобы избежать огласки. Эти поведенческие особенности потерпевших формируют специфическую обстановку совершения преступления, которая требует учета при разработке оперативно-розыскных версий и планировании мероприятий.

Взаимосвязь личности потерпевшего с другими элементами ОРХ НДКИ обеспечивает возможность построения комплексной модели преступления, что существенно повышает эффективность оперативно-розыскной деятельности. Установление характеристик потерпевшего, таких как уровень цифровой грамотности, особенности поведения в сети или организационные уязвимости, позволяет не только выявить способ и орудия преступления, но и прогнозировать потенциальные объекты посягательств. Например, анализ цифровых следов, оставленных в результате НДКИ, таких как IP-адреса или журналы доступа, в сочетании с информацией о поведении потерпевшего, может указать на круг подозреваемых или используемые злоумышленниками технические средства.

Таким образом, личность потерпевшего как элемент ОРХ НДКИ является системообразующим фактором, обеспечивающим целостность информационной модели преступления и определяющим эффективность оперативно-розыскной деятельности. Анализ социально-психологических, профессиональных и поведенческих характеристик потерпевших, включая уровень цифровой грамотности и особенности поведения

в цифровой среде, позволяет прогнозировать способы и орудия совершения НДКИ, выявлять потенциальные объекты посягательств и оптимизировать тактические приемы раскрытия указанного преступления. Установление причинно-следственных связей между личностью потерпевшего и другими элементами ОРХ способствует не только раскрытию совершенных преступлений, но и разработке профилактических мер, направленных на повышение информационной безопасности. Дальнейшие исследования должны сосредоточиться на углублении анализа факторов уязвимости потерпевших и разработке методических рекомендаций по предотвращению НДКИ, что позволит минимизировать угрозы информационной безопасности и обеспечить устойчивость цифровой среды.

УДК 343.97

Е.П. Шляхтин

ПРОБЛЕМНЫЕ АСПЕКТЫ ВЗАИМОДЕЙСТВИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ И ОБЩЕСТВЕННЫХ ОБЪЕДИНЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ НЕГАТИВНОМУ ВЛИЯНИЮ УГОЛОВНО-ПРЕСТУПНОЙ СРЕДЫ НА ПОДРАСТАЮЩЕЕ ПОКОЛЕНИЕ

Российская Федерация и Республика Беларусь в последнее время активизировали совместную деятельность по противодействию внешним и внутренним угрозам, к числу которых мы относим и противодействие преступности. Собственный опыт служения народу, обществу и государству в рядах милиции, а теперь и полиции показывает, что в противодействии негативному влиянию уголовно-преступной среды на морально-нравственные устои гражданского общества и подрастающее молодое поколение мелочей не бывает. Следует отметить, что система противодействия преступности со стороны органов внутренних дел состоит из трех взаимосвязанных элементов. Во-первых, это предупреждение причин и условий существования уголовно-преступной среды и, одновременно, индивидуальная профилактика в отношении лиц с криминальными наклонностями. Во-вторых, это непосредственная борьба с преступностью в целом и ее отдельными видами в частности. В-третьих, это минимизация и (или) ликвидация последствий негативных проявлений уголовно-преступной среды. Соответственно, если в полной мере, своевременно и эффективно реализуется первый элемент противодействия (предупреждение и профилактика), то необходимость во втором и третьем элементах противодействия преступности отпадает, что позволяет также экономить значительные человеческие и материальные ресурсы.

Все три задачи, которые выполняют во время повседневной оперативно-служебной и иной деятельности оперативные и иные подразделения органов внутренних дел, классифицируются на главные, специальные и обеспечивающие. Соответственно, главные задачи связаны с предназначением и компетенцией того или иного подразделения органов внутренних дел; специальные задачи определяются складывающейся криминальной обстановкой на территории оперативного обслуживания, линии работы или на объекте, а также установками и директивными указаниями Министерства внутренних дел Российской Федерации. К числу обеспечивающих задач относятся обучение и переподготовка полицейских, информирование населения о появляющихся новых вызовах со стороны уголовно-преступной среды и др.

В частности, к проблемному аспекту противодействия общеуголовной и иной преступности следует отнести раскрытие организации и отдельных моментов тактических действий оперативных подразделений полиции, формирование негативного образа полицейского, а также одновременно представление в приукрашенном виде представителей криминалитета в средствах массовой информации, художественной литературе и кинофильмах.

Согласно Указу Президента Российской Федерации от 23 мая 2011 г. № 668 «Об общественных советах при Министерстве внутренних дел Российской Федерации и его территориальных органах» в целях обеспечения согласования общественно значимых интересов граждан Российской Федерации, федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, общественных объединений, правозащитных, религиозных и иных организаций, в том числе профессиональных объединений предпринимателей, и решения наиболее важных вопросов деятельности органов внутренних дел при Министерстве внутренних дел Российской Федерации и его территориальных органах образуются общественные советы. Одной из их основных задач является привлечение граждан, общественных объединений и организаций к реализации государственной политики в сфере охраны общественного порядка, профилактики правонарушений, обеспечения общественной безопасности, а также содействие реализации государственной политики в сфере противодействия преступности.

