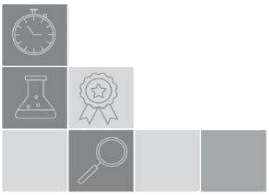
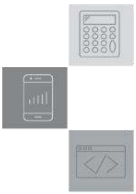
СТРАТЕГИЧЕСКИЕ АСПЕКТЫ СОТРУДНИЧЕСТВА ОРГАНОВ ВНУТРЕННИХ ДЕЛ (ПОЛИЦИИ) СТРАН СОДРУЖЕСТВА В ПРОТИВОДЕЙСТВИИ ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОСТИ В КОНТЕКСТЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА ПОД ЭГИДОЙ СОВЕТА МИНИСТРОВ ВНУТРЕННИХ ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Международная научно-практическая конференция
(1 октября 2021 г.)

Сборник тезисов выступлений





Москва
Московский университет
МВД России имени В.Я. Кикотя
2022

УДК 341.4
ББК 67.910.7
С83

Рецензенты:
заместитель начальника Санкт-Петербургского университета МВД России по научной работе доктор юридических наук, профессор **М. В. Бавсун**; начальник кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор **А. В. Еськов**

С83 **Стратегические аспекты сотрудничества органов внутренних дел (полиции) стран Содружества в противодействии транснациональной преступности в контексте развития информационного общества под эгидой Совета министров внутренних дел государств – участников Содружества Независимых Государств**: Международная научно-практическая конференция : сборник тезисов выступлений, 1 октября 2021 г. – М. : Московский университет МВД России имени В.Я. Кикотя, 2022. – 207 с.
ISBN 978-5-9694-1270-5

Сборник тезисов выступлений содержит статьи руководителей и сотрудников Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников СНГ, Научно-консультативного совета при Антитеррористическом центре государств – участников СНГ, руководства Московского университета МВД России имени В.Я. Кикотя, руководителей подразделений по борьбе с киберпреступностью МВД Республики Казахстан, Республики Молдовы, руководителей кафедр Академии МВД Республики Таджикистан, практических сотрудников МВД России, общественных организаций, а также научных сотрудников ВНИИ МВД России, научно-педагогического состава Московского университета МВД России имени В.Я. Кикотя и Крымского филиала Краснодарского университета МВД России и иных высших учебных заведений.

Материалы сборника можно рекомендовать научно-педагогическому составу, обучающимся образовательных организаций при подготовке учебных материалов по преподаваемым дисциплинам, научно-исследовательских и курсовых работ, сотрудникам практических подразделений МВД России для применения в служебной деятельности по выявлению, предупреждению, пресечению, профилактике, а также раскрытию и расследованию преступлений, которые совершаются с помощью современных информационных технологий.

УДК 341.4
ББК 67.910.7

ISBN 978-5-9694-1270-5

СОДЕРЖАНИЕ

Коновалов О. Ф.[1],
директор Бюро по координации борьбы
с организованной преступностью
и иными опасными видами преступлений
на территории государств – участников СНГ,
кандидат юридических наук

Уважаемые коллеги! Друзья!

Разрешите от имени Совета министров внутренних дел государств – участников Содружества Независимых Государств поприветствовать всех участников форума!

Сегодня можно утверждать, что конференции, проводимые под эгидой СМВД СНГ, стали востребованной дискуссионной площадкой для обмена опытом практических сотрудников правоохранительных органов и представителей академической науки, апробированным способом выработки обоснованных управленческих решений.

Хотел бы выразить слова благодарности за организацию и проведение форума руководству Министерства внутренних дел Российской Федерации, лично начальнику Московского университета МВД России имени В.Я. Кикотя генерал-лейтенанту полиции Калиниченко Игорю Александровичу, и сотрудникам вуза.

Тема сегодняшней конференции – «Стратегические аспекты сотрудничества органов внутренних дел (полиции) стран Содружества в противодействии транснациональной преступности в контексте развития информационного общества» – имеет особую актуальность не только в странах Содружества, но и во всем мире.

Сложный и многогранный характер комплекса проблем, которые планируется рассмотреть, не имеет простых, однозначных решений, и во многом выходит за рамки компетенции органов внутренних дел. Это обосновывает представительный характер

нашего форума, несмотря на его дистанционный формат, обусловленный пандемией. И здесь нельзя не подчеркнуть, что именно в условиях «ковидных» ограничений на первый план вышла необходимость налаживания новых форм сотрудничества, базирующихся на современных информационных технологиях.

Целью конференции, прежде всего, является поиск нетривиальных действенных решений и подготовка соответствующих предложений, направленных на совершенствование механизма согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию транснациональной преступности, эволюционирующей в среде глобальной цифровизации всех сфер жизни общества.

На повестке дня вопросы, требующие поиска и формулирования ответов на крайне актуальные вызовы современности, связанные с необходимостью выработки инновационных стратегических решений в организации взаимодействия правоохранительных органов с учетом взрывного развития информационно-телекоммуникационных технологий.

Не вызывает сомнения тот факт, что необходимо укреплять механизмы сотрудничества и в целях противодействия преступному использованию кибертехнологий, повысить практическую отдачу от международного правоохранительного взаимодействия, у которого, по нашему мнению, имеется высокий потенциал.

Полагаю, что обмен мнениями широкого круга участников предоставит возможность проанализировать и дать оценку выдвинутым идеям, что в свою очередь позволит обеспечить выработку предложений по эффективному взаимодействию на всех уровнях и при участии всех заинтересованных сторон.

Убежден, что конференция пройдет успешно, а ее выводы и рекомендации будут востребованы в практической деятельности.

Желаю Вам плодотворной работы и всего самого доброго!

Благодарю за внимание!

Калиниченко И. А.[1],
начальник Московского университета
МВД России имени В.Я. Кикотя,
кандидат педагогических наук

Уважаемые коллеги!

Сегодня в стенах Московского университета МВД России имени В.Я. Кикотя мы рады приветствовать участников Международной научно-практической конференции под эгидой Совета министров внутренних дел государств – участников СНГ «Стратегические аспекты сотрудничества органов внутренних дел (полиции) стран Содружества в противодействии транснациональной преступности в контексте развития информационного общества».

Организация международного форума, посвященного столь актуальной проблеме стала для нас доброй традицией. Реализация Межгосударственной программы совместных мер борьбы с преступностью на 2019–2023 годы, утвержденной Советом глав государств СНГ 28 сентября 2018 года, способствует объединению усилий и обеспечению эффективного взаимодействия для повышения качества жизни граждан, развития социально-политической, экономической, культурной и духовной сфер жизни общества, совершенствования системы государственного управления, обеспечения безопасности. Цель конференции – обсуждение актуальных проблем сотрудничества органов внутренних дел (полиции) стран Содружества в борьбе с транснациональной преступностью и путей их решения в контексте развития информационного общества.

В работе конференции принимают участие сотрудники органов внутренних дел (полиции), научных и образовательных организаций стран Содружества, а также представители Исполнительного комитета и органов отраслевого сотрудничества СНГ.

---

[1] © Калиниченко И. А., 2022.

Заявленная тематика требует комплексного обсуждения, и Университет будет всегда открыт для предоставления площадки в целях объединения специалистов различного уровня – ученых, педагогов, практиков.

Это продиктовано тем, что с развитием информационных технологий мировое интернет-сообщество столкнулось с массовой информационной угрозой со стороны экстремистских и террористических организаций. Университет с 2019 г. является базовой организацией государств – участников Содружества Независимых Государств по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий. В рамках сотрудничества Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств – участников Содружества Независимых Государств совместно с Московским университетом МВД России имени В.Я. Кикотя в 2019 году подготовлены и опубликованы сборники актуальных документов Совета министров внутренних дел, Совета глав государств и Совета глав правительств[1].

Позвольте представить главного организатора данного мероприятия – это Бюро по координации борьбы с организованной

[1] См.: Сотрудничество министерств внутренних дел государств – участников Содружества Независимых Государств : сборник актуальных документов Совета глав государств и Совета глав правительств. Т. I. Ч. I. (1993–2006 гг.). М. : Московский университет МВД России имени В.Я. Кикотя, 2019; Сотрудничество министерств внутренних дел государств – участников Содружества Независимых Государств : сборник актуальных документов Совета глав государств и Совета глав правительств. Т. I. Ч. II (2007–2018 гг.). М. : Московский университет МВД России имени В.Я. Кикотя, 2019; Сотрудничество министерств внутренних дел государств – участников Содружества Независимых государств : сборник актуальных документов Совета министров внутренних дел. Т. II. Ч. I (1992–2007 гг.). М. : Московский университет МВД России имени В.Я. Кикотя, 2019; Сотрудничество министерств внутренних дел государств – участников Содружества Независимых Государств : сборник актуальных документов Совета министров внутренних дел. Т. II. Ч. II (2008–2018 гг.). М. : Московский университет МВД России имени В.Я. Кикотя, 2019.

преступностью и иными опасными видами преступлений на территории государств – участников Содружества Независимых Государств.

Желаю всем участникам мероприятия успехов, а также интересной и результативной дискуссии. Надеюсь, что заявленные темы выступлений найдут отражение в резолюции, которая будет утверждена по итогам мероприятия.

Волков Р. А.[1],
начальник управления по координации борьбы
с организованной преступностью, терроризмом,
незаконным оборотом наркотических средств,
психотропных веществ и их прекурсоров
Бюро по координации борьбы с организованной преступностью
и иными опасными видами преступлений
на территории государств – участников СНГ

СОВРЕМЕННОЕ СОСТОЯНИЕ ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОСТИ НА ТЕРРИТОРИЯХ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Оценивая современное состояние транснациональной преступности на территориях государств – участников СНГ в условиях глобализации информационного пространства, невозможно не учитывать последствий мировой пандемии, вызванной новой коронавирусной инфекцией и повлиявшей без исключения на все сферы развития современного общества.

Ограничительные меры, направленные, прежде всего, на сдерживание межличностного общения, как фактора повышенного риска распространения заболевания, стали дополнительным условием стремительного развития цифровой коммуникации, как альтернативного способа взаимодействия.

К сожалению, не исключением стала и преступность. Министерствами внутренних дел (полицией) государств – участников СНГ отмечается существенный рост преступлений, совершенных с использованием информационно-коммуникационных технологий. Общее количество таких противоправных деяний за период 2020 г. по сравнению с периодом 2018 г. увеличилось более чем

в два раза и продолжает показывать отрицательную динамику роста в 2021 г.

При этом наибольшее количество преступлений (порядка 82 %), совершенных с применением ИКТ, составляют разного рода хищения (кража, мошенничество), далее в процентном соотношении следуют преступления, связанные со сбытом наркотических средств и психотропных веществ (около 8–9 %), условное третье место (порядка 6–7 %) занимают противоправные деяния, связанные с экстремистской деятельностью и вовлечением несовершеннолетних в различные деструктивные группы суицидальной направленности (синий кит), на другие виды преступлений, относимых к рассматриваемой категории, приходится до 4 %.

Исходя из обозначенной характеристики, видно, что наибольшую проблему для правоохранительных органов стран Содружества представляют именно имущественные преступления, связанные с хищением денежных средств с расчетных счетов граждан. Наиболее остро указанная проблема стоит для МВД Республик Беларусь (2018 г. – 3 585 таких преступлений, 2019 г. – 8 047, 2020 г. – 23 574), Казахстан (2018 г. – 4 510, 2019 г. – 8 033, 2020 г. – 14 919) и Российской Федерации (2018 г. – 142 359, 2019 г. – 239 943, 2020 г. – 375 895). При этом раскрываемость данной категории преступных деяний снизилась с 26,6 % – 2018 г., до 23 % – 2020 г.

Факторами, способствующими активному использованию возможностей сети Интернет и устройств беспроводного доступа к ней в преступных целях, являются трансграничность, многоуровневость, анонимность, дистанционность, скорость принимаемых решений и обмена данными, возможность использования криптовалюты и других электронных средств оплаты, отсутствие прямых контактов как между звеньями преступной цепи, так и конечным потребителем.

Указанные условия существенным образом осложняют работу правоохранительных органов по пресечению противоправной деятельности. Меры конспирации, повышенная корыстная мотивация, продуманная система сокрытия следов преступлений, высокая техническая оснащенность, использование высококлассных специалистов в IT-сфере, а также понимание сложности проведения оперативно-разыскных и следственных мероприятий на территории иностранного государства позволяют преступникам организовывать транснациональные схемы совершения преступлений, с применением ИКТ с минимальным для себя риском.

Безусловно, существующая модель совершения преступлений с использованием сферы высоких технологий при их раскрытии (расследовании) требует консолидированного усилия правоохранительных и государственных органов различных стран.

В целях усиления принимаемых мер, направленных на противодействие международной преступности с использованием киберсферы, по инициативе Бюро 20 июля 2018 г. на заседании Совета министров внутренних дел государств – участников Содружества Независимых Государств принят Регламент согласованных действий органов внутренних дел (полиции) государств – участников СНГ по противодействию новым видам преступлений, совершаемых на территории стран Содружества в сфере современных информационных технологий. Регламент определяет порядок взаимодействия, основные задачи, направления, формы, методы и организационные основы механизма согласованных действий, осуществляемых органами внутренних дел (полиции) государств – участников СНГ в пределах полномочий, предоставленных им национальным законодательством по противодействию новым видам преступлений, совершаемых на территории стран Содружества в IT-сфере, а также закрепляет за БКБОП функции координирующего органа в пределах своих полномочий.

Осознавая дальнейшую перспективу развития информационно-телекоммуникационного пространства во всех сферах жизнедеятельности человека, Бюро совместно с заинтересованными органами стран Содружества инициировало разработку Концепции развития информационного взаимодействия между компетентными органами государств – участников Содружества Независимых Государств, органами СНГ в сфере безопасности и правопорядка в вопросах борьбы с преступностью, как возможного практического механизма эффективного взаимодействия на современном этапе технического развития. В настоящее время проект указанного документа проходит процедуру внутригосударственных согласований и внесения предложений государствами – участниками Содружества.

Отдельного внимания заслуживает предложение Республики Узбекистан, выраженное в проекте Концепции по созданию Единой электронной платформы Содружества Независимых Государств для обмена информацией, направленном 22 апреля 2021 г. в Исполнительный комитет СНГ для дальнейшего согласования.

Многие имеющиеся механизмы межгосударственного взаимодействия, к сожалению, не соответствуют духу современного развития общественных отношений, направленных на глобализацию и информатизацию различных процессов, в том числе обмена информацией.

В этой связи, 27 июля 2021 г. Россия внесла в Спецкомитет ООН по разработке всеобъемлющей конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях российский проект первого в истории универсального договора по борьбе с киберпреступностью с соответствующим наименованием: (Конвенция Организации Объединенных наций о противодействии использованию информационно-коммуникационных технологий в преступных целях).

Вместе с тем, осознавая значимость международного сотрудничества, МВД (полиция) государств – участников СНГ стремятся к консолидации совместных усилий в противодействии трансграничной преступности. Имеется положительный опыт межгосударственного взаимодействия подразделений уголовного розыска, противодействия незаконному обороту наркотиков, экстремизму в вопросах борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий, который необходимо развивать по следующим направлениям:

– создание и динамическое совершенствование межгосударственной нормативно-правовой базы, регламентирующей сферу борьбы с преступлениями в IT-сфере, блокчейн-технологий и оборота криптовалюты;

– формирование и непрерывное развитие высококвалифицированного научно-педагогического потенциала правоохранительных органов в данной сфере;

– создание, внедрение и постоянное совершенствование практических методик обучения сотрудников полиции раскрытию преступлений в сфере информационных технологий, в том числе с применением блокчейна при совершении незаконных сделок в криптовалюте, а также процессуальных алгоритмов документирования указанной противоправной деятельности;

– обмен наиболее эффективным международным опытом.

Переходя к вопросам криминальных рисков и трансформации преступности на территории государств – участников СНГ, безусловно следует учитывать специфику киберпространства, окружающего современного человека, а также имеющийся опыт противодействия преступлениям в IT-сфере, в связи с чем комплекс мер, направленных на противодействие данной проблеме, должен учитывать:

– создание и развитие практических международно-правовых механизмов, направленных на противодействие угрозе использования IT-технологий в преступных целях, в том числе путем своевременного обмена правоохранительными органами стран Содружества соответствующей информацией в электронном виде по защищенным каналам связи;

– создание, развитие и модернизацию механизмов непосредственного сотрудничества в рамках совместных международных следственно-оперативных групп по конкретным уголовным делам, связанным с трансграничным совершением преступлений с использованием ИКТ;

– мониторинг и своевременный четко отработанный механизм блокировки интернет-ресурсов, распространяющих противоправный контент или осуществляющих противоправную деятельность;

– создание и развитие системы базовых научных организаций для служб по противодействию хищениям имущества граждан, НОН, экстремистским действиям с целью подготовки высококвалифицированных кадров в IT сфере с учетом имеющегося передового опыта расследования преступлений рассматриваемой категории.

В заключение мне бы еще раз хотелось высказать слова благодарности организаторам настоящей конференции за возможность обсуждения инициатив по актуальным проблемам состояния транснациональной преступности на территориях государств – участников СНГ в условиях глобализации информационного пространства, а также выразить надежду, что данная площадка станет стартапом научно-практического потенциала, способного оказать существенное влияние на формирование и развитие механизмов межгосударственного взаимодействия и обмена информацией, которые позволят противостоять криминальному использованию современного киберпространства.

Благодарю за внимание!

Алексеева М. М.[1]**,**
доцент кафедры прав человека и международного права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ СОТРУДНИЧЕСТВА ГОСУДАРСТВ – ЧЛЕНОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРТЕРРОРИЗМУ

На протяжении уже нескольких десятков лет терроризм представляет всевозрастающую опасность для безопасности государств и международного сообщества в целом. Характерна эта угроза и для безопасности отдельных регионов, в том числе и для Содружества Независимых Государств.

Разработанный в 1999 г. Договор о сотрудничестве государств – участников СНГ в борьбе с терроризмом [1] положил начало региональному антитеррористическому взаимодействию государств и определил основные задачи, направления и порядок антитеррористического взаимодействия государств – членов Содружества. Позже были приняты договоры, регламентирующие отдельные аспекты противодействия террористической угрозе: Договор о противодействии легализации (отмыванию) преступных доходов и финансированию терроризма 2007 г. [2], Договор о межгосударственном розыске лиц 2010 г. [3]. Отметим, что в указанные соглашения имплементированы основные принципы и нормы антитеррористического сотрудничества, содержащиеся в универсальных антитеррористических конвенциях, принятых в рамках Организации Объединенных Наций [4; с. 26–33].

Кроме того, по итогам Стамбульского саммита ОБСЕ была разработана Целевая программа борьбы с терроризмом и экстремизмом 2000 г., которая в целях координации сотрудничества компетентных органов государств – участников Содружества предусмотрела создание Антитеррористического центра СНГ. В 2003 г. было утверждено Положение об Антитеррористическом центре Содружества, в котором определены основные задачи и функции Центра, а также его состав и организационные основы деятельности. Таким образом, разработка правовой основы сотрудничества и создание институционального механизма взаимодействия способствовали повышению эффективности противодействия терроризму как общеуголовному транснациональному преступлению.

Однако стремительное развития научно-технического прогресса, информационных и компьютерных технологий предопределили и развитие нового типа террористической угрозы – кибертерроризма. Сеть Интернет стала таким же орудием терроризма, как в свое время химическое и бактериологическое оружие, в связи с чем назрела необходимость выработки специальных мер противодействия такого вида угрозе.

В праве Содружества Независимых Государств нет специальных договоров, посвященных противодействию кибертерроризму. Правовые меры борьбы предусмотрены, как правило, национальными уголовными законами. В случае, когда последствия кибертерроризма выходят за рамки национальных границ, сотрудничество правоохранительных органов строится по отработанным схемам противодействия общеуголовным преступлениям [5; с. 56–57].

В ранее уже упомянутом Договоре о сотрудничестве государств – участников СНГ в борьбе с терроризмом 1999 г. в ст. 1 в качестве одного из противоправных деяний, образующих состав преступления терроризм, указан и «технологический терроризм», таким образом, данный договор можно распространить и

на противодействие кибертерроризму. В настоящее время совершенно очевидно, что существуют огромные риски использования виртуального пространства в качестве кибероружия и негативные последствия такой деятельности могут представлять большую общественную опасность интересам как непосредственно государств так и всего Содружества в целом и в несколько раз превышать ущерб, наносимый в результате проведения непосредственных террористических атак. Несанкционированное вмешательство в функционирование систем управления потенциально опасными объектами инфраструктуры может спровоцировать техногенные катастрофы с большим числом человеческих жертв, а также глобальным экологическим, экономическим, социальным ущербом.

Но для того, чтобы противодействие кибертерророизму было эффективным, необходимо определиться с единым пониманием данной угрозы и гармонизировать законодательство государств – членов, прежде всего, в области информационной безопасности. На настоящий период времени можно выделить два состава, образующие данный вид преступления – совершение террористических действий с помощью компьютеров (и иных технических средств) и информационно-телекоммуникационных технологий; и второй – использование киберпространства в преступных целях организованных террористических групп и сообществ. При этом, как в первом, так и во втором случае целью преступных действий являются нарушение национальной и международной безопасности, устрашение населения и провокация вооруженных конфликтов.

Достаточно серьезную опасность представляет и такой тип кибертерроризма как распространение информации террористического толка. Осознавая необходимость защиты регионального сегмента киберпространства, государства Содружества заключили Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [6], в том числе в целях предотвра-

щения возможности использования информационно-коммуникационных технологий для нарушения целостности инфраструктуры государств. В указанном договоре были определены и в настоящее время реализуются основные направления взаимодействия компетентных органов государств – членов: гармонизация законодательства государств Содружества, регламентирующих отношения в сфере обеспечения информационной безопасности; прогрессивное развитие нормативно-правового регулирования проведения совместных скоординированных мероприятий в информационном пространстве; организация трансграничной передачи информации; проведение мероприятий, направленных на недопущение несанкционированного доступа к информации, размещенной в телекоммуникациях и ее утечки по техническим каналам.

В целях гармонизации национального законодательства государств – членов Содружества Межпарламентской Ассамблеей государств – участников СНГ принят Модельный закон об информации, информатизации и обеспечении информационной безопасности 2005 г. [7], который закрепляет основные понятия, принципы правового регулирования информационных отношений, основы правового положения информации, ограничения на доступ к информации и на распространение информации, а также меры по защите информации. В настоящее время анализ реализации в национальном законодательстве Модельного закона СНГ показывает, что национальное законодательство государств – участников СНГ в целом соответствует Модельному закону.

Задача защиты информационного пространства от угроз кибертерроризма во многом тождественна задачам обеспечения национальной безопасности и является одним из приоритетных направлений деятельности государств и компетентных органов Содружества, и только организация тесного взаимодействия позволит эффективно противостоять новым угрозам и вызовам. В настоящее время противодействие кибертерроризму будет вклю-

чать также обеспечение информационной безопасности, противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий, техническую защиту объектов информационной инфраструктуры. С учетом участившихся случаев мошенничества путем незаконного сбора и использования персональных данных необходима также защита прав и свобод человека в информационной среде.

Необходимо продолжать выработку правовых, управленческих и технических решений, направленных на противодействие высокотехнологичному терроризму, а также приступить к проведению совместных командно-штабных учений оборонных и правоохранительных ведомств государств – членов Содружества по отражению атак на объекты инфраструктуры.

Список литературы

1. Договор о сотрудничестве государств – участников СНГ в борьбе с терроризмом (Минск, 4 июня 1999 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/12130305/.

2. Договор о противодействии легализации (отмыванию) преступных доходов и финансированию терроризма (Душанбе, 5 октября 2007 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/2566684/.

3. Договор государств – участников СНГ о международном розыске лиц (Москва, 10 декабря 2010 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/2570891/.

4. Алексеева М. М. Сотрудничество государств в борьбе с терроризмом: сопоставление глобальных и региональных инструментов. М. : Граница, 2019. С. 26–33.

5. Шинкарецкая Г. Ш. Сотрудничество государств СНГ в борьбе с киберугрозами // Международное сотрудничество евразийских государств: политика, экономика и право. 2020. № 1. С. 56–57.

6. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности в (Санкт-Петербург, 20 ноября 2013 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/70604710/.

7. Модельный закон об информации, информатизации и обеспечении информационной безопасности (18 ноября 2005 г.) // URL: https://docs.cntd.ru/document/901972159.

Арипов А. Л.[1],
начальник кафедры уголовного процесса
Академии МВД Республики Таджикистан,
кандидат юридических наук

СОТРУДНИЧЕСТВО ОРГАНОВ ВНУТРЕННИХ ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ В КОНТЕКСТЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

На современном этапе развитие информационных технологий достигло такого уровня, что решение большинства задач, которые видятся вполне обыденными, в недавнем прошлом требовало больших усилий в плане привлечения средств и времени. Прогресс в точных науках, разработка и производство в промышленных масштабах высокотехнологичных и в то же время компактных устройств позволяют решать задачи, которые до этого требовало не только лабораторных условий и дорогостоящей техники, но и специальных знаний.

В значительной степени подверглась большим изменениям отрасль связи, телекоммуникационные и информационные технологии, чему способствовали новейшие достижения в электронной технике и радиоэлектронике. Внедрение этих достижений в промышленное производство позволили получить доступ к большим объемам информации, ее обработки (обмену, отправке и загрузке в хранилища новых данных), которые все более и более совершенствуются. Данные технологии вкупе с возможностью легкого высокоскоростного доступа в интернете делают общение и передачу достаточно объемных данных в течение нескольких минут обычным делом.

Чуть больше чем за два десятилетия стремительное развитие Интернета и информационно-коммуникационных технологий обеспечили условия для экономического роста и широкого доступа к важным услугам, создав наряду с этим новые возможности для преступной деятельности.

В настоящее время злоумышленники все больше пользуются новыми технологиями, поскольку эти достижения позволяют им совершать преступления и извлекать из них выгоду. Наблюдается совершение незаконной деятельности на цифровых платформах таким образом, чтобы снизить риски, в частности, риск обнаружения.

С другой стороны, возникающие и существующие технологии открывают новые возможности для правоохранительных органов в раскрытии и расследовании преступлений. Возможности правоохранительных органов, в частности, органов внутренних дел в раскрытии и расследовании преступлений на основе потенциала информационных технологий и развития информационного пространства могут оказать позитивное воздействие на достижение целей, а также отдельных пунктов, указанных в Межгосударственной программе совместных мер борьбы с преступностью на 2019–2023 годы, утвержденной Решением Совета глав Содружества Независимых государств 28 сентября 2018 г. в г. Душанбе [1].

Не смотря на то, что использование современных технических средств в определенной степени может облегчить реализацию преступного умысла, в то же время их использование не остается бесследным и это обстоятельство представляет интерес в деле раскрытия и расследования преступлений. Однако, такое понятие как следы преступления, традиционно широко используемое в криминалистической и процессуальной литературе, в своем содержании не в полной мере охватывает тех «следов», которые остаются при совершении преступлений с использованием современных технических средств и в особенности информационных технологий с использованием международной сети Интернет. Практически все действия в «цифровом пространстве» не

пропадают, бесследно, начиная от подключения к сети, создания каких-либо документов, файлов их изменение или редактирование. Все эти действия и операции с электронными файлами сохраняются и с помощью специальных инструментов – программного обеспечения могут быть выявлены и получены для использования в интересах раскрытия и расследования преступлений. В отличие от традиционных «следов», которые по объективным и субъективным факторам могут быть искажены или утеряны, следы в цифровом пространстве зачастую сохраняются без каких-либо потерь и искажений и их можно получить в том виде, в каком они были созданы или же проследить те изменения, которые были внесены. Хоть и в непосредственном виде эти изменения и другие данные не видны, однако их анализ посредством использования специальных программ помогает их выявить. Данное обстоятельство касается действий, осуществляемых в сети Интернет, посещенных сайтов, просмотренного материала или использованных услуг.

Все большее распространение сети Интернет и его использование в предоставлении различного рода услуг населению обуславливает его повсеместное использование. Предоставление финансовых услуг в этом плане не является исключением и здесь вполне справедливо ожидание совершения противоправных действий с целью завладения платежными средствами не только граждан, но и различных организаций и предприятий.

