

Краснодарский университет МВД России

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
XIII Всероссийской научно-практической конференции
(17 октября 2024 г.)

Краснодар
2025

УДК 343
ББК 67.408
А437

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Редакционная коллегия:

А. А. Сафронов, кандидат юридических наук, доцент (председатель);
А. Н. Горбунов, кандидат юридических наук (заместитель председателя);
М. Ю. Савченко (ответственный секретарь);
Н. С. Железняк, доктор юридических наук, профессор;
В. И. Еремченко, кандидат юридических наук, доцент;
Р. Н. Кучмезов, кандидат юридических наук

Актуальные проблемы теории и практики оперативно-розыскной деятельности [Электронный ресурс] : материалы XIII Всерос. науч.-практ. конф., 17 окт. 2024 г. / редкол.: А. А. Сафронов, А. Н. Горбунов, М. Ю. Савченко и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2025. – 1 электрон. опт. диск.

ISBN 978-5-9266-2168-3

Представлены доклады и тезисы выступлений участников XIII Всероссийской научно-практической конференции «Актуальные проблемы теории и практики оперативно-розыскной деятельности», состоявшейся в Краснодарском университете МВД России 17 октября 2024 г.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 343
ББК 67.408

ISBN 978-5-9266-2168-3

© Краснодарский университет
МВД России, 2025

СОДЕРЖАНИЕ

Баженов В.А., Агаев Э.Н. Особенности осуществления розыска и идентификация лиц.....	6
Баженов В.А., Скитская В.А. Инновации в предупреждении и раскрытии преступлений, совершаемых с использованием искусственного интеллекта.....	12
Батоев В.Б. К вопросу о противодействии мошенничеству, совершаемому с использованием синтетических медиа.....	16
Васильев Э.А., Мороз Р.Н. Актуальные проблемы борьбы с преступлениями коррупционной направленности в сфере государственных закупок.....	21
Введенская О.Ю. Актуальные направления использования информационно-телекоммуникационных технологий для получения первоначальной информации о незаконном сбыте наркотических средств.....	26
Вытовтов А.Е. Оперативные подразделения органов внутренних дел по борьбе с преступлениями в сфере экономической деятельности как незаинтересованный субъект предупреждения таких преступлений.....	34
Глубоковских Р.В., Денищик А.Ю. Перспективные направления отождествления личности в розыскной работе подразделений уголовного розыска.....	39
Гора Е.В., Маркарова А.М. Медицинские картели как наиболее опасная форма организованной коррупционной преступности.....	44
Гора Е.В., Мотрук К.К. Провайдеры услуг виртуальных активов и их польза для оперативно-розыскной деятельности.....	51
Горбунов А.Н. Значение оперативно-розыскной деятельности в противодействии незаконному обороту оружия.....	55
Горбунов А.Н., Широков А.В. Организация оперативно-розыскной деятельности, направленной на выявление жаргонов, используемых преступными группами	59
Горковенко И.А. Отдельные аспекты противодействия преступности несовершеннолетних оперативно-розыскными мерами.....	63
Данильян Э.С. Проблемы расследования нераскрытых преступлений в форме дознания.....	67
Железняк Н.С. К вопросу о необходимости корректировки пункта 8 части 2 и части 3 статьи 7 Федерального закона «Об оперативно-розыскной деятельности».....	70

Зоз В.А., Бардин О.А. Особенности применения инструментов и методик OSINT в целях выявления лиц, совершающих преступления в сети Интернет.....	74
Зоз В.А., Фетисов А.Н. Особенности раскрытия преступлений, связанных с незаконным оборотом драгоценных металлов.....	77
Зюзина А.В. Геополитический экстремизм как угроза национальной безопасности.....	81
Зюзина А.В., Жуков М.А. Особенности осуществления оперативно-розыскной деятельности по противодействию экстремизму и терроризму с помощью информационных технологий.....	88
Иванов С.И., Никандрова Д.А. Оперативно-розыскная операция и ее место в системе оперативно-розыскной деятельности.....	94
Лагуточкин А.В., Бурмистров В.А. Актуальные проблемы предупреждения преступлений, связанных с незаконным оборотом наркотических средств с использованием сети Интернет.....	97
Легостаев В.П. Проблемы правоприменения части 4 статьи 18 Федерального закона «Об оперативно-розыскной деятельности» и пути их решения.....	101
Редкоус В.М. Об усилении гарантий защиты прав и свобод личности в оперативно-розыскной и следственной деятельности (опыт Республики Узбекистан).....	105
Савченко М.Ю., Коваленко А.А. Инфоцыганство как деликт в уголовном законодательстве и использование оперативно-розыскной деятельности для его пресечения.....	110
Савченко М.Ю., Самойленко О.А. Особенности раскрытия и расследования преступлений, совершаемых на территории проведения специальной военной операции.....	115
Сафронов А.А. О некоторых вопросах использования результатов оперативно-розыскной деятельности в уголовном судопроизводстве.....	119
Сафронов А.А., Доттуев Э.Ю. Особенности проведения проверочной закупки сотрудниками оперативных подразделений МВД России.....	124
Старостенко О.А., Биттиров А.А. Особенности оперативно-розыскного противодействия киберпреступлениям....	128
Старостенко О.А., Скрипка С.А. Некоторые особенности оперативно-розыскного противодействия идеологии экстремизма...	132
Студнев А.С., Жугова Д.Э. Результаты оперативно-розыскной деятельности как средство доказывания по уголовным делам.....	137

Студнев А.С., Мазурова М.А. Современные технологии в оперативно-розыскной деятельности.....	140
Стукалов В.В. Особенности раскрытия мошенничества, совершенного с использованием средств мобильной связи.....	144
Стукалов В.В., Храмченков И.А. Проблемы выявления и раскрытия убийств по найму.....	149
Ховавко С.М. Поощрительная норма статьи 205 УК РФ как средство предотвращения террористических актов.....	154
Ховавко С.М., Сорокина А.А. Причины и условия преступлений против половой неприкосновенности и половой свободы личности.....	158
Шатилов А.В. О некоторых проблемах, возникающих у сотрудников оперативных подразделений, связанных с установлением местонахождения и доставлением лица, не обладающего статусом подозреваемого или обвиняемого, в регион ведения предварительного расследования.....	163
Южанинов В.С., Назаров Ю.А. О вопросах правового регулирования профилактики преступлений в сфере информационно-коммуникационных технологий.....	168
Южанинов В.С., Расулов Н.Н. Фишинг как самостоятельный вид уголовного преступления.....	174

Баженов Василий Андреевич,
преподаватель кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Агаев Эльман Несрединевич,
курсант 4 курса
Краснодарского университета МВД России

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ РОЗЫСКА И ИДЕНТИФИКАЦИЯ ЛИЦ

Начать необходимо с того, что розыскная деятельность является самостоятельным направлением деятельности оперативных подразделений органов внутренних дел, что включает в себя не только обнаружение не только разыскиваемых лиц, но также их идентификацию и установление личности. В теории оперативно-розыскной деятельности уделяется повышенное внимание розыску лиц, но больше применительно к уголовному судопроизводству.

Мы выражаем согласие с точкой зрения П.И. Иванова¹, что розыскная и идентификационная деятельность является единой системой со множеством структурных элементов. Также автор справедливо подчеркивает, что эффективность розыскной и идентификационной деятельности зависит не только от совершенства действующего нормативно-правового регулирования, но и от научно-теоретического осмысления основ розыскной и идентификационной деятельности. При этом под идентификацией личности П.И. Иванов понимает признание тождественности, опознание личности человека.

В теории принято выделять две группы идентификаторов личности, а именно:

- бумажные идентификаторы, например, паспорт человека, водительское удостоверение, и иные документы, которые могут способствовать идентификации;
- биометрические идентификаторы, которые основаны на физических и поведенческих особенностях человека. К таковым, например, относятся:
 - походка;
 - почерк человека;
 - радужная оболочка глаза;
 - отпечатки пальцев;
 - форма лица;
 - форма носа;

¹ Иванов П.И. Розыскная и идентификационная деятельность как единая система: точка зрения // Вестник Уральского юридического института МВД России. 2023. № 3 (39). URL: <https://cyberleninka.ru/article/n/rozysknaya-i-identifikatsionnaya-deyatelnost-kak-edinaya-sistema-tochka-zreniya> (дата обращения: 16.09.2024).

- наличие физических отклонений;
- отсутствие конечности;
- и многие другие¹.

Все сказанное относится к деятельности по идентификации лица, осуществляемой оперативными подразделениями.

Еще в советский период ученые Аتماжитов В. М., Лукашов В. А.², что на доктринальном уровне необходимо глубокое осмысление функций, целей, задач, принципов, факторов, тенденций и закономерностей деятельности по розыску и идентификации лиц. Авторы подчеркивали, что анализируемый вид деятельности в правоприменительной действительности осуществляется «механически», без создания и уяснения соответствующих доктринальных основ. Стоит согласиться с точкой зрения данных советских исследователей, так как на современном этапе ситуация не изменилась. Анализ научной и учебной литературы показывает, что единичные научные работы посвящаются комплексному исследованию деятельности по осуществлению розыска и идентификации лиц.

Однако данный вид деятельности очень важен для всего общества и государства, в связи с чем представляется, что он нуждается в более полном и всестороннем доктринальном исследовании.

П.И. Иванов³ в другой своей научной работе обозначил направления, которые необходимо исследовать применительно к идентификационной и розыскной деятельности оперативных подразделений:

- оперативно-розыскная методика, включающая в себя, в том числе: идентификация лица по элементам трупа; розыск несовершеннолетних лиц, розыск пропавших без вести и т.п.

То есть автор обосновывает необходимость разработки на доктринальном уровне методик по розыску и идентификации в зависимости от характеристик разыскиваемого лица; от сложившейся ситуации; от наличия или отсутствия трупа (его частей) и т.п.;

- особенности документирования оперативно-розыскной деятельности, направленной на розыск и идентификацию лиц;

- моделирование криминальных и оперативно-розыскных ситуаций, связанных с исчезновением человека;

¹ Лапин, Е. С. Оперативно-розыскная деятельность : учебник и практикум для среднего профессионального образования / Е. С. Лапин. – 8-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 469 с. – (Профессиональное образование). – ISBN 978-5-534-17798-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/533751> (дата обращения: 16.09.2024).

² Аتماжитов В. М., Лукашов В. А. Розыскная работа оперативных аппаратов органов внутренних дел: учебное пособие. Москва: Академия МВД СССР, 1987.

³ Иванов П. И. Концептуальные основы формирования оперативно-розыскной политики: понятие, сущность и содержание // Вестник Владимирского юридического института. 2022. № 2 (63). С. 26–33.

– разработка в условиях цифровой трансформации общества современного механизма информационного обеспечения процесса документирования, т. е. реализация инновационной технологической составляющей с учетом возможных (вероятных) рисков и указанием путей их минимизации, что позволит повысить эффективность розыскной работы;

– и др.

Цели розыска в Российской Федерации могут быть разнообразными и включать следующие основные аспекты:

– Расследование преступлений: Розыск используется правоохранительными органами для выявления и установления местонахождения лиц, подозреваемых или обвиняемых в совершении преступлений.

– Поиск пропавших: Розыск применяется для поиска людей, которые могли пропасть по разным причинам, включая пропажу без вести, киднеппинг или другие обстоятельства, которые могут угрожать их жизни и безопасности.

– Исполнение судебных решений:

– Поиск свидетелей и потерпевших: Розыск может быть направлен на поиск свидетелей или потерпевших в уголовных делах, а также в гражданских и административных процессах для получения их показаний и свидетельств¹.

О важности и значимости осуществления розыска и идентификации лиц свидетельствует многочисленная судебная практика судов общей юрисдикции Российской Федерации по уголовным делам, где осуществлялся розыск лиц. Рассмотрим конкретный пример из практики – дело № 1-57/2024(1-1055/2023;) (УИД 64RS0042-01-2023-009163-33)². Как следует из материалов данного дела, показаниями свидетеля ФИО16, данными в ходе предварительного расследования, согласно которым у нее находилось дело административного надзора в отношении Х.А.ША. 21.11.2022 года Х.А.ША. написал заявление о смене местожительства, с просьбой осуществлять административный надзор по адресу: <адрес>, 22 января 2023 года поступали рапорта участковых уполномоченных полиции о том, что Х.А.ША. отсутствовал дома в ночное время. 23.01.2023 года в соответствии с установленным графиком Х.А.ША. не прибыл для регистрации в отдел полиции. Затем 23, 24, 25, 26 января 2023 года поступили еще рапорта сотрудников полиции об отсутствии Х.А.ША. дома в ночное

¹ Лапин, Е. С. Оперативно-розыскная деятельность : учебник и практикум для среднего профессионального образования / Е. С. Лапин. – 8-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 469 с. – (Профессиональное образование). – ISBN 978-5-534-17798-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/533751> (дата обращения: 16.09.2024).

² Приговор Энгельсского районного суда Саратовской области от 22.04.2024 № 1-57/2024(1-1055/2023;) (УИД 64RS0042-01-2023-009163-33) // СПС «Консультант-Плюс» 2024 (дата обращения 30.09.2024).

время. 27 января 2023 года Х.А.ША. был объявлен в розыск, на него было заведено контрольно-наблюдательное дело по розыску лица, в отношении которого установлен административный надзор, не прибывшего к месту его осуществления либо самовольно оставившего его. 20 марта 2023 года ею было вынесено постановление о прекращении розыска лица, в отношении которого установлен административный надзор в связи с поступившими сведениями из отдела дознания МУ МВД России «Энгельское» Саратовской области, о том, что Х.А.ША. был объявлен в федеральный розыск, как лицо, скрывшееся от следствия. Собранный материал проверки передан по подследственности в орган дознания МУ МВД России «Энгельское» для принятия решения в порядке ст. 144, 145 УПК РФ. В отношении Х.А.ША. в ОД МУ МВД России «Энгельское» Саратовской области, было возбуждено уголовное дело по ч. 1 ст. 314.1 УК РФ. (т. 3 л.д. 160-163).

Вот также примеры дел, где осуществлялся розыск лица:

- дело № 1-29/2024(1-249/2023;) (УИД 36RS0005-01-2023-000503-59)¹;
- дело № 1-709/2024 (УИД 50RS0026-01-2024-012826-55)²;
- дело № 1-2-14/2024 (УИД 13RS0006-02-2024-000155-39)³;
- дело № 1-363/2024 (УИД 50RS0016-01-2024-003614-91)⁴;
- дело № 1-49/2023⁵;
- и др.

Особое внимание необходимо обратить на процесс цифровизации и цифровой трансформации, который активно протекает во всем мире. И который затронул, в том числе, и оперативно-розыскную деятельность. При осуществлении розыска и идентификации лиц необходимо применять современные цифровые технологии, а также, по нашему мнению, необходимо активно внедрять искусственный интеллект и нейронные сети. Последние уже показали свою эффективность и результативность во многих отраслях. Однако в Российской Федерации процесс внедрения искусственного интеллекта и нейронных сетей идет достаточно медленно, что во многом связано с недостатками действующего нормативного правового регулирования, так

¹ Приговор Советского районного суда города Воронежа от 03.05.2024 № 1-29/2024(1-249/2023;) (УИД 36RS0005-01-2023-000503-59) // СПС «КонсультантПлюс» 2024 (дата обращения 30.09.2024).

² Приговор Люберецкого городского суда Московской области от 26.07.2024 № 1-709/2024 (УИД 50RS0026-01-2024-012826-55) // СПС «КонсультантПлюс» 2024 (дата обращения 30.09.2024).

³ Приговор Атяшевского районного суда Республики Мордовия от 25.07.2024 по делу № 1-2-14/2024 (УИД 13RS0006-02-2024-000155-39) // СПС «КонсультантПлюс» 2024 (дата обращения 30.09.2024).

⁴ Приговор Королевского городского суда Московской области от 22.07.2024 № 1-363/2024 (УИД 50RS0016-01-2024-003614-91) // СПС «КонсультантПлюс» 2024 (дата обращения 30.09.2024).

⁵ Приговор Грайворонского районного суда Белгородской области от 13.11.2023 по делу № 1-49/2023// СПС «КонсультантПлюс» 2024 (дата обращения 30.09.2024).

как оно не успевает развиваться в «ногу со временем», в связи с чем не всегда отвечает потребностям объективной действительности. Так, например, в положениях Закона об ОРД¹ нет ни слова о цифровизации, о порядке применения искусственного интеллекта и т.п. Пока в рамках оперативно-розыскной деятельности активно применяется технология «DEEPFAKE», которая применяется для синтеза изображения, голоса, речи и т.п.

О необходимости более активного применения возможностей искусственного интеллекта и нейронных сетей в рамках оперативно-розыскной деятельности также указывает В.Б. Батоев².

Говоря о дальнейшем углубленном изучении розыскной работы с научной точки зрения, необходимо выделить три взаимосвязанные проблемы:

1) отсутствие обновленного понятийного аппарата (в настоящее время появились новые понятия: оперативно-розыскной риск, идентификация бенефициарных владельцев собственности, идентификация цифровой личности, компьютерное моделирование ситуации, объекты розыскной и идентификационной деятельности и др., но они не в полной мере отражают направления рассматриваемых видов деятельности);

2) влияние цифровой трансформации;

3) необходимость корректировки информационных потоков при возникновении некоторых сложностей в ходе международного сотрудничества с правоохранительными органами иностранных государств³.

Подведем итоги.

Таким образом, можно заключить, что осуществление розыска и идентификация лиц является единым «механизмом», который не исследован в современной доктрине.

Комплексные исследования отсутствуют как в рамках теории оперативно-розыскной деятельности, так и в рамках иных юридических наук, например, криминалистики.

Считаем целесообразным создание доктринальных основ деятельности по осуществлению розыска и идентификации лиц. Представляется, что первостепенной задачей является разработка на доктринальном уровне со-

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

² Батоев В.Б. Об использовании технологии «DEEPFAKE» в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. №1 (61). URL: <https://cyberleninka.ru/article/n/ob-ispolzovanii-tehnologii-deepfake-v-operativno-rozysknoy-deyatelnosti> (дата обращения: 16.09.2024).

³ Лапин, Е. С. Оперативно-розыскная деятельность : учебник и практикум для среднего профессионального образования / Е. С. Лапин. – 8-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 469 с. – (Профессиональное образование). – ISBN 978-5-534-17798-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: <https://urait.ru/bcode/533751> (дата обращения: 16.09.2024).

ответствующих методик, а также изучение вопроса о возможностях искусственного интеллекта и нейронных сетей в рамках анализируемого вида деятельности, осуществляемого оперативными подразделениями. Ведь искусственный интеллект и применение нейронных сетей могут сократить время обработки данных, ускорить процесс поиска лица, его идентификации. Однако для повсеместного внедрения искусственного интеллекта и нейронных сетей в деятельность оперативных подразделений по розыску и идентификации лиц необходимо разрешить проблему с действующим нормативно-правовым регулированием. Пока искусственный интеллект и нейронные сети применяются в оперативно-розыскной деятельности «сегментарно», то есть не используются весь их потенциал и весь спектр возможностей.

Баженов Василий Андреевич,
преподаватель кафедры ОРД в ОВД
Краснодарского университета МВД России

Скитская Виктория Андреевна,
курсант 4 курса
Краснодарского университета МВД России

ИННОВАЦИИ В ПРЕДУПРЕЖДЕНИИ И РАСКРЫТИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Современный век характеризуется тенденцией активного развития информационных технологий. На данный момент сложно представить какую-либо сферу, которая обходится без внедрения технологический или информационных инноваций. Данная особенность обусловлена упрощением благодаря их использованию многих рутинных, ежедневных задач. И безусловно стоит отметить такой скачок, в обозначенной сфере, как искусственный интеллект.

Искусственный интеллект представляет из себя сферу в области компьютерного направления, которая основана на обработке большого объема данных и последующего их анализа, итогом деятельности которого является выявление закономерностей обрабатываемой информации и выполнением поставленных задач.

Искусственный интеллект имеет тенденцию скачкообразного развития. Только в 2020 году с помощью него создавались хоть и детализированные, но в некотором роде несуразные фотоизображения, и вот на настоящий момент он способен генерировать целые видео и даже имитировать голос человека. Данная особенность вызывает некоторую настороженность, так как невозможно предсказать в каком направлении может и будет развиваться данная технология, поскольку в нее заложено программным путем функция самообучения и какие возможности в себе откроет новое программное обеспечение в виде искусственного интеллекта и как это будет использовано – неизвестно.

Искусственный интеллект нашел свое применение и в преступной сфере. Развитие информационных технологий обуславливает новые тенденции совершения преступлений. Только в данной сфере количество зафиксированных преступлений в 2024 году составляет 577 тысяч¹. Многие специалисты выражают обеспокоенность по отношению к искусственному интеллекту, поскольку он обеспечивает автоматизацию криминальных действий

¹ URL: <https://journal.sovcombank.ru/news/uscherb-ot-it-prestuplenii-v-2024-godu-sostavil-99-mlrd-rublei?ysclid=m2nfr2wgd327143330>

преступника, что освобождает его от непосредственных направленных действий в совершаемых преступлениях, что крайне затрудняет раскрытие преступлений и поиск самого исполнителя.

Поэтому для раскрытия и предупреждения преступлений, совершаемых с использованием искусственного интеллекта, сотрудникам оперативных подразделений необходимо следовать тенденциям развития технологий. Искусственный интеллект постепенно проходит тестирование и используется в раскрытии и предупреждении преступлений, ну как минимум используется в виде дополнительного инструмента.

Так, к примеру, в испанском университете Леона были проведены исследования в сфере искусственного интеллекта, в результате чего, данная технология постепенно обучается выявлять доказательства на месте преступления и систематизировать их. Как это происходит? Искусственный интеллект представляет из себя программу, которая создаётся путём прописывания различных формул и комплексов действий для выполнения определённых задач. Анализируя исходные данные и внедрение заранее предусмотренных некоторых шаблонных действий, искусственный интеллект учится подстраиваться под введённые данные, используя исходные шаблоны, которые с помощью сложных математических формул могут порождать новые действия – так и проходит его самообучение. То есть, программисты ввели в искусственный интеллект информацию ранее раскрытых преступлений, а как говорилось и ранее, искусственный интеллект способен выявлять закономерности, а следовательно причинно-следственные связи, следовательно, введя новые исходные данные по совершенному преступлению, программа будет проводить анализ на основе ранее совершаемых и определять вероятность дальнейшего поведения преступника. Конкретно в институте Леона, данная программа использовалась при фотографировании вещественных доказательств и для выявления различных значимых для дела элементов. В оперативно розыскной деятельности возможно создать банк данных, в который необходимо внести паттерны поведения преступников по мере раскрытия преступления, те действия, которые они совершали, будь то финансовые махинации, либо пути следования, способы сокрытия преступления и самого лица. После чего ввести оперативно розыскные мероприятия, которые способствовали раскрытию данных преступлений и получаемую оперативно значимую информацию, которая имела значения для раскрытия или предупреждения преступления. На основе принципа самообучения искусственный интеллект сможет формировать комплексы действий для раскрытия и предупреждения преступлений с введёнными данными, а также прогнозировать действия, которые преступник может предпринять для сокрытия от органов дознания и следствия.

Даже если учитывать несовершенство программ, то следует отметить, что от того, насколько качественно будет построен изначальный банк данных, содержащий первоначальные оперативно розыскные мероприятия,

которые необходимо провести при том или ином преступлении – то искусственный интеллект будет очень полезен для вновь прибывших на службу молодых и неопытных оперативных сотрудников. Так с помощью искусственного возможно определить план проводимых оперативно-розыскных мероприятий на начальном этапе, и определить направления раскрытия преступления для оперативного сотрудника.

Также стоит уделить внимание возможности идентификации человека, а именно выявлению с помощью искусственного интеллекта потенциальных преступников на основе анализа поведенческих черт. На данный момент участились случаи совершения террористических актов и экстремистских преступлений. Также не стоит обделять вниманием и массовые беспорядки. Особенностью этих обозначенных видов преступлений стоит выделить массовость, которая проявляется в виде наличия толпы. Террористические акты должны устрашать население, поэтому проявляются в виде поджогов, взрывов в людных местах. Некоторые экстремистские преступления и массовые беспорядки имеют особенность наличия толпы при продвижении каких-либо лозунгов или недовольств. Тем не менее, в каждом из этих преступлений имеются свои отдельные присущие поведенческие черты исполнителей и участников конфликтов. Почему этому следует уделить внимание и как искусственный интеллект связан с этим? Язык тела зачастую может рассказать за человека больше, чем он сам, поскольку его психологическая составляющая при определённых условиях рефлексивно выдаёт внутреннее состояние. Используя возможности искусственного интеллекта, возможно разработать систему, которая автоматически идентифицирует подозреваемых с помощью методов глубокого обучения на основе жестов, позволяя тем самым установить среди толпы людей конкретного человека, ответственного за массовые беспорядки, а также предупредить совершение преступлений.

Такие программы уже не грёзы или научная фантастика, данная сфера развивается как за рубежом, так и в России. К сожалению, пока что данная программа только разрабатывается, но медленно и верно начинает функционировать. «Национальный центр информатизации», входящий в структуру госкорпорации «Ростех» уже занимается данным вопросом.¹

Разберём устройство программы. Касаясь террористических актов, то в систему следует заложить паттерны поведения, которые являются потенциально опасными. К сожалению, черты присущие террористам достаточно сложны для выявления, так как многие из них могут проявляться и у законопослушных граждан. Таковыми могут являться скованность движений, избегание представителей правоохранительных органов, уклонение от

¹ URL: <https://novayagazeta.ru/articles/2021/11/30/kommersant-vlasti-razrabatyvaiut-sistemu-dlia-predskazaniia-massovykh-besporiadkov-i-mitingov-s-pomoshchiu-iskusstvennogo-intellekta-news>

камер видеонаблюдения и т.д. При выявлении данных паттернов, программа может уведомить сотрудника о потенциальной опасности для принятия последующих действий.

При массовых беспорядках стоит уделять внимание, что активность участников конфликта выражается в разных чертах поведения. Это могут быть провокаторы, кричащие громкие лозунги, призывающие к активному противодействию сотрудников, агрессоры, которые применяют физическую силу и различные средства, представляющие опасность для жизни и здоровья человека и гражданина. Также связисты, которые передвигаясь в толпе поддерживают связь с организаторами массового беспорядка, содействуя в разжигании конфликтов. Заложение данных особенностей позволит оперативным сотрудникам наиболее быстро выявлять активных участников толпы, без непосредственного внедрения в неё и нейтрализовать их в последующем.

Для достижения поставленной цели система будет анализировать сообщения в СМИ, данные социальных сетей, «умных» камер и других источников. Также возможно заложение тактико-практической базы, искусственный интеллект будет анализировать поведение толпы и рекомендовать силовикам порядок действий. Также возможен вариант обеспечения «многофакторного мультивариантного анализа вероятностей возникновения массовых беспорядков и несанкционированных публичных мероприятий». Для этого система будет постоянно анализировать все вышеобозначенное, данные из систем интеллектуального видеонаблюдения и мониторинга общественного транспорта. Если массовые беспорядки уже начались, с целью предотвращения эскалации система будет анализировать число участников митинга, поведение зачинщиков, направление движения толпы, число пострадавших, количество сотрудников, задействованных в обеспечении порядка, и т.д. Действующие в мире цифровые платформы уже наработали весь набор необходимых решений для анализа текстов, эмоционального состояния и закономерностей поведения групп населения.

Создание подобной технологии потребует немалых затрат, ведь массив данных, который будет обрабатывать программное обеспечение будет огромным. Системе придётся работать с постоянным потоком людей, а также каждого из них проверять на наличие заложенного параметра, поведенческих черт. Необходимо обеспечить места массового скопления людей камерами видеонаблюдения с максимальным обзором для того, чтобы система могла распознавать те или иные заложенные паттерны поведения в бесчисленном потоке людей.

Таким образом, искусственный интеллект возможно использовать не только в преступной сфере, но и на благо сотрудникам оперативных подразделений, что способствует наиболее эффективному раскрытию и предупреждению преступлений.

Батоев Владимир Батоевич,
старший научный сотрудник отдела специальной техники
НИИСТ ФКУ НПО «Специальная техника и связь» МВД России,
кандидат юридических наук, доцент

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ МОШЕННИЧЕСТВУ, СОВЕРШАЕМОМУ С ИСПОЛЬЗОВАНИЕМ СИНТЕТИЧЕСКИХ МЕДИА

Рассматривая вопросы противодействия преступности в IT-сфере важно отметить, что сложившаяся ситуация продолжает оставаться крайне напряженной. Об актуальности данного утверждения свидетельствуют официальные данные статистики. Так, за 8 месяцев 2024 года на территории Российской Федерации (далее – РФ) было зарегистрировано 500389 преступлений, совершенных с использованием информационно-телекоммуникационных технологий, где сумма причиненного ущерба превысила отметку в 116 млрд. руб.

За указанный период органами внутренних дел (далее – ОВД) выявлено более 250 тысяч IT-мошенничеств, из которых по ч. 1 ст. 159 УК РФ – около 4000.

За 8 месяцев 2024 года традиционно зарегистрировано большинство IT-преступлений, в том числе мошенничеств, совершенных с использованием: средств мобильной связи – более 230000; сети «Интернет» – более 400000; мессенджеров – более 140000; методов социальной инженерии – более 80000 противоправных фактов.

По этому поводу важно обратить внимание на то, что 14 октября 2024 года состоялось заседание Объединенной коллегии министерств внутренних дел Российской Федерации и Республики Казахстан. Основным вопросом повестки заседания стало совместное противодействие киберпреступности. Министр внутренних дел Российской Федерации генерал полиции Колокольцев отметил, что если еще пять лет назад доля таких посягательств в России составляла менее 15%, то в текущем году – уже 40%. С учетом социальной значимости данного вопроса на государственном и ведомственном уровнях принят ряд неотложных мер. В частности, серьезно усовершенствованы законодательство, а также нормативная база Министерства. Выработаны алгоритмы взаимодействия органов внутренних дел с другими компетентными ведомствами и структурами. Созданы специализированные оперативные и следственные подразделения.

Непрерывный рост числа зарегистрированных IT-преступлений берет причины в возможности их совершения в дистанционном формате, а также беспрецедентным уровнем возможности обеспечения анонимности личности пользователя информационно-телекоммуникационными технологиями и их производными продуктами, программным обеспечением, мобильными

приложениями и иным софтом, находящемся в свободном обороте, в том числе на безвозмездной основе.

Помимо этого, особое внимание обращает на себя внимание факт, при котором криминально настроенные лица все чаще и активнее применяют в своей противоправной деятельности телекоммуникационное оборудование в виде sim-банков. По данным практики только в текущем году в ходе проведения оперативно-розыскных мероприятий и следственных действий органами внутренних дел изъято более 600 таких устройств. Более того обнаружены и изъяты более 120000 sim-карт различных операторов мобильной связи. Как показывает практика подобное количество sim-карт обеспечивало возможность преступникам совершать до 30 млн телефонных звонков в сутки. Как следствие, 9 из 10 жителей нашей страны минимум один раз выступали в роли потенциальных жертв преступников, а каждый пятый признавался потерпевшим.

Подобное стало возможным, в том числе в силу использования киберпреступниками современного высокотехнологичного инструментария, которому присуще постоянное совершенствование как аппаратно-программной части, так и навыков его использования, а также непрерывный поиск новых технологичных методов и средств решения криминальных задач.

В данном случае не без внимания остался такой инновационный феномен в преступной практике как использование технологий искусственного интеллекта. Речь идет о технологии создания с использованием генеративных состязательных нейросетей синтетического контента (медиа – фото-, видео-, аудиосообщения).

Технология «Дипфейк» является комплексом методов интеграции фото-, видеоизображений и аудиоинформации посредством использования нейросетей в единое целое, в нашем случае выступающее в качестве поддельного.

Данная технология разработана в 2014 году в США, и получила резонансную известность, когда в сети Интернет получили широкое распространение противоправное компрометирующее видео известных лиц киноиндустрии.

Существенно усугубляет, с одной стороны, обстоятельство, при котором криминально настроенные лица используют фото-, видеоизображения и аудиозаписи голосов граждан, которые в основном получают посредством несанкционированного взлома их аккаунтов в социальных сетях, мессенджерах, группах и др.

Наиболее резонансным по сумме причиненного ущерба примером использования дипфейков является совершение преступления в Гонконге, при котором сотрудник финансовой компании, находясь в состоянии введенного заблуждения и видеообмана обеспечил перечисление преступникам денежной суммы равной около 25 млн долларов США.

В данном случае поддельная личность, сформированная нейросетью с использованием фото- и видеоизображений реального лица, выступила гарантом совершения преступления в силу обеспечения высокого уровня доверия видеозвонку. Финансовый работник до последнего предполагал, что общается по видеозвонку с руководителем фирмы, что, собственно, и обеспечило совершения перевода денежной суммы на счета, указанные поддельной синтетической личностью. Подобный пример, в том числе может косвенно указывать, что совершение преступниками мошеннических атак на граждан с использованием подобной технологии и применением указанного способа совершения преступления способствует кратному увеличению ИТ-мошенничеств в ближайшей перспективе.

Об этом уже свидетельствует практика. Так, общее число кибератак с использованием фото- и видеодипфейков в финансовой отрасли увеличилось более чем на 13 % (около 5,7 тыс. фактов), где процент их эффективности составил цифру равную 20. Это лишь в очередной подтверждает, что ИТ-мошенники более чем на 600 % стали чаще использовать дипфейки в сфере финансов, что может указывать на тенденцию смещения вектора их деятельности от традиционных направлений выбора жертв ИТ-преступлений. Здесь объектами преступных посягательств на первом плане выступают как сами клиенты учреждений кредитно-финансовой системы, так и их сотрудники. Уже сейчас в практике встречаются случаи создания и использования «синтетических» видеоконсультантов, видеоэкспертов и др., где границу их реальности или поддельности становится все сложнее определить обычному человеку. Все это указывает на необходимость проведения с данной категорией граждан профилактических мер, как стороны самих финансовых организаций, так и со стороны органов внутренних дел, общественности, средств массовой информации, социальных сетей и др.

Как показывает практика, в настоящее время наиболее распространенными способами совершения ИТ-мошенничеств являются:

1. ИТ-мошенничества с использованием поддельного голоса, когда преступники используют аудиодипфейки для имитации голосов реальных людей при совершении преступлений.

2. ИТ-мошенничества в кредитно-финансовой сфере, где преступники путем обмана сотрудников через использование видео- и аудиодипфейков изображений и голосов руководителей вводят в преступных целях в заблуждение последних.

3. ИТ-мошенничества в социальных медиа и рекламе, где преступники используют синтетические голоса и изображения известных личностей в целях побуждения граждан к совершению контролируемых действий с принадлежащими им финансовыми активами.

4. IT-мошенничества в сфере проведения лжесобеседований, когда мошенники используют дипфейки при проведении собеседований с кандидатами на те или иные вакантные места с последующим преступным завладением искомых финансовых и иных средств потерпевших.

5. IT-мошенничества посредством использования дипфейков при решении вопросов обхода системы аутентификации учреждений кредитно-финансовой сферы с последующим получением доступа к учетным записям их клиентов.

К сожалению, приходится констатировать, что перечень способов совершения IT-мошенничеств не носит исчерпывающего характера. Однако полагаем, что представленные нами сведения о способах преступной активности найдут познавательное применение в практической, научной и образовательной деятельности в части расширения представлений о подобном негативном социальном явлении.

Одновременно с этим, изучение юридической литературы позволяет заключить, что в нормах отечественного законодательства не предусмотрена какая-либо ответственность за использование дипфейков в повседневных целях. Внимание ученых обращено в основном на необходимость разрешения вопросов уголовно-правовой квалификации использования дипфейков в криминальных целях. Иными словами, речь идет либо о признании уголовно-наказуемым деянием использование дипфейков в преступных целях, либо отягчающим обстоятельством того или иного криминального события.

Справедливо возникает вопрос о том, как же все-таки бороться с IT-мошенничествами в современных непростых условиях. По этому поводу в юридической литературе существуют множество точек зрения, со своими положительными и отрицательными сторонами.

Отвечая на такой вопрос, отметим следующее. В данное время существуют множество способов и методов, сконцентрированных в виде программного обеспечения, мобильных приложений и иного софта, находящегося в свободном доступе, целью использования которых является выявление признаков дипфейка в том или ином фото-, видеоизображении или аудиосообщении. Такие технические решения основаны на использовании определенных алгоритмов анализа контента на предмет определения следов использования нейросетей в процессе их создания или монтажа. Подобные технические решения становятся все более востребованными, что обусловлено необходимостью проверки подлинности контента на содержание достоверной информации.

Особое место в противодействии IT-мошенничествам, совершаемым с использованием дипфейков занимает деятельность лиц, обладающих специальными глубокими познаниями в деле их выявления. Здесь речь идет о помощи экспертов экспертно-криминалистических подразделений органов внутренних дел.

С учетом дозволенных объемов изложения материала важно обратить внимание практических сотрудников, научных работников, представителей органов различных ведомств, задействованных в противодействии использованию дипфейков, используемых при подготовке и совершении различных видов противоправных деяний на результаты одной научно-исследовательской работы. ФКУ НПО «СТиС» МВД России совместно с ЭКЦ МВД России выполнена научно-исследовательская работа «Исследование возможных способов выявления признаков внутрикадрового монтажа видеоизображений, выполненного с помощью нейронных сетей, шифр «Зеркало (Верблюд)». Полученные в ходе проведенных работ результаты теоретических, экспериментальных и экспертных исследований позволили сделать вывод о наличии возможности выявления признаков внутрикадрового монтажа видеоизображений, выполненного с помощью нейросетей, а также необходимость проведения опытно-конструкторской работы по созданию аппаратно-программного комплекса по выявлению видеодипфейков.

Помимо указанных результатов в рамках данной работы был разработан прототип нейронной сети, обеспечивающей возможность эксперту с его помощью выявлять наличие признаков видеомонтажа в исследуемом видеоизображении. О необходимости и эффективности подобного технического решения свидетельствует практика, где присутствуют примеры применения экспертами указанного прототипа нейросети в ходе раскрытия и расследования преступлений. Так, с его помощью был установлено, что видеоизображение ранее пропавшего без вести, направленное его родственникам с целью получения денежных средств, оказалось дипфейком.

Таким образом, с учетом изложенного отметим, что перед субъектами оперативно-розыскной и уголовно-процессуальной деятельности назрела задача противопоставить соответствующий действенный инструментарий не только IT-мошенничествам, но и иным преступлениям, где возможно применение дипфейков. Это предполагает принятие соответствующих мер по разработке действенного законодательства по всем вопросам правового регулирования использования дипфейков; по выработке эффективных практик, методов и средств выявления дипфейков и использования их результатов в деятельности органов внутренних дел и иных правоохранительных органов. Отсюда крайне важно организовать проведение научных исследований в образовательных и научных организациях МВД России в данном направлении с целью выработки научно обоснованных предложений и рекомендаций правового, организационного и тактического характера, направленных на совершенствование деятельности органов внутренних дел в частности и правоохранительной деятельности в целом. Безусловно, такие разработки потребуют своевременной разработки и корректировки образовательных программ подготовки и переподготовки сотрудников органов внутренних дел в данном направлении.

Васильев Эдуард Анатольевич,
главный научный сотрудник ВНИИ МВД России,
доктор юридических наук, доцент

Мороз Роза Нураддиновна
старший научный сотрудник ВНИИ МВД России

АКТУАЛЬНЫЕ ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПЛЕНИЯМИ КОРРУПЦИОННОЙ НАПРАВЛЕННОСТИ В СФЕРЕ ГОСУДАРСТВЕННЫХ ЗАКУПОК

Действующая в настоящее время система приобретения товаров, выполнения работ и оказания услуг для решения нужд муниципальных и государственных учреждений (иное название – госзакупки) остается наиболее финансируемым направлением национальной экономики. В частности, в Единой информационной системе (ЕИС¹) госзакупок на 2024 г. размещено 166 222 планов-графиков, их сумма по всей России составила 11,6 трлн рублей (АППГ – 15,7 трлн рублей), из них 2,9 трлн рублей федеральные заказчики, 8,6 трлн рублей региональные и муниципальные заказчики (динамику государственных закупок за период с 2020 по 2024 гг. см. в табл. 1).

Таблица 1

Справка

о состоянии государственных закупок

	2020	2021	2022	2023	2024
Количество размещенных планов графиков	180665	177788	172012	173094	166222
Планирование/ Общая сумма размещенных планов графиков в млрд рублей	13376,21	14306,2	15833,22	15771,12	11618,31
Количество размещенных извещений	2178149	2360574	2297869	2422361	1071177
Общая сумма размещенных извещений	9578,2	10560,97	10986,75	10646,51	4691,42
Количество заключенных контрактов	3419866	3333109	3209594	3341481	1489216
Общая сумма заключенных контрактов в млрд рублей	9308,84	9948,66	11514,3	10200,36	4337,49
Относительная экономия при заключении контрактов в %	8,03	6,88	5,72	5,68	4,79
Экономия при заключении контрактов в млрд рублей	441,69	400,59	415,41	436,56	181,25

¹ Единая информационная система в сфере закупок (ЕИС) была создана в соответствии с федеральными законами № 44-ФЗ и № 223-ФЗ для облегчения доступа к сведениям о торгах и минимизации коррупции в сфере закупок.

Максимальное число заказов дислоцировано в г. Москве, где размещено 1970 планов-графиков на сумму 975 млрд рублей, в Московской области – 3208 планов-графиков на сумму 651,6 млрд рублей, в Санкт –Петербурге – 3079 планов графиков на 480 млрд рублей, в Краснодарском крае – 6175 планов графиков на 341,6 млрд рублей, в Красноярском крае – 3807 планов графиков на 262,3 млрд рублей.

На июнь 2024 г. заключено 1 489 216 контрактов, цена которых по всем способам определения поставщика составила 4,34 трлн рублей из них 47,2% приходится на электронный аукцион (1,04 трлн рублей), 34,81% на открытый конкурс в электронной форме (1,51 трлн рублей), 14,74% закупка у единственного поставщика (исполнителя, подрядчика), 2,95% запрос котировок в электронной форме (127,8 млрд рублей), 0, 32% (13,85 млрд) – закупка осуществляемая в соответствии с ч. 12 ст. 93 ФЗ-44, иные способы 0,01 или 481,71 млрд рублей.

По итогам первого квартала 2024 г. в России на 1,3% снизилось число госзакупок, осуществляемых по Закону № 44-ФЗ по сравнению с аналогичным периодом прошлого года – с 1,036 млн до 1,022 млн процедур, при этом сумма завершенных закупок снизилась на 14% с 2,87 трлн рублей до 2,45 трлн рублей. Средняя цена закупок также уменьшилась: в первом квартале 2023 г. она составила 3,04 млн рублей, за аналогичный период 2024 г. – 2,68 млн рублей.

Вероятнее всего такая тенденция связана с перераспределением средств федерального бюджета в сторону обеспечения военных нужд. Самыми затратными отраслями стали строительство, архитектура и недвижимость, в которых осуществлено 127538 торгов на сумму 1,06 трлн руб., медицина и фармакология – 262039 торгов на сумму 393 млрд руб., закупки на поставку топлива и энергии – 196 067 торгов на сумму 333 млрд руб.

Проведенное в 2024 году ВНИИ МВД России исследование¹ показало, что отношение бизнеса к госзакупкам остается неоднозначным. Так, в 1 кв. 2024 г. в производстве ФАС России находилось 8,3 тыс. жалоб в сфере закупок, из них обоснованными или частично обоснованными ведомство признало 3,3 тыс. обращений, по результатам рассмотрения которых выявлено 3,7 тыс. нарушений.

Руководство ФАС России признает, что в последние годы нарушения в рассматриваемой сфере стали носить более скрытый (латентный) характер², что подтверждается оперативно-служебными документами ГУЭБиПК МВД России. Усилиями его сотрудников и подразделений ЭБиПК территориальных органов МВД России в январе-декабре 2023 г. на учет поставлено

¹ См.: пункт 3.6 Плана научного обеспечения деятельности органов внутренних дел Российской Федерации на 2024 год и пункт 8.1 Плана – графика научно-исследовательской работы ВНИИ МВД России на 2024 год.

² Подробнее об этом см.: <https://fas.gov.ru/publications/24331>

2757 преступлений, из них 1257 в связи с осуществлением закупок государственными и 1500 – муниципальными заказчиками. В основном это преступления против собственности – 1747 (63,4%), в том числе мошенничество – 1571 (57,9%), против государственной службы – 783 (28,4%), связаны с получением взятки – 249 (9,03%), дачей взятки – 173 (6,27%), посредничество во взятке – 67 (2,43%). Из общего числа зарегистрированных преступлений 546 связаны с подкупом, коммерческим подкупом, а также незаконной передачей должностному лицу заказчика денежных средств, получаемых поставщиком (подрядчиком, исполнителем) в связи с исполнением государственного или муниципального контракта, за «предоставление» права заключения такого контракта (так называемые «откаты»). Больше половины преступлений (59,67%) связаны с причинением крупного и особо крупного ущерба либо совершены в крупном размере. Общая сумма ущерба по окончанным и приостановленным делам составила 8,6 млрд руб. при этом в целях обеспечения приговора в части гражданского иска, взыскания штрафа или возможной конфискации имущества – наложен арест на имущество, добровольно погашено, изъято имущества, денег, ценностей на сумму более 5,9 млрд руб., что составило 69,5% от суммы причиненного ущерба. Всего по уголовным делам данной категории выявлено 1113 лиц, совершивших преступления, по обвинению которых в суд направлено 974 уголовных дела, из них 122 в отношении организованных групп или преступных сообществ.