На наш взгляд, требуется внести определенные коррективы в деятельность общественных советов при органах внутренних дел, направленные на активизацию взаимодействия с «миром искусства». Суть проблемы состоит в том, что современное телевидение и киноиндустрия выработали определенные стандарты для привлечения внимания насе-

ления к своей продукции, которые основываются на воспевании культа отдельной личности, культивировании низменных потребностей, правового нигилизма и вседозволенности.

В качестве примера можно привести тот факт, что экстремистской организацией в Российской Федерации признано такое проявление уголовно-преступной среды, как неформальное общественное объединение «Арестантский уклад един». Его лидеры, используя ореол таинственности, блатной романтики, кастовости, предпринимали активные действия по привлечению в свои ряды детей и подростков и привитию им норм и правил поведения, принятых в уголовно-преступной среде. Российское государство приняло меры и через судебные органы запретило его деятельность.

В то же время в сети Интернет активно осуществлялся прокат сериала «Слово пацана». Сейчас поступила информация, что хотят снять фильм о действовавшей на территории г. Казани молодежной организованной преступной группировке «Тяп-Ляп», многие участники которой впоследствии были осуждены за бандитизм, убийства и другие особо тяжкие преступления.

Данные факты свидетельствуют, что существует диссонанс между государственной политикой, направленной на морально-нравственное и патриотическое воспитание молодых людей, и реальными действиями отдельных людей от «мира искусства», которые, решая сиюминутные вопросы получения прибыли, не предвидят долговременных последствий. Молодежь склонна к подражанию и нигилизму, не всегда правильно и в полной мере анализирует тот информационный контент, который ей преподносится, особенно в сети Интернет.

Оставляя вне данной статьи качественную оценку художественной и искусствоведческой ценности вышеуказанных материалов, полагаем необходимым отметить, что подобные «кино и видеошедевры» оказывают огромное негативное влияние на подрастающее поколение, да и на все морально-нравственные устои российского населения в целом. Когда постоянно с экрана телевизора граждане, и прежде всего дети и подростки, видят фильмы, в которых «герой-одиночка» легко и непринужденно справляется с преступниками, а образ милиционера представлен «пьяницей, коррупционером, бездельником и т. п.», который никоим образом не старается защитить простого человека и гражданина от уголовного произвола. Соответственно у населения формируется негативный образ сотрудника органов внутренних дел, которого следует бояться и не помогать ему в борьбе с преступностью.

Полагаем необходимым отметить, что таких сериалов, авторы которых пытаются как бы раскрыть исторические события на криминальную тематику, показать организацию и тактику деятельности отдельных подразделений органов внутренних дел, с каждым годом становится все больше и больше. Вероятно, их создатели, пытаясь заработать свои «тридцать сребреников», забывают о том, что есть молодежь, которая не имеет собственного жизненного опыта, склонна к подражанию, что именно представители этой молодежи через пару десятков лет будут формировать облик нашего государства и направления его позитивного развития.

В 70-80-е гг. XX в. советские органы внутренних дел активно привлекали «людей искусства» к взаимодействию, направленному на противодействие преступности, и воспитанию милиционеров. Данное время характеризуется созданием художественных произведений и кинофильмов, в которых правдиво показаны суровые будни милиционеров, развенчивалась блатная романтика. Тем самым у населения и молодежи формировались соответствующие морально-нравственные установки, в том числе связанные с оказанием помощи органам внутренних дел по предупреждению и борьбе с преступностью. В качестве примера необходимо привести функционирование «Юных отрядов инспекторов дорожного движения», добровольных народных дружин, оперативных комсомольских отрядов дружинников и др.

С учетом изложенного полагаем необходимым в современных условиях использовать вышеуказанный исторический опыт. Для чего общественным советам при органах внутренних дел следует активно взаимодействовать с институтами гражданского общества, гражданами и организациями, создающими художественные произведения и фильмы. В частности, предлагается разработать алгоритм взаимодействия, чтобы в составе вышеуказанного творческого коллектива по предложению общественного совета при Министерстве внутренних дел Российской Федерации в качестве консультанта при создании кинофильма на криминальную тематику или о работе органов внутренних дел обязательно привлекался компетентный руководитель или ветеран органов внутренних дел. Это позволит не только правильно расставить акценты, показывая повседневную работу отдельных подразделений органов внутренних дел и их сотрудников, не раскрыть организационные и тактические аспекты их деятельности (т. е. не нарушить принцип конспирации), но также показать негативное влияние уголовно-преступной среды на население и, что особенно важно, на подрастающее поколение молодежи. Участие консультанта будет способствовать тому, чтобы не было показано карикатурное изображение полицейских, часто с нарушением правил ношения форменного обмундирования, знаков различий и т. п.