Наибольшее использование населением сети Интернет и его возможностей можно было наблюдать в период действовавших ограничений в связи с эпидемической обстановкой, вызванной распространением инфекционного заболевания COVID-19 в начале 2020 г. [2]. В этот период большинство государственных и частных предприятий и учреждений были вынуждены перейти на дистанционный режим работы, и вся деятельность, которая была возможна, осуществлялась с помощью различных программ

и сервисов. В их числе интернет-торговля, проведение дистанционных занятий, встреч и конференций, размещение заказов на доставку различных товаров. С одной стороны, введенные ограничения, связанные с перемещением, положительно повлияли на сокращение количества совершения определенных преступлений, к примеру, в Республике Таджикистан наблюдалось снижение количества краж. Однако в других странах наблюдалось резкое увеличение количества преступлений в сфере информационных технологий, что вполне ожидаемо. Более того, учитывая дальнейшее развитие данной отрасли, в будущем можно ожидать только увеличение совершения подобного рода преступлений. Эти тенденции обуславливают принятие мер для успешного противодействия подобного рода преступлениям.

Для принятия эффективных мер в первую очередь видится необходимым принятие нормативно-правовых основ для осуществления оперативного сотрудничества между правоохранительными органами. В особенности между органами внутренних дел стран СНГ, что позволило бы оперативно обмениваться информацией, касающейся новых методов совершения преступлений с использованием информационных технологий (в том числе способы сокрытия, используемые уязвимости в сервисах и программах и т. п.), а также осуществлять правовую помощь по уголовным делам. Действующие Международные нормативные акты по оказанию правовой помощи по уголовным делам приняты и действуют, сотрудничество по ним осуществляется достаточно успешно [3]. Однако на момент их принятия реалии действительности не предполагали таких угроз преступности, которые существуют в современных условиях.

Необходимость получить данные из источников (серверов, хранилищ, а также облачных сервисов), физическое местоположение которых находится в другом государстве, диктуют необходимость направления международных запросов, срок исполнения которых достаточно значителен, а по прошествии времени,

необходимого для составления и направления запроса в том порядке, который предусмотрен в действующих нормах, есть возможность уничтожения данных или приведения их в негодность.

Следующим немаловажным шагом в этом направлении видится осуществление подготовки кадров, специализирующихся на выявлении, раскрытии и расследовании преступлений, совершенных с использованием информационных технологий. Данная отрасль признается достаточно объемной и наукоемкой, что требует наличия определенных знаний, в большей части касающихся точных и прикладных наук – математики, различных направлений программирования и т. п. Без достаточных знаний выявление и раскрытие преступлений в этой сфере будет сложным. В этом направлении эффективно будет использование потенциала ведущих высших учебный заведений, осуществляющих подготовку специалистов в интересующей области, а также использование опыта, зарекомендовавших себя компаний – в том числе и частных, занимающихся вопросами безопасности в сфере информационных технологий и защиты данных. На базе данных компаний, используя их опыт и накопленные знания, можно будет осуществлять подготовку или проводить курсы для сотрудников органов внутренних дел.

Список литературы

1. Решение Совета глав государств СНГ от 28 сентября 2018 г. «О Межгосударственной программе совместных мер борьбы с преступностью на 2019–2023 годы (принято в г. Душанбе) // URL: http://cis.minsk.by/reestr/ru/index.html#reestr/-view/text?doc=5863.

2. Указ Президента Российской Федерации от 25 марта 2020 г. № 206 «Об объявлении в Российской Федерации нерабочих дней» // URL: http://kremlin.ru/events/president/news/63065.

3. Указ Президента Республики Таджикистан от 5 июня 2020 г. № 1544 «О предотвращении воздействия инфекционного

заболевания COVID-19 на социально-экономические сферы Республики Таджикистан» // URL: http://president.tj/ru/node/23055.

4. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (заключена в г. Минске 22.01.1993) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5942/.

5. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (, заключена в г. Кишиневе 07.10.2002) // URL: https://cis.minsk.by/page/614.

Богданов А. В.[1],
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Ильинский И. И.[2],
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Хазов Е. Н.[3],
главный научный сотрудник
научно-исследовательского института ФСИН России,
кандидат юридических наук, профессор

ЦИФРОВЫЕ, КОММУНИКАЦИОННЫЕ И КИБЕРТЕХНОЛОГИИ КАК ОДНО ИЗ СРЕДСТВ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ

Мир изменился с появлением информационных технологий, которые существенно облегчили жизнь человека, но и вместе с тем создали множество проблем. В настоящее время общество существует и развивается вместе с процессами динамичной информатизации многих направлений своей деятельности. Владимир Путин, выступая 3 марта 2021 г. на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации, сказал, что «Ваша задача – эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от

мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. И конечно, нужно наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи» [1].

В развитых странах и городах граждане уже не могут представить свою жизнь без регулярного использования технологий. В связи с отмеченными процессами цифровизации открылись новые привлекательные возможности: экономия времени и ресурсов, общение и работа на расстоянии. Но также с эрой информатизации общества добавилось множество новых проблем, неочевидных угроз безопасности и информационная безопасность в России – это главная задача государства. В век информационно-телекоммуникационных технологий злоумышленники все чаще совершают преступления дистанционным способом [2].

Киберпреступность по праву можно назвать серьезной проблемой XXI века. Таковыми являются, например, кража информации с различных носителей, скачивание вредоносного программного обеспечения, совершаемое с помощью информационно-коммуникационных технологий, финансовое мошенничество, преступления экстремисткой и террористической направленности, саботаж, хакерские атаки (DoS и DDOS-атаки, MITB-атаки, BEC-атаки и др.) [3]. Помимо неочевидных угроз информационной безопасности некоторые проблемы легко обнаружить, но при этом также затруднительно устранять их последствия. С каждым годом такие действия хакеров становятся все более усовершенствованы, приносящими вред личности, обществу и государству [4].

Такой проблемой, например, является деструктивный контент в масс-медиа и сети Интернет.

Таким образом, классификацию основных видов киберпреступлений можно привести следующим образом:

– преступления против конфиденциальности, целостности, доступности компьютерной информации;

– кибер-мошенничество;

– завлечение детей в противоправную сферу или «груминг».

Тема киберпреступлений в настоящее время является актуальной. По данным МВД, за 2020 г. число преступлений, совершенных с применением IT-технологий, выросло на 94,6 %, также тяжкие и особо тяжкие преступления с применением информационно-коммуникационных средств резко выросли на 129,7 % [5, с. 56–63]. Число киберпреступлений в России за пять лет выросло в 11 раз. В связи с быстрым развитием киберпреступлений и их разнообразием правоохранительным органам необходимо создать оперативную и слаженную структуру борьбы с преступлениями. Каждый вид таких преступлений сложно раскрыть из-за множества различных проблем [6].

Так, преступления против конфиденциальности, целостности и доступности обычно совершаются с помощью создания и распространения вредоносных программ, Dos и DDos атак (атака, которая осуществляется с помощью сетевых ресурсов, а именно ограниченной пропускной способностью данных ресурсов, отправляя огромное количество запросов, которых веб-ресурс не может обработать, и, соответственно, происходит отказ в обслуживании), порчи веб-сайтов. Не вызывает сомнений тот факт, что преступления, совершаемые с использованием современных информационно-телекоммуникационных систем, имеют существенную специфику [7].

Нарушение конфиденциальности является большой проблемой для многих компаний, которые работают с конфиденциальными данными своих клиентов. Хакерские атаки преступники часто направляют в такие учреждения, как клиники пластической хирургии, компании, оказывающие психологическую помощь и ряд других компаний. После получения данных клиентов, например, о том, когда они осуществляли определенную пластическую операцию, преступники связываются с данными лицами и шантажируют их. Нарушение целостности также является огромной

проблемой для множества компаний, работающих с документами или базами данных, да и нарушение доступности вызовет определенные трудности для компаний, которыми преступники ловко пользуются, выманивая из компаний денежные средства [8].

Кибермошенничество является огромной проблемой, ведь кибер-мошенничество увеличилось во много раз и приобрело массовый характер. Каждый второй житель России связывался с мошенниками, которые осуществляют свою деятельность с помощью телефонов, интернет-ресурсов, подделки сайтов банков и т. д. Проблема обнаружения действий хакеров и их возможности совершать преступления в киберпространстве, не имеющем государственной грани, многократно увеличивает степень общественной опасности [9].

В связи со стремительным развитием краж и мошенничества в этой области вступил в силу Федеральный закон от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». Этим законом в новой редакции изложены некоторые положения уголовного закона, устанавливающие ответственность за кражу и специальные виды мошенничества. Представляется, что с учетом понятия электронных средств платежа и разъяснений о разграничении мошенничества и кражи в отношении безналичных денежных средств, содержащихся в Постановлении Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48, на практике при применении новой редакции ст.ст. 158, 159.3 и ст. 159.6 УК РФ возникнут немалые трудности [10].

Так, составление распоряжения о перечислении денежных средств с карты потерпевшего на карту виновного через онлайн-банк, пароль от которого был получен путем обмана или злоупотребления доверием, подпадает и под признаки ст. 159.3 УК РФ в части использования электронных средств платежа, и под признаки ст. 159.6, поскольку предполагает ввод компьютерной ин-

формации, а с точки зрения Пленума Верховного Суда Российской Федерации, должно быть квалифицировано как кража. Изучение судебной и следственной практики показывает, что основная часть таких ошибок приходится на ошибки при определении объективных признаков состава преступления. Отметим, что не все представители правоприменительных органов правильно понимают причины введения анализируемого вида кражи в ч. 2 ст. 158 УК РФ. Также судьи не всегда верно оценивают обстановку совершения данного преступления [11].

Способов кражи электронных денег довольно много. Самый распространенный способ – кража с помощью сети Интернет. Это делается с помощью заражения вирусом-трояном (вирус заражает обычные компьютерные файлы и изменяет их) операционной системы компьютера или смартфона, который перенаправляет пользователя на поддельную веб-страницу, которая является точной копией банковского сайта. Потерпевший, не подозревая о том, что данная страница является поддельной, вводит свои данные (логин, пароль), которые получают злоумышленники и, соответственно, они вводят эти данные на настоящей веб-странице того или иного банка и переводят денежные средства на свой счет. Также часто злоумышленники узнают данные о карточке, создав фальшивые электронные сайты интернет-магазинов известных брендов [12].

Немаловажной проблемой в настоящее время является вовлечение детей в деструктивный контент и деструктивные сообщества. В 1994 г. впервые появляется сайт с доменом «.ru». После чего отечественный интернет стал стремительно развиваться [13].

К настоящему моменту статистика активности пользователей в сети Интернет по отчету Digital 2020 составляет:

– число пользователей глобальной сети увеличилось до 4,54 млрд, это на 7 % выше значения, полученного годом ранее (+ 298 млн новых пользователей в сравнении с данными на январь 2019 г.);

– в первом месяце 2020 г. количество аккаунтов социальных сетей составило 3,80 млрд, аудитория выросла на 9 % в сравнении с предыдущим периодом (321 млн человек за год);

– сегодня более 5,19 млрд пользователей прибегают к услугам мобильной телекоммуникации – прирост числа абонентов сотовой связи на 124 млн (2,4 %) за последний год.

В ушедшем году, согласно статистике, предоставленной агентством We Are Social и сервисом Hootsuite, самыми популярными платформами социальных сетей и сервисов были: Facebook, YouTube, WhatsApp, Instagram, Twitter, Skype, Snapchat, Viber, TikTok. В России пользователи отдают свое предпочтение использованию преимущественно YouTube и «ВКонтакте», а из мессенджеров самыми популярными у россиян являются WhatsApp и Viber.

В наиболее популярном видеохостинге YouTube можно встретить множество разнообразного информационного материала, удовлетворяющего огромное количество разнообразных интересов пользователей. Вместе с тем, на данной интернет-площадке присутствуют материалы, содержащие насилие, жестокие драки в различных ситуациях: драки в военных частях, драки между представителями различных национальностей, избиение мужем жены. Также на данной информационной платформе можно увидеть различного рода стримы. Часто стримы содержат виды насилия: издевательство над собственным телом, над родственниками, избиение, даже убийства. Также стримы содержат в себе огромное количество деструктивной лексики, оскорблений. YouTube активно борется с деструктивным контентом, блокируя видео, содержащие насилие, порнографические сцены и другие виды деструктивного контента. Но, несмотря на это, алгоритм блокирования таких видео работает недостаточно эффективно [14].

Наиболее популярная социальная сеть рунета «ВКонтакте» изначально была представлена как социальная сеть для студентов

и выпускников российских вузов. Сегодня данная платформа предоставляет пользователям ресурсы и средства для общения с помощью создания профилей, обмена различными материалами, также можно использовать как блог, площадку для рекламы. «ВКонтакте» заполнена различными группами, которые продвигают деструктивный контент любой направленности.

Распространение деструктивного контента в мессенджерах, как правило, происходит с помощью пересылок сообщений негативного содержания и ментально разрушающей направленности. Например, в мессенджере WhatsApp несколько лет назад массово пересылалось сообщение, преследующее цель разжигания межнациональных конфликтов, основанных на травле [15].

Таким образом, указанные сервисы и веб-платформы представляют очевидную опасность для психического и ментального состояния пользователя. Об этом уже давно высказывается научное сообщество в области IT-решений и информационной безопасности, многие государственные деятели, эксперты и ученые. Так, на форуме «Цифровая гигиена» Наталья Касперская затронула проблему деструктивного контента в сети Интернет, где отметила, что резкий рост деструктивного контента произошел в 2017 г. В 2018 г., по словам Натальи Касперской, деструктивный контент возрос в несколько раз и дополнился движениями сатанического и террористического характера, кроме этого появился культ обесценивания чужой и собственной жизни [16].

Стоит отметить, что в 2021 г. данная проблема только усугубилась, к ней также добавились разного рода политические лозунги, идеи выступлений на митингах. В настоящее время в социальных сетях бесконтрольно распространяется контент различного характера и степени влияния. Пользователи могут найти множество полезной информации: сведений о науке и искусстве, об образовании, саморазвитии и не только. Однако часто пользователи сталкиваются именно с деструктивным контентом, что

вызывает тревогу у представителей власти. Информация подобного содержания зачастую выражается не в форме оскорбления или травли определенного лица, а в форме попыток разжигания межнациональных конфликтов, расовой розни, призывов к митингам, в виртуальной среде реализуются попытки свергнуть власть, призывы к экстремизму, сепаратизму и терроризму [17].

Следует также отметить, что целевой аудиторией, адресатами деструктивного контента в сети Интернет чаще всего выступают подростки. На это есть несколько причин.

Сознание подростка не сформировано полностью, в связи с этим на молодежь проще психологически воздействовать, навязать определенную политическую, религиозную идею.

Основная часть пользователей в социальных сетях – лица подросткового возраста.

Использование злоумышленниками IT-телефонии, программного обеспечения, позволяющего избежать или существенно затруднить идентификацию абонента – VPN, TOP, SSL, и технологий, позволяющих создавать динамические или нераспознаваемые IP-адреса.

Деструктивный контент в сети Интернет – это мировая проблема. Так, Италия частично заблокировала платформу TikTok из-за гибели 10-летней девочки, которая пыталась повторить тренд из вышеупомянутой видеоплатформы [18]. В Германии Google и Facebook должны удалять информацию, содержащую в себе разжигание межнациональной розни, клевету и любой контент, признанный незаконным в стране. В случае, если компании откажутся исполнять закон, власти имеют право наложить на них штраф в размере 50 млн евро.

Сеть Интернет и социальные сети, в частности, являются огромным потенциалом для распространения деструктивного контента. Пользователю рекомендуют посмотреть определенную информацию, предлагают вступить в группы и т. д. Кроме того,

производится приоритетность определенного материала над другим. Таким образом, информация в социальной сети становится однотипной и усеченной, направлена на одну или несколько деструктивных тем.

Яркий пример – вызовы на митинг за освобождение Алексея Навального в январе 2021 г. За неделю до проведения незаконного митинга на сайте «ВКонтакте» циркулировали новости о «Дворце Путина». В социальной сети Instagram многие популярные личности (певцы, блогеры, общественные деятели) также призывали граждан выходить на митинги. Кроме того, в данной социальной сети вся новостная лента была забита темой митинга за свободу Алексея Навального. По данному поводу консультант ПИР-центра IT-эксперт Олег Демидов говорит следующее: «Есть неизбежный риск фрагментации и поляризации онлайн-сообществ. Усеченная картина мира. Формируются сообщества с похожим набором шаблонов, с похожей выборкой тем и источников информации» [19].

Проблема проявлений деструктивного контента в сети Интернет стала значительной угрозой для общества Российской Федерации. Не стоит забывать и о том, что социальные сети используются деятелями других стран как эффективный инструмент дестабилизации внутриполитической и социальной целостности. В Указе Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [20] к основным угрозам национальной безопасности государства отнесена деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе». В третьем квартале прошлого года Общественная Палата Российской Федерации предложила внести поправки в Федеральный закон от 29 де-

кабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющий вред их здоровью и развитию» [21] к запрещенной информации шантаж, угрозы, клевету для борьбы с кибербулингом.

Таким образом, популярность социальных сетей, масштабная активность пользователей в них в настоящее время являются одним из самых распространенных инструментов ментального воздействия на подсознание населения. В связи с этим с 1 февраля 2021 г. вступают в силу новые положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 02.07.2021). Данные положения назвали «Закон о саморегулировании социальных сетей» [22]. Новые положения обяжут владельцев интернет-площадок принимать меры по устранению на таких площадках информации, которая нарушает законодательство Российской Федерации. Рассмотрев основные способы совершения преступлений с помощью информационно-телекоммуникационных систем, напрашиваются следующие выводы.

Для правоохранительных органов в данных ситуациях появляются следующие проблемы.

Многие потерпевшие не обращаются в полицию, боясь, что информация шантажа распространится, или потому, что не верят в возможности пресечения таких преступлений сотрудниками правоохранительных органов.

Данные преступления, в особенности Dos, DDOS, атаки не оставляют «следов» преступления. Найти лицо, которое совершило данную атаку или другую хакерскую атаку, а также доказать умысел данного лица становится почти непосильной задачей для правоохранительных органов. Часто преступления совершаются с помощью даркнета [23], скрытая сеть имеет свою систему, которая позволяет преступникам заметать следы. Например, если пользователь сидит через даркнет, то сложность найти его сетевой IP-адрес заключается в лукавой системе даркнета. Дело в том, что даркнет использует собственную систему и для того, чтобы

найти местонахождение лица, нужно пройти через множество стадий. Так, человек, который посылал запрос из Москвы, сидит по IP-адресу в Нью-Йорке или в Париже, Лондоне и т. д., а чтобы раскрыть цепочку и найти конечный и реальный IP-адрес, правоохранительным органам придется отправлять множество запросов в разные страны, что делает поиск местонахождения преступника практически невозможным, да и с выдачей запросов будут проблемы с рядом стран.

Проблемы в уголовном законодательстве. Во многих странах, например, в Китае установлена уголовная ответственность за кражу Wi-Fi, взлом социальной сети, прочих преступлений, совершенных с помощью информационно-телекоммуникационных технологий.

Российское законодательство пока не пришло к разграничению киберпреступлений на конкретные преступления по видам их совершения, что довольно часто является проблемой для следователей при квалификации деяния в соответствии со статьей Уголовного кодекса Российской Федерации (вспомним проблему разграничения мошенничества электронных денежных средств и кражи электронных денежных средств). Для совершенствования мер и методов борьбы с киберпреступлениями следует проводить массовые агитационные работы, в которых гражданам будет пояснено, каким образом их могут обмануть, каким образом нужно себя вести, куда обращаться и как, по возможности, избежать киберпреступления. Кроме этого, для совершенствования мер борьбы с вовлечением в незаконные сообщества подростков следует проводить профилактические беседы в школах сотрудниками полиции, учителями, а также наладить грамотную и доверчивую атмосферу подростков при работе со школьным психологом.

Также следует наладить способы доказательств данных преступлений. Для этого следует включить новые оперативно-разыскные мероприятия, которые позволят наладить оперативное доказательство «по горячим следам», запретить использование даркнета

и отслеживать пользователей, которые его используют, применяя к ним санкции. Нормы российского законодательства с развитием технологий совершенствуются, но этого мало для быстрого расследования преступлений. Совершающий данные преступления хакер практически всегда подготовлен и обладает определенным набором программно-аппаратных методов и навыков, позволяющих облегчить совершение преступления [24]. Возникают сложности в классификациях преступлений, вопросы о применении той или иной статьи административного и уголовного кодекса. Помимо этого, Верховный Суд Российской Федерации должен выпускать конкретные методы и способы поиска преступников, собирания доказательства и определения той или иной статьи Уголовного кодекса Российской Федерации.

Итак, можно сделать вывод, что миру грозит информационный поток, т. е. информационный коллапс. В связи с этим цифровая зависимость может выйти из-под контроля и любая информация в Интернете будет доступной для киберпреступлений.

Список литературы

1. Выступление Владимира Путина 3 марта 2021 г. на ежегодном расширенном заседании коллегии Министерства внутренних дел Российской Федерации // Расширенное заседание коллегии МВД России. URL:http://www.kremlin.ru/events/president/news/65090.

2. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [А. В. Богданов и др.]; под ред. В. П. Кувалдина, Л. Л, Тузова, И. А. Климова. 6-е изд., перераб. и доп. М. : ЮНИТИ-ДАНА, 2021. 431 с.

3. Богданов А. В., Ильинский И. И., Хазов Е. Н. Информационно-телекоммуникационная сеть Интернет как один из наиболее востребованных ресурсов в противодействии незаконному обороту наркотиков // Вестник Московского университета МВД России. 2018. № 3. С. 173–179.

4. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

5. Комплексный анализ состояния преступности в Российской Федерации и расчетные варианты ее развития : аналитический обзор / [Ю. М. Антонян и др.]. М. : ФГКУ «ВНИИ МВД России», 2018. 86 с.

6. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [И. А. Климов и др.]. 4-е изд., перераб.и доп. М. : Юнити, 2019. 439 с.

7. Кузьмин Н. А. К вопросу о понятии и содержании коррупции // Вестник Московского университета МВД России. 2020. № 6. С. 128–131.

8. Кузьмин Н. А. К вопросу о необходимости закрепления в действующем законодательстве понятия «коррупционное преступление» // Вестник Московского университета МВД России. 2020. № 2. С. 196–198.

9. Квалификация взяточничества (по материалам судебной практики) : научно-практическое пособие / [М. Г. Жилкин и др.]. М. : МосУ МВД России имени В. Я. Кикотя, 2019.

10. Противодействие преступлениям террористической и экстремистской направленности / [Е. Н. Хазов и др.] // Вопросы теории и практики оперативно-розыскной деятельности. 2013.

11. Хазов Е. Н., Богданов А. В., Мартынюк В. М. Основные направления, проблемы и пути решения организации работы по розыску лиц, скрывшихся от органов дознания, следствия и суда сотрудниками оперативно-розыскных подразделений ОВД МВД России на современном этапе // Вестник Московского университета МВД России. 2012. № 10. С. 148–152.

12. Богданов А. В., Хазов Е. Н. Основные направления деятельности оперативных подразделений органов внутренних дел

по выявлению и предупреждению преступлений, связанных с мошенничеством // Вестник Московского университета МВД России. 2014. № 10. С. 276–279.

13. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

14. Богданов А. В., Хазов Е. Н. Основные направления взаимодействия оперативных подразделений и органов предварительного следствия полиции, их значение по выявлению и раскрытию преступлений // Вестник Московского университета МВД России. 2010. № 11. С. 71–75.

15. Богданов А. В., Ильинский И. И., Хазов Е. Н. Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Всероссийский криминологический журнал. 2020. № 1. С. 15.

16. Богданов А. В., Хазов Е. Н., Комахин Б. Н. Преступность несовершеннолетних: новые решения и новые проблемы // Вестник Московского университета МВД России. 2013. № 4. С. 34–38.

17. Исламский экстремизм : сущность, идеология, организация и тактика их деятельности / [К. М. Лобзов и др.]. Хабаровск, 2018.

18. Богданов А. В., Ильинский И. И., Хазов Е. Н. Терроризм и экстремизм – угроза современной цивилизации // Вестник экономической безопасности. 2021. № 1. С. 181–187.

19. URL: https://news.rambler.ru/internet/41961699-tsifra-dnya-skolko-podrostkov-vovlecheny-v-destruktivnye-gruppy-v-sotssetyah/.

20. Экстремистские организации: сущность, идеология, тактика их деятельности / [К. М. Лобзов и др.]. Новосибирск, 2021.

21.URL:https://yandex.ru/news/instory/V_Italii_chastichno_zablokirovali_TikTok_iz-za_gibeli_10-letnej_devochki--748b4efd378e-703fd9808729cc94211a?lr=21623&content=alldocs&stid=HaFk5pt4ERGc9bpWYLIM&persistent_id=127246821&from=story.

22. Предательство в форме государственной измены: духовно-нравственный, криминально-психологический и уголовно-правовой аспекты (опыт критического анализа) / [К. М. Лобзов и др.]. М., 2020.

23. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2021. № 27 (часть II). Ст. 5351.

24. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (ред. от 01.07.2021) // Собрание законодательства Российской Федерации. 2011. № 1. Ст. 48.

25. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

26. URL: https://trends.rbc.ru/trends/industry/602f668a9a7947d5f06e0c7a#.

27. Богданов А. В., Ильинский И. И., Завьялов И. А. Организованная преступность и ее общественная опасность // Вестник Московского университета МВД России. 2013. № 7. С. 116–120.

28. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [А. В. Богданов и др.]. 5-е изд., перераб. и доп. М., 2020.

29. Кузьмин Н. А., Чикова Я. Н., Завьялов И. А. Противодействие органов внутренних дел преступлениям в сфере незаконного оборота наркотиков с использованием возможностей Интерпола // Вестник экономической безопасности. 2015. № 7. С. 67–71.

30. Кузьмин Н. А., Завьялов И. А. Противодействие оперативных подразделений органов внутренних дел наркопреступности на современном этапе // Актуальные вопросы подготовки сотруд-

ников правоохранительных органов к противодействию современным угрозам : сборник научных трудов круглого стола, 2018. С. 410–415.

31. Завьялов И. А. Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений // Вестник Московского университета МВД России. 2021. № 3. С. 228–236.

Гринберг С. А.[1],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России имени В.Я. Кикотя

СОВРЕМЕННАЯ ИНФОРМАЦИОННАЯ СРЕДА КАК ФАКТОР ДЕТЕРМИНАЦИИ ОРГАНИЗОВАННЫХ ФОРМ ПРОФЕССИОНАЛЬНОЙ ПРЕСТУПНОСТИ В МЕГАПОЛИСЕ

Значение информации для современного общества и отдельно взятого индивида сегодня сложно переоценить. Поскольку информационная связь с окружающим миром является необходимым условием нормальной жизнедеятельности человека и функционирования общества, с информацией и функционированием и использованием информационных форм коммуникаций напрямую или опосредованно связаны все без исключения виды человеческой деятельности [1]. Технологическое развитие человечества и глобализационное влияние информационных технологий, определяет все большую зависимость человека от социально значимой информации, которая во многом конструирует современный социум и влияет на интеллект современного человека, его мировоззренческие установки, соответственно, на его поведение [2].

Интенсивное развитие информационного общества в России определяется тем, что технологии, созданные на основе передовых знаний (нано- и биотехнологии, искусственный интеллект, оптические технологии и пр.), становятся сегодня доступными для населения. Так, частью повседневной жизни россиян стали информационные системы, социальные сети, электронные средства массовой информации и коммуникации, доступ к которым осуществляется с использованием сети Интернет. Россияне

имеют широкий доступ к мобильным устройствам (в среднем на одного человека приходится два абонентских номера мобильной связи), а также беспроводным технологиям и сетям связи. Более половинным имеют доступ (подключение) к сети Интернет. В электронной форме имеет место прямая и обратная связь населения с органами публичной власти, функционирует система предоставления государственных и муниципальных услуг в электронной форме и прочее [3].

Таким образом, российское общество можно охарактеризовать как развивающееся информационное общество. При этом информационная среда является как фактором прогрессивного, конструктивного развития общества, так и фактором, детерминирующим определенные риски, включая риски, непосредственно связанные с использованием самих информационных технологий, в том числе риски криминогенного характера.

И именно современный мегаполис, являясь центром социальной, финансовой, экономической, политической, интеллектуальной активности и культурной жизни и ресурсов, центром концентрации больших масс населения, обладает развитой информационной инфраструктурой и выступает центром развития и внедрения информационных технологий. Таким образом, современная информационная среда существенным образом определяет криминогенный «облик» современного мегаполиса, формируя условия и обстановку осуществления различных видов преступной деятельности, в том числе организованных форм профессиональной преступной деятельности.

Рассматривая современную информационную среду как фактор детерминации организованных форм профессиональной преступности в мегаполисе, следует учитывать следующие аспекты.