Больше всего преступлений выявлено в Московской области (347), г. Москва (332), Краснодарском (188) и Красноярском крае, Воронежской области (по 93), г. Санкт-Петербург (89), Республике Крым (88), Омской области (84), Республике Татарстан (74), Смоленской (70) и Брянской (69) области. Одинаковое количество деликтов вскрыто в Республике Дагестан и Новосибирской (62)б области, а также Кемеровской и Самарской (54) области. Незначительные результаты работы демонстрируют подразделения полиции по Ивановской, Калужской, Саратовской, Ульяновской, Тюменской (по 5), Тульской, Псковской, Калининградской (по 4), Липецкой, Магаданской (по 3), Вологодской, Мурманской (по 2) области, по Республике Коми, Карачаево-Черкесской (4), Северной Осетии (Алании) (3), Кабардино-Балкарской, Мордовии, Тыва (по 2), Калмыкии (1), Хабаровского и Камчатского края (по 1). Отсутствуют результаты работы МВД России по Чеченской Республике и Марий Эл, а также в Еврейской автономной области.

По статье 200.5 УК РФ выявлено 19 преступлений, из них 16 в крупном или особо крупном размере. Криминальные деликты вскрыты на территории Белгородской (3), Челябинской (8), Новосибирской (3), Пензенской (4) областей, в г. Москва (1). По выявленным фактам возбуждено 19 уголовных дел, из которых 2 прекращены по реабилитирующим основаниям (г. Москва). Выявлено 8 лиц, совершивших преступления, в отношении 5 из них уголовные дела направлены в суд по обвинению в совершении

9 преступлений. Наложено арест на имущество, добровольно погашено, изъято имущества, денег, ценностей на сумму более 18,7 млн рублей.

Преступления, предусмотренные ст. 200.4 УК РФ в 2023 году подразделениями ЭБиПК не выявлялись.

Значительно снижена эффективность работы по выявлению преступлений, связанных с заключением антиконкурентных соглашений (- 36%), всего выявлено 7 таких преступлений по которым возбуждено 6 уголовных дел по признакам преступления, предусмотренного статьей 178 УК РФ (ограничение конкуренции). Преступления выявлены на территориях: г. Санкт-Петербурга и Ленинградской области, республик Татарстан, Хакасия, Ставропольского, Приморского краев, Брянской, Ростовской областей. По результатам расследования в суд направлено 4 уголовных дела в отношении 13 обвиняемых (Республика Татарстан – 2, г. Санкт-Петербург и Ленинградская область, Воронежская область – по 1), прекращено 3 уголовных дела (Ставропольский, Хабаровский края, Нижегородская область), 1 уголовное дело приостановлено (Хабаровский край). Размер причиненного материального ущерба (по оконченным и приостановленным уголовным делам) составил более 22,3 млн рублей, наложен арест на имущество, добровольно погашено, изъято имущества, денег, ценностей на сумму более 30,4 млн рублей.

Анализ эмпирических материалов, собранных в рамках данной публикации, свидетельствует о том, что больше всего преступления коррупционной направленности совершаются при реализации национальных проектов «Жилье и городская среда», «Демография», «Образование». Самыми криминогенными направлениями при реализации государственных и муниципальных контрактов являются выполнение работ (81% от всех зарегистрированных в сфере госзакупок преступлений), особенно по таким направлениям деятельности как строительство, реконструкция или капитальный ремонт, где преобладает завышение объемов выполненных работ и замена материалов. На долю поставок товаров приходится 15% преступлений, как правило у преступников популярна закупка товаров по завышенной цене либо поставка товаров не соответствующего качества, лидирующие позиции в данном сегменте занимают товары медицинского назначения и продовольствие. На долю оказания услуг приходится 4% преступлений, в большинстве случаев это оказание образовательных услуг.

Как показало исследование, чаще всего криминальным посягательствам подвергается жилищно-коммунальный комплекс (строительство и ремонт жилых домов и объектов социального назначения, тепло- и водоснабжения, благоустройство) – 64,0%. Далее следуют: строительство и ремонт автомобильных дорог – 10,3%, оборонная промышленность – 10,0%, оказание социальных услуг, культура и спорт – 8,4%, образование, наука, сфера высоких технологий – 2,3%, промышленное строительство – 1,9%, здравоохранение – 1,6%.

В завершающей части небольшой по объему статьи отметим, что принципиальная и последовательная борьба с коррупцией, которая отравляет общество, ломает законопослушный бизнес, крадёт деньги, необходимые для обороны страны, для её движения вперед в экономике и социальной сфере, остается в числе главных задач, которые стоят перед органами внутренних дел¹.

¹ Директива МВД России от 17 ноября 2023 года «О приоритетных направлениях деятельности органов внутренних дел Российской Федерации в 2024 году».

Введенская Ольга Юрьевна,
старший преподаватель кафедры криминалистики
Краснодарского университета МВД России,
кандидат юридических наук

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПОЛУЧЕНИЯ ПЕРВОНАЧАЛЬНОЙ ИНФОРМАЦИИ О НЕЗАКОННОМ СБЫТЕ НАРКОТИЧЕСКИХ СРЕДСТВ

Понятие первоначальной информации весьма широкое и включает в себя любые сведения (как процессуальной природы, так и не процессуальной), имеющие значение для раскрытия и расследования преступлений, раскрывающие признаки определенного состава преступлений, определяющие наличие, либо же отсутствие преступного факта.

А.А. Рудых, рассматривая преступления в сфере информационных технологий, включает в содержание первоначальной информации о них: сведения о пользователях, проявлявших сетевую активность, и о событиях, произошедших в связи с ней. В частности, сюда отнесены:

сведения об используемых в преступных целях номерах мобильных телефонов;

сведения о номере банковской карты либо электронного платежного средства;

информация о доменном имени или адресе используемого преступниками интернет-ресурса;

адреса электронной почты причастных к совершению преступления лиц;

идентификационные номера страниц в социальной сети;

IP адреса и т. д.¹

Верховный Суд РФ к первоначальным сведениям о незаконном сбыте наркотических средств относит информацию о возмездной либо безвозмездной реализации (продаже, дарении, обмене, уплате долга, даче взаймы и т. д.) наркотических средств².

¹ Рудых А.А. Информационно-технологические обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Ростов н/Д, 2020. С. 136–137.

² О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ. 2006. № 14. Доступ из справ. правовой системы «КонсультантПлюс».

Таким образом, в понятие первоначальной информации об анализируемых преступлениях следует включать сведения о пользователях информационно-телекоммуникационных технологий и систем, а также об их сетевой активности, связанной с реализацией наркотических средств.

На наш взгляд, такие признаки сетевой активности могут быть разделены на две группы:

прямо свидетельствующие об осуществлении незаконного сбыта наркотических средств (содержательная часть сообщений в мессенджерах, чатах, социальных сетях, информационный контент веб-сайтов, личных аккаунтов, push-уведомлений, баннерная реклама в сети Интернет и т. п.);

косвенно указывающие на осуществление незаконного сбыта наркотических средств (регистрация и регулярное осуществление финансовых операций по электронным счетам, кошелькам, платежным системам, специфические перемещения пользователя, отраженные в данных программ геолокации и геопозиционирования, использование программ-ботов, попытки анонимизации сетевой активности, использование мессенджеров с функциями шифрования сообщений, нецелевое использование нетипичного или специального программного и аппаратного обеспечения и т. п.).

Признаки второй группы имеют криминалистическое значение лишь в совокупности с признаками первой, позволяя конкретизировать анализируемую преступную деятельность, определить ее масштабы и круг участвующих лиц.

Говоря о получении первоначальной информации следует отметить ее специфику, определяемую использованием информационно-телекоммуникационных технологий: первичным должно явиться исследование информационной плоскости преступлений, связанных с незаконным сбытом наркотических средств, и, следуя по пути преступника, появляется возможность восполнить все информационные пробелы криминальной картины.

В ранее проведенном исследовании¹ были рассмотрены основные группы методов получения такой информации. Однако, как очевидно, преступность не стоит на месте, регулярно расширяя свой преступный арсенал, в противовес принимаемым контрмерам. В связи с чем предлагаем рассмотреть ряд актуальных для этой сферы подходов.

Рассматривая данную категорию уголовных дел, основной объем доступной правоохранительным органам первоначальной информации о незаконном сбыте наркотических средств будет находиться именно в информационном пространстве, тем самым и определяется содержание методов ее получения:

¹ Введенская О.Ю. Особенности предварительного и первоначального этапов расследования незаконного сбыта наркотических средств с использованием информационно-телекоммуникационных технологий: дис. ... канд. юрид. наук. Краснодар, 2022. 201 с.

Интернет-анализ контента – это процесс исследования содержания сетевой активности пользователей информационно-телекоммуникационных систем и технологий для выявления подозрительного поведения и идентификации угроз. Специалисты по цифровой криминалистике используют различные инструменты и методы, такие как анализ трафика, поиск аномалий и обнаружение вторжений, для выявления и расследования преступлений, связанных с сетевой активностью и сетевым поведением. Его можно проводить как точно, целенаправленно, так и с использованием систем искусственного интеллекта:

- регистрационные данные – для абсолютного большинства сетевых ресурсов логина и пароля доступа к ним оказывается недостаточно. И пользователи, желающие посещать этот ресурс, вынуждены указывать персональные данные. Например, дата рождения, имя и т.п., вполне могут не соответствовать действительности, то номер телефона или адрес e-mail, зачастую, приходится указывать реальный, потому что этого требует алгоритм проверки и персонификации. Результат сопоставления регистрационных данных нескольких ресурсов вполне вероятно откроет доступ к третьему.

- из вышеописанного вытекает еще один аспект – мультиник – использование одного и того же ника (логина) на разных информационных площадках.

- стили и характеристики письменной речи – лингвистический анализ криминалистически значимых сведений позволяет определить пол, приблизительный возраст, образовательный уровень, хобби, профессиональную принадлежность и т.п. Причем, учеными-лингвистами выявлено, что для идентификации человека достаточно весьма небольшого объема текста.

- профессиональная тематика – знания о способах изготовления, культивирования и иных действий с наркотическими средствами представляют весьма узкую направленность и постоянно обновляются, в связи с чем представляется актуальным анализ соответствующих тематических сетевых ресурсов, являющихся площадкой общения заинтересованных пользователей.

- кросспосты – публикация на различных интернет-ресурсах однотипных постов. Данный факт может явиться основанием для объединения этих ресурсов и их последующего совокупного анализа.

- общие друзья – анализ контента социальных сетей в совокупности с комментариями на различных тематических интернет-ресурсах, по типу: «см. у NiKa...» поможет вполне точно определить круг общения

- и др.

Причем, анализ активности в сети Интернет покажет максимальную эффективность лишь при работе с множеством источников. Точное их количество, как и степень верификации полученной информации, должен определить человек, осуществляющие его. Для чего активно разрабатывается и внедряется программное обеспечение специального назначения.

Например, на основе технологий искусственного интеллекта создана нейросеть «Товарищ майор». Важнейшей ее функцией является определение владельцев анонимных Telegram-каналов. Кроме того, возможности программы позволяют устанавливать подписи к мультимедиа (сообщениям, в том числе во встроенном чате, стикерпаках, документах и видеороликах, загруженных в сообщество); анализировать контент с информацией о привязанных к профилю пользователя номерах мобильных телефонов, адресах и других цифровых следах; проводить анализ других идентификаторов, а также получать данные из блогах, веб-сайтах и социальных сетей; проверять юридических лиц по их ИНН, аккумулируя из различных источников общую информацию о компании и др.

Очевидно, что платформы Telegram-каналов имеют особую популярность в среде наркобывтчиков. В связи с чем использование подобных программных решений в деятельности правоохранительных органов поднимет результаты противодействия наркопреступности на новый уровень.

Кроме того, ГРЧЦ активно использует систему искусственного интеллекта «Окулус»: автоматическое обнаружение и выделение в общем потоке сведений экстремистского характера, наносящие вред детям, про-наркотический контент, призывы к массовым незаконным мероприятиям, суициду и пропаганду ЛГБТ.¹

Согласно Ведомственной программе цифровой трансформации МВД России на 2023-2025 годы² разработаны проекты технических заданий для подготовки и тестирования систем искусственного интеллекта для нужд МВД.

В данной Программе речь ведется о системах «Клон» (для выявления фактов фальсификации видеоизображений) и «Конъюнктура» (составление прогнозов появления негативных событий и чрезвычайных ситуаций, а также моделирование сценарии реагирования на них). Их внедрение в практическую деятельность планируется уже в 2025 г. Подобные тенденции позволяют ожидать разработки и внедрения систем, задачей функционирования которых будет являться борьба с отдельными видами преступлений. В частности, с незаконным сбытом наркотических средств, совершаемом рассматриваемым способом.

Извлечение данных – в данном случае речь ведется как об извлечении отдельных данных, части системы так и об ее полном извлечении из цифровых устройств: персональных компьютеров, средств мобильной связи, иных

¹ В России запустили систему поиска запрещенного контента в интернете «Окулус»: Известия от 13 февраля 2023 г. – URL <https://iz.ru/1469322/2023-02-13/v-rossii-zapustili-sistemu-poiska-zapreshchennogo-kontenta-v-internete-okulus> (дата обращения: 10.10.2024).

² Об утверждении Ведомственной программы цифровой трансформации МВД России на 2023-2025 годы: Распоряжение МВД России от 25 января 2023 г. № 1/649. Доступ из справочной правовой системы «Гарант».

цифровых устройств – ключевых инструментов рассматриваемой преступной деятельности, и, соответственно, носителей первоначальной криминалистически значимой информации о них.

Для IOS наиболее перспективным представляется использование уязвимостей, например, в цикле обновления операционной системы, а также агентов-экстракторов – специальных приложений, после установки которых открывается доступ к файловой системе, например Elcomsoft iOS Forensic Toolkit.

Способы извлечения данных из устройств Android гораздо шире. Особый интерес представляет собой использование уязвимостей системы. Современная практика открывает обширные возможности извлечения полной файловой системы через Android KeyStore, применения специализированных инструментов для получения root-доступа¹ и извлечения данных и др.

Стоит отметить альтернативный метод – Chip-off, заключающийся в извлечении из одного устройства чипа памяти и в его установке в другое. Как правило, таким образом проводится работа по получению криминалистически значимой информации их неработающих устройств.

Практическими сотрудниками в ходе рассматриваемой деятельности по получению первоначальной криминалистически значимой информации из цифровых устройств активно используется «Мобильный криминалист»². Инструменты весьма универсальны и предназначены для работы с широким спектром мобильных устройств, персональных компьютеров и облачных сервисов. Возможности работы со средством мобильной связи представлены на рисунке.

Функционал данного программного обеспечения представляет весьма широкий спектр возможностей: это не только экспертный анализ цифровых данных, но и аналитические возможности. Например, «Мобильный криминалист Десктоп» предоставляет возможность извлечения данных из систем Windows, macOS, Linux и их последующего анализа посредством разнообразных интегрированных утилит.

Также, имеется ряд альтернативных программных инструментов (Magnet AXIOM, Belkasoft Evidence Center и др.), предоставляющих схожие возможности по извлечению данных из мобильных устройств и жестких дисков.

Анализ метаданных – речь ведется о данных, описывающих непосредственное содержание файла.

Современная классификация метаданных весьма обширна: внутренние, административные, по характеристикам внешних признаков и др.

¹ Возможность получить полный доступ к системным процессам и утилитам на устройстве с операционной системой Android.

² МКО системы. URL.: <https://mko-systems.ru/> (дата обращения 3.10.2014).

Также различаются их форматы: DCMI, MARC, vCard, XML и др., в зависимости от содержания. Упорядочивание метаданных позволяет структурировать информацию, придавая ей целостный вид, провести ее анализ.

Например, веб-приложение DataHub представляет собой открытую платформу для поиска и обнаружения метаданных.

К сожалению, современная практика свидетельствует о недостаточном внимании метаданным, в то время как их анализ окажет содействие в идентификации пользователя информационных систем и технологий, а также позволит составить весьма полное представление о масштабах и участниках преступной деятельности, после проведенного логического анализа полученной информации.

Восстановление удаленных данных – наркосбытчики стремятся к максимальному сокрытию следов своей преступной деятельности. В связи с чем весьма наивно полагать что цифровое устройство, ставшее носителем первоначальной криминалистически значимой информации, сохранит интересующие правоохранные органы сведения в первозданном виде. В связи с чем приобретает особую актуальность восстановление удаленных данных. На самом деле, процесс элементарного удаления цифровой информации, как правило, не всегда предполагает его физическое удаление. А представляет собой выполнение команды «del» в каталоге файла. Кроме того, существует ряд физических причин: от неисправности контроллера до выхода из строя блока магнитных головок (БМГ). В связи с чем современные технологии открывают широкие возможности для восстановления удаленных данных – то есть извлечения удаленных, недоступных, утерянных, поврежденных или форматированных данных из вторичного хранилища, съемных носителей или файлов, когда к хранящимся на них данным невозможно получить доступ обычным способом¹. Для получения первоначальной криминалистически значимой информации о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий разработан и активно используется целый ряд как бесплатного и общедоступного, так и коммерческого программного обеспечения, решающего вопросы разной природы и сложности (Феникс, Recuva, Disk Drill, Pandora recovery, ФотоДОКТОР и др.). Также, зачастую, требуется проведение работ по приведению в рабочее состояние носителя информации.

Получение первоначальной информации из иных источников – деятельность по незаконному сбыту наркотических средств, как было отмечено выше, протекает как в информационном, так и в физическом пространстве, тем самым расширяя перечень носителей криминалистически значимой информации о рассматриваемых преступлениях: видеорегистраторы, БПЛА, камеры наружного наблюдения и др. В связи с чем могут использоваться

¹ Восстановление данных. URL.: https://en.wikipedia.org/wiki/Data_recovery (дата обращения 3.10.2024).

результаты применения иных комплексов, например, разработанных для нужд Министерства Обороны и др.

Например, для контроля аномальных передвижений в наземной и надводной обстановке разработаны мобильные комплексы «Зверобой», «Ратник», «Амулет» – также предполагает и работу с источниками мобильной связи и др.

Казалось бы, не имеющие отношение к правоохранительной деятельности по противодействию незаконному сбыту наркотических средств с использованием информационно-телекоммуникационных технологий сведения, могут быть успешно использованы правоохранительными органами. Полагается, фильтрация такой информации должна происходить согласно заранее разработанным критериям соответствия, определяемым содержанием криминалистической характеристики рассматриваемых преступлений, актуальной в текущий момент с учетом оперативной обстановки в заданном регионе, а их предоставление в рамках межведомственного взаимодействия.

Получение данных наружной фото- видеofиксации (например, в рамках взаимодействия с подразделениями ГИБДД и др., данные системы распознавания лиц и автомобилей – «Следопыт», ПАРСИВ), также позволит, согласно заранее разработанным критериям, получить максимальный объем первоначальной уголовно-релевантной информации о рассматриваемых преступлениях.

Анализ больших данных. Скорость информационного обмена не вызывает сомнений. Структурированную или неструктурированную информацию большого объема недостаточно просто получить, вопрос заключается в ее обработке и в выделении в общем массиве криминалистически значимой. Такая работа требует специальных навыков. Которые, к сожалению, имеются далеко не у всех сотрудников правоохранительных органов. Сегодня данный вопрос настолько актуален, что успешно функционируют отдельные программные продукты и даже целые платформы (например, PolyAnalyst), позволяющие осуществлять анализ больших данных даже непрофессионалам. Посредством передовых алгоритмов машинного обучения и технологий искусственного интеллекта открываются широкие возможности извлечения из объема больших данных криминалистически значимой информации и структурирование полученных результатов в веб-отчеты. Критерии, предъявляемые к полезности информации должны определяться актуальностью криминалистических знаний, так же, как и алгоритмы обучения искусственного интеллекта.

Касаемо введения полученных результатов в процессуальную деятельность вызывают интерес предложения¹ о дополнении перечня мероприятий для документирования исследованием информации, содержащейся в технологических системах ее передачи.

Организационная составляющая – Например, в США действуют такие ведомства, как United States Emergency Computer Readiness Team (Компьютерная команда экстренной готовности США), US Cyber Command (подразделение вооруженных сил, осуществляющее деятельность в киберпространстве), Computer Intellectual and Crime Property Section (подразделение уголовного отдела Министерства юстиции США) и др. – то есть, подразделения, занимающиеся IT-безопасностью и инцидентами, осуществляют свою деятельность в составе большей части силовых ведомств США. В России же относительно недавно создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий в структуре Министерства внутренних дел РФ. Очевидно, введение подобных подразделений в структуру и других силовых ведомств позволит оказывать всестороннее противодействие преступности рассматриваемого вида.

Очевидно, что описанные методы не исчерпывающие и лишь раскрывают в доступной для неспециалиста в данном вопросе форме современные направления получения первоначальной криминалистически значимой информации о рассматриваемых преступлениях.

Широкие возможности работы с цифровой информацией, в форме которой и существует значительная часть первоначальной криминалистически значимой информации о рассматриваемых преступлениях, безусловно, созданы соответствующими специалистами, тем не менее, их использование может быть вполне адаптировано и для непрофессионалов в IT-сфере.

К сожалению, на практике складывается ситуация, что преступность идет в ногу со временем, а правоохранительные органы по ее следам. В связи с чем необходимо постоянное совершенствование криминалистических знаний, внедрение передовых разработок в практическую деятельность, а также аналитическая работа, позволяющая разрабатывать эффективные контрмеры, направленные на опережение преступников.

¹ URL.: <https://www.vedomosti.ru/society/articles/2023/08/16/990319-mvd-rasshiryaet-perechen-operativno-rozisknih-meropriyatii-dlya-dokumentirovaniya-kiberprestuplenii> (дата обращения 13.09.2024).

Вытовтов Александр Евгеньевич,
доцент кафедры оперативно-разыскной
деятельности и специальной техники в ОВД
Восточно-Сибирского института МВД России,
кандидат юридических наук

ОПЕРАТИВНЫЕ ПОДРАЗДЕЛЕНИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ПО БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ КАК НЕЗАИНТЕРЕСОВАННЫЙ СУБЪЕКТ ПРЕДУПРЕЖДЕНИЯ ТАКИХ ПРЕСТУПЛЕНИЙ

Экономическая преступность привлекает к себе внимание не только ученых-исследователей, но также журналистов и общественных деятелей различных категорий. Обусловлено это, на наш взгляд, тем, что финансовая составляющая как результат таких противоправных деяний нередко выражается в крупных денежных суммах (добытых по – мнению некоторых граждан ловким способом). Мы считаем, что подход к предупреждению экономических преступлений существенно различается в зависимости от охраняемых Уголовным кодексом Российской Федерации общественных интересов. Так, преступления, где потерпевшим является государство, как правило, имеют более латентный характер, в отличие от преступлений, где ущерб причиняется крупным корпорациям, различным субъектам предпринимательской деятельности, собственности граждан и т. д.

В августе 2023 года Приказом МВД России № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений»¹ (далее – Приказ № 619) был отменен ранее действовавший Приказ МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений». Представляется, что одной из основных отличительных черт нового приказа является постановка во главу угла профилактики правонарушений различными методами, в том числе и оперативно-розыскными, а именно, как указано в пункте 4.3.1 Приказа № 619: «Использование результатов оперативно-розыскной деятельности о лицах, намеревающихся совершить преступление либо подготавливающих его совершение, с целью недопущения его совершения», при этом реализовываться указанное предписание должно с учетом ст. ст. 11–12 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее – Закон «Об ОРД»).

¹ Приказ от 24 августа 2023 г. № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений» // СТРАС «Юрист» (дата обращения: 10.10.2024).

Следует отметить, что Приказ № 619 в правовом плане соотнесен с Федеральным законом от 23 июня 2016 года № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»¹ (далее – Закон № 182-ФЗ), и это, на наш взгляд, положительно отличает его от Приказа МВД России от 17 января 2006 г. № 19, утратившего свою силу.

Также в Приказе № 619 определены субъекты ведомственной системы профилактики – это «подразделения центрального аппарата МВД России, территориальные органы МВД России и организации, созданные для выполнения задач и осуществления полномочий, возложенных на органы внутренних дел Российской Федерации». Эта деятельность регулируется Приказом МВД России от 29 сентября 2022 г. № 715 «Об организационных вопросах профилактики правонарушений в системе МВД России», в соответствии с которым общим координатором является оперативный штаб Министерства внутренних дел Российской Федерации по профилактике правонарушений².

При этом хотелось бы отметить некоторое разночтение между целями профилактики правонарушений и выполнением основных показателей территориальными оперативными подразделениями экономической безопасности и противодействия коррупции (далее – ОЭБиПК) при выполнении задач по выявлению, предупреждению, пресечению и раскрытию преступлений экономической и коррупционной направленности, а также выявлению и установлению лиц, их подготавливающих, совершающих или совершивших³.

Так, согласно п. 1 ст. 2 Закона № 182-ФЗ, «правонарушение – это преступление или административное правонарушение, представляющие собой противоправное деяние (действие, бездействие), влекущее уголовную или административную ответственность». В п. 2 ст. 2 указанного Закона дается понятие профилактики правонарушений – «это совокупность мер социального, правового, организационного, информационного и иного характера,

¹ Об основах системы профилактики правонарушений в Российской Федерации : Федер. закон № 182-ФЗ (в послед. ред.) : принят Гос. Думой 10 июня 2016 года : одобрен Советом Федерации 15 июня 2016 года // КонсультантПлюс : сайт. URL: <http://172.30.6.144/cons/cgi/online.cgi?req=doc&ts=DIkxywTRKixRwzw5&cacheid=A93BC23815B952714199666B42EE4224&mode=splus&rnd=0.16181800315595507&base=LAW&n=199976#ELsRzwTq0FedKPul> (дата обращения: 21.09.2024). Режим доступа: для зарегистрированных пользователей.

² Об организационных вопросах профилактики правонарушений в системе МВД России : приказ МВД России от 29 сентября 2022 г. № 715 // СТРАС «Юрист» (дата обращения: 10.10.2024).

³ Об утверждении Типового положения о подразделении экономической безопасности и противодействия коррупции территориального органа МВД на региональном уровне и о внесении изменений в Положение о Главном управлении экономической безопасности и противодействия коррупции Министерства внутренних дел Российской Федерации, утвержденное приказом Министерства внутренних дел Российской Федерации от 16 марта 2015 г. № 340 : приказ МВД России от 06.06.2017 № 363 // СТРАС «Юрист» (дата обращения: 20.09.2024).

направленных на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения совершения правонарушений». Бесспорно, профилактика преступлений имеет огромное значение для социально здорового функционирования общества, но подход к ней не может быть односторонним, и наличие управленческих решений не означает их автоматического выполнения теми субъектами, которым они предписаны. В частности, меры профилактики правонарушений оперативно-розыскными методами, обозначенные в Приказе № 619, должны основываться на результатах оперативного подразделения ОЭБиПК по выполнению показателей по выявлению и раскрытию преступлений. Но, исходя из этих показателей, оперативным сотрудникам нет необходимости применять меры, направленные на выявление и устранение причин и условий, способствующих совершению правонарушений, а также на оказание воспитательного воздействия на лиц в целях недопущения антиобщественного поведения или совершения правонарушений. В системе оценки и организационных форм работы предпочтение отдается оперативно-розыскному направлению, что, во-первых, вступает в противоречие с задачами криминологического характера, а во-вторых – ведет к отсутствию личного и коллективного интереса достижения цели.

Так, Приказ МВД России от 28 февраля 2012 года № 134 «О статистической отчетности органов внутренних дел Российской Федерации»¹ предусматривает несколько форм статистической отчетности:

- Оперативная статистическая информация о состоянии преступности и результатах выявления и раскрытия преступлений;
- Отчет о результатах работы подразделений экономической безопасности и противодействия коррупции органов внутренних дел Российской Федерации;
- Отчет о результатах работы по защите средств федерального бюджета, направленных на реализацию приоритетных национальных проектов;
- Отчет о преступлениях, совершенных иностранными гражданами и лицами без гражданства, а также в отношении них;
- Отчет о результатах деятельности органов внутренних дел Российской Федерации по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, а также результатах деятельности структурных подразделений органов внутренних дел Российской Федерации, специализирующихся на противодействии преступлениям данного вида.

¹ О статистической отчетности органов внутренних дел Российской Федерации : приказ МВД России от 28.02.2012 № 134 // СТРАС «Юрист» (дата обращения: 20.09.2024).

Как мы видим, предметный отчет о профилактической деятельности отсутствует, и во главу поставлены конкретные результаты территориальных оперативных подразделений ОЭБиПК. Согласно отчету о результатах работы подразделений экономической безопасности и противодействия коррупции органов внутренних дел Российской Федерации формы «5-БЭП», уделяется внимание выявленным преступлениям, следствие по которым обязательно, сведениям о причиненном материальном ущербе и изъятых предметах преступной деятельности. Необходимо отметить и Приказ МВД России от 31 декабря 2013 г. № 1040 «Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации»¹, который содержит инструкцию по оценке деятельности различных подразделений МВД России и в котором присутствуют оценочные категории, касающиеся предупреждения и пресечения преступлений (но они также не являются профилактическими, а формируются за счет лиц, подпадающих под надзор или состоящих под административным надзором), несовершеннолетних, доли преступлений, выявленных сотрудниками органов внутренних дел на стадии приготовления или покушения, и т. д.

Также необходимо обратить внимание на рациональное использование результатов оперативно-розыскной деятельности при профилактике правонарушений. Представляется, что в этом случае полученные по итогам проведенных оперативно-розыскных мероприятия сведения должны анализироваться на предмет имеющихся устойчивых связей фигурантов, механизмов, способов, мотива совершения противоправного деяния, алгоритма сокрытия следов преступления, с тем чтобы выяснить эти самые причины и условия совершения правонарушений с целью дальнейшего влияния на них и минимизации возможностей для совершения противоправных деяний. Но учитывая негласный характер оперативно-розыскной деятельности, проведение такого анализа представляется затруднительным и нецелесообразным для сотрудника оперативного подразделения, осуществляющего оперативную работу по данному преступлению, т. к. его задача – выявить, раскрыть преступление и заработать необходимую оценочную позицию в статистическом отчете.

Таким образом, можно констатировать, что оперативные подразделения, компетенцией которых является борьба с преступлениями в сфере экономики и коррупции, не являются полноценными субъектами по выполнению задачи предупреждения преступлений соответствующей направленности. На это обращает внимание Е.В. Кузнецов, отмечая, что органы, осуществляющие оперативно-розыскную деятельность при выполнении задач по предупреждению преступлений (буквально истолковывая ряд положений Закона «Об ОРД»), не всегда имеют право на проведение оперативно-

¹ Вопросы оценки деятельности территориальных органов Министерства внутренних дел Российской Федерации : приказ МВД России от 31.12.2013 № 1040 : послед. ред. // СТРАС «Юрист» (дата обращения: 20.09.2024).

розыскных мероприятий в целях решения указанных задач, и констатирует, что оперативные подразделения практически лишены возможности предупредить замышляемые преступления¹. Кроме того, В.Д. Ларичев и В.Д. Исаев указывали на это еще в 2010 году: «...оперативные подразделения предназначены в основном для выявления и раскрытия преступлений, а не для их предупреждения. О несоответствии задач предупреждения преступлений в сфере экономики реальному положению дел свидетельствует и тот факт, что, несмотря на наличие таких задач, деятельность по предупреждению преступлений в сфере экономики не входит в показатели оценки деятельности подразделений органов милиции и оперативных подразделений»².

На основании вышеизложенного считаем, что необходимо менять вектор правоохранительной деятельности в этой сфере и уделять больше внимания работе по предупреждению экономических преступлений, особенно в сфере деятельности государства и муниципалитетов по формированию и удовлетворению государственных и муниципальных нужд, реализации национальных проектов, т. к. эффективный контроль за расходованием бюджетных денежных средств без участия оперативно-розыскной деятельности невозможен.

В связи с этим для устранения указанных выше сдерживающих факторов можно предложить дополнительно внести в оценочные индикаторы показатели по итогам работы аппаратов по борьбе с экономическими и коррупционными преступлениями, отражающие деятельность сотрудников соответствующих оперативных подразделений по профилактике, предупреждению экономических и коррупционных преступлений. Активизирующая роль этих показателей может проявить себя при адекватной оценке деятельности сотрудника или оперативного подразделения.

Конечно, учитывая тяжелое кадровое положение в системе МВД России, такие предложения могут показаться фантастическими, но современная экономико-политическая ситуация в нашей стране и имеющиеся нормативные правовые акты призывают обеспечить сохранность финансовых и материальных ценностей. Предлагаемые нами меры могут избавить следственные органы от раскрытия сложных, многоэпизодных уголовных дел и причинения ущерба как государству, так и гражданам. Достижение таких результатов вполне возможно при условии повышения уровня подготовки кадров для достижения обозначенных целей, разработки методик аналитической работы в этом направлении с намерением применения такого подхода в деятельности оперативных подразделений экономической безопасности и противодействия коррупции.

¹ Кузнецов, Е. В. Предупреждение преступлений органами, осуществляющими оперативно-розыскную деятельность: проблемы теории и практики // Вестник Восточно-Сибирского института МВД России. 2011. № 4 (59). С. 45–52.

² Ларичев, В. Д., Исаев, О. Ю. Понятие и характеристика основных субъектов предупреждения преступлений в сфере экономики в современных условиях // Общество и право. 2010. № 1 (28). С. 198–208.

Глубоковских Роман Владимирович,
преподаватель кафедры ОРД ОВД Калининградского филиала
Санкт-Петербургского университета МВД России,
кандидат юридических наук

Денищик Александр Юрьевич,
курсант 4 курса
Калининградского филиала
Санкт-Петербургского университета МВД России

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ОТОЖДЕСТВЛЕНИЯ ЛИЧНОСТИ В РОЗЫСКНОЙ РАБОТЕ ПОДРАЗДЕЛЕНИЙ УГОЛОВНОГО РОЗЫСКА

Биометрия, в качестве метода идентификации личности, основывается на уникальных биологических или поведенческих характеристиках, на это в своей работе обращала внимание Кисиль Т.В.¹. В анализе О. Петровой и А. Райляна представлена детальная статистика по распределению биометрических методик в зависимости от уровня их распространенности². Системы идентификации по отпечаткам пальцев доминируют, занимая 59% от общего объема. Технологии распознавания по геометрии лица и идентификация по радужной оболочке глаза составляют 17% и 7% соответственно. Методика идентификации по геометрии руки, рисунку вен ладони или пальца руки, а также идентификация по голосу показывают приблизительно одинаковые результаты на уровне 7%. Интересным является факт, что идентификация по почерку занимает всего 1% от общего объема, в то время как остальные методики, такие как идентификация по сетчатке глаза, ДНК, термограмме лица, форме ушных раковин, запаху, клавиатурному почерку и анализ биоэлектрической активности головного мозга, также составляют лишь 1% от общего распределения биометрических методов.

Перспективы использования биометрических данных при розыске человека в деятельности уголовного розыска представляют собой значительный шаг в направлении эффективного и точного выявления личности. Применение отпечатков пальцев, распознавания лица, голоса и других биометрических параметров позволяет ускорить процесс идентификации, сократить ошибки и повысить точность результатов.

¹ Кисиль, Т. В. Особенности проведения оперативно-розыскного отождествления личности / Т. В. Кисиль // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2024. – № 1(75). – С. 70-74. – EDN WQVYYM.

² Петрова О., Райлян А. Обзор существующих методов биометрической идентификации // Безопасность для всех: [сайт]. 29.01.2012. URL: <http://www.sec4all.net/modules/myarticles/article.php?storyid=1265> (дата обращения: 04.11.2023).

Идентификация по отпечаткам пальцев, геометрии лица и радужной оболочке глаза, обозначаемая как «три большие биометрики», представляет собой эффективные методы подтверждения личности. Оценка надежности этих методов осуществляется через показатели FAR (False Acceptance Rate – вероятность ошибочного пропуска) и FRR (False Rejection Rate – вероятность ошибочного отклонения).

В контексте идентификации по отпечаткам пальцев, FAR варьируется от 0,1 до 0,001%, а FRR – от 0,3 до 0,9%. Метод идентификации по геометрии лица, используя два измерения, имеет FAR от 0,1 до 0,001%, а FRR – от 2,5 до 9,0%; при использовании трех измерений FAR составляет 0,0047%, а FRR – 0,103%. Для метода идентификации по радужной оболочке FAR составляет 0,00001%, а FRR – 0,13%. Идентификация по радужной оболочке глаза считается наиболее надежным методом.

Тем не менее, несмотря на высокую надежность, не все методы равнозначны в плане удобства для пользователей. По мнению О.В. Дубчака, системы идентификации по отпечаткам пальцев могут вызывать беспокойство в плане гигиеничности, а идентификация по радужной оболочке глаза может быть неудобной из-за требований к движениям и видимости глаза. Автор считает, что распознавание по лицу и голосу более предпочтительны благодаря дистанционности и отсутствию строгих требований к позиционированию пользователя.

Для бесконтактной идентификации личности на расстоянии, оптимальным методом служит распознавание по геометрии лица. Этот подход широко применяется в системах интеллектуального видеонаблюдения правоохранительных органов, чей объем внедрения постоянно расширяется. Анализируя плюсы и минусы метода распознавания по радужной оболочке глаз, можно выделить его потенциал в обеспечении информационной безопасности правоохранительных органов, ставя его в сравнение с дактилоскопической идентификацией.

Эффективность этих методов идентификации проявляется в их способности успешно выявлять лиц, связанных с актами терроризма, и предотвращать их международное перемещение.

Тем не менее, необходимо отметить общий недостаток данных методов – увеличение случаев взлома систем, обеспеченных биометрическими технологиями. Это поднимает вопросы безопасности и выдвигает требование по постоянному совершенствованию систем защиты для противостояния современным угрозам в области кибербезопасности.

Отметим важные аспекты обмана систем распознавания лица, включая сценарии использования фотографий или изображений на экране устройств. Приведем пример, где некоторые системы, работающие на платформе Android и предназначенные для контроля доступа, подвержены обману при направлении телефона или планшета на фотографию или видеозапись истинного владельца.

Во многих ноутбуках с встроенными веб-камерами применяется аутентификация с использованием систем распознавания лиц. Исследователи из Вьетнама продемонстрировали обход защитных программ, таких как Lenovo Veriface III, Asus SmartLogon версии 1.0.0005 и Toshiba Face Recognition 2.0.2.32. Этот обход осуществлялся путем систематического перебора изображений с различными типами лиц и фотографий владельца ноутбука.

Также документированы случаи обмана систем идентификации по радужной оболочке глаза при использовании цветных фотографий глаза.

В контексте противодействия обману биометрических систем предлагается наличие оператора, контролирующего процесс идентификации. Однако в ситуациях, где оператор не присутствует, требуется, чтобы сама система способна автономно различать биометрические характеристики человека от муляжа. Это включает в себя регистрацию дополнительных признаков, подтверждающих истинность идентификации.

Применение многофакторной биометрии, объединяющей широко используемые методы с менее распространенными, представляет собой эффективный подход для предотвращения использования муляжей вместо реальных биометрических данных. Этот метод добавляет дополнительный уровень безопасности, учитывая, что подделать одну характеристику гораздо проще, чем две или более.

Биометрические технологии способствуют улучшению работы правоохранительных органов, обеспечивая более оперативное реагирование на преступления и поиск преступников. Возможность интеграции биометрических данных с базами данных о преступлениях и ранее установленными профилями лиц позволяет улучшить систему розыска и обеспечить более эффективное сотрудничество между различными службами.

Однако, внедрение таких технологий также вызывает вопросы о конфиденциальности и защите данных. Необходимо разработать строгие нормы и механизмы контроля, чтобы предотвратить возможное злоупотребление и обеспечить соблюдение прав граждан.

Таким образом, использование биометрических данных при розыске человека в оперативно-розыскной деятельности обещает значительное улучшение эффективности и точности идентификации, но требует внимательного внедрения с соблюдением принципов законности и приватности¹.

В контексте уголовного розыска, биометрические технологии могут быть весьма полезными для идентификации и розыска лиц, представляющих интерес для правоохранительных органов. Ниже представлены несколько способов использования биометрии в уголовном розыске:

¹ Бекмурзин М.С., Захаров В.П., Зачек О.И. Биометрические технологии в антитеррористической деятельности правоохранительных органов: перспективы и проблемы использования // Вестник Московского университета МВД России. 2014. №10. С.44.

1. Идентификация по отпечаткам пальцев:
 - Воспользоваться системами идентификации по отпечаткам пальцев для сопоставления с имеющейся базой данных.
 - Применять портативные устройства для сбора отпечатков на месте происшествия и последующей отправки в базу данных для анализа.
2. Распознавание по геометрии лица и радужной оболочке глаза:
 - Использовать системы распознавания по геометрии лица для анализа фотографий и видеоматериалов с камер наблюдения в общественных местах.
 - В случаях, когда доступны биометрические данные, применять идентификацию по радужной оболочке глаза для более точного сопоставления.
3. Идентификация по голосу:
 - Использовать технологии идентификации по голосу для анализа аудиозаписей, если доступны голосовые данные подозреваемого.
4. Комбинированный подход многофакторной биометрии:
 - Применять многофакторную биометрию, комбинируя различные методы, например, идентификацию по отпечаткам пальцев и распознавание по лицу, для увеличения точности идентификации.
5. Автоматизированный поиск в базах данных:
 - Разрабатывать и использовать специализированные программы для автоматического поиска и сопоставления биометрических данных с базами данных правоохранительных органов.

Важно отметить, что при использовании биометрии в уголовном розыске следует соблюдать принципы конфиденциальности и обеспечивать высокий уровень безопасности для предотвращения возможных злоупотреблений и утечек информации.

В уголовном розыске использование биометрии на основе данных видеосъемки может быть эффективным инструментом для идентификации и поиска подозреваемых. Вот несколько способов, как это можно реализовать:

1. Распознавание по лицу:
 - Применение систем распознавания лиц для анализа видеоматериалов с камер наблюдения в общественных местах.
 - Интеграция технологий, способных выявлять и сопоставлять характерные черты лица подозреваемого с данными из базы лиц.
2. Идентификация по движению:
 - Анализ видеопотока для выделения уникальных характеристик движения подозреваемого.
 - Использование алгоритмов машинного обучения для сопоставления этих характеристик с предварительно обученной базой данных.
3. Распознавание по уникальным чертам:
 - Использование биометрии на основе уникальных черт, таких как татуировки, родинки, шрамы, которые могут быть выявлены на видеозаписях.

– Разработка программ, способных автоматически выделять и сопоставлять эти уникальные черты.

4. Интеграция с другими биометрическими методами:

– Комбинирование данных видеосъемки с другими биометрическими методами, такими как идентификация по отпечаткам пальцев или голосу, для повышения точности.

5. Системы массового распознавания:

– Развитие систем массового распознавания, способных быстро анализировать видеопотоки на территории города и выявлять подозреваемых.

Важно соблюдать принципы конфиденциальности и обеспечивать высокий уровень безопасности при использовании биометрии на основе видеосъемки. Также необходимо учитывать правовые нормы и регулирования, чтобы избежать возможных нарушений прав граждан.

Итак, биометрические технологии представляют собой значительный потенциал для эффективного использования в уголовном розыске. Можно сделать следующие выводы:

1. Распределение методик биометрии:

– Отпечатки пальцев, геометрия лица и радужная оболочка глаза занимают ведущие позиции среди биометрических методов.

2. Надежность и точность:

– Методы биометрии, особенно идентификация по радужной оболочке глаза, обладают высокой надежностью и точностью, что делает их перспективными для использования в правоохранительной деятельности.

3. Проблемы безопасности:

– Возрастающие случаи взлома биометрических систем подчеркивают необходимость постоянного совершенствования методов защиты и обеспечения безопасности данных.

4. Применение в уголовном розыске:

– Биометрия, основанная на видеосъемке, может эффективно использоваться в уголовном розыске для идентификации и поиска лиц, включая распознавание по лицу, уникальным чертам и движению.

5. Многофакторная биометрия:

– Комбинация различных методов биометрии, известная как многофакторная биометрия, может усилить точность и надежность идентификации, снижая вероятность обмана.

6. Соблюдение правовых норм и этических принципов:

– При внедрении биометрических технологий в уголовный розыск необходимо строго соблюдать правовые нормы, обеспечивать конфиденциальность данных и соблюдать этические принципы.

В целом, биометрия представляет собой мощный инструмент для улучшения эффективности уголовного розыска, но ее внедрение требует баланса между инновацией и защитой личных данных, а также постоянного совершенствования средств защиты от возможных угроз.

Гора Евгений Викторович,
преподаватель кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Маркарова Анастасия Маратовна,
курсант 3 курса
Краснодарского университета МВД России

МЕДИЦИНСКИЕ КАРТЕЛИ КАК НАИБОЛЕЕ ОПАСНАЯ ФОРМА ОРГАНИЗОВАННОЙ КОРРУПЦИОННОЙ ПРЕСТУПНОСТИ

Коррупция является социально-негативным и разноплановым явлением, которое охватывает практически все сферы деятельности человека и приносит ущерб общественным интересам, экономике страны и гражданам. Она является одной из основных угроз государственной безопасности. Коррупция как явление криминальное связана с экономическими процессами. В экономической сфере коррупция включает в себе различные преступления. Она приводит к разрушению экономики и превращает государственный аппарата в инструмент удовлетворения частных экономических потребностей. А это, в свою очередь, способствует развитию теневого сектора, повышению уровня криминализации общества.

В уголовном законе коррупция является собирательным составом, охватывающим ряд должностных преступлений. Это взяточничество, злоупотребление служебными полномочиями и др. Коррупция проявляется в совершении преступлений соответствующей направленности: хищение материальных и денежных средств с использованием служебного положения, дача взятки, получение взятки, коммерческий подкуп¹ и т.д.

Наиболее полный перечень и признаки преступлений коррупционной направленности содержатся в совместном Указании Генпрокуратуры России № 35/11 и МВД России № 1 от 24.01.2020 «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» (перечень № 23), в который включены (с разного рода оговорками) 52 вида преступлений, а также в Приказе Генпрокуратуры России от 26.12.2013 № 553 «Об утверждении формы федерального статистического наблюдения № 1-КОРР», используемого в целях организации федерального статистического наблюдения за работой правоохранительных органов по борьбе с коррупционными преступлениями.

¹ Лекционный материал на тему: «Коррупция (понятие, ответственность, противодействие коррупции)» // Моя школа URL: https://mouschool2.moy.su/lekcija_korrupcija.pdf (дата обращения: 28.11.2024).