Кроме того, с помощью консультанта можно показать всю сложность и ответственность службы сотрудников органов внутренних дел на страже закона, во благо простого человека и защиты граждан наших государств от преступных посягательств. Ведь сейчас у многих граждан, да и определенных руководителей государственных органов, общественных объединений складывается впечатление, что с момента совершения любого преступления до его раскрытия и направления материалов в суд проходит время, равное одной или двум «коротким киносериям».

Завершая публикацию, полагаем необходимым отметить важность и актуальность каждой научно-практической конференции, организованной Академией Министерства внутренних дел Республики Беларусь. Участие в ней и возможность обменяться мнениями по многим аспектам противодействия преступности позволяют получить новые знания, увидеть новые перспективы не только в непосредственном противодействии преступности, но и в подготовке молодых специалистов для органов внутренних дел.

УДК 363.985.8

А.А. Шульченко

АНАЛИЗ ВЗГЛЯДОВ НА ПРОБЛЕМУ ДЕЗИНФОРМАЦИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Эффективное использование дезинформации в оперативно-розыскной деятельности (ОРД) выступает инструментом, позволяющим воздействовать на объекты оперативного интереса и достигать целей в условиях дефицита информации, включая скрытые угрозы. Ее успешное применение требует понимания сущности дезинформации, умения распознавать ее и создавать условия для ее формирования и распространения. Подход, основанный на тактической выверенности и учете оперативной обстановки, делает дезинформацию действенным механизмом в предупреждении, выявлении и пресечении преступной деятельности.

Термин «дезинформация» восходит к латинскому dis- и informatio, обозначая введение в заблуждение посредством ложных сведений. В современном виде он активизировался в XX в., особенно в военной и разведывательной сферах. Исторически дезинформация применялась для сокрытия данных, дезориентации противника и деморализации. Военные стратеги древности утверждали: «Война – это путь обмана».

Со временем дезинформация распространилась и на оперативно-розыскную сферу. В ОРД она используется для выявления преступлений,

розыска лиц, обеспечения безопасности конфиденциальных помощников. Военный опыт дезинформации адаптирован правоохранительными органами, включая ее в оперативные комбинации и нейтрализацию угроз. Дезинформация как инструмент работы опирается на психологические механизмы, связанные с доверием, восприятием и когнитивными искажениями. В юридической и оперативно-розыскной психологии обман изучается как метод управляемого воздействия на сознание. Следовательно, дезинформация в ОРД – не просто ложь, а сложный психотехнический прием.

В научных исследованиях дезинформация изучается с разных сторон: от роли в ОРД до применения в профилактике. Р.С. Белкин акцентирует внимание на допустимости обмана, его этических границах и последствиях. Он считает обман оправданным в условиях, когда он служит меньшему злу и способствует раскрытию.

Д.Н. Лахтиков анализирует дезинформацию в контексте оперативно-розыскной профилактики, но ограничивается тактическим уровнем, не раскрывая ее системного места в ОРД.

Е.С. Дубоносов рассматривает дезинформацию как элемент организационно-тактических действий, вводящий подозреваемых в заблуждение. Анализирует механизмы социальных взаимодействий, классифицирует дезинформацию по каналам распространения: средства массовой информации, неформальные коммуникации, конфиденциальные источники. Он исследует также слухи как элемент неформальной коммуникации, подчеркивая их двойственную природу – как носителей информации и инструментов дезинформации. Ученый указывает, что слухи могут быть индикатором оперативной обстановки, но требуют критического анализа.

Д.С. Амелина сосредотачивается на распознавании ложной информации от конфиденциальных помощников. Она делит дезинформацию на заведомо ложную и случайно искаженную, подчеркивая необходимость верификации даже достоверных источников.

П.П. Елисов рассматривает применение дезинформации и инсценировок при выявлении коррупции, акцентируя внимание на рисках провокаций и правовых коллизиях. Он указывает на необходимость правовой регламентации, чтобы соблюсти баланс между эффективностью и законностью.

А.Г. Белый разграничивает обман (воздействие на отдельного человека) и дезинформацию (массовое распространение ложных сведений). Он выделяет способы дезинформирования: личное общение, средства массовой информации, интернет, инсценировки. Однако недостаточно раскрыты правовые риски и возможность злоупотреблений.

А.Ю. Румянцев рассматривает дезинформацию как тактико-криминалистический прием, направленный на создание ложных представлений у преступников. Он отмечает, что, несмотря на эффективность метода, его допустимость вызывает споры, особенно в контексте морали и права.

В.Б. Батоев анализирует технологию Deepfake как средство дезинформации. Он указывает на ее возможности в дезориентации преступной среды и создании инсценировок. Автор акцентирует на необходимости правового регулирования, чтобы минимизировать риски. Однако рассматривать дипфейки только как инструмент дезинформации – ограниченно.