1. Детерминационная роль современной информационной среды в реализации организованных форм профессиональной преступности в мегаполисе определяется, прежде всего, тем, что

информационная среда обеспечивает реализацию такой конституирующей характеристики данного вида преступной деятельности, как криминальная коммуникация.

Криминальная коммуникация предполагает как обмен информацией внутри преступного объединения (сообщества), так его информационное взаимодействие с внешней, прежде всего, криминальной средой. Именно во взаимосвязи (коммуникации) с криминальной средой проявляется качество системности как организованной, так и профессиональной преступности [4]. Один из ключевых признаков профессиональной преступности выделяет ее связь с криминальной средой, которая обеспечивает сохранение и воспроизводство криминального профессионализма [5]. Криминальные специализация и квалификация не могут существовать изолированно, вне криминальной среды, поскольку предполагают обучение, профессиональную оценку и конкуренцию [6].

Соответственно, развитие информационных технологий и совершенствование информационной среды, обеспечивая реализацию коммуникационной составляющей (от получения новых знаний до обмена данными), обеспечивает развитие и совершенствование организованной профессиональной преступности, в том числе ее трансграничность.

2. Современная информационная среда является источником генерации новых способов реализации организованных форм профессиональной преступности в мегаполисе, связанных с использованием информационных технологий как способа совершения преступления, а также является источником продуцирования принципиально новых видов криминальной активности, т. е. выступает непосредственно сферой реализации данного вида преступной деятельности.

Качественные характеристики современной преступности определяются сегодня ростом качественного разнообразия сфер и способов совершения преступлений, разнообразием субъектов преступления и организационно-структурным усложнением кри-

минализации. Масштабный свободный доступ к информационным ресурсам и сетям (национальным и мировым) во многом обусловливает и криминальный характер деятельности [7]. Развитие информационных технологий и масштабы информационно-телекоммуникационных сетей изменяют конфигурацию всей системы преступной деятельности, которая все больше смещается в виртуальное пространство, а высоколатентная киберпреступность вытесняет из структуры преступности «традиционные» преступления [8].

Информационно-телекоммуникационные сети используются, например, для совершения преступлений в сфере экономики, связанных с приобретением и сбытом определенных предметов (поддельных денег, ценных бумаг, банковских карт и пр.) [9]. Кроме того, следует учитывать, что хотя информационно-телекоммуникационные сети и не используются напрямую при выполнении объективной стороны других преступлений, однако могут использоваться в процессе приготовления к ним, в том числе для поиска необходимой информации, подыскания соучастников преступления и сговора с ними, обмена информацией, приобретения необходимых орудий и средств совершения преступления. Использование информационных технологий и информационно-телекоммуникационных сетей для планирования преступной деятельности, приготовления и совершения преступлений, сокрытия преступной деятельности и следов совершения преступлений, использования и легализации имущества, добытого преступным путем, дистанционность совершения преступлений и прочее определяют усложненный, преимущественно организованный и профессиональный характер преступной деятельности, предполагающий наличие и криминальное применение виновными знаний, умений и навыков в области информационных технологий, существенно повышая объем общественно опасных последствий данной преступной деятельности, характер и степень ее общественной опасности [10].

Учитывая специфику информационных связей индивида и социума и непосредственную взаимосвязь информационных технологий с когнитивными, все большую криминальную угрозу представляет также использование в качестве способа совершения преступлений информационно-когнитивных технологий [11]. Данный способ может быть использован в деятельности организованной профессиональной преступности для совершения таких преступлений, как: мошенничество и иные преступления в сфере экономики (в том числе в финансовой сфере и сфере потребительского сектора), нарушение неприкосновенности частной жизни, личной и семейной тайны и иные посягательства на конституционные права и свободы человека и гражданина, доведение до самоубийства, причинение вреда здоровью (психическому) различной степени тяжести и другие преступления против жизни и здоровья, вовлечение в преступную деятельность и пр.

Современная информационная среда выступает фактором, трансформирующим и определяющим актуальные виктимологические параметры организованных форм профессиональной преступности в мегаполисе.

Криминогенность и специфика оперативной обстановки в современном мегаполисе во многом определяются поликомпонетностью состава населения, его национальным, этническим и конфессиональным разнообразием, сложными демографическими и миграционными процессами. Современный мегаполис, прежде всего, является местом массового проживания и притяжения большого количества людей, при этом массовость и высокая мобильность населения мегаполиса несут значительный криминогенный и виктимогенный потенциал. В свою очередь современные информационные технологии существенным образом способствуют как формированию виктимных качеств населения, так и выбору профессиональными преступниками жертв преступного посягательства.

Вынуждены согласиться с тем, что в сложившихся условиях социализации, развития и реализации личностного потенциала

виктимность является характерным атрибутом нашей жизни и свойством общества. Причиной этого во многом является существенная дисфункция системы обеспечения безопасности жизнедеятельности, порождаемая не только и не столько дефектами организационной компоненты в структуре общей и специальной превенции преступности, сколько несформированностью прогностического (не говоря уже о криминологическом) типа мышления у большинства населения, а особенно у молодежи [12]. Прямой иллюстрацией указанному является открытость, в большинстве случаев инициируемая самим человеком, персональных и иных личных данных в социальных сетях и т. п.

Также следует учитывать, что современные информационные технологии существенно влияют на такие параметры как восприятие, так и продуцирование различных форм поведения человека. Целенаправленное воздействие на сознание человека может формировать и канализировать как деструктивное, так и виктимное поведение как отдельного индивида, так и социальных групп [13].

Масштабность и глубина вовлеченности и погруженности населения в социальные сети и иные инструменты коммуникации существенным образом трансформируют и определяют его виктимологические характеристики. В свою очередь изменения данных виктимологических характеристик, обусловленные развитием информационных технологий и трансформацией информационной среды, определяют виктимологические параметры организованных форм профессиональной преступности в современном мегаполисе.

Таким образом, роль современной информационной среды в детерминации организованных форм профессиональной преступности в мегаполисе определяется тем, что она:

– обеспечивает реализацию криминальной коммуникации, обеспечивает развитие и совершенствование организованной профессиональной преступности, в том числе ее трансграничность;

– является источником генерации новых способов реализации организованных форм профессиональной преступности в мегаполисе и сферой реализации данного вида преступной деятельности;

– конструирует и трансформирует актуальные виктимологические параметры организованных форм профессиональной преступности в мегаполисе.

Список литературы

1. Иванцов С. В. Использование информационно-телекоммуникационных сетей для совершения преступлений: вопросы уголовно-правового воздействия и предупреждения / под общ. ред. Н. А. Лопашенко // Уголовно-правовое воздействие и его роль в предупреждении преступности : сборник материалов IV Всероссийской научно-практической конференции «Саратовские уголовно-правовые чтения». Саратов, 2019. С. 155–158.

2. Игнатов А. Н. Информационно-когнитивные технологии в арсенале способов совершения преступлений // Гуманитарные, социально-экономические и общественные науки. 2020. № 11-2. С. 82–89.

3. Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

4. Иванцов С. В. Обеспечение органами внутренних дел системного подхода в изучении и предупреждении организованной преступности : монография. М. : ЮНИТИ-ДАНА, 2017. С. 54–55.

5. Предупреждение преступлений и административных правонарушений органами внутренних дел : учебник для студентов, обучающихся по направлениям подготовки «Юриспруденция» и «Правоохранительная деятельность» / под ред. В.Я. Кикотя, С.Я. Лебедева. 3-е изд., перераб. и доп. М. : ЮНИТИ-ДАНА, 2017. С. 340.

6. Фарышев Е. В. Современное понятие и содержание профессиональной преступности // Вестник Краснодарского университета МВД России. 2016. № 3 (33). С. 91–92.

7. Шеслер А. В., Шеслер С. С. Криминальный профессионализм: понятие и признаки // Gaudeamus Igitur. 2015. № 2. С. 73.

8. Гринберг С. А. Организованные формы профессиональной преступности: определение понятия // Вестник Московского университета МВД России. 2020. № 8. С. 106–110.

9. Суходолов А. П., Иванцов С. В., Борисов С. В., Спасенников Б. А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 13–21.

10. Иванцов С. В., Новиков С. В. Преступления на рынке ценных бумаг: криминологическая характеристика и предупреждение : монография. М. : ЮНИТИ-ДАНА, 2012.

11. Суходолов А. П., Иванцов С. В., Борисов С. В., Спасенников Б. А. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 13–21.

12. Игнатов А. Н. Информационно-когнитивные технологии в арсенале способов совершения преступлений // Гуманитарные, социально-экономические и общественные науки. 2020. № 11-2. С. 82–89.

13. Игнатов А. Н. Свобода виктимности // Вестник Дальневосточного юридического института МВД России. 2017. № 3 (40). С. 79–85.

14. Вишневецкий К. В. Криминогенная виктимизация социальных групп в современном обществе: монография / под ред. С. Я. Лебедева. М. : ЮНИТИ-ДАНА, 2010.

15. Вишневецкий К. В. Механизм виктимологической детерминации // Теория и практика общественного развития. 2014. № 10. С. 154–157.

Дегтярев А.[1],
начальник 3-го отдела управления
по борьбе с информационными преступлениями
Национального инспектората расследований
Генерального инспектората полиции
МВД Республики Молдова

СЕКСУАЛЬНАЯ ЭКСПЛУАТАЦИЯ И СЕКСУАЛЬНОЕ НАСИЛИЕ НАД ДЕТЬМИ В ИНТЕРНЕТЕ. БОРЬБА С ФЕНОМЕНОМ В РЕСПУБЛИКЕ МОЛДОВА

Уважаемые коллеги!

В настоящее время информационные технологии используются все чаще в повседневной жизни. В частности, к этому относятся мобильные устройства, сеть Интернет и прочие технологии, с которыми мы порой не расстаемся и на час. По мере развития преступности в онлайн пространстве самыми уязвимыми в сети интернет стали дети, которые, в частности, легко могут стать жертвами сексуального насилия или сексуальной эксплуатации.

На сегодняшний день в Республики Молдова был установлен ряд случаев использования услуг, предоставляемых провайдерами, с целью совершения данного рода преступлений. Речь о таких услугах как: интернет-подключение, хостинг/mirroring, прокси/VPN, а также облачные хранилища. Порой некоторые из упомянутых услуг используются преступниками, находящимися за границей, против граждан разных государств, и, таким образом, цифровые данные и оборудование из Республики Молдова являются лишь инструментальной частью состава преступления. Самые распространенные преступные деяния, направленные против детей – это груминг (совращение детей в сексуальных целях) и детская порнография, создание и администрирование сайтов

[1] © Дегтярев А., 2022.

специально для распространения детской порнографии, в том числе в коммерческих целях, также часто для выгрузки данного контента используются законно действующие сайты файлового хостинга или хостинга изображений.

В сети Интернет также распространены целые руководства по сексуальному совращению детей. Одно из них было разработано на другом языке, после чего заинтересованные лица перевели и адаптировали версию на русском специально для стран СНГ. Многие из лиц, которые имеют сексуальный интерес в отношении детей и были привлечены к ответственности на территории Республики Молдова, имеют очень продвинутые навыки в области ИТ, в том числе высшее образование либо работают в данной сфере.

Самые часто используемые методы манипуляции детьми – это предлог любовных отношений, индустрия красоты и использование фейковых аккаунтов. Обмен данными осуществляется, в частности, в виде текста, изображений, видео, аудио, эмодзи, гиперссылок и пр. Для получения интимных фото/видео детей используются веб-камеры либо жертв убеждают создать и отправить интимные «селфи». Обычно чем популярнее социальная сеть, тем больше злоумышленников поджидают в ней детей. В случае Республики Молдова – это сети «ВКонтакте», «Одноклассники», Facebook, Instagram и Skype.

Детская порнография изготовляется и распространяется в различных целях. Чаще всего она является для педофила инструментом собственного сексуального удовлетворения. Также детская порнография используется для оправдания педофилии, груминга, сексуального шантажа жертв, доказательства собственных «достижений» насилия детей в кругу педофилов, для памяти физического сексуального насилия ребенка, для обмена (бартера), а также для финансовой выгоды (в том числе в коммерческих целях). Среди самых популярных инструментов обмена детской порнографии числятся одноранговые сети (peer to peer).

Стоит упомянуть, что в наши дни в определенных случаях дети выгружают собственные интимные фото/видео в интернет без влияния насильников, ошибочно полагая, что таким образом получат популярность либо для самоутверждения среди сверстников в периоде полового созревания. В случае, если ребенок стал жертвой сексуального насилия или сексуальной эксплуатации на территории Республики Молдова, доступны несколько горячих линий для помощи (бесплатный телефонный звонок или путем связи в интернете).

В рамках расследования данного рода преступлений правоохранительные органы в Республике Молдова используют ряд каналов сообщения: специализированное подразделение полиции, прямые каналы в рамках международных конвенций, а также через представительства правоохранительных ведомств при посольствах стран в Республике Молдова. Также используются такие прямые каналы как специализированная База данных «ICSE» Интерпола, «Европейская платформа экспертов» Европола и платформа Национального центра пропавших и эксплуатируемых детей (NCMEC) из США. Для автоматизации обработки данных используется национальная база данных по детской порнографии – информационная система «Защита детей» и база данных «Aviator», разработанная в рамках проекта НПО «Inhope».

В ходе анализа данных с изъятых носителей используется копия (клон), а не сам вещь док, также применяются инструменты предварительного быстрого поиска «триаж» с использованием поиска изображений/видео, хэш-алгоритмов, ключевых слов, списка интересующего программного обеспечения и др. В качестве примера прямого получения данных от администраторов интернет-услуг можно отметить международные запросы, направленные провайдеру сетей Facebook и Instagram посредством специализированного портала для правоохранительных органов.

В заключение считаем крайне необходимым продвижение информирования детей о безопасности в интернете аналогично уже давно привычному для нашего общества объяснению правил дорожного движения. Ведь в онлайн среде риски также велики, как и в оффлайновом мире.

Благодарю за внимание!

Дюсетаев Р. С.[1],
заместитель начальника
Центра по борьбе с киберпреступностью
Департамента криминальной полиции МВД
Республики Казахстан

О НАРАЩИВАНИИ ПОТЕНЦИАЛА ВЗАИМОДЕЙСТВИЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, В ТОМ ЧИСЛЕ ИНТЕРНЕТ-МОШЕННИЧЕСТВ

Борьба с преступлениями в сфере информационных технологий на сегодняшний день является одной из важных задач, стоящих перед правоохранительными органами.

Для реализации своих целей преступники все чаще используют весь потенциал интернет-технологий, таких как социальные сети «ВКонтакте», Instagram, Telegram, а также различные электронные платежные системы и криптовалюту.

Интернет-ресурсы выступают в качестве площадки для обучения планированию и осуществлению актов терроризма, организуется финансирование этой деятельности, размещаются подробные инструкции по изготовлению оружия, боеприпасов и взрывных устройств.

Процессы размещения экстремистских материалов в социальных сетях в последнее время приобретают все более масштабный характер.

Зачастую для совершения преступлений используются сервисы, позволяющие скрыть идентификационные данные пользователя, его местонахождение. Особенно популярно в настоящее

время использование прокси-серверов, VPN-каналов, а также сервисов по подмене абонентского номера.

Наиболее актуальным видом киберпреступлений являются электронные хищения, в том числе интернет-мошенничества.

За последние годы в Казахстане, впрочем, как и во всем мире, наблюдается стремительный рост регистрации таких преступлений.

В определенной мере этому способствует цифровизация общественных отношений, особенно, развитие онлайн-услуг в связи с принятыми в период пандемии карантинными мерами.

На этом фоне проявляют активность и криминальные элементы. На протяжении пяти лет, начиная с 2016 г., их число ежегодно увеличивается в арифметической прогрессии (2016 г. – 1 046, 2017 г. – 2 046, 2018 г. – 4 287, 2019 г. – 7 739, 2020 г. – 14 175).

С начала 2021 г. в Казахстане уже зарегистрировано свыше 16 тыс. таких преступлений, что в два раза превышает показатель 2020 г. (8 348 преступлений).

Проведенный анализ по способам совершения таких преступлений выявил следующие распространенные способы.

С начала 2021 г. около двух с половиной тысяч интернет-мошенничеств совершены путем оформления онлайн-займов через сайты микрофинансовых организаций.

При этом в ряде случаев персональные данные граждан преступники получали из открытых интернет-источников (объявления об утере документов, рассылка в группах и чатах мессенджеров).

Свыше тысячи семисот случаев связаны с хищениями денег с банковских счетов путем завладения реквизитами жертв, в основном мошенники представлялись сотрудниками служб безопасности банков либо финансовых организаций.

Необходимо отметить, что почти треть оставшихся нераскрытыми (11 243) интернет-мошенничеств совершена с территории государств бывшего союза (Россия, Беларусь, Украина).

В большинстве случаев похищенные средства выводились через зарубежные банки (российские, белорусские и украинские).

Абонентские номера, использованные мошенниками, обслуживались на территории государств СНГ, похищенные деньги обналичивались также в зарубежных банках, с использованием электронных платежных систем (Сбербанк, Тинькофф Банк, Яндекс Деньги, QIWI Кошелек, Газпромбанк, VEDEN).

Следует отметить, что зачастую соучастниками таких преступлений выступают граждане Республики Казахстан и в качестве транзита используются казахстанские счета.

Имеются случаи задержания граждан СНГ, прибывших в Казахстан для вербовки так называемых обнальщиков, т. е. владельцев пластиковых карт для получения переводов и последующего перечисления денег посредством электронных платежей.

Процесс установления лиц, совершающих такие преступления сложен и занимает длительное время, поскольку они зачастую носят трансграничный характер

Рядом государств ратифицировано (Законом Республики Казахстан от 9 декабря 2019 года № 277-VI ЗРК) «Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий» (28 сентября 2018 г., г. Душанбе).

Решением Совета глав государств Содружества Независимых Государств от 28 сентября 2018 г. утверждена Межгосударственная программа совместных мер борьбы с преступностью на 2019–2023 годы. В рамках плана по ее реализации проводятся комплексные совместные оперативно-профилактические мероприятия.

Вместе с тем, несмотря на наличие подписанных соглашений, до настоящего времени механизм взаимодействия компетентных органов в данной области не урегулирован. Направляемые поручения и запросы об оказании правовой помощи исполняются длительное время (от двух месяцев), что не обеспечивает оперативности при раскрытии указанных преступлений.

Вследствие нахождения преступников за пределами государства практически все уголовные дела остаются нераскрытыми, а преступники продолжают осуществлять свою противоправную деятельность.

В этой связи полагается целесообразным расширить механизмы обмена оперативной информацией и оперативного взаимодействия правоохранительных органов по противодействию киберпреступности.

Кроме того, учитывая трансграничность преступлений рассматриваемой категории, полагается целесообразным рассмотреть вопрос о создании межгосударственного информационного ресурса МВД государств – участников СНГ, содержащего криминалистический учет преступлений в IT-сфере по способам их совершения.

Целесообразно рассмотреть вопрос о проведении совместных расследований уголовных дел о трансграничных преступлениях.

Указанные меры позволят повысить эффективность принимаемых мер, а также оперативно отслеживать злоумышленников и устанавливать их причастность к другим преступлениям, совершенным на территории государств – участников СНГ.

Завьялов И. А.[1],
заместитель начальника кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Молянов А. Ю.[2],
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

К ВОПРОСУ О ФОРМИРОВАНИИ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ СПЕЦИАЛЬНОГО ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Специальное техническое обеспечение оперативно-разыскной деятельности органов внутренних дел Российской Федерации (СТО ОРД ОВД РФ) является масштабной областью деятельности подразделений ОВД, целями которой являются оснащение оперативных подразделений специальной техникой; разработка комплекса мероприятий по рациональному применению имеющихся и вновь поступающих технических средств; определение многовариантности действий сотрудников оперативных подразделений и возможности успешного выполнения поставленных задач в различных оперативно-тактических ситуациях, в том числе и при резких ее ухудшениях; проведение обязательного резерви-

рования всех видов ресурсов; ведение учетной и отчетной документации; использование современных программных, телекоммуникационных и электронно-вычислительных средств управления.

Организация специального технического обеспечения выражается в деятельности оперативных подразделений по подготовке, размещению, перемещению и согласованному применению средств СТО ОРД ОВД; нормированию, истребованию (закупок), получению, хранению и обновлению указанных средств; взаимодействию органов управления СТО всех уровней между собой; использованию децентрализованного снабжения на местах; совершенствованию управления инфраструктурой СТО ОРД ОВД; служебной и специальной подготовке органов управления, подразделений и должностных лиц, ответственных за решение задач СТО ОРД ОВД; а также решению других задач.

Следует признать, что наличие целого комплекса проблем в системе органов внутренних дел требует незамедлительного решения в рамках реформы МВД России. При этом в основе большинства из них прямо или опосредованно лежат причины организационно-управленческой природы, которые не могут расцениваться, как проблемы отдельного региона, отдельной службы или отдельного подразделения, а носят общественный характер. Речь идет об организационных деформациях, т.е. явлениях, способствующих формированию определенных сбоев, препятствующих эффективному достижению поставленных перед ОВД задач.

Выявление и раскрытие преступлений, независимо от их тяжести, а также установление лиц, их подготавливающих, совершающих или совершивших, как направление оперативно-разыскной деятельности реализуется в комплексе со всеми ее формами (оперативная проверка, оперативная разработка, оперативно-разыскное сопровождение предварительного расследования), обеспечивающими решение таких задач, как предупреждение, пресечение и раскрытие преступлений. В этих целях подразделения уголовного розыска организуют предварительный сбор,

накопление и систематизацию сведений о лицах, представляющих оперативный интерес, и фактических данных, указывающих на различные признаки тайной, с элементами маскировки противоправной деятельности. Собираемые сведения необходимы для контроля за преступниками, своевременной нейтрализации их противоправной деятельности, а также для привлечения к различным видам ответственности. Безусловно, выполнение указанного перечня задач невозможно без применения современных достижений науки и техники.

Прежде всего, необходимо определиться с перечнем тех оперативно-разыскных мероприятий, которые преимущественно осуществляют при раскрытии преступлений, и перечнем основных технических средств, применяемых в ходе проведения оперативно-разыскных мероприятий. Отвечая на первую часть вопроса, следует сказать, что в соответствии с нормами ч. 2; 4 и ч. 9 ст. 8 ФЗ «Об ОРД», при наличии признаков любого из преступлений, по которому в соответствии ч. 2 ст. 150 УПК РФ предварительное следствие обязательно, допускается проведение ОРМ, указанных в ч. 1 ст. 6 указанного закона. В этот перечень входят оперативно-разыскные мероприятия (включая получение компьютерной информации), которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, проводимые на основании судебного решения.

Анализ перечня преступлений, по которым требуется предварительное следствие, показывает, что к данной категории относятся также преступления средней и небольшой тяжести, например, ст. 106, ч. 2 ст. 107, ч. 3 ст. 109, ст. 110 и др. Однако в соответствии с нормами ч. 4 и ч. 9 ст. 8 ФЗ «Об ОРД» только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких пре-

ступлений, допускается прослушивание телефонных и иных переговоров, а также проведение оперативного эксперимента в целях выявления, предупреждения, пресечения и раскрытия преступлений указанных категорий. Это обстоятельство как минимум значительно снижает применение оперативно-разыскных средств как правового инструментария, и, как максимум, фактически лишает органы, осуществляющие оперативно-разыскную деятельность, одного из действенных механизмов борьбы с преступностью. В этой связи А.Е. Чечетин рассматривает возможность проведения всех рассматриваемых ОРМ по преступлениям средней тяжести. Допустимость проведения прослушивания телефонных переговоров по преступлениям небольшой и средней тяжести, а также оперативного эксперимента в своих работах рассматривают С.И. Захарцев и Ю.Ю. Игнащенков, Н.А. Бояркина, А.В. Красовский.

Относительно преступлений небольшой тяжести, а также преступлений средней тяжести, по которым проведение предварительного следствия не обязательно, нормами ст. 8 ФЗ «Об ОРД» законодатель установил запрет на проведение указанных мероприятий в целях выявления, предупреждения, пресечения и их раскрытия, а также в целях выявления и установления лиц, их подготавливающих, совершающих или совершивших.

Применительно к предмету нашего исследования необходимо остановиться на анализе социально-криминологической характеристики преступности в России за 2013–2020 гг., который показывает, что, в среднем, процентное соотношение количества тяжких и особо тяжких преступлений к количеству преступлений небольшой и средней тяжести выглядит как 22 % и 78 %. Среди зарегистрированных преступлений сохраняется интегральное соотношение преступлений по степени тяжести и их удельному весу. Так, удельный вес составляет:

– особо тяжких преступлений – 5–6 %;

– тяжких преступлений – 15–21 %;

– преступлений средней тяжести – 33–35 %;

– преступлений небольшой тяжести – 42–45 %.

При этом, если раскрываемость по некоторым видам тяжких и особо тяжких преступлений приближается к 90–97 %, то раскрываемость преступлений небольшой и средней тяжести находится в пределах 30–35 % и 40–43 % соответственно.

Подводя итог вышесказанному, мы видим, что в 78 % раскрытия совершенных преступлений сотрудники оперативных подразделений, во-первых, лишены возможности проводить оперативно-разыскные мероприятия с использованием специальных технических средств, эффективность которых не подлежит сомнениям. Во-вторых, сложившееся положение с техническим обеспечением деятельности сотрудников оперативных подразделений стало следствием организационной деформации, проявляющейся в господстве структуры над функцией. В нашем случае структура и функция приобрели черты обособленных сторон организации управления ОВД. Это выражается в содержании Типового положения об отделе (отделении, пункте) полиции территориального органа Министерства внутренних дел Российской Федерации на районном уровне, в соответствии с которым полномочия должностных лиц по вопросам материально-технического обеспечения полностью отсутствуют. Это означает только одно, что У(О)МВД района в организации процесса обеспечения материально-техническими средствами не участвует.

Мы согласимся с мнением А. Г.Андриасова, что исключение возникшей организационной деформации возможно лишь в результате реализации дальнейшего совершенствования системы СТО ОРД ОВД за счет внедрения новых организационных форм. Вместе с тем необходимо отметить, что не всякое организационное новшество будет способствовать улучшению управления.

Проблемы организационных структур не являются теоретической новеллой. Различные организационные аспекты проблем управления в органах внутренних дел исследовались в трудах

Л. Ш. Берекашвили, С. Е. Вицина, Н. Н. Иванова, И. И. Колесникова, Л. М. Колодкина, Г. А. Туманова и других ученых. Их анализ показывает, что отсутствуют научно обоснованные методики проектирования организационных структур управления в системе ОВД. Поскольку организационная структура управления имеет целый ряд признаков, мы выделим лишь те, которые имеют существенное значение для нашего исследования – это элементы и их взаимосвязи; характер взаимосвязей; тип построения; уровни управления.

Рассмотрение структуры МВД России показывает, что центральный аппарат и территориальные органы МВД России построены не по целевому, а по отраслевому принципу, в соответствии с которым организационной структурой СТО ОРД ОВД является линейно-функциональный тип построения, который предусматривает возможность создания в структуре дополнительных исполнительных элементов.

Это позволит сформировать в структуре МВД России многоуровневую систему специализированных подразделений, объединенных в единую централизованную службу, обозначив ее как, например, техническая, научно-техническая или инженерно-техническая. Подразделения этой службы в территориальных органах МВД России можно было бы определить как научно-технические или инженерно-технические группы, отделения, отделы, бюро и т. д. оперативных подразделений уголовно-разыскной направленности. Основной целью указанной службы будет «вернуть» специальную технику в оперативные подразделения городского и районного уровней.

Создание указанных подразделений приведет к совершенствованию единой научно-технической политики министерства внутренних дел, организации разработок средств СТО ОРД ОВД на основе анализа практического применения, их внедрение в практику борьбы с преступностью. В настоящее время эти задачи централизованно в системе МВД России не решаются.

Список литературы

1. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [А. В. Богданов и др.]. 5-е изд., перераб. и доп. М., 2020.

2. Завьялов И.А. Зарубежный опыт использования искусственного интеллекта в раскрытии преступлений // Вестник Московского университета МВД России. 2021. № 3. С. 228–236

3. Богданов А. В., Завьялов И. А., Хазов Е. Н. Противодействие организованной преступности в сфере экономики // Криминологический журнал. 2020. № 2. С. 91–100.

4. Михайлов Б. П., Тузов Л. Л., Завьялов И. А. Социально-криминальные особенности современной наркоситуации в Российской Федерации // Закон и право. 2017. № 9. С. 15–21.

5. Михайлов Б. П., Воронцов А. В., Завьялов И. А. Особенности криминальной среды России // Вестник Московского университета МВД России. 2013. № 6. С. 186–190.