К преступлениям коррупционной направленности относятся противоправные деяния, имеющие все перечисленные ниже признаки:

- наличие надлежащих субъектов уголовно наказуемого деяния;
- связь деяния со служебным положением субъекта, отступлением от его прямых прав и обязанностей;
- обязательное наличие у субъекта корыстного мотива, получения имущественных прав и выгод;
- совершение преступления только с прямым умыслом.¹

Чтобы преступления можно было отнести к категории преступлений коррупционной направленности, помимо конкретно указанных, в перечне предусматривается наличие определенных условий.

Коррупционные преступления включают случаи, когда должностные лица или управляющие организации создают условия для получения незаконных выгод, что отражается в ст. 178 УК РФ, касающейся ограничения конкуренции.

Период	Правоохранительными органами по ст. 178 УК РФ		Подразделениями ЭБиПК ОВД РФ по ст.178 УК РФ		Подразделениями ЭБ и ПК ОВД РФ по ст.178 УК РФ, связанных с коррупцией	
	Возбуждено уголовных дел	Направлено в суд	Выявлено преступлений	Возбуждено уголовных дел	Возбуждено уголовных дел	Направлено в суд
2020	0	0	0	0	0	0
2021	1	1	1	1	1	1
2022	2	2	2	2	2	2

Уголовная практика по статье 178 УК РФ

Таким образом, общие сведения о состоянии преступности за отчетный период говорят о росте указанных общественно опасных деяний, но в общей структуре преступлений занимают незначительное место.

Статистика результатов работы подразделений ЭБиПК органов внутренних дел Российской Федерации свидетельствует о тенденции к наращиванию выявленных и возбужденных уголовных дел, связанных с ограничением конкуренции. Надо отметить, что все зарегистрированные преступления совершены в особо крупном размере. Количество же преступлений, связанных с коррупционными проявлениями, предусмотренных статьей 178 УК РФ, носят практически нулевые показатели.

¹ ПЕРЕЧЕНЬ № 23 преступлений коррупционной направленности // Судебные и нормативные акты РФ URL: <https://sudact.ru/law/ukazanie-genprokuratury-rossii-n-1111-mvd-rossii/prilozhenie/perechen-n-23-prestuplenii-korrupsionnoi/> (дата обращения: 27.11.2024).

Коррупционные проявления всегда возникают там, где есть доступ к деньгам. Часто это проявляется в случаях сговора на торгах, при проведении государственных закупок. Антиконтурентные соглашения в сфере государственной торговли, в которых участвуют хозяйствующие субъекты, а также государственные органы и должностные лица в целях извлечения личной или групповой выгоды – частое явление в правоохранительной сфере. Свыше 80% картелей – это сговоры на торгах, в которых обязательно покровительство заказчика, либо организаторов торгов, а картельная сверхприбыль, в свою очередь, приводит к появлению коррупции.

По оценкам экспертов, ущерб от антиконкурентных соглашений на товарных рынках и торгах составляет 1,5-2% от размера ВВП ежегодно, завышение цен в случае картелей на торгах достигает 30% от начальной стоимости предмета торгов, завышение цен картелями на товарных рынках составляет 18%, трансграничными, международными картелями – 23%.¹ По оценке ФАС России, общий доход, извлеченный компаниями в результате участия в картеле, составил свыше 800 млн рублей.

Многомиллиардные картели в сфере государственных закупок, создаваемые должностными лицами органов государственной власти – крайне опасная форма организованной преступности, поскольку:

- способствует тенденциям монополизма в экономике;
- нарушает механизм рыночной конкуренции;
- приводит к нецелевому разделу денежных поступлений и финансов бюджета страны;
- мешает успешному осуществлению программ Правительства РФ и национальных проектов;
- формирует теневую экономику и криминализацию общества;
- посягает на интересы государственной службы;
- является источником финансовой подпитки коррупции и т.д.

В соответствии с Указом Президента РФ от 13.05.2017 г. №208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года», одной из основных задач по реализации направления, касающегося развития системы государственного управления, прогнозирования и стратегического планирования в сфере экономики является совершенствование механизмов бюджетного планирования, осуществления контроля в сфере закупок для государственных и муниципальных нужд, предотвращение картельных сговоров.

Определение понятия «картель» содержится в ст.11 ФЗ от 26.07.2006 года № 135-ФЗ «О защите конкуренции» (соглашение между хозяйствующими субъектами – конкурентами, то есть между хозяйствующими субъектами, осуществляющими продажу товаров на одном товарном рынке, или

¹ ФАС в СМИ: Картельная партия ФАС // ФАС России URL: <https://fas.gov.ru/publications/13498> (дата обращения: 27.11.2024).

между хозяйствующими субъектами, осуществляющими приобретение товаров на одном товарном рынке, если такие соглашения приводят или могут привести к перечисленным в ч. 1 данной статьи последствиям, в том числе к повышению, снижению или поддержанию цен на торгах).

Данный Федеральный закон предусматривает деление сговора на торгах:

- на картели на торгах;
- ограничивающие конкуренцию соглашения организатора (заказчика) и участника торгов, что является нарушением ст. 16 и п.1 ст.17 Закона о защите конкуренции. Такие сговоры отличаются высокой степенью коррупционной составляющей, поскольку, являясь коррупционным преступлением, сопровождаются другими преступлениями подобной направленности.

При данных условиях уголовно-правовая квалификация может даваться одновременно по разным статьям УК РФ – 159 («Мошенничество»), 285 («Злоупотребление должностными полномочиями»), 285.1 («Нецелевое расходование бюджетных средств»), 286 («Превышение должностных полномочий»). Задействование в сговоре должностных лиц часто сопровождается совершением ими иных должностных преступлений – получения взятки, служебного подлога.

Во всех отраслях экономики России картели получили широкое распространение, в частности, в стратегически важных и социально значимых, таких как медицина.

В данный момент объем фармацевтического рынка Российской Федерации можно оценить приблизительно в 1,5 триллиона рублей. Около 300-400 миллиардов из указанной суммы осваивается за счёт бюджетных средств. Все остальное – розничный рынок. Доля закупаемых для государственных нужд лекарственных препаратов составляет около 30% во всем объеме реализуемых на территории страны лекарств, поэтому формирование цен при государственных закупках оказывает существенное влияние на экономику отрасли в целом.

Главное негативное последствие сговоров на торгах – увеличение бюджетных расходов в связи с отсутствием реальной конкуренции на аукционах и конкурсах.¹

Картели в сфере здравоохранения и снабжения населения медикаментами наносят серьезный ущерб как государственному бюджету, так и гражданам страны. Государство вынуждено финансировать расходы на социальные нужды, привлекая дополнительные средства, однако эти деньги уходят «на картели» и не позволяют сфере развиваться. Из-за антиконкурентных соглашений с заказчиками бюджетные средства расходуются нецелевым образом. Участники картеля не заинтересованы в качестве приобретаемой

¹ Статья Дмитрия Артюшенко «Роль конкурентного ведомства в борьбе с коррупцией и хищениями на торгах» // ФАС России URL: <https://fas.gov.ru/documents/561857> (дата обращения: 27.11.2024).

продукции. Это приводит к негативным последствиям в отрасли и уровне услуг, которые предоставляются гражданам.

«Картель на торгах ведет к тому, что цена не снижается, экономии нет, страдают добросовестные участники рынка, а при условии сговора с заказчиком, в цену закладываются и коррупционные расходы», – отметил начальник Управления по борьбе с картелями, Андрей Тенишев, на региональном семинаре-совещании в г. Калуга.¹

Рассмотрим некоторые дела о сговорах на торгах. Чиновники вступили в сговор с коммерсантами с целью ограничения конкуренции и обеспечения победы на торгах определенных компаний.

Так, Прокуратура Республики Саха (Якутия) совместно с ЭБиПК МВД по Республике Саха (Якутия) и УФАС по Республике Саха (Якутия) провела проверку на соблюдение законодательства в сфере закупок.

По результатам проверки были выявлены факты мошенничества и картельного сговора среди руководителей коммерческих организаций, зарегистрированных в регионе, при заключении госконтрактов с медицинскими учреждениями на поставку лекарственных препаратов и медицинских изделий.

Общая сумма заключенных контрактов с представителями картеля и их аффилированными лицами, составила около 3 миллиардов рублей.² По данным прокуратуры, в ряде случаев цены закупок превышали розничные цены в 2-4 раза. При этом представители медицинских учреждений сотрудничали с картелем в целях ограничить конкуренцию и устранить возможных соперников на торгах.

На основании рассмотренных материалов следственные органы возбудили уголовные дела по признакам состава преступлений, предусмотренных п. п. «а», «в» ч.2 ст. 178 («Ограничение конкуренции») и ч. 4 ст.159 УК РФ («Мошенничество»)

Еще одно преступление было зафиксировано Комиссией Санкт-Петербургского УФАС России, которая выявила картельное соглашение в действиях тринадцати компаний. Эти организации участвовали в более чем 200 торгах на поставку медикаментов и расходных материалов для бюджетных медучреждений Санкт-Петербурга в период с 2015 по 2018 годы.

В ходе расследования по делу было установлено, что компании, участвуя в электронных торгах, использовали одни и те же IP-адреса, а иногда

¹ Андрей Тенишев о снижении количества дел по «мелким» картелям и контроле за нацпроектами // ФАС России URL: <https://fas.gov.ru/news/27948> (дата обращения: 25.11.2024).

² В Якутии по материалам проверки прокуратуры возбуждены уголовные дела по факту картельного сговора и мошенничества в особо крупном размере // Прокуратура Республики Саха(Якутия) URL: https://epp.genproc.gov.ru/web/proc_14/mass-media/news?item=7198017 (дата обращения: 25.11.2024).

одновременно изменяли их. Конкуренты имели общих сотрудников, использовали одну инфраструктуру и вели совместную хозяйственную деятельность.

Также было установлено, что эти организации следовали заранее согласованной модели поведения, что исключало конкуренцию и способствовало поддержанию высоких цен на закупки.

Более того, стал известным тот факт, что сговор зарождался еще на этапе момент предоставления коммерческих предложений бюджетным организациям, что приводило к увеличению начальной (максимальной) цены контракта в два раза. Участники картеля для получения сверхприбыли снижали цену во время торгов незначительно - от 0,5% до 1,5%.

Суммарная прибыль «медицинского» картеля в Санкт-Петербурге превысила 849 миллионов рублей. Поскольку действия компаний содержат признаки преступления, предусмотренного п. «в» ч.2 ст.178 УК РФ, Санкт-Петербургское УФАС передало материалы дела в УЭБиПК МВД России по Санкт-Петербургу и Ленинградской области.

Подчеркивая коррупционную составляющую картелей и сговоров на торгах, на сегодняшний день можно отметить активное участие государственных органов и служащих в таких правонарушениях, включая преступления, направленные на сокрытие и поддержку антикоррупционных соглашений. Часто антиконкурентные соглашения сопровождаются коррупционным покровительством со стороны властей.

Общественная опасность антиконкурентных соглашений, в которых участвуют государственные служащие, очень высока, так как вред причиняется не только свободной конкуренции, но и интересам государственной службы.¹

Также характеризуя современные картели на фоне достаточно высокого уровня латентности, данные правонарушения стали многоэпизодными, продолжительными и детально планируемыми, а сами картели – высокоорганизованными и структурированными группами, имеющими все признаки организованной преступной группы и преступного сообщества.²

При этом нет ни одного дела, связанного с организацией преступного сообщества (преступной организации), или участием в нем (ст. 210 УК РФ), которое было создано с целью заключения картельных соглашений, относящихся к категории тяжких преступлений (ч. 2 и 3 ст. 178 УК РФ).

¹ Правительство утвердило межведомственную программу мер по выявлению и пресечению картелей // ФАС России URL: <https://fas.gov.ru/news/27902> (дата обращения: 27.11.2024).

² Правительство утвердило межведомственную программу мер по выявлению и пресечению картелей // ФАС России URL: <https://fas.gov.ru/news/29307> (дата обращения: 27.11.2024).

Поэтому, учитывая повышенную общественную опасность и наличие признаков организованной преступности, в статью 178 УК РФ целесообразно ввести отдельным подпунктом такой квалифицирующий признак, как совершение преступления посредством ОПГ.

Также наказание, предусмотренное санкцией статьей 178 УК РФ (в виде штрафа от 300 до 500 тыс. рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до двух лет) несоразмерно с тяжестью преступления (сумма крупного ущерба составляет 10 млн рублей, а сумма крупного дохода 50 млн рублей), что также требует корректировки.

Возможно, будет правильным выделить в отдельную статью преступления, связанные с ответственностью за сговор при проведении торгов, в том числе в качестве квалифицированного состава выделить сговор при проведении торгов по государственным контрактам.

Видится необходимым ужесточить уголовную ответственность должностных лиц, представителей государственного или муниципального заказчика в пределах существующих составов должностных преступлений, и установить специальные составы преступлений таких лиц в УК РФ.

Для результативной работы правоохранительных органов и антимонопольных органов по выявлению и пресечению деятельности картелей важно налаживать устойчивое межведомственное взаимодействие, проводить совместные мероприятия и проверки.

Гора Евгений Викторович,
преподаватель кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Мотрук Кристина Константиновна,
курсант 3 курса
Краснодарского университета МВД России

ПРОВАЙДЕРЫ УСЛУГ ВИРТУАЛЬНЫХ АКТИВОВ И ИХ ПОЛЬЗА ДЛЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

В современном мире, где огромную роль играет стремительный технологический прогресс, большое значение приобретают виртуальные активы, такие как криптовалюта или токены. По мере роста популярности данных активов возникает необходимость в их регулировании. Для этого используются провайдеры услуг виртуальных активов (Далее – VASP). VASP играют важную роль в системе виртуальных активов, предоставляя широкий спектр услуг, включая обмен, хранение и перевод. Провайдеры выступают в роли посредников между пользователями и рынками виртуальных активов и обеспечивают быструю и безопасную обработку транзакций. В научной работе мы рассмотрим, что представляют собой виртуальные активы и их провайдеры, разберем функции.

Под виртуальными активами понимается цифровое выражение ценности, которое может цифровым образом обращаться, переводиться, а также использоваться для различных платежей и инвестиций.

Провайдеры услуг виртуальных активов – это физические или юридические лица, которые осуществляют операции над виртуальными активами.

К таким можно отнести:

- обмен между виртуальными активами;
- обмен между формами виртуальных активов;
- перевод виртуальных активов;
- хранение виртуальных активов или инструментов, которые позволяют контролировать виртуальные активы, а также их администрирование.

Функция обмена позволяет пользователям покупать, продавать и обменивать виртуальные активы на фиатные валюты или иные криптовалюты, что упрощает конвертацию виртуальных активов.

VASP облегчает перевод виртуальных активов между пользователями и на различные платформы, что делает данную операцию эффективной и быстрой.

Провайдеры услуг виртуальных активов предоставляют хранилища для них и обеспечивают безопасность и удобство для пользователей. Хранилища могут быть онлайн или оффлайн, в зависимости от уровня безопасности. Их также называют горячими (онлайн) и холодными (оффлайн).

Разберем, что может попадать под категорию VASP.

Провайдеры услуг, которые характеризуются как поставщики услуг виртуальных активов:

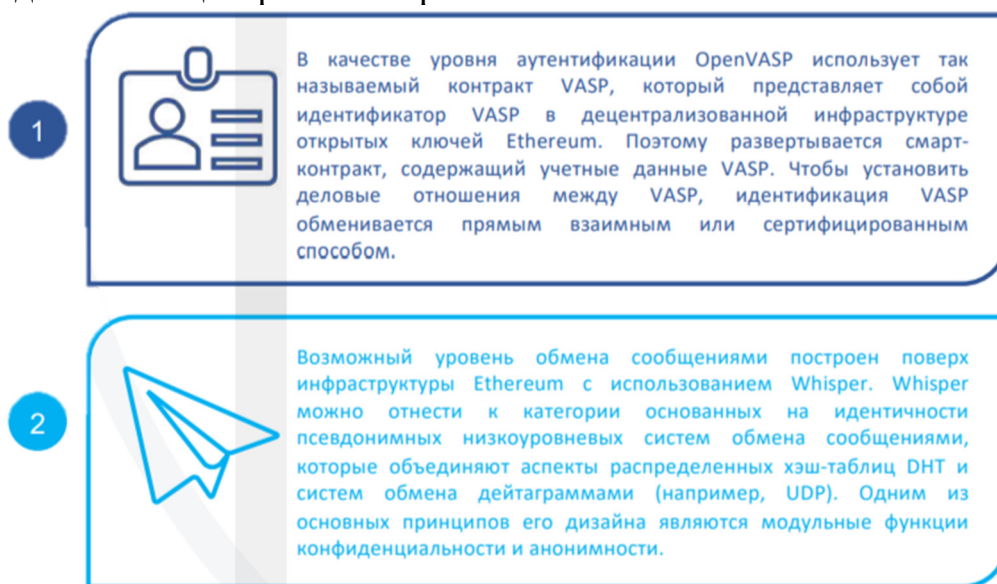
- фиат-крипто обменщики;
- крипто биржи;
- платежные системы;
- крипто банкоматы;
- услуги хранения кошельков (кастоди);
- крипто фонды.

Провайдеры услуг, которые могут характеризоваться как поставщики услуг виртуальных активов:

- P2P;
- DeFi;
- DApps.

Открытый протокол для реализации правила переводов FATF для виртуальных активов:

Протокол OpenVASP основан на «децентрализованной» философии разработчиков и участников. Это отражено в конструкции и архитектуре протокола. Используя некоторые возможности блокчейна Ethereum, протокол утверждает, что обеспечивает криптографически защищенную связь и аутентификацию с целью обеспечения конфиденциальности данных без необходимости в центральном органе.



В 2019 году ФАТФ включила в стандарты по противодействию отмыванию денег и финансированию терроризма виртуальные активы, а впоследствии провайдеры услуг виртуальных активов. Причиной этого стало то, что

виртуальные активы стали использоваться террористическими организациями, в том числе ИГИЛ. С их помощью они оплачивают поставки оружия, взрывчатки и в целом финансируют свою преступную деятельность.

Существует риск-ориентированный подход к надзору и мониторингу VASP. Он направлен на разработку мер по предотвращению или смягчению рисков, соразмерных рискам ОД/ФТ. Надзорным органам следует глубже изучать рынок VASP, его структуру и роль в финансовой системе и экономике страны, чтобы обеспечить высокий уровень информированности при осуществлении оценки рисков в данном секторе. Надзорные органы обязаны опираться на различные источники при определении рисков ОД/ФТ, которые связаны с продуктами, услугами и различными действиями в сфере виртуальных активов и их провайдеров.¹

Провайдеры услуг виртуальных активов могут иметь важное значение и в помощи для оперативно-розыскной деятельности органов внутренних дел.

VASP могут предоставлять информацию о транзакциях, связанных с виртуальными активами, например, о отправителях, получателях, суммы и даты. Такая информация может помочь сотрудникам органов внутренних дел отслеживать финансовые потоки, которые могут быть связаны с преступной деятельностью.

Провайдеры услуг виртуальных активов обязаны проводить процедуры на платформе «Знай своего клиента», которые включают сбор и проверку личной информации пользователей, что может помочь сотрудникам ОВД идентифицировать лиц, которые участвуют в преступной деятельности, связанной с использованием виртуальными активами.

VASP могут блокировать и изымать виртуальные активы, связанные с преступной деятельностью по запросу правоохранительных органов. Это позволит предотвратить такие действия, как легализация доходов, полученных преступным путем, финансирование экстремизма и терроризма.

VASP по запросу правоохранительных органов могут предоставить доступ к данным о пользователях и транзакциях для проведения анализа с целью выявления закономерностей и тенденций, связанных с преступной деятельностью с использованием виртуальных активов.

Провайдеры услуг виртуальных активов могут внедрять меры по предотвращению преступлений, например, мониторинг транзакций, отчетность и подозрительной деятельности, которая предоставляется сотрудникам ОВД.

¹ Рекомендации ФАТФ (FATF) по регулированию оборота виртуальных активов (VA) и деятельности провайдеров услуг в сфере виртуальных активов (VASP) URL: <https://mgimo.ru/upload/2020/02/rekomendacii-fatf-fatf-po-regulirovaniyu-oborota-virtualnyh-aktivov-i-deyatelnosti-provajderov-uslug-v-sfere-virtualnyh-aktivov.pdf?ysclid= m4b1zxa5ub773633076> (дата обращения: 27.11.2024).

VASP могут сотрудничать с подразделениями экономической безопасности и противодействия коррупции (Далее – ЭБиПК) в совместных расследованиях, связанных с отмыванием денег или финансированием экстремизма и терроризма. Они могут предоставлять техническую экспертизу и доступ к данным, которые могут помочь в расследовании.

Немало важной формой взаимодействия провайдеров услуг виртуальных активов и сотрудников подразделений ЭБиПК является обучение и повышение осведомленности сотрудников оперативных подразделений ЭБиПК о виртуальных активах и связанных с ними рисками.

Провайдеры услуг виртуальных активов играют важную роль в оперативно-розыскной деятельности, предоставляя правоохрательным органам ценную информацию для раскрытия и расследования преступлений, связанных с виртуальными активами.

Регулирование VASP и внедрение мер по борьбе с отмыванием денег и финансированием экстремизма и терроризма позволили правоохрательным органам отслеживать и пресекать незаконную деятельность, связанную с виртуальными активами.

Подводя итог нашего исследования, хотелось бы отметить, что по мере развития экосистемы виртуальных активов правоохрательным органам необходимо продолжать адаптироваться и совершенствовать свои методы раскрытия и расследования, чтобы противостоять новым угрозам и не отставать от новых тенденций. Регулирование VASP и сотрудничество с ними останутся ключевыми элементами в обеспечении безопасности и целостности финансовой системы и предотвращении использования виртуальных активов в преступных целях.

Горбунов Алексей Николаевич,
заместитель начальника
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

ЗНАЧЕНИЕ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ ОРУЖИЯ

Исследование значения ОРД в противодействии преступности в сфере незаконного оборота оружия очень важно, так как на современном этапе все большее число преступлений совершается с применением различного рода оружия и, как следствие, становится необходимым проводить судебно-баллистические экспертизы. Данное во многом стало связано с доступностью оружия в виду его незаконного оборота, современные технические средства и приборы позволяют изготавливать орудие в «домашних» и «подпольных» условиях. Так даже на сайте РБК опубликовано, что за минувший год в Российской Федерации наблюдается рост числа преступлений, совершенных с применением оружия, практически на 30 процентов, что является очень существенным негативным фактором. Лидирующее место заняла курская область, где прирост таких преступлений составил 675%, на втором месте – Белгородская область 213,2%, третье место заняла Москва – прирост 203%¹. То есть цифры пугающие. Мы видим, что рост приходится в основном на пограничные районы с Украиной, где сейчас производится специальная военная операция, а как следствие, на территории данных субъектов Российской Федерации наблюдается скопление оружия, наблюдается работа вражеских разведывательных групп и т.п., что неизбежно оказывает негативное влияние на криминогенную обстановку на данных территориях.

Закон об ОРД² предусматривает ряд оперативно-розыскных мероприятий, которые могут показать высокую эффективность и результативность при борьбе с незаконным оборотом оружия. В частности, особое внимание необходимо обратить на проверочную закупку.

Проверочная закупка – это оперативно-розыскное мероприятие, которое заключается в создании органом, осуществляющим оперативно-розыскную деятельность, ситуации, в которой под оперативным контролем возмездно приобретаются товары или предметы без цели потребления или сбыта у лица, обоснованно подозреваемого в совершении преступления, с

¹ РБК. Официальный сайт [Электронный ресурс]. – Режим доступа: <https://www.rbc.ru/society/23/11/2022/637ccfa59a79478ef249f44d?ysclid=lnzq5qswcm315658204> (дата обращения 16.11.2023).

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // «Российская газета», № 160, 18.08.1995.

целью получения информации о вероятной преступной деятельности, а также решения иных задач оперативно-розыскной деятельности¹.

Закон об ОРД² предусматривает проведение проверочной закупки. Однако, проверочная закупка не может проводиться на «пустом месте». В связи с этим Е.В. Степанов³ поднимает вопрос об оценочном характере понятия достаточности при определении ситуации, когда оперативные подразделения могут проводить проверочную закупку. Ведь российский законодатель предписывает проводить данное оперативно-розыскное мероприятие, когда у оперативного органа имеется достаточно оснований предполагать, что совершается или готовится к совершению преступление. Например, данная информация может быть получена по заявлению третьих лиц или при проведении других оперативно-розыскных мероприятий, например, мониторинга сети Интернет.

Однако, торговцы оружием стараются быть аккуратными и не оставлять следов, в том числе и в рамках онлайн-пространства.

Отметим, что на современном этапе в теории оперативно-розыскной деятельности можно наблюдать своеобразный «перекос», который заключается в том, что проверочная закупка исследуется и изучается применительно к преступности в сфере незаконного оборота наркотических средств. Очень мало работ посвящается правовой природе проверочной закупки, проблемам ее правовой регламентации, реализации на практике и т.п. В том числе мало работ, посвященных проверочной закупке оружия в целях борьбы с преступлениями в сфере незаконного оборота оружия, то есть можно заключить, что на современном этапе имеется своеобразный «пробел» доктринального характера в теории оперативно-розыскной деятельности.

Например, А.Н. Трохова⁴ пишет, что проверочная закупка является незаменимым средством по борьбе с незаконным оборотом наркотических средств и психотропных веществ. Г.А. Хачатрян⁵ анализирует тактику проведения проверочной закупки наркотических средств. В.Н. Курченко⁶ ис-

¹ Омелин В.В., Веселовский А.А. Проверочная закупка и провокационные риски при ее проведении // Научный портал МВД России. 2016. №3 (35). – С. 32.

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // «Российская газета», № 160, 18.08.1995.

³ Степанова Е.В. Основные требования, предъявляемые к проведению оперативно-розыскного мероприятия «проверочная закупка» // Российский следователь. 2019. № 10. С. 47 - 51.

⁴ Трохова А.Н. Юридическое содержание, особенности проведения и использования результатов оперативно-розыскного мероприятия «проверочная закупка» // Вопросы российской юстиции. 2019. №4.

⁵ Хачатрян, Г. А. Тактика проведения проверочной закупки наркотических средств и психотропных веществ / Г. А. Хачатрян. – Текст : непосредственный // Молодой ученый. – 2019. – № 2 (2). – С. 221-223.

⁶ Курченко В.Н. Обоснование прокурором законности проверочной закупки наркотиков в суде первой инстанции // Законность. 2023. № 7. С. 15 - 19.

следует вопросы и проблемы осуществления прокурорского надзора за проверочной закупкой, но снова применительно к сфере незаконного оборота наркотиков. И подобного рода исследований ежегодно появляется большое количество. Однако, анализируемое оперативно-розыскное мероприятие обладает куда более широкой сферой применения. Например, проверочную закупку можно производить при незаконном обороте оружия.

При проверочной закупке происходит имитация купли-продажи, где сотрудник оперативного подразделения выступает только на стороне покупателя (на стороне посредника или продавца он выступать не может). Отметим, что данное ОРМ далеко не ограничивается только, как таковой, сделкой по покупке какого-либо запрещенного товара, предмета и т.п. мы видим, что проверочная закупка требует тщательной подготовки, в связи с чем на практике рекомендовано уделять повышенное внимание подготовительному этапу проверочной закупки.

По нашему мнению, данные аспекты нуждаются в более глубоком доктринальном исследовании, так как обладают не только теоретическим, но и практическим значением. Закон об оперативно-розыскной деятельности с самого начала его принятия и вступления в силу традиционно подвергался и продолжает подвергаться широкой критике. Не совершенно также и правовое регулирование проверочной закупки. Соответственно, более глубокое доктринальное исследование основ проверочной закупки позволит выявить все недостатки действующего нормативно-правового регулирования данного оперативно-розыскного мероприятия, а также разработать практические рекомендации по его усовершенствованию.

О.М. Овчинников¹ пишет, что для повышения эффективности борьбы с незаконным оборотом оружия и боеприпасов, изъятия из незаконного оборота этих предметов, необходимо организовывать оперативную работу по следующим направлениям:

- совместное изучение, анализ и оценка данных оперативной обстановки;
- изучение и принятие решений по поступающим в органы внутренних дел сообщениям о преступлениях и иных происшествиях;
- разработка совместных планов следственных и оперативно-розыскных мероприятий по конкретным уголовным делам и участие в проведении данных мероприятий;
- организация совместной работы по оперативному внедрению в преступную группу, использование метода контролируемой поставки оружия,

¹ Овчинников О.М. Направления совершенствования оперативно-розыскной деятельности по противодействию незаконному обороту оружия // Инновационная наука. 2020. №4-4. URL: <https://cyberleninka.ru/article/n/napravleniya-sovershenstvovaniya-operativno-rozysknoy-deyatelnosti-po-protivodeystviyu-nezakonnomu-oborotu-oruzhiya> (дата обращения: 15.11.2023).

проведение других оперативно-розыскных мероприятий с целью изъятия из незаконного оборота оружия, до возбуждения уголовного дела;

- организация и проведение совместных оперативных совещаний по обсуждению проблем раскрытия и расследования конкретных преступлений (в том числе рассмотрение вопросов исполнения поручений следователей (дознавателей) сотрудниками оперативных и других служб);

- информирование заинтересованных сторон о преступлениях и чрезвычайных происшествиях, связанных с применением огнестрельного оружия и боеприпасов. Обмен оперативной и иной информацией по линии борьбы с незаконным оборотом оружия и боеприпасов;

- планирование и проведение (в профилактических целях или при наличии конкретной информации) оперативно-розыскных, профилактических и специальных операций по выявлению и изъятию из незаконного оборота оружия и боеприпасов.

Таким образом, в настоящее время противодействие незаконному обороту оружия является одним из ключевых направлений реализации оперативно-розыскной деятельности.

Горбунов Алексей Николаевич,
заместитель начальника
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Широков Илья Владимирович,
курсант 4 курса
Краснодарского университета МВД России

ОРГАНИЗАЦИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ, НАПРАВЛЕННОЙ НА ВЫЯВЛЕНИЕ ЖАРГОНОВ, ИСПОЛЪЗУЕМЫХ ПРЕСТУПНЫМИ ГРУППАМИ

Зачастую, при развитии общества, параллельно с ним развивается и преступность. Для успешной реализации своих преступлений, преступникам приходится использовать свой жаргон, понятный только им, для шифрования своей деятельности от правоохранных органов. Исходя из этого, с развитием преступности, развивается и так называемый «язык преступности», который также необходимо знать сотрудникам правоохранительных органов, особенно оперуполномоченным уголовного розыска, которые напрямую взаимодействуют с лицами, тем или иным образом причастными к преступности. Таким образом, для поднятия уровня эффективности раскрываемости преступлений, необходимо знать особенности и тактику выявления и распознавания преступного жаргона.

В научной литературе преступный жаргон обозначается как эвфемизмы и арго преступных групп. Эвфемизмы и арго преступных групп – это лексические явления, которые возникают в определённых социальных группах и используются для шифрования речи, избегания прямых высказываний или создания особого языка общения, понятного только членам группы. Корни арго преступных групп уходят в глубокую древность. В разные эпохи преступные элементы использовали свой язык – от «воровского жаргона» в средневековой Европе до современного языка преступных группировок. В России одним из самых известных вариантов арго был «феня» – жаргон преступного мира, который активно развивался в тюрьмах и лагерях ГУЛАГа. Этот язык включал в себя множество заимствований из еврейского, цыганского и других языков.

Сегодня слово «эвфемизм» стало международным лингвистическим термином, который понимается и трактуется по-разному. На сегодняшний день существует достаточно большое количество определений эвфемизма. Одно из самых распространенных гласит, что под «эвфемизмами» принято понимать «эмоционально нейтральные слова или выражения, употребляе-

мые вместо синонимичных им слов или выражений, представляющихся говорящему неприличными, грубыми или нетактичными». В криминальном контексте эвфемизмы могут использоваться, чтобы говорить о преступлениях и их последствиях с минимальной откровенностью. Например:

«Решить вопрос» вместо «убить» или «устранить».

«Пойти в гости» – выражение, которое может означать кражу со взломом или нападение.

«Взять кассу» – ограбить банк или инкассаторскую машину.

Такие эвфемизмы позволяют участникам преступной деятельности говорить о незаконных действиях без прямого их обозначения, что усложняет понимание их содержания для посторонних и для правоохранительных органов.

Арго преступных групп – это специализированный язык, который получил свое развитие в криминальной среде.¹ Он включает в себя не только эвфемизмы, но и специфические жаргонные слова и фразы, которые предназначены для кодирования сообщений и идентификации «своих». Такой язык часто формируется под влиянием культурных, региональных и исторических факторов. Примеры преступного арго:

Предметы тюремного обихода: «параша» – унитаз, «шконка», «нары» – лежанка

Документ, удостоверение личности или фальшивый паспорт – «ксива»

Обыск – «шмон»

Работники правоохранительных органов: «хозяин» – начальник исправительного учреждения, «кум» – начальник оперативной части, оперативный сотрудник исправительного учреждения, «лежавый», «мент»

«Барыга» – торговец краденым или наркоторговец.

Исходя из смысла эвфемизмов и арго преступных групп, можно сделать вывод, что они выполняют следующие функции:²

Соккрытие преступной деятельности- использование жаргона и эвфемизмов помогает скрыть истинное значение сказанного, что затрудняет понимание посторонним.

Одна из функций уголовного жаргона – выявление с его помощью подсланных правоохранительными органами лиц. Обычно лица, выдающие себя за воров в законе, других крупных авторитетов или просто внедренные в уголовную среду для выполнения какого-либо задания успешно проваливаются на языковом «экзамене»

Немало важной функцией также является кодирование информации – преступные группы используют арго для передачи информации так, чтобы она была понятна только узкому кругу лиц.

¹ Красковский Я.Э. Уголовный жаргон. Труды Международного симпозиума «Надежность и качество». 2018 г.

² Даштар-Оол В. Ю. Жаргон – элемент криминальной среды. 2020 г.

Использование арго и эвфемизмов помогает преступным группам сохранять свою идентичность и автономию, а также защищать себя от вмешательства внешних структур, таких как правоохранительные органы.

Как уполномоченный сотрудник уголовного розыска, занимающийся оперативно-розыскной деятельностью, выявление и анализ эвфемизмов и жаргона, используемых преступной группой, имеет важное значение для раскрытия их незаконной деятельности. Для достижения этой цели мы считаем целесообразным применить следующие предусмотренные законом оперативно-розыскные мероприятия:

1. Оперативное наблюдение – п.6 ст.6 ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»¹

Наблюдение за подозреваемыми с целью выявления их повседневной деятельности и общения. Немало важным является то, что необходимо использовать различные виды наблюдения, как традиционный вид наблюдения, когда оперуполномоченный сотрудник лично проводит оперативно-розыскное мероприятие, так и негласное, путем использования технических средств, для фиксации встреч и разговоров разрабатываемых лиц. Необходимо это для анализа встреч, контактов и мест общения, для выявления закономерностей используемого сленга, а также используемых его соучастников.

2. Прослушивание телефонных переговоров – п.10 ст.6 ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»²

Реализуется путем сбора информации из телефонных разговоров подозреваемых и других каналов связи. Перед осуществление данных действий необходимо судебное разрешение на перехват и отслеживание телефонных звонков, а также SMS-сообщений. Необходимо это для того, чтобы проанализировать перехваченные сообщения на предмет характерных слов, фраз и эвфемизмов, чтобы понять жаргон группы и структуру общения.

3. Снятие информации с технических каналов связи – п.11 ст.6 ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»³

Мониторинг интернет-активности, социальных сетей, и других интернет-каналов, используемых группой, может дать немало информации о преступном жаргоне, особенно в наше время. Для получения данной информации необходимо использовать специализированное программное обеспечение для доступа к онлайн-коммуникациям и их мониторинга.

После осуществления данных действий возможно выявить символы, шифры и сокращения, которые не характерна для обычной речи, указывающие на внутреннюю структуру и связи группы.

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» п.6, ст.6.

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» п.10, ст.6.

³ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» п.11, ст.6.

4. Оперативное внедрение – п.12 ст.6 ФЗ от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»¹

Один из эффективных способов, применяемых сотрудниками оперативных подразделений является внедрение конфидента в структуру преступной группы. При их помощи возможно получить непосредственный доступ к внутренним коммуникациям и понаблюдать за использованием сленга в естественных условиях, что позволит получить ценную информацию о значении и происхождении терминов.

Алгоритм идентификации и анализа преступного жаргона предлагается осуществлять следующим образом:

1. Сбор первичной информации

Необходимо использовать оперативное наблюдение и коммуникационный мониторинг для сбора исходных данных. Уделять пристальное внимание контексту, в котором используется конкретный жаргон. При помощи данного ряда действий – сформировать базовое понимание моделей общения в группе.

2. Создание лингвистической базы данных

Далее необходимо составить полный список идентифицированных слов и выражений включая документирование возможных значений, контекстов и частоту употребления участниками преступной группы. Все это позволит установить закономерности и взаимосвязи в рамках группового жаргона.

3. Консультация с экспертами

Считается необходимым привлекать криминологов и специалистов по криминальному жаргону. Ведь их опыт очень важен для интерпретации сложных или необычных выражений. При их помощи удастся повысить точность интерпретации жаргонных выражений с помощью экспертных заключений.

4. Проверка значений

Для проверки выявленных жаргонов предлагает информировать о них агентов, после чего давать им задания, связанные с использованием этих слов и словосочетаний. Таким образом удастся подтвердить предполагаемые значения определенных слов и фраз в практических сценариях.

Подводя итог изложенному, мы полагаем, что применение этих оперативно-розыскных мероприятий позволяет эффективно идентифицировать сленг и закодированные выражения, используемые преступной группой. Систематически собирая, анализируя и проверяя лингвистические данные, мы можем установить конкретные факты о преступной деятельности группы и собрать убедительные доказательства для рассмотрения уголовного дела в суде. Обеспечение того, чтобы все действия проводились в рамках закона и с надлежащего разрешения суда, не только обеспечивает целостность расследования, но и повышает допустимость доказательств в суде.

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» п.12, ст.6.

Горковенко Игорь Александрович,
начальник Калининградского филиала
Санкт-Петербургского университета МВД России

ОТДЕЛЬНЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ НЕСОВЕРШЕННОЛЕТНИХ ОПЕРАТИВНО-РОЗЫСКНЫМИ МЕРАМИ

Проблема борьбы с преступлениями, совершаемыми несовершеннолетними в настоящее время не утрачивает своей актуальности, а критичность постановки вопроса повышается по причинам реформирования ювенального законодательства, а также изменения качественных характеристик преступлений, совершенных несовершеннолетними. Противодействие преступлениям несовершеннолетних представляют собой одно из звеньев обеспечения правопорядка и законности.

Актуальность исследования подтверждается пристальным вниманием к проблемам криминализации среды несовершеннолетних со стороны государства. Так, стратегической задачей, которая стоит перед обществом, представляется поиск эффективных путей противодействия преступности несовершеннолетних как опасному социальному явлению. Президент России Владимир Путин, выступая на расширенном заседании коллегии Генпрокуратуры РФ, напомнил о важности ограждать молодежь от втягивания в криминальную среду¹. Также, Распоряжением Правительства Российской Федерации от 18 марта 2021 г. № 656 «Об утверждении Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года» (включающего «План мероприятий на 2021-2025 гг. по реализации Концепции развития системы профилактики безнадзорности и правонарушений несовершеннолетних на период до 2025 года») и приказом МВД России № 908 от 27 ноября 2023 г. «Об утверждении Наставления по организации деятельности центров временного содержания для несовершеннолетних правонарушителей органов внутренних дел», предусмотрена профилактика и поведенческая коррекция правонарушений несовершеннолетних.

В оперативно-розыскной науке проблемы деятельности оперативных подразделений органов внутренних дел по борьбе с преступностью несовершеннолетних рассматривали в своих работах такие ученые как Ю.М. Антонян, В.Г. Бобров, Н.С. Железняк, В.И. Когтев, О.П. Кириллов, С.Я. Лебедев, А.Г. Маркушин, О.П. Мельниченко, А.В. Семенов и др. Надо отметить, что

¹ Путин: Важно усилить работу по защите молодежи от преступных посягательств [Электронный ресурс] // Российская газета: электр. Издание. 26.03.2024. URL: <https://rg.ru/2024/03/26/putin-vazhno-usilit-rabotu-po-zashchite-molodezhi-ot-prestupnyh-posiagatelstv.html> (дата обращения: 17.09.2024)

данные исследователи в большей степени изучали сферу агентурной работы. Вопросы содействия граждан органам внутренних дел в теории оперативно-розыскной деятельности рассматривались в исследованиях В.М. Атмажитова, Ю.С. Блинова, В.Г. Боброва, О.А. Вагина, К.К. Горяинова, Д.В. Гребельского, А.Г. Лекаря, В.Ф. Луговика, А.В. Парфенова и др.

Вопросы негласного содействия граждан органам внутренних дел исследовали А.И. Алексеев, Н.С. Железняк, Луговик, А.А. Маслов, Э.В., В.С. Овчинский, С.С. Овчинский, В.Н. Омелин, Н.В. Павличенко, Г.А. Рукавишников, В.В. Сергеев, А.В. Солдатов, А.И. Тамбовцев, А.В. Шахматов, А.Ю. Шумилов и др.

В сложившейся в настоящее время тенденции к «стремлению обеспечить применение адекватных, соответствующих личности несовершеннолетнего и тяжести деяния, гуманных мер государственного воздействия, и одновременно – гарантировать эффективную защиту от проявлений преступности несовершеннолетних, которая может принимать достаточно жестокие и очень агрессивные формы»¹ требуется активизация теоретических разработок в этой сфере, так как без научного обоснования эффективность борьбы с описываемыми негативными явлениями среди несовершеннолетних будет недостаточной. Указанное будет способствовать повышению качества и интенсивности работы правоохранительного блока в интересующем нас направлении.

Существуют проблемы, не позволяющие органам внутренних дел осуществлять рассматриваемое направление деятельности в полной мере. Так, сотрудники оперативных подразделений ориентированы на борьбу с преступностью несовершеннолетних, прежде всего, через раннее выявление и предотвращение совершения преступлений несовершеннолетними. Одним из инструментов противодействия преступности несовершеннолетних является использование негласного аппарата. Наиболее проблемным с точки зрения закона представляется привлечение к содействию в борьбе с преступлениями, совершаемыми несовершеннолетними, самих же несовершеннолетних. На данный момент законодательно запрещено использование лиц, не достигших 18-летнего возраста, для негласного содействия по контракту с органами, осуществляющими оперативно-розыскную деятельность. Так, в статье 17 ФЗ «Об оперативно-розыскной деятельности»: «Содействие граждан органам, осуществляющим оперативно-розыскную деятельность» указывается, что «органы, осуществляющие оперативно-розыск-

¹ Тучина, О. А. Меры пресечения в отношении несовершеннолетних, не связанные с изоляцией от общества, в государствах постсоветского пространства / О. А. Тучина // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2020. – № 4(62). – С. 86-90.

ную деятельность, могут заключать контракты с совершеннолетними дееспособными лицами»¹. Однако данный инструмент является одним из самых высокоэффективных, так как именно несовершеннолетний может предоставить наибольший объем оперативно значимой информации.

Также следует отметить, что с момента помещения несовершеннолетнего лица в учреждения ФСИН РФ возникают широкие возможности для получения оперативно значимой информации о нераскрытых и готовящихся преступлениях в условиях их содержания в данных учреждениях, а также розыска несовершеннолетних². В указанном ключе остро стоит проблема взаимодействия оперативных подразделений ФСИН России и оперативных подразделений органов внутренних дел. От оперативности и своевременности передачи информации оперативными сотрудниками ФСИН РФ оперативным сотрудникам органов внутренних дел непосредственно зависит степень эффективности противодействия преступности несовершеннолетних. Существующие механизмы взаимодействия указанных подразделений далеки от совершенства и требуют научной проработки и внесения предложений по их совершенствованию.

Несмотря на значительное количество научных трудов, посвященных различным аспектам противодействия преступности несовершеннолетних, указанные вопросы остаются недостаточно изученными. Постоянные изменения в социально-экономической жизни общества и оперативной обстановке, несовершенство законодательного регулирования ряда вопросов, связанных с оперативно-розыскным противодействием преступности несовершеннолетних, в совокупности указывают на необходимость проведения исследования, соответствующего современным социальным и правовым реалиям, затрагивающего отдельные частные вопросы данной проблематики.

В свете стремительного научно-технического прогресса, совершенствования форм преступной деятельности в сочетании с усложнением социально-экономической обстановки, существованием практических правовых проблем в сфере борьбы с преступностью несовершеннолетних оперативными подразделениями органов внутренних дел исследование представляется своевременным.

1 Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ // Собрание законодательства Российской Федерации от 14.08.1995, № 33, ст. 3349.

2 Глубоковских, Р. В. Вопросы правоприменительной практики розыска без вести пропавших несовершеннолетних / Р. В. Глубоковских // Процессуально-правовые особенности взаимодействия следственных органов с органами, осуществляющими оперативно-розыскную деятельность : Сборник материалов Международного научно-практического круглого стола, Санкт-Петербург, 22 октября 2021 года / Под общей редакцией И.А. Антонова, М.Р. Глушкова. – Санкт-Петербург: Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургская академия Следственного Комитета Российской Федерации», 2022. – С. 72-78.

Ставя перед собой ряд промежуточных задач по изучению и обобщению научных взглядов к проблеме противодействия преступности несовершеннолетних в оперативно-розыскной науке, рассмотрению социально-правовых, психологических особенностей несовершеннолетних, анализу современного состояния оперативно-розыскного противодействия преступности несовершеннолетних, исследованию правовой регламентации конфиденциального содействия и сотрудничества несовершеннолетних, взаимодействия с оперативными подразделениями ФСИН России прогнозируем достижения положительных результатов по совершенствованию оперативно-служебной деятельности оперативных подразделений в рассматриваемом направлении.

Теоретическая значимость предстоящего исследования заключается в дальнейшей проработке вопросов оперативно-розыскного противодействия преступности несовершеннолетних на основе существующих теоретических разработок и тенденций правоприменительной практики.