В действительности информационно-коммуникационные технологии (ИКТ) включают в себя генеративные нейросети, аудиоманипуляции, спуфинг, бот-сети, психологическое таргетирование, цифровые личности. Широкий подход позволяет выстроить систему оценки их ценности и рисков. Научный анализ подтверждает значимость дезинформации в ОРД. Однако отсутствие единого подхода к ее сущности, видам, методам применения осложняет практическое использование. Некоторые авторы не выделяют ее как самостоятельный инструмент, что ограничивает понимание ее потенциала. Отсутствие единых критериев правомерности, риски злоупотреблений, соотношение с инсценировкой и другими категориями требуют дальнейшего изучения.

Противодействие дезинформации преступных элементов остается проблемным. Вопросы выявления ложных сведений, проверки информации, ролевого поведения сотрудников и взаимодействия с помощниками требуют разработки. Необходима адаптация методик применения дезинформации с учетом ИКТ, поскольку преступники также используют цифровые инструменты дезинформации. Совершенствование тактики, ролевых моделей поведения сотрудников и систематизация подходов позволят повысить эффективность применения дезинформации в ОРД.

УДК 377 (07)

Д.С. Якжик

ОТ КИБЕРБЕЗОПАСНОСТИ ДО ДАКТИЛОСКОПИИ: КАК ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРЕОБРАЖАЕТ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

Современная оперативно-розыскная деятельность (ОРД) переживает трансформацию благодаря стремительному развитию технологий искусственного интеллекта (ИИ). Этот инструмент открывает новые

возможности для анализа данных, прогнозирования преступлений и автоматизации рутинных задач, существенно обогащая традиционные подходы. ИИ кардинально преображает криминалистическое обеспечение ОРД, расширяя ее потенциал в решении сложных задач.

Цифровая криминалистика занимается исследованием данных, извлеченных из электронных устройств – компьютеров, смартфонов, серверов, облачных хранилищ и разнообразных умных гаджетов. В условиях цифровизации общества преступления все чаще оставляют цифровой след, будь то переписка в мессенджерах, история браузера или транзакции в криптовалюте. ИИ играет центральную роль в обработке этих данных, позволяя сотрудникам правоохранительных органов справляться с их объемом и сложностью.

Одним из ключевых применений ИИ в цифровой криминалистике является восстановление и анализ удаленной или зашифрованной информации. Алгоритмы машинного обучения способны реконструировать фрагментированные файлы, такие как изображения или документы, даже если они были частично стерты. Например, системы на основе нейронных сетей используются для восстановления данных с поврежденных жестких дисков, что может стать решающим доказательством в расследовании. Кроме того, ИИ помогает классифицировать содержимое – например, автоматически выявлять изображения или видео с запрещенным контентом, что значительно сокращает время, необходимое для анализа.

В сфере противодействия киберпреступности ИИ применяется для обнаружения мошенничества и анализа вредоносного программного обеспечения. Алгоритмы выявления аномального поведения отслеживают необычные паттерны в сетевом трафике, банковских операциях или действиях пользователей. Например, системы предотвращения фишинга используют обработку естественного языка для анализа текстов писем и выявления подозрительных фраз или ссылок. В случае с криптовалютными преступлениями, такими как отмывание денег, графовые нейронные сети, помогают отслеживать цепочки транзакций в блокчейнах, идентифицируя участников даже при использовании анонимизирующих технологий.

Еще одним важным аспектом является анализ вредоносного программного обеспечения. ИИ позволяет не только обнаруживать известные угрозы, но и прогнозировать поведение новых вирусов, анализируя их код и паттерны распространения. Системы на основе глубокого обучения в сочетании со сверточными нейронными сетями классифицируют исполняемые файлы как вредоносные или безопасные с точностью, превышающей традиционные сигнатурные методы. Это особенно акту-

ально в условиях роста числа атак с использованием уязвимостей нулевого дня, где скорость реакции критична.

Обнаружение мошенничества с помощью ИИ выходит за рамки киберпространства и включает в себя финансовые преступления в реальном мире. Банки и страховые компании используют алгоритмы кластеризации и классификации для выявления подозрительных транзакций или заявлений на выплаты. Например, системы на основе градиентного бустинга анализируют исторические данные о клиентах, выявляя аномалии, такие как необычно крупные переводы или несоответствия в поведении. Это помогает связывать финансовые преступления с конкретными лицами или организованными преступными группами.

Примером практического применения является работа антифрод систем с данными о кредитных картах. ИИ может сопоставлять транзакции с геолокацией, временными метками и покупательскими привычками, чтобы определить, был ли платеж совершен законным владельцем карты или мошенником. Такие системы уже доказали свою эффективность в сокращении числа ложных срабатываний и ускорении расследований.

Не менее значимые изменения происходят в традиционных областях криминалистики, например, в дактилоскопии. Не одно столетие отпечатки пальцев используются в качестве уникального идентификатора, но их использование ограничивается сопоставлением образцов отпечатков одного и того же пальца. Опубликованные в январе 2024 г. в журнале Science Advances результаты исследования Гейба Гуо меняют этот подход, демонстрируя, как ИИ может раскрыть новые аспекты анализа отпечатков.