6. Богданов А. В., Завьялов И. А., Хазов Е. Н. Карманные кражи в России (современное состояние, тенденции и перспективы противодействия) // Вестник Московского университета МВД России. 2013. № 10. С. 38–41.

Зинеева И. Н.[1]**,**
соискатель по кафедре криминологии
Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ РЕГУЛИРОВАНИЯ СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ОХРАНЫ ВОДНЫХ БИОЛОГИЧЕСКИХ РЕСУРСОВ

Несмотря на значительное ухудшения состояние водной флоры и фауны, а также среды обитания, анализ совершения нарушений правил охраны водных биологических ресурсов свидетельствует о ее высоком уровне латентности. Выявление фактов совершения преступлений в данной сфере остается практически неизменным. Для усиления государственного контроля в этой сфере предусмотрена административная ответственность за негативное воздействие на водные биологические ресурсы и среду их обитания на начальных этапах производственной деятельности. Представляется возможным сокращение негативного воздействия на водные биологические ресурсы путем применения комплексного подхода, в том числе, введения административной преюдиции.

Анализ состояния преступности в сфере охраны водных биологических ресурсов свидетельствует о ее высоком уровне латентности и одновременном росте. Несмотря на то, что нарушения правил охраны водных биологических ресурсов наблюдаются на большинстве водных объектов Российской Федерации, выявление фактов совершения преступлений в данной сфере практически не происходит.

В целях установления контроля за негативными последствиями на водные биологические ресурсы и среду их обитания на начальных этапах производственной деятельности на водных объектах законодатель ввел административную ответственность

за саму возможность негативного воздействия на них. Эта норма закреплена в ст. 8.38 КоАП РФ.

Можно с определенной уверенностью говорить о том, что существует серьезный разрыв между количеством фактически совершаемых деяний и реальным применением уголовно-правовой ответственности.

Анализ приведенных статистических данных показывает, что в России в последние годы наблюдается тенденция роста количества возбуждаемых дел об административных правонарушениях по ст. 8.38 КоАП, а также лиц, привлеченных к ответственности за их совершение. К сожалению, такая динамика в области применения уголовно-правовой нормы об ответственности не наблюдается.

Можно согласиться с высказываемой в литературе точкой зрения, что органы прокуратуры, которые призваны обеспечить законность реализации мер юридической ответственности, зачастую неправомерно подменяют уголовную ответственность административной. Говоря об административной ответственности за нарушение правил охраны водных биологических ресурсов, следует обратить внимание на возрастание количества денежных средств, взысканных в бюджет в качестве административных штрафов [1]. Напрашивается вывод о том, что именно материальная ответственность становится основной при охране водных биологических ресурсов, она же представляется наиболее легкой и выгодной обеим сторонам.

Аналогичная тенденция существует и при назначении уголовных наказаний по ст. 257 УК РФ: в 2016 и 2018 гг. – это были штрафы, а в 2017 г. – обязательные работы.

Применение уголовно-правовых мер ответственности на практике осложнено проблемами, влияющими на возможность регулирования правопорядка. Первой проблемой является наличие пробелов в уголовном законодательстве, которое составляет правовую базу мер предупреждения и пресечения. Второй, более

сложной проблемой, влияющей на частоту применения указанных мер, является определенное пренебрежение к ним работников правоохранительных органов, а также уполномоченных лиц органов государственного контроля, надзора, охраны водных биологических ресурсов и среды их обитания.

Таким образом, встает задача по изменению собственных стереотипов при использовании указанных мер.

Рост числа правонарушений в сфере охраны водных биологических ресурсов свидетельствует о том, что существующая система мер административного принуждения и уголовно-правовой ответственности недостаточно эффективна.

Законодательное регулирование сохранения и защиты водных биологических ресурсов Российской Федерации направлено в основном на противодействие таким преступлениям, как незаконное строительство дамб и транспортировка древесины. Результатом подобных преступных деяний становятся загрязнение окружающей среды, уничтожение среды обитания водных растений и животных. К сожалению, последствия вредного воздействия редко принимаются во внимание законодательством России. Зачастую наказание за неправомерное использование водных биоресурсов и загрязнение окружающей среды не соответствует степени нанесенного ущерба. Установленные санкции в виде штрафа в размере до двухсот тысяч рублей, лишения права занимать определенные должности на срок до трех лет и исправительных работы на срок до двух лет, либо обязательные работы на срок до четырехсот восьмидесяти часов представляются слишком щадящими.

Подобные методы противодействия не останавливают потенциальных преступников и не воспринимаются ими всерьез, поскольку выгода, которую они получают за свою незаконную деятельность, в разы превышает наказание. Вместе с тем, мы считаем обоснованной практику принятия судами смягчающих об-

стоятельств в виде наличия у подсудимого детей, тяжелого материального положения, совершения преступления впервые и другие обстоятельства.

Непрекращающийся рост нарушений в области охраны водных биоресурсов по всей стране, преступные посягательства и намеренное уничтожение природных ресурсов с целью получения выгоды наносят непоправимый ущерб экологическим интересам государства. Принимая во внимание масштабы преступлений и охват территории их совершения, последствия подобных действий могут быть довольно плачевными. Ситуация требует введения более жестких уголовно-правовых санкций.

Представляется необходимым дополнить Уголовный кодекс Российской Федерации ст. 257 ч. 2, которая бы предусматривала уголовную ответственность за повторное совершение нарушения, предусмотренного ст. 8.38 КоАП «Нарушение правил охраны водных биологических ресурсов».

Различие уголовного и административного составов заключается в наступлении последствий: в случае административного состава – это угроза последствий в виде массовой гибели рыбы или других водных животных, а также уничтожение в значительных размерах кормовых запасов либо иные тяжкие последствия. Однако приведенная и проанализированная статистика относительно количества уголовных дел по ст. 257 УК РФ и количества правонарушений по ст. 8.38 КоАП позволяет сделать вывод, что в большинстве случаев правоохранительные органы не доказывают наличие ущерба водным биологическим ресурсам в виду сложности и трудозатратности данного процесса и привлекают виновных лиц вместо административной к уголовной ответственности. Таким образом, представляется целесообразным введение уголовной ответственности за повторное нарушение ст. 8.38 КоАП и привлечение к уголовной ответственности.

Подобный подход продемонстрирован законодателям в составах, предусмотренных ст.ст. 116.1, 151.1, 157, 158.1, 212.1, 215.4,

264.1 УК РФ. Введение административной преюдиции в рассматриваемом составе будет иметь профилактическое значение.

Анализ нормативных правовых актов и законов России, относящихся к сфере защиты водных биологических ресурсов, показал, что многие инструменты, используемые для достижения снижения уровня преступности, нуждаются в корректировке. Мы считаем, что работу в этом направлении необходимо начинать со сферы правого регулирования и правового воспитания, а также с приведения к общему порядку правил организации бизнеса, связанного с использованием биоресурсов.

Список литературы

1. Амирбеков К. И. К вопросу о подмене органами прокуратуры иных государственных органов // Законность. 2015. № 9. С. 40.

Иванцов С. В.[1],
профессор кафедры криминологии
Московского университета МВД России имени В.Я. Кикотя,
доктор юридических наук, профессор

Ломов И. Б.[2],
студент магистратуры
Международного юридического института

ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ В РОССИИ И СОВРЕМЕННЫЕ ТЕХНОЛОГИИ: ВЫЗОВЫ НОВОГО ВРЕМЕНИ

Невозможно недооценивать роль цифровых технологий в жизни современного Российского общества. Хотя процесс цифровизации в России был запущен несколько позже, нежели в большей части европейских государств, современный житель России во многом организует и выстраивает свою жизнь в том или ином объеме с помощью цифровых технологий. Подавляющее большинство работников получают заработную плату через банковские системы, практически все виды бизнеса имеют сайты в сети Интернет и используют специальное программное обеспечение в своей повседневной деятельности. Многие важные правовые и государственные процессы, такие как законодательный процесс, процесс организации государственного тендера или закупки, процессы, связанные с налогообложением, и многие другие имеют высокую степень автоматизации и происходят без использования бумажных носителей или с их минимальным участием. По многим признакам в основных лидирующих мировых государствах, в том числе и в Российской Федерации, сложилось такое явление, как общество цифровой эпохи.

Вместе с тем преступность как социальное явление тесно связана с общественными отношениями и необходимостью преступников «подстраиваться» под них – чем лучше преступник «адаптируется» под новые реалии общественной жизни, тем более он «успешен» и тем выше его шансы остаться безнаказанным. Конечно же, в этом правиле присутствует определенная зависимость. Чем более общественно опасно потенциальное преступное посягательство на охраняемые уголовным законом права и обязанности человека и гражданина, тем больших усилий по своей адаптации оно требует от преступников. Иными словами, такие сравнительно «простые» преступления как мошенничество, кража, грабеж (не связанные с цифровыми технологиями) не претерпели серьезных изменений за последнее столетие.

Совершенно иная ситуация складывается в сфере организованной профессиональной преступности. В данную категорию входят организованные группы, преступные сообщества и организации. Как правило, именно организованная преступность вне зависимости от страны ее происхождения ответственна за систематическое совершение самых общественно опасных преступлений, будь то преступления насильственного характера, направленные против жизни и здоровья, преступления против собственности, преступления, связанные с экономикой или с оборотом наркотиков или их прекурсоров. В отличие от преступников, которые могут совершать преступления из хулиганских побуждений, из-за бытовых причин, из-за спонтанно возникшего конфликта, членам организованной преступности традиционно приписываются профессиональные личностные качества преступников, такие как ориентированность на извлечение прибыли, правовой нигилизм, неуважение общества и государственной власти, наличие специальных навыков, используемых при совершении преступлений, и уважение к культуре преступного мира.

К условиям современного мира преступность в целом и организованная преступность, в частности, сумела адаптироваться,

причем получившееся в результате явление «цифровой» преступности имеет гораздо более выраженное отличие от преступности прошлого. Для оценки того, насколько перспективным для преступников является сфера цифровых технологий и коммуникаций, достаточно упомянуть, что в 2017 г. в комплексном аналитическом обзоре Научно-исследовательского института МВД России доля преступлений в сфере компьютерной информации оценивалась всего в 0.3 % (наиболее популярными являлись преступления экономического характера и связанные с оборотом наркотиков) от остальных преступлений, совершаемых организованной преступностью [1], а данные о преступности в целом в данной сфере даже не включались в краткие ежегодные сводки МВД. Вместе с тем 2017 г. также является отправной точкой для правильной статистической оценки динамики развития преступности в сфере информационных технологий, ведь исходя из ежегодных отчетов о состоянии преступности МВД России, по сравнению с 2017 г. в 2018 г. было зафиксировано на 92.8 % больше преступлений в рассматриваемой сфере. Увеличение количества преступлений практически в два раза само по себе является феноменальной цифрой, но дальше – больше.

В 2019 г. (по сравнению с 2018 г.) рост несколько остановился, но все еще оставался достаточно значительным, ведь речь идет о 68.5 %, в 2020 г. (по сравнению с 2019 г.) рост составил 73.4 %. Сравнивая показатели 2017 г. с 2020 г., можно отметить, что общий процентный рост преступлений, совершенных с помощью информационно-коммуникационных технологий составил 563 % [2]. Такое колоссальное значение наглядно показывает, в каком направлении преступность развивалась, развивается и, скорее всего, будет развиваться в будущем, если не принять должные меры.

Конечно же, сомнительным представляется идея того, что в данной сфере преступность повышает активность только с 2017 г. Более разумным является идея о том, что кроме достаточно

длительной деятельности в данной сфере, отдельные яркие примеры которой можно найти, начиная с 2013 г. (а некоторые даже ранее), такая цифра является результатом как повышения привлекательности данной сферы, так и активизации деятельности правоохранительных органов в ней же, что и привело к такому значительному увеличению, ведь до этого многие всерьез считали, что сфера сети Интернет является свободным пространством, что частично оправдывалось достаточно ограниченным вниманием правоохранительных органов к действиям граждан в глобальной сети, недостатком как технологического уровня их развития, так и отсутствием во многом надлежащей правовой основы, исключающей системную правоприменительную практику.

Кроме того, в связи с использованием особых технологий в ходе своей деятельности высокоразвитая преступность пользуется преимуществами высокой латентности, анонимности и обезличенности, о чем более подробно будет описано далее в данной работе [3]. Нельзя также вкратце не упомянуть, что подавляющее большинство преступлений, которые и составляют данную статистику, представляют из себя кражи и мошенничества (в 2019 г. мошенничества и кражи составляли 80 % от общего числа преступлений, в 2020 г. – 80.4 %, при этом в 2019 и 2020 гг. в среднем половина подобных преступлений относилась к категориям тяжких или особо тяжких), которые совершены, как правило, непрофессиональными преступниками на относительно невысоком технологическом уровне. В эту категорию попадают телефонные мошенники, лица, рассылающие фишинговые ссылки, простое вредоносное программное обеспечение, рекламные программы и иные преступления, которые хотя и совершены с использованием компьютеров, коммуникаций и сетевых технологий, но имеют сравнительно невысокий уровень технологической составляющей [4].

Предметом же интереса данной статьи являются наиболее технологически комплексные формы преступности, в том числе

организованной, а также технологии, применяемые ими в процессе своей деятельности. Для начала стоит поговорить о том, почему подобная преступность обладает столь высоким уровнем латентности и в некоторой степени безнаказанности. Основными причинами данных свойств является существование таких явлений, как даркнет (от англ. DarkNet – «скрытая сеть», «темная сеть» или «теневая сеть») и криптовалюта. Глубинный интернет (от англ. deep web) является отдельным уровнем сети, представляющим из себя систему связей и туннелей, формируемых между доверенными пользователями или компьютерами и с использованием специальных протоколов, предоставляя пользователям повышенный уровень анонимности, что обеспечивается невозможностью получения конкретной и достоверной информации с помощью специальных технических средств, в отличие от обычного интернета, в котором с помощью определенных средств можно получить достаточно полную информацию о конкретном компьютере или человеке.

По сути, глубинный интернет является децентрализованным аналогом обычного интернета, получить доступ к которому с помощью обычных браузеров нельзя. Тем не менее существуют специальные программы и браузеры (TOR), которые способны заходить на сайты формата «onion» или «.i2p», а также на другие, используемые в данных сетях. Многие из этих программ находятся в свободном доступе, соответственно давая возможность практически любому владельцу персонального компьютера или иного устройства с базовыми навыками получить доступ к глубинному интернету.

Исходя из исследований британских специалистов по кибербезопасности, из 5 200 сайтов работающими были 2 700, на 1 500 из которых находился запрещенный контент. В подобных сетях организуются онлайн-площадки, занимающиеся продажей наркотиков и их прекурсоров, оружия, поддельных документов и удостоверений, распространением детской порнографии. Одним

из наиболее существенных явлений, являющихся результатом деятельности непосредственно организованной преступности в России, является существование крупных онлайн-площадок по продаже наркотиков, которые по некоторым оценкам полностью изменили рынок наркотических веществ России.

Одними из самых крупных проектов в данной сфере являются RAMP (Russian Anonymous Marketplace) и Hydra. В то время как RAMP, исходя из заявления МВД, был ликвидирован в 2013 г., Hydra продолжает существовать и является самой крупной закрытой интернет-площадкой по распространению наркотических средств. Площадка работает по следующему принципу: администрация площадки предоставляет возможность магазинам арендовать место на ресурсе для размещения своих объявлений, взамен этого магазины платят администрации как за саму аренду, так и определенный процент от продаж. Сама администрация Hydra кроме предоставления мест имеет в своей внутренней структуре специализированные отделы, занимающиеся разными задачами, такими как специализированная реклама, использование SMM-технологий для рекламы наркотических средств в социальных сетях, мессенджерах, имеет свою наркологическую службу, в которой работают специалисты с медицинским образованием [5].

По оценкам расследования проекта Lenta.ru, произведенном в 2019 г., за три года своей деятельности аудитория Hydra составила 800 000 жителей России, наркокурьеры ежедневно устанавливали тайники с наркотическими веществами на сумму 227 млн руб., рекламные компании в социальных пространствах имели бюджеты в миллиарды рублей и все это в условиях практически полной и абсолютной безнаказанности. В 2017 г. Hydra смогла продвинуть свою рекламу в сервис YouTube через систему Google AdWords, а затем повторно в том же году и еще один раз в 2018 г. С 2016 г. Hydra занимается массовой рассылкой рекламы в мессенджерах WhatsApp и Viber. По самым разным оценкам, суммарный доход площадки за год может составлять десятки

миллиардов рублей, а в 2018 г. Hydra потратила один миллиард рублей на маркетинг [7]. Не вызывает сомнения то, что такие образования, как Hydra являются примером высшего уровня организации преступности в сфере современных технологий, в которой присутствует сплоченность, внутренняя иерархия, разделение на специальные подразделения, что нельзя квалифицировать иначе, как преступное сообщество.

Основными факторами, создающими проблемы при борьбе с данным явлением, составляет оперирование в глубинном интернете, что само по себе усложняет возможности по контролю и получению информации правоохранительными органами (хотя нельзя не отметить, что достаточный процент активности находится за пределами полностью анонимного пространства), так же факт того, что по сути значительный процент деятельности по продаже наркотиков осуществляет не сама Hydra, а магазины, арендующие у нее место. Соответственно, при задержании курьера в процессе доставки наркотических веществ либо даже при успешном пресечении деятельности самого магазина никакого существенного вреда самой площадке Hydra это не приносит. Такие ресурсы оперируют гигантскими финансовыми потоками, почти все эти деньги проходят мимо внимания надзорных органов, ведь все операции осуществляются с использованием следующего предмета обсуждения данной статьи, а именно криптовалют.

Криптовалюта представляет из себя квазифинансовое средство платежа, являющееся по сути набором компьютерной информации, не имея при этом конкретного физического или цифрового формата. Из-за особенностей передачи информации при осуществлении платежа с помощью криптовалют обеспечивается исключительно высокий уровень анонимности участников транзакции, более того, данную транзакцию невозможно перехватить, отменить (как правило), а при желании ее детали можно скрыть без возможности выявления адреса либо отправителя, либо полу-

чателя. Существуют разные виды криптовалюты (Bitcoin, Etherium, Dogecoin и многие другие), все они работают по примерно схожим общим принципам, в частности, существует возможность хранить практически неограниченное количество криптовалюты на так называемых холодных носителях – внешних устройствах хранения информации, при этом в данной ситуации не существует никакой возможности либо отследить, либо установить местонахождение подобных средств, ведь они ни в каком виде не внедрены в электронные сети.

Практический каждый человек, имеющий компьютер, может производить криптовалюту путем ее *майнинга* – добыча путем использования вычислительной мощи своего устройства либо путем создания майнинг ферм, т. е. целой сети компьютеров, оптимизированной сугубо под процесс добычи криптовалюты. Также существует множество сетевых бирж, готовых обменивать реальные деньги на криптовалюту, либо одну криптовалюту на другую, а также целые криптовалютные онлайн-банки (а иногда и вполне реальные банковские организации), предоставляющие схожие с банками услуги. Криптовалюта снискала определенную популярность как в России, так и во всем мире. Ярким признаком этого является кризис продукции на рынке графических процессоров для компьютеров, которые в основном используются для производства криптовалют, когда практически все запасы процессоров скупаются лицами, занимающимися майнингом, а обычному пользователю товара не остается.

Проблемой является также вопрос правового статуса криптовалюты. Несмотря на то, что данное финансовое средство не предоставляет никаких практических преимуществ законопослушному гражданину и используется в полном функционале в основном, в лучшем случае, при осуществлении полулегальных операций, для сокрытия средств при банкротстве или для манипулирования рынком, а в худшем случае для финансирования международного терроризма и совершения множества цифровых

преступлений на регулярной основе, мировые государства не спешат строго регулировать оборот криптовалюты, а некоторые (например, Япония), наоборот, движутся в сторону ее легализации.

В Российской Федерации криптовалюта на данной момент находится вне сферы правового регулирования. Не существует нормативного правового акта, который определял бы правовое понятие криптовалюты либо объектом нормативного регулирования которого была бы криптовалюта. Существует ограниченная правовая практика, осуществляемая отдельными органами судебной власти и прокуратуры, согласно которой использование криптовалюты в качестве средства платежа либо обмен криптовалюты на реальные денежные средства образуют диспозицию состава преступления отдельных статей Уголовного кодекса Российской Федерации, в частности, ст. 172 «Незаконная банковская деятельность», а в одном из своих разъяснений в 2017 г. прокуратура Свердловской области выразила мнение о том, что использование криптовалюты в сделках напрямую связано с легализацией доходов, полученных преступным путем и финансированием терроризма.

В период с 2013 по 2020 гг. никаких правовых продвижений в данном вопросе не было, однако в указанный период множество должностных лиц и видных деятелей различных отраслей высказывали свое мнение по этому вопросу. В 2017 г. заместитель министра финансов заявил, что Министерство финансов решило «не торопиться» с введением уголовной ответственности за использование криптовалют, в 2016 г. ФНС опубликовало письмо, в котором высказало мнение о том, что с точки зрения ведомства операции с криптовалютой являются валютными операциями, так как отсутствует прямой запрет, а также правовое определение понятий «денежный суррогат» или «виртуальная валюта», фактически признав наличие существенных пробелов отечественного законодательства в правовом регулировании электронных средств платежа,

то есть продемонстрировав наглядный пример того, как национальная система права не соответствует уже сложившимся и устоявшимся особенностям функционирования цифрового общества.

С точки зрения авторов, криптовалюту, несомненно, стоит рассматривать в первую очередь как инструмент совершения преступлений и уклонения от уголовной ответственности. Обычному законопослушному гражданину криптовалюта не предоставляет абсолютно никаких преимуществ, а все его потребности в совершении денежных операций, получении зарплаты либо иные нужды полностью удовлетворяются системами электронных платежей (МИР, Visa, MasterCard и т. д.). В то же время криптовалюта является не только исключительным способом осуществления операций в глубинном интернете при покупке наркотиков, оружия, организации заказных убийств, методом осуществления уклонения от уплаты налогов в реальном мире, при легализации денежных средств, добытых преступным путем, при сокрытии имущества, но и критически важной основной существования таких крайне опасных вызовов правовому государству, как Hydra, в случае с которой криптовалюта является жизненно необходимым залогом выживания высокоорганизованных преступников.

Проводя аналогии между криптовалютой и иными объектами реального мира, некую схожесть с неотслеживаемым средством платежа имеют оружие без серийного номера, автомобиль без государственного регистрационного знака, маска или перчатки у человека, ведь все это преследует в реальном применении исключительную цель – остаться анонимным и скрыть свою личность, что является теоретической основой поведения лица, занимающегося не совсем легальной деятельностью.

Делая общие выводы из вышесказанного и подводя итоги, с сожалением можно сказать, что на данный момент те самые вызовы нового времени, указанные в названии работы, остаются в большей степени нерешенными. Организованная преступность

сумела полностью поставить под контроль значительную долю рынка наркотиков в России, придумав инновационный метод их распространения с привлечением PR и SMM-технологий, в первую очередь направленный на молодое поколение, таким образом создавая непосредственную угрозу благополучию гражданского общества и будущего государства. Не вызывает сомнения то, что без принятия надлежащих правовых мер ситуация сама по себе не только не разрешится, но и продолжит развиваться, вовлекая все больше участников в пагубный процесс распространения и потребления наркотиков, образуя все больше коррупционных связей и приводя к увеличивающемуся количеству жертв. Тем не менее, нельзя не отметить и то, что в вопросах любых изменений в праве, будь то вопросы борьбы с анонимными интернет-площадками или вопросы регулирования криптовалюты, нельзя также принимать и поспешных решений. Необходимо убедиться, что принимаемые меры эффективны и не нарушают основных прав и свобод человека и гражданина, либо в случае их ограничения убедиться, что выгода от такого ограничения превышает все недостатки, а общественная опасность является достаточно серьезной.

Список литературы

1. Комплексный анализ состоянии преступности в Российской Федерации и расчетные варианты ее развития. М. : ВНИИ МВД России, 2018.

2. Состояние преступности в России за 2017 г. – 2020 г. (данные ГИАЦ МВД России) // Официальный сайт Министерства внутренних дел Российской Федерации. URL: мвд.рф/reports/1.

3. Актуальные проблемы предупреждения преступлений в сфере экономики, совершаемых с использованием информационно-телекоммуникационных сетей / [А. П. Суходолов и др.] // Всероссийский криминологический журнал. 2017. Т. 11. № 1. С. 13–21.

4. Иванцов С. В., Молчанова Т. В. Информационно-телекоммуникационные технологии – современная реальность // Вестник Санкт-Петербургского университета МВД России. 2020. № 4 (88). С. 89.

5. Laurent Gayard. Darknet: Geopolitics and Uses. Wiley, 2018. 196 p.

6. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / [С. В. Иванцов и др.] // Всероссийский криминологический журнал. 2019. Т. 13. № 1. С. 85–93.

7. Россия под наркотиками // Проект Лента.ру. URL: https://darknark.lenta.ru/article/part2-the-world-leader.

Кизилов А. П.[1],
старший преподаватель кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

Николаенко Д. Н.[2],
старший преподаватель кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук

Макошин П. В.[3],
преподаватель кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя

К ВОПРОСУ О ПРИЗНАКАХ ОПЕРАТИВНО-РАЗЫСКНОГО ВЗАИМОДЕЙСТВИЯ ПОДРАЗДЕЛЕНИЙ УГОЛОВНОГО РОЗЫСКА И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ В БОРЬБЕ С ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТЬЮ И ФАКТОРАХ, ЕГО ОБУСЛОВЛИВАЮЩИХ

Оперативно-разыскное взаимодействие в борьбе с преступностью, в том числе с организованными его формами имеет крайне важное значение. Основными звеньями данной цепочки

являются подразделения уголовного розыска (далее – УР) и экономической безопасности и противодействия коррупции (далее – ЭБиПК).

Одним из элементов, позволяющим определить сущность оперативно-разыскного взаимодействия подразделений УР и ЭБиПК при противодействии организованной преступности, являются факторы, его обусловливающие:

Общий объект оперативной заинтересованности. Им являются организованные группы, преступные сообщества (преступные организации).

Высокий уровень коррупции в органах государственной власти.

Данный фактор проявляется в том, что в то время, как одна из структур в значительной степени может быть поражена коррупцией и иметь соответствующие связи с курирующими ее оперативными подразделениями, сторонняя оперативная служба, не имея подобных связей и какой бы то ни было заинтересованности, способна оказать ей противодействие, взаимодействуя в данном направлении либо с некоррумпированной частью вышеуказанного субъекта, либо привлекая для этого иные сторонние силы и организации.

Многосубъектность оперативных подразделений ОВД и некоторая их структурная разобщенность при объективной необходимости комплексного выполнения стоящих перед ними задач в сфере противодействия ОПФ. Любое из оперативных подразделений ОВД в связи с осуществлением своей служебной деятельности располагает оперативной информацией относительно функционирующих ОПФ. Подобными данными не всегда могут обладать иные субъекты, занимающиеся оперативной работой, и в чьи служебные обязанности входит борьба с организованными формами преступной деятельности. Также у каждого оперативного подразделения есть свои специфические силы и средства для решения поставленных перед ними задач.

Обостренная политическая ситуация в ряде регионов России.

Под воздействием данного фактора совершаются различные уголовные преступления, притом, что подобные процессы нередко обличаются в организованную форму, которая имеет свои источники финансирования и преследует вполне конкретные цели: от дестабилизации общественной обстановки внутри страны до получения каких-либо материальных преференций. Данный фактор в настоящее время ярко себя проявляет в активизации деятельности молодежных неформальных организаций, проповедующих идеи расовой нетерпимости, осуществления убийств ряда религиозных деятелей и совершения террористических актов [1].

Правовая регламентация рассматриваемой согласованной деятельности. Определяет общность поставленных перед подразделениями УР и ЭБиПК задач по борьбе с ОПГ. Также приходится отмечать, что деятельность рассматриваемых оперативных подразделений регулируется едиными нормативными документами, регламентирующими организацию и тактику их оперативно-служебной деятельности.

Следует признать, что подразделения УР и ЭБиПК обладают не одинаковым правовым положением, ввиду некоторого различия в силах, средствах, тактике и методике оперативной работы, а также специфике их применения. Также нужно отметить, что, решая задачи борьбы с преступностью, каждое из взаимодействующих подразделений УР и ЭБиПК реализует вполне конкретные и четко определенные ему законодательством и ведомственными нормативными правовыми актами функции, за реализацию которых и несет ответственность. Данный тезис свидетельствует о том, что в ходе осуществления взаимодействия постоянно возникает необходимость выделения субъекта, занимающего, в известной мере, лидирующее положение и осуществляющего руководство и управление силами и средствами взаимодействующих

подразделений. При выполнении промежуточных задач роль лидирующего субъекта управления взаимодействием может варьироваться.