Данильян Элина Сергеевна,
начальник кафедры криминалистики
Краснодарского университета МВД России,
кандидат юридических наук, доцент

ПРОБЛЕМЫ РАССЛЕДОВАНИЯ НЕРАСКРЫТЫХ ПРЕСТУПЛЕНИЙ В ФОРМЕ ДОЗНАНИЯ

На заседании коллегии Генпрокуратуры России Президент Российской Федерации В.В. Путин отметил, что «начиная с 2016 года, общее число преступлений в стране выросло. Увеличилось и количество нераскрытых преступлений...но, к сожалению, получается, что практически каждое второе преступление остается нераскрытым. Здесь есть над чем подумать...Нужны и глубокий анализ проблем, и конкретные проработанные меры, направленные на их решение.»¹ Прошло достаточно времени после выступления Президента России, а проблема остается до настоящего времени одной из актуальных для правоохранительных органов. Эта проблема является так же актуальной и для ученых. Проблему расследования нераскрытых преступлений В.П. Лавров назвал «одной из наиболее острых в деятельности правоохранительных органов»². Количество нераскрытых преступлений возрастает с каждым годом.

При расследовании преступлений, по которым предварительное расследование проводится в форме дознания, существуют определенные проблемы:

– противодействие расследованию преступлений. Активное противодействие расследованию преступлений, во-первых, сильно влияет на рост общего количества нераскрытых преступлений; во-вторых, существенно осложняет следственную и оперативную работу по их раскрытию, а также процесс дальнейшего расследования. В этих условиях каждая капля крови, каждый волос, оставленный преступником, каждый окурок (со слюной неустановленного преступника), находящиеся в материалах приостановленных дел, приобретают важнейшее значение как идентифицирующие объекты, идентификационная роль которых со временем не снижается, а наоборот, возрастает при условии их надлежащего хранения и правильного использования в поисковой работе³.

– отсутствие налаженного взаимодействия между подразделениями полиции. О взаимодействии между членами следственно-оперативной

¹ Выступление В.В. Путина на заседании коллегии Генпрокуратуры России, 17 марта 2020 г. Официальный сайт Президента России. Электронный ресурс: режим доступа: <http://kremlin.ru/events/president/news/62998>. Дата обращения 24.04.2024 г.

² Лавров В.П. Проблема расследования нераскрытых преступлений прошлых лет и некоторые пути ее решения // Предварительное следствие. Выпуск 4(6). 2009. С. 28.

³ Лавров В.П. Указ. соч. С. 32.

группы, между оперативными подразделениями и лицами, проводящими дознание, специалистами написано много работ учеными, эта проблема стоит остро в каждом отделе внутренних дел. При исследовании данного вопроса нами было выявлено, что 90% опрошенных дознавателей указали, что они самостоятельно составляют план совместных следственных действий и оперативно-розыскных мероприятий, самостоятельно выдвигают версии и определяют совокупность следственных действий и оперативно-розыскных мероприятий по отработке каждой из них. Сотрудники заинтересованных служб в этом участия не принимают.

– незнание дознавателями методики расследования нераскрытых преступлений. Необходимо соблюдать рекомендации ученых-криминалистов по методике расследования данных преступлений. При опросе дознавателей из пяти отделов дознаний нами было установлено, что о методике расследования нераскрытых преступлений слышали 35% опрошенных, в связи с тем, что они обучались в ведомственных образовательных организациях системы МВД России. Остальные опрошенные заявили, что слышат о таковой впервые. В связи с ростом нераскрытых преступлений необходимо в образовательных организациях на юридических факультетах ввести спецкурсы, либо увеличить количество аудиторных часов, отведенных на изучение данной темы в рамках дисциплины «Криминалистика»;

– отсутствие активной поисковой работы по уголовным делам данной категории. Проведенное нами исследование показало, что после вынесения постановления о приостановлении предварительного расследования дознаватели не ведут никакой поисковой работы, это подтвердили 87% опрошенных. С другой стороны, о какой работе после вынесения постановления о приостановлении предварительного расследования можно говорить, если у каждого дознавателя в производстве по 10-15 уголовных дел по нераскрытым преступлениям и еще уголовные дела, возбужденные в отношении конкретных лиц; штат отдела дознания неукomплектованный и в связи с этим нагрузка так же остается высокой;

– отсутствие постоянно действующих следственно-оперативных групп по раскрытию нераскрытых преступлений. В связи с неукomплектованными подразделениями в ОВД данные группы занимаются раскрытием и расследованием указанных преступлений «от случая к случаю», либо только по преступлениям, имеющим общественный резонанс;

– отсутствие должного ведомственного контроля за раскрытием и расследованием нераскрытых преступлений. При изучении уголовных дел, по которым предварительное расследование производится в форме дознания, нами установлено, что контроль за ходом расследования осуществляется только после ходатайств или жалоб потерпевшей стороны либо по преступлениям, имеющим общественный резонанс.

Мы перечисли некоторые проблемы, которые нами были выявлены при изучении уголовных дел и анкетировании дознавателей и руководителей подразделений дознания.

Решение проблем по расследованию нераскрытых преступлений, как нам видится, зависит от ряда факторов: наладить работу специализированных следственно-оперативных групп по раскрытию нераскрытых преступлений на постоянной основе; осуществлять должный ведомственный контроль за раскрытием и расследованием данных уголовных дел, и «нельзя успешно решить без значительного улучшения работы по расследованию преступлений «по горячим следам»»¹.

¹ Лавров В.П. Указ. соч. С. 38.

Железняк Николай Семенович,
профессор кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России
доктор юридических наук, профессор,
заслуженный юрист Российской Федерации,

**К ВОПРОСУ О НЕОБХОДИМОСТИ КОРРЕКТИРОВКИ
ПУНКТА 8 ЧАСТИ 2 И ЧАСТИ 3 СТАТЬИ 7
ФЕДЕРАЛЬНОГО ЗАКОНА
«ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ»**

Федеральный закон «Об оперативно-розыскной деятельности» (далее – ФЗ об ОРД) за почти тридцатилетний период своего существования неоднократно подвергался корректировкам¹, лучше, хуже, а иногда и никак не влияющим на оперативно-розыскную практику. Периодически законодателем осуществлялись уточнения, дополнения содержащихся в нем норм, вводились абсолютно новые положения. Цель таких преобразований, как представляется, была благая – совершенствование оперативно-розыскной деятельности (далее – ОРД), а значит – оптимизация возможностей борьбы с преступностью.

Мы уже неоднократно осуществляли оценку такой законотворческой работы², в большей мере подвергая критике принимаемые нормотворческие решения. Вместе с тем нас порадовало дополнение задач ОРД установлением имущества подлежащего конфискации.³ Почему это вызвало такое удовлетворение, можно подробно прочитать в одной из работ автора, позитивно оценившего данное нововведение применительно к борьбе с международным наркобизнесом.⁴

В это же время Федеральным законом от 02.11.2013 № 302-ФЗ в перечень ч. 2 ст. 7 ФЗ об ОРД было введено предписание, позволяющее органам, осуществляющим ОРД, «собирать данные, необходимые для принятия решений: ... о достоверности сведений о законности происхождения денег,

¹ Мы насчитали 38 редакций, повлекших 83 изменения содержащихся в нем норм.

² Из наиболее свежих: Железняк Н.С. Вопросы актуализации Федерального закона «Об оперативно-розыскной деятельности» / Н.С. Железняк. – Краснодар: Краснодарский университет МВД России, 2024.

³ Установление имущества, необходимого для обеспечения исполнения приговора в части гражданского иска, взыскания штрафа, других имущественных взысканий, или имущества, подлежащего конфискации (в ред. Федерального закона от 28.06.2022 № 202-ФЗ).

⁴ Железняк Н.С. О конфискации имущества как одном из ключевых средств противодействия преступности в сфере незаконного оборота наркотиков / Уголовное и оперативно-разыскное законодательство: проблемы межотраслевых связей и перспективы совершенствования: материалы IV межведомственной научно-практической конференции. – М., 2019. С. 49-55.

ценностей, иного имущества и доходов от них у близких родственников, родственников и близких лиц лица, совершившего террористический акт, при наличии достаточных оснований полагать, что деньги, ценности и иное имущество получены в результате террористической деятельности, но не ранее установленного факта начала участия лица, совершившего террористический акт, в террористической деятельности и (или) являются доходом от такого имущества».

Верное, по сути, решение, на наш взгляд, сформулировано не совсем корректно. С одной стороны, отмеченная норма позволяет оперативным подразделениям инициативно (при наличии сомнений в подлинности представленной информации о правомерности происхождения материальных ценностей) осуществлять проверку возникших подозрений – и это, естественно, плюс. В качестве минуса оцениваемого нормативного положения выступает характеристика фигуранта как лица, совершившего террористический акт. В связи с этим, во-первых, возникает сомнение в правильности оценки упомянутого лица, во-вторых, в продуктивности рассматриваемого предписания.

Критический взгляд на описываемую ситуацию позволяет судить, что, с одной стороны, фиксация в предписании только одного фигуранта – лица, совершившего террористический акт – «оставляет за бортом» индивидов, организовавших или проспонсировавших акт терроризма, способствовавших его совершению, с другой – изъятие у исполнителя рассматриваемых материальных ценностей не содержит существенного негативного свойства для террориста и его близких.¹ Напротив, конфискация имущества у организаторов и спонсоров совершения преступления представляет совершенно иной подход к проблеме как с точки зрения содержания наказания, так и пополнения государственного бюджета.

Террористические акты, наверное, благодаря работе как спецслужб и оперативных подразделений МВД России, так и компетентных органов других государств, совершаются не так часто, хотя и наносят большой ущерб государству и его населению.² В этом смысле в последнее время преобладающими стали преступления коррупционной направленности.³

¹ Практика свидетельствует, что оплата таких действий либо вообще не осуществляется, либо, как правило, является мизерной. Денежные средства и иные ресурсы тратятся на подготовку преступления, а поэтому не могут быть впоследствии изъяты.

² Террористическая активность в России достигла рекордного уровня за последние 18 лет. Только за первое полугодие текущего года в нашей стране было совершено более 1 600 преступлений, связанных с терроризмом. Такого высокого уровня террористической деятельности в России не наблюдалось в аналогичные периоды как минимум 18 лет.

³ Конечно, нельзя забывать о преступлениях с использованием ИТ-технологий (за семь месяцев 2024 года в России зафиксировано 577 тыс. ИТ-преступлений, 437 тыс. из них приходится на кибермошенничество), но они не являются предметом настоящего исследования.

Официальные средства массовой информации, телеграмм- и иные каналы в последнее время изобилуют сообщениями о выявлении коррупционных преступлений, расследовании уголовных дел в отношении чиновников силовых ведомств, органов региональной власти и т.п.

Руководитель ГУЭБ и ПК МВД России в одном из интервью так оценил создавшуюся ситуацию: «Пожалуй, наиболее подверженными коррупционным проявлениям в настоящее время являются финансово-кредитные отношения, сфера потребительского рынка, деятельность органов власти и управления, сфера освоения бюджетных средств, а также строительства. Кроме того, нередко коррупция выявляется в сфере транспорта и ЖКХ»¹.

Даже ленивый не сомневается, что коррупция стала бичом государства и требует адекватного ответа в лице правоохранительных органов.

В связи с этим обратим внимание на ч. 3 ст. 7 ФЗ об ОРД, согласно которой «органы, осуществляющие ОРД, *при наличии запроса* (здесь и далее выделено нами – Н.Ж.), направленного в соответствии с Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции», другими нормативными правовыми актами Российской Федерации в области противодействия коррупции в пределах своих полномочий проводят оперативно-розыскные мероприятия в целях добывания информации, необходимой для принятия решений о достоверности и полноте сведений», предоставляемых гражданами, претендующими на замещение ряда государственных должностей Российской Федерации, ее субъектов и муниципалитетов, некоторых наиболее значимых организаций, а также на замещение должности судьи.

Оценивая это предписание, в целом заслуживающее позитивного отзыва с точки зрения борьбы с коррупцией, мы тем не менее сомневаемся в том, что в случае отсутствия указанного выше запроса оперативные подразделения смогут проводить какие-либо мероприятия, поскольку не до конца сложившиеся подозрения правоохранительных органов о подготовке коррупционного преступления по закону не являются основанием для осуществления ОРМ.

Таким образом, оценка существующих нормативных правовых реалий, обусловленных недостаточно правильными, на наш взгляд, акцентами в регулировании оперативной работы вообще и проведения ОРМ, в частности, позволяет сделать вывод об отсутствии реальных возможностей борьбы с террористическими и коррупционными преступлениями, особенно, на стадии их оперативно-розыскной профилактики.

¹ <https://tass.ru/interviews/13145931>.

Существует ли выход из создавшейся ситуации? Безусловно, он имеется и неоднократно предлагался в работах автора.¹ Речь идет о такой категории как оперативное обслуживание, которое представляет собой систему действий оперативных подразделений, направленных на *постоянный* преимущественно негласный контроль социальных явлений и криминальной ситуации на криминогенных объектах и территориях с целью предотвращения и раскрытия преступлений, решения других задач ОРД.

¹ См., например, Железняк Н.С. Парадокс неприменения оперативно-розыскных мероприятий в предупреждении наркопреступлений – Сибирский юридический институт МВД России – XXXII международная научно-практическая конференция «Актуальные проблемы борьбы с преступностью: вопросы теории и практики». – Красноярск (4-5 апреля 2024 г.).

Зоз Владимир Александрович,
старший преподаватель
кафедры оперативно-разыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России

Бардин Олег Алексеевич,
слушатель 5 курса
Крымского филиала Краснодарского университета МВД России

ОСОБЕННОСТИ ПРИМЕНЕНИЯ ИНСТРУМЕНТОВ И МЕТОДИК OSINT В ЦЕЛЯХ ВЫЯВЛЕНИЯ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ В СЕТИ ИНТЕРНЕТ

Россия является правовым государством, в котором права, свободы человека и гражданина являются высшей ценностью и гарантируются государством. Государство принимает на себя обязательство по обеспечению должного уровня жизни человека и общества, поддержанию нормальных условий для реализации предоставляемых прав, а также создание благоприятных условий, одним из компонентов которых выступает безопасность. В сущности, этот элемент является неотъемлемым компонентом полноценной и нормальной жизни социума и страны.

Преступность – один из наиболее опасных социально-негативных феноменов, ставящий в опасность множество неоднородных общественных отношений, деструктивно влияющих на интересы человека, общества и государства¹. Противодействие данному явлению имеет выраженный социальный подтекст и представляет собой потребность национального уровня, ведь современные государства, где наблюдается активная деятельность криминальных формирований, стагнируют в своем развитии, претерпевают экономические и социальные кризисы. В свете изложенного, противодействие криминальной активности – залог развития государственных, социальных и культурных институтов и необходимость в построении правового государства.

Актуальность выбранной темы вызвана тем, что, в настоящее время, такая информационно-коммуникационная сеть, как Интернет, пользуется особым спросом среди криминальных элементов, о чём нам говорят официальные статистические данные. Так, в 2023 году, по сравнению с 2022 годом, количество преступлений, совершённых в сети Интернет, возросло более чем на 38%².

¹ Антонян Ю.М. Преступность: понятие и типология // Вестник Нижегородского университета им. Н.И. Лобачевского. 2022. № 6. С. 62.

² Состояние преступности в России за январь-декабрь 2023 года / Москва // Министерство внутренних дел Российской Федерации / ФКУ «Главный информационно-аналитический центр». С. 28

Несмотря на прогрессирующие отчётные данные, выявлять киберпреступников становится более сложным и затруднительным процессом, так как ими постоянно модернизируются схемы совершения преступлений, а также осуществляется поиск новых путей сокрытия следов своей преступной деятельности.

Учитывая вышесказанное, необходимо отметить, что методики правоохранительных органов по выявлению лиц, совершающих преступления в сети Интернет, также эволюционируют, что доказывается применением такой современной технологии, как OSINT (от англ. – Open Source Intelligence), основной функцией которой является сбор, обработка и анализ информации, содержащейся в медиапространстве (Интернете)¹.

М.Е. Сидорова и А.Р. Кузьмин выделили ряд особенностей применения инструментов и методик разведки по открытым источникам данных (OSINT).

Первой особенностью является планирование работы. Под планированием, в данном контексте, понимается разработка основных целей проводимого сбора и анализа информации, постановка конкретных задач, способствующих эффективному выявлению киберпреступников, а также определение методологии, используемой при осуществлении запросов.

Следующая особенность заключается в соблюдении принципа законности. Так, сотрудники правоохранительных органов, в первую очередь, должны руководствоваться законодательными актами Российской Федерации, а также осуществлять действия, не нарушающие права граждан, за исключением случаев их ограничения, в соответствии с нормами Конституции России.

Определение источников, которые будут использованы при сборе интересующей информации, является третьей особенностью, описанной авторами².

Для правоохранительной деятельности, значимыми источниками информации, которую анализирует рассматриваемая нами технология, являются следующие:

1. Научные статьи и работы, содержащиеся в различных издательских выпусках, и которые могут содержать или содержат материалы экстремистского характера;
2. Новостные издания и иные материалы, выпускаемые средствами массовой информации (СМИ), в частности, «жёлтой» прессой, содержащие расистские или ксенофобные высказывания;

¹ Что такое OSINT и как он применяется в кибербезопасности // Интернет-газета «СБЕР БАНК». [Электронный ресурс]. Режим доступа: URL: <https://www.sberbank.ru/ru/person/kibrary/articles/chto-takoe-osint-i-kak-on-primenyaetsya-v-kiberbezopasnosti>

² Сидорова М.Е., Кузьмин А.Р. Разведка по открытым источникам данных и ее применения для решения задач кибербезопасности // [Электронный ресурс]. Режим доступа: URL: https://vestnik-rosnou.ru/sites/default/files/61_PDFsam_N1.pdf

3. Открытые посты и комментарии, публикующиеся в различных мессенджерах, и содержащие мошеннические ссылки, незаконную рекламу, экстремистские высказывания и лозунги, а также незаконно распространяющие порнографические материалы и прочее;

4. Официальные государственные сайты, содержащие в открытом доступе информацию, с помощью которой, становится возможным изучение обстоятельств совершенного незаконного деяния, а также информацию, характеризующую лица, совершившего преступления в сети Интернет (судебные акты);

5. Онлайн-платформы, помогающие сотрудникам получить сведения о провайдере, предоставляющем уникальный идентификационный номер устройства, с помощью которого был осуществлён хакерский взлом сайта или аккаунта, а также о указанных номерах устройств, координирующих работу сайтов, используемых с целью совершения киберпреступлений.

6. Другие онлайн-ресурсы, которые могут содержать данные о совершённых противоправных деяниях и лицах, их совершивших.

Также, необходимо отметить, что OSINT позволяет отследить сообщений лиц, подозреваемых или обвиняемых в совершении киберпреступлений, путём анализа коммуникаций, последних лиц, происходящих в виртуальном пространстве¹.

Четвертая особенность содержит в себе контроль за достоверностью данных, предоставляемых OSINT.

Последняя особенность применения инструментов и методик разведки по открытым данным заключается в обеспечении безопасности и целостности сведений, что обязывает контролирующее лицо кодировать указанные сведения и системы, в которых они содержатся².

Таким образом, мы рассмотрели основные особенности применения инструментов и методик OSINT, используемых в целях выявления лиц, совершающих преступления в сети Интернет.

Исходя из вышесказанного, мы можем сделать вывод, что OSINT является инновационной технологией, которая помогает сотрудникам правоохранительных органов в кратчайшие сроки выявить не только киберпреступность, но и киберпреступников, а также повысить эффективность правоохранительной деятельности.

¹ Дворянкин О.А. OSINT, PENTEST и нетсталкинг – информационные технологии интернета // Национальная ассоциация ученых (НАУ). 2022. № 84. С. 7.

² Сидорова М.Е., Кузьмин А.Р. Разведка по открытым источникам данных и ее применения для решения задач кибербезопасности // [Электронный ресурс]. Режим доступа: URL: https://vestnik-rosnou.ru/sites/default/files/61_PDFsam_N1.pdf

Зоз Владимир Александрович,
старший преподаватель
кафедры оперативно-разыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России

Фетисов Александр Николаевич,
слушатель 5 курса
Крымского филиала Краснодарского университета МВД России

ОСОБЕННОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ ДРАГОЦЕННЫХ МЕТАЛЛОВ

На протяжении столетий драгоценные металлы и драгоценные камни являлись и остаются важнейшим инструментом денежно-кредитной политики стран. Лишь относительно недавно большинство государств отказались от привязки национальной валюты к золотому запасу. Вступление России в 1992 году в Международный валютный фонд ознаменовало проведение демонетизации и с указанного периода драгоценные металлы утратили свою главенствующую позицию и обозначились как простой товар. Однако, в связи с уникальными свойствами и большим спросом, число экономических преступлений связанных с незаконным оборотом драгоценных металлов ежегодно растет. В условиях современности, оборот драгоценных металлов строго регламентируется как Федеральным законом «О драгоценных металлах и драгоценных камнях», так и постановлением Правительства Российской Федерации «О некоторых вопросах контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота...»¹, а контроль за соблюдением законности по ввозу и вывозу драгоценных металлов и изделий из них возлагается на Федеральную пробирную палату.

Согласно ст. 2 Федерального закона № 41 «О драгоценных металлах и драгоценных камнях» закрепляет право собственности и ведение вопросами владения, пользования и распоряжения драгоценными металлами и драгоценными камнями за Российской Федерацией и соответствующим субъектом Российской Федерации.² В случае не лицензируемой добычи дра-

¹ Постановление Правительства РФ от 26.02.2021 № 720 (ред. от 24.08.2024) «О некоторых вопросах контроля за оборотом драгоценных металлов, драгоценных камней и изделий из них на всех этапах этого оборота и внесении изменений в некоторые акты» // URL: https://www.consultant.ru/document/cons_doc_LAW_377990/aff08796f44b5a1fee66db10e78841462f1fe372/

² Федеральный закон от 26.03.1998 № 41-ФЗ «О драгоценных металлах и драгоценных камнях» (с изм. и доп., вступ. в силу с 01.09.2024) // URL: https://www.consultant.ru/document/cons_doc_LAW_18254/bb9e97fad9d14ac66df4b6e67c453d1be3b77b4c/

гоценных металлов, право собственности закрепляется за Российской Федерацией, а неконтролируемая купля-продажа драгоценных металлов как внутри территориальных границ Российской Федерации, так и их вывоз за рубеж, способна причинить значительный вред экономической безопасности государства. Исходя из ранее сказанного, следует определить, что понимается под термином драгоценные металлы. Указанный термин имеет законодательное закрепление, в ст.1 ФЗ № 41-ФЗ под драгоценным металлом понимается – «золото, серебро, платина и металлы платиновой группы (палладий, иридий, родий, рутений и осмий)»¹. В случае нарушения правил оборота драгоценных металлов лицо подлежит привлечению к уголовной ответственности, предусмотренной 191 статьей Уголовного кодекса Российской Федерации (Незаконный оборот янтаря, нефрита или иных полудрагоценных камней, драгоценных металлов, драгоценных камней либо жемчуга).

В связи с чем возникает закономерный вопрос, каким именно образом осуществляется раскрытие преступлений данного вида, а равно с этим какие возникают проблемы противодействия преступности в сфере экономики. Данный проблемный аспект рассматривался сотрудниками НИЦ №3 в соответствии с заявкой ГУЭБиПК МВД России, и по результатам рассмотрения был подготовлен аналитический обзор «Практика выявления преступлений, связанных с незаконным оборотом и контрабандой драгоценных металлов»². Согласно указанной практики, к ряду особенностей по выявлению и дальнейшему раскрытию преступлений, связанных с незаконным оборотом и контрабандой драгоценных металлов относятся:

1. Высокий уровень латентности. Предполагается, что выявление преступлений, рассматриваемой категории в основном возможно только в ходе производства комплекса оперативно-розыскных мероприятий, среди которых: постоянное оперативное наблюдение за местами сбыта, и лицами ранее привлекавшихся к уголовной ответственности за аналогичные преступления; оперативный эксперимент; проверочная закупка; контролируемая поставка; квартирные, а равно с этим заlegenдированные опросы граждан; Обследование помещений, зданий, сооружений и иных участков местности, на которых, исходя из полученных оперативным путем сведений, могут хра-

¹ Федеральный закон от 26.03.1998 № 41-ФЗ «О драгоценных металлах и драгоценных камнях» (с изм. и доп., вступ. в силу с 01.09.2024) // URL: https://www.consultant.ru/document/cons_doc_LAW_18254/bb9e97fad9d14ac66df4b6e67c453d1be3b77b4c/

² Статистическая отчетность формы федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» // ЦСИ ФКУ «ГИАЦ МВД России» (10.5.0.16/csi).

ниться драгоценные металлы или располагается место их сбыта; оперативно-экономический анализ криминогенной обстановки на добывающих или перерабатывающих предприятиях¹.

2. Децентрализация мест сбыта, которая предполагает не одну, а множество точек сбыта драгоценных металлов, расположение мест сбыта зачастую меняется, и не используются повторно. В связи с чем затруднено проведение наблюдения и организация задержания с поличным.

3. Использование информационно-коммуникационных технологий как способ сбыта драгоценных металлов. Использование таких ресурсов как информационно-коммуникационная сеть «Интернет» и расположенных на просторах сети «Даркнет» маркетплейсов, не дают возможности сотрудникам оперативных подразделений своевременно получать информацию о скупщике и приобретателе драгоценных металлов, а также дислокации места сбыта. Таким образом, большинство таких нелегальных сделок по купле-продаже драгоценных металлов в сети Интернет и иных ресурсах остаются неизвестными для сотрудников правоохранительных органов.

4. Нехватка квалифицированных специалистов, а также не укомплектованность территориальных подразделений МВД России.

В ходе проведенного анализа сотрудниками НИЦ №3 был предложен план по выявлению и пресечению преступлений, связанных с незаконным оборотом драгоценных металлов. В первую очередь предполагается использование осведомителей, которые играют важную роль в выявлении преступлений. Получая от сотрудников оперативных подразделений те или иные указания, аппарат конфиденентов способствует выявлению и раскрытию ряда преступлений. После получения оперативной информации, перед сотрудником оперативного подразделения стоит задача, каким образом можно воспользоваться полученной информацией и является ли полученная информация достоверной². Для проверки достоверности полученной информации, предлагается следующий пункт плана по раскрытию такого рода преступлений, а именно залегендированный опрос граждан проживающих непосредственно рядом с местом предполагаемого «схрона» драгоценных металлов, или рядом с местами сбыта, а так же рекомендуется отработка граждан, ранее судимых за аналогичные преступления.³ Далее после подтверждения

¹ Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»

² Приказ МВД России, Минобороны России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, Следственного комитета Российской Федерации от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд»

³ Решение коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»

факта незаконного оборота драгоценных металлов, сотрудникам оперативных подразделений необходимо подготовить доказательственную базу, для последующей передачи информации сотрудникам следственных подразделений, или в орган дознания. Для этих целей могут быть задействованы сотрудники подразделений специальных технических мероприятий или оперативно-поисковых подразделений для получения информации, имеющей особое оперативное значение.

Подводя итоги, следует прийти к выводу, что подобные преступления характеризуются высоким уровнем латентности и выявляются только в ходе проведения комплекса оперативно-розыскных мероприятий. Направляющей и ориентирующей является оперативно-розыскная деятельность, посредством которой устанавливаются сам факт преступления, обстоятельства его совершения и лица, его совершившие.

Зюзина Анастасия Викторовна,
преподаватель кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,

ГЕОПОЛИТИЧЕСКИЙ ЭКСТРЕМИЗМ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

В данной статье мы рассмотрим геополитический экстремизм не просто как социальное явление или противоправную деятельность определенных субъектов, а постараемся определить саму суть и природу данных процессов, поскольку, как известно, чтобы успешно противодействовать какому-либо негативному явлению, необходимо бороться с его причиной, а не с последствиями.

В научной литературе отсутствует общепринятое четкое понятие даже политического экстремизма как такового, тем более в контексте геополитики. Политический экстремизм часто понимается и как специфическая линия в политике, отвергающая компромиссы с противодействующей стороной и отражающая агрессивные установки субъекта; и как разновидность политических течений, находящихся в крайне левых или крайне правых политических позициях; и как метод политической борьбы, отвергающей сотрудничество с политическими оппонентами или противниками; и как негативный социальный протест, развивающийся на различных уровнях – общество, классы, различные социальные слои, профессиональные и этноконфессиональные группы¹.

При всем многообразии проявлений политического экстремизма, любое из таковых представляет собой общественную опасность не только для законных прав и интересов отдельной личности, но и для всего социума, а, следовательно, для публичной власти, как части общества, наиболее задействованной в государственной жизни.

Таким образом, отсутствие четкого понятия политического экстремизма ведет к размытости критериев, имеющих значение для соответствующей квалификации совершенных противоправных деяний, а значит – к отсутствию репрезентативной статистики совершенных преступлений и правонарушений указанной направленности. Что, в свою очередь, влечет сложности в прогнозировании преступности данной категории и выработке стратегических мер по противодействию таковой.

Несмотря на регулярно вносимые законодателем изменения и дополнения, направленные на противодействие преступлениям данной категории, их криминализацию и пенализацию, а также вменение функции профилак-

¹ «Политический экстремизм в современном мире: сущность и понятие»; Ю.П. Карючин; [Электронный ресурс]. Cyberleninka.ru.

тики экстремистских проявлений практически всем органам публичной власти Российской Федерации, деяния, связанные с политическим экстремизмом, продолжают оставаться одной из фундаментальных угроз российской государственности.

Отдельной проблемой в противодействии преступлениям экстремистской направленности, совершенным по политическим мотивам (равно как и в противодействии иным современным преступлениям), являются радикальные качественные изменения, произошедшие в российском и мировом обществе в последние два года. Речь идет о переходе к принципиально новому формату общественных отношений, обусловленных новой цифровой реальностью, когда информация приобретает свойства не просто средства передачи данных, а уникального всеобъемлющего инструмента влияния на мировые политические и экономические процессы.

Изложенные обстоятельства подтверждают потребность в современном комплексном научном анализе политического экстремизма, а также ответе на вопрос: что же такое экстремизм, реализуемый в международной политике?

Нестабильная ситуация в государстве, накаленность социальной обстановки, внешнеэкономический кризис и санкционное давление оказывают непосредственное влияние на политические настроения в обществе, являющиеся детерминирующими факторами проявлений экстремизма на почве политических настроений. В п.8 Стратегии национальной безопасности, принятой указом президента Российской Федерации от 02.07.2021г. № 400, указано, что «усиливающаяся нестабильность в мире, рост радикальных и экстремистских настроений могут привести к попыткам разрешить нарастающие межгосударственные противоречия за счет поиска внутренних и внешних врагов, к разрушению экономики, традиционных ценностей и игнорированию основных прав и свобод человека».

Следовательно, проявления политического экстремизма не только оказывают деструктивное влияние на экономику, социальную сферу, уровень преступности в целом, что значительно затрудняет полноценное и разностороннее развитие государства, но и (при крайних его проявлениях) представляют непосредственную угрозу самому его существованию. Соответственно, при всестороннем и углубленном исследовании данного явления, разработке мер по предупреждению преступлений данной категории должны быть изучены как первопричины, так и социальные последствия данного явления, предложены пути их минимизации.

Несмотря на прогрессивные изменения в законодательстве, активно принимаемые государственными и правоохранительными органами меры по противодействию преступлениям экстремистской направленности, совершенным по политическим мотивам, они продолжают существовать и наносить вред не только отдельным видам общественных отношений, но и всему государству в целом.

Защита конституционного строя и территориальной целостности страны является экзистенциальной необходимостью любой государственной власти. Изменения геополитической ситуации, произошедшие в последнее время на международной арене, ставят перед Российской Федерацией и ее руководством новые задачи.

Вместе с тем стремительные процессы цифровизации всех сфер общественной жизни не могли не сказаться на изменении структуры, характера и способов современной преступности, в том числе и экстремистского характера. Особенно наглядно это проявляется в преступлениях, совершаемым по политическим мотивам, с которыми неразрывно связано воздействие на информационное пространство в целом и на отдельную личность в частности.

За последние пару десятилетий российскими учеными написано множество научных трудов, посвященных исследованию экстремизма, в том числе политического. Однако, признавая высокую научную и практическую ценность этих трудов, необходимо отметить, что данные исследования проводились в основном до появления так называемого искусственного интеллекта и связанных с ним экзистенциальных рисков. Рубеж 2022-2023 года ознаменовался созданием принципиально новых когнитивных форм (LLM), приведших к небывалым изменениям во всех сферах общественной жизни, что подтверждает необходимость актуализации имеющихся данных. В новых условиях преступность имеет свойство видоизменяться и приобретать новые характеристики. Политический экстремизм – не исключение.

Но зачастую политический экстремизм принимает настолько крупномасштабные формы проявления, что дает основания считать экстремистскую деятельность продуктом глобализационных изменений, поскольку идентифицируется с социально-политическими процессами планетарного масштаба.

В последние годы экстремизм в различных его формах стал выступать одним из эффективнейших инструментов ведения внешней политики и достижения геополитических интересов. Но для того, чтобы понять, почему экстремизм стал столь успешным средством влияния на политическое пространство объекта воздействия, необходимо разобраться, что изменилось в мировых политических тенденциях на современном историческом этапе.

Итак, мы видим, что практически по всему миру различными политическими акторами целенаправленно создаются экстремистские организации всевозможного (чаще всего религиозного или псевдорелигиозного) толка. Данные организации выполняют роль прокси-сил, воздействующих противоправными методами на те или иные общественные отношения, позволяя при этом главным выгодоприобретателям от их действий оставаться в тени. При этом, говоря о прокси-силах, речь идет не только о незаконных вооруженных формированиях, ведущих боевые действия против государствен-

ных сил, но и о более скрытых и хорошо законспирированных силах, проникающих в сами государственные и общественные институты с целью оказания длительного и планомерного подрывного воздействия на них изнутри.

Следовательно, для того, чтобы успешно противостоять указанным силам, необходимо четко понимать, кто является главным негласным интересантом подрывной деятельности, кто осуществляет организационное и, самое главное, финансовое руководство экстремистскими организациями.

На сегодняшний день многие ученые сходятся во мнении, что мир вступил в эпоху так называемого «глобального неофеодализма». Говоря простым языком, это этап исторического развития человечества, когда происходит эрозия основных государственных институтов и государств в целом, как общественных образований. При этом, вместо них в качестве основных политических субъектов начинают выступать крупные корпорации и их экосистемы. В основном это касается транснациональных корпораций, особенно в сфере новых технологий, цифровизации и искусственного интеллекта. С появлением «большой цифры» феодализм становится естественным для многих стран, вытеснив капитализм. Просто теперь «феодал», то есть корпорация, владеет не землей, а виртуальным пространством. А так как финансовые возможности таких корпораций давно выросли далеко за пределы чистого бизнеса, они готовы входить в высшие эшелоны власти и вести свою политику, распространяя свое влияние все дальше и дальше.

Почему нужно это понимать? Потому что сейчас в цифровое пространство активно уходят и легальные и нелегальные виды бизнеса: перевозки, юридические консультации, медицина, финансы, продажа наркотиков, через Даркнет можно купить оружие или нанять киллера. Отдельному государству все сложнее контролировать эти сферы: сервер находится в другой стране, связь с преступником поддерживается через Даркнет. Спецслужбы различных государств пытаются влиять на владельцев мессенджеров и соцсетей, чтобы заставить их предоставить доступ (ключи) к содержащейся в них информации, насколько успешно это делается можно судить на примере П. Дурова. Это только начало подобных глобальных процессов и на сегодняшний день государство проигрывает в этой борьбе по контролю за виртуальным миром. Не исключено, что в недалеком будущем произойдет усиление глобализации, при которой государства сольются в большие объединения с единой цифровой экосистемой. И ведущую роль в них будут играть не государственные институты, а технологические корпорации, а это, в свою очередь, значит, что появится некий трансконтинентальный IT-монополист в какой-либо сфере, который будет более влиятелен, чем правительство отдельно взятой страны.

Почему еще важно понимать, в каких условиях предстоит противодействовать преступлениям экстремистской направленности в ближайшие годы? Потому что экстремизм, как явление, чрезвычайно многолик и разно-

образен и зачастую прикрывается вполне благовидными мотивами и идеями. Это происходит ввиду того, что наиболее эффективно экстремизм приживается и действует там, где есть так называемый вакуум центральной власти, то есть, где существуют территории, находящиеся вне контроля федерального правительства. Причем, в данном контексте под территориями следует понимать не только физическое, но и виртуальное пространство. Наличие таких «неуправляемых территорий» не может не оказывать влияние на политический ландшафт страны.

Таким образом, любую сферу, в которой государство ослабит или потеряет свое влияние, сразу же займет тот или иной политический игрок с целью извлечения политической или экономической выгоды (зачастую эти цели неразрывно связаны или вовсе идентичны).

Стоит ли говорить, что на примере Российской Федерации мы видим максимально пестрое и разнородное во всех аспектах общество. Социальное, этническое, религиозное и иное его многообразие создает идеальную почву для информационной подпитки существующих противоречий либо вброса новых, искусственно созданных, и дальнейшего разжигания розни с целью достижения конкретных политических целей. Кроме того, в силу большой территории и определенных политических традиций, в нашей стране наблюдается довольно существенный разрыв между регионами не только в размере федерального финансирования и, соответственно, в уровне жизни, но и, что гораздо хуже, в некоторых особенностях местного законодательства и правоприменительной практики. Во-первых, это влечет перекос в сторону приоритета местных законов над федеральными, традиций над правом. Во-вторых, порождает недовольство и запрос на социальную справедливость. И, наконец, в-третьих, провоцирует пассионарную часть общества на достижение своих целей определенными, не всегда легитимными способами.

Однако, не стоит забывать, что похожие или иные социальные проблемы присутствуют практически во всех государствах. Другой вопрос – использование подобных противоречий в политических технологиях, одним из основных инструментов которых является информационная война.

Информационная война – это процесс, нацеленный на овладение информационным пространством другого государства путем имплементации определенных идеологических установок.

Именно поэтому в последнее время наблюдается беспрецедентное усиление деструктивного информационного влияния со стороны западных стран в отношении граждан России, в том числе, с использованием информационно-телекоммуникационных технологий.

Полным ходом идет внедрение в массовое сознание ложных тезисов, взглядов и концепций, а также чуждых нашему обществу установок, ценностей и норм.

Нарастающий с каждым годом объем информации, попадающей в сознание отдельного индивида, приводит к неспособности разграничить факты и фейки, конструктивный и деструктивный контент, формирует «клиповое мышление» и краткосрочную память на события. Все это делается для того, чтобы подвергаемые негативному воздействию граждане оказались неспособны противостоять агрессивным замыслам противника.

Наряду с идеологическим воздействием на население, в качестве еще одного мощного «тарана» против государственной системы, как правило, применяется так называемый экономический экстремизм, как отдельный вид экстремизма. К нему относятся принимаемые в одностороннем порядке экономические санкции и другие «меры», нацеленные на разрушение экономической основы существующего строя.

Вообще, следует помнить, что экономика – это всегда базис и основной двигатель любых глобальных процессов. А уже под экономические интересы той или иной действующей силы подстраиваются политические идеи, лозунги, движения и методы их реализации. С этой точки зрения легко объяснимы процессы, происходящие сейчас на постсоветском пространстве – в России и странах СНГ. Многочисленные локальные вооруженные конфликты, вспышки радикализма, террористическая активность, национализм, религиозный фанатизм, захлестнувшие бывшие союзные республики – есть не что иное, как последствия распада СССР, в том числе экономические последствия. События в Северокавказском регионе, Средней Азии, Закавказье есть не что иное, как последствия тектонических сдвигов на политической арене начала 90-х годов XX века.

Кроме того, развернувшаяся в последние годы борьба за рынки сбыта и логистические цепочки «Европа-Азия» привела к всплеску эскалации и раскручиванию ближневосточной «воронки», затягивающей все большее количество стран данного региона. Эти события не только оказывают прямое экономическое и политическое влияние на нашу страну (да и весь мир), но и являются одной из непосредственных причин и источников проникновения в Россию террористических ячеек. Так, Турция, пытаясь распространить свое влияние на Азию, Ближний Восток и часть наших территорий, исповедующих ислам, давно является базой для подготовки русскоговорящих боевиков. Значительная их часть последние годы воевала в Сирии, но, с падением власти Башара Асада, необходимость в этом отпала. Огромное количество задержанных и ликвидированных на территории РФ террористов были подготовлены на территории Турции. Некоторые «особо ценные» кадры обучались в Великобритании, имеющей сильную разведку и, благодаря ей, традиционно играющей огромную роль в продвижении мигрантов и представителей различных диаспор на территории России. Ряд ликвидированных террористических ячеек имели не только оружие и взрывчатые вещества, но и очень хорошо сделанные документы. Что неудивительно, так как для его получения террористы с боевым опытом сначала приезжают в

Среднюю Азию, где за определенную сумму покупают местный паспорт, с внесением во все баз данных. А уже после этого легализуются в РФ, как обычные мигранты, добиваясь получения гражданства со всеми вытекающими последствиями, включая право на приобретение оружия. Таким образом, можно прогнозировать, что в ближайшее время боевики из Сирии массово двинутся в нашу страну, где пополнят ряды экстремистских и террористических организаций либо будут мимикрировать под обычных рабочих, ожидая инструкций западных кураторов.

Показательно, что на фоне указанных событий, в новой Стратегии противодействия экстремизму, принятой указом президента 28.12.2024г. № 1124, особое внимание уделяется именно противоправной деятельности мигрантов, как одного из факторов распространения экстремизма в РФ, а также деструктивному влиянию иностранных и международных неправительственных организаций, осуществляемому под видом культурной, образовательной и гуманитарной работы.

Отражение данных детерминант экстремистской преступности в документе стратегического планирования государственного уровня говорит о том, что федеральной властью полностью осознаются реальные предпосылки угроз экстремистского характера, и их специфика именно в нашей стране. А, значит, и законодательная политика в этой области будет меняться (и уже меняется) с их учетом.

Зюзина Анастасия Викторовна,
преподаватель кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Жуков Марк Александрович,
курсант 3 курса
Краснодарского университета МВД России

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ С ПОМОЩЬЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие информационных технологий оказывает глубокое влияние как на государство, так и на общество в целом, принося с собой как положительные, так и отрицательные последствия. К числу таких негативных последствий относится появление новых видов преступлений деятельности, особенно тех, которые осуществляются в сети интернет.¹

Примечательно, что наиболее опасными из них являются уголовные преступления, связанные с экстремизмом. Обзор уголовного законодательства показывает, что законодатели все чаще стремятся запретить подобные действия, особенно когда они совершаются через информационные и телекоммуникационные сети. Например, такие конкретные разделы, как часть 2 статьи 280.1 и пункт «б» части 2 статьи 280.4 Уголовного кодекса Российской Федерации, демонстрируют эту законодательную тенденцию². Введение этих новых правовых мер требует разработки новых криминалистических методов, направленных на борьбу с экстремистскими преступлениями, совершаемыми через глобальную сеть Интернет, а также на их расследование.

Стоит отметить изначально, что ни в Законе о противодействии экстремизму³, ни в Законе о противодействии терроризму⁴, ни в Законе об ОРД⁵

¹ Куликов А.Г. К вопросу совершенствования оперативно-разыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. №2. URL: <https://cyberleninka.ru/article/n/k-voprosu-sovershenstvovaniya-operativno-rozysknoy-deyatelnosti-po-protivodeystviyu-ekstremizmu-v-seti-internet> (дата обращения: 28.09.2024).

² Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

³ Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 15.05.2024) «О противодействии экстремистской деятельности» // Российская газета, № 138-139, 30.07.2002.

⁴ Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 10.07.2023) «О противодействии терроризму» // Собрание законодательства РФ, 13.03.2006, № 11, ст. 1146.

⁵ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-разыскной деятельности» // Российская газета, № 160, 18.08.1995.

не установлены особенности или хотя бы основы применения информационных технологий оперативно -розыскными подразделениями.

Мы выражаем согласие с позицией О.А. Меликян¹, который выражает нижеследующие особенности работы органов, осуществляющих оперативно-розыскную деятельность, по противодействию экстремизму и терроризму с применением информационных технологий:

- использование программ и специализированных аппаратных средств, таких как, например, программа мониторинга Интернет-трафика, программы для отслеживания переписки в мессенджерах и социальных сетях;
- проведение оперативно-розыскных мероприятий в сети Интернет только при наличии подозрений в совершении противоправных действий;
- проведение различного рода профилактических мероприятий, которые направлены на информирование пользователей сети Интернет о возможных негативных последствиях совершения противоправных деяний террористического и экстремистского характера.

А.Г. Куликов² подчеркивает, что правовое регулирование оперативно-розыскной деятельности и противодействие экстремизму и терроризму в сети Интернет направлено на обеспечение общественного порядка и общественной безопасности, на защиту прав и свобод граждан.

Стоит отметить, что не смотря на применение в рамках оперативно-розыскной деятельности современных информационных технологий, противодействовать экстремизму и терроризму становится сложнее, что также связано с научно-техническим прогрессом. Злоумышленники также применяют различного рода современные информационные технологии и программы, чтобы скрывать следы экстремистской и преступной деятельности в сети Интернет.

Также не стоит забывать, что постоянно происходит расширение онлайн пространства, которое также не поддается в силу своей специфики нормативно-правовой регламентации. Постоянно наблюдается увеличение числа пользователей сети Интернет, мессенджеров, социальных сетей; многие люди заводят по несколько аккаунтов, номеров телефонов и т.п., что все в совокупности неизбежно ведет к затруднению в осуществлении противодействия экстремизму и терроризму в рамках оперативно-розыскной деятельности.

¹ Меликян, О. А. Оперативно-розыскная деятельность в сети Интернет в условиях противодействия экстремизму: некоторые вопросы правового регулирования / О. А. Меликян. – Текст : непосредственный // Молодой ученый. – 2023. – № 19 (466). – С. 370-373. – URL: <https://moluch.ru/archive/466/102506/> (дата обращения: 28.09.2024).

² Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. №2. URL: <https://cyberleninka.ru/article/n/k-voprosu-sovershenstvovaniya-operativno-rozysknoy-deyatelnosti-po-protivodeystviyu-ekstremizmu-v-seti-internet> (дата обращения: 28.09.2024).

При этом анализ достаточно многочисленного эмпирического материала в виде судебной практики судов общей юрисдикции Российской Федерации свидетельствует, что очень многие преступления и административные правонарушения террористического и экстремистского характера выявляются благодаря применению в оперативно-розыскной деятельности современных информационных технологий.

Рассмотрим конкретный пример из практики – дело № 5-93/2021¹. Как следует из материалов данного дела, в рамках проведения оперативного мониторинга сети Интернет был выявлен факт распространения материалов экстремистского характера, в связи с чем лицо было привлечено к административно-правовой ответственности по статье 20.29 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ²).

Благодаря применению информационных технологий при мониторинге сети Интернет оперативными сотрудниками было обнаружено, что «на странице О. «ВКонтакте» размещен и до настоящего времени в открытом доступе видеофайл «Американское шоу», который включен в список экстремистских материалов по решению суда. При проведении проверки ею было установлено, что данный видеофайл разместил в открытом доступе лично сам О». Согласно поступившему делу об административном правонарушении в отношении О., последний 17 апреля 2011 года находясь по адресу <адрес>, используя ноутбук «Эйсер» разместил в публичном доступе на личной странице «В контакте» с никнеймом «ФИО1» по сетевому адресу № разместил видеоролик «Американское шоу» длительностью 18 минут 32 секунды, который признан экстремистским по решению Новомоскорбского городского суда Тульской области от 26.07.2010 и добавлен в Федеральный список экстремистских материалов Минюста России под № §30. Действия О. сотрудниками полиции квалифицированы по 20.29 КоАП РФ.

Другой интересный пример – дело № 5-94/2021³. В рамках данного дела физическое лицо было привлечено к административно-правовой ответственности уже по статье 20.3 КоАП РФ. Как следует из материалов обозначенного административного дела, виновность лица подтверждается «актом о проведении ОРМ «наблюдение» от 02.03.2021 (л.д. 4), из которого следует, что в 02.03.2021 в ходе проведения оперативно – розыскных мероприятий ст. о/у ОУР ОМВД России по Острогожскому району Воронежской области в соответствии с Законом об ОРД, Федеральным законом № 114-ФЗ от 25.07.2002 «О противодействии экстремистской деятельности», в ходе

¹ Постановление Каширского районного суда Воронежской области от 01.07.2021 № 5-93/2021 // СПС «КонсультантПлюс» 2024 (дата обращения 29.09.2024).

² Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ, 07.01.2002, № 1 (ч. 1), ст. 1.

³ Постановление Острогожского районного суда Воронежской области от 04.03.2021 № 5-94/2021// СПС «КонсультантПлюс» 2024 (дата обращения 29.09.2024).

ОРМ «Наблюдение» произведен мониторинг информационно-телекоммуникационной сети «Интернет», расположенной по электронному адресу <адрес> в социальной сети «instagram.com», в ходе которого было установлено, что на указанной странице в открытом доступе размещено для всеобщего обозрения изображение, публично демонстрирующее атрибутику экстремистской организации, а именно, фотография О. в футболке с надписью «АУЕ», т.е. атрибутикой общественного движения «Арестанское уголовное единство», ликвидированного в соответствии с Федеральным законом «О противодействии экстремистской деятельности».

Вот также примеры из практики, где правонарушение экстремистского или террористического характера было выявлено с применением информационных технологий благодаря проведению оперативно-розыскной деятельности: дело № 2а-81/2021¹, дело № 5-1186/2022², дело №5-6/2019³ и другие.

При изучении основных нормативно-правовых актов, регулирующей оперативно-розыскную деятельность в сети Интернет, возникает важный и нерешенный вопрос: обеспечение соответствия тайных операций, направленных на сбор личной и конфиденциальной информации, Конституции Российской Федерации. Важно понимать, что раскрытие большинства преступных действий, связанных с экстремизмом, в Интернете требует от правоохранительных органов использования секретных методов сбора персональных данных.

Кроме того, следует отметить, что физическим лицам не требуется давать согласие на сбор, хранение или обработку их информации в ходе оперативно-розыскных мероприятий, дознаний и расследований, как это предусмотрено Федеральным законом «Об оперативно-розыскной деятельности» и Уголовно-процессуальным кодексом Российской Федерации.

Вторая категория нормативных правовых документов, лежащих в основе ОРВ, состоит из международных правовых стандартов. Важно также подчеркнуть, что в ряде стран сбор информации из общедоступных источников может рассматриваться как нарушение конфиденциальности.

С нашей точки зрения, основные элементы национального законодательства, регулирующего оперативно-розыскную деятельность в Интернете, особенно в контексте борьбы с экстремизмом, полностью приведены

¹ Решение Вачского районного суда Нижегородской области от 26.02.2021 по делу № 2а-81/2021// СПС «КонсультантПлюс» 2024 (дата обращения 29.09.2024).

² Постановление Красносельского районного суда города Санкт-Петербурга от 15.07.2022 по делу № 5-1186/2022// СПС «КонсультантПлюс» 2024 (дата обращения 29.09.2024).

³ Постановление Шалинского городского суда Чеченской Республики от 07.02.2019 № 5-6/2019// СПС «КонсультантПлюс» 2024 (дата обращения 29.09.2024).

в соответствие с требованиями международного права и не требуют дальнейших детальных корректировок.¹

Третий уровень правового регулирования деятельности ОРДО включает положения соответствующих общих законов, которые определяют стратегии и методы борьбы с экстремистскими преступлениями как специализированной области государственной деятельности. К этой категории относятся, в частности, такие федеральные законы, как «Об оперативно-розыскной деятельности», «О связи»², «Об информации, информационных технологиях и защите информации»³, «О противодействии экстремистской деятельности» и другие.⁴

Таким образом, в рамках данной статьи автор выявил и проанализировал особенности работы органов, осуществляющих оперативно-розыскную деятельность по противодействию экстремизму или экстремизму с помощью современных информационных технологий. Анализ эмпирического материала в виде судебной практики судов общей юрисдикции Российской Федерации по уголовным и административным делам экстремистского и террористического характера, показал, что применение информационных технологий в оперативно-розыскной деятельности показало свою эффективность и результативность. Именно благодаря проведению оперативно-розыскных мероприятий в сети Интернет и с применением информационных технологий позволяет выявить большую часть совершаемых правонарушений в онлайн пространстве указанной направленности.

При этом анализ научной и учебной литературы позволил прийти к выводу, что большая часть авторов и исследователей высказывают обеспокоенность недостатками действующего нормативного правового регулирования, с чем стоит согласиться. Анализ положения основных нормативно-правовых актов позволил прийти к выводу, что российский законодатель не регламентировал должным образом порядок применения информационных технологий в рамках административно-розыскной деятельности в целях

¹ Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. №2. URL: <https://cyberleninka.ru/article/n/k-voprosu-sovershenstvovaniya-operativno-rozysknoy-deyatelnosti-po-protivodeystviyu-ekstremizmu-v-seti-internet> (дата обращения: 28.09.2024).

² Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 08.08.2024) // Собрание законодательства РФ, 14.07.2003, № 28, ст. 2895.

³ Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» // Парламентская газета, № 126-127, 03.08.2006.

⁴ Куликов А.Г. К вопросу совершенствования оперативно-розыскной деятельности по противодействию экстремизму в сети Интернет // Криминалистика: вчера, сегодня, завтра. 2021. №2. URL: <https://cyberleninka.ru/article/n/k-voprosu-sovershenstvovaniya-operativno-rozysknoy-deyatelnosti-po-protivodeystviyu-ekstremizmu-v-seti-internet> (дата обращения: 28.09.2024).

противодействия экстремизму и терроризму, что является серьезным пробелом, который необходимо устранять законодательным путем.

Подобного рода недостатки действующего нормативного правового регулирования позволяют говорить о несоответствии его требованиям и потребностям объективной действительности, на что также обращают внимание многие авторы и исследователи.

Более того, наличие пробелов в праве замедляет процесс внедрения современных информационных технологий в оперативно- розыскную деятельность, что может оказать сугубо негативное влияние на ее эффективность и результативность в борьбе с правонарушениями террористического и экстремистского характера. Соответственно, представляется, что российскому законодателю следует задуматься о реформировании положений нормативно-правовых актов, которые были приведены автором в статье.

Иванов Святослав Игоревич,
начальник кафедры
оперативно-розыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России,
кандидат юридических наук, доцент

Никандрова Диана Александровна,
курсант 4 курса
Крымского филиала Краснодарского университета МВД России

ОПЕРАТИВНО-РОЗЫСКНАЯ ОПЕРАЦИЯ И ЕЕ МЕСТО В СИСТЕМЕ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Согласно определению понятия оперативно-розыскной деятельности (далее – ОРД), закреплённому в Федеральном законе «Об оперативно-розыскной деятельности» (далее – ФЗ «Об ОРД»), она осуществляется посредством проведения оперативно-розыскных мероприятий (далее – ОРМ). Таким образом, ОРМ являются начальным элементом системы ОРД и включают в себя все мероприятия, представленные в ч.1 ст. 6 ФЗ «Об ОРД»¹.

По своей структуре в организационном плане ОРМ не однородны и могут быть разделены на: простые и сложные (комплексные, комбинированные). К простым относятся ОРМ, в организационную основу которых положено одно определяющее название ОРМ действие, например: опрос, наблюдение, наведение справок. Сложными (комплексными, комбинированными) принято считать: оперативный эксперимент, проверочную закупку, контролируруемую поставку, оперативное внедрение. Такие ОРМ подразумевают совершение двух и более действий определяющих их сущность. Например, оперативное внедрение предполагает под собой внедрение в криминальную среду оперативного сотрудника или конфиденанта, получение ими оперативно значимой информации с последующей её передачей оперативному подразделению. В том числе по причине своей организационной сложности указанные ОРМ, в соответствии с ФЗ «Об ОРД», требуют ведомственного санкционирования и это требование не имеет исключений².

После сложных (комплексных, комбинированных) ОРМ в системе ОРД идут комплексы ОРМ, под которыми понимается одновременное проведение нескольких ОРМ. Примером этого является личный сыск, суть ко-

1 Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ. URL: <https://base.garant.ru/10104229/89300effb84a59912210b23abe10a68f/> (дата обращения: 20.10.2024).

2 Об оперативно розыскной деятельности: Федеральный закон от 12.08.1995 №144-ФЗ. URL: <https://base.garant.ru/10104229/89300effb84a59912210b23abe10a68f/> (дата обращения: 20.10.2024).

торого заключается в получении оперативной информации непосредственно самим оперативным сотрудником с помощью проведения комплекса ОРМ, а также применения иных приёмов и методов ОРД. Таким образом, мы видим, что, рассматривая элементы системы ОРД, от более простых к более сложным, в них отмечается все большее присутствие как самих разнообразных сочетаний простых и сложных (комплексных, комбинированных) ОРМ, так и применение обеспечивающих их результативность тактических способов действий, включающих применение приёмов и методов ОРД.

Одним из тактических приемов в системе ОРД является оперативная комбинация, которая представляет собой набор действий, объединенных общей идеей и сценарием, целью которых является выполнение ряда ОРМ. Она предполагает использование рефлексивных методов психологии, что позволяет вводить противника в заблуждение и преодолевать его сопротивление¹. Проведение оперативных комбинаций особенно актуально в рамках проведения сложных (комплексных, комбинированных) ОРМ и комплексов ОРМ.

Иерархически выше комплексов ОРМ находится система ОРМ и других действий, осуществляемых сотрудниками оперативных подразделений, управляемых из единого центра, в соответствии с единым замыслом и планом, скоординированных по времени, месту, объектам и целям для решения сложных задач ОРД, в том числе связанных с необходимостью преодоления противодействия преступников или действием в неблагоприятных для решения задач ОРД условиях. Такая система является подсистемой системы ОРД и представляет собой оперативно-розыскную операцию (далее – ОРО) и определяется как её высшая организационно-тактическая форма деятельности оперативных подразделений органов внутренних дел (далее – ОВД).

По нашему мнению, идентификация ОРО одновременно как системы, подсистемы и высшей организационно-тактической формы ОРД не несёт в себе противоречий, так как названные термины описывают ОРО с точки зрения её сущности, места внутри системы ОРД и её соотношения с другими организационно-тактическими формами ОРД. «Любая система состоит из подсистем, подсистема любой системы может быть сама рассмотрена как система»². Относительно обоснования высшего места ОРО среди других организационно-тактических форм ОРД считаем целесообразным рассмотреть следующие отличительные признаки ОРО:

1. Реализация ОРО по ранее разработанному плану, он является основным элементом любой операции. Замысел операции формируется после

¹ Абрамов А.М. Оперативная комбинация как способ решения оперативно-тактических задач // Вестник российской Таможенной академии. 2012. URL: <https://cyberleninka.ru/article/n/operativnaya-kombinatsiya-kak-sposob-resheniya-chastnyh-operativno-takticheskikh-zadach> (дата обращения: 24.10.2024).

² Описания, базовые структуры и этапы анализа систем. URL: [//kgau.ru/istiki/umk/tssa/c_2](http://kgau.ru/istiki/umk/tssa/c_2) (дата обращения: 20.10.2024).

анализа оперативной обстановки и конкретной оперативно-розыскной ситуации, учитывая силы и средства противоборствующей стороны; возможности противника; собственные силы и средства; возможности других оперативных подразделений ОВД (при их предполагаемом участии).

На основе этой оценки принимается решение о проведении операции, выбираются тактические действия, определяются необходимые силы и средства, планируется маневр в пространстве и времени, распределяются функции оперативных сотрудников, а также решается вопрос о привлечении других подразделений ОВД.

2. Управление ОРО происходит из единого центра. С учётом строгой согласованности действий сотрудников, если участвует несколько подразделений, то действия и приказы начальников этих подразделений должны не противоречить друг другу, быть согласованным между собой и нацелены на выполнение задач, поставленных руководителем ОРО.

3. ОРО – согласованное действие нескольких участников. В простейшем случае это группа оперативных сотрудников, конфиденты, действующие под руководством начальника. Однако чаще всего для проведения ОРО требуются силы и средства нескольких оперативных подразделений ОВД, а также других служб.

4. ОРО требуют всестороннего обеспечения, отличающегося от того, что необходимо для других видов организационно-тактических форм. Это обусловлено их спецификой, которая зачастую требует быстрого развёртывания и действий в сложных условиях. В ОРО особую важность приобретает боевая поддержка, включающая в себя такие элементы, как разведка, маскировка и радиоэлектронная борьба, которые традиционно ассоциируются со специальными операциями.

Ключевым элементом оперативного обеспечения являются конфиденты. Их набор, управление и постоянная готовность к оказанию помощи играют решающую роль в успехе ОРО. Они могут предоставлять ценные сведения о местности, маршрутах, предполагаемых противниках, что значительно повышает эффективность поисковых действий.

Необходимо отметить, что ОРО все чаще опираются на передовые технологии, которые повышают эффективность розыскных действий, но также выдвигают новые требования к обеспечению их безопасного и эффективного использования.

5. Обязательной чертой ОРО также будет являться тактический аспект её проведения. Если для обеспечения проведения ОРМ и их комплексов обычно применяется оперативная комбинация, то для обеспечения проведения ОРО проводится оперативная игра, которая включает в себя совокупность различных оперативных комбинаций, объединённых единым замыслом и направленных на решение задач ОРО и достижение её целей.

Таким образом, мы видим, что ОРО сложная многоуровневая система, которая может включать в себя в качестве подсистем другие организационно-тактические формы или их сочетания.

Лагуточкин Андрей Владимирович,
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России,
кандидат юридических наук

Бурмистров Вячеслав Александрович,
курсант 3 курса
Крымского филиала Краснодарского университета МВД России

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРЕДУПРЕЖДЕНИЯ
ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ
ОБОРОТОМ НАРКОТИЧЕСКИХ СРЕДСТВ
С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ**

Теневая сеть: как интернет становится инструментом наркотрафика. Информационно-телекоммуникационные технологии принесли человечеству беспрецедентные возможности: доступ к информации, глобальное общение, дистанционное обучение и работу. Однако эта же технологическая революция открыла новые пути для преступности, в том числе для распространения наркотических средств и психотропных веществ. Если раньше наркоторговля ограничивалась физическим контактом и локальными сетями, то интернет превратил её в глобальный, децентрализованный и трудно контролируемый бизнес.

Развитие ИКТ радикально изменило ландшафт наркоторговли. Традиционные методы сбыта, требующие личного контакта и физического перемещения товара, быстро уступают место виртуальным площадкам. Преступники используют интернет для достижения нескольких ключевых целей: 1. Расширение аудитории – онлайн-платформы позволяют обратиться к потенциальным покупателям по всему миру, преодолевая географические границы и ограничения. Реклама наркотиков в социальных сетях, на форумах и специализированных сайтах достигает огромного числа людей, значительно превышающего аудиторию, доступную при традиционных методах. 2. Обеспечение анонимности: криптовалюты, анонимные мессенджеры и виртуальные частные сети обеспечивают высокий уровень конфиденциальности для организаторов и участников наркобизнеса. Трассировка финансовых потоков и идентификация участников становится сложной задачей для правоохранительных органов. 3. Глобализация преступности: организаторы наркотрафика могут находиться в любой точке земного шара, управляя сетью сбыта дистанционно. Это создает серьезные проблемы для международного сотрудничества и расследования преступлений. Нередки случаи, когда «мозговой центр» преступной организации находится за ру-

бежом, а исполнители действуют на территории конкретной страны, например, России. 4. Создание устойчивых онлайн-платформ: современные наркоторговцы создают не просто отдельные объявления, а целые интернет-платформы, работающие как полноценные онлайн-магазины. Эти сайты предлагают широкий ассортимент НСПВ, различные способы оплаты и доставки, часто используя сложные системы шифрования и защиты от блокировки. Их долгосрочная работа свидетельствует о высокой степени организации и адаптации к противодействию правоохранительных органов.

Борьба с этим видом преступности требует комплексного подхода. Необходимы не только усиление технических средств контроля интернет-пространства, но и международное сотрудничество, совершенствование законодательства, повышение правовой грамотности населения и разработка эффективных программ профилактики наркомании. Только интегрированный подход, сочетающий в себе технические, правовые и социальные меры, способен эффективно противостоять угрозе, которую представляет собой использование интернета для распространения наркотиков. Проблема требует постоянного мониторинга и адаптации стратегий борьбы к постоянно меняющимся методам работы преступных группировок.

Цифровой наркотрафик, как преступность мигрирует в онлайн сферу. Преступления, совершаемые с использованием информационно-телекоммуникационных технологий, представляют собой одну из наиболее острых проблем современности, и Россия не является исключением. Если раньше наркоторговля велась на улицах и в подворотнях, то сегодня она уверенно переместилась в цифровую среду, обретая новые масштабы и сложность. Статистика неумолима: рост числа преступлений, связанных с незаконным оборотом наркотиков через интернет, пугает своими темпами. Цифры говорят сами за себя: с 323 уголовных дел в 2015 году до 53471 в 2020 – это не просто увеличение, это взрывной рост, демонстрирующий неэффективность прежних методов борьбы.

Эта тенденция вызывает серьезную обеспокоенность не только у правоохранительных органов, но и у депутатов Государственной Думы. Депутат В.М. Власов, например, обоснованно указывает на необходимость ужесточения наказаний за сбыт наркотиков через Даркнет – теневую часть интернета, практически неподконтрольную государству. Предложение об увеличении сроков лишения свободы для преступников, использующих Даркнет, логично, но сталкивается с основной проблемой – отсутствием эффективных оперативных рычагов для пресечения подобной деятельности.

Ярким примером масштабов проблемы является площадка «Гидра», которая, по некоторым оценкам, стала мировым лидером в онлайн-торговле наркотиками. Ее аудитория в первой половине 2019 года составляла, по оценкам экспертов, 750 тысяч человек. Ежедневно на сайте оставлялось

13625 закладок с наркотиками общей стоимостью около 227 миллионов рублей. Эти цифры шокируют и наглядно демонстрируют огромный потенциал онлайн-платформ для организации преступной деятельности.

Проблема усугубляется использованием популярных мессенджеров, таких как Telegram, для координации сделок и коммуникации между участниками наркобизнеса. Анонимность, обеспечиваемая этими платформами, значительно усложняет работу правоохранительных органов.

Таким образом, борьба с цифровым наркотрафиком требует комплексного подхода. Простые увеличения сроков наказания, хотя и необходимы, не являются панацеей. Необходимо: развитие новых технологий для мониторинга и анализа информации в Даркнете. Это потребует вложений в специальное программное обеспечение и обучение специалистов. Укрепление международного сотрудничества для борьбы с транснациональной преступностью. Наркотрафик в интернете не знает границ, поэтому совместные усилия разных стран крайне важны. Повышение уровня киберграмотности населения. Просвещение граждан о рисках, связанных с онлайн-покупкой наркотиков, поможет снизить спрос. Совершенствование законодательства, направленное на блокировку онлайн-платформ, занимающихся незаконным оборотом наркотиков, и преследование их создателей и администраторов.

Проблема цифрового наркотрафика требует незамедлительных и решительных действий. Только комплексный подход, объединяющий правоохранительные органы, законодателей, специалистов в области информационных технологий и общественность, сможет эффективно противостоять этой растущей угрозе. Игнорирование проблемы лишь приведет к еще более трагическим последствиям.

Характерной особенностью данного способа преступной деятельности является то, что она тщательно маскируется, имеет более длительный инкубационный период при распространении через различные мессенджеры или непосредственно в «Даркнете». При этом следует отметить, что начальным этапом деятельности по предупреждению и дальнейшему предотвращению незаконного оборота наркотиков является мониторинг электронных ресурсов, осуществляемый Роскомнадзором. Так, за девять месяцев 2020 года было заблокировано 14000 сайтов, на которых размещалась информация, пропагандирующая употребление наркотиков или предлагающая их приобрести. Однако, поскольку регистрация таких сайтов происходила за рубежом, зачастую невозможно установить владельцев этих электронных ресурсов, а значит, довольно сложно, если вообще возможно, полностью пресечь их деятельность и привлечь к ответственности. Кроме того, владельцы интернет-сайтов, занимающихся распространением запрещенных препаратов, часто «привлекают» покупателей с помощью различных маркетинговых уловок. Например, они предлагают наркотики в первый раз без взимания платы (для «новых покупателей») или предлагают различные

скидки (для постоянных покупателей). Создание такой бесконтактной системы характерно для наркобизнеса: каждое звено строго замаскировано, покупатель контактирует с продавцом только посредством информационно-коммуникационных технологий, а курьер, распространяющий наркотики, не знает не только личности покупателя, но и личности «закладчика» (лица, прибывшего с наркотиками в назначенное место). У этой тенденции есть несколько аспектов. Во-первых, конфиденциальность-вероятность того, что правоохранные органы выявят организаторов того или иного преступного замысла, крайне мала из-за незнания низшими слоями населения своих работодателей. Во-вторых, отсутствие личного контакта, а исключительно общение посредством информационно-коммуникационных технологий, быстро информирует потенциальных клиентов о возможности приобретения нелегальных наркотиков, и выгода быстро увеличивается.

Именно поэтому совершенствование методов совершения преступлений требует совершенствования методов борьбы с ними. Повышение эффективности при помощи информационно-телекоммуникационных технологий в преступной сфере может дать такой же результат, в том случае, если роль таких технологий вырастет и в правоохранных органах.

Да, с этой целью было создано относительно новое подразделение по раскрытию преступлений в сфере использования информационно-телекоммуникационных технологий, однако его фокус сосредоточен на мошеннических действиях. Я считаю, что если переквалифицировать данное преступление на профильную борьбу с незаконным оборотом наркотиков, то это принесет огромные плоды, так как масштабная информационная война, развязанная в таком случае органами внутренних дел против сбытчиков наркотических средств, повергнет их в шок, и не даст времени обдумать шаги, предпринять попытки найти способы обхода санкций.

Поэтому в перспективе мы можем говорить о создании еще одного оперативного подразделения, которое будет специализироваться на борьбе с распространением наркотических средств с использованием информационно-телекоммуникационной сети «Интернет», что позволит расширить спектр воздействия правоохранных органов на преступников.

Легостаев Вячеслав Петрович,
профессор кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

**ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ
ЧАСТИ 4 СТАТЬИ 18 ФЕДЕРАЛЬНОГО ЗАКОНА
«ОБ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ»
И ПУТИ ИХ РЕШЕНИЯ**

В соответствии с ч.1 ст. 18 ФЗ «Об ОРД», лица, содействующие органам, осуществляющим оперативно-розыскную деятельность, находятся под защитой государства. Эта защита проявляется в том, что государство обязуется принимать все необходимые меры по предотвращению противоправных действий в отношении защищаемых лиц. Одним из обстоятельств, гарантирующим защиту, являются положения Федерального закона «Об ОРД», касающиеся освобождения от уголовной ответственности лиц, сотрудничающих с органами, осуществляющими ОРД.

Вопросы освобождения лиц от уголовной ответственности в связи с привлечением их к конфиденциальному сотрудничеству, всегда являлись одними из основных в теории оперативно-розыскной деятельности и неоднократно являлись объектом научных исследований и дискуссий¹. Это проявлялось не только в значимости названной категории граждан, используемых в борьбе с преступностью правоохранительной системой, но и нашло в себя в законодательном закреплении, благодаря чему, в стране стабилизировалась ситуация, связанная с противодействием проявлениям организованной преступности в различных ее проявлениях.

Впервые положения об освобождении от уголовной ответственности лиц, согласившихся на сотрудничество на законодательном уровне, было закреплено в ч. 4 ст. 18 ФЗ Об ОРД, а позднее в 2009 году с учетом дополнений в ст. 317¹⁻⁹, УПК РФ и было реализовано в форме досудебного соглашения о сотрудничестве.

¹ Оперативно-розыскная деятельность: Учебник. 2-е изд., доп. и перераб. /Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова. М.: ИНФРА-М, 2004. -XIV, (Высшее образование). С.104; О. А. Вагин, А. П. Исиченко, А. Е. Чечетин. Федеральный закон Об оперативно-розыскной деятельности / постатейный комментарий к ФЗ №144-ФЗ. В ред. ФЗ от 29 апреля 2008 г. №58-ФЗ. М., 2009. С.144; Гусев В. А. Права оперативных подразделений полиции: законодательство и практика: монография / В. А. Гусев. М.: издательский дом Шумиловой И. И., 2014. (Теория и практика профессионального сыска). С. 57-60; Железняк, Н.С. Вопросы актуализации Федерального закона «Об оперативно-розыскной деятельности» : монография / Н.С. Железняк. – Красноярск: СибЮИ МВД России, 2019. С.297., и др.

Указанная норма, подчеркивает В. А. Гусев, исходя из анализа текста статьи, представляет собой попытку решения уголовно-правовых и оперативно-разыскных проблем в сфере борьбы с наиболее опасными проявлениями преступности: ее групповыми и организованными формами. Здесь законодатель четко ограничил круг лиц, подлежащих при наличии указанных условий освобождению от уголовной ответственности, участием в преступной группе¹.

В самом деле, значение привлечения членов преступных групп к сотрудничеству с органами, осуществляющими ОРД очень велико, поскольку последние как никто другой обладают оперативно-значимой информацией и разведывательными возможностями получать такую информацию. В связи с чем, основными условиями освобождения от уголовной ответственности в ч.4 ст. 18 ФЗ Об ОРД законодатель назвал факт сотрудничества с органами, осуществляющими оперативно-розыскную деятельность и содействие в раскрытии преступлений. При этом выступают обязательные условия, которые выражаются в отсутствии тяжких последствий и возмещению причиненного ущерба.

Поэтому, согласно регламентации ч.4 ст.18 ФЗ Об ОРД следует сделать вывод о том, что названные условия освобождения от уголовной ответственности законодатель применил к лицу, участнику преступной группы, который совершал преступления, но они не повлекли тяжких последствий, который является участником уголовного судопроизводства в качестве обвиняемого или подозреваемого и который желая избежать уголовной ответственности дал согласие на сотрудничество с органом, осуществляющим оперативно-розыскную деятельность.

В теории оперативно-розыскной деятельности рассматриваемые положения у многих ученых вызвали неоднозначную реакцию и в научных публикациях указывают на противоречие ч.4 ст. 18 ФЗ Об ОРД положениям ст. 75 УК РФ. Ст. 75 УК РФ предусматривает следующие основания освобождения от уголовной ответственности: совершение преступления небольшой или средней тяжести; деятельное раскаяние и содействие раскрытию преступления, а также возмещение причиненного ущерба или заглаживание причиненного вреда. По мнению ряда ученых, данное условие является оценочным, и его не следует отождествлять с одноименным квалифицирующим признаком, предусмотренным в некоторых статьях Особенной части УК России².

¹ Гусев В. А. . Права оперативных подразделений полиции: законодательство и практика: монография / В. А. Гусев. М.: издательский дом Шумиловой И. И., 2014. . (Теория и практика профессионального сыска). С.58.

² Федеральный закон «Об оперативно-розыскной деятельности»: науч.-практ. коммент. / под ред.: проф. В.В. Николюк, доц. В.В. Кальницкий, А.Е. Чечетин. 4-е изд., перераб. и доп. Омск.: ЮИ МВД России, 1999. С. 157.

Так, Н. С. Железняк полагает, что вышеуказанная норма, закрепленная в оперативно-розыском законодательстве, вступает в противоречие с действующими уголовным и уголовно-процессуальным законами, не имеет процедурных механизмов и поэтому является декларативной¹. Не оспаривая выводы Н.С. Железняка, тем не менее следует обратить внимание на возможность применения ст. 317¹⁻⁹ УПК РФ, которые регламентируют порядок освобождения лица, заключившего досудебное соглашение о сотрудничестве от уголовного наказания. Как нам представляется, по аналогии можно было бы и реализовать предписания ч. 4 ст. 18 ФЗ Об ОРД.

Теория оперативно-розыскной деятельности и предписания приказов МВД России, содержащих вопросы привлечение лица к сотрудничеству с органами, осуществляющими ОРД, предполагают это делать исключительно на добровольных началах. «Привлечение» – означает побуждение лица принять участие в осуществлении ОРМ. Отсюда следует, во-первых, что предложение о сотрудничестве должно исходить, как правило, от оперативно-розыскного органа и, во-вторых (самое существенное), что окончательное решение о возможности использования лица в ОРМ принимает только оперативно-розыскной орган (в лице своих должностных лиц), но не привлекаемое лицо².

Как нам представляется, о добровольности речи в данном случае идти не может. Очевидно, что лицу предлагается самому сделать выбор в пользу сотрудничества или быть привлеченному к уголовной ответственности. В целом, согласно данным практики в семидесяти случаях из ста, привлечение к негласному сотрудничеству осуществляется оперативными сотрудниками полиции с использованием компрометирующих материалов. С этой позиции нам интересна точка зрения А. М. Плешакова, который справедливо считает, что после совершения противоправного деяния и фактического разоблачения лицо, привлеченное к сотрудничеству, должно активно способствовать раскрытию преступлений. Данное правоустановление состоит из искусственного симбиоза элементов деятельного раскаяния (ст.75 УК РФ) и конструктивных частей специальных видов освобождения от уголовной ответственности (ст.ст.210, 228, 228.3 УК РФ и другие). Виновный должен не просто пассивно способствовать раскрытию преступлений (т.е. дать

¹ Железняк, Н.С. Вопросы актуализации Федерального закона «Об оперативно-розыскной деятельности» : монография / Н.С. Железняк. – Красноярск: СибЮИ МВД России, 2019. С.260.

² Оперативно-розыскная деятельность: Учебник. 2-е изд., доп. и перераб. /Под ред. К.К. Горяинова, В.С. Овчинского, Г.К. Синилова, А.Ю. Шумилова.М.: ИНФРА-М, 2004. -XIV, (Высшее образование).С.77.

правдивые и подробные показания), но и лично (активно) участвовать в проведение следственных действий и собирания доказательств¹.

И в самом деле, положения ч.4 ст.18 ФЗ Об ОРД, отражающие проблемы привлечения к сотрудничеству члена преступной группы не дают понятия и не раскрывают способы привлечения – на гласной или негласной основе. Как нам представляется законодатель предоставил действовать органу, осуществляющему ОРД на свое усмотрение, подразумевая:

во-первых, в силу того, что оперативные сотрудники имеют дело с подозреваемым или обвиняемым, а процедура, связанная с его освобождением будет осуществляться в рамках ст. 317¹⁻⁹ УПК РФ, то необходимо иметь в виду обстоятельства, связанные с тем, что соглашение о сотрудничестве в ряде случаев может стать достоянием других членов преступной группы;

во-вторых, ст. 317.⁹ УПК РФ, предусматривает меры социальной и правовой защиты такого лица, а механизм защиты детально прописан в нормах Федерального закона РФ от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства».

Идентичность уголовно-процессуального освобождения от наказания, предусмотренная в ст. 317¹⁻⁹ УПК РФ, указывает на то, что процедура освобождения в соответствии с ч.4 ст.18 ФЗ Об ОРД может пойти и по пути уголовно-процессуального досудебного соглашения о сотрудничестве, применив, например, закрытый порядок судебного разбирательства для такого лица.

Таким образом, учитывая то, что положения ч.4 ст. 18 ФЗ Об ОРД, являются разновидностью деятельного раскаяния следует сделать следующие выводы:

возможно освобождение лица, который изъявил желание сотрудничать с органом, осуществляющим ОРД от уголовного наказания при условии соблюдения процедур, содержащихся в предписаниях ст. 317¹⁻⁹ УПК РФ и Федерального закона РФ от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»;

полагаем возможным распространить уголовно-процессуальный порядок, регламентирующий освобождения на указанных лиц от уголовного наказания, поскольку они своими правомерными действиями утратили общественную опасность.

¹ Плешаков А. М. Освобождение от уголовной ответственности лица, привлеченного к сотрудничеству с правоохранительным органом [upord.ru>wp-content/uploads/2021/07/Плешаков.pdf](http://upord.ru/wp-content/uploads/2021/07/Плешаков.pdf)

Редкоус Владимир Михайлович,
ведущий научный сотрудник сектора административного права
и административного процесса Института государства и права РАН,
профессор кафедры управления деятельностью подразделений обеспечения
охраны общественного порядка центра командно-штабных учений
Академии управления МВД России,
доктор юридических наук, профессор

ОБ УСИЛЕНИИ ГАРАНТИЙ ЗАЩИТЫ ПРАВ И СВОБОД ЛИЧНОСТИ В ОПЕРАТИВНО-РОЗЫСКНОЙ И СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ (ОПЫТ РЕСПУБЛИКИ УЗБЕКИСТАН)

В современных условиях возрастают требования к эффективности проведения оперативно-розыскной деятельности для достижения целей ее осуществления, предусмотренных Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»¹. В этих условиях необходимо усиливать гарантии защиты прав и свобод личности², что важно для организации деятельности органов внутренних дел как Российской Федерации, так и государств – участников СНГ³.

Рассмотрим опыт Республики Узбекистан, где проводится большая работа по совершенствованию деятельности органов внутренних дел в системе правоохранительных органов Республики. В Республике Узбекистан действует Закон Республики Узбекистан от 25 декабря 2012 г. № ЗРУ-344 «Об оперативно-розыскной деятельности»⁴.

Оперативно-розыскная деятельность в Законе РУз об ОРД определена как «вид деятельности, осуществляемый оперативными подразделениями государственных органов, специально уполномоченных на то настоящим Законом (далее – органы, осуществляющие ОРД) посредством проведе-

¹ Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

² Кирюхин, В.В. Цифровая полиция для цифрового общества / В. В. Кирюхин // Цифровая трансформация системы МВД России : Сборник научных статей по материалам Международного форума. В 2-х частях, Москва, 20 октября 2022 года / под ред. И.Г. Чистобородова. Том Ч. 1. – М: Академия управления Министерства внутренних дел Российской Федерации, 2022. – С. 357-363.

³ Редкоус, В. М. Проблемы правового регулирования обеспечения личной безопасности в современных условиях / В. М. Редкоус // Конституционные права и свободы человека как высшая ценность государства и общества : Сборник научных трудов Всероссийской научно-практической конференции, Москва, 08 декабря 2022 года. – Москва: Московский университет МВД РФ им. В.Я. Кикотя, 2023. – С. 106-111.

⁴ Закон Республики Узбекистан от 25 декабря 2012 г. № ЗРУ-344 «Об оперативно-розыскной деятельности» // Народное слово. – 2012. – 26 декабря.

ния оперативно-розыскных мероприятий». Основными задачами ОРД являются: обеспечение защиты прав, свобод и законных интересов человека, собственности юридических и физических лиц, безопасности личности, общества и государства; предупреждение, выявление, пресечение и раскрытие преступлений, а также выявление и установление лиц, причастных к их подготовке и совершению; осуществление розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, без вести пропавших лиц и иных лиц в случаях, предусмотренных законодательством, а также установление личности неопознанных трупов; сбор информации о лицах, событиях, действиях (бездействии), создающих угрозу безопасности личности, общества и государства.

Большую роль в правовом регулировании ОРД играют основные принципы ее осуществления¹. Основными принципами оперативно-розыскной деятельности являются законность, приоритет прав, свобод и законных интересов человека, конспирация, сочетание гласных и негласных методов.

Законность в ОРД означает, что органы, осуществляющие ОРД, и их работники обязаны точно соблюдать и исполнять требования Конституции Республики Узбекистан, настоящего Закона и других актов законодательства. Отступление от точного соблюдения и исполнения законодательства при осуществлении ОРД является нарушением законности и влечет за собой установленную ответственность.

Принцип приоритета прав, свобод и законных интересов человека означает, что органы, осуществляющие ОРД, и их работники при проведении оперативно-розыскных мероприятий обязаны соблюдать права, свободы и законные интересы человека.

Запрещается осуществление действий, которые приводят к разглашению сведений об обстоятельствах частной жизни человека, ставят под угрозу его жизнь, здоровье, унижают честь и достоинство. Никто не может быть подвергнут пыткам, насилию, другому жестокому или унижающему честь и достоинство человека обращению.

Полученная в результате проведения оперативно-розыскных мероприятий информация, не связанная с совершением преступления или иного правонарушения, не может быть использована для ограничения прав, свобод и законных интересов человека.

В случае нарушения органами, осуществляющими ОРД, и их работниками прав, свобод и законных интересов человека, данные органы и их руководители обязаны принять меры по восстановлению этих прав, свобод и законных интересов, возмещению причиненного вреда и привлечению виновных к ответственности в установленном порядке.

¹ Редкоус, В. М. Правовое регулирование оперативно-розыскной деятельности в Республике Узбекистан / В. М. Редкоус // Актуальные вопросы борьбы с преступлениями. – 2021. – № 4. – С. 9-17.

Органы, осуществляющие ОРД в республике Узбекистан, обязаны: принимать в пределах своих полномочий все необходимые меры по защите прав, свобод и законных интересов человека, собственности юридических и физических лиц, а также по обеспечению безопасности личности, общества и государства; принимать меры по предупреждению, выявлению, пресечению и раскрытию преступлений, а также выявлению и установлению лиц, причастных к их подготовке и совершению; организовать работу по осуществлению розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от уголовного наказания, без вести пропавших лиц и иных лиц в случаях, предусмотренных законодательством, а также по установлению личности неопознанных трупов; принимать все необходимые меры по исполнению письменных поручений органов дознания, следствия, указаний и поручений прокурора о проведении оперативно-розыскных мероприятий; соблюдать принцип конспирации при осуществлении ОРД; не разглашать без согласия граждан сведения, касающиеся их частной жизни, затрагивающие их честь и достоинство; обеспечивать безопасность жизни и здоровья граждан, имущества юридических и физических лиц при проведении оперативно-розыскных мероприятий; обеспечивать безопасность окружающей среды при проведении оперативно-розыскных мероприятий; обеспечивать безопасность своих работников и лиц, оказывающих содействие органам, осуществляющим ОРД, а также членов их семей, защиту их имущества от преступных посягательств; информировать друг друга о ставших известными им фактах преступной деятельности, относящихся к компетенции этих органов, и оказывать друг другу необходимую помощь в решении возложенных на них задач; эффективно применять имеющиеся силы и средства ОРД в решении возложенных на них задач. Органы, осуществляющие ОРД, могут нести и иные обязанности в соответствии с законодательством.

В Республике Узбекистан был принят Указ Президента Республики Узбекистан от 10 июня 2024 г. №№ УП-89 «О мерах по дальнейшему усилению гарантий надежной защиты прав и свобод личности в оперативно-розыскной и следственной деятельности»¹. Рассмотрим более подробно ряд его основных положений.

В Республике Узбекистан проводится широкомасштабная работа, направленная на поднятие на новый уровень системы защиты прав человека на основе принципа «Во имя чести и достоинства человека», усиление гарантий защиты прав и свобод личности в деятельности судебных и правоохранительных органов, а также укрепление доверия населения к правоохранительной системе. Однако, судебнo-следственная практика показывает неполное задействование эффективных механизмов обеспечения гарантий защиты

¹ Указ Президента Республики Узбекистан от 10 июня 2024 г. №№ УП-89 «О мерах по дальнейшему усилению гарантий надежной защиты прав и свобод личности в оперативно-розыскной и следственной деятельности»// Национальная база данных законодательства, 11.06.2024 г., № 06/24/89/0412.

прав и свобод человека, а также наличие необходимости усиления мер по надежному обеспечению судом конституционных прав на свободу и личную неприкосновенность лица, обвиняемого в совершении преступления.

Исходя из приоритетных направлений, определенных в Стратегии «Узбекистан – 2030», в целях повышения эффективности судебной деятельности, обеспечения на практике принципа равенства и состязательности сторон в досудебном производстве, а также достижения эффективной защиты прав и свобод лица в оперативно-розыскной и следственной деятельности предложено согласиться с предложениями Верховного суда, Генеральной прокуратуры, Министерства внутренних дел, Службы государственной безопасности и Министерства юстиции Республики Узбекистан, предусматривающими с 1 января 2025 года:

внедрение порядка рассмотрения вопроса выдачи санкции на процессуальные решения на стадии досудебного производства по уголовным делам отдельными судьями – следственными судьями в районных, городских судах по уголовным делам;

введение должности следственного судьи в районных, городских судах по уголовным делам;

определение порядка единоличного пересмотра санкций на процессуальные решения, выданных следственным судьей на стадии досудебного производства по уголовным делам судом Республики Каракалпакстан, областными и Ташкентским городским судами, Военным судом Республики Узбекистан, только в апелляционной инстанции;

предоставление следственным судьям полномочия по рассмотрению дел об административных правонарушениях;

сохранение действующего порядка пересмотра дел об административных правонарушениях, рассматриваемых следственными судьями, в вышестоящих инстанциях.

Следственный судья наделяется полномочием рассмотрения следующих уголовных материалов, в частности вопроса применения санкций и мер принуждения:

а) *санкций по*: ходатайству, связанному с применением меры пресечения в виде заключения под стражу или домашнего ареста; ходатайству, связанному с продлением срока содержания под стражей или домашнего ареста; ходатайству о приостановлении действия паспорта (проездного документа); ходатайству об эксгумации трупа; ходатайству об аресте почтово-телеграфных отправок; ходатайству о производстве обыска; ходатайству о прослушивании переговоров, ведущихся с телефонов и других телекоммуникационных устройств, снятии передаваемой по ним информации; ходатайству об аресте имущества;

б) мер принуждения по: ходатайству об отстранении обвиняемого от должности; ходатайству о помещении лица в медицинское учреждение; ходатайству о продлении срока пребывания обвиняемого в медицинском учреждении; ходатайству о продлении срока задержания до сорока восьми часов;

в) ходатайств прокурора о предварительном закреплении показаний свидетеля и потерпевшего (гражданского истца).

Определены основные направления деятельности следственного судьи:

справедливое и объективное выполнение обязанностей, возложенных на следственного судью в порядке, предусмотренном законодательством;

обеспечение верховенства закона, социальной справедливости, гражданского мира и согласия;

эффективная защита прав и законных интересов граждан и юридических лиц в судебном порядке.

Также определено, что

следственный судья осуществляет свою деятельность независимо с осуществлением правосудия;

следственных судей, а также формирование судейского корпуса осуществляются согласно порядку, установленному законом;

руководство организационной деятельностью следственного судьи осуществляется соответственно председателями суда Республики Каракалпакстан, областных и Ташкентского городского судов, Военного суда Республики Узбекистан.

Формируется штатная численность для должности следственного судьи за счет действующих штатных единиц судов, а также дополнительных штатных единиц, выделяемых на 2025 – 2027 годы.

Таким образом, представленные в рассмотренном указе Президента Республики Узбекистан меры должны способствовать повышению эффективности оперативно-розыскной и следственной деятельности в Республике Узбекистан, что будет способствовать повышению эффективности деятельности органов внутренних дел в целом¹.

¹ Кирюхин, В.В. Участие граждан в охране общественного порядка: в поисках разумного баланса / В. В. Кирюхин // Закон и правопорядок в Третьем тысячелетии : IX Балтийский юридический форум. Материалы международной научно-практической конференции, Калининград, 12 декабря 2020 года. – Калининград: Калининградский филиал Санкт-Петербургского университета МВД России, 2021. – С. 93-94.

Савченко Михаил Юрьевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России

Коваленко Анна Андреевна,
курсант 4 курса
Краснодарского университета МВД России

ИНФОЦЫГАНСТВО КАК ДЕЛИКТ В УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ И ИСПОЛЬЗОВАНИЕ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ДЛЯ ЕГО ПРЕСЕЧЕНИЯ

В связи с развитием технологий, медиапространства, сети Internet увеличивается количество преступлений и правонарушений в сфере телекоммуникаций. Одним из видов подобного мошенничества является «инфоцыганство» и представляет собой опасное явление в современном информационном обществе. Данный термин получил известность в последние 5 лет, что связано с появлением нового поколения блогеров, преимущественно специализирующихся на продаже инфопродуктов.