Исследовательская группа применила парные глубокие нейронные сети для анализа отпечатков пальцев, извлекая векторные представления центрального узора, которые позволили выявить сходство между отпечатками разных пальцев одного человека. С вероятностью более 99,99 % исследователи показали, что такие отпечатки обладают значительными общими чертами, независимо от сочетания пальцев (например, указательный правой руки и мизинец левой). Это открытие опровергает традиционное предположение о полной уникальности каждого отпечатка и открывает новые возможности для криминалистики.

Ключевая находка исследования заключается в том, что сходство определяется преимущественно ориентацией гребней, особенно в центральной части отпечатка, а не минуциями, роль которых доминирует в классической дактилоскопии.

Это открытие может иметь прямое применение в ОРД. Например, если на двух местах преступления обнаружены отпечатки разных пальцев, традиционные методы не смогли бы установить их связь с одним

человеком без полного набора отпечатков подозреваемого. Метод Гуо позволяет сократить список подозреваемых с тысячи до нескольких десятков, повышая эффективность расследований почти на два порядка. Это особенно важно для дел, по которым подозреваемый не установлен, где доступны лишь фрагментарные улики.

Кроме того, технология может быть интегрирована в системы автоматизированной идентификации отпечатков, улучшая их способность фильтровать ложные совпадения.

Несмотря на потенциал, метод имеет ограничения. Его производительность уступает системам для сопоставления одного следа пальца руки, а обучение проводилось на высококачественных отпечатках, что не всегда соответствует реальным условиям. Г. Гуо отмечает необходимость тестирования на больших базах данных и адаптации к частичным или низкокачественным образцам.

ИИ меняет ОРД, объединяя цифровую и традиционную сферы. В цифровой сфере он ускоряет анализ данных, выявляет киберпреступления и предотвращает мошенничество, тогда как в традиционной сфере открывает новые горизонты идентификации. Эти достижения подчеркивают потенциал ИИ как инструмента, способного не только решать текущие задачи, но и «переосмысливать» фундаментальные принципы криминалистики.

УДК 343.985

В.В. Якубук

ВЫНЕСЕНИЕ РЕШЕНИЯ ОБ ОТКАЗЕ В ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА И ДРУГИХ ПРЕСЕКАТЕЛЬНЫХ РЕШЕНИЙ КАК ОСНОВАНИЕ ОЗНАКОМЛЕНИЯ СО СВЕДЕНИЯМИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Проблематика правовых последствий вынесения решений об отказе в возбуждении уголовного дела на стадии возбуждения уголовного дела исследовалась многими правоведами и получила определенное освещение в научной литературе. Так, белорусские правоведы С.И. Бординович, И.А. Шаматульский, Д.В. Ковалевич, С.Ю. Мельников и некоторые другие рассматривали в своих работах вопросы реализации права на ознакомление со сведениями оперативно-розыскной деятельности в связи с вынесением указанного процессуального решения. Однако пра-

вовые последствия вынесения этого решения, в том числе возможность возникновения такого права, на следующей стадии уголовного процесса – стадии предварительного расследования – в научных источниках не получили должного осмысления.

Так, указанные постановления в ходе расследования уголовных дел могут выноситься при наличии соответствующих оснований как по расследуемому факту преступного деяния (в частности, в отношении давшего взятку лица при расследовании получения взятки), так и по другим выявляемым отдельным самостоятельным деяниям, по которым не вынесены иные процессуальные решения (например, устанавливаемым фактам причастности к обороту определенного имущества). В указанных случаях в силу правовой неопределенности с целью дачи соответствующей правовой оценки правоприменителями используется институт аналогии закона и применяются правовые нормы, регламентирующие порядок вынесения решения об отказе в возбуждении уголовного дела на соответствующей стадии уголовного процесса. В связи с отсутствием соответствующей детальной правовой регламентации правоприменительной практикой выработан указанный механизм вынесения такого процессуального решения о наличии обстоятельств, исключающих ведение уголовного судопроизводства. Принятие указанных постановлений производится как в настоящее время, так и, согласно работе М.С. Шалумова, производилось в советский период.

На основании абзаца пятого части второй ст. 10 Закона Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» (далее – Закон) граждане имеют право на ознакомление со сведениями, их касающимися, полученными при проведении оперативно-розыскных мероприятий, в случае отказа в возбуждении уголовного дела в их отношении. Законодательство, как Уголовно-процессуальный кодекс Республики Беларусь (далее – УПК), так и Закон, не содержит запрета реализации рассматриваемого права в случаях вынесения указанного процессуального решения на стадии предварительного расследования.

По нашему мнению, выработанный правоприменительной практикой в условиях правовой неопределенности механизм дачи правовой оценки также следует рассматривать в контексте возникающих непосредственно в связи с этим уголовным процессом правоотношений. В связи с наличием реабилитирующих обстоятельств данная органами уголовного преследования оценка деяний определенного лица влечет необходимость принятия соответствующих мер по восстановлению его нарушенных прав и законных интересов. Право граждан ознакомиться с полученными о них сведениями в связи с осуществлением оперативно-розыскной деятельности выступает одной из таких восстановительных мер. Положения ст. 11, части второй ст. 34 Конституции Республики Беларусь обязывают государственные органы и должностных лиц осуществить предоставление гражданам возможности ознакомления с материалами в случаях вмешательства в их законные интересы и права.