Оперативно-разыскное взаимодействие подразделений УР и ЭБиПК имеет ряд характерных черт (признаков), которые проявляются при его осуществлении и к которым, в свою очередь, предъявляются определенные требования. Применительно к теме исследования, наиболее актуальным нам представляется деление данных черт (признаков) на четыре группы.

К первой группе черт (признаков) необходимо отнести конфликтный характер ситуаций, связанный с активным противодействием организованных преступных формирований оперативным подразделениям, которое заключается в стремлении их членов нарушить, затруднить или заблокировать оперативно-разыскное взаимодействие подразделений УР и ЭБиПК, снизить согласованность в действиях их сил и средств, а, следовательно, и их оперативные возможности. Данное противодействие может осуществляться путем подкупа должностных лиц и сотрудников правоохранительных органов; осуществления вербовки и контрвербовки членов преступных организаций в правоохранительные органы; физического давления (вплоть до устранения) на сотрудников указанных оперативных подразделений, членов их семей, а также свидетелей и очевидцев преступлений.

В данных обстоятельствах требования, предъявляемые к совместной согласованной деятельности рассматриваемых оперативных подразделений, представляют собой, во-первых, обеспечение его устойчивости, а во-вторых, наличие достаточности сил, средств и методов для эффективного противодействия преступным формированиям. Устойчивость данного взаимодействия должна достигаться постоянной и непрерывной согласованностью их действий, а также способностью выполнять поставленные перед ними задачи в любых условиях изменяющейся обстановки. Достаточность сил и средств должна определяться таким

количественно-качественным их составом, который обеспечивает эффективное противодействие организованной преступности. При этом достаточность не может быть определена однозначно по всем регионам Российской Федерации и безотносительно к временному периоду функционирования. Поэтому она будет варьироваться в зависимости от данных факторов.

Ко второй группе признаков следует отнести повышенную общественную опасность организованной преступной деятельности и ее высокую латентность. Данные черты предопределяют такие важные требования к взаимодействию подразделений уголовного розыска и экономической безопасности и противодействия коррупции, как непрерывность, целенаправленность, активность, скрытность и четкость. Непрерывность достигается за счет твердости и устойчивости управления и постоянного взаимного обмена информацией между взаимодействующими оперативными подразделениями. Целенаправленность взаимодействия предусматривает необходимость его организации в интересах подразделений, решающих основную задачу. Активность заключается в настойчивом и решительном проведении оперативно-разыскных мероприятий и иных предпринимаемых взаимодействующими субъектами отдельных действий. Скрытность взаимодействия обеспечивается надежной взаимной защитой получаемой информации, а также ограничением круга лиц, имеющих к ней доступ. Четкость организации и поддержания взаимодействия состоит в строгом распределении частных задач между его субъектами, в соответствии с их предназначением и возможностями, а также в обеспечении своевременного и точного их выполнения.

Третьей группой признаков, определяющих рассматриваемое взаимодействие, является высокий динамизм организованной преступной деятельности и неравномерность ее развития. Эти обстоятельства определяют сложный и быстро меняющийся

характер оперативной обстановки, в которой приходится действовать подразделениям УР и ЭБиПК. Данные черты предопределяют такие требования к исследуемому оперативно-разыскному взаимодействию, как гибкость и централизация.

Гибкость заключается в сохранении согласованности в действиях субъектов взаимодействия в условиях высокодинамичной и быстроменяющейся обстановки. При этом она должна обеспечиваться возможностью своевременного уточнения или изменения хода осуществляемых взаимодействующими подразделениями согласованных действий при решении задач борьбы с организованной преступностью на основании результатов предыдущих действий, реакции на них членов организованных преступных формирований, а также вследствие иных изменений оперативной обстановки.

Централизация оперативно-разыскного взаимодействия предполагает наличие единого органа (руководящего субъекта), который осуществляет управление и координацию действий разнородных сил и средств подразделений УР и ЭБиПК по единому замыслу и плану. В качестве единого органа (руководящего субъекта) должен выступать заместитель начальника полиции по оперативной работе либо начальник полиции соответствующего органа внутренних дел. В случае осуществления взаимодействия в рамках совместных групп оперативной разработки в качестве руководящего субъекта может дополнительно выступать и оперативный сотрудник, являющийся старшим данной группы, в чьем производстве находится дело оперативного учета.

Четвертая группа признаков взаимодействия рассматриваемых оперативных подразделений определяется недостаточностью нормативного правого обеспечения данной совместной согласованной деятельности и непонимание многими оперативными сотрудниками ее необходимости. В рамках данной группы черт требования к исследуемому взаимодействию, представляют собой необхо-

димость принятия мер по нормативному обеспечению данной согласованной деятельности, а также проведению систематичной и последовательной работы по повышению уровня подготовленности сотрудников данных оперативных подразделений в ключе понимания ими ее важности и востребованности.

Таковы, на наш взгляд, основные признаки рассматриваемой совместной согласованной деятельности и факторы, ее обусловливающие.

Список литературы

1. Национальная политика России: история и современность / сост. Н. И. Наумова. М. : Русский мир, 1997.

2. Здравомыслов А. Г. Межнациональные конфликты в постсоветском пространстве. М. : Аспект-пресс, 1997. 285 с.

3. Гаджиев К. С. Геополитика : учебник. 4-е изд., перераб. и доп. М. : Юрайт, 2011.

4. Авксентьев В. А. Этнические конфликты: история и типология // Социологические исследования. 1996. № 12.

5. Гельвановский М. Россия на пути к нормальной хозяйственной системе // Общественные науки и современность. 1993. № 5.

7. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [А. В. Богданов и др.]. 5-е изд., перераб. и доп. М., 2020.

6. Кузьмин Н. А., Чикова Я. Н., Завьялов И. А. Противодействие органов внутренних дел преступлениям в сфере незаконного оборота наркотиков с использованием возможностей Интерпола // Вестник экономической безопасности. 2015. № 7. С. 67–71.

7. Богданов А. В., Завьялов И. А., Хазов Е. Н. Противодействие организованной преступности в сфере экономики // Криминологический журнал. 2020. № 2. С. 91–100.

8. Михайлов Б. П., Воронцов А. В., Завьялов И. А. Особенности криминальной среды России // Вестник Московского университета МВД России. 2013. № 6. С. 186–190.

Кузьмин Н. А.[1],
начальник кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
доктор юридических наук, доцент

О СОВЕРШЕНСТВОВАНИИ ПОДГОТОВКИ КАДРОВ ДЛЯ ОПЕРАТИВНЫХ ПОДРАЗДЕЛЕНИЙ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В современных условиях деятельности оперативных подразделений ОВД основное внимание уделяется подготовке высококвалифицированных кадров, отвечающих современным требованиям по уровню профессиональной подготовки и развитию профессионально-значимых качеств.

В условиях новых вызовов и угроз, стоящих перед оперативными подразделениями по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в Московском университете МВД России имени В.Я. Кикотя совершенствуется система подготовки кадров.

На профильном факультете подготовки сотрудников для оперативных подразделений полиции, выпускники которого пополняют состав подразделений уголовного розыска, подразделений по контролю за оборотом наркотиков, подразделений по противодействию экстремизму, подразделений экономической безопасности и противодействия коррупции, благодаря тесно налаженному взаимодействию с практическими подразделениями наших основных комплектующих подразделений-заказчиков кад-

ров – ГУ МВД России по г. Москве и ГУ МВД России по Московской области, а также подразделениями центрального аппарата постоянно наращивается практическая составляющая обучения.

Так, в целях формирования у обучающихся специальных компетенций успешно реализуется комплекс дисциплин-практикумов, направленный на выработку у курсантов и слушателей профессионально-значимых навыков служебной деятельности оперуполномоченного полиции.

Преподавание дисциплин-практикумов, производных от учебного курса «Оперативно-разыскная деятельность органов внутренних дел», к которым относятся: «Практикум по борьбе с преступлениями в сфере незаконного оборота наркотиков»; «Деятельность оперативных сотрудников уголовного розыска в ходе досудебного производства по уголовным делам»; «Выявление и раскрытие преступлений с использованием современных технических средств»; «Практикум по документированию действий лиц, совершающих преступления»; «Практикум по оперативно-разыскной психологии», позволяет сформировать у курсантов и слушателей навыки работы оперуполномоченного с учетами органов внутренних дел и иных организаций; осуществления оперативно-разыскного производства по делам оперативного учета; документирования действий лиц, представляющих оперативный интерес, организации содействия граждан органам внутренних дел; организации и тактики розыска лиц, пропавших без вести, скрывшихся от органов дознания, следствия и суда, установления личности граждан по неопознанным трупам и другие.

Особое место среди дисциплин-практикумов занимает дисциплина «Выявление и раскрытие преступлений с использованием современных технических средств», которая формирует у курсантов навыки работы с системой АПК «Безопасный город» и раскрытия с ее помощью преступлений. Также в рамках этого спецкурса формируются навыки использования цифровых мобильных устройств при выявлении и раскрытии преступлений,

изучаются механизмы следообразования при работе с цифровыми мобильными устройствами, порядок изъятия оперуполномоченным различных технических устройств, с сохранением на них исходной информации и другие вопросы.

Заключительным этапом практико-ориентированного подхода в обучении является проведение государственной итоговой аттестации, которая в университете проводится в виде комплексного междисциплинарного экзамена в форме учений, где выпускники наряду с теоретическими знаниями демонстрируют практические умения и навыки деятельности оперативного сотрудника.

В рамках совершенствования подготовки оперативных сотрудников полиции по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в рамках реализации набора 2021 г. в университете были сохранены все показавшие свою эффективность и успешно апробированные в учебном процессе элементы, а также усилена подготовка специалистов для оперативных подразделений полиции по следующим направлениям.

Во-первых, была изменена структура дисциплины «Оперативно-разыскная деятельность ОВД». Произошло увеличение аудиторных часов с 32 до 68, отводимых на рассмотрение тематики борьбы с преступлениями, совершаемыми с использованием информационно-телекоммуникационных технологий.

Во-вторых, были введены новые дисциплины специализации, призванные расширить специальную подготовку по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий: «Организация поиска оперативно-значимой информации в сети Интернет»; «Практикум по борьбе с преступлениями в сфере незаконного оборота наркотиков, совершаемых с использованием информационно-телекоммуникационных технологий»; «Практикум по квалификации отдельных видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий»; «Практикум по проведению отдельных следственных действий по

преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий», «Тренинг комплексного моделирования оперативно-служебной деятельности по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий».

В-третьих, были введены дисциплины, позволяющие курсантам более углубленно овладеть технической стороной выявления и раскрытия преступлений в сфере высоких технологий, в частности, была введена дисциплина «Информационно-техническое обеспечение раскрытия преступлений, совершаемых с использованием информационно-телекоммуникационных технологий». Также были введены дисциплины, расширяющие базовые представления обучающихся в области информационной безопасности и киберпреступности: «Основы кибербезопасности», «Информационное право», «Киберпреступность в финансово-кредитной сфере».

В-четвертых, в 2021 г. в университете были проведены киберучения, в которых приняли участие практические сотрудники, а также представители стратегических партнеров университета, к которым относятся ПАО «СберБанк», АО «Лаборатория Касперского», компания BI.ZONE, Международная платежная система Master Card. Это комплексные межкафедеральные учения, на которых комплексно отрабатывалась вводная по раскрытию хищений денежных средств путем подключения внешнего электронного устройства к программному обеспечению устройства самообслуживания. Результаты действий следственно-оперативной группы оценивали ведущие специалисты практических подразделений по данной линии работы, а также вышеназванных стратегических партнеров университета.

Стоит подчеркнуть, что данная система подготовки в совокупности с введением в эксплуатацию дополнительного спектра специализированных полигонов позволит нам осуществлять подготовку специалистов для оперативных подразделений полиции, отвечающих современным требованиям.

Любан В. Г.[1],
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

АНАЛИЗ ОПЕРАТИВНОЙ ОБСТАНОВКИ В СФЕРЕ КРИПТОПРЕСТУПЛЕНИЙ

В современном мире использование криптовалют приобретает все более широкое распространение. Наблюдается активное развитие блокчейн-технологий и самого криптовалютного пространства. Технические инновации и быстро развивающаяся новая торговая парадигма продолжают привлекать все большее количество людей. А криптовалюты хорошо себя зарекомендовали не только как способ вложения средств, но и как расчетная единица, позволяющая проводить финансовые операции без контроля со стороны государства.

При этом правовой режим криптовалют значительно различается в разных странах. В одних странах их признают инвестиционным активом или товаром, в других – платежной единицей, в-третьих объявляют вне закона. В каких-то государствах и вовсе сталкиваются противоположные подходы к легализации криптовалюты. Так, правительство Китая запретило проведение операций с Bitcoin и другими цифровыми деньгами финансовым учреждениям, но разрешило вести эту деятельность частным лицам [1]. В Швейцарии криптовалюта приравнена в правах к традиционным иностранным валютам. В Эквадоре, Киргизии, Ливане, Таиланде, Боливии, Исландии, Индонезии, Вьетнаме транзакции с использованием цифровых денег находятся под запретом, хотя майнинг законом не преследуется. В Сингапуре выпущены в обращение специальные платежные карты для хранения криптовалюты и удобного способа расчета цифровыми деньгами.

В большинстве государств с развитой экономикой криптовалюта в целом признана, а нормативная правовая база для ее внедрения в реальный сектор экономики официально разработана и принята. К таким странам относятся США, Великобритания, Южная Корея, Канада, Израиль, Дания, Франция, Кипр, Австралия, Новая Зеландия, Германия, Гонконг, Италия, Япония, Норвегия, Чехия, Сингапур, Швейцария и многие другие [2].

Однако такой рост экономической ценности и переход на новый профиль деятельности имеют и негативные стороны в виде появления целого направления криптопреступности. Под криптопреступностью сегодня понимается совокупность обладающих едиными системными свойствами деяний, совершаемых в отношении виртуальной валюты либо с ее использованием [3; с. 87]. Но поскольку данное явление находится в стадии своей институционализации, применение этого термина носит достаточно условный характер.

Анализ оперативной обстановки позволяет судить, что преступность на фоне осведомленности о формах, методах, силах и средствах оперативно-разыскной деятельности все динамичнее использует неограниченные возможности сети Интернет, эксплуатируя особенности его технического построения и функционирования, в том числе по вопросам оборота денежных средств и цифровых финансовых активов. Как показывает проведенное исследование, появление многочисленных программных решений, современных технических средств и способов анонимизации личности пользователей сети Интернет обеспечило достаточный уровень безопасности субъектов криптопреступлений, посредством сокрытия следов их противоправной деятельности. Современная криптопреступность отличается тем, что ее организаторы и участники нередко находятся за пределами страны совершения преступлений. Однако имеющиеся платежные инструменты позволяют им дистанционно управлять заданными процессами, перемещая полученные от криптопреступности финансовые средства из одной точки мира в другую, размещая их на различных

криптоплощадках с целью легализации, сохранения, извлечения дополнительной прибыли или последующего обналичивания. Отсутствие прямого контакта между преступником и потерпевшим делает выявление, раскрытие и расследование криптопреступлений чрезвычайно затратным и трудоемким процессом.

Так, с 2015 г. в Российской Федерации и ряде стран СНГ, таких как Украина, Беларусь, Казахстан, Азербайджан, Армения, Киргизия, Узбекистан, Таджикистан и Молдавия, заработала крупнейшая торговая интернет-площадка «Гидра» (от англ. Hydra), размещающая только в российском сегменте более 3 000 интернет-магазинов, предлагающих запрещенный контент. По подсчетам специалистов, с 2016 по 2019 гг. пользователи внесли на «Гидру» 64,7 млрд руб. [4]. Доступ на маркетплейс «Гидра» возможен только в даркнете [5] и осуществляется через TOR-браузер. Сделки и оплата происходят непосредственно на площадке, а сама оплата производится с использованием различных криптовалют, но преимущественно через биткоин. Площадка охватывает все сферы теневого бизнеса, включая продажу наркотиков, оружия, фальшивых денег, персональных данных, поддельных документов, банковских карт, оформленных на подставных лиц, специальных технических средств для негласного слежения и съема информации, поиск заказчиками исполнителей планируемого преступления, а также предоставление различных информационных услуг.

Кроме того, для совершения криптопреступлений активно используется сквозное шифрование [6], IP-телефония, анонимные мессенджеры, интернет-магазины, специализированные закрытые форумы, а также электронные платежные системы. Посредством таких интернет-мессенджеров, как WhatsApp, Telegram, Signal, Wickr, Threema, Briar, Confide, Dust и других, использующих технологию сквозного шифрования (E2EE), осуществляется организация и координация преступных действий, общение членов преступных формирований между собой и с другими лицами.

К сожалению, на сегодняшний день ГИАЦ МВД России не ведет отдельного учета преступлений, совершаемых с использованием и в отношении криптовалют. Тем не менее, анализ практики работы оперативных подразделений в этом направлении позволяет судить, что количественные показатели данных преступлений в целом сопоставимы с динамикой преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, учет которых ведется и представлен в открытой статистике органов внутренних дел.

Так, если в 2015 г. было зарегистрировано 43 816 преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, то в 2016 г. – 65 949, в 2017 г. – 90 587, в 2018 г. – 174 674, в 2019 г. – 294 409, а в 2020 г. – уже 510 396. Как видно, в течение шести лет количество зарегистрированных преступлений этой категории выросло почти в двенадцать раз. Что касается их раскрываемости, то она остается на низком уровне и не превышает в среднем по стране 19 %. Более глубокий анализ структуры данных преступлений позволяет прийти к выводу, что именно дистанционные хищения безналичных финансовых активов граждан, в числе которых выделяются кражи и мошенничества, занимают среди них «ядерную» часть – 80,4 %.

Так, по итогам 2020 г. доля мошенничеств составила почти половину от числа всех преступлений в сфере информационно-телекоммуникационных технологий – 41,2 %, а доля краж – 34 %. Особенно поражают темпы динамики роста дистанционных мошенничеств, количество которых за шесть лет с 2015 по 2021 гг. увеличилось в 15 раз. Так, если в 2015 г. было зарегистрировано 13 501 мошенничество, совершенное с использованием информационно-телекоммуникационных технологий (ст. 159 УК РФ), то в 2016 г. – 32 875, в 2017 г. – 51 513, в 2018 г. – 106 787, в 2019 г. – 136 709, а в 2020 г. – уже 210 493 мошенничеств. Для сравнения, по сведениям ГИАЦ МВД России, в 2020 г. в стране всего было зарегистрировано 335 631 преступлений по ст.ст. 159–159.6 УК РФ, раскрываемость которых составила 20,1 %.

Кражи (ст. 158 УК РФ) находятся на втором месте среди всех преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий. В 2015 г. таких краж было зарегистрировано 8 452, в 2016 г. – 9 762, в 2017 г. – только 6 945, в 2018 г. – уже 36 167, в 2019 г. – 98 798, а в 2020 г. – 173 416. По итогам 2020 г. количество зарегистрированных дистанционных краж возросло в два раза по сравнению с аналогичным периодом прошлого года и в пять раз по сравнению с аналогичным периодом позапрошлого года. Частично на позицию правоприменителя по определению уголовно-правовой квалификации деяний повлияло изменение взгляда высшего судебного органа на квалификацию мошенничеств и включение законодателем в ч. 3 ст. 158 УК РФ нового пункта «г», предусматривающего ответственность за кражу с банковского счета, а равно в отношении электронных денежных средств.

Вместе с тем, по мнению ряда специалистов-практиков, латентность дистанционных хищений безналичных денежных средств и криптовалют чрезвычайно высока и, по косвенным признакам, превышает в несколько раз сведения официальной статистики.

Дистанционные хищения, совершаемые с использованием или в отношении криптовалюты, относятся к категории технически сложных по замыслу и исполнению преступлений. Для их осуществления преступники часто объединяются в группы с четким распределением ролей в процессе подготовки и реализации преступного замысла. Организаторы и исполнители нередко обладают высокой квалификацией и глубокими знаниями в области информационных технологий, в том числе технологий блокчейна, психологии, банковского обслуживания, инвестиций цифровых финансовых активов, SMM-менеджмента и т. д. Поэтому органам внутренних дел особенно важно противопоставить их действиям своевременные и квалифицированные меры по выяв-

лению, пресечению и предупреждению преступных посягательств в этой сфере, их разоблачению и привлечению виновных к уголовной ответственности.

Исходя из оперативно-разыскной практики можно выделить четыре основных сектора криптопреступности:

– незаконная продажа предметов, веществ и продукции, свободная реализация которых запрещена либо оборот которых ограничен, а также иных запрещенных товаров, контента или услуг с использованием криптовалюты;

– преступления против собственности, совершаемые с использованием или в отношении криптовалюты, лидирующее место среди которых занимают хищения;

– легализация (отмывание) преступных доходов с использованием криптовалюты;

– финансирование террористической и экстремистской деятельности с использованием криптовалюты.

Из получивших на сегодняшний день наибольшее распространение преступлений, совершаемых с использованием или в отношении криптовалют, можно выделить:

– мошенничество в сфере криптовалютных инвест-проектов (ст.ст. 159, 171 УК РФ);

– мошенничество в сфере купли-продажи криптовалют (159 УК РФ);

– скрытый майнинг криптовалют с помощью вредоносного программного обеспечения – криптоджекинга[1] (ст.ст. 272, 273 УК РФ) [9];

– организация заказных убийств (ст. 105 УК РФ);

– коммерческий подкуп (ст. 204 УК РФ);

– дача и получение взятки (ст.ст. 290, 291 УК РФ);

[1] Криптоджекинг (от англ. cryptojacking – «вредоносный майнинг») – это заражение компьютерного оборудования пользователей (компьютеров, планшетов, мобильных телефонов) вредоносным программным обеспечением, которое использует их ресурсы для добычи (майнинга) электронных денег – криптовалют.

– сбыт наркотических средств и психотропных веществ (ст.ст. 228, 228.1 УК РФ);

– сбыт поддельных денег (ст. 186 УК РФ);

– сбыт оружия и боеприпасов (ст. 222 УК РФ);

– сбыт поддельных документов (ст. 327 УК РФ);

– реализация поддельных банковских платежных карт (ст. 187 УК РФ);

– легализация преступных доходов (ст.ст. 174, 174.1 УК РФ);

– финансирование терроризма (ст. 205.1 УК РФ) и др.

В заключении отметим, что данный перечень не является исчерпывающим и очевидно будет пополняться новыми уголовно-правовыми составами в процессе развития криптопреступности. К тому же, незавершенный процесс формирования правового режима самих криптовалют не только в России, но и в мире позволяет нам прогнозировать дальнейшее увеличение их роста в количественном и качественном выражении.

Список литературы

1. Правовой режим криптовалют // URL: https://ru.wikipedia.org/wiki/Правовой_режим_криптовалют.

2. Законодательство о криптовалюте – в России представили закон о криптовалютах // URL: https://conspi.ru/raznoe-2/zakonodatelstvo-o-kriptovalyute-v-rossii-predstavili-zakon-o-kriptovalyutax-gosekonomika-ekonomika-lenta-ru.html.

3. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции / [С. В. Иванцов и др.] // Всероссийский криминологический журнал. 2019. Т. 13. № 1. С. 87.

4. Дорожный А., Хачатурянц А. Вся эта дурь. Исследование о том, на чем сидит Россия // Интернет-издание «Проект». URL: https://www.proekt.media/research/narkotiki-v-darknete/?utm_-source=tlgrm&utm_medium=chnl&utm_campaign=dur.

5. URL: https://ru.wikipedia.org/wiki/Даркнет.

6. URL: https://ru.wikipedia.org/wiki/Сквозное_шифрование.

7. Общие сведения о состоянии преступности в России // Состояние преступности в России за январь–декабрь 2020 года. М. : ФКУ ГИАЦ МВД РФ, 2021.

8. Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_-doc_LAW_283918/.

9. Копелян А. Криптоджекинг (Cryptojacking) что за птица? // URL: https://habr.com/ru/post/535932/.

Мацкевич И. М.[1],
заведующей кафедры криминологии
и уголовно исполнительного права Московского государственного
юридического университета имени О.Е. Кутафина,
главный ученый секретарь
Высшей аттестационной комиссии при Минобрнауки России,
доктор юридических наук, профессор

ОРГАНИЗОВАННАЯ И НЕ ОРГАНИЗОВАННАЯ ПРЕСТУПНОСТЬ: НЕ МИРНОЕ СОСУЩЕСТВОВАНИЕ

В течение последних 10 лет я разрабатывал и в дальнейшем постоянно совершенствовал учебную программу для университета имени О.Е. Кутафина, которая называется «Проблемы борьбы с организованной преступностью». Преподавание курса студентам неизбежно сопровождалось непрерывным сбором материалов, что в конце концов привело к подготовке и опубликованию пособия с аналогичным курсу названием – «Проблемы борьбы с организованной преступностью», пособие подготовлено в соавторстве с опытным ученым Мариной Валериановной Королевой.

В процессе работы над пособием я понял, что организованная преступность прошла удивительные и многочисленные метаморфозы. Преступность существует в диалектическом и крайне неустойчивом положении, ее разрывают две противоположные внутренние тенденции, с одной стороны она стремится к самоорганизации и структурированию, с другой стороны, она по своей природе хаотичная и не укладывается ни в какие организованные рамки. Следуя известной поговорке, главари организованной преступности все время пытаются всех уверить, что организованной преступности не существует, что ее нет.

Проблема заключается в том, что преступность (увы) стала составным элементом общественной действительности, а организованная преступность – содержанием определенной негативной стороны общественной жизни. При этом убедив всех, что ее нет, и усыпив бдительность простых людей, которые, в отличие от главарей криминальной среды, разобщены и полагаются на политических руководителей, которых они избирают и на которых надеются, организованная преступность в новом XXI в. не спеша вписалась в структуру мировой действительности. Организованная преступность стала частью мировой цивилизации, как бы дико и парадоксально это не звучало. Подтверждение этого тезиса мы видим повсюду – от блатной тюремной музыки (которая транслируется и по радио, и по телевидению) до киноиндустрии, львиная доля которой приходится на фильмы о преступности и преступниках. Я считаю, что организованная преступность стала частью общества, и вопрос о том, почему культура, которую мы создали, породила преступность, и которую мы почему-то продолжаем называть цивилизованной, должен быть включен в повестку дня.

В настоящей статье я остановлюсь на нескольких ключевых моментах, навеянных в процессе работы над пособием, и тех мыслях, которые прямо не указаны в пособии, но предполагается, что они должны быть естественным следствием работы в борьбе с организованной преступностью.

Любой преступности даже в ее примитивных (условно) формах всегда свойственны (присущи) элементы организованности. Поскольку преступность есть побочное негативное следствие общественного устройства человеческого общества, оно, как и само общество, – организованно. В этом относительно легко убедиться, если изучать исторические документы, а также факты и свидетельства о преступности разных стран и разных эпох. Тот же Ванька Каин (Иван Осипов) был едва ли не первым в мире

самым настоящим мафиози (в современном понимании – руководитель мафии), который не только возглавлял различные преступные шайки Москвы и ее окрестностей, но и наладил устойчивые коррупционные связи с представителями государственной власти. Он же первый пострадал из-за того, что в какой-то момент попытался стать составной частью этой самой государственной власти.

Следовательно, организованная преступность конкурирует с государственной властью, но не может стать частью государственной власти.

Любая организованная система не может контролировать все процессы, которые существуют внутри нее, как системы. Преступность – это заранее не запланированное относительно прогнозируемое арифметическое множество отдельных преступлений, каждое из которых может либо не быть связанным с организованной преступностью, либо выйти из-под контроля организованной преступности. Поэтому организованность в преступности настолько же закономерна, насколько закономерна сама преступность, и настолько же хаотична, насколько хаотична преступность. Другими словами, общие тенденции в преступности и в организованной преступности должны совпадать.

Преступность явление настолько же закономерное, насколько случайными кажутся отдельные противоправные действия людей. О статистических свойствах преступности как массового явления говорил, как известно бельгийский математик и астроном Артур Жак Кетле. На эти же статистические закономерности указывал Александр Радищев (он не только раньше Кетле говорил об этом, но был более последователен, поскольку сопоставлял эти закономерности с общественным устройством современного ему мира). Позже статистические методы изучения преступности многократно использовались другими учеными и, как правило, результаты были схожими – преступность неизбежно подтверждала свои собственные закономерности. Следовательно, преступность,

а, значит, и преступления – это статистические единицы. Значит, они должны соответствовать математической логике. Не случайно формальным составам преступлений присущи математические закономерности. Об этом я говорил в своих статьях: «Математическое моделирование уголовного закона», «Геометрия уголовного закона», «Интеллектология права: предварительные итоги математического моделирования закона» [1].