Инфоцыгане – это артисты, блогеры, тиктокеры, другие представители медиапространства, которые занимаются продажей собственных книг, курсов, тренингов, не обладающих практической пользой и ценностью. Технология привлечения клиентов строится на достаточно простой по своей реализации схеме: злоумышленники, с помощью психологических приемов и манипуляций воздействуют на разум и чувства своих жертв, тем самым, заставляют их поверить в успешность их инфопродукта.

Схема привлечения клиентов состоит из нескольких важных этапов, с прохождением которых у жертв мошенников возникает интерес и желание приобрести курс.

Первый этап: прогрев аудитории. Создатель «волшебных курсов» рассказывает о своем проекте, который помог ему разобраться в себе, улучшил его жизнь, мозг, фигуру, помог построить отношения и многое другое. При этом, многократно говорится о скидках, акциях, о том, что «не будет другой возможности приобрести продукт». Вокруг такого события создается искусственный спрос: говорят о том, что количество мест ограничено, прикрепляются фейковые комментарии и отзывы, где можно якобы увидеть гарантированный результат использования продукта.

Второй этап: привлечение внимания с помощью «кричащих», провокационных картинок и слоганов. Цель злоумышленника на этом этапе – сделать так, чтобы его заметили. Это могут быть не только картинки и слова, но и музыка, социальные ролики, в целом, все, что привлекает внимание.

Как правило, здесь же начинается внедрение в разум жертвы: мошенники пишут свои истории и истории других своих жертв, поясняя, как им удалось изменить свою жизнь и каким способом. Обычно инфопродукты обещают практически мгновенный результат за невысокую стоимость. Нередко говорят и о договоренности с банком о рассрочке или кредите. Некоторые даже обещают, что сами выплатят проценты банку, а покупателям нужно будет оплатить только стоимость курса.

Третий этап: покупка курса и осознание его бесполезности. На этом этапе человек приобретает курс или тренинг, вникает в него, а в результате обнаруживает бесполезность его использования. Чаще всего это происходит через некоторое время после покупки, после нескольких попыток следовать правилам тренинга, следом – отсутствие изменений и осознание сделанной ошибки. Оказывается, что вся информация, которой наделен инфопродукт, находится в свободном доступе в интернете, нужно лишь поискать.

Каковы действия оперативных подразделений по профилактике, предупреждению и раскрытию мошеннических схем инфоцыган?

Первостепенно, необходимо информирование населения о существовании такого вида мошенничества как инфоцыганство, о его активном распространении. Целью данного противоправного деяния является завладение денежными средствами, путем внедрения в сознание граждан и использования психологических приемов.

Далее, необходимо выявить наиболее уязвимую категорию граждан. Как правило, перед тем как осуществить покупку какого-либо продукта, у человека есть определённый запрос, ответ на который они находят в продукте злоумышленником. Это может быть, например желание научиться писать научные статьи, рисовать, обучиться SMM, стать блогером или продюсером. И у таких людей есть характерные признаки, по которым мошенники их вычисляют:

- эмоциональное выгорание
- утрата бизнеса или работы
- поиск работы после декретного отпуска
- люди с психическими расстройствами или отклонениями, которые считают, что у них не сложилась жизнь.

Ещё двумя важными категориями жертв являются:

1. Люди в возрасте, обладающий низкой финансовой грамотностью, которые с лёгкостью могут довериться злоумышленнику
2. Молодёжь, у которой отсутствует жизненный опыт и которая надеется получить профессию или разбогатеть.

В целях контроля за ними и недопущения в отношении их совершения данного противоправного деяния, необходимо периодически опрашивать их о попытках внедрения в их доверия третьих лиц, а также участвовать в родительских собраниях (если речь идет о школьниках).

Необходимо понимать также и сложность в квалификации подобного рода преступлений. С точки зрения Гражданского Кодекса РФ действия инфоцыган попадают под ст. 1102 ГК РФ: неосновательное обогащение вследствие оказания услуг без подписания договора, а также Закона о защите Прав Потребителей РФ:

- отсутствие своевременной и полной информации о товарах и услугах, которое должно обеспечивать возможность их правильного выбора (ст. 10 ЗоЗПП РФ);
- ответственность исполнителя за ненадлежащую информацию о товаре, услуге (ст. 12 ЗоЗПП РФ);
- нарушение прав потребителя в случае его одностороннего отказа от еще неисполненного договора (ст. 782 ГК РФ, ст. 29 ЗоЗПП РФ, ст. 32 ЗоЗПП РФ);

В остальных случаях, когда урегулировать конфликт по возврату денег заказчику миром не удаётся, действия преступника можно рассматривать через призму Уголовного Кодекса РФ, а именно:

- незаконная предпринимательская деятельность (ст. 171 УК РФ)
- мошенничество (ст. 159 УК РФ),

Осуществляя предпринимательскую деятельность в сфере оказания услуг, «инфоцыгане», зачастую, не являются субъектами предпринимательской деятельности в РФ (не работают через ИП или ООО, без регистрации в налоговой), не указывают своё настоящее имя (используют псевдоним) и фактический адрес, куда можно отправить официальную претензию о возврате денег в случае недовольства качеством их продуктов, а также могут быть юридически оформлены в другой стране. Это является существенным препятствием для защиты прав лиц, пострадавших от данного вида недобросовестной деятельности. В практике судопроизводства есть немного случаев, когда «инфоцыган» привлекали к уголовной ответственности по статьям 171 и 159 УК РФ. Например, дело по ч. 2 ст. 171 УК РФ в отношении куратора «Бизнес Молодости», Пудова А.Н., который активно использовал мошеннические схемы: псевдо-образовательную (его знания были построены на опыте магов и чародеев из 90-х) и псевдо-предпринимательскую деятельность (применение статьи 171 УК РФ стало возможным в результате того, что Пудов осуществлял свою деятельность без лицензии, хотя в данном случае она была обязательна). Он наблюдал за «экстрасенсом» Анатолием Кашпировским, изучал движения, тембр голоса, взгляд, работу с аудиторией Кашпировским. Он понял, что при правильной подаче на бессмысленном наборе слов можно заработать. В результате проведения таких схем сумма ущерба, пострадавшим от его Международным научным журналом «ВЕСТНИК НАУКИ» № 6 махинаций (которых на данный момент не менее девяти человек) составила 13 654 633 рубля.

Депутат Государственной Думы Б. Чернышев предложил определить порядок лицензирования бизнес-тренингов и курсов личностного развития,

чтобы оградить от аферистов в этой сфере. Для получения лицензии, предполагает Чернышев, нужно не только наличие личных заявлений, но и достоверные данные (о посещении образовательных организаций) и документы (диплом об образовании, документ, свидетельствующий о прохождении аттестации, удостоверение о повышении квалификации), которые подтверждали бы компетентность человека в образовательной сфере. Если это личная, самостоятельно разработанная методика, то она должна быть утверждённой, апробированной Министерством образования.¹

В целях раскрытия данного противоправного деяния необходимо следующее:

1. Собирать и документировать действия и бездействия лиц, совершающих данный вид мошенничества.

2. Проведение таких оперативно-розыскных мероприятий как:

- опрос
- прослушивание телефонных переговоров;
- снятие информации с технических каналов связи;
- получение компьютерной информации.

А также важным оперативно-розыскным мероприятием является проверочная закупка, благодаря которой можно изобличить факт мошенничества.

3. Тесное взаимодействие с такими подразделениями как:

- Бюро специальных технических мероприятий;
- Оперативно-поисковое бюро;
- Информационный центр;
- Главный информационно-аналитический центр.

Обмен информацией и совместное проведение оперативных мероприятий позволяет эффективно раскрыть и пресечь экономические преступления, в том числе и инфоцыганство.

4. Разработка

Для раскрытия многоэпизодности данного деяния собираются все факты причинения имущественного вреда проводится отдельная разработка лица, совершившего преступления (например, внутрикамерная разработка).

5. Направление запросов о движении денежных средств в налоговую, коммерческие банки и другие финансовые организации.

6. Одним из эффективных методов раскрытия экономических преступлений, в том числе по статье мошенничество, является проведение финансового анализа хозяйственной деятельности подозреваемого лица или его организации. При использовании этого метода можно выявить расхождения по бухгалтерской отчетности, выявить схемы отмывания денег и иные признаки преступной деятельности.

¹ Инфоцыганство как явление в интернет-пространстве // URL: <https://cyberleninka.ru/article/n/infotsyganstvo-kak-yavlenie-v-internet-prostranstve/viewer> (дата обращения: 27.11.2024)

Все материалы проверки направляются следователю для возбуждения уголовного дела.

Что можно сделать, чтобы усилить контроль над медиа– сектором?

На сегодняшний день в Государственной Думе создана рабочая группа для подготовки законопроекта об урегулировании работы инфобизнесменов и коучей. В совете федерации также прошли совещание для обсуждения поправок. Одним из предложений по данному законопроекту является создание реестра о продаже онлайн-услуг. Если законопроект будет принят, то данный реестр позволит пользователям, которые хотят приобрести услуги у блогера, проверить наличие определённой лицензии, реальные отзывы, диплом об образовании коуча и т.д.¹

Необходимо отметить, что на сегодняшний день в уголовном законодательстве нет статьи, которая содержала бы в себе признаки и определение инфоцыганства. Соответственно, пока данная норма не будет принята, контролировать данную область будет проблематично. Потому как законодательство не просто определяет преступления и устанавливает их квалификацию, но и устанавливает сроки давности, процедуру и правила расследования, устанавливает ответственность. То есть, можно сказать, что законодательство создает правовые рамки, в которых осуществляется процесс раскрытия преступления.

¹ В Госдуме готовят поправки о коучах, блогерах и инфоцыганах - новости Право.ру (pravo.ru) // URL: <https://pravo.ru/news/251450/> (дата обращения: 27.11.2024)

Савченко Михаил Юрьевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России

Самойленко Ольга Александровна
курсант 3 курса
Краснодарского университета МВД России

ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ НА ТЕРРИТОРИИ ПРОВЕДЕНИЯ СПЕЦИАЛЬНОЙ ВОЕННОЙ ОПЕРАЦИИ

Изменение геополитических отношений в мире привело к введению режима Специальной Военной Операции (далее СВО) в Российской Федерации. Этот режим обусловил множество процессов, которые негативно сказались на состоянии преступности. Так в 2022 году в Уголовный Кодекс РФ были введены 14 составов преступлений, которые связаны с реализацией СВО, например такие статьи, как ст. 207.3 УК РФ, ст.280.3 УК РФ, 284.2 УК РФ. Так же прослеживается рост преступлений, совершенных с использованием информационно-телекоммуникационных технологий (ст.205.1, ст.205.21, ст.207, ст. 282 УК РФ). В период с 2020-2022 г. средние показатели такого рода преступлений возросли свыше 200% по сравнению с предшествующими годами, и наиболее активный рост наблюдается в 2022, то есть с началом СВО. На освобожденных территориях преступления обладают высоким уровнем латентности. Несмотря на усиление охраны общественного порядка ситуация, связанная с преступностью, остается нестабильной.

Так 24.06.2023 года вступил в силу Федеральный Закон 270-ФЗ «Об особенностях уголовной ответственности лиц, привлекаемых к участию в специальной военной операции». В статье 1 говорится о правовых гарантиях освобождения от уголовной ответственности лиц, призванных на военную службу, заключивших контракт о прохождении военной службы в ВС РФ в период мобилизации, военного положения или в военное время¹. Теперь лица, совершившие преступления небольшой или средней тяжести могут освобождаться от уголовной ответственности если они подписывают контракт с ВС РФ или же призваны в условиях мобилизации.

Большой проблемой так же остается самовольное оставление места службы и дезертирство. Несмотря на всю строгость наказания за данные

¹ Федеральный Закон от 24.06.2023 № 270-ФЗ (ред. от 24.06.2023) «Об особенностях уголовной ответственности лиц, привлекаемых к участию в специальной военной операции» // Собрание законодательства РФ. - 26 июня 2023. - № 26. ст. 4678.

преступления, это не останавливает военных. Такие случаи нередко освещаются в СМИ.

Для розыска и задержания данных лиц сотрудники оперативных подразделений уголовного розыска используют все методы оперативно-розыскной деятельности. Так, первым из методов является объявление плана «перехват» при условии, что сообщение об оставлении военной части или же дезертирстве поступило в кратчайший срок, для выявления военнослужащих по «горячим следам». Если же военный, оставивший место несения службы, не был найден в кратчайшие сроки, то оперативные подразделения уведомляют жителей близлежащих населенных пунктов о том, что эти лица разыскиваются и, если граждане обладают какой-либо оперативно-значимой информации о местонахождении этих лиц, им необходимо связаться с правоохранительными органами. Параллельно с вышеперечисленными мероприятиями производится обход близлежащих районов и опрос граждан. В следствие его проведения оперативные подразделения получают информацию о последнем их местонахождении или же особых приметах, вооружены ли разыскиваемые лица и в каком психическом состоянии они находились.

Как правило, военнослужащие предпочитают выбирать в качестве временного укрытия заброшенные и (или) полуразрушенные дома, коих много, квартиры, реже подвалы. В основном военные с целью сокрытия своей личности военные приобретают гражданскую форму одежды в целях «смешаться с толпой». В данной ситуации наиболее логичным и эффективным способом розыска данных лиц является обход близлежащих магазинов, в ассортименте которых представлен интересующий товар. При наличии камер следует запросить и проанализировать видеозаписи с них. Если же таковых не имеется применяется опрос продавцов и консультантов).

Следует учитывать, что поиск может быть осложнен отсутствием камер видеонаблюдения в населенных пунктах. Как правило, в малонаселенных районах постоянно проживающие там лица обращают внимание на «чужие» машины и могут предоставить информацию о направлении ее движения, а так данные о ее государственном номере, марки и цвета. Исходя из имеющихся данных о скрывающихся лицах, а именно фамилии, имени, отчества и даты рождения, целесообразно произвести оперативно-розыскное мероприятие «наведение справок» с параллельной проверкой по учетам. В результате произведенных ОРМ оперативные сотрудники уголовного розыска получают информацию о наличии судимостей, а также нахождении в розыске скрывшегося лица.

Следует брать во внимание, что на присоединенных территориях военнослужащие украинских военных сил и граждане, разделяющие их позицию, ведут «подпольную» борьбу с российскими военными, что так же является преступлением, запрещенным Уголовным Кодексом Российской Фе-

дерации. А именно, некоторые гражданские лица добровольно либо вследствие вербовки, осуществляемой путем шантажа, угроз применения насилия, производят сбор сведений о численности, перемещении и местах дислокации российских сил.

Одним из примеров является 51-летний гражданин Украины Александр Соколов. Собранные данные он передавал украинским военным посредством сети «Интернет» с использованием мессенджеров. В марте 2023 года Соколов разместил на личной странице социальной сети публикации, призывающие к убийству сотрудников правоохранительных органов и судебного сообщества Российской Федерации.

Оперативными сотрудниками Луганской области в подобных случаях проводится комплекс ОРМ, включающий в себя:

- мониторинг социальных сетей, с целью выявления факта совершения преступления и для предположения цели публикации того или иного сообщения.

- наведение справок на лицо путем использования известных данных с целью выявления его круга общения, места работы, проживания, так как все эти данные в последующих оперативно-розыскных мероприятиях могут помочь при дальнейшем раскрытии преступления и задержании преступника.

- по ранее выясненным данным оперуполномоченные могут провести проверку по учетам, тем самым выяснить, был ли гражданин ранее судим, где проживает и полную информацию о его личности. (Например, может пригодиться информация, где прописан подозреваемый, нередко такие люди прописаны на территории Украины).

имеет место легендированная беседа с лицами, состоящих в какой-либо связи с подозреваемым, как правило, такие граждане состоят в группах в социальных сетях с тематикой, направленной на поддержку армии Украины или же, напротив, дискредитации армии Российской Федерации.

- если лицо использует приложения для зашифровки информации (примером могут выступать так называемые VPN) о себе и своем местонахождении, сотрудники оперативного подразделения направляют поручение в подразделения БСТМ для расшифровки этой информации и установления местонахождения лица.

В отношении Соколова Верховный суд вынес обвинительный приговор по статье 276 (шпионаж) УК РФ и ч.2 ст.280 (публичные призывы к осуществлению экстремистской деятельности) УК РФ. Он был приговорен к 16 годам лишения свободы.

В следствии военных действий, происходящих в зоне конфликта, граждане имеют несанкционированный и беспрепятственный доступ к различным видам оружия и боеприпасов, а также взрывных устройств и веществ. Результатом этого является создание так называемых «схронов», то есть тайников с оружием.

Примером данного преступления является дело гражданина Украины Эмира Бекирова, который на территории полуострова Крым, а именно в городе Севастополе оказался причастен к созданию «схрона», в котором правоохранительные органы обнаружили две сотни патронов к огнестрельному оружию и 12 кг тротила.

Сотрудники уголовного розыска провели скрытое наблюдение за подозреваемым лицом, целью которого было узнать, где именно расположен схрон, как действует подозреваемый, есть ли у него «помощники». Параллельно проводились зашифрованные опросы для выяснения оперативно-значимой информации об особенностях его личности. Данный гражданин Украины был приговорен к семи годам лишения свободы.

Из всего вышесказанного можно сделать вывод, что на присоединенных территориях большая часть преступлений обладает высокой латентностью. А та часть, которую удалось раскрыть свидетельствует о том, что в новых регионах преобладают преступления, связанные с дезертирством, создание складов с оружием – «схронов» и шпионаж.

Также необходимо учитывать специфику местности, которая значительно отягощает раскрытие преступлений. Иногда это просто невозможно из-за проводимых боевых действий.

Сафронов Андрей Алексеевич,
начальник кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

О НЕКОТОРЫХ ВОПРОСАХ ИСПОЛЬЗОВАНИЯ РЕЗУЛЬТАТОВ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

Успех в деятельности по выявлению и раскрытию преступлений обусловлен эффективностью взаимодействия подразделений, уполномоченных на выполнение данных государственно-властных функций.

Во многом эффективность раскрытия, расследования и предотвращения преступлений в значительной степени зависит от четко налаженной и согласованной деятельности следователя и оперативных подразделений, сочетания процессуальных и оперативно-розыскных форм получения доказательств. Одной из таких форм является использование информации полученной оперативно-розыском путём для установления истины по уголовному делу¹.

Процесс использования результатов оперативно-розыскной деятельности требует строгой нормативно-правовой регламентации, так как проведение оперативно-розыскных мероприятий зачастую затрагивает конституционные права и свободы человека и гражданина, признанные в нашей стране высшей ценностью государства. Так, например, при проведении такого мероприятия, как прослушивание телефонных переговоров, нарушает право на тайну телефонных переговоров, регламентированную статьей 23 Конституции Российской Федерации². Так, перехватывая информацию, передаваемую между абонентами, одним из которых является объектом ОРМ, во время диалога, оперативный сотрудник получает информацию о его личной жизни, о различного рода данных, составляющих ту или иную тайну, защищаемую законом. Сотрудник подразделения, осуществляющего ОРД, прежде чем начать прослушивание телефонных переговоров, обязан получить санкцию суда. Это возлагает на него обязанность по сохранению полученной информации и недопущению ее распространения или перехвата кем-либо. Таким образом, завладев информацией о личной жизни другого человека, субъект ОРМ обязан также принять меры к ее сохранности, чтобы в дальнейшем ее использование в установлении истины по делу. Исходя из

¹ Сорокин Игорь Николаевич Использование результатов оперативно-розыскной деятельности в уголовном судопроизводстве // Концепт. 2014. №12. URL: <https://cyberleninka.ru/article/n/ispolzovanie-rezultatov-operativno-rozysknoy-deyatelnosti-v-ugolovnom-sudoproizvodstve> (дата обращения: 18.07.2022).

² Конституция Российской Федерации [Текст]: (с гимном России). – Москва : Проспект, 2022. – С. 8.

важности процедуры перенаправления информации от оперативных подразделений к подразделениям, осуществляющим предварительное следствие по уголовному делу, законодатель подходит к данному вопросу строго императивно.

Порядок и условия реализации информации, полученной посредством проведения оперативно-розыскных мероприятий (далее ОРМ), в процессе доказывания по уголовному делу отражены в большом объеме нормативно-правовых актов. В частности в ст. 11 ФЗ «Об оперативно розыскной деятельности» сказано, что результаты оперативно-розыскной деятельности (далее ОРД) могут быть использованы для подготовки осуществления следственных и судебных действий¹, в ст. 89 УПК РФ также разъясняется, что в процессе доказывания запрещается использование только тех результатов ОРД, которые не отвечают требованиям, предъявляемым доказательствам уголовно-процессуальным законом². Информации полученная оперативно-розыскным путём может служить и основанием для возбуждения уголовного дела в соответствии со ст. 5 УПК РФ.

Вместе с тем, ОРД не может существовать как отдельный вид деятельности, он находится в тесной связи с уголовным процессом. Как правило, любые результаты ОРМ, представленные следователю или дознавателю, подлежат тщательной проверке на предмет законности получения указанной информации, достоверности и допустимости доказательств. Для этих целей может осуществляться ряд следственных действий, для каждой ситуации подбираются наиболее подходящие тактические приёмы и методы их проведения. Несмотря на то, что в законе закреплена возможность использования результатов ОРМ в процессе расследования и в доказывания по уголовному делу, на сегодняшний день существует множество проблем касательно возможности реализации такой информации в уголовном процессе. Большинство из них связаны с тем, что оперативные сотрудники не всегда видят перспективы применения тех или иных результатов ОРМ. Более того, требования к оценке и использованию результатов доказательств в уголовном процессе существенно противоречат требованиям, предъявляемым к ОРД. Это проявляется в излишней осторожности регламентации уголовно-процессуального использования результатов ОРМ.

На сегодняшний день круг ученых считает, что применение результатов ОРМ является необходимым подспорьем для доказательственной базы, собранной посредством проведения следственных действий. Однако следует указать, что в научной литературе все еще можно встретить негативные оценки использования результатов ОРД в качестве доказательств. Но такие

¹ Об оперативно-розыскной деятельности [Текст]: Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ // СЗ РФ. - 1995. - № 33. - Ст. 11.

² Уголовно-процессуальный кодекс Российской Федерации. [Текст]: – Москва : Проспект, 2022. – С. 25.

суждения основываются на неверном толковании ст. 89 УПК РФ, сформулированной в запретительном контексте. Поскольку указанная норма не исключает возможность использования результатов ОРД в доказывании, а лишь требует неукоснительного соблюдения законодательства при их получении и использовании. Следует отметить, что это не противоречит принципу законности – одному из главных принципов оперативно-розыскной деятельности¹.

Для решения указанных выше проблем следует разобраться в причинах этих негативных тенденций, рассмотреть сущность правоотношений, возникающих из взаимодействия органов предварительного следствия и оперативных подразделений и дать определение основным понятиям. Пункт 36.1 статьи 5 УПК РФ определяет результаты ОРД как сведения, полученные в соответствии с ФЗ «Об ОРД» о признаках подготавливаемого, совершаемого или совершенного преступления, лицах подготавливающих, совершающих, совершивших преступление или скрывшихся от органов дознания, следствия или суда². При этом использование результатов оперативно-розыскной деятельности определено не только федеральными законами, но и ведомственными нормативно-правовыми актами.

Порядок и условия передачи результатов ОРД подразделениям, осуществляющим предварительное расследование, отражены в Инструкции, утвержденной приказом МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68. Так, согласно Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд результаты ОРД могут служить поводом и основанием для возбуждения уголовного дела; быть использованы для подготовки и осуществления следственных действий; быть использованы в доказывании по уголовным делам³.

¹ Об оперативно-розыскной деятельности [Текст]: Федеральный закон Российской Федерации от 12 августа 1995 г. № 144-ФЗ // СЗ РФ. - 1995. - № 33. - Ст. 3.

² Уголовно-процессуальный кодекс Российской Федерации. [Текст]: – Москва : Проспект, 2022. – С. 5.

³ Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд – Приказ МВД России, Министерства обороны РФ, ФСБ России, Федеральной службы охраны РФ, Федеральной таможенной службы, Службы внешней разведки РФ, Федеральной службы исполнения наказаний, Федеральной службы РФ по контролю за оборотом наркотиков, Следственного комитета РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68 [Электронный ресурс] // СПС «Гарант» URL: <https://base.garant.ru/70531824/53f89421bbdaf741eb2d1ecc4ddb4c33/> (дата обращения 19.07.2022).

Третий раздел вышеуказанного нормативно-правового акта содержит в себе требования, которые должны предъявляться к результатам ОРД, согласно статье 89 УПК РФ.

Как было отмечено ранее, оперативно-розыскные мероприятия направлены на установление истины по делу – изобличение преступника и раскрытие преступления. Однако сами результаты ОРД могут стать доказательствами только после закрепления их процессуальным путём. Таким образом, можно сделать вывод о том, что сведения, полученные в рамках ОРМ, представляют собой некий информационный продукт. Информация, полученная посредством проведения ОРМ, может быть отражена в различных документах (справках, рапортах, актах и др.) или зафиксирована на материальных носителях (фото пленках, фотоснимках, дисках, накопителях информации и т.д.). Далее необходимо придание гласности указанной информации (рассекречивание) с сокрытием при необходимости тех категорий источников, которые подлежат разглашению только с их письменного согласия. Именно на этом этапе возникает проблема, поскольку оперативный сотрудник рассекречивает материалы ОРД лишь в той части, в которой считает необходимым. Часто это становится причиной невозможности оценки следователем полноты всех обстоятельств по уголовному делу и вытекающими из этого отрицательными последствиями в виде продления сроков расследования или нарушения разумных сроков уголовного судопроизводства. Это связано с различием в принципах работы двух подразделений – следственного и оперативного. Если в последнем применим симбиоз негласных и гласных методов (статья 3 ФЗ об ОРД), то деятельность следствия – только публичная. При этом не представляется возможным исключение негласных способов получения информации оперативными подразделениями, так как необходимая скрытность ОРД является, на наш взгляд, справедливым ответом государства на латентные проявления преступности, а также скрытность преступников и маскировка следов совершения преступления. Многие авторы в своих трудах акцентируют внимание на этом вопросе. Так, например, Полуянов и Филатова указывают не только на возможность, но и декларируют необходимость использования конспиративных элементов в оперативно-розыскной деятельности: «На сегодняшний день оперативные сотрудники должны правильно использовать все формы негласности в оперативно-розыскной деятельности, эффективно применять их в борьбе с преступностью»¹.

Информация, полученная оперативными сотрудниками по поручению должностного лица, осуществляющего предварительное расследование по

¹ Полуянов Сергей Анатольевич, Филатова Виктория Александровна Вопросы негласности и конспирации в оперативно-розыскной деятельности органов внутренних дел // Юридическая наука. 2021. №5. URL: <https://cyberleninka.ru/article/n/voprosy-neglasnosti-i-konspiratsii-v-operativno-rozysknoy-deyatelnosti-organov-vnutrennih-del> (дата обращения: 20.07.2022).

уголовному делу, не может целиком быть передана последнему в связи с необходимостью соблюдения режима секретности. Очевидно, что полное рассекречивание методов и форм, применяемых в процессе осуществления ОРД невозможно и нецелесообразно. Данные действия могут повлечь расшифровку негласных источников информации и разглашение других данных, в том числе личных сведений о лице, в отношении которого осуществлялись ОРМ, что недопустимо с точки зрения основного закона Российской Федерации, принципов ОРД и уголовного судопроизводства в целом. В связи с чем, представляется, что решение данной проблемы заключается в необходимости упрощения процедуры расследования. По нашему мнению, следует внедрить в ОРД возможность проведения процедуры, которая позволила бы оперативному сотруднику при негласном непосредственном контакте со следователем передавать ему какую-либо информацию в той части, в которой это не будет противоречить принципам оперативно-розыскной деятельности. Данное мероприятие соответственно необходимо регламентировать на уровне ведомственных нормативно-правовых актов, детально установить порядок встреч и другие важные аспекты, с целью недопущения утечки информации.

Из всего вышесказанного следует сделать вывод, что одно из самых главных средств, обеспечивающих эффективное раскрытие и пресечение преступлений является взаимный обмен информацией. Оперативный сотрудник должен предоставить следователю возможность ознакомиться с материалами ОРМ в полном объёме для объективной оценки информации, за исключением тех аспектов, разглашение которых может повлечь нарушение закона. Следователь в свою очередь должен информировать о результатах следственных действий. Качество выдвинутых в дальнейшем следственных версий зависит именно от результатов взаимного обмена информацией. Эти данные ложатся и в основу составления плана проверки версий, после чего принимается решение – продолжить оперативную разработку и отслеживать поступающую информацию, или начать реализацию полученных оперативных данных. При принятии последнего решения очень важно совместно продумать вопрос о легализации и процессуальном закреплении в ходе расследования той информации, которая была получена оперативным путем, то есть проведения следственных действий, которые преобразуют полученные в ходе оперативно-розыскных мероприятий данные в доказательства.

Сафронов Андрей Алексеевич,
начальник кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук, доцент

Доттуев Эльдар Юсуфович,
курсант 4 курса
Краснодарского университета МВД России

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ПРОВЕРОЧНОЙ ЗАКУПКИ СОТРУДНИКАМИ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ МВД РОССИИ

Оперативно-розыскное мероприятие «проверочная закупка» уже давно показала свою эффективность и результативность в борьбе со многими преступлениями видами преступлений, в частности, сопряженных с незаконным оборотом наркотических и психотропных веществ. Проверочная закупка проводится при расследовании многих преступлений, но обладает некоторыми правовыми и организационно-тактическими особенностями, которым традиционно уделяется повышенное внимание в теории оперативно-розыскной деятельности.

Законодатель установил, что проверочная закупка представляет собой оперативно-розыскное мероприятие, при котором исключительно с ведома и под контролем оперативных органов осуществляется приобретение наркотических или психотропных веществ, их прекурсоров, а также инструментов и оборудования. Такая закупка производится в рамках оперативно-розыскной деятельности, которая регулируется нормами специального закона об ОРД¹.

Проверочная закупка является важным и сложным оперативно-розыскным мероприятием, которое проводится далеко не по всем категориям уголовных дел. Контрольная закупка занимает одно из центральных мест в системе оперативно-розыскных мероприятий, а также данному ОРМ традиционно уделяется повышенное внимание на доктринальном уровне. Отметим, что проверочной закупке уделяется высокое внимание не только в теории оперативно-розыскной деятельности, но и в иных юридических науках – в теории российского уголовного процесса, в криминалистике и иных науках.

Как показывает анализ достаточно многочисленного эмпирического материала в виде судебной практики судов общей юрисдикции Российской Федерации по уголовным делам, на современном этапе проверочная закупка

¹ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 30.12.2022) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

является востребованным оперативно-розыскным мероприятием. Вот примеры из практики, где ключевая роль в доказывании по уголовному делу принадлежала результатам, полученным по итогам проведения оперативными подразделениями МВД России проверочной закупки: дело № 1-250/2024 (УИД 50RS0004-01-2024-003208-05)¹, дело № 1-316/2024 (УИД 36RS0004-01-2024-008498-05)², дело № 1-53/2024 (УИД 31RS0017-01-2024-000689-73)³, дело № 1-769/2024 (УИД 50RS0031-01-2024-015756-21)⁴, дело № 1-1/2024(1-233/2023;) (УИД 50RS0034-01-2023-002024-11)⁵, дело № 1-368/2024 (УИД 50RS0029-01-2024-005198-82)⁶, дело № 1-153/6/2024 (УИД 46RS0029-01-2024-001307-21)⁷, дело № 1-177/2024 (УИД 50RS0027-01-2024-002102-67)⁸, дело № 1-204/2024 (УИД 50RS0041-01-2024-002565-70)⁹ и др.

Так, практика показывает, что чаще всего проверочная закупка проводится в целях выявления:

- незаконного оборота наркотических и психотропных веществ;
- незаконного оборота алкогольной и спиртосодержащей продукции;
- незаконного оборота лекарственных средств;
- незаконного оборота сильнодействующих и ядовитых веществ;
- незаконного оборота экзотических и краснокнижных животных;

¹ Приговор Волоколамского городского суда Московской области от 12.09.2024 № 1-250/2024 (УИД 50RS0004-01-2024-003208-05) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

² Приговор Ленинского районного суда города Воронежа от 10.09.2024 по делу № 1-316/2024 (УИД 36RS0004-01-2024-008498-05) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

³ Приговор Прохоровского районного суда Белгородской области от 09.09.2024 по делу № 1-53/2024 (УИД 31RS0017-01-2024-000689-73) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁴ Приговор Одинцовского городского суда Московской области от 06.09.2024 по делу № 1-769/2024 (УИД 50RS0031-01-2024-015756-21) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁵ Приговор Павлово-Посадского городского суда Московской области от 05.09.2024 № 1-1/2024(1-233/2023;) (УИД 50RS0034-01-2023-002024-11) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁶ Приговор Наро-Фоминского городского суда Московской области от 05.09.2024 по делу № 1-368/2024 (УИД 50RS0029-01-2024-005198-82) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁷ Приговор Кировского районного суда города Курска от 29.08.2024 по делу № 1-153/6/2024 (УИД 46RS0029-01-2024-001307-21) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁸ Приговор Можайского городского суда Московской области от 28.08.2024 по делу № 1-177/2024 (УИД 50RS0027-01-2024-002102-67) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

⁹ Приговор Рузского районного суда Московской области от 28.08.2024 по делу № 1-204/2024 (УИД 50RS0041-01-2024-002565-70) // СПС «КонсультантПлюс» 2024: <https://consultantplus> (дата обращения 25.10.2024).

- создания и распространения вредоносных компьютерных программ;
- распространение порнографических материалов;
- незаконный оборот оружия, боеприпасов;
- и др.

Одним из составных элементов правовой основы ОРД являются законодательные акты, регламентирующие деятельность отдельных субъектов ОРД. Они закладывают основы разграничения полномочий оперативных аппаратов, определяют их задачи, устанавливают права и обязанности. К этой группе можно отнести: Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции»¹, который в числе прав полиции, перечисленных в ст. 12, закрепил возможность осуществления оперативно-розыскных мер для выполнения возложенных на нее обязанностей; получения от граждан и должностных лиц необходимых объяснений, справок и документов; безвозмездного получения от предприятий, организаций и учреждений информации, за исключением случаев, когда законом установлен специальный порядок ее получения, и другие полномочия, используемые для осуществления ОРД.

Можно сделать вывод, что проверочная закупка является сложным с организационно-правовой точки зрения оперативно-розыскным мероприятием, а нарушение тактических рекомендаций и методик может привести к негативному последствию – не будет достигнута цель проверочной закупки, а как следствие не будет получена важная оперативная информация. Проверочная закупка благодаря своим свойствам помогает эффективно бороться с целым рядом преступлений, а в первую очередь в сфере незаконного оборота наркотиков, о чем явно свидетельствует проанализированная автором судебная практика судов общей юрисдикции. В теории оперативно-розыскной деятельности традиционно уделялось и уделяется повышенное внимание организационно-правовым и тактическим особенностям и основам проведения закупки. При этом мы видим, что правовая основа для проведения проверочной закупки напрямую зависит от того, в какой сфере она производится и должна учитывать требования специальных законов. Так, например, если анализируемое оперативно-розыскное мероприятие проводится в сфере незаконного оборота наркотиков, то должны в обязательном порядке учитываться нормы Закона № 3-ФЗ. Проверочная закупка является важнейшим ОРМ, которое помогает получить доказательства по уголовному делу, получать оперативную информацию и т.п.².

Подведем итоги.

Сделан вывод, что проверочная закупка представляет собой оперативно-розыскное мероприятие, которое проводится в виде закупки опреде-

¹ Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 08.08.2024) «О полиции» // Собрание законодательства РФ, 14.02.2011, № 7, ст. 900.

² Хромов Е.В., Зябликов В.Ю. Особенности применения оперативного эксперимента и проверочной закупки // Законность. 2022. № 7. С. 56 - 62.

ленных товаров, веществ и предметов в цели проверки соблюдения определенных правил, установленных законом, или правовых предписаний. Анализ судебной практики судов общей юрисдикции позволяет сделать вывод, что проверочная закупка является востребованным в правоприменительной действительности мероприятием, которое чаще всего проводится по делам, связанных с незаконным оборотом наркотических средств или в сфере незаконного оборота табачной или алкогольной продукции. Нами были приведены конкретные примеры из практики, где по уголовному делу проводилось анализируемое оперативно-розыскное мероприятие.

Сделан вывод, что проверочная закупка подлежит проведению оперативными сотрудниками правоохранительных органов только при наличии признаков преступности. Если такие признаки не установлены, то проведение проверочной закупки исключается. Анализ научной и учебной литературы позволил прийти к выводу, что проверочной закупки уделяется повышенное внимание среди исследователей в рамках многих юридических наук и дисциплин, что обуславливается ее важностью в деятельности по раскрытию преступлений и ее эффективностью.

Старостенко Олег Александрович,
старший преподаватель
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Биттиров Амир Арсенович,
курсант 4 курса
Краснодарского университета МВД России

ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКНОГО ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ

Современная эпоха цифрового информационного общества характеризуется поступательным и стремительным внедрением новейших информационных технологий во все сферы жизни и деятельности физических, юридических лиц, а также общества и государства в целом. Так, упрощение способов оплаты, возможность переводов денежных средств в удаленном формате позволяют совершать платежные операции «не выходя из дома», используя свой компьютер или смартфон, значительно облегчают совершение финансовых операций. Однако эти и другие преимущества информационных технологий стали использоваться и в криминальных целях. Исследователи отмечают, что «стремительное развитие информационных технологий привело к распространению компьютерных преступлений», констатируя появление «самостоятельной группы компьютерных преступлений, посягающих на охраняемую законом информацию и безопасность информационно-коммуникационной инфраструктуры¹».

Следует отметить, что как в научных кругах, так и среди практических работников отмеченные криминальные деяния обозначают по-разному: «компьютерные преступления», «киберпреступность», «преступления в информационной среде», «информационные преступления», «цифровая преступность²». Не вдаваясь в дискуссию о схожести и различии используемого понятийного аппарата, отметим, что под рассматриваемыми в настоящей статье преступными деяниями будем понимать преступления, указанные в «Перечне № 25 преступлений, совершенных с использованием (применением) информационно-телекоммуникационных технологий или в сфере

¹ Мелешко Д. А., Чернявский Д. О., Шарафетдинова Г. А. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию // Законность. 2020. № 3. С. 55–57.

² Малышкин Р. Н. О понятиях цифровой преступности и цифровых преступлениях // Пробелы в праве в условиях цифровизации: сборник научных трудов / Д. Р. Алимова, С.А. Афанасьева, Л. Т. Бакулина и др.; под общ. ред. Д. А. Пашенцева, М. В. Залого. М.: Инфотропик Медиа, 2022. 472 с.

компьютерной информации¹», применяемым в статистической отчетности о состоянии преступности.

Как отмечают Е. П. Полянская и А. А. Никоноров, низкая раскрываемость в данной сфере обусловлена тем, что у действующих сотрудников нет необходимого багажа знаний в данной сфере, а численность специалистов, способных оказать реальную помощь, в системе правоохранительных органов остается на низком уровне².

В связи с этим полагаем, что, решая эту проблему, действующим сотрудникам в большей степени необходимо уделять внимание вопросам взаимодействия.

Уже начиная с этапа проверки сообщения о преступлении необходимо в процессе взаимодействия эффективно использовать существующие силы и средства органов предварительного расследования, дознания с органами оперативных и экспертно-криминалистических подразделений. При планировании первоначальных действий следователь должен определить, с какими подразделениями ему необходимо организовать взаимодействие, которое ему поможет достичь необходимого результата.

Осуществляя работу по раскрытию данных преступлений, следователь, прежде всего, взаимодействует с сотрудниками оперативных подразделений, особенно с сотрудниками подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий органов внутренних дел.

Взаимодействие следственных и оперативных подразделений, как обобщенно отмечает Э. С. Данильян, должно «соответствовать двум условиям:

- 1) все действия должны быть законными;
 - 2) работа по раскрытию должна быть совместной и согласованной», и отвечать принципам, которыми «являются:
- скоординированные действия следователя с действиями оперуполномоченного;
 - разграничение задач и целей, которые стоят перед субъектами правоприменительной деятельности;
 - ответственное отношение к выполняемой деятельности всех участников взаимодействия;

¹ О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности: указание Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации от 30 июня 2022 г. № 361/11/1. Доступ из справ.-правовой системы «КонсультантПлюс».

² Полянская Е. П., Никоноров А. А. Информационное взаимодействие следователя со службами негосударственных организаций и подразделениями правоохранительных органов как основа успешного расследования преступлений в сфере высоких технологий // Вестник экономической безопасности. 2021. № 1. С. 199–202.

- управление всей деятельностью следственно-оперативной группы;
- соблюдение следственной тайны;
- совместное планирование различных действий с субъектами правоприменительной деятельности;
- использование всех имеющихся возможностей следователя и оперативноуполномоченного с целью раскрытия и расследования неочевидного преступления;
- адекватное восприятие результатов взаимодействия при изменяющихся следственных ситуациях¹«.

Как правило, взаимодействие обязательно должно сопровождаться совместным составлением планов проведения следственных и оперативных мероприятий. Такие планы могут включать в себя:

- версии, которые необходимо исследовать и проверить, путем проведения оперативно розыскных мероприятий;
- следственные действия, при производстве которых следователю необходимо взаимодействие с оперативными сотрудниками;
- определение сроков исполнения;
- определение ответственных за исполнение запланированных мероприятий;
- формы контроля за исполнением мероприятий.

При раскрытии и расследовании рассматриваемых преступлений следует в обязательном порядке обращаться за помощью сотрудников экспертно-криминалистических подразделений. Особенно к их помощи следует обращаться при проведении первоначальных действий. Грамотная и профессиональная работа со следами преступления, помощь при фиксации обстоятельств и объектов в протоколе осмотра места происшествия, а также изъятия для проведения экспертиз, способствует появлению новой доказательственной базы, а также установлению новых обстоятельств дела.

Таким образом, внутри системы органов внутренних дел следователь в ходе раскрытия и расследования компьютерных преступлений, прежде всего, взаимодействует с сотрудниками оперативных подразделений, в первую очередь с сотрудниками подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий, а также экспертами, оказывающими содействие в подготовке и проведении следственных действий, производстве сложных компьютерных и иных экспертиз.

Однако специфика рассматриваемых преступлений такова, что в процессе их раскрытия и расследования в обязательном порядке необходимо

¹ Данильян Э. С. Проблемы взаимодействия следователя и оперативного работника при расследовании преступлений против службы в органах местного самоуправления // Гуманитарные, социально-экономические и общественные науки. 2020. № 8. С. 61–64.

взаимодействовать не только со службами и подразделениями органов внутренних дел, но и с иными организациями, связанными с предоставлением услуг цифрового характера, в том числе осуществляющие финансово-кредитные услуги, разработку программного обеспечения или социальных сетей и др. Данные организации обладают большим объемом информации, которая может иметь решающее значение для раскрытия рассматриваемых преступлений. Так, если преступление связано с хищением денежных средств с использованием дистанционных технологий, то все операции проходят по соответствующим базам данных той или иной финансовой организации, от которой можно получить информацию о том, на какой счет были переведены денежные средства, кому может принадлежать данный счет, а также дальнейшие операции с данными средствами.

С крупными организациями необходимо налаживать взаимодействие на уровне руководства. Так, например, некоторые территориальные органы заключают соглашения об электронном документообороте и обмене информацией в короткие сроки, с возможностью использования систем удаленного доступа. Подобное взаимодействие делает расследование оперативным и сокращает срок предварительного расследования.

Таким образом, грамотная организация взаимодействия будет способствовать эффективному расследованию и повышению раскрываемости киберпреступлений. Кроме того, полагаем, эффективность оперативно-розыскной деятельности напрямую зависит не просто от эффективности реализации указанных задач, но и от одновременного, комплексного их осуществления. Этим обосновывается актуальность совершенствования процесса решения оперативных задач на современном этапе.

Старостенко Олег Александрович,
старший преподаватель
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

Скрипка Софья Алексеевна
курсант 4 курса
Краснодарского университета МВД России

НЕКОТОРЫЕ ОСОБЕННОСТИ ОПЕРАТИВНО-РОЗЫСКОГО ПРОТИВОДЕЙСТВИЯ ИДЕОЛОГИИ ЭКСТРЕМИЗМА

В нынешнюю эпоху повышенной глобальной напряженности, согласованных усилий враждующих государств по нарушению стабильности современное общество сталкивается с коварным проявлением радикальных экстремистских идеологий. В Стратегии противодействия экстремизму в Российской Федерации на период до 2025 года (раздел 16) недвусмысленно утверждается, что экстремистская идеология служит основной связующей силой, объединяющей отдельных лиц в экстремистские группировки и определяющей характер и направление их деятельности¹.

Религиозные культы все чаще признаются благодатной почвой для распространения экстремистских идеологий, что является серьезной проблемой, усложняющей процесс их выявления. В современном обществе религия часто используется в качестве фона для организации различных преступных действий, имеющих значительный общественный резонанс, таких как печально известные инциденты с сожжением Корана, свидетелями которых стали пользователи онлайн-платформ в 2023 году как внутри страны, так и за рубежом. Данные действия, несомненно, направлены на подстрекательство к нарушениям государственного порядка и национального суверенитета, способствуя прямому неповиновению со стороны ультрарадикальных группировок, таких как незаконная неонацистская группировка «Маньяки М.К.У.: Культ убийц», которую, как утверждается, поддерживает Служба безопасности Украины.

Спектр проявлений религиозного экстремизма широк, что предоставляет преступникам универсальный инструмент для манипулирования общественными настроениями через киберпространство. Следовательно, такие платформы, как социальные сети, переполнены социально агрессивным контентом, включая нацистскую пропаганду, религиозный экстремизм и

¹ Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» // СПС «КонсультантПлюс».

националистическую риторику, которые широко распространяются. Примечательно, что такие запрещенные организации, как крымскотатарское движение «Меджлис», используют Facebook для продвижения своей политической программы, маскируясь под массовое освободительное движение, в то время как такие организации, как «Остановите вагоны», занимающиеся диверсиями на железной дороге, сталкиваются с цифровым противодействием со стороны российских властей.