Таким образом, единая процессуальная природа решений приводит, по нашему мнению, к выводу о возможности предоставления права ознакомления со сведениями, полученными в связи с осуществлением оперативно-розыскных мероприятий, при вынесении решения об отказе в возбуждении уголовного дела как на стадии возбуждения уголовного дела, так и на стадии предварительного расследования.

Вместе с тем одновременно возникает вопрос о возможности такого ознакомления в период расследования уголовного дела до окончания по нему производства. Этот же вопрос необходимо рассмотреть и при соответствующем прекращении уголовного преследования. УПК не регламентирует порядок ознакомления с расследуемым уголовным делом до окончания его предварительного расследования. Ст. 198 УПК определяет невозможность разглашения данных предварительного расследования в случаях несоответствия такого разглашения интересам расследования. Ознакомление со сведениями, полученными в ходе оперативно-розыскной деятельности, может предоставить возможность повлиять (напрямую или опосредованно) на ход предварительного расследования, оказать воздействие на участников уголовного процесса или сделать невозможным дальнейшее собирание необходимых доказательств. В связи с изложенным, по нашему мнению, реализация права на ознакомление с такими сведениями возможна только по окончанию в установленном порядке уголовного судопроизводства.

Кроме того, в связи с настоящим исследованием следует рассмотреть и предусмотренное при производстве по уголовным делам частного обвинения вынесение судьей постановления об отказе в принятии заявления о таком преступлении (при установлении обстоятельств, исключающих производство по уголовному делу, в частности реабилитирующего характера). В случае осуществления ранее процессуальной деятельности, в том числе «доследственной» проверки с принятием решения об ее прекращении с разъяснением заявителю права на возбуждение такого уголовного дела в суде, в отношении определенного лица возможно проведение оперативно-розыскных мероприятий. При этом в связи с упомянутыми положениями Конституции Республики Беларусь в таком случае также необходимо рассмотрение возможности предоставления этому лицу права ознакомления со сведениями, полученными

при проведении оперативно-розыскных мероприятий. Однако вынесение органом уголовного преследования решения о таком прекращении «доследственной» проверки или судьей постановления об отказе в принятии заявления по делам частного обвинения, в том числе при наличии реабилитирующих оснований, не указаны в ст. 10 Закона. На основании ст. 178[1] УПК лицо, в отношении которого принято решение о таком прекращении проверки, вправе ознакомиться с ее материалами, в том числе с возможно имеющимися в них сведениями о проведении в его отношении оперативно-розыскных мероприятий. Нормы Конституции Республики Беларусь имеют прямое действие, при этом в Законе указанные случаи не определены, в связи с чем, по нашему мнению, необходимо дальнейшее рассмотрение научным сообществом вопросов возможной регламентации рассматриваемого права граждан при указанных правовых обстоятельствах.

На основании вышеизложенного можно прийти к выводу о вариативности правовых обстоятельств вынесения решений в отношении определенных лиц об отказе в возбуждении уголовного дела, являющихся правовым основанием возникновения права именно этих граждан на ознакомление со сведениями, их касающимися, полученными в связи с осуществлением оперативно-розыскной деятельности. При этом, по нашему мнению, реализация права на ознакомление с такими сведениями возможна только по окончанию судопроизводства как на стадии возбуждения уголовного дела, так и на стадии предварительного расследования. Кроме того, необходимо дальнейшее научное осмысление вопроса регламентации рассматриваемого права граждан в случаях вынесения постановлений: органом уголовного преследования – о прекращении «доследственной» проверки с разъяснением заявителю права на возбуждение уголовного дела частного обвинения в суде; судьей – об отказе в принятии заявления о таком преступлении. Результаты настоящего исследования могут быть использованы в качестве основы для дальнейших исследований, в процессе совершенствования законодательства и непосредственно в правоприменительной практике.

СВЕДЕНИЯ ОБ АВТОРАХ

АНАНЯН Давид Гагикович – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

АНИШКЕВИЧ Игорь Олегович – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

АНЯНОВА Екатерина Сергеевна – юрисконсульт ООО «Балторг», г. Калининград, Российская Федерация.

АФАНАСЕНКО Алексей Викторович – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

БАСОВА Алина Игоревна – курсант Калининградского филиала Санкт-Петербургского университета МВД России.

БАТЮКОВ Александр Валерьевич – оперуполномоченный отдела уголовного розыска криминальной милиции управления внутренних дел администрации Московского района г. Минска.

БАШАН Алексей Владимирович – первый заместитель начальника Академии МВД Республики Беларусь, кандидат юридических наук, профессор.

БЕРЕЗКО Анастасия Алексеевна – преподаватель кафедры конституционного и административного права Академии управления при Президенте Республики Беларусь.