Преступность кажется явлением хаотическим. В то же время организованная преступность в самом своем названии опровергает хаос. Но не кажется ли странным, если не удивительным, что, не имея никакого планового органа, организованная преступность регулярно складывается в относительно стройную систему из самых разрозненных элементов. Полагаю, что организованная преступность является одним из наглядных примеров так называемой хаотической системы. Хаотические системы, несмотря на название, являются детерминированными. В хаотических системах движение их элементов описывается строго определенными уравнениями и не подвержено воздействию случайных факторов. Отсюда вывод, что будущее развитие хаотической системы предопределено начальными условиями ее возникновения. Следовательно, хаотические системы в действительности совсем не хаотические, они имеют свои закономерности развития. Однако трудность предсказания движения хаотических систем делает их на практике похожими на случайные.

Понятие хаоса известно со времен Древней Греции (от др.-греч. χαίνω – раскрываюсь, разверзаюсь), где под ним понимали неупорядоченное состояние явлений в противовес упорядоченному космосу. Примечательно, что первым на особенности проявления хаоса обратил внимание древнегреческий поэт Гесиод, который утверждал, что хаос как наивысшее отрицание порождает исключительно негативные силы.

Сегодня отношение к хаосу менее однозначное. Например, в математике хаос используется для описания поведения нелинейных динамических систем, подверженных при определенных условиях динамическому хаосу. Появление такой модели кажется случайным, хотя математически доказано, что она детерминирована, т. е. не случайна. Таким образом, теория хаоса позволяет акцентировать внимание на особом характере изучаемого явления, которое по своим внешним проявлениям и внутреннему содержанию выглядит крайне непредсказуемым, а потому кажется очень неустойчивым.

Теория хаоса – это область междисциплинарных исследований, связывающих математику и физику. В теории хаоса принято использовать понятие аттрактора (от англ. attract – привлекать, притягивать), под которым понимается неограниченное множество состояний динамической системы, к каждому из которых эта система стремится максимально приблизиться с течением времени. Наиболее простыми вариантами аттрактора являются притягивающая неподвижная точка (например, точка трения в маятнике) и периодическая траектория (например, самовозбуждающиеся колебания с положительной обратной связью).

Примерами динамического хаоса являются: атмосфера (поэтому так трудно предсказать погоду); все социальные системы и, конечно, человеческое общество, как наивысший результат хаоса, детерминированная система, проявляющая себя как наивысшая самовоспроизводящая и саморазрушающаяся система.

Здесь можно было бы построить целую пирамиду ассоциаций, начиная от рождения вселенной и заканчивая апокалипсисом, но в данном случае важно другое – то, что с помощью теории хаоса можно изучать и человеческое общество и составляющие его элементы, одним из которых является преступность и ее наивысшая форма – организованная преступность.

Таким образом, из сказанного вытекают следующие выводы:

– общество можно изучать в том числе математическим моделированием, одним из вариантов которого является теория хаоса;

– раз это так, то и преступность, и особенно организованную преступность можно изучать такими же математическими способами.

Ключевым фактором в изучении любой хаотической системы, в том числе организованной преступности является время. Без понимания влияния временных факторов невозможно понять, насколько хаотическая система жива, насколько организованная преступность (ее конкретные формы и виды, например, сицилийская мафия или российские транснациональные организованные преступные объединения) устойчива и способна к мимикрированию (от англ. mimicry – подражание, маскирование).

Сложность заключается в том, что эти модели чрезвычайно подвижны и крайне неустойчивы. Организованная преступность как наивысшее социальное негативное проявление преступности является самой неустойчивой моделью. В то же время особенность этих неустойчивых моделей заключается в их постоянном, если не сказать неизбежном возобновлении и трансформировании. Можно сказать, что чем модель неустойчивее, тем она скорее возродится в случае ее ликвидации. Следовательно, неустойчивые модели, как это не парадоксально, более живучие модели.

В физике хаотическими могут быть и сложные, и простые системы. Примером простой системы может быть логистическое отображение, которое описывает изменение количества населения с течением времени. В другом примере простой системой будет клеточный аромат, т. е. набор клеток, образующих некоторую периодическую систему с заданными правилами перехода. Клеточный аромат является дискретной (от лат. discretus – разделенный, прерывистый) динамической системой, поведение которой полностью определяется локальными зависимыми условиями. При этом эволюция даже простых дискретных систем непосредственно зависит от начальных условий их возникновения.

Преступность – это простая хаотическая система, которая состоит из дискретных систем – преступлений.

Организованная преступность – это сложная хаотическая система.

Поскольку обе эти системы являются системами хаотическими, принципиальной разницы между ними нет. Обе эти системы крайне неустойчивы и крайне противоречивы.

Но поскольку эти хаотические системы отличаются друг от друга как простые и сложные системы – разница между ними колоссальная, и закономерности, проявляющиеся в преступности, могут либо по-другому проявиться в организованной преступности, либо не проявиться вовсе. Соответственно закономерности, присущие организованной преступности, отсутствуют в неорганизованной преступности.

Более того, простые и сложные хаотические системы не сосуществуют, они враждуют. Отсюда вечный конфликт преступности и организованной преступности, преступников и организованных преступников. Таким образом, преступность сама себя порождает, и сама себя уничтожает и вновь порождает. В том числе точно так же она ведет себя по отношению к организованной преступности – порождает, убивает и вновь ее возрождает.

Сложную хаотическую систему организованной преступности можно классифицировать на другие хаотические подсистемы:

– абсолютная организованная преступность;

– относительная организованная преступность;

– не очевидная организованная преступность.

Абсолютная организованная преступность – это наркотики, развлекательная индустрия (сексуальная и игровая), финансовая преступность, профессиональное устранение конкурентов.

Относительная организованная преступность – это экстремизм и терроризм.

Неочевидная организованная преступность – это профессиональные нищие, карманные и квартирные кражи.

Простая хаотическая система преступности состоит из неорганизованной преступности; неочевидной неорганизованной преступности; очевидной неорганизованной преступности

Неорганизованная преступность – это грабежи и разбои.

Неочевидная неорганизованная преступность – это преступления мигрантов и преступления против местных жителей как элемент их дискриминации, запугивания и вытеснения.

Очевидная неорганизованная преступность – это хулиганство и домашнее насилие.

Проявления борьбы сложной хаотической системы организованной преступности и простой хаотической системы преступности наблюдаются в местах лишения свободы; в среде профессиональных преступников; в судьбах рецидивистов.

Организованная преступность в местах лишения свободы посредством хаоса умело противостоит строгим официальным порядкам и одновременно борется с любыми проявлениями самостоятельности со стороны осужденных. При таких условиях нередко представители администрации исправительных учреждений предпочитают не замечать конфликтов в среде осужденных, надеясь, что эти конфликты будут разрешены без их участия.

Профессиональные преступники одновременно участвуют в двух хаотических системах (в организованной преступности и в простой преступности), реализуя на практике, сами того не подозревая, модель поведения хаотичной системы. Тем самым их поведение способствует внутреннему неразрешимому конфликту обоих систем – простой и сложной.

Рецидивная преступность является прямым продолжением борьбы организованной и неорганизованной преступности. Судьба рецидивиста определяется не только пробелами в работе служб социальной реабилитации, но в общей хаотичной модели организованной преступности, которая не может отпустить человека, который стал ее составным элементом в тот самый момент, когда он совершил преступление. Если простая хаотичная модель

преступности заинтересована в том, чтобы вовлекать в свою орбиту новых членов и, таким образом, скорее отпустит бывшего преступника, отбывшего наказание и желающего вернуться к обычной жизни, чем станет его удерживать, то модель хаотичной организованной преступности работает на безусловное удержание любого своего члена и не отпустит его от себя ни при каких условиях, кроме одного – смерти.

Убийства как одни из наиболее тяжких преступлений проявляются в обеих хаотических системах также по-разному. В простой хаотической системе убийства выглядят более случайно, хотя в общей своей массе они соответствуют статистическим закономерностям и могут быть объяснены в соответствии с тенденциями, наблюдающимися в обществе в конкретное время и в конкретной исторической обстановке – рост домашнего насилия и общее ухудшение социальной ситуации в обществе, политическая нестабильность в мире и локальные войны прямо ведут к росту убийств. В сложной хаотической системе организованной преступности убийства выглядят закономерно, хотя гибель того или иного главаря происходит значительно реже, чем это могло бы быть, следуя логике этой системы, предполагающей конфликты главарей между собой и конфликты внутри самой системы.

Тем не менее можно с уверенностью утверждать, что криминальные войны являются закономерным следствием хаотической системы организованной преступности, также является ее закономерным явлением гибель главарей организованной преступности разного ранга (криминальные авторитеты).

Войны в преступном мире (криминальные войны) как продолжение не мирного сосуществования организованной и не организованной преступности неизбежны. Такие криминальные войны можно разделить на войны организованной и неорганизованной преступности, войны внутри организованной преступности и войны внутри неорганизованной преступности.

Статистики результатов этих криминальных войн по понятным причинам не ведется. В то же время рискну предположить, что большая часть жертв так называемых «криминальных разборок» – это жертвы войн внутри неорганизованной преступности. Отсюда рост латентных убийств и рост числа лиц, пропавших без вести. Хаотический характер убийств бездомных людей, людей, оказавшихся случайными жертвами пьяных грабителей, погибшие родственники и близкие люди в результате спонтанно возникших или наоборот длящихся месяцами и годами домашних ссор, жертвы дележа награбленного, а часто просто неосторожно брошенного оскорбительного слова предопределяется случайными причинами, которые действуют вопреки своему названию совершенно не случайно, а вполне определенно. При этом убийства внутри организованной преступности происходят не часто по той причине, что главари стараются договариваться и не прибегать к крайним мерам разрешения конфликтов, поскольку это привлекает излишнее внимание к их проблемам со стороны не только правоохранительных органов, но и конкурентов. Убийства как средство решение проблемы далеко не всегда демонстрирует силу той или иной организованной преступной группы (далее – ОПГ), скорее даже наоборот, это может восприниматься как слабость и неумение заниматься криминальными видами деятельности.

Давление хаотической системы преступности на хаотическую систему организованной преступности посредством убийств состоит в том, что эти системы динамичные и очень подвижные. Обе системы не могут находиться в состоянии покоя. Их пересечение между собой не только является активным, но чрезвычайно агрессивным.

Подводя итоги, можно сказать, что понимание хаоса преступности и хаоса организованной преступности, составление моделей развития этих систем могут быть полезными для сотрудников правоохранительных органов.

Работа над такими моделями применительно, например, к конкретной ОПГ может помочь:

– понять причины ее возникновения в данном конкретном месте и в данное конкретное время;

– понять, насколько ОПГ устойчива;

– рассчитать возможное время ее существования;

– предсказать конфликты внутри и вовне ОПГ;

– определить уровень и степень эффективности руководства ОПГ.

Задачи сотрудников правоохранительных органов применительно к хаотическим системам организованной и неорганизованной преступности могут быть решены посредством последовательных действий по определению (пониманию модели организационной формы преступности); разобщению (оперативное исключение членов из ОПГ); разделению (осуждению и направлению в места лишения свободы); исключению (подталкиванию к самоликвидации); нейтрализации (реализации комплекса уголовно-правовых и иных правовых средств по недопущению возрождения) этих систем.

Понимание сути хаотического состояния преступности может пригодиться для разработки стратегических и тактических планов работы полиции.

Список литературы

1. Предупреждение преступности // Журнал Казахстанской криминологической ассоциации. 2017. № 3. С. 48–54.

2. Lex Russica (Русский закон). 2018. Т. 142. № 9. С. 9–20

3. Мониторинг правоприменения. 2019. № 1. С. 4–15.

Минаев В. А.[1],
профессор кафедры специальных информационных технологий Московского университета МВД России имени В.Я. Кикотя

НОВЫЕ МОДЕЛИ И ТЕХНОЛОГИИ ТРАНСГРАНИЧНОГО ОБМЕНА ИНФОРМАЦИЕЙ ПОЛИЦЕЙСКИМИ ПОДРАЗДЕЛЕНИЯМИ

В современном обществе крайне обострились экстремистские проявления, проникнув во все сферы жизни и приведя к образованию мощных угроз его социальным группам в различных странах, в том числе имеющим общую границу. Деструктивному воздействию особенно подвержены подростки и молодежь, предпочитающие распространять информацию путем применения высокоскоростных мессенджеров и социальных сетей. В такой, с каждым годом усложняющейся ситуации необходимо применять новые модели и технологии трансграничного обмена полицейскими подразделениями информацией о состоянии и развитии криминогенного потенциала стран, имеющих общие границы. Особо это относится к террористической и экстремистской деятельности, опасно воздействующей на население и критические промышленные, банковские, информационные и иные структуры соседних государств.

Среди современных методов, применяемых для решения задач противодействия трансграничному распространению криминального влияния, идеологии экстремизма, перспективны разработки в области компьютерного имитационного моделирования [1–4] и методы искусственного интеллекта [5–7].

Полученные на их основе результаты позволяют систематизировать особенности и закономерности криминальных проявлений, экстремизма в социальных сетях, связанных в трансграничном

информационном обмене временными особенностями «информационным заражением», и в территориальном – параметрами сетевых информационных связей и узлов в граничащих странах.

На основе методов искусственного интеллекта получены важные результаты при выявлении деструктивного контента экстремистской направленности в социальных мессенджерах и социальных сетях. А именно, пропаганда нацизма, антисемитизма, радикального ислама, суицидального поведения подростков и др. Точность распознавания деструктивного контента – не менее 91 % [8–10].

Среди основных практических результатов, на которые направлены модели противодействия криминальным явлениям в социальных медиа, включая экстремистские проявления, выступают:

– методы выявления деструктивного контента, содержащего информацию, обостряющую криминогенную обстановку по обе стороны границ, в том числе – экстремистского характера;

– выработка противодействия в информационных сетях с учетом дестабилизирующих влияний со стороны криминалитета;

– методы добывания сведений о лидерах, структуре и ресурсах преступных группировок на трансграничных территориях.

Решение указанных задач позволяет повысить эффективность проведения правоохранительными органами сотрудничающих государств полицейских операций с целью дестабилизации и функционального разрушения криминальных организаций транснационального характера.

В настоящей статье рассмотрим некоторые результаты моделирования информационного противодействия опасным криминальным проявлениям, активно развивающимся в трансграничном аспекте. Эти результаты относятся к моделированию динамики распространения криминальной, в том числе экстремистской идеологии в социальных медиа граничащих стран; территориальному проявлению криминалитета в социальных медиа приграничных зон соседних государств; выявлению с помощью

нейронных сетевых технологий контента криминального характера в социальных медиа.

Моделирование динамики распространения идеологии криминального характера в социальных медиа

Основная цель социальных медиа (далее –СМ) – обеспечение и поддержание связей между людьми, даже когда они находятся по разные стороны границ. Наряду с данным положительным явлением имеется и отрицательная сторона применения СМ – это распространение деструктивной манипулятивной информации в приграничных зонах и далее – вглубь соседних государств.

Действующие платформы СМ в большинстве стран продолжают прирастать аудиторией, происходит активное появление новых участников. Использование современных средств информационного воздействия (ИВ), к сожалению, нашло большой практический интерес у экстремистских организаций. Оно позволяет им без серьезных материальных затрат, обходя государственные границы, негативно влиять на определенную аудиторию, осуществлять акции, влекущие за собой громкий общественный резонанс.

Проведенное исследователями [12] изучение подверженности социальных групп россиян различным негативным ИВ показало следующие результаты.

Так, наибольшее опасение вызывает риск мошенничества и воздействие навязчивой рекламы. С этим чаще всего сталкиваются пенсионеры в силу определенной ограниченности общения, низких компетентностей в экономической и финансовой областях, подверженности телевизионным технологиям воздействия.

В социальных группах подростков и студентов указывается на высокий риск агрессии. Здесь ведущую роль отводят кибербуллингу. Он проявляется в умышленном агрессивном поведении в интернете или мобильных телефонных сетях. Особенностью поведения является его направленность на того, кто слабее с целью унижения достоинства.

Поэтому наиболее вероятные сценарии воздействия со стороны криминалитета, экстремистов связаны с детьми, подростками, молодежью. Именно данным социальным группам следует уделять наибольшее внимание при исследованиях распространения агрессивных и опасных преступных проявлений.

Учитывая весьма высокую подверженность социальных групп населения, особо уязвимых в информационно-психологическом отношении, существует необходимость создания трансграничных баз данных и информационно-аналитических систем мониторинга агрессивного и особо опасного преступного поведения (прежде всего, экстремистского характера) в масштабах граничащих стран.

При этом в основу высокотехнологичного противодействия распространению криминальной, экстремистской идеологии должны быть положены новейшие теоретические и практические результаты в области системного моделирования и информационных технологий.

Особое внимание при организации противодействия со стороны полицейских подразделений распространению криминальной, экстремистской, деструктивной информации, продуцируемой преступными структурами, должно быть уделено исследованию процессов, которые связаны с сетевой организацией инфокоммуникаций в современном обществе.

Агентный, системно-динамический и дискретно-событийный подходы, реализованные в виде имитационных моделей, предоставляют огромные возможности для исследования распространения криминальной идеологии в информационных сетях граничащих стран. При этом системно-динамический подход позволяет наиболее качественно описывать их распространение и управление противоборством с их влиянием.

Аппаратно-программной платформой для реализации системно-динамических моделей ИВ и ИПД выступает современная российская система имитационного моделирования AnyLogic.

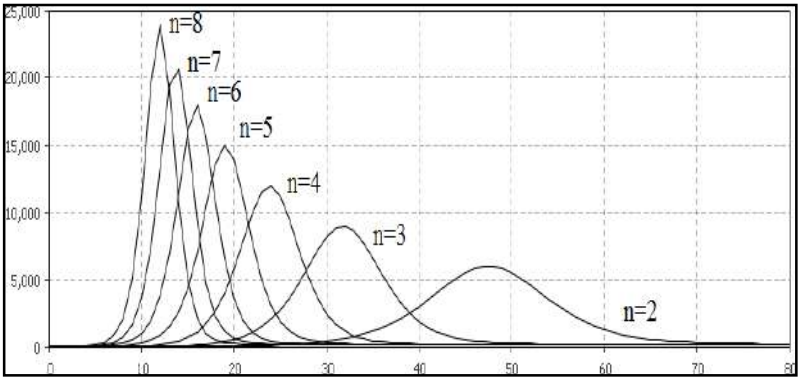


Рис. 1. Зависимость скорости принятия криминального воздействия от частоты асоциальных контактов

Приведем результаты имитационного эксперимента [13–15], где исследуется зависимость скорости распространения криминальной идеологии пользователями сети от частоты асоциальных контактов (рис. 1). Из анализа рис. 1 следует, что, например, при двух контактах в день ($n=2$) скорость принятия криминальной идеи достигнет своего максимума через 48 дней, а уже при восьми ($n=8$) – через 12 дней. Очевидно, что целенаправленное использование социальных медиа на порядки увеличивает указанные показатели, доводя их до нескольких часов. Подобную зависимость экстремистские структуры активно используют в своей вербовочной деятельности.

В рамках моделирования эволюции экстремистских структур, постоянно возникающих в различных государствах, на основе подходов, предложенных в работе [16], в качестве антиэкстремистских мер рассмотрены две их категории, отражающие.

1. *Жесткие стратегии борьбы* (далее – ЖСБ). Они включают в себя нейтрализацию экстремистов радикальными методами вплоть до их физической ликвидации, тотальную проверку всех, продвигающихся через контрольно-пропускные пункты или блокпосты, и другие подобные меры. В целом, данные дей-

ствия влекут за собой существенные нарушения прав и значительный материальный ущерб непричастного к экстремизму населения. Вызывая тем самым недовольство и даже противодействие, в том числе – среди тех его групп, где экстремисты ищут и находят новых рекрутов. Таким образом, жесткие стратегии борьбы могут иметь прямую выгоду от ликвидации действующих экстремистов, но и отрицательный косвенный эффект от стимулирования процесса вербовки новых членов экстремистских структур, используя для этого такой современный информационный инструмент, как СМ.

2. *Интеллектуальные стратегии борьбы* (далее – ИСБ). Это точечные, выверенные операции, в том числе – информационного характера. Они базируются на интеллектуальных решениях, направлены против лиц, виновность которых в экстремистской деятельности полностью доказана. Важная особенность подобных операций состоит в том, что они никак не затрагивают непричастное к экстремистской деятельности население.

ИСБ выглядят более приемлемой мерой в глазах населения и не подпитывают дополнительную вербовку в экстремистские структуры. Но такие стратегии дороже и сложнее в применении, чем ЖСБ. При проведении операций данного типа существует ряд ограничений, вызванных необходимостью высокой подготовки соответствующих кадров, в том числе – в области информационных технологий и информационной безопасности.

В рамках исследования эволюции экстремистской организации с учетом ее взаимодействия с населением региона, в том числе – через СМ, рассмотрены трехмерные модели [17, 18], учитывающие противодействие экстремизму со стороны правоохранительных структур.

Население региона рассмотрено в виде трех составляющих:

– экстремисты;

– восприимчивые как к экстремистской, так и к пацифистской пропаганде;

– невосприимчивые к такого рода информационным воздействиям.

Из анализа рис. 2 можно сделать вывод, что, используя информационное противодействие, в том числе и через СМ, деструктивным влияниям криминального, в том числе – экстремистского характера, можно оказать значительное влияние на пропагандистские возможности экстремистских групп.

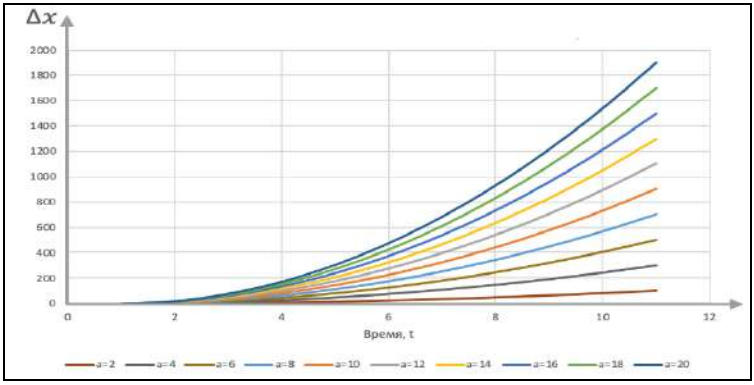


Рис. 2. Приращение численности экстремистов (Δx) при увеличении эффективности вербовки (параметр a)

Зависимость, изображенная на рис. 3, похожа на зеркальное отражение рис. 2. Но она отражает убыль численности экстремистов по квадратичному закону по мере роста антиэкстремистских мер.

Сравнивая зависимости на рис. 2 и 3, отметим, что для формирования эффективных мер борьбы в каждый момент времени важно понимать, какой процесс превалирует на данной территории – рост экстремистского потенциала или его спад.

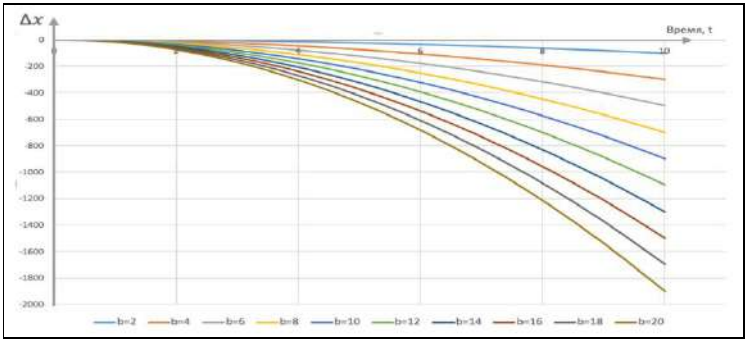


Рис. 3. Уменьшение размера экстремистской организации с ростом мер противодействия экстремизму (параметр b)

Таким образом, принятие обоснованных и целенаправленных мер по борьбе с экстремизмом связано с системным пониманием и интерпретацией динамических изменений в структуре и характеристиках экстремистских организаций. Для этого в моделях целесообразно комплексно рассматривать как факторы воспроизводства экстремизма и борьбы с ним, в том числе, связанные с антиэкстремистской деятельностью со стороны полицейских органов, так и информационные взаимодействия различных групп населения государств, в основном – в СМ.

Моделирование территориальных различий распространения информации в социальных сетях

Для реализации модели территориальных различий распространения информации в СМ необходимо по специальной методике выгружать статистические данные из СМ. Так, в российском сегменте социальной сети (далее – СС) «ВКонтакте» по всем 647 населенным пунктам России с количеством жителей от 10 до 20 тыс. человек выяснены все сетевые узлы «друзей» пользователей, зарегистрированных в этом населенном пункте. По группам «друзей» для всех населенных пунктов рассчитаны математическое ожидание, дисперсия, медиана, диаметр графа и средняя длина пути графа.

Для моделирования распространения информации в населенных пунктах использована указанная выше программная среда Anylogic.

В качестве характерных параметров, отражающих динамику распространения информации в региональных СС, как показали исследования, целесообразно выбрать время исхода 95 % индивидов из множества уязвимых к информационному воздействию, а также время достижения в популяции максимума индивидов в латентном состоянии («информационно заражен», но не распространяет деструктивную идею).

Как показали расчеты зависимостей указанных параметров применительно к статистическим характеристикам множества «друзей» в каждом из рассмотренных населенных пунктов, наилучшими в смысле объясняемости являются модели, зависящие от дисперсии, рассчитываемой по формуле:

$$D_i = \frac{1}{n_i} \cdot \sum_{j=1}^{j=n_i} (x_j - \bar{x}_i),$$

где n_i– количество информационных узлов (пользователей) в i-м населенном пункте;

x_j – количество «друзей» у j-го пользователя в i-м населенном пункте;

$\bar{x}_i$ – среднее количество «друзей» в i-м населенном пункте; i=1, …, 647.

Исходя из того, что зависимость (1) достаточно хорошо объясняет территориальные особенности времени исхода 95 % индивидов из множества уязвимых целесообразно решить задачу выделения однородных групп населенных пунктов со схожими условиями распространения информации.

Такая задача успешно решена. Для выявления однородных групп среди всех исследованных 647 поселений Российской Федерации проведен их многомерный кластерный анализ. Для этого применительно к каждому поселению использовались конкретные статистические характеристики, отражающие пользовательское сообщество, и параметры организации информационных сетей.

В результате построены дендрограммы [13], позволившие выделить пять групп поселений, географически компактно и содержательно хорошо интерпретируемо расположенных на территории страны, включая приграничные зоны. Выявлены зависимости времени исхода 95 % индивидов из множества уязвимых к информационному воздействию ($T_г$), а также времени достижения в популяции максимума индивидов в латентном состоянии (T_k).