Крайне важно признать, что религиозный экстремизм выходит за рамки «исламского экстремизма», и его проявления наблюдаются также в христианской и языческой сферах. Языческое влияние особенно заметно в современных неонацистских и националистических группировках, примером чего являются боевики с языческой символикой в вооруженных формированиях Украины. Более того, потоки иностранного финансирования, поступающие через религиозные объединения и государства, способствуют распространению экстремистских идеологий, подпитывая онлайн-вербовку для совершения актов насилия и социальной дестабилизации в нашей стране.

Таким образом, 22 октября 2022 года в ходе специальной военной операции в Запорожской области были выявлены координаторы, способствовавшие вербовке лиц для экстремистской деятельности на территории Российской Федерации. Эти центры, действующие под эгидой религиозно-экстремистской организации со штаб-квартирой в России, укрывали «свидетелей Иеговы»¹, которых, очевидно, поддерживали многочисленные антагонистические организации.

Решение этих локальных проблем требует реализации комплексных стратегий по противодействию распространяющемуся влиянию экстремистских идеологий, которые составляют основу такой деятельности. Следовательно, становится необходимым определить ключевые принципы, способствующие эффективному идеологическому противодействию.

Важнейшим из этих принципов является создание законодательной базы, учитывающей специфику действий экстремистов, что позволит властям систематически бороться с их идеологической пропагандой. В настоящее время примечательно, что наша страна может похвастаться такой законодательной базой, которая характеризуется системным и многоуровневым характером.

Прежде всего, важно обратить внимание на положения, изложенные в административном и уголовном законодательстве. Кодекс об Административных Правонарушениях Российской Федерации охватывает широкий спектр правонарушений², включая распространение нацистской атрибутики

¹ Штаб-квартиру Свидетелей Иеговы обнаружили в Запорожской области // URL: <https://smotrim.ru/video/2502564> (дата обращения : 21.05.2024).

² Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СПС «КонсультантПлюс».

или символики (статья 20.3), публичное оскорбление военнослужащих (статья 20.3.3), а также изготовление и распространение экстремистских материалов (статья 20.29). Кроме того, религиозные объединения несут административную ответственность за сокрытие информации о финансовых операциях от международных организаций (статья 5.26).

Аналогичным образом Уголовный кодекс всесторонне разграничивает уголовные преступления с экстремистским подтекстом¹, такие как публичные призывы к осуществлению экстремистской деятельности (статья 280), возбуждение ненависти или вражды и унижение человеческого достоинства (статья 282). Кроме того, в нем рассматриваются, в частности, вопросы организации экстремистских сообществ (статья 282.1), содействия деятельности экстремистских организаций (статья 282.2) и финансирования экстремистских начинаний (статья 282.3).

В дополнение к этим правовым положениям действуют различные федеральные законы, направленные на эффективную борьбу с распространением экстремистских идеологий. В частности, основополагающим документом в этом отношении является Федеральный закон № 114-ФЗ от 25 июля 2002 года². Кроме того, Федеральные законы № 374-ФЗ³ и № 375-ФЗ⁴ от 6 июля 2016 года определяют рамки защиты информационных и телекоммуникационных ресурсов от распространения социально деструктивного, экстремистского и террористического контента, а также меры по мониторингу и противодействию его распространению на территории России.

Кроме того, ряд нормативных мер позволяет правоохранительным органам получать доступ к информации, хранящейся у операторов связи и поставщиков интернет-контента, для документирования и расследования экстремистской деятельности. Срок хранения такой информации соответствует постановлениям правительства, предусмотренным постановлениями № 445⁵

¹ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СПС «КонсультантПлюс».

² Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс».

³ Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС «КонсультантПлюс»

⁴ Федеральный закон от 6 июля 2016 г. № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС «КонсультантПлюс».

⁵ Постановление Правительства Российской Федерации от 12 апреля 2018 г. № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» // СПС «КонсультантПлюс».

и № 256 от 12 апреля 2018 года и 26 февраля 2022 года соответственно, которые устанавливают срок хранения до шести месяцев.

Важно подчеркнуть, что большинство преступлений экстремистской направленности совершается в Интернете, и доказательства часто берутся из интернет-хранилищ данных. Эти материалы служат ключевыми доказательствами в последующих уголовных разбирательствах.

Еще одним важным аспектом в борьбе с экстремистскими идеологиями является проведение оперативно-розыскных мероприятий. Это предполагает организованный поиск информации, имеющей оперативное значение, в первую очередь на просторах Интернета. Специализированное программное обеспечение, как запатентованное, так и общедоступное, помогает оперативным подразделениям выявлять IP-адреса, на которых размещен запрещенный контент, собирать данные о пользователях и каналах связи, используемых для распространения, а также отслеживать переписку организаторов экстремистских организаций и их сообщников.

Оперативный персонал все чаще использует интеллектуальные платформы с открытым исходным кодом (OSINT) для мониторинга социальных сетей и форумов, что облегчает получение соответствующих оперативных данных.

Третий аспект предполагает совместные усилия подразделений внутренних дел с другими ведомствами и организациями. Совместные профилактические меры включают в себя проведение различными подразделениями внутренних дел обследований по месту жительства с целью выявления мест, способствующих экстремистской деятельности, таких как импровизированные молитвенные помещения или места вербовки или собрания приверженцев радикальных религиозных культов или других экстремистских организаций.

В настоящее время оперативные подразделения, занимающиеся борьбой с экстремизмом, наладили структурированные партнерские отношения с подразделениями, ответственными за управление информационными ресурсами и их обслуживание. Примечательно, что в Москве в сотрудничестве с Департаментом информационных технологий используется программно-аппаратный комплекс «Безопасный город», насчитывающий более 250 000 камер видеонаблюдения, более 100 000 из которых оснащены функциями искусственного интеллекта. Данная система позволяет выявлять скрытые экстремистские элементы и получать соответствующие оперативные данные о субъектах, вовлеченных в экстремистскую деятельность, включая схемы их передвижения, контроль доступа в определенные места, мероприятия, предшествующие экстремистским актам, подготовку транспортных средств для совершения преступных действий, а также о собраниях экстремистов и их сообщников.

Очевидны положительные примеры сотрудничества между оперативными подразделениями Министерства внутренних дел России и такими

учреждениями, как Росфинмониторинг, что способствует получению данных о финансовых перемещениях лиц, причастных к экстремизму, включая меры по замораживанию средств и другие соответствующие действия. Сотрудничество распространяется на регулирующие органы, такие как Роскомнадзор, и известных российских интернет-провайдеров, таких как «ВКонтакте» и «Яндекс», направленное на получение доступа к оперативной информации, блокирование экстремистского контента и ограничение доступа к экстремистским веб-сайтам.

Кроме того, деятельность ряда организаций, включая Федеральное агентство по делам молодежи и Национальный центр информационного противодействия терроризму и экстремизму, в образовательной и интернет-среде играет ключевую роль в формировании антиэкстремистских настроений среди детей и молодежи. Эти согласованные усилия в значительной степени способствуют пресечению распространения экстремистской идеологии.

Сотрудничество между оперативными подразделениями и этими организациями облегчает выявление экстремистского контента в интернет-сетях, позволяя принимать меры по ограничению доступа к таким платформам.

В заключение важно признать, что описанные меры представляют собой лишь часть многогранных оперативных стратегий, применяемых подразделениями по борьбе с экстремизмом. Данная система постоянно развивается и адаптируется к изменяющимся реалиям и прогрессированием экстремистской деятельности, гибко реагируя на возникающие угрозы.

Студнев Александр Сергеевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России

Жугова Дарина Эдуардовна,
курсант 4 курса
Краснодарского университета МВД России

РЕЗУЛЬТАТЫ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ КАК СРЕДСТВО ДОКАЗЫВАНИЯ ПО УГОЛОВНЫМ ДЕЛАМ

В настоящее время существуют проблемы применения результатов оперативно-розыскной деятельности как средства доказывания по уголовным делам экстремисткой направленности. Данная проблема идет еще из теории уголовного процесса и норм УПК РФ, где российский законодатель не поименовал в качестве доказательств по уголовным делам результаты ОРД. Более того, на доктринальном уровне, само по себе, понятие «результат оперативно-розыскной деятельности» является спорным и дискуссионным. Такая правовая неопределенность оказывает сугубо негативное влияние на деятельность по доказыванию, в том числе, и по преступлениям экстремистской направленности. Многочисленные споры и дискуссии о результатах оперативно-розыскной деятельности и возможности их применения в доказывании связаны именно с недостатками в действующем нормативно-правовом регулировании, что оказывает негативное воздействие на деятельность по доказыванию анализируемой категории поступлений.

Акцентируем внимание на определении юридической природы результатов оперативно-розыскной деятельности в доказывании по делам экстремисткой направленности.

Изначально стоит отметить, что ни нормы УПК РФ¹, ни положения Закона об ОРД² не содержат определения данных результатов. При характеристике данного аспекта необходим комплексный и системный подход – как с позиции доктрины российского уголовного процесса, так и теории оперативно-розыскной деятельности. Данный нормативно-правовой пробел вызывает множественные дискуссии среди современных авторов и исследователей на доктринальном уровне.

Перейдем к характеристике самой проблемы.

¹ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 02.10.2024) // Собрание законодательства РФ, 24.12.2001, № 52 (ч. I), ст. 4921.

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

В статье 11 российский законодатель устанавливает общие положения о применении результатов ОРД, но данный порядок не нашел своего отражения в нормах УПК РФ.

В.А. Саморока¹ справедливо отмечает, что нельзя игнорировать значение результатов ОРД. Данный автор подчёркивает, что большинство уголовных дел по преступлениям экстремистской направленности возбуждаются на основе предоставленных результатов оперативно-розыскной деятельности, которые впоследствии используются и в рамках доказывания на стадии предварительного расследования и судебного следствия.

Стоит отметить, что результаты ОРД, применяемые при доказывании по преступлениям экстремистского характера, получаются, в первую очередь, в связи с проведением следующих ОРМ:

- получение компьютерной информации;
- оперативный мониторинг сети Интернет.

О.В. Михайловская² обосновывает позицию, что результаты оперативно-розыскной деятельности целесообразно относить к «иным документам», как разновидности доказательств по уголовным делам. Сказанное также применимо и к доказыванию по делам экстремистской направленности.

Законодатель разрешает использовать результаты, полученные органом дознания в ходе осуществления оперативно-розыскной деятельности в целях исполнения поручения следователя (дознателя), в качестве доказательств по уголовному делу. Единственным условием для признания полученных результатов в качестве доказательств выступает их соответствие уголовно-процессуальному закону (ст. 89 УПК РФ³, ч. 2 ст. 11 ФЗ об ОРД⁴).

При этом положение ч. 2 ст. 74 УПК РФ устанавливает исчерпывающий перечень доказательств, среди которых отсутствуют прямо обозначенные «результаты ОРД», то есть сведения, полученные в соответствии с ФЗ об оперативно-розыскной деятельности, о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда (п. 36.1 ст. 5 УПК РФ).

В связи с установленными российским законодателем рамками признания сведений доказательствами следователю (дознателю) приходится

¹ Саморока В. А. Использование результатов оперативно-розыскной деятельности при возбуждении уголовных дел экстремистской направленности // Вестник Московского университета МВД России. 2019. №7. URL: <https://cyberleninka.ru/article/n/ispolzovanie-rezultatov-operativno-rozysknoy-deyatelnosti-pri-vozbuzhdenii-ugolovnyh-del-ekstremistskoy-napravlenosti> (дата обращения: 22.10.2024).

² Михайловская О.В. Результаты оперативно-розыскной деятельности в доказывании по уголовным делам // Российская юстиция. 2019. № 1. С. 45 - 46.

³ Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 02.10.2024) // Собрание законодательства РФ, 24.12.2001, № 52 (ч. I), ст. 4921.

⁴ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

выбирать способ узаконивания результатов ОРД, обличая их в форму одного из доказательств¹.

Таким образом, можно заключить, что проблемы использования и применения результатов оперативно-розыскной деятельности в доказывании по уголовным делам экстремистской направленности возникают из-за недостатков действующего нормативно-правового регулирования. На сегодняшний день можно констатировать, что нормы Закона об ОРД не согласуются с положениями уголовно-процессуального закона о доказывании. Подобного рода законодательные проблемы могут оказывать негативное воздействие на деятельность по доказыванию по уголовным делам, в том числе, по преступлениям экстремистской направленности. В связи со сказанным представляется необходимым внести комплексный и системные поправки в два обозначенных нормативно-правовых актов и официально передать результатам оперативно-розыскной деятельности статус доказательств по уголовным делам. Данное нововведение позволит усовершенствовать действующее нормативно-правовое регулирование как процесса доказывания по уголовным делам, так и оперативно-розыскной деятельности. Указанные нововведения окажут и благоприятное воздействие на деятельность по доказыванию по уголовным делам экстремистской направленности, так как более не будет возникать проблем при применении в качестве доказательств по обозначенной категории дел результатов оперативно-розыскной деятельности.

Также такие нововведения положат конец дискуссиям о понятии «результат оперативно-розыскной деятельности», его юридической природе и спорам о правомерности их применения в качестве доказательств по уголовным делам, в том числе и по преступлениям экстремистской направленности.

¹ Михайловская О.В. Результаты оперативно-розыскной деятельности в доказывании по уголовным делам // Российская юстиция. 2019. № 1. С. 45 - 46.

Студнев Александр Сергеевич,
старший преподаватель
кафедры оперативно-розыскной деятельности в ОВД
Краснодарского университета МВД России

Мазурова Малена Андреевна,
курсант 4 курса
Краснодарского университета МВД России

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

В рамках данной статьи, будут подняты вопросы и проблемы применения современных технологий в рамках оперативно-розыскной деятельности (далее – ОРД). На современном этапе во всем мире происходят активные процессы цифровизации, цифровой трансформации, компьютеризации и т.п., что обуславливает появление новых технологий, применяемых во всех сферах жизнедеятельности общества и государства, включая оперативно-розыскную деятельность. Однако стоит констатировать, что процесс внедрения современных технологий в ОРД происходит слишком медленно, не используется весь потенциал искусственного интеллекта, нейронных сетей и т.п., что во многом связано не только с нехваткой финансирования, но и недостатками действующего нормативного правового регулирования, которое просто не успевает развиваться «в ногу со временем».

Анализ научной и учебной литературы позволяет сделать вывод, что очень многие современные авторы и исследователи указывают на необходимость применения современных технологий в ОРД. Рассмотрим мнения некоторых из исследователей.

Так, А.Ю. Малянов¹ указывает, что повышенное внимание необходимо уделять техническому обеспечению ОРД, чтобы обеспечить ее скрытый и негласный характер. По мнению данного автора, в первую очередь в рамках ОРД необходимо внедрять те современные технологии, которые будут способствовать конспирации и сохранению принципа негласности, так как это основные отличительные свойства ОРД как особого вида правоохранительной деятельности.

Однако стоит отметить, что большая часть авторов поднимает проблемы, связанные с внедрением в ОРД современных цифровых технологий, а также искусственного интеллекта и нейронных сетей. По нашему мнению,

¹ Молянов А.Ю. Конституционные принципы специального технического обеспечения оперативно-розыскной деятельности полиции // Российская юстиция. 2019. № 7. С. 58 - 62.

цифровизация и информатизация процессов в рамках ОРД должно стать основным вектором ее развития на современном этапе. О необходимости повсеместного внедрения цифровых технологий в своей работе обращает внимание С.С. Булгаков¹.

Многие авторы давно указывают на необходимость расширения практики применения искусственного интеллекта и нейронных сетей в ОРД. В частности, на данный аспект обращает внимание Д.И. Иванов². Однако данный автор справедливо отмечает, что на современный период искусственный интеллект и нейронные сети применяются «сегментарно» в правоохранительной деятельности, включая ОРД. Данное идет из-за недостатков действующего нормативного правового регулирования. Например, Закон об ОРД³ не подвергался изменениям под влиянием процессов цифровизации, цифровой трансформации, компьютеризации, расширения онлайн пространства. Соответственно для того, чтобы в рамках оперативно-розыскной деятельности более активно начали применяться современные технологии необходимо заняться совершенствованием норм Закона об ОРД и иных нормативно-правовых актов, включая подзаконный уровень – приказы МВД России.

Например, в рамках ОРД на сегодняшний день предлагается применять технологию «DEEPFAKE»⁴. Технология DEEPFAKE функционирует на базе нейронных сетей и представляет собой совокупность методов соединения или объединения, ранее разрозненных фото и видео изображений и аудиосообщений посредством применения технологии генеративно-состязательных нейронных сетей в единое поддельное целое. Данная технология активно применяется преступниками в онлайн пространстве и с применением сети Интернет. Ряд авторов предлагает данную технологию внедрить в ОРД, предполагается, что она будет способствовать выявлению фейковых

¹ Булгаков С.С. Сравнительно-правовой анализ понятий цифровизации и информатизации в сфере оперативно-розыскной деятельности // Право и государство: теория и практика. 2023. №4 (220). URL: <https://cyberleninka.ru/article/n/sravnitelno-pravovoy-analiz-ponyatiy-tsifrovizatsii-i-informatizatsii-v-sfere-operativno-rozysknoy-deyatelnosti> (дата обращения: 18.09.2024).

² Иванов, Д. И. Применение искусственного интеллекта в отдельных областях российской правовой сферы / Д. И. Иванов. – Текст : непосредственный // Молодой ученый. – 2022. – № 47.1 (442.1). – С. 65-66. – URL: <https://moluch.ru/archive/442/96799/> (дата обращения: 18.09.2024).

³ Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности» // Российская газета, № 160, 18.08.1995.

⁴ Батоев В.Б. об использовании технологии “deepfake” в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. №1 (61). URL: <https://cyberleninka.ru/article/n/ob-ispolzovanii-tehnologii-deepfake-v-operativno-rozysknoy-deyatelnosti> (дата обращения: 18.09.2024).

страниц, фишинговых сайтов, поддельных видеоизображений и т.п. Разумеется, что технология DEEPFAKE должна быть оптимизирована под реалии ОРД.

Так, современные технологии и искусственный интеллект может применяться в рамках ОРД для сбора и анализа информации; для передачи информации; он может использоваться для обработки большого объема данных; для анализа телефонных переговоров; для анализа соединений между абонентами и т.п. Искусственный интеллект и нейронные сети, цифровые технологии дано уже зарекомендовали себя во многих областях. Например, для поиска и идентификации лиц применяется система распознавания лиц, которая также функционирует на основе современных цифровых технологий и с применением искусственного интеллекта. А ведь розыск и идентификация лиц является важным направлением ОРД оперативных подразделений органов внутренних дел. Особенно применение данной технологии востребовано в рамках мегаполиса и крупных городов, районных центров, где наблюдается большее скопление людей.

Считается, что с позиции правоприменителя целесообразно под технологиями искусственного интеллекта понимать способность высокотехнической системы повторять отдельные функции, схожие с мыслительной деятельностью человека, которые будут обеспечивать самообучение искусственного интеллекта, а также определять поиск и нахождение решений, направленных на получение при выполнении определенных задач обработки данных таких результатов, которые будут сопоставимы с мыслительной деятельностью. Мы полагаем, что разрабатываемая система искусственного интеллекта, являясь важным элементом в деятельности государственных органов и правоохранительной системы в целом, должна соответствовать требованиям доступности, своевременности, понятности и полноты информации о ней, причем как для общества, так и для участников правоотношений.

На наш взгляд, применение новых технологий искусственного интеллекта и новых технологических решений должно найти отражение в отраслевом оперативно-розыскной законодательстве, что, несомненно, будет способствовать повышению уровня противодействия преступности, а также будет закреплять правовую систему гарантий обеспечения законности при использовании технических решений на базе искусственного интеллекта в противодействии преступности и защите общества и государства от противоправных посягательств, при осуществлении ОРД¹.

¹ Батоев В.Б. об использовании технологии “deepfake” в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. №1 (61). URL: <https://cyberleninka.ru/article/n/ob-ispolzovanii-tehnologii-deepfake-v-operativno-rozysknoy-deyatelnosti> (дата обращения: 18.09.2024).

Для устранения выявленных в ходе исследования пробелов оперативно-розыскного законодательства мы считаем, что необходимо дополнить ч. 1 ст. 10 ФЗ «Об ОРД», изложив текст статьи в следующей редакции: «Оперативные подразделения, для решения задач ОРД, могут создавать и использовать информационные системы, под которыми понимается совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

При осуществлении ОРД и проведении оперативно-розыскных мероприятий использовать возможности технологий искусственного интеллекта, под которыми понимается способность высокотехнической системы повторять отдельные функции, схожие с мыслительной деятельностью человека, которые будут обеспечивать самообучение искусственного интеллекта, а также определять поиск и нахождение решений, направленных на получение при выполнении определенных задач обработки данных таких результатов, которые будут сопоставимы с мыслительной деятельностью»¹.

¹ Батоев В.Б. об использовании технологии “deepfake” в оперативно-розыскной деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. №1 (61). URL: <https://cyberleninka.ru/article/n/ob-ispolzovanii-tehnologii-deepfake-v-operativno-rozysknoy-deyatelnosti> (дата обращения: 18.09.2024).

Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук

ОСОБЕННОСТИ РАСКРЫТИЯ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Актуальность данной темы обусловлена тем, что с развитием экономики происходит изменения финансово-экономических отношений, что создает предпосылки для развития новых видов преступлений, в том числе и мошенничеств, совершаемых с использованием средств мобильной связи. На сегодняшний день уровень развития технологий связи, а также доступность к мобильной связи практически всех слоёв населения повлияло на возникновение и широкое распространение данного вида преступления. Ежегодно телефонными мошенниками причиняется существенный имущественный вред гражданам. Об этом свидетельствует характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года. В отчетном периоде число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4%, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3%, в том числе мошенничество ст. 159 УК РФ на 75,6%, мошенничество в сфере компьютерной информации ст. 159.6 УК РФ на 10,8%.¹ В 2023 году темп роста данного вида преступления немного снизился, составив 1,4%. За 6 месяцев 2024 года зарегистрировано на 4% больше преступлений, совершенных с использованием информационно-телекоммуникационных технологий по сравнению с 2023 года.²

Эксперты считают, что такой резкий рост числа зарегистрированных случаев мошенничеств обусловлен ограничениями, связанными с эпидемией коронавируса (COVID-19).

Это подтверждается выступлением главы Следственного Департамента РФ Лебедевым С.Н., который 12 октября 2020 г. заявил о том, что пандемия неблагоприятно повлияла на рост информационно-телекоммуникационных мошенничеств. Так, количество мошенничеств, совершаемых с использованием средств мобильной связи выросло практически в два раза.³

¹ Статистика и аналитика. Состояние преступности. [Электронный ресурс]. – URL: <https://мвд.рф/reports/item/22678184/>

² Статистика и аналитика. Состояние преступности. [Электронный ресурс]. – URL: <https://xn--b1aew.xn--plai/reports/item/28726056/>

³ Озеров К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий// Вестник Санкт-Петербургского университета МВД России, 2021, с. 167-171.

В связи с вышесказанным можно прийти к выводу о том, что перед органами дознания стоит важная задача выработки высокоэффективного и результативного алгоритма действий при раскрытии мошенничеств, совершаемых с использованием средств сотовой связи.

В настоящее время в век развития информационных и коммуникационных технологий данный вид преступления приобретает всё большее распространение, совершается различными способами, в том числе с использованием сети Интернет. Причины и условия совершения данной категории преступления довольно разнообразны, но выделим следующие, на наш взгляд, наиболее значимые:

- слабая информированность граждан о распространённых видах мошенничеств, мерах предосторожности и алгоритме действия при получении информации сомнительного характера;
- недостаточный контроль со стороны участковых уполномоченных, ведущих административный контроль за лицами, судимыми за аналогичные деяния.

Основная цель мошенничеств, совершаемых с использованием средств мобильной связи – сообщить потерпевшему ложные сведения, убедить его в их истинности, тем самым вынудив потерпевшего передать свои денежные средства по собственной воле. Что касается сведений, сообщаемых мошенниками, то они могут быть разнообразны, но приведём перечень получивших широкое распространение:

1. О задержании его родственника сотрудниками полиции за совершение административного правонарушения или преступления. Это один из самых популярных видов телефонного мошенничества. Злоумышленники производят звонок и говорят, что ваш родственник – чаще всего, кто-то из детей и внуков, – попал в беду и необходимо срочно перевести сумму денег на какую-то карту, чтобы их выручить;

2. СМС- просьба о помощи. Зачастую потерпевшими становятся пожилые люди или слишком юные владельцы телефона. Как правило, абонент получает на мобильный телефон сообщение с следующим содержанием: «У меня проблемы, кинь определенную сумму (100, 500, 1000 и т.д.) рублей на этот номер. Не звони, вечером всё объясню».

3. Звонок от ложного представителя вашей сотовой компании, который предлагает пополнить счёт карточкой экспресс- оплаты. Мошенник рекомендует действовать следующим образом: перед оплатой Вы должны сообщить ему ПИН-код, перезвонив на определенный номер. По итогу совершения указанных действий злоумышленник присваивает средства с этих карт.

Приведённый выше перечень сообщаемых сведений и способов совершения мошенничеств, совершаемых с использованием средств мобильной связи, многообразен и далеко не исчерпывающий. Мошенники совершенствуют способы совершения преступления, создают новые схемы, что,

безусловно, затрудняет процесс проверки, выявления, раскрытия преступления. Перед органами дознания стоит важная задача планирования по выбору наиболее целесообразного, последовательного и результативного алгоритма для раскрытия данного вида мошенничества. Перечень первоначальных оперативно-розыскных мероприятий, а также порядок их проведения будут зависеть от информации, имеющейся на момент заявления. Следует отметить, что на первоначальном этапе, как правило, идеальные следы отсутствуют. Прежде всего это связано с тем, что преступник и потерпевший находятся на значительном расстоянии друг от друга, то есть между ними отсутствует визуальный контакт¹, а также довольно часто у правоохранительных органов и вовсе отсутствует какая-либо информация о телефонном мошеннике. Указанные факты, бесспорно, влияют на алгоритм действий по установлению непосредственных исполнителей и их пособников.

Сложность раскрытия рассматриваемой категории преступлений состоит в следующем:

- анонимность преступников. Злоумышленники зачастую находятся за границей или используют иностранное программное обеспечение, сервера, что позволяет изменять IP адрес и др., а это, соответственно, существенно затрудняет получение оперативно-розыскной информации, можно сказать, делает это невозможным;

- получение информации от операторов сотовой связи и банковский организаций требует относительно длительного времени и в большинстве случаев носит малоинформативный характер. Это связано с тем, что при регистрации сим-карты в учетные документы вносятся недостоверные сведения, а также используются карты подставных лиц, что делает выход на преступника практически невозможным;

- устаревшие методики раскрытия мошенничеств, совершенных с использованием средств мобильной связи;

- слабая эффективность внутриведомственного и межведомственного взаимодействия между подразделениями. К примеру, формальность ответов на поручения, направляемые в другие регионы;

- недостаточная подготовка (профессионализм) оперативных сотрудников в компьютерной сфере.

С целью повышения качества раскрытия мошенничеств, совершаемых с использованием средств мобильной связи, выделим ряд действий, которые необходимо произвести сотруднику оперативного подразделения при получении сообщения о преступлении:

1. Произвести опрос заявителя по факту совершения в отношении него противоправного деяния. Основная цель данного оперативно-розыскного

¹ Кириллов, И.С. Проблемы выявления телефонного мошенничества / И.С. Кириллов // Современное право. - 2017

мероприятия- получить как можно больше существенной информации, имеющей значение для дела, а именно: в какое время поступил звонок, с какого абонентского номера звонили; кем представился преступник; что предлагал сделать; какие действия совершены потерпевшим; какой способ передачи денежных средств; была ли переведена сумма, если да, то какая сумма и на какой расчетный счёт.

2. В целях установления сведений о лице, на имя которого зарегистрирован номер, с которого был совершён звонок, необходимо направить запрос в сотовую компанию или Бюро специальных технических мероприятий УМВД России конкретного региона.

3. Провести ряд оперативно-розыскных мероприятий, направленные на установление личности преступника. Комплекс таких мероприятий может варьироваться в зависимости от первоначальной информации. Сотрудник оперативного подразделения вправе производить в установленном порядке ряд оперативно-розыскных мероприятий, указанных в ст.6 ФЗ «Об оперативно-розыскной деятельности»¹. На начальном этапе самыми распространёнными мероприятиями будут следующие: опрос, наведение справок, наблюдение, отождествление личности, прослушивание телефонных переговоров, снятие информации с технических каналов связи и другие. Комплекс таких мероприятий может варьироваться в зависимости от первоначальной информации. Если представить ситуацию, когда информация о преступнике отсутствует, то логично, что оперативному сотруднику необходимо ряд действий, направленный на получение всех данных о лице, совершившем противоправное деяние. Следует отметить, что полученный объём материала должен быть достаточным для формирования представления о лице, совершившем мошенничество. Если сложилась ситуация, когда информация о преступнике имеется, то целесообразно производить оперативно-розыскные мероприятия, благодаря которым будет возможно установить местонахождение лица, причастного к совершению преступления, и осуществить его задержание. Из вышесказанного можно сделать вывод о том, что на первоначальном этапе перед оперативным сотрудником стоит важная задача: правильно оценить сложившуюся ситуацию, спланировать комплекс действий и произвести их в установленном законном порядке. Дальнейший ход раскрытия и расследования мошенничества зависит от того, насколько безошибочно и целесообразно были произведены оперативно-розыскные мероприятия.

Хотелось бы отметить, что на наш взгляд, одним из наиболее важных и информативных ОРМ, является исследование предметов и документов².

¹ Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно- розыскной деятельности» (ред. от 29.12.2022).

² Маркушин, А. Г. Оперативно-розыскная деятельность : учебник и практикум для бакалавриата и специалитета // . – 5-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2019. – 342 с.

Необходимо отметить, что мобильное устройство потерпевшего является, пожалуй, одним из самых распространённых объектов, подлежащих исследованию. Также не стоит забывать, что характерной чертой проведения указанного оперативно-розыскного мероприятия является необходимость привлечения лиц, обладающих специальными знаниями в различных областях науки и техники. Благодаря проведению исследования может быть конкретизирован способ совершения мошенничества и получены необходимые сведения о мошеннике.

4. Установленных лиц проверить по всем имеющимся оперативно-справочным, криминалистическим, розыскным учетам информационных центров, в том числе других регионов России.

5. В установленном порядке получить детализацию телефонных переговоров и информацию о движении денежных средств по счёту потерпевшего.

6. С участием потерпевшего посредством использования сети Интернет или обращения в кредитную организацию получить информацию о перечислении похищенных денежных средств со счёта потерпевшего на иные счёта.

Хотелось бы отметить, что, в связи с быстрым ростом дистанционных видов преступлений, было бы целесообразно повышать уровень профессионализма оперативных сотрудников. На наш взгляд, для этого следует совершенствовать методы обучения в образовательных учреждениях системы МВД России, таким образом выпускать наиболее подготовленных в данной сфере будущих сотрудников уголовного розыска. Что касается действующих сотрудников, то для них следует организовывать обучение в сфере изучения IT технологий, современных средств программного обеспечения и т.д.

По итогу проведения указанных выше действий, оперативный сотрудник передаёт соответствующие материалы в орган предварительного следствия.

С момента получения материалов следователь возбуждает уголовное дело и проводит ряд следственных и процессуальных действий.

По завершению выполнения указанных выше действий, необходимо определить последующие следственные и оперативно-розыскные мероприятия согласно материалам, собранным в рамках уголовного дела и полученной информации.

На основании вышеизложенного становится очевидным тот факт, что перед органами дознания стоит сложная и важная задача по построению наиболее эффективной системы действий по раскрытию мошенничеств, совершаемых с использованием средств мобильной связи. От того, насколько правильно и рационально будет построен алгоритм действий, соответственно, будет зависеть весь процесс и в конечном счёте итог расследования, поэтому необходимо своевременно выбрать тактику и последовательность производства следственных и оперативно-розыскных мероприятий, определить и обеспечить эффективное использование дополнительных сил и средств.

Стукалов Вячеслав Владимирович,
доцент кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук,

Храмченков Илья Александрович,
курсант 3 курса
Краснодарского университета МВД России

ПРОБЛЕМЫ ВЫЯВЛЕНИЯ И РАСКРЫТИЯ УБИЙСТВ ПО НАЙМУ

В современных условиях на фоне происходящих событий в Российской Федерации среди наиболее тяжких преступлений против жизни и здоровья граждан в последнее время широкое распространение получили заказные убийства, также известные как «убийства по найму». Заказные убийства представляют собой одну из наиболее сложных и опасных форм преступной деятельности. Несмотря на то, что их количество невелико (2-3%) от общего числа совершаемых умышленных убийств, но эти преступления имеют широкий общественный резонанс.

Заказные убийства часто связаны с преступными организациями и могут использоваться как средство разрешения конфликтов между различными группами и устранения конкурентов по бизнесу. Такие преступления не только оказывают значительное влияние на отдельных жертв и их семьи, но и подрывают общественную безопасность и веру в верховенство закона.

Заказчиком убийства может быть, как частное лицо, так и организация, стремящаяся устранить нежелательного конкурента, избежав при этом прямой ответственности. Мотивы, лежащие в основе таких преступлений, варьируются от личной мести до экономической выгоды, что делает их ещё более сложными для предотвращения и выявления.

Убийства, совершаемые наёмниками, отличаются тщательной подготовкой и изощрённостью, когда их используют представители крупных корпораций, коррумпированные чиновники, лидеры и руководители организованных преступных групп и организаций. Во многих случаях убийству предшествует анализ поведения жертвы, изучение места жительства, её родственников, средств и маршрутов передвижения, режима работы и отдыха. Анализируется планировка места проживания или рабочего места будущей жертвы, характер охраны и технические средства безопасности.

Пленум Верховного Суда РФ в своём постановлении от 27.01.1999 № 1 определил «убийство по найму надлежит квалифицировать убийство, обусловленное получением исполнителем преступления материального или иного вознаграждения. Лица, организовавшие убийство за вознаграждение,

подстрекавшие к его совершению или оказавшие пособничество в совершении такого убийства, несут ответственность по соответствующей части статьи 33 и пункта «з» части 2 статьи 105 УК РФ.»¹

Раскрытие таких убийств представляет собой сложную задачу в силу разнообразия мотивов и способов их совершения, многообразия способов сокрытия следов преступного деяния, а также мер, принимаемых преступниками. Существующие меры по борьбе с заказными убийствами сталкиваются с рядом проблем, в результате этих факторов общество продолжает сталкиваться с соответствующими угрозами. Эффективное выявление и раскрытие таких преступлений требуют комплексного подхода, включающего как правовые, так и криминалистические аспекты.

В то же время демонстративный способ оставления тел на видных и часто людных местах явно характерен для террористических преступных методов, включающих элементы угрозы и запугивания. Не стоит забывать, что именно такой способ используется в большинстве убийств, связанных с разделом экономических интересов.

Из-за недостатка информации заказные убийства либо не раскрываются совсем, либо раскрываются, когда исполнитель заказного убийства установлен и найден, но зачастую заказчик остаётся неустановленным и безнаказанным.

Рассмотрим проблемы, которые не позволяют получить полный спектр информации при раскрытии и расследовании убийств по найму:

В большинстве случаев при раскрытии и расследовании преступления не учитываются все возможные непредвиденные обстоятельства, либо комплекс следственных действий и оперативно-розыскных мероприятий не соответствует криминалистической версии. В результате чего часто необходимо изменять и планировать дополнительные оперативно-розыскные мероприятия, а в некоторых случаях разрабатывать новые версии. Это обусловлено нехваткой квалифицированных сотрудников оперативных и следственных подразделений, а также ресурсов для расследования преступлений данного вида.

Также одной из проблем является недостаточное изучение личности преступника, так как оно необходимо для анализа его психологического портрета, выявления характерных черт его «почерка», что в свою очередь позволяет изучить тактику, стиль, определённые способы совершения преступлений, которые могут позволить связать преступления с конкретными лицами, а также обнаружить некоторую связь между несколькими преступлениями, совершенных одним лицом.

Ещё одной проблемой является недостаточное осуществление контроля за продажей товаров черного рынка, таких как огнестрельное оружие, взрывные устройства и яды. Так как они зачастую являются орудием убийства и в целом представляют собой серьезную угрозу безопасности жизни и

¹ Постановление Пленума Верховного Суда РФ от 27.01.1999 № 1 (ред. от 03.03.2015) «О судебной практике по делам об убийстве (ст. 105 УК РФ)».

здоровью граждан. Этот рынок процветает благодаря слабым законодательным мерам, слабой координации между правоохранительными органами и отсутствию эффективных механизмов контроля. Отсутствие строгого контроля облегчает преступникам приобретение огнестрельного оружия и взрывных устройств.

Также одной из основных проблем является недостаточный уровень изучения места преступления, путей отхода и подхода убийцы, и, меры по обнаружению следов либо не осуществляются должным образом, либо не применяются совсем. Важным элементом является также неправильное обращение с вещественными доказательствами, обнаруженными на месте преступления. Убийства по найму тщательно спланированы и количество следов, оставленных преступником на месте преступления ничтожно мало, поэтому осмотр места происшествия требует от сотрудников внимательности и сосредоточенности. Эти следы могут являться достаточным доказательством при расследовании других видов преступлений, но в данном случае они не так полезны. Например, обнаружение орудия убийства со следами преступника важно для раскрытия преступления и установления вины. Однако при заказных убийствах орудие убийства, зачастую оставляют на месте преступления, и оно в большинстве случаев нелегальное, не имеет следов, которые позволили бы идентифицировать преступника, поэтому оно не имеет большого значения.

Также к проблемам можно отнести и то, что эксперты не используют весь перечень криминалистических экспертиз. Это может привести к игнорированию или недооценке важных следов, которые необходимы для детального изучения событий преступления. Следы могут дать ценную информацию о передвижениях подозреваемого, выявить связь между местом преступления, подозреваемым или жертвой.

Негативным моментом является недостаточное изучение личности жертв. Этот недостаток характеризуется тем, что в большинстве случаев не направляются специальные запросы в соответствующие инстанции и, следовательно, не выявляется возможно значимая информация о личности. Кроме того, не изучаются вопросы, касающиеся связей убитого с преступными организациями.

Так как убийства по найму – это тщательно спланированные преступления, они сводят возможность появления свидетелей к минимуму, поскольку предполагается, что каждый участник чётко выполнил отведённую ему роль как на стадии подготовки, так и в момент совершения преступления. Поэтому установление свидетелей, которые могут предоставить следствию информацию об обстоятельствах совершенного преступления, является одним из самых сложных факторов. При выезде на место преступления руководитель следственно-оперативной группы должен определить основные поисковые мероприятия. Во-первых, должны быть организованы поквартирные обходы, во-вторых, поиск и задержание преступников по «го-

рячим следам». Перечисленные оперативные мероприятия в первую очередь направлены на поиск исполнителей. Основная задача по выявлению организаторов и посредников должна основываться на анализе полученной в ходе расследования информации о мотиве преступления и потенциальных заказчиках. Особенно важным на этом этапе является открытое сотрудничество следователей и оперативников для продвижения расследования. Главный принцип взаимодействия – взвешенное совместное принятие решений на основе информации из разных источников и своевременный обмен этой информацией.

Ещё одной проблемой современного расследования заказных убийств являются использование современных технологий. Заказчик может связаться с исполнителем через телекоммуникационную сеть Интернет, анонимные мессенджеры, посредников. Также использование преступниками для сокрытия следов криптовалют и анонимизирующих технологий делает финансовые потоки практически невозможными к отслеживанию.¹

Не предоставляется защита участникам уголовного процесса от угроз, преследования и расправ со стороны преступников, понуждающих потерпевших и свидетелей к даче заведомо ложных показаний и отказу от дачи показаний.²

Общая статистика показывает, что расследования заказных убийств продолжают годами и не приносят положительных результатов. Во многих уголовных делах, где имеются явные признаки «заказных убийств», из-за тактических ошибок теряются улики, скрываются следы преступления, а заинтересованные лица уходят от ответственности. В связи с этим возникает необходимость разработки научно обоснованных рекомендаций, направленных на повышение эффективности действий по выявлению и расследованию заказных убийств. Для этого необходимо выявить характерные закономерности, присущие данному виду преступлений, и уточнить взаимосвязь его структурных элементов, то есть признаков преступления.

На основе вышеизложенных проблем предлагаются следующие пути их решения:

1) Усиление мер государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства. Необходимо создать меры, обеспечивающие анонимность и безопасность потерпевших, свидетелей, а также иных лиц, участвующих в уголовном судопроизводстве. Это не только увеличит число лиц, сотрудничающих с исполнительными и судебными органами, но и способствует повышению доверия к правоохранительным органам.

¹ Петрова М.В. «Технологические аспекты расследования заказных убийств» // Криминалистика и судебная экспертиза, 2021

² Яшин, А. А. Проблема расследования заказных убийств (убийств по найму) / А. А. Яшин, Р. П. Кузьмин, А. Е. Бебех. // Юридические науки: проблемы и перспективы: материалы IV Междунар. науч. конф. (г. Казань, май 2016 г.). – Казань : Бук, 2016. – С. 281-284.

2) Введение новых стимулов для лиц, осуществляющих содействие органам внутренних дел. Новые системы вознаграждения за оперативно значимую информацию могут стать стимулом для её передачи. Также правоохранительные органы должны информировать общественность о подобных нововведениях путём использования средств массовой информации и телекоммуникационной сети Интернет.

3) Для повышения качества и эффективности получения оперативной информации может послужить оснащение сотрудников передовыми технологиями и средствами получения информации. Важно и обеспечение обучения сотрудников для использования новых технологий в своей работе. Регулярные инструктажи и тренировки помогут повысить уровень подготовки сотрудников. Также совершенствование системы межведомственной коммуникации позволит быстро обмениваться информацией и координировать действия, а также может повысить эффективность работы при сложной оперативной обстановке. Для обработки и визуализации данных, выявления закономерностей и принятия более обоснованных решений на ранних стадиях может поспособствовать внедрение аналитической платформы.

4) Для сокращения подобных преступлений необходимо усиление контроля за продажей предметов, изъятых из гражданского оборота. Внедрение технологий для отслеживания продаж и сделок на «чёрном» рынке может помочь правоохранительным органам обнаружить преступление ещё на стадии приготовления.

Расследование заказных убийств является сложной задачей, которая требует комплексного подхода. Качественный осмотр места происшествия, использование новейших технологий, усиление контроля за оборотом на «чёрном» рынке, усиление мер защиты свидетелей и межведомственное сотрудничество являются ключевыми элементами, которые могут значительно повысить эффективность расследования. Следует отметить, что успешное раскрытие подобных преступлений зависит не только от технологий, но и от высококачественной подготовки сотрудников полиции в данной категории преступлений.

Исходя из вышесказанного, можно сделать вывод, что заказное убийство имеет ряд особенностей, отличающих его от других преступлений, угрожающих жизни или здоровью человека. Эти особенности заключаются в том, что заказное убийство – это всегда заранее спланированное, хорошо продуманное и подготовленное преступление, направленное на решение конкретной задачи, и, как правило, между потерпевшим и непосредственным убийцей (исполнителем) нет никаких отношений, он лишь выполняет заказ третьего лица. Поэтому для раскрытия заказных убийств необходимо шире использовать оперативно-розыскные мероприятия, которые, хотя и являются в определённой степени более сложными по организации и проведению, но, несомненно, наиболее эффективными.

Ховавко Сергей Михайлович,
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России,
кандидат юридических наук, доцент

ПООЩРИТЕЛЬНАЯ НОРМА СТАТЬИ 205 УК РФ КАК СРЕДСТВО ПРЕДОТВРАЩЕНИЯ ТЕРРОРИСТИЧЕСКИХ АКТОВ

Угроза террористических актов в различные исторические периоды является актуальной для российского государства и общества, только с 1990 года жертвами терактов в России стали 4,7 тыс. человек. С началом специальной военной операции Российской Федерации фактически объявлена террористическая война – теракте в «Крокус Сити Холле» стал одним из крупнейших в Европе по числу жертв (22 марта 2024 года погибли 145 человек, в том числе шестеро детей). Предотвращение террористических актов является приоритетным направлением деятельности как оперативных подразделений, так и всех субъектов, вовлеченных в антитеррористическую деятельность. При этом основой противодействия терроризму является нормотворческая работа.

Ответственность за совершение террористического акта предусмотрена в ст. 205 УК РФ – за совершение террористического акта законодателем установлены одни из наиболее суровых уголовных наказаний, однако, вместе с тем, в анализируемой статье УК РФ предусмотрена и поощрительная норма, которая, при выполнении установленных в ней условий, допускает освобождение от уголовной ответственности. В частности, в соответствии с примечанием к ст. 205 УК РФ, лицо, участвовавшее в подготовке террористического акта, освобождается от уголовной ответственности, если оно своевременным предупреждением органов власти или иным способом способствовало предотвращению осуществления террористического акта и если в действиях этого лица не содержится иного состава преступления. Поощрительная норма ст. 205 УК РФ по сути является правовым средством предотвращения террористического акта при условии ее своевременного и эффективного использования в профилактической работе.

Планировать и организовывать профилактическую работу, в частности по разъяснению как ответственности за совершение террористических актов, так и возможности быть освобожденным от уголовной ответственности в соответствии с примечанием к ст. 205 УК РФ, следует с учетом характеристики лиц, совершающих террористические акты.

Террористы в целом делятся на две основные группы: 1) так называемые рядовые террористы-исполнители, в том числе смертники, 2) вербов-

щики, организаторы, идеологи, заказчики терроризма. При этом образование идеологов и лидеров террористических групп характеризуется более высоким уровнем по сравнению с рядовыми террористами-исполнителями, образование которых зачастую может ограничиваться неполным школьным.¹

Проведенное А.Е. Красильниковым исследование² позволило сделать ему следующие выводы: 1) практически никто из террористов не имел постоянного источника доходов, они существовали на деньги, получаемые в результате террористической деятельности; 2) преобладающая часть лидеров террористических группировок была осуждена ранее по уголовным статьям за совершение грабежей, бандитизм и иные преступления с корыстным мотивом и отягощенными насильственными действиями; 3) большая часть рядовых террористов ранее не были осуждены, профессиональными преступниками, пришедшими в терроризм из общеуголовной преступности, не являлись; 4) возраст большей части рядовых участников террористической деятельности составляет от 18 до 25 лет; 5) возраст руководителей террористических группировок находится в диапазоне 25-40 лет.