БОРОВИК Петр Леонидович – доцент кафедры информационного права факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

БОРОДИЧ Алексей Иванович – профессор кафедры конституционного и международного права Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ВАНАГЕЛЬ Сергей Геннадьевич – начальник отдела пятого управления (по г. Минску) ГУБОПиК МВД Республики Беларусь.

ВЕРЕМЕЕНКО Виталий Михайлович – доцент кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ВОРОДЮХИН Станислав Евгеньевич – доцент кафедры государственно-правовых дисциплин Белгородского юридического института МВД России им. И.Д. Путилина, кандидат юридических наук.

ВОРОНЦОВА Юлия Александровна – доцент кафедры гуманитарных и социально-экономических дисциплин Белгородского юридического института МВД России им. И.Д. Путилина, кандидат юридических наук, доцент.

ГЛУБОКОВСКИХ Роман Владимирович – преподаватель кафедры оперативно-розыскной деятельности Калининградского филиала Санкт-Петербургского университета МВД России.

ГРИБ Денис Вячеславович – старший преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук.

ГРИНЬ Павел Сергеевич – курсант Академии МВД Республики Беларусь.

ГУЛЮК Артём Александрович – старший оперуполномоченный по особо важным делам управления по противодействию киберпреступности криминаль-

ной милиции управления внутренних дел Брестского областного исполнительного комитета.

ГУЩИНА Виктория Дмитриевна – курсант Калининградского филиала Санкт-Петербургского университета МВД России.

ДЗЫРУК Михаил Сергеевич – старший преподаватель кафедры организации режима, охраны и конвоирования Воронежского института ФСИН России.

ДОРОЖИНСКАЯ Кристина Валерьевна – курсант Белгородского юридического института МВД России им. И.Д. Путилина, кандидат юридических наук, доцент.

ЕРОФЕЕВ Кирилл Алексеевич – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

ЕСЬКО Александр Владимирович – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

ЕСЮТИНА Екатерина Олеговна – слушатель Калининградского филиала Санкт-Петербургского университета МВД России.

ЕФИМОВИЧ Владислав Владимирович – старший преподаватель кафедры экономической безопасности Академии МВД Республики Беларусь.

ИВУШКИНА Ольга Викторовна – начальник кафедры уголовного права и криминологии, профессор кафедры уголовного процесса Восточно-Сибирского института МВД России, кандидат юридических наук, доцент.

КАЗАКЕВИЧ Геннадий Аркадьевич – заместитель Министра внутренних Республики Беларусь – начальник криминальной милиции.

КАЙБЕЛЕВ Павел Андреевич – старший преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

КОВАЛИК Борис Владимирович – преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

КОЗЛЕНКО Юлий Денисович – студент Академии управления при Президенте Республики Беларусь.

КОЗЛОВ Вадим Алексеевич – курсант Академии МВД Республики Беларусь.

КОМСЮКОВА Наталья Юрьевна – курсант Омской академии МВД России.

КОМСЮКОВА Яна Юрьевна – курсант Омской академии МВД России.

КОПАЧ Кирилл Сергеевич – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

КРАВЕЦ Владислав Владимирович – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

КРАВЦОВА Марина Александровна – доцент кафедры экономической безопасности Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

КРУПЕННИКОВА Кристина Константиновна – слушатель факультета подготовки дознавателей Белгородского юридического института МВД России им. И.Д. Путилина.

КУДРЯВЦЕВ Дмитрий Сергеевич – доцент кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук.

КУРНАВИН Сергей Сергеевич – старший преподаватель кафедры оперативно-розыскной деятельности органов внутренних дел Калининградского филиала Санкт-Петербургского университета МВД России.

ЛИСАУСКАЙТЕ Валентина Владо – профессор кафедры уголовного права и криминологии Восточно-Сибирского института МВД России, кандидат юридических наук, доцент.

ЛОПУХ Денис Викторович – начальник сектора юридического управления Государственного пограничного комитета Республики Беларусь.

ЛЫСЕНКО Виктория Александровна – начальник кафедры государственно-правовых дисциплин Белгородского юридического института МВД России им. И.Д. Путилина, кандидат юридических наук, доцент.

МАРТЫНОВ Артём Олегович – заместитель начальника кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук.

МЕДВЕДЕВА Анастасия Юрьевна – курсант Воронежского института ФСИН России.

МЕЗЯК Вадим Юрьевич – преподаватель кафедры информационного права факультета криминальной милиции Академии МВД Республики Беларусь.

МЕЛЬНИКОВ Сергей Юрьевич – старший преподаватель кафедры оперативно-розыскной деятельности факультета милиции Могилевского института МВД Республики Беларусь.

МЕРКУЛОВА Марина Викторовна – доцент кафедры уголовного права и процесса Московского университета им. С.Ю. Витте, кандидат юридических наук.

МИЛОВ Павел Сергеевич – преподаватель кафедры оперативно-розыскной деятельности органов внутренних дел Омской академии МВД России.

МИНЗЯНОВА Диляра Фарильевна – старший преподаватель кафедры оперативно-разыскной деятельности Казанского юридического института МВД России, кандидат юридических наук.