Как показано на рис. 3 и 4, соответствующие функциональные кривые (коэффициент объясняемости близок к 100 %) представляются соотношениями:

$$T_{rj} = 71.75 \cdot D_j^{-1.155} \quad (2)$$

$$T_{kj} = 56.9 \cdot D_j^{-1.153}, \text{ (j=1, …, 5)} \quad (3)$$

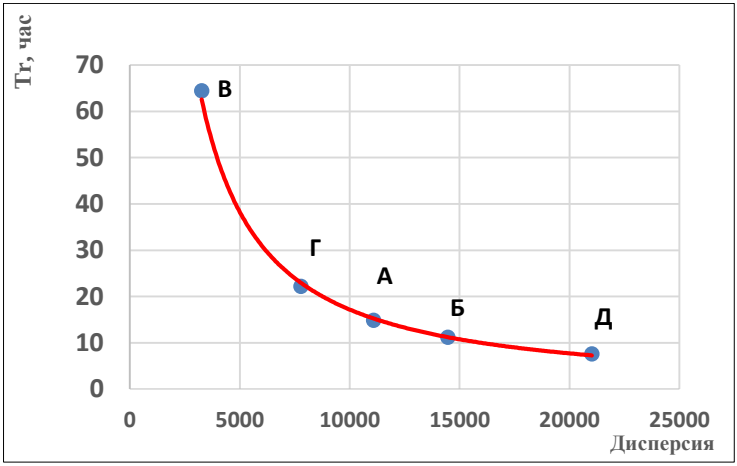


Рис. 4. Зависимость динамического параметра $T_г$ от дисперсии (кружками обозначены эмпирические данные)

Итак, в процессе моделирования территориальных различий получены новые научно-практические результаты, важные для обоснования полицейских мероприятий противодействия распространению идеологии экстремизма в социальных медиа, а

также целенаправленного трансграничного обмена информацией между подразделениями полиции, а именно:

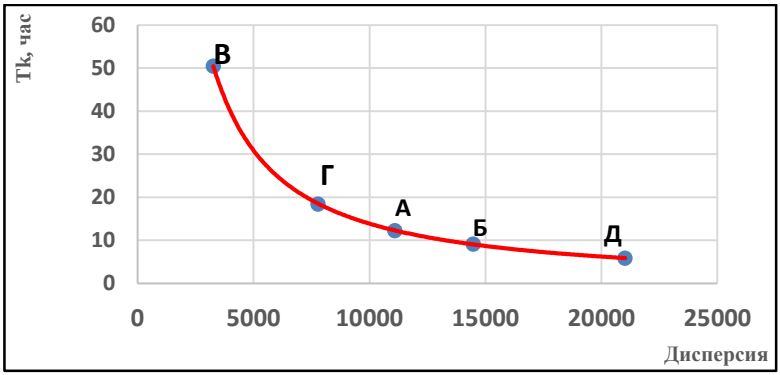


Рис. 5. Зависимость динамического параметра T_k от дисперсии (кружками обозначены эмпирические данные)

Найдено функциональное описание зависимостей времени исхода индивидов из состояния «уязвимые» к информационным воздействиям, а также времени достижения в популяции максимума индивидов в латентном состоянии, от дисперсии числа «друзей» пользователей СС в однородной группе поселений кластеров. Безусловно, результаты подобного исследования в соседних странах весьма важны для полиции Российской Федерации.

Выявленные функциональные зависимости позволяют отделять одни поселения от других по степени восприимчивости населения к информационным криминальным воздействиям в СС, включая деструктивные воздействия экстремистского характера. Последнее дает возможность органам власти, силовым структурам, исходя из принадлежности к тому или иному кластеру, целенаправленно строить политику и тактику противодействия таким влияниям.

Построено географически компактное территориальное распределение поселений кластеров, дающее возможность детально исследовать причины региональных различий скорости распространения информации, которые определяются как организацией

сетевых сообществ и самих сетей на различных территориях, так и экономическими, социальными, демографическими, этническими и иными факторами проживающего там населения.

Методы выявления контента экстремистского содержания в социальных медиа

Приведем пример выявления контента экстремистского содержания в текстовых массивах из СМ: отражающих информацию антисемитского характера; содержащих высказывания, направленные на реабилитацию нацизма; восхваляющих лозунги радикального ислама [8–10]. В табл. 1 приведены названия и объемы текстовых массивов в виде коротких сообщений из социальных мессенджеров и социальных сетей, исследованных на предмет экстремистского содержания, а также точность распознавания в процентах.

Таблица 1

Текстовые массивы, исследованные на предмет экстремистского содержания

Название текстового массива	Количество сообщений, тыс.	Точность распознавания, %
Антисемитизм	**268**	**91**
Реабилитация нацизма	**284**	**93**
Радикальный ислам	**310**	**95**

Из табл. 1 следует, что точность распознавания сообщений экстремистской направленности не менее 91 %, причем наилучшим образом выявляются тексты, содержащие различные формулировки из области радикального ислама – 95 %.

В статье показана необходимость глобального противодействия распространению криминальной идеологии, идей экстремизма в социальных медиа, развития все более глубоких системных исследований факторов, определяющих тенденции этого опасного явления. Данное положение дел заставляет вырабатывать новые стратегии и тактики противоборства в этой сложной сфере,

осуществлять операции информационного характера со стороны полицейских структур, расположенных по разные стороны границ.

Объединение информационных ресурсов полиции соседних государств позволит существенно модернизировать алгоритмы сбора, обработки и хранения данных, повысить качество решения задач по противодействию криминалитету, экстремизму, возложенных на полицейские подразделения, увеличить скорость обработки запросов, усилить уровень защиты информации, повысить эффективность работы их служб.

Обобщен материал о возможностях моделирования при исследовании процессов формирования криминальных структур, разрушения их потенциала вследствие активных воздействий со стороны государства и общества. Воздействия формируются на принципиально различной основе, включая две стратегии – жесткую и интеллектуальную, каждая из которых имеет свои преимущества и недостатки в управлении процессами вербовки новых членов криминальных структур, в том числе – экстремистского характера.

На основе исследования генеральной совокупности (647 поселений России с населением от 10 до 20 тыс. человек) изучены территориальные характеристики распространения информации в наиболее популярной СС «ВКонтакте». На основе кластерного анализа указанные поселения классифицированы на пять однородных групп, отличающихся скоростями распространения информации в социальных медиа, а, следовательно – показателями «информационного заражения» населения деструктивной информацией. Полученное кластерное деление населенных пунктов страны является важной основой для интерпретации территориальных различий распространения информации, исследования их комплексной обусловленности такими факторами, как организация сетевых сообществ и самих социальных медиа, экономическими, социальными, демографическими, этническими и иными факторами.

Итоги моделирования связаны с обоснованием количественных параметров, позволяющих органам власти, силовым структурам и другим заинтересованным организациям относить оцениваемые поселения к разным кластерам по степени восприимчивости населения к информационным влияниям в сети, включая деструктивные воздействия экстремистского характера. Такая информация является критически важной при трансграничном обмене ею между полицейскими подразделениями.

В рамках проведенного исследования на основе использования глубинных информационных сетей найдены наиболее точные алгоритмы и методы выявления деструктивного контента в публикациях и комментариях по трем темам:

– реабилитация нацизма;

– антисемитизм;

– радикальный ислам.

Рассмотренные методы выявления деструктивного контента целесообразно применять в аналитической деятельности полицейских подразделений и других заинтересованных государственных органов.

Описанные модели к настоящему времени апробированы, прошли проверку на реальных статистических данных, показали необходимый уровень релевантности, подтвердили свою научную и практическую значимость.

Список литературы

1. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства. М. : Физматлит, 2010. 228 с.

2. Как управлять массовым сознанием: современные модели : монография / [В. А. Минаев и др.]. М. : Издательство РосНОУ, 2013. 200 с.

3. Андреев А. А., Бондарь К. М., Минаев В. А. Терроризм и экстремизм: моделирование информационного противодействия : монография. Хабаровск : Дальневосточный юридический институт МВД России, 2020. 251 с.

4. Минаев В. А., Сычев М. П., Бондарь К. М., Вайц Е. В. Системно-динамическое моделирование сетевых информационных операций // Инженерные технологии и системы. 2019. Т. 29. № 1. С. 20–39.

5. Еремин Д. М., Гарцеев И. Б. Искусственные нейронные сети в интеллектуальных системах управления. М. : МИРЭА, 2004. 75 с.

6. Методы тематического моделирования, их развитие и применение для контента, циркулирующего в региональных онлайн-сообществах / [Е. Н. Телегин и др.] // Информация и безопасность. 2019. Т. 22. № 3(4). С. 325–344.

7. Гончаров А. А., Чапурин Е. Ю., Белоножкин В. И., Радько Н. М. Развитие методов и построение алгоритмов поиска и классификации деструктивного контента, циркулирующего в социальной сети // Информация и безопасность. 2019. Т. 22. № 3 (4). С. 345–360.

8. Минаев В. А., Реброва А. Д., Симонов А. В. Выявление деструктивного контента в социальных медиа на основе моделей машинного обучения // Информация и безопасность. 2021. Т. 24. № 1. С. 7–20.

9. Минаев В. А., Симонов А. В. Количественная оценка деструктивности больших текстовых массивов в социальных медиа // Информация и безопасность. 2021. Т. 24. № 2. С. 267–280.

10. Минаев В. А., Поликарпов Е. С., Симонов А. В. Применение глубинных нейронных сетей для выявления деструктивного контента в социальных медиа // Информация и безопасность. 2021. Т. 24. № 3. С. 361–372.

11. Социальные сети в России: цифры и тренды // Блог Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2019.

12. Безбогова М. С. Социальные сети как фактор формирования социальных установок современной молодежи // URL: https://guu.ru/files/dissertations/2016/12/bezbogova_m_s/dissertation.pdf.

13. Минаев В. А., Федорович В. Ю. Моделирование информационных воздействий в социальных сетях: территориальный аспект // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2019. № 4. С. 8–16.

14. Минаев В. А. Исследование модели динамики деструктивных информационно-психологических воздействий на массовое сознание // Безопасность информационных технологий. 2016. № 4. С. 52–58.

15. Вайц Е. В. Системно-динамический подход к моделированию информационных воздействий // Интернет-журнал «Технологии техносферной безопасности». 2017. № 2. С. 296–306.

16. Optimal Control of Nonlinear Processes. With Applications in Drugs, Corruption and Terror / [D. Grass etc.]. Springer-Verlag Berlin Heidelberg, 2008. 552 p.

17. Feichtinger G., Hartl R. F., Kort P. M., Novak A. J. Terrorism Control in the Tourism Industry // Journal of Optimization Theory and Applications. 2001. № 108 (2), pp. 283–296.

18. Feichtinger G., Novak A. J. Terror and Counter-Terror Operations: A Differential Game with a Cyclical Nash Solution // Forthcoming in Journal of Optimization Theory and Applications. 2008. Vol. 139, pp. 113–120.

Олимпиев А. Ю.[1],
заведующий кафедрой теории и истории, государства и права
Института социальных наук,
доктор исторических наук, кандидат юридических наук

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В СИСТЕМЕ СОЦИАЛЬНЫХ И ГУМАНИТАРНЫХ НАУК В РОССИЙСКОЙ ФЕДЕРАЦИИ

Предметом данной статьи является оперативно-разыскная деятельность, как отрасль юридической науки и ее место в системе социальных и гуманитарных наук в Российской Федерации.

Авторы Н. В. Румянцев и А. В. Агарков проанализировали «филологический и философский подходы к содержанию понятий “оперативно-розыскное мероприятие” и “осуществление оперативно-розыскного мероприятия”». «Из вышеуказанного возможно выделить некоторые признаки. Нормативный характер, т. е. предусмотренность рассматриваемых действий в оперативно-разыскном законе. Ограничение по кругу субъектов, т. е. возможность осуществления оперативно-разыскных мероприятий только оперативными подразделениями установленных законодательством государственных органов. Любое оперативно-разыскное мероприятие представляется совокупностью действий, включающих в себя морально-волевые (например, самостоятельное принятие решений), управленческие (например, согласование и санкционирование некоторых действий), организационные (например, дача задания конфиденту) и непосредственно оперативно-разыскные (направленные на получение информации, например, ведение наблюдения) действия. Направленность оперативно-разыскного мероприятия на решение задач оперативно-разыскной деятельности. Направленность на решение иных задач в результате указанных действий исключает их из

[1] © Олимпиев А. Ю., 2022.

числа оперативно-разыскных мероприятий, что обусловливает тщательную научную разработку задач оперативно-разыскной деятельности»).

Ю. В. Астафьев выделяет «два обстоятельства»: «В завершение хотелось бы отметить два обстоятельства. Оперативно-разыскная деятельность не может быть “прозрачной”. Закрытость ее обоснованна и естественна в любом государстве, которое не может быть беспомощным участником охранительных отношений. Однако это не исключает жесткого контроля за ОРД и ее результатами. Контроль предполагает различные способы: судебную деятельность, уголовно-процессуальный механизм проверки и оценки, оперативный контроль руководителей подразделений, осуществляющих ОРД, прокурорский надзор. Несовершенство законодательства в определенной степени препятствует этим процедурам. Однако многое зависит от уровня правосознания следователей и судей, их желания и умения использовать возможности, предоставляемые действующим законодательством. Кроме того, из правоприменительной практики должна быть исключена тенденция “скрытого” использования результатов ОРД в качестве доказательств. Никакие “особые” случаи не могут служить оправданием нарушения законности при проверке и оценке оперативно-разыскной информации».

М. В. Лапатников анализировал «дискуссионные аспекты толкования специалистами критерия пассивного поведения сотрудников правоохранительных органов при решении вопроса об отграничении правомерного оперативно-разыскного мероприятия от провокации на основе практики Европейского суда по правам человека». «Тем не менее мы не готовы полностью отвергнуть критический пафос приведенных в нашей статье оценок. Нельзя не согласиться с тем, что предложенный Европейским судом критерий пассивности представляет правоохранительным органам достаточно жесткие требования, которые, при их буквальном толковании, ставят исход уголовного преследования (в

оперативно-разыскной форме) в зависимость от воли уголовно-преследуемого лица. На наш взгляд, вопрос понимания критерия пассивности необходимо рассматривать как одно из частных проявлений фундаментальной проблематики отечественного уголовного процесса – соотношение правозащитного и карательного начал в следственно-судебной практике по уголовным делам. И, судя по всему, сам Европейский суд пока еще далеко не полностью нашел здесь ту золотую середину, которая в идеале должна сбалансировать эти два начала».

Д. В. Зиборов к числу «первоочередных задач ОРД на современном этапе развития пенитенциарной системы» предлагает относить: «1) определение роли и значения ОРД в системе исполнения уголовных наказаний; 2) изменение и дополнение законов и подзаконных нормативных правовых актов, регламентирующих ОРД с учетом специфики ее осуществления в учреждениях УИС; 3) формирование собственной ведомственной нормативной правовой базы ОРД; 4) разработку оптимальной модели организационно-структурного обеспечения ОРД в органах и учреждениях УИС; 5) совершенствование информационного обеспечения ОРД путем формирования собственных учетов оперативной информации на основе автоматизированных банков данных; 6) разработка системы правовой и социальной защиты всех участников оперативно-разыскного процесса в УИС; 7) совершенствование сотрудничества оперативных подразделений УИС с иными правоохранительными органами и их оперативными аппаратами, прежде всего, по таким злободневным вопросам, как терроризм и организованная преступность, незаконный оборот наркотиков, розыск бежавших преступников, раскрытие преступлений прошлых лет, предупреждение замышляемых и подготавливаемых преступлений; 8) совершенствование иных организационных и тактических основ пенитенциарной разведки».

Противоречивые результаты научных исследований относительно оперативно-разыскной деятельности и ее места в системе

социальных и гуманитарных наук предопределяют и несовершенство законодательства Российской Федерации.

Первоначально обращаемся к нормативному правовому акту, специально предназначенному для регулирования оперативно-разыскной деятельности в Российской Федерации, и по юридической силе приравненному к федеральному закону. Речь идет о Федеральном законе от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», который определяет «содержание оперативно-розыскной деятельности, осуществляемой на территории Российской Федерации, и закрепляет систему гарантий законности при проведении оперативно-розыскных мероприятий» (преамбула).

В приказе Министра науки и высшего образования Российской Федерации от 24 февраля 2021 г. № 118 «Об утверждении номенклатуры научных специальностей, по которым присуждаются ученые степени, и внесении изменения в Положение о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук, утвержденное приказом Министерства образования и науки Российской Федерации от 10 ноября 2017 г. № 1093» приведен перечень разновидностей социальных и гуманитарных наук: «5.1.1. Теоретико-исторические правовые науки; 5.1.2. Публично-правовые (государственно-правовые) науки; 5.1.3. Частно-правовые (цивилистические) науки; 5.1.4. Уголовно-правовые науки; 5.1.5. Международно-правовые науки».

Оперативно-разыскная деятельность, несомненно, должна включаться в уголовно-правовые науки (5.1.4), на что уже обращается внимание в юридической литературе.

Таким образом, научные исследования относительно места оперативно-разыскной деятельности в системе социальных и гуманитарных наук в Российской Федерации необходимо продолжить.

Изложенное позволяет нам высказать несколько суждений. Во-первых, термин «оперативно-разыскная деятельность» многозначен. Во-вторых, оперативно-разыскная деятельность может рассматриваться в качестве отрасли юридической науки.

В-третьих, принятие вышеупомянутого приказа Министра науки и высшего образования Российской Федерации от 24 февраля 2021 г. № 118 должно повлечь переосмысление места и роли оперативно-разыскной деятельности в системе социальных и гуманитарных наук.

Маслов А. А.[1],
главный научный сотрудник Всероссийского научно-исследовательского института МВД России, доктор юридических наук

О ЦЕЛЕСООБРАЗНОСТИ УСИЛЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ВОВЛЕЧЕНИЕ НЕСОВЕРШЕННОЛЕТНИХ В СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ ИЛИ АНТИОБЩЕСТВЕННЫХ ДЕЙСТВИЙ

Анализ сложившийся криминологической ситуации в Российской Федерации показывает, что в условиях развивающегося информационного общества происходит масштабное изменение структуры преступности. Так, в течение последних трех лет сократился уровень традиционных преступлений (убийств, грабежей, разбоев, квартирных краж и краж автотранспорта) на 25–35 % (в зависимости от состава). При этом происходит активный рост количества регистрируемых преступлений, связанных с использованием информационно-телекоммуникационных технологий (далее – ИТТ).

В 2020 г. он составил 73,4 %, в 60 % случаев преступниками использовалась сеть Интернет [1].

Имеются объективные и субъективные трудности в раскрытии данного вида преступлений, их раскрываемость в 2,5 – 3 раза ниже раскрываемости преступлений, совершаемых в реальной среде.

Проявляется тенденция снижения уровня выявления групповой преступности, которое составило в 2018 г. – 3,2 %, в 2019 и 2020 гг. оно удвоилось и составило по 7,4 % ежегодно.

Это в полной мере относится и к лицам, вовлекающим несовершеннолетних в совершение преступлений и антиобщественных действий, для которых открылись новые технологические

[1]

возможности на фоне минимизации риска быть привлеченными к ответственности.

Несовершеннолетние уже участвуют в совершении преступлений с использованием ИТТ, при этом криминализация затронула даже школьников средних классов. Так, 18 % из числа несовершеннолетних, совершивших преступления с использованием ИТТ, причастны к незаконному обороту наркотиков. При этом школьниками таких преступлений совершено в два раза больше, чем студентами.

Более 80 % имущественных преступлений, совершенных несовершеннолетними с использованием ИТТ, являются тяжкими. Так, более полутора тысяч несовершеннолетних совершили кражи с банковского счета, а равно в отношении электронных денежных средств (п. «г» части 3 ст. 158 УК РФ).

Не может не вызывать тревогу тот факт, что самая высокая динамика роста количества преступлений с использованием ИТТ отмечена среди несовершеннолетних в возрасте 14–15 лет.

Вербовка несовершеннолетних преступным элементом достигла небывалого размаха. С помощью виртуальной (цифровой) среды формируется качественно новая более опасная идеология и практика вовлечения несовершеннолетних в преступную и антиобщественную деятельность, а также их «воровского» порабощения и эксплуатации.

Это явление часто называют «АУЕ», однако оно имеет сотни названий и охватывает виртуальную и реальную среду почти всего постсоветского пространства [2].

Злоумышленники нацелены вовлекать несовершеннолетних не только в совершение конкретного преступления или антиобщественного действия, но также обучают и готовят их к противоправному (преступному) образу жизни.

При этом часть из них подготавливают для выполнения под управлением старших роли несовершеннолетних сверстников-

вербовщиков. Данное явление является распространенной практикой не только в России, но и в странах ЕС, особенно в сфере сексуальной эксплуатации детей [3; с. 103].

Очевидна недостаточность уголовно-правовых мер по борьбе с вовлечением несовершеннолетних в совершение преступлений.

Так, анализ правоприменительной практики по ст. 150 УК РФ (Вовлечение несовершеннолетнего в совершение преступления) показывает, что в настоящее время привлечению к уголовной ответственности взрослых лиц по данной статье предшествуют два условия:

– несовершеннолетний должен совершить конкретное преступление;

– взрослое лицо должно являться его соучастником.

Проблема будет более очевидна, если мы соотнесем подростковую преступность в сфере ИТТ с мерами по пресечению деятельности лиц, вовлекающих их в совершение преступлений.

Как известно, большое влияние на криминализацию несовершеннолетних, используя их возрастные психофизиологические особенности, оказывают взрослые, особенно ранее судимые. Не исключается также внешнее деструктивное целенаправленное влияние.

Несмотря на это, на протяжении последнего десятилетия за вовлечение несовершеннолетних в совершение преступлений и антиобщественных действий привлекается взрослых лиц в 30 раз меньше, чем подростков за совершенные ими преступления. При этом за последние пять лет количество данных лиц сократилось на 15 %.

Однако в условиях развития информационного общества ситуация обострилась.

Так, в 2020 г. в суд направлены уголовные дела, возбужденные всего в отношении шестерых взрослых лиц, вовлекавших

несовершеннолетних в совершение преступлений с использованием ИТТ, это уже в 448 раз меньше, чем выявлено несовершеннолетних преступников в данной сфере.

Существующий уголовно-правовой подход в части установления ответственности взрослого лица в зависимости от совершения подростком конкретного преступления в деятельности оперативных подразделений фактически снял с повестки дня вопрос оперативно-разыскного документирования именно процесса вовлечения, как непосредственного, так и дистанционного. Фактически норма ст. 150 УК РФ работает в отношении взрослых лиц при задержании смешенных групп с участием несовершеннолетних. При этом разница в возрасте соучастников бывает не велика.

Действия криминалитета, связанные с оказанием целенаправленного негативного влияния на правосознание несовершеннолетнего в форме пропаганды воровской романтики, нигилистического отношения к нормам права и морали, воспитания враждебного отношения к государственным, в том числе правоохранительным органам, в основном, остаются за рамками уголовного закона, а, соответственно, и ОРД. Также как обучение несовершеннолетнего способам совершения преступлений с использованием новых ИТТ или тактике вербовки сверстников реально или дистанционно в различные антиобщественные формирования.

Можно сделать вывод, что в равной степени представляет общественную опасность как вовлечение несовершеннолетних в совершение конкретного преступления, так и подготовка его к преступному образу жизни.

Так, можно выделить и конкретизировать для оценки с позиции УК РФ такие действия, как:

– пропаганда преступного (воровского) образа жизни;

– обучение несовершеннолетнего способам совершения преступлений, в том числе с использованием ИТТ, сокрытия их следов, а также противодействия правоохранительным органам;

– подготовка и управление действиями несовершеннолетних для исполнения ими роли сверстника-вербовщика;

– неоднократное получение от несовершеннолетнего денежных средств, неустановленного происхождения и т. п.

Представляется, что это не весь перечень, он может быть дополнен при предметном обсуждении специалистов в сфере криминологии, криминалистики, уголовного права и ОРД. В этом случае может быть применима административная преюдиция, которая могла бы помочь взрослому лицу вовремя пересмотреть свое поведение.

Таким образом, не отвергая сложившуюся уголовно-правовую практику, считаем целесообразным в рамках реагирования на современные вызовы и угрозы в условиях развития информационного общества, начать разработку дополнительной ст. 150.1 УК РФ (условно: вовлечение несовершеннолетних в преступную деятельность), как было в прежнем кодексе.

Принятие вышеназванных мер на законодательном уровне позволит сформировать на данном направлении полноценное ведомственное и межведомственное нормативное регулирование оперативно-разыскного противодействия вовлечению несовершеннолетних в совершение преступлений и иных антиобщественных действий, как в реальной, так и в цифровой среде.

Список литературы

1. Богданов А. В., Завьялов И. А., Ильинский И. И. О некоторых аспектах розыска несовершеннолетних, пропавших без вести, и профилактики правонарушений и преступлений в их среде // Актуальные вопросы организации розыскной работы : электронный сборник научных статей по материалам межведомственного круглого стола, 2017. С. 26–37.

2. Глухова А. А., Шпилев Д. А. Особенности организации и функционирования сайтов, посвященных тематике «АУЕ», и их роль в формировании социопатических и противоправных

установок у подростков и молодежи // Актуальные проблемы экономики и права. 2019. Т. 13. № 4.

3. Жданов Ю. Н., Овчинский В. С. Киберполиция XXI века : международный опыт / под ред. С.К. Кузнецова. М. : Международные отношения, 2020. 285 с.

4. Лобачева Л. П. Субкультура «АУЕ» среди подростков. Особенности проявления в современной России // Образование и наука в России и за рубежом. 2018. № 12.

5. Меняйло Д. В., Иванова Ю. А., Меняйло Л. Н. АУЕ – криминальное молодежное движение: сущность и способы распространения // Вестник Московского университета МВД России. № 3. 2019.

6. Состояние преступности в России за январь – декабрь 2020 г. // Статистика ФКУ «ГИАЦ МВД России». М., 2021.

7. Хромов И. Л., Кузьмин Н. А., Завьялов И. А. Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности / под ред. В. С. Овчинского // Оперативно-розыскная деятельность в цифровом мире : сборник научных трудов. М. : Инфра-М, 2021. С. 94–103.

Пузарин А. В.[1]*,*
начальник учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя

ПРОБЛЕМЫ ПОДГОТОВКИ ТЕХНИЧЕСКИХ СПЕЦИАЛИСТОВ ДЛЯ ПРЕСЕЧЕНИЯ, РАССЛЕДОВАНИЯ И РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ В ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ

В настоящее время задачами органов внутренних дел являются эффективный ответ на криминальный вызов IT-преступности, защита граждан и добросовестного бизнеса, который активно осваивает цифровое пространство. Важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. Сохранилась динамика существенного роста количества преступлений рассматриваемой категории, уголовные дела которых находились в производстве правоохранительных органов Российской Федерации.

Сложившиеся обстоятельства социально-экономического характера, обусловленные распространением и преодолением последствий новой коронавирусной инфекции COVID-19, создали дополнительные условия для усиления криминальной активности, связанной с использованием IT-технологий. Данная ситуация требует эффективных незамедлительных мер, самая сложная проблема – это организация качественной подготовки технических специалистов.

В результате преобразований в системе МВД России стало очевидно, что решающим фактором успеха является человеческий ресурс. В этой связи возникла необходимость формирования стратегического подхода к управлению персоналом, в основе

которого – наличие долгосрочной концепции кадровой политики Министерства.

Кадровая политика в системе МВД России направлена на формирование профессионального состава кадров, сохранение, воспроизводство, укрепление, развитие, рациональное и эффективное использование кадрового потенциала органов внутренних дел в интересах оперативно-служебной деятельности. Важнейшей стратегической целью МВД России является повышение качества кадрового потенциала органов внутренних дел, приведение его в соответствие с требованиями инновационного социально ориентированного развития Российской Федерации.

Пути к достижению этой цели находятся в плоскости модернизации системы подготовки кадров, которая представляет собой крупнейшую ведомственную педагогическую систему, в ее основе – непрерывное образование на базе многоуровневого обучения по дифференцированным, преемственным программам, удовлетворяющим профессиональным требованиям к сотруднику органов внутренних дел, сочетанием федерального и регионального компонентов с использованием современных форм и методов обучения.

Условием успешного компетентностного подхода в обучении выступает комплексный, всеобъемлющий подход. В числе приоритетных задач определено развитие многоуровневой практико-ориентированной системы непрерывного профессионального образования, приведение содержания и структуры профессиональной подготовки кадров в соответствие с динамично изменяющимися потребностями органов внутренних дел.

Одним из условий обеспечения практической направленности обучения является комплексное научно-методическое обеспечение федеральных государственных образовательных стандартов, а также разработка и реализация практико-ориентирован-

ных образовательных программ, обеспечивающих, наряду с базовым академическим образованием, качественную прикладную профильную подготовку.

Требуется изменить подходы и к системе переподготовки и повышения квалификации, в том числе научно-педагогических и профессорско-преподавательских кадров. Прежде всего, речь идет о создании кадрового резерва всех уровней с организацией эффективной стажировки, а также последовательном повышении научной квалификации профессорско-преподавательского состава.

Современная материально-техническая база, без которой невозможно внедрить новые образовательные технологии и инновационные модели образовательных программ, должна быть адаптирована для использования современных информационных и коммуникационных технологий, электронных образовательных ресурсов и пособий, обеспечения эффективного доступа профессорско-преподавательского состава и обучающихся к источникам информации в области науки и техники.

Пузырева Ю. В.[1],
заместитель начальника
кафедры прав человека и международного права
Московского университета МВД России имени В.Я. Кикотя,
кандидат юридических наук, доцент

Мысина А. И.[2],
адъюнкт факультета подготовки
научно-педагогических и научных кадров
Московского университета МВД России имени В.Я. Кикотя

К ВОПРОСУ О ПЕРСПЕКТИВАХ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА В БОРЬБЕ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Рассматривая вопросы противодействия транснациональной преступности, необходимо отметить, что традиционные подходы к борьбе с противоправной деятельностью далеко не всегда могут быть успешно применимы к неправомерному использованию информационных технологий в преступных целях. В настоящее время существует множество проблем противодействия противоправным деяниям в области информационных технологий, значительная часть из которых относится к трудностям, возникающим в ходе раскрытия и расследования транснациональных преступлений. В данном контексте особое значение приобретает международное сотрудничество в борьбе с преступлениями в области информационных технологий, что определяет возрастающую потребность совершенствования правовых, аналитических,

информационных, технических и иных возможностей органов внутренних дел Российской Федерации в данной сфере.