Террористический акт совершают в основном в соучастии лица, ранее не судимые, но тщательно к нему подготовленные. Выделяют две формы соучастия: группа лиц по предварительному сговору – 83,1% и организованная группа лиц – 11,1%.³

Самыми распространенными, по мнению А.Е. Красильникова мотивами вовлечения рядовых террористов-исполнителей в террористическую деятельность являются идейные соображения, возникшие на почве мести за погибших близких, разрушенное жилье и др., а также идеи ложного патриотизма и обмана на религиозной почве. Хотя в последнее время все чаще присутствует корыстный мотив – банальное желание получить деньги за совершенный теракт.

Действительно, достаточно сложно представить себе определенный портрет личности террориста, так как на протяжении нескольких десятков лет он менялся. Если еще двадцать лет назад теракты совершались в основ-

¹ Магомедов А.А., Макарян Т.А. Криминологическая характеристика личности преступника-террориста. / Вестник Академии экономической безопасности МВД России 2011, №2. – с.42-46. С.42-43

² Красильников А. Е Личность террориста: криминологический аспект // Законность. 2008. № 5. С. 46-48.

³ Гришко А.Я. Личность террориста: криминологический портрет // Терроризм. Правовые аспекты борьбы. Нормативные и международные правовые акты с комментариями, научные статьи / под ред. И.Л. Трунова и Ю.С. Горбунова. Изд. 2-е, перераб и доп., М., 2007. 518с. С.510

ном мужчинами, то на сегодняшний день для совершения данного вида преступлений стали привлекать женщин и даже несовершеннолетних лиц.¹ Возрастные критерии понижены (27,9 лет), по отношению к возрасту лиц, совершающих другие виды преступлений (32,1 год). Следует отметить, что террорист-исполнитель – это лицо с достаточно низким образовательным уровнем, однако с высоким уровнем притязаний и мотивацией. В настоящее время среди лиц, непосредственно совершающих террористические акты на территории РФ, преобладают выходцы из республик Средней Азии, въезжающие как трудовые мигранты, а также граждане РФ, в том числе несовершеннолетние, завербованные украинскими спецслужбами. При этом рядовые террористы-исполнители перед совершением террористического акта стараются так вести себя в повседневной жизни, чтобы не привлекать к себе внимание окружающих и ничем не выделяться из общей массы обычных людей.

Таким образом выявить конкретных террористов, подготавливающих теракт, крайне затруднительно, но в тоже время существует возможность проведения профилактической работы среди отдельных категорий лиц, в среде которых могут находиться потенциальные террористы. Это такие лица, как трудовые мигранты, прибывающие на территорию РФ из постсоветских государств; подростки и молодые люди, обучающиеся в различных учебных заведениях; лица, совершающие регулярные выезды в страны, где функционируют радикальные культурно-образовательные центры или религиозные организации; лица, регулярно участвующие в несанкционированных массовых мероприятиях и допускающие нарушения общественного порядка; лица, вовлеченные в деятельность экстремистских или террористических организаций, а также различных неформальных субкультур агрессивного типа.

Профилактическая работа среди этих категорий лиц может быть организована путем проведения разъяснительных групповых или индивидуальных бесед или раздачи памяток по месту работы, обучения, занятия спортом; при получении или продлении регистрационных документов или при привлечении к административной ответственности; рассылка смс-сообщений или сообщений по электронной почте со ссылкой на предварительно подготовленные и размещенные в сети Интернет пропагандистско-профилактические видеоролики.

Предметным содержанием такой профилактики должно быть разъяснение как особенностей объективной стороны террористического акта, так и сущности поощрительной нормы ст. 205 УК РФ. Кроме того, при прове-

¹ Станкевич А.М., Пушкин А.В. Особенности криминологического портрета личности современного террориста / Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 2-2. с. 185-190. С

дении профилактических бесед оперативные сотрудники могут использовать поощрительную норму ст. 205 УК РФ в целях склонения отдельных лиц, возможно уже вовлеченных в террористическую деятельность, к конфиденциальному содействию и сотрудничеству.

Таким образом, поощрительная норма ст. 205 УК РФ может быть эффективно использована как в пропагандистско-разъяснительной работе, так и в оперативно-розыскной деятельности по линии противодействия терроризму в целях привлечения лиц к конфиденциальному содействию и сотрудничеству и в целях предотвращения террористических актов.

Ховавко Сергей Михайлович,
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Крымского филиала краснодарского университета МВД России
кандидат юридических наук, доцент

Сорокина Анастасия Алексеевна,
курсант 4 курса
Крымского филиала краснодарского университета МВД России

ПРИЧИНЫ И УСЛОВИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ И ПОЛОВОЙ СВОБОДЫ ЛИЧНОСТИ

Преступления против половой неприкосновенности и половой свободы личности являются одними из самых опасных посягательств на моральное и физическое здоровье человека. Они занимают особое место в системе уголовных деяний в силу своей распространенности, о чем свидетельствует постоянно меняющаяся статистика.

Анализ статистики МВД России показывает, что в 2022-2023 гг. общее количество зарегистрированных преступлений категории «изнасилование и покушение на изнасилование» характеризуется незначительным уменьшением (-6,5%; 3096) по сравнению с аналогичным периодом прошлого года (-4,2%; 3311). Отмечается значительное уменьшение изнасилований и покушений на изнасилование, совершенных на транспорте и их рост в общественных местах (296; +10,4). При этом снизился уровень раскрытых преступлений прошлых лет по данной категории (- 2,1%; 283)¹.

Защита личной жизни, в особенности половой неприкосновенности, – это фундаментальная потребность каждого человека, вызванная стремлением к чувству безопасности и защищенности. Поэтому в судебной практике за совершение умышленных половых преступлений предусмотрено достаточно суровое наказание.

Так, судебная статистика свидетельствует, что в 2023 г. по ст. 131 УК РФ «Изнасилование» было осуждено 1921 человек, а за иные посягательства против половой неприкосновенности и половой свободы личности (ст. 132-135 УК РФ) – 6989 человек. Показательно, что число оправданных лиц составило 12 и 34 человека соответственно ².

Обязанность борьбы с такого рода преступлениями, выявление их причин и условий возложена на сотрудников органов внутренних дел.

¹ Состояние преступности в России (за январь – декабрь 2023 года). – М., ГИАЦ МВД России. 2024. 64 с.

² Уголовное судопроизводство. Общие показатели по категориям дел [URL//https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/11/s/1](https://stat.xn----7sbqk8achja.xn--p1ai/stats/ug/t/11/s/1)

Отсутствие понимания детерминантов затрудняет своевременную и эффективную разработку мер по профилактике и предупреждению половых преступлений.

Причинами половых преступлений называются внутренние факторы, лежащие в основе мотивации, побуждающие к совершению противоправных действий. Под условиями же понимаются – внешние факторы, которые обеспечивают возможность, способствуют или облегчают совершение преступлений. Они создают благоприятную обстановку для реализации преступного умысла. Эти две категории тесно связаны между собой и необходимы для возникновения преступности, то есть внутренние факторы, без соответствующих условий не могут породить такое явление.

Чтобы повлиять на преступность, предупредить совершение преступлений и уменьшить их количество, необходимо воздействовать не только на причины преступности, но и на условия их совершения. Следует сказать, что ранее ученые уже затрагивали в своих работах тему исследования причин и условий, способствующих совершению насильственных преступлений.

Так, Ю.М. Антонян, считает, что одной из главных причин совершения данного рода преступлений, является отказ противоположного пола на вступление в контакт, вследствие чего возникает враждебное отношение, женщина чаще всего становится олицетворением зла и разрушения, и такое негативное отношение распространяется в последующем на весь мир¹.

Г.А. Аванесов применительно к преступлениям насильственного характера, выделяет две группы причин и условий, а именно:

1) внутренние (по отношению к личности преступника) – это результат нездоровых процессов в психике человека, которые не исключают вменяемости, но постоянно звучат в сознании (непреодолимая тяга к виду крови, получение удовольствия от действий, связанных с причинением другим людям страданий);

2) внешние – негативное социальное окружение, отрицательное влияние различных факторов в процессе становления личности (недостатки в воспитании, дурной пример родителей или друзей, ведущих аморальный образ жизни и т.п.)².

С.В. Шевелева помимо общих детерминант преступности к причинам, способствующим совершению половых преступлений, называет следующие: недостатки в формировании личности, преобладание в характере таких негативных качеств, как жестокость, зависть, злоба; идеология и стандарты поведения криминальных и криминализованных структур, где обязатель-

¹ Антонян Ю.М. Криминология: учебник для академического бакалавриата. – 3-е изд., перераб. и доп. – М. : Издательство Юрайт, 2017. 268 с.

² Аванесов Г.А., Иншаков С.М., Аминов Д.И., Эриашвили Н.Д. Криминология: учебник для студентов вузов, обучающихся по специальности «Юриспруденция». – 6-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2013. 400 с.

ным является применение насилия в определенных ситуациях; деморализация, связанная с алкоголизацией и наркотизацией, приводящая к возникновению малых социальных групп, в которых единственным способом разрешения конфликтов является любой вид насилия¹.

Исходя из анализа работ этих и других авторов, к числу основных причин преступлений против половой неприкосновенности и половой свободы личности можно отнести следующие:

1. Высокий уровень латентности. Та часть сведений, которые не попали в официальные отчетные данные, то есть не были зарегистрированы правоохранительными органами в силу объективных обстоятельств (отсутствие заявления потерпевших). Данная категория преступлений возбуждается по заявлению потерпевшего, однако большая часть потерпевших из-за угроз в их сторону или в сторону их близких, боятся обратиться за помощью к правоохранительным органам, поэтому у потенциальных преступников, чувствующих свою безнаказанность, появляется больше желания и стремления совершать новые подобные преступления.

2. Внутренние убеждения и противоречия самого преступника. Сильная обида с раннего детства на методы воспитания матери, расставание, измена, предшествующее неподобающее поведение любимой девушки или супруги могут быть причинами мести и как следствие совершение половых преступлений в отношении похожих по внешним признакам или поведению женщин. Желание постоянного доминирования и ощущения власти, неудовлетворенность своей сексуальной жизнью, также являются главными мотивами совершения данного вида противоправных деяний.

3. Нарушение норм социального поведения. Совершение половых актов в присутствии несовершеннолетних в дальнейшем может вылиться в обнаружение нарушений психики несовершеннолетнего или во вступление в беспорядочные половые связи.

4. Приобретенные или наследственные психические заболевания. Особое восприятие окружающего мира и своеобразные эмоциональные реакции, недоразвитость некоторых психических функций в головном мозге обычно приводят к совершению насилия, так как больные не находят других способов удовлетворения своих сексуальных желаний.

5. Резкое увеличение уровня миграции. В большинстве стран психологические и социальные нормы сексуального поведения существенно отличаются от норм, принятых в нашей стране.

6. Провоцирующее поведение со стороны жертвы. Такое поведение создает напряженную обстановку, подталкивающую виновного к совершению преступления. Раскрепощенное поведение из-за чрезмерного употребления алкогольных напитков или одурманивающих веществ, вызывающий

¹ Шевелева С.В., Гребеньков А.А., Новичков В.Е. Криминология: учеб. пособие. Юго-Зап. гос. ун-т. Курск, 2011. 191 с.

внешний вид, частое посещение ночных клубов и других увеселительных заведений являются аморальным поведением потерпевшего. Возможно, жертва на самом деле дала согласие на половой акт, но в силу мести решила оклеветать своего обидчика. Поэтому важно учитывать и уделять особое внимание виктимности потерпевших.

Еще одна распространенная причина совершения насильственных преступлений – повышенная агрессивность. Негативный детский опыт агрессии обеспечивает сохранение и в дальнейшем ее демонстрацию другим людям. Агрессия может быть вызвана детскими травмами, неправильным воспитанием или игнорированием детских потребностей со стороны родителей. Также на уровень агрессии влияет наличие алкогольной или наркотической зависимости, что является научно доказанным и обоснованным.

Условиями, способствующими совершению преступлений против половой неприкосновенности и половой свободы личности, являются:

1. Недостатки в работе правоохранительных органов. Упущения в организации и проведении профилактических и воспитательных работ с лицами, склонными к совершению данного вида преступлений, низкий уровень организации мероприятий по выявлению лиц с отклоняющимся поведением и своевременному применению к ним соответствующих мер воспитательного характера. Условно-досрочное освобождение осужденных без достаточного изучения особенностей личности сексуального преступника, назначение мягкого наказания за совершение насильственных действий против личности. Недостаточный контроль за криминогенными объектами, в которых довольно-таки распространены половые преступления (неосвещенные и безлюдные места, где вовсе отсутствуют камеры видеонаблюдения).

2. Отсутствие требований к нормам морали. Увеличилось количество ночных клубов, разного рода увеселительных заведений, в которых широко и чрезмерно употребляется алкогольная продукция, табачные изделия, а иногда и наркотические средства, одурманивающие разум потерпевших. Резкое увеличение порнографических сайтов в Интернете, доступ к которым не всегда является ограниченным, чаще всего – открытый, а также рост уровня проституции.

3. Отрицательное влияние средств массовой информации, Интернета и телевидения. Большинство современных фильмов, книг, игр романтизируют преступность и все ее проявления. У людей формируется неправильное представление реальности, что приводит к имитации преступного поведения. Возникает мнение, что решить все имеющиеся проблемы, можно только путем совершения преступлений. Происходит пропаганда насилия и жестокости, искажаются и формируются ложные идеалы и ценности вследствие чего, в обществе возникает разлад и дестабилизация, увеличивается уровень агрессии, а также появляется дополнительный стимул, побуждающий к совершению действий сексуального характера.

4. Недостатки в системе образования. Отсутствие полового воспитания в образовательных организациях, которое необходимо для ознакомления людей разных возрастных категорий с особенностями построения взаимоотношений между полами, для формирования правильного представления о сексуальной жизни в целом.

5. Пробелы в действующем законодательстве. Наличие недостатков в разработке и совершенствовании законодательства в части ужесточения ответственности, связанной с проституцией, а также закрепления определенных понятий на правовом уровне для четкого понимания, отделения от смежных статей и для единого метода квалификации содеянного. Проституция выступает одним из основных детерминантов насильственных преступлений, однако за занятие проституцией предусмотрена только административная ответственность в виде штрафа, вместо уголовной с более жесткой мерой наказания. Отсутствуют нормы, предусматривающие в качестве меры принуждения – принудительное лечение в отношении лиц, совершивших противоправное деяние и страдающих алкогольной, наркотической или иной зависимостью.

Своевременное изучение причин и условий, способствующих совершению преступлений против половой неприкосновенности и половой свободы личности имеет большое и важное значение в деятельности правоохранительных органов при создании мер предупреждения и профилактики данной категории преступлений.

Грамотный анализ и понимание детерминант преступности, а также их взаимосвязей с различными сферами жизни общества, позволяют разрабатывать эффективные программы профилактики и борьбы с правонарушениями данного вида, учитывать их при планировании мероприятий по розыску насильников, сбору и использованию изобличающих их вину доказательств.

Шатилов Алексей Валерьевич,
старший преподаватель
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России,
кандидат юридических наук,

**О НЕКОТОРЫХ ПРОБЛЕМАХ, ВОЗНИКАЮЩИХ
У СОТРУДНИКОВ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ,
СВЯЗАННЫХ С УСТАНОВЛЕНИЕМ МЕСТОНАХОЖДЕНИЯ
И ДОСТАВЛЕНИЕМ ЛИЦА, НЕ ОБЛАДАЮЩЕГО СТАТУСОМ
ПОДОЗРЕВАЕМОГО ИЛИ ОБВИНЯЕМОГО, В РЕГИОН ВЕДЕНИЯ
ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ**

Право на свободу передвижения, выбор места пребывания и жительства¹, закрепленное за гражданами в Конституции РФ в отдельных случаях ведения предварительного расследования по уголовным делам создает определенные трудности в оперативности принятия процессуальных решений по расследуемым уголовным делам для привлечения к ответственности виновных лиц.

Зачастую несвоевременность или непрофессиональное принятие органами предварительного расследования действий, направленных на получение процессуальных доказательств по расследуемым уголовным делам, указывающих на причастность тех или иных лиц к совершенному преступлению, приводит к смене местожительства или места пребывания этими лицами в рамках территории страны, но другого субъекта Российской Федерации. Перемещение «потенциальных подозреваемых» может происходить как в силу объективных причин их личной жизни, смены работы и других так и субъективных, граничащих с желанием уйти от будущей возможной ответственности, за совершенное правонарушение, зная, что ведется предварительное следствие по уголовному делу.

Смена места жительства или места пребывания «потенциальным подозреваемым» на ключевом этапе, непременно создаёт определенные трудности для проведения и окончания предварительного расследования по уголовному делу в предусмотренные уголовно-процессуальным законодательством сроки с привлечением лица в качестве обвиняемого и требует активизацию дополнительных ресурсов для достижения цели.

¹ Ст. 27 Конституция Российской Федерации Принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года.

Согласно п. 38 ст. 5 УПК, розыскные меры – это «меры, принимаемые дознавателем, следователем, а также органом дознания по поручению дознавателя или следователя для установления лица, подозреваемого в совершении преступления»¹.

Как правило, дознаватель или следователь ограничиваются вынесением постановления в адрес сотрудников оперативного подразделения о необходимости проведения оперативно-розыскных, розыскных или отдельных следственных действий по установлению местонахождения лица, причастного к совершению преступления и фиксацию фактических данных, которые при условии их закрепления процессуальным путем будут являться доказательствами.

Сотрудники оперативных подразделений при проведении розыскных мероприятий, направленных на установление местонахождения лица вне региона ведения предварительного расследования, даже учитывая имеющиеся современные возможности проведения специальных технических мероприятий и развитости мессенджеров и социальных сетей сталкиваются с определенными трудностями, в том числе в виду отсутствия у «потенциального подозреваемого» (в данном случае и далее по тексту речь идет о лицах, не имеющих статус «подозреваемого» или «обвиняемого» по возбужденному уголовному делу, которые не были допрошены по делу или были допрошены в качестве свидетеля) в новом регионе его пребывания, устойчивых социальных связей, постоянного места регистрации, работы и так далее. Часть оперативно-розыскных мероприятий, направленных на установление места пребывания и жительства возможно провести в регионе ведения предварительного расследования, но полученные результаты скорее всего будут носить вероятностный характер. Для получения категоричных сведений о точном местонахождении «потенциального подозреваемого», проведения с его участием отдельных следственных действий и последующим его доставлением к лицу, ведущему предварительное расследование, возникает необходимость по проведению розыскных мероприятий сотрудниками оперативных подразделений непосредственно в регионе нахождения лица.

На практике сотрудники оперативных подразделений, прибывшие в регион местонахождения «потенциального подозреваемого», очень часто могут сталкиваться с коррупционными или иными противодействующим в розыске и задержании лица проявлениями, для дальнейшего его доставления, со стороны «местных» сотрудников оперативных или иных подразделений, которые постоянно проживая и работая в регионе нахождения «потенциального подозреваемого» могут как лично быть знакомы с преступником, так и через круг общих знакомых и предупредить его в том числе за

¹ Ст. 5 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изменениями и дополнениями) [Электронный ресурс]. Доступ из справочно-правовой системы «Гарант»).

денежное вознаграждение или иную выгоду материального или нематериального характера. Данное обстоятельство непременно ведет к недоверию и нежеланию в бедующем «ставить в известность» о целях, задачах своего пребывания в командировке по установлению местонахождения и задержании «потенциального подозреваемого». В данном случае речь идет также и привлечении спецподразделений Росгвардии для задержания лица. В связи с вышесказанным, как один из выходов из данной заведомо «проигрышной» ситуации для оперативников, находящихся в командировке, в настоящее время используется вариант использования только служб БСТМ и ОПБ региона нахождения, учитывая специфику статуса сотрудников этих подразделений. Сотрудники этих подразделений связываются напрямую с сотрудниками оперативных подразделений, прибывших в командировку (инициатором), и сообщают всю имеющуюся информацию лично.

После того как местонахождение «потенциального подозреваемого» установлено, произведено его задержание (в данном случае речь идёт не о процессуальном задержании в порядке ст. 91 УПК РФ), получены фактические сведения, будь то показания, сообщенные в качестве свидетеля или вещественные доказательства, изобличающие его в совершении преступления, естественно возникает необходимость его доставления в регион ведения предварительного расследования, для допроса его следователем или дознавателем, избрания соответствующего статуса с последующим при необходимости избранием меры пресечения. Именно на этом этапе и возникают сложности, связанные с доставкой лица, которые на практике могут проявляться в двух видах.

Первый вид – доставка путем вручения повестки о вызове на допрос к лицу, ведущим предварительное расследование в которой указывается кто и в каком качестве вызывается, к кому и по какому адресу, дата и время явки на допрос, а также последствия неявки без уважительных причин.¹ Обеспечение явки в данном случае обеспечивается с добровольно выразившимся желанием проследовать сразу и вместе с оперативниками в регион ведения предварительного расследования, будь то на служебном автомобиле или посредством транспорта общественного пользования.

Второй вид – доставка посредством оформленного процессуальным путем вынесения постановления о приводе. Постановление оформляется лицом, производящим предварительное расследование и направляется в регион используя любой из имеющихся в настоящее время современный способ связи (ИСОД, факсимильная связь, электронная почта, мессенджеры и так далее). После получения такого документа, придания ему бумажной формы, лицо, которое будет подвергнуто приводу ознакомившись с ним

¹ Ст. 188 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изменениями и дополнениями) [Электронный ресурс]. Доступ из справочно-правовой системы «Гарант».

удостоверяет его подписью на постановлении.¹ Доставка также происходит, как и в первом случае или на служебном автомобиле, или на другом виде общественного транспорта.

В обоих перечисленных случаях могут возникнуть две явно выраженные проблемы, связанные: первая с волеизъявлением лица для доставления его к месту проведения предварительного расследования, а вторая, что является наиболее важным с временным промежутком нахождения в пути следования в регион проведения предварительного расследования. Если разрешение первой проблемы основывается в основном на субъективных аспектах лиц и граничит как правило с опытом, профессионализмом сотрудников оперативных подразделений, умением высказывать мотивированные доводы направленные на убеждение, то вторая проблема несёт собой больше объективный характер, например обстоятельства, которые могут возникнуть в дороге, или другие препятствия, что может помешать или затруднить прибытие к месту проведения предварительного расследования в срок, не превышающий 48 часов. В данном случае имеется в виду процессуальный срок задержания в случае дальнейшего избрания меры пресечения в виде «заключение под стражу» подозреваемому, обвиняемому. Очевидно, что следователь выходя с ходатайством в суд об избрании меры пресечения в виде «заключение под стражу» должен указывать в нем время фактического ограничения свободы передвижения лица, а также соблюдать другие положения уголовно-процессуального законодательства.² Несоблюдение этих обстоятельств влечет за собой не только нарушение конституционных прав гражданина, на свободу перемещения, но и невозможности в дальнейшем избрания меры пресечения в виде «заключения под стражу», а значит как следствие избрание другой меры пресечения несвязанной с лишением свободы и соответственно возможности скрыться от органов внутренних дел. На это так или иначе ссылаются и другие авторы, М.В. Давыдов указывает, что действительно, неверно определенный момент задержания и неверное исчисление его сроков могут привести к существенному нарушению прав подозреваемого.³ О.А. Теплякова и М.М. Рафиков в своей статье также указывают на возможные допущения. В частности, следователь может произвольно зафиксировать в протоколе задержания «удобное» для него время

¹ Ст. 113 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изменениями и дополнениями) [Электронный ресурс]. Доступ из справочно-правовой системы «Гарант»)

² Ст. 91 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (с изменениями и дополнениями) [Электронный ресурс]. Доступ из справочно-правовой системы «Гарант».

³ Давыдов М.В. Проблемы правового регулирования исчисления срока задержания полицией: административный и уголовно-процессуальный аспект // Российская юстиция. – 2016 – № 10 – С. 56–59.

фактического задержания (до момента составления соответствующего протокола). Порой время составления протокола и факт задержания вовсе совпадают. Подобные ситуации нашли свое отражение в практике Европейского суда по правам человека, указывающего, например, в принятом им Постановлении по делу «Фортальнов и другие (Fortalnov and Others) против Российской Федерации»¹, что отсутствие протокола задержания подозреваемого или его несвоевременное составление свидетельствует о незарегистрированном содержании под стражей лица, права которого нарушаются уже в силу данного факта (отсутствие протокола задержания или его несвоевременное составление). Данное обстоятельство Европейский суд по правам человека (далее – ЕСПЧ) обозначает как абсолютное отрицание основополагающих гарантий прав человека (п. 76 рассматриваемого постановления ЕСПЧ).²

В обоих перечисленных случаях ответственность, в том числе и связанная с возможным совершением должностного преступления несет оперативный сотрудник, который в буквальном смысле должен импровизировать по ходу развития событий, чтобы не выйти за рамки правового поля. Считаю, что в данном случае назрела необходимость совершенствования правового регулирования и вмешательства в законодательство, а именно необходимо законодательно закрепить нормы, защищающие и обеспечивающего определенными правами сотрудников оперативных подразделений, которые наиболее чаще других служб сталкиваются с описанными по ходу статьи явлениями.

1 Постановление Европейского суда по правам человека по делу «Фортальнов и другие (Fortalnov and Others) против Российской Федерации» (жалоба № 7077/06 и 12 других жалоб): [от 26 июня 2018 г.] // Бюллетень Европейского суда по правам человека. Российское издание. – 2020 – № 1

2 Теплякова О.А. Рафиков М.М. О некоторых проблемах, возникающих в деятельности органов предварительного расследования при осуществлении задержания согласно нормам УПК РФ // Вестник Московского университета им. С.Ю. Витте. Серия 2. Юридические науки 2002. № 1(31)

Южанинов Василий Сергеевич,
старший преподаватель
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Назаров Юрий Андреевич
курсант 3 курса
Краснодарского университета МВД России

О ВОПРОСАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Развитие нашего общества и переход его с индустриального на пост-индустриальный уровень, неразрывно связано с появлением информационных технологий. С каждым годом, изобретения человечества обретали все более широкую популярность и актуальность по всему миру, что требовало новаторских идей и усовершенствований, в связи с растущими потребностями общества. На сегодняшний день нельзя представить полноценную жизнь без инновационных информационных технологий, которые окружают нас повсюду и применяются во всех сферах жизнедеятельности: наука, медицина, образование, бизнес и другие. Информационные технологии помогают нам эффективно обмениваться информацией, управлять данными, создавать и приобретать товары и услуги. Однако подобные технологии могут использоваться не только лишь для того, чтобы приносить в общество полезный вклад, но и могут выступать в качестве средства и орудия совершения преступлений. В связи с повсеместной информатизацией и цифровизацией, активно растет количество совершаемых преступлений с использованием информационно-коммуникационных технологий. Данный вид преступлений принято называть «киберпреступлениями».

На сегодняшний день, понятие «киберпреступление» не нашло своего законодательного отражения в нормативно-правовых актах и международных договорах, однако, среди ученых существуют различные мнения относительно толкования данного определения. Большинство научных деятелей предлагает не закреплять «рамочные» определения данного понятия, они обуславливают это тем, что ввиду постоянного роста производства новых телекоммуникационных и технических средств его трактовка будет иметь закономерный характер изменяться и дополняться новыми составляющими и структурными элементами.¹

¹ Федорович В.Ю. Что такое «киберпреступление»? // Вестник Московского университета МВД России. 2020. № 3. С. 14.

На наш взгляд, наиболее подходящее определение «киберпреступлению» дает Л.И. Бутова, которая считает наиболее важным аспектом – проведение глубокого анализа смысловой и содержательной части рассматриваемого термина. По ее мнению, «Киберпреступление – это общественно опасное деяние, выраженное в форме действия или бездействия, совершаемое в информационно-телекоммуникационной сфере с использованием телекоммуникационных средств и способов, с помощью технических устройств, компьютерных сетей и систем, их программных компонентов в отношении информации, размещенной, используемой, обрабатываемой во всех информационно-телекоммуникационных сетях».¹

По официальным статистическим данным МВД России, в 2019 году было зарегистрировано 294,4 тысячи преступлений, совершённых с использованием информационно-телекоммуникационных технологий. В 2020 году данный показатель составил 510 тысяч преступлений, в 2021 году – 517 тысяч, в 2022 году – 522 тысячи, в 2023 – 677 тысяч преступлений, а также в период с января по сентябрь 2024 данный показатель составил 564 тысяч преступлений. В сравнении с аналогичным периодом предыдущего года в январе – сентябре 2023 года в России было зарегистрировано 15,3% меньше преступлений, совершённых с использованием информационно-телекоммуникационных технологий.²

Согласно статистическим данным, приведенным на официальном сайте МВД РФ, можно сделать вывод, что данный вид преступлений обретает высокий рост и все больший охват с каждым годом.

Киберпреступники могут совершать различные виды преступлений, такие как кража личных данных, взлом компьютерных систем, распространение вредоносного программного обеспечения и другие, оставаясь при этом анонимными или незамеченными, поэтому данное преступление следует называть высоклатентным.

Одной из причин высокой латентности киберпреступлений является сложность их выявления и раскрытия, кроме этого, многие жертвы могут даже не осознавать, что стали объектом кибератаки, особенно если злоумышленник действует скрытно. Также, некоторые киберпреступления могут совершаться из-за рубежа, что усложняет процесс раскрытия и расследования, это прежде всего связано с проблемами международного сотрудничества в области борьбы с киберпреступностью.

Для снижения уровня латентности киберпреступлений необходимо повышать осведомленность общества о возможных угрозах и способах за-

¹ Бутова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник 2016. № 3 (15). С 28-31

² Краткая характеристика состояния преступности в Российской Федерации за январь - сентябрь 2024 года // [Электронный ресурс] Режим доступа: <https://мвд.рф/reports/item/50761212/>

щиты от них, а также улучшать технические средства и методы обнаружения и предотвращения таких преступлений. Ввиду этого, представляется необходимым усиление контроля над данной сферой деятельности, которую осуществляют сотрудники правоохранительных органов. Важную роль играет профилактика совершения данных преступлений, выраженная в проведении профилактических бесед, а также в активной работе с населением и лицами, которые могут быть стать жертвами киберпреступлений. На примере сотрудников оперативных подразделений ОВД РФ, уполномоченных проводить оперативно-розыскную деятельность, следует рассмотреть более подробно проведение и обеспечение данных профилактических мероприятий. Безусловно, меры, которые предпринимаются государством, в том числе Министерством Внутренних Дел Российской Федерации имеют свои положительные результаты. Вместе с тем, следует понимать, что недоработки в данном направлении отражаются на раскрываемости, рассматриваемых преступлений.

По данным МВД России, в 2019 году органами внутренних дел было раскрыто 55 тысяч преступлений, совершённых с использованием информационно-телекоммуникационных технологий. В 2020 году данный показатель составил 82 тысячи раскрытых ОВД преступлений, в 2021 году – 105 тысяч, в 2022 году – 124,9 тысяч, в 2023 – 150 тысяч преступлений, а также в период с января по сентябрь 2024 данный показатель составил 118 тысяч раскрытых ОВД преступлений. В сравнении с аналогичным периодом предыдущего года в январе – сентябре 2023 года органами внутренних дел было раскрыто 116 тысяч преступлений, совершённых с использованием информационно-телекоммуникационных технологий.¹

Для того, чтобы предотвратить совершение киберпреступлений, мы предлагаем рассмотреть более подробно каким образом устроена профилактика преступных деяний оперативными подразделениями.

Согласно ст. 1 Федерального закона от 12.08.1995 N 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности»: «Оперативно-розыскная деятельность – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом, в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств».²

¹ Краткая характеристика состояния преступности в Российской Федерации за январь - апрель 2024 года // [Электронный ресурс] Режим доступа: <https://мвд.рф/reports/item/50761212/>

² Федеральный закон от 12.08.1995 № 144-ФЗ (ред. от 29.12.2022) «Об оперативно-розыскной деятельности»

Благодаря реализации оперативно-розыскных мероприятий создаются условия для всестороннего учёта противоправных действий и неизбежности наказания, что позволяет восстановить социальную справедливость, исправить осуждённого и предотвратить новые преступления. Важную роль в работе по предупреждению преступлений играет поиск лиц, скрывающихся от правосудия. Такие лица, находясь на свободе, продолжают совершать противоправные действия, запрещённые уголовным законодательством, и вовлекают добропорядочных граждан, включая несовершеннолетних, в совершение общественно опасных деяний. Соглашаясь с Е.С. Лапиным, мы считаем, что ключевым направлением профилактической работы оперативно-розыскных подразделений является: профилактика преступлений общего характера, которая заключается в целенаправленной деятельности субъектов профилактики преступлений по выявлению, устранению и нейтрализации факторов, способствующих совершению преступлений; индивидуальная профилактика, которая предполагает выявление конкретных лиц, от которых можно ожидать совершения преступления, и воздействие на них или на окружающую их среду с целью предотвращения преступления и изменения поведения от антиобщественного к законопослушному.¹

Как уже было упомянуто выше, оперативные подразделения осуществляют свои полномочия, в соответствии с нормативно-правовой базой. В том числе и осуществление профилактических мероприятий осуществляется в соответствии с Конституцией РФ, Федеральными законами РФ и приказами МВД России. На примере основных нормативно-правовых актов, регламентирующих данную деятельность, следует рассмотреть проблематику осуществления профилактических мер.

В соответствии со ст. 5 Федерального закона от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации», к субъектам профилактики правонарушений относятся федеральные органы исполнительной власти, в том числе к которым относятся МВД РФ.² Оперативные подразделения являются структурными подразделениями МВД РФ. В следствии чего мы приходим к выводу, что к компетенции оперативных подразделений также относится осуществление профилактических мероприятий. Ввиду специфики деятельности, при осуществлении профилактических мероприятий, которая была рассмотрена нами выше основными направлениями являются общая и индивидуальная профилактика, что более подробно отражается в ведомственных приказах МВД России от 04.03.2020 № 119 и от 24.08.2023 № 619.

Согласно п.2 Приложения N 1 к приказу МВД России от 04.03.2020 № 119: «Официальное предостережение (предостережение) может быть

¹ Лапин Е.С. «Оперативно-розыскная деятельность. Курс правовых и теоретических основ» учебное пособие 4е издание, дополн. М., Юрлитинформ, 2014 г, 256 с.

² Федеральный закон от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации»

объявлено физическому лицу, в том числе в отношении которого применяются меры индивидуальной профилактики правонарушений, при осуществлении им действий, создающих условия для совершения правонарушений, либо в целях недопустимости продолжения антиобщественного поведения, только в случае отсутствия в его действиях признаков деяния, за совершение которого данное лицо могло бы быть привлечено к уголовной или административной ответственности».¹

Ввиду принятия нового приказа МВД РФ от 24.08.2023 год № 619², оперативные подразделения осуществляют деятельность по профилактике правонарушений в соответствии с ним. Так, к мерам оперативно-розыскного характера относятся:

1) Осуществление в установленном порядке комплексного анализа оперативной обстановки на соответствующей территории и объектах, результатах работы, выявление и прогнозирование тенденций и отклонений, выработка на этой основе своевременных, обоснованных и оптимальных управленческих решений, направленных на эффективное решение задач в сфере профилактики правонарушений.

2) Осуществление в установленном порядке регулярного обмена оперативной и иной информацией, включая обобщенные информационные письма (представления), имеющей значение для предупреждения правонарушений, между субъектами ведомственной системы профилактики, в соответствии с компетенцией либо передача ее в иной орган государственной власти.

3) Участие в пределах компетенции в разработке и реализации мероприятий в сфере профилактики правонарушений, предусмотренных государственными программами Российской Федерации, федеральными целевыми программами, межгосударственными программами, национальными проектами (программами), федеральными и ведомственными проектами, а также документов планирования по профилактике преступности либо пресечению отдельных преступлений.

4) Изучение и обобщение практики применения законодательных и иных нормативных правовых актов Российской Федерации по проблемам профилактики правонарушений, проведение анализа реализации полномочий в сфере профилактики правонарушений.

¹ Приказ МВД России от 04.03.2020 № 119 «О некоторых вопросах объявления органами внутренних дел Российской Федерации официального предостережения (предостережения) о недопустимости действий, создающих условия для совершения преступлений, административных правонарушений, разрешение которых отнесено к компетенции полиции, либо недопустимости продолжения антиобщественного поведения» (Зарегистрирован Минюстом России 22.06.2020, № 58737) (ред. 14.03.2023)

² Приказ МВД России от 24.08.2023 № 619 «О некоторых организационных вопросах деятельности органов внутренних дел Российской Федерации по профилактике правонарушений»

Все перечисленные законодателям оперативно-розыскные меры профилактического воздействия, на наш взгляд, носят «слишком общий» характер и могут толковаться правоприменителем по-разному. Закон не дает четкого понимания пределов и масштабов их применения, не устанавливает периодичность и контроль за их применением. Обозначенных законодателем мер достаточно для профилактики и предотвращения «традиционных» видов преступлений, так, мы видим, что общее количество преступлений в 2024 году (в период с января по сентябрь) сократилось на 2,5% по сравнению с этим же периодом 2023 года. Вместе с тем, если говорить о преступности, применяющей информационно-телекоммуникационные технологии, то мы видим, что за девять месяцев 2024 года, количество киберпреступлений в России увеличилось на 15,3% в сравнении с аналогичным периодом прошлого года, кроме этого в общем числе зарегистрированных преступлений их удельный вес увеличился с 33,3% в январе – сентябре 2023 года до 39,3% в 2024 году.¹

Таким образом, обозначенных законодателем мер явно недостаточно, на наш взгляд, необходимо значительно расширить имеющиеся нормативно-правовые акты или создать новый, где будут предусматриваться конкретные меры профилактического воздействия, как общего, так и индивидуального характера, направленные на предупреждение ИТ-преступлений, отдельно для каждого оперативного подразделения, специализирующегося на выявлении и раскрытии киберпреступлений.

¹ Краткая характеристика состояния преступности в Российской Федерации за январь - апрель 2024 года // [Электронный ресурс] Режим доступа: <https://мвд.рф/reports/item/50761212/>

Южанинов Василий Сергеевич,
старший преподаватель
кафедры оперативно-разыскной деятельности в ОВД
Краснодарского университета МВД России

Расулов Нариман Надирович,
курсант 3 курса
Краснодарского университета МВД России

ФИШИНГ КАК САМОСТОЯТЕЛЬНЫЙ ВИД УГОЛОВНОГО ПРЕСТУПЛЕНИЯ

В России наблюдается рост преступлений с использованием информационных технологий, причем почти 50% этих преступлений связаны со взломом пин-кодов банковских карт. Мошенники постоянно изобретают новые способы взлома систем, содержащих реквизиты банковских карт и пин-коды, к которым даже системы защиты не всегда успевают адаптироваться. В 2022 году мошенничество в Интернете, в частности фишинг, нанесло пользователям российских банковских карт ущерб на сумму, превышающую 74 млрд рублей, в основном из-за невнимательного отношения пользователей к своим данным. Одной из таких распространённых проблем является фишинг.

Фишинг – это распространенный метод атаки, при котором злоумышленники используют массовую рассылку, чтобы заманить пользователей на поддельные сайты для получения личной информации, такой как данные банковской карты и пароли. Пользователи должны избегать ввода конфиденциальной информации на непроверенных сайтах и должны быть осторожны с подозрительными кампаниями по электронной почте.¹

Сам по себе фишинг не может считаться уголовным преступлением по УК РФ, но последствия преступления, такие как неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ, подпадают под действие статьи 272 и 273. Фишинг – это просто инструмент, используемый мошенниками для совершения этих преступлений.²

Одним из примеров проявления данного вида мошенничества можно выделить необычное «киберпреступление».

¹ Что такое фишинг? Описание и определение термина. URL: <https://biznesprost.ru/fishing.html> (дата обращения: 10.04 2021 г.)

² Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.03.2022) (с изм. и доп., вступ. в силу с 23.03.2022) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

Рахматуллин Ф.Р. использовал на своем ноутбуке заведомо вредоносную программу для ЭВМ, предназначенную для несанкционированного копирования компьютерной информации. В определенную дату и время он умышленно скопировал информацию с веб-сайта, нанеся тем самым вред интернет-ресурсу.

Действия подсудимого суд квалифицирует по ч. 1 ст. 273 УК РФ, как использование компьютерной программы, заведомо предназначенной для несанкционированного копирования компьютерной информации.¹

Приведу пример нарушения статьи 272 УК РФ, запрещающей неправомерный доступ к компьютерной информации.

Представитель Кашлинского районного отделения Федеральной почтовой связи заподозрил, что их компьютерная система заражена вирусом, и сообщил об этом в отдел полиции. В ходе проведения следственных и оперативно-розыскных мероприятий было установлено, что Гражданин Ф. скопировал троянскую программу на свой рабочий компьютер, а затем отправил ее по электронной почте в РУФПС. При открытии письма программа сработала, что позволило преступнику получить доступ к конфиденциальным данным.

Таким образом, своими действиями гражданин Ф. совершил преступление, предусмотренное ст. 272 ч. 2 УК РФ – неправомерный доступ к компьютерной информации, а также ч. 1 ст. 165 УК РФ – причинение имущественного ущерба путем обмана или злоупотребления доверием.

Фишинговые атаки представляют собой серьезную угрозу в России: ежедневно физическим лицам и организациям отправляется до 1 миллиона поддельных сообщений с сайтов. Около 70% всех целевых атак на российские компании и организации начинаются с фишинга, который позволяет преступникам получить доступ к корпоративной инфраструктуре и потенциально контролировать всю сеть. Последствия успешной атаки могут быть серьезными, включая утечку конфиденциальных данных и взлом банковских счетов. Фишинговые атаки используют как хакерские группы, так и отдельные киберпреступники.

Существует несколько типов фишинговых атак, в том числе:

1. Фишинг по электронной почте: это наиболее распространенный тип фишинговой атаки, когда злоумышленник отправляет электронное письмо, которое выглядит как доверенное, и просит получателя предоставить конфиденциальную информацию, такую как пароли, номера кредитных карт или личные данные.

¹ Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

2. Целевой фишинг. Этот тип атаки часто нацелен на конкретных людей, выдавая преступника за кого-то, кого жертва знает, например, за коллегу или друга. Злоумышленник использует информацию о жертве, чтобы электронное письмо выглядело более убедительно.

3. Smishing или SMS-фишинг – это тип фишинговой атаки, которая осуществляется с помощью текстовых сообщений. Злоумышленник отправляет текстовое сообщение, которое, как представляется, из законного источника, просит получателя щелкнуть ссылку или предоставить конфиденциальную информацию.

4. Вишинг или голосовой фишинг – это разновидность фишинговой атаки, которая осуществляется по телефону. Злоумышленник звонит жертве и выдает себя за законный источник, такой как банк или государственное учреждение, запрашивая конфиденциальную информацию.¹

5. Фишинг на основе вредоносного ПО. Этот тип фишинговой атаки заключается в том, что злоумышленник отправляет электронное письмо со ссылкой или вложением, содержащим вредоносное ПО. Когда получатель нажимает на ссылку или открывает вложение, вредоносное ПО загружается на его устройство.²

Каждый может стать жертвой таких преступлений в Интернете. По этой причине стоит задаться вопросом: «Как же самостоятельно защитить свои данные от мошенников?»

От фишинга нет универсального способа защиты, кроме того, как внимательно следить за своими персональными данными. Простые способы:

1. Будьте осторожны с любыми нежелательными электронными письмами, сообщениями или звонками с просьбой предоставить личную информацию.

2. Проверьте адрес электронной почты или номер телефона отправителя, чтобы убедиться, что они действительны.

3. Не переходите по ссылкам в подозрительных электронных письмах или сообщениях.

4. По возможности используйте двухфакторную аутентификацию.

5. Обновляйте свой компьютер и программное обеспечение безопасности.

6. Не вводите личную информацию на незащищенных сайтах.

7. Используйте менеджер паролей для создания надежных уникальных паролей.

8. Расскажите себе и другим о фишинге и о том, как его избежать.

9. Остерегайтесь срочных или угрожающих выражений в электронных письмах или сообщениях.

¹ URL <https://habr.com/ru/company/varonis/blog/544140/>

² URL https://www.securitylab.ru/blog/company/PandaSecurityRus/350582.php?ysclid=1fo278_z8nz341167371

10. Свяжитесь с компанией или организацией напрямую, если вы не уверены в законности электронного письма или сообщения.

Подводя итог, мы пришли к выводу, что кибератаки – это постоянная угроза для корпораций, стартапов и для физических лиц, поэтому крайне важно уделять внимание защите от мошенничества. Однако пользователи также должны предпринять простые шаги, чтобы не стать жертвой злоумышленников.

Полностью искоренить фишинг сложно, поскольку мошенники постоянно придумывают новые уловки, а меры кибербезопасности с трудом справляются с ростом числа мошеннических действий. Следовательно, люди должны иметь базовые знания для защиты своих личных данных, так же стоит отметить, что в законодательстве отсутствует необходимая уголовно-правовая норма, которая предусматривает ответственность за фишинг, а последствия данной кибератаки квалифицируют по различным статьям Уголовного Кодекса Российской Федерации.

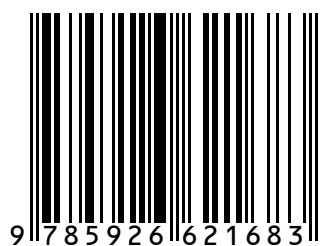
Научное издание

**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ
ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ**

Материалы
XIII Всероссийской научно-практической конференции
(17 октября 2024 г.)

В авторской редакции
Компьютерная верстка Г. А. Артемовой

ISBN 978-5-9266-2168-3



Подписано в печать 27.01.2025.
Авт. л. 10,3. Заказ 325.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.