МУРАТОВА Алина Айнуровна – курсант Калининградского филиала Санкт-Петербургского университета МВД России.

ОЛЕКСЮК Александр Александрович – заместитель начальника УУР УМВД России по Калининградской области.

ПАШКЕВИЧ Диана Александровна – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

ПИКТА Владислав Игоревич – старший преподаватель кафедры информационного права факультета криминальной милиции Академии МВД Республики Беларусь.

ПРИЁМКА Сергей Сергеевич – преподаватель-методист учебно-методического управления Академии МВД Республики Беларусь.

РОДЕВИЧ Андрей Валерьевич – старший преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

САВЧУК Олег Владимирович – старший преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

САЦУК Павел Иванович – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

СИМОНЕНКО Дмитрий Александрович – начальник Барнаульского юридического института МВД России, кандидат юридических наук.

СОРОКО Вероника Сергеевна – студент Академии управления при Президенте Республики Беларусь.

СТЕФАНЕНКО Алексей Петрович – старший преподаватель кафедры экономической безопасности Академии МВД Республики Беларусь.

СУБЦЕЛЬНЫЙ Александр Михайлович – старший преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

ТРАЙНЕЛЬ Алексей Валерьевич – курсант факультета криминальной милиции Академии МВД Республики Беларусь.

ТУКАЛО Алексей Николаевич – начальник кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ФОМИНА Инна Анатольевна – доцент кафедры уголовного права и криминологии, профессор кафедры уголовного процесса Восточно-Сибирского института МВД России, кандидат юридических наук.

ХАРЕВИЧ Дмитрий Людвикович – доцент кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

ХЛЫСТОВА Яна Александровна – слушатель Калининградского филиала Санкт-Петербургского университета МВД России.

ЦЫНКЕВИЧ Владимир Николаевич – преподаватель кафедры оперативно-розыскной деятельности факультета криминальной милиции Академии МВД Республики Беларусь.

ЧЕРНИЦКИЙ Никита Валерьевич – старший оперуполномоченный группы противодействия киберпреступности отдела внутренних дел администрации Мостовского районного исполнительного комитета.

ЧЕХОВИЧ Александр Александрович – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

ШАСТИТКО ДМИТРИЙ ВИТАЛЬЕВИЧ – Академия управления при Президенте Республики Беларусь, старший преподаватель.

ШЛЯХТИН Евгений Павлович – начальник кафедры оперативно-розыскной деятельности Казанского юридического института МВД России.

ШУЛЬЧЕНКО Андрей Александрович – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь.

ЯКЖИК Дмитрий Сергеевич – старший преподаватель кафедры информационного права факультета криминальной милиции Академии МВД Республики Беларусь.

ЯКУБУК Владислав Владимирович – заместитель начальника отдела юридического управления Государственного пограничного комитета Республики Беларусь.

ЯСКЕВИЧ Александр Васильевич – профессор кафедры экономической безопасности Академии МВД Республики Беларусь, кандидат юридических наук, доцент.

СОДЕРЖАНИЕ

Научное издание

АКТУАЛЬНЫЕ ВОПРОСЫ ТЕОРИИ И ПРАКТИКИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Республиканская научно-практическая
заочная конференция
(с международным участием)
(Минск, 2 июня 2025 г.)

Тезисы докладов

Технический редактор *Ю.С. Санина*
Корректор *М.С. Прушак*

Подписано в печать 28.05.2025. Формат 60×84 $^{1}/_{16}$.
Бумага офсетная. Ризография. Усл. печ. л. 10,93. Уч.-изд. л. 10,67.
Тираж 40 экз. Заказ 76.

Издатель и полиграфическое исполнение:
учреждение образования
«Академия Министерства внутренних дел Республики Беларусь».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий № 1/102 от 02.12.2013.
Пр-т Машерова, 6А, 220005, Минск.

А43 **Актуальные вопросы теории и практики оперативно-розыскной деятельности** : тез. докл. респ. науч.-практ. заоч. конф. (с междунар. участием) (Минск, 2 июня 2025 г.) / Акад. М-ва внутр. дел Респ. Беларусь ; редкол.: А.Н. Тукало (отв. ред.) [и др.]. – Минск : Академия МВД, 2025. – 186, [1] с.

ISBN 978-985-576-482-4.

Рассматриваются проблемы теории и практики оперативно-розыскной деятельности, актуальные вопросы проведения оперативно-розыскных мероприятий и совершенствования законодательства, регламентирующего осуществление оперативно-розыскной деятельности; отдельные аспекты выявления (раскрытия) преступлений. Анализируются тенденции использования передовых форм и методов, информационных технологий в деятельности уполномоченных государственных органов по борьбе с преступностью.

Научное издание предназначено для научных сотрудников, преподавателей, аспирантов, адъюнктов, лиц, обучающихся в высших учебных заведениях юридического профиля, практических работников правоохранительных органов.

УДК 343.985.8
ББК 67.408