Позиционно, различные направления международного правоохранительного сотрудничества по борьбе с преступлениями в области информационных технологий имеют определенное значение для представителей многих подразделений органов внутренних дел Российской Федерации, в частности, например, для следователей, экспертов-криминалистов, оперативных сотрудников полиции, инспекторов по делам несовершеннолетних и др.

Так, в соответствии с положениями п. 3 ч. 2 ст. 151 УПК РФ предварительное следствие по уголовным делам о преступлениях, предусмотренных, к примеру, такими статьями УК РФ, как, ст. 159.6 «Мошенничество в сфере компьютерной информации», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», осуществляется следователями органов внутренних дел Российской Федерации. Обозначенные составы преступлений нередко приобретают транснациональных характер. В подобных ситуациях успех расследования во многом зависит от эффективности межгосударственного взаимодействия.

Кроме того, возникают проблемы определения юрисдикции и подследственности преступлений международного характера в сфере информационных технологий, что, в свою очередь, лишает правоохранительные органы перспективы расследования преступления по горячим следам и влечет утрату возможности своевременного проведения следственных действий, главным образом, в связи с недолговечностью доказательств. Концептуально, международно-правовая регламентация единообразных подходов к урегулированию вопросов борьбы с информационной преступностью на универсальном уровне, в том числе направленная на гармонизацию норм уголовного права в контексте заявленной

проблематики, оказала бы положительное влияние на работу следователей, в частности, применительно к реализации института экстрадиции, главным образом, на основании Европейской конвенции о выдаче, заключенной в г. Париже (Французская Республика) 13 декабря 1957 г., и Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам, подписанной в г. Минске (Республика Беларусь) 22 января 1993 г.

Что касается профессиональной деятельности экспертов-криминалистов, следует обратить внимание на необходимость совершенствования работы по проведению компьютерных экспертиз. Актуальность развития обозначенного направления экспертной деятельности стремительно возрастает, поскольку на сегодняшний день в процессе расследования преступлений все чаще возникает потребность в проведении компьютерной экспертизы. Значительное внимание в данном контексте сообразно уделить исследованию передового опыта международных организаций (например, таких как ООН и Интерпол) по профессиональной подготовке полицейских кадров в области проведения компьютерных экспертиз. С позиции авторов возрастает необходимость в направлении представителей экспертно-криминалистических подразделений на стажировку в специализированные международные организации для изучения передового опыта в области проведения компьютерных экспертиз, а также увеличения набора курсантов в Московский университет МВД России имени В.Я. Кикотя по данной специальности. Кроме того, значительная роль также отводится разработке и принятию международно-правовых стандартов проведения компьютерной экспертизы в целях гармонизации норм национального права в рассматриваемой сфере. Указанные меры позволят с наибольшей результативностью использовать в расследовании преступлений результаты цифровых экспертиз, проводимых компетентными органами иностранных государств.

В свете развития транснационального сотрудничества по противодействию информационной преступности большое значение имеет налаживание двустороннего межгосударственного взаимодействия в области судебно-экспертной деятельности. Так, 12 октября 2017 г. подписано Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Государственным комитетом судебных экспертиз Республики Беларусь в сфере судебно-экспертной деятельности, которое нацелено на развитие межведомственного взаимодействия по проведению научных исследований в области судебно-экспертной деятельности, научно-методического обеспечения производства судебных экспертиз, а также экспертных исследований, оказания практического и методического содействия, в частности, обмена опытом относительно экспертной практики.

Относительно деятельности оперативных сотрудников полиции международное сотрудничество по противодействию информационной преступности представляется не менее актуальным, поскольку в п. 15 ст. 6 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» предусмотрена возможность проведения оперативно-разыскного мероприятия «получение компьютерной информации» , что, в свою очередь, имеет непосредственное значение для раскрытия преступлений в сфере информационных технологий. Кроме того, если рассматриваемые противоправные деяния приобретают транснациональный характер, возникает потребность в инициировании межгосударственного розыска в соответствии с положениями Инструкции о едином порядке осуществления межгосударственного розыска лиц, утвержденной на заседании СМВД 6 сентября 2007 г. или международного розыска по линии Интерпола. Более того, существует практика направления компетентным органам разыскных заданий, связанных с проведением различного рода оперативно-разыскных мероприятий на территории иностранного государства. В рамках борьбы с информационной преступностью разыскные задания последних лет нередко содержат

просьбу иностранного государства относительно установления IP-адресов предполагаемых киберпреступников.

В определенной степени международное сотрудничество в борьбе с информационной преступностью затрагивает и профессиональную деятельность инспекций, по делам несовершеннолетних. В первую очередь это касается противодействия распространению детской порнографии, поскольку преступления подобного рода характеризуются вовлечением несовершеннолетних лиц в противоправную деятельность и наносят серьезный ущерб потерпевшим и общественным отношениям. Позиционно, борьбой с распространением детской порнографии занимается большое количество международных организаций. К их числу представляется возможным отнести ООН, Интерпол, Европол, Совет Европы, СНГ, Африканский союз, Лигу арабских государств и др. Все они призывают государства осуществлять активное противодействие преступлениям в сфере информационных технологий, в том числе в плане нормативно-правового регулирования. Негативно окрашенной тенденцией в сфере информационных технологий является также деструктивное воздействие различных социальных сетей на личность несовершеннолетних интернет-пользователей, которое все чаще приводит к суицидальным проявлениям, необоснованной агрессии, совершению противоправных деяний и т. д., что на сегодняшний день представляется весьма серьезной проблемой.

Подводя итоги, необходимо сделать вывод о том, что международное сотрудничество в борьбе с информационной преступностью имеет большое значение для представителей различных подразделений органов внутренних дел Российской Федерации. Значительную роль в данном контексте играет возможность информационного обмена по каналам связи международных правоохранительных организаций, таких как Интерпол и Европол, а также использование возможностей специализированных отраслевых структур.

Наиболее актуальным представляется межгосударственное взаимодействие по линии СНГ, поскольку механизмы транснационального сотрудничества по противодействию преступности в рамках обозначенной организации рационально адаптированы к особенностям национальных правовых систем государств, расположенных на постсоветском пространстве. О значимости транснационального сотрудничества в области противодействия информационной преступности для органов внутренних дел Российской Федерации свидетельствуют рассмотрение данного вопроса в качестве одной из основных проблем различными органами СНГ (СГГ, СМИД, СМВД и др.) и принятие в рамках исследуемой проблематики международных документов, в частности, Решения СМИД от 5 апреля 2019 г. о базовой организации государств – участников СНГ по подготовке кадров в сфере борьбы с преступлениями, совершаемыми с использованием информационных технологий, по образовательным программам высшего образования и дополнительным профессиональным программам и Положения о базовой организации. Отдельное внимание отводится организации под эгидой СМВД международных научно-представительских мероприятий, посвященных противодействию преступлениям в сфере информационных технологий. Большое значение также имеют выработка и международно-правовая регламентация единообразных подходов к осуществлению противодействия преступлениям в сфере информационных технологий, а также совершенствование процессов обмена данными между правоохранительными органами различных государств, в частности, возрастает необходимость передачи информации в электронном виде, что значительно ускорит получение необходимых сведений.

Таким образом, органам внутренних дел Российской Федерации в контексте исследуемой проблематики необходимо и в дальнейшем принимать активное участие в налаживании диалога с зарубежными партнерами по развитию международного сотрудни-

чества в борьбе с преступлениями в сфере информационных технологий в целях расширения технологических и нормативно-правовых возможностей противодействия преступлениям, совершаемым в данной области.

Список литературы

1. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.) // Законодательство стран СНГ. URL: http://base.spinform.ru/showdoc.fwx?rgn=110821.

2. Ализаде В. А., Волеводз А. Г. Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания // Библиотека криминалиста. Научный журнал. 2018. № 1 (36). С. 306–333.

3. Мысина А. И. К вопросу о региональных правовых основах сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Российская юстиция. 2019. № 5. С. 20–24

4. Пузырева Ю. В. Тенденции развития транснациональной организованной преступности под влиянием пандемии COVID-19 // Актуальные проблемы медицины и биологии. 2021. № 1. С. 143–146.

5. Русскевич Е. А. Уголовное право и «цифровая преступность» : проблемы и решения : монография. М. : научно-издательский центр Инфра-М, 2020. 227 с.

Смирнов А. А.[1],
ответственный секретарь Научно-консультативного совета при Антитеррористическом центре государств – участников Содружества Независимых Государств,
кандидат юридических наук, доцент

ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ ПРОЯВЛЕНИЯМ ТЕРРОРИЗМА И ЭКСТРЕМИЗМА В ЦИФРОВОЙ СРЕДЕ В ДЕЯТЕЛЬНОСТИ КОМПЕТЕНТНЫХ ОРГАНОВ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

В условиях современного цифрового мира информационно-коммуникационные технологии активно применяются во всех сферах общественной жизни и выступают одним из ключевых драйверов развития. Вместе с тем их мощный потенциал задействуется и в деятельности преступных элементов, террористических и экстремистских акторов. Причем наблюдается постоянная адаптация противоправной активности под достижения научно-технического прогресса.

В основных документах стратегического планирования в области национальной безопасности – в Стратегии национальной безопасности Российской Федерации, Стратегии противодействия экстремизму в Российской Федерации до 2025 года, Доктрине информационной безопасности Российской Федерации и др. – идентифицируется в качестве угроз деятельность, связанная с использованием ИКТ для распространения и пропаганды идеологии терроризма и экстремизма, вовлечения в террористическую и экстремистскую активность, организации и координации противоправных акций. Так, в Доктрине информационной безопасности Российской Федерации отмечается, что террористиче-

ские и экстремистские группировки используют возможности современных информационно-коммуникационных технологий «для ведения пропагандистской и вербовочной деятельности, для информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников».

Данные угрозы зафиксированы и на международном уровне – в Глобальной контртеррористической стратегии ООН, принятой резолюцией A/RES/60/288 Генеральной Ассамблеи от 8 сентября 2006 г., Соглашении между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., Конвенции Совета Европы о предупреждении терроризма от 16 мая 2005 г., Договоре о сотрудничестве государств – участников СНГ в борьбе с терроризмом от 4 июня 1999 г., Шанхайской Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (г. Шанхай, 15 июня 2001 г.), Конвенции ШОС по противодействию экстремизму от 9 июня 2017 г. и других подобных документах.

Антитеррористическим центром государств – участников СНГ проводится большой объем аналитической работы по изучению проявлений терроризма и экстремизма в цифровой среде.

Террористическими и экстремистскими акторами возможности ИКТ применяются для реализации различных форм своей противоправной активности. Наиболее изученными в этом плане являются интернет-технологии. Видный израильский эксперт Г. Вейман выделил восемь способов использования интернета террористами:

– ведение психологической войны;

– поиск информации;

– обучение;

– сбор денежных средств;

– пропаганда;

– вербовка;

– организация сетей;

– планирование и координация террористических действий [1].

Схожий перечень приводится в специальном аналитическом докладе Управления ООН по наркотикам и преступности (UNODC) «Использование Интернета в террористических целях» [2]:

– пропаганда (в том числе вербовка, радикализация и подстрекательство к терроризму);

– финансирование;

– подготовка террористов;

– планирование (в том числе с использованием секретной связи и открытых источников информации);

– исполнение;

– кибератаки.

Экстремистская и террористическая активность в цифровой среде постоянно эволюционирует. Это связано во многом с прогрессом в сфере информационно-коммуникационных технологий, новые достижения которого берут на свое вооружение радикалы всех мастей.

В настоящий момент можно выделить следующие *основные тренды развития экстремизма в цифровой среде:*

1. Использование основных социальных сетей и мессенджеров как главных каналов экстремистской пропаганды – крупнейшие и наиболее популярные в мире социальные сети (Facebook, Instagram, YouTube, «ВКонтакте») и мессенджеры (WhatsApp, Telegram, Viber) задействуются экстремистами для распространения своих деструктивных идей и вербовки новых сторонников через многочисленные сообщества, паблики, чаты и аккаунты.

2. Активный поиск и освоение альтернативных коммуникационных платформ – в связи с усилением борьбы с виртуальным присутствием экстремистов на популярных интернет-площадках

со стороны их администрации и силовых структур радикалы постоянно ищут новые «тихие гавани», где можно было бы обосноваться им самим и их сторонникам. В качестве таковых ими рассматриваются альтернативные социальные сети (Voat, Gab, Reddit) и мессенджеры (Signal, Discord, Threema), а также имиджборды (4chan, 8chan), всегда выступавшие прибежищем маргинальных течений.

3. Ведение штормовой пропаганды – характеризует стремление радикалов максимально насытить информационное пространство экстремистским контентом и распространить его среди как можно более широкой аудитории с целью увеличения числа своих сторонников в глобальном масштабе.

4. Применение бесструктурных способов вовлечения в экстремистскую деятельность – террористические и экстремистские организации все чаще дополняют классические методы вербовки своих сторонников путем их индивидуальной психологической обработки приемами стимулирования экстремистской деятельности как отдельных лиц (например, террористов-одиночек), так и больших групп людей (например, путем вовлечения молодежи в незаконные публичные акции). Для этого радикалы не только транслируют свои идеи в инфополе, но размещают призывы и пошаговые алгоритмы совершения терактов и иных насильственных акций.

5. Использование «воронок вовлечения» – означает использование радикалами методов поэтапного вовлечения в экстремистскую деятельность путем просеивания через такую «воронку» заинтересовавшихся их идеями лиц. На верхнем уровне этой вороники действуют многочисленные группы широкого охвата, содержащие базовую информацию и пропаганду темы. Далее следуют группы более узкой тематики для тех, кто «созрел». В них уже имеются специальные условия вступления и предполагается выполнение заданий участниками. На следующем уровне действуют частные группы, которые отличает четкая тематика и наличие своей субкультуры. И на последнем этапе

уже происходит приватное общение с лицом и выполнение им действий в реальном мире [3].

5. Активное использование доксинга, в том числе в отношении силовиков – экстремисты активно оказывают информационное противодействие силовым структурам путем деанонимизации их сотрудников и последующей их травли в социальных сетях и реальной жизни. Данная технология активно использовалась в ходе массовых антиправительственных акций в Республике Беларусь в 2020 г.

6. Геймификация радикализации и экстремизма – означает применение различных игровых методик вовлечения в террористическую и экстремистскую деятельность. Включает в себя использование образов из компьютерных игр в пропагандистских материалах, онлайн-стримов в террористической и экстремистской деятельности, встраивание игровых элементов в пропагандистские материалы и коммуникационные приложения, а также создание компьютерных игр, сценарий которых связан с осуществлением экстремистской деятельности.

7. Появление новых экстремистских идеологий и «перезагрузка» старых проектов каналы радикализации – характеризует постоянное развитие идеологической базы и течений экстремизма и терроризма. Так, после разгрома МТО «ИГИЛ» упавшее знамя джихадизма подхватили движение «Талибан», вернувшее власть в Афганистане после 20-летия присутствия в стране американских войск, и другие исламистские группировки (к тому же саму террористическую организацию ИГИЛ еще рано списывать со счетов). В страны СНГ все шире проникают новые деструктивные молодежные субкультуры, способные провоцировать насилие и аутодеструктивное поведение (суицидальные сообщества, «АУЕ», «Колумбайн», «инцелы» и др.).

Антитеррористическим центром государств – участников СНГ изучается положительный опыт компетентных органов стран Содружества в области противодействия деструктивной

информационной активности террористических и экстремистских организаций в цифровой среде.

Правовую основу деятельности правоохранительных органов в рассматриваемой области составляют международно-правовые акты и национальное законодательство в сфере борьбы с терроризмом и экстремизмом. В рамках Содружества Независимых Государств принят ряд важных документов в рассматриваемой области, включая Договор о сотрудничестве государств – участников СНГ в борьбе с терроризмом 1999 г., Концепцию сотрудничества государств – участников СНГ в борьбе с терроризмом и иными насильственными проявлениями экстремизма 2005 г., Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности 2013 г., а также пакет модельных законов. Ряд значимых практических мероприятий по противодействию информационным угрозам экстремистского характера закреплен в межгосударственных программах СНГ по борьбе с терроризмом и иными насильственными проявлениями экстремизма. В настоящее время действует программа, рассчитанная на период 2020–2022 гг.

Основными направлениями противодействия проявлениям терроризма и экстремизма в цифровой среде в деятельности компетентных органов государств – участников СНГ выступают:

– мониторинг террористической и экстремистской активности в сети Интернет;

– выявление, уголовное и административное преследование лиц и организаций за совершение правонарушений террористической и экстремистской направленности;

– профилактическая работа, включая повышение цифровой грамотности;

– информационное противодействие терроризму и экстремизму, включающее противодействие кибератакам, ограничение доступа к противоправному контенту и контрпропаганду.

Особое значение в современных условиях приобретает контрпропагандистская работа. В 2020 г. Антитеррористическим

центром государств – участников СНГ издано научно-практическое пособие по данной тематике [4]. В нем на основе обобщения практического опыта работы правоохранительных органов стран Содружества и собственных научных наработок изложены практические рекомендации по организации данной деятельности.

Список литературы

1. Вейман Г. Как современные террористы используют Интернет. Специальный доклад № 116 // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analytics/-Tropina_01/.

2. Использование Интернета в террористических целях // Доклад Управления Организации Объединенных Наций по наркотикам и преступности. URL: https://www.unodc.org/do-cuments/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_the_internet_for_terrorist_purposes_Russian.pdf.

3. Самосват О. Деструктивные течения в социальных медиа и способы их выявления // Доклад на форуме «Цифровая гигиена. Молодежь в сети», 2019.

4. Смирнов А. А. Организация контрпропаганды в области борьбы с терроризмом и экстремизмом : научно-практическое пособие / под ред. А. П. Новикова. М. : АТЦ СНГ, 2020.

Фирсова Е. В.[1],
заместитель начальника отдела
по противодействию легализации доходов
от незаконного оборота наркотиков
управления организации оперативно-профилактических мероприятий, противодействия наркоугрозе
в сфере IT-технологий и легализации наркодоходов
Управления по контролю за оборотом наркотиков МВД России

ИНФОРМАЦИОННЫЕ МАТЕРИАЛЫ ГУНК МВД РОССИИ ПО ИСПОЛЬЗОВАНИЮ «ЦИФРОВЫХ ОТПЕЧАТКОВ», ИНФОРМАЦИОННОМУ ВЗАИМОДЕЙСТВИЮ С КРЕДИТНЫМИ УЧРЕЖДЕНИЯМИ И ПРОВАЙДЕРАМИ ЦИФРОВЫХ УСЛУГ, МЕХАНИЗМОВ АРЕСТА И КОНФИСКАЦИИ ВИРТУАЛЬНЫХ АКТИВОВ ПО ЛИНИИ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИКОВ

Наркобизнес активно использует услуги финансового рынка по дистанционному управлению деньгами.

Электронные средства платежа, комбинации через личный кабинет или в мобильном приложении – такие онлайн-сервисы позволяют совершать переводы «с карты на карту», «с кошелька на кошелек», «со счета абонента оператора связи на кошелек или карту» и другие варианты, в том числе в целях конвертации криптовалюты.

Распространены платежные средства, оформленные на подставных физических лиц (так называемых «дропов»), также существуют подставные «онлайн-сервисы». Операции с электрон-

[1] © Фирсова Е. В., 2022.

ными денежными средствами, транзакции с виртуальными активами практически всегда имеют финансовый след как в части маршрута, так и возможности логирования данных на веб-сервере, обнаружения цифровых отпечатков используемых устройств – то есть идентификационной информации об устройстве (например, MAC-адрес и прочие данные).

При использовании в преступной деятельности сети Интернет также остаются цифровые следы. До недавнего времени считалось, что браузеры типа TOR надежно защищают криминальные структуры, действующие через Даркнет.

Вместе с тем сегодня обнаружение и мониторинг цифровых отпечатков – это не фантастика, а данность и перспективное направление для использования в правоохранительной деятельности. На сегодняшний день интернет представляет собой:

– пропагандистскую площадку;

– средство коммуникации, вербовки продавцов и курьеров;

– способ и место сбыта наркотиков.

В контексте пандемии произошла стихийная активизация общественных процессов в виртуальном формате, в том числе и криминального характера.

Цифровизация наркорынка, повышение его технологичности, задатки которых появились более 20 лет назад, в минувшем году из-за введения мировых карантинных мер в связи с COVID-19 концентрировались настолько, что отныне рынок ряда криминальных услуг может стать исключительно дистанционным.

Подобные тенденции требуют тщательного анализа и выработки мер противодействия в формате международного сотрудничества.

Российская правоохранительная практика последних 10 лет уверенно подтверждает, что основные объемы наркотиков и психотропов сбываются через сетевую структуру бесконтактным способом. То есть с использованием интернет-ресурсов, программ-коммуникаторов, электронных и цифровых способов

оплаты. При этом сам незаконный товар оптом или в розницу доставляется заказчикам через размещение в тайниках.

Структуры бесконтактного преступления, связанного с незаконным сбытом наркотиков, состоят из нескольких фрагментов, требующих документирования и последующего наложения друг на друга для формирования убедительной системы доказательств:

– интернет-конструкция (база в используемом информационном пространстве: социальная сеть, сайт, блог, форум, хостинг-провайдер);

– интернет-коммуникация (браузеры, мессенджеры, аккаунты);

– интернет-оплата (банковская модель, небанковская модель, провайдеры платежных услуг);

– интернет-геолокация (расположение тайника с наркотиками).

Выше приведена статистика по наркопреступлениям, совершенным в России с использованием информационных и финансовых технологий. Резкий скачок произошел в первом пандемийном 2020 г. Следует признать, что эта негативная тенденция захватила и текущий год.

Основная часть (99,1 %) таких преступлений связана с незаконным производством, сбытом или пересылкой наркотиков, а также с легализацией наркодоходов.

В ответ на вызовы в системе МВД России и территориальных подразделениях органов внутренних дел в соответствии с поручением Президента Российской Федерации в 2020 г. созданы подразделения по противодействию наркоугрозе в сфере IT-технологий.

В ГУНК МВД России такой отдел функционирует в рамках одного оперативного управления параллельно с отделом по противодействию легализации доходов от незаконного оборота наркотиков.

2019 год	**2020 год**	**8 месяцев 2021 года**
Зарегистрировано 297 преступлений, связанных с легализацией наркодоходов: ст. 174 УК РФ – 6 ст. 174.1 УК РФ – 291	Зарегистрировано 296 преступлений, связанных с легализацией наркодоходов: ст. 174 УК РФ – 5 ст. 174.1 УК РФ – 291	Зарегистрировано 197 преступлений, связанных с легализацией наркодоходов: ст. 174 УК РФ – 4 ст. 174.1 УК РФ – 193
Предварительно расследовано 67 преступлений по ст.ст. 174, 174.1 УК РФ совершенных в организованных преступных формах:	Предварительно расследовано 49 преступлений по ст.ст. 174, 174.1 УК РФ совершенных в организованных преступных формах:	Предварительно расследовано 31 преступление по ст.ст. 174, 174.1 УК РФ совершенное в организованных преступных формах:
39 – ОГ И ПС, 28 – группой лиц по предварительному сговору	31 – ОГ И ПС, 18 – группой лиц по предварительному сговору	16 – ОГ И ПС, 15 – группой лиц по предварительному сговору

Переход к электронной наркокоммерции увеличил доходность наркоиндустрии.

Технологии предоставляют преступникам дополнительные ресурсы не только для конспирации и дистанционного управления людьми, задействованными в криминальной деятельности. Дистанционно перемещаются преступные товары и активы, что, безусловно, укрепляет во всем мире потенциал организованной преступности во всех ее проявлениях.

Способы расчетов за наркотики и схемы легализации наркодоходов разнообразны. Они построены на использовании инструментов, относящихся как к традиционной финансовой системе, так и к альтернативным ее видам, например, виртуальные активы.

Криптовалютой оплачивают оптовые поставки наркотиков и разовые «закладки», перечисляют вознаграждение участникам преступной деятельности, используют для решения логистических вопросов, создания интернет-магазинов и сокрытия полученных доходов.

То есть сейчас наркоденьги активно размещаются в криптосфере, которая по своей структуре децентрализована и не имеет какого-либо аналога по типу мировой системы SWIFT, позволяющей контролировать финансовые и расчетные риски. Более того, превалирующее число криптопровайдеров даже не имеют привязки к конкретной юрисдикции.

Криптовалюты переформатировали финансовую составляющую наркобизнеса, чем задали новый вектор бесконтактному сбыту, увеличив доходность электронной наркокоммерции.

Несмотря на криминальную активность различных мессенджеров, внедряющих специальные боты по автоматической продаже наркотиков, большую угрозу представляют крупные криминальные агрегаторы, сосредоточенные в даркнете, которые на своих площадках объединяют тысячи интернет-магазинов с криминальными продуктами, как говорится, «на любой вкус и кошелек».

Анализ спроса и предложения наиболее популярных для российских потребителей наркотиков на площадках даркнета вы-

строил следующий рейтинг: марихуана (части растений и соцветия) – 27 %, амфетамин – 18 %, гашиш – 15 %, мефедрон – 14 %, альфа-ПВП – 11 %, кокаин – 9 %, метадон – 3 %, героин – 2 %.

Транснациональная организованная преступность уже внедряла подобные высокотехнологичные стартапы.

Я сейчас имею в виду ныне ликвидированные благодаря полицейскому сотрудничеству маркетплейсы в сети даркнет: Silk Road, AlphaBay, Hansa, RAMP и другие.

Они стали неким алгоритмом криминальной инновационной инфраструктуры, которая представляет собой совокупность организационных, управленческих, материально-технических, финансовых, информационных, кадровых, консультационных и рекламных услуг.

По сути – это теневой прообраз легальных торговых интернет-площадок, потому что наркобизнес решил следовать по проторенному официальным предпринимательством пути, чтобы гарантированно добиться колоссального уровня криминальной прибыли.

В настоящее время преступные плацдармы в даркнете развиваются за счет функционала дополнительных сервисов.

Приведем в качестве примера, безусловно, негативного, одну известную в России и странах постсоветского пространства торговую площадку, скрытую TOR-ом, которая вместила более пяти тысяч магазинов, половина из которых осуществляет незаконный сбыт наркотиков.

Дополнительные сервисы, предлагаемые к основному виду преступной деятельности, связаны с предоставлением услуги «Dose.help». Это «калькулятор дозировок» для различных видов наркотиков в сочетании с информацией об их совместимости, о способах оказания первой медицинской помощи при передозировке, действиях по восстановлению после употребления психоактивных веществ.

Есть и параллельный проект «SafeKlad», который предназначен для информирования наркопотребителей и наркосбытчиков об участках местности, на которых правоохранительные органы осуществляют патрулирование для выявления фактов сбыта наркотиков через тайники.

Еще один сервис «what3words» позволяет зашифровать географические координаты в трех словах (доступны несколько языков) в целях конспиративного информирования о местах размещения тайников с наркотиками.

Укрепляют работоспособность маркетплейса и форумы для подбора персонала наркомагазинов, в числе которых курьеры, операторы, закладчики, региональные менеджеры и прочие лица преступной сети.

Практикуется и тестирование продаваемых наркотиков на качество. В магазинах проводятся контрольные закупки с последующим специальным анализом наркотических средств для определения чистоты и процентного содержания состава.

Созданные таким тщательным образом на IT-платформах пронаркотические проекты приносят преступникам колоссальные преступные доходы, которые образуют риски для системы как отдельных государств, так и для мирового сообщества в целом.

Основные угрозы для международной системы противодействия отмыванию доходов и финансированию терроризма (далее – ПОД/ФТ):

– транснациональный характер организованной преступности;

– финансирование организованной преступной деятельности, включая международный терроризм и экстремизм, за счет наркодоходов;

– бесконтактная форма сетевого наркосбыта;

– использование информационных и финансовых технологий;

– сокрытие активов от наркопреступлений в иностранных юрисдикциях.

Одним из ключевых элементов международного сотрудничества является четкое понимание рисковых зон.

Если говорить в целом, то сегодня – это сама модель сетевого наркосбыта, построенная на информационных и финансовых технологиях.

Заявление Президента ФАТФ Маркуса Плейера на втором заседании министров финансов и управляющих центральных банков G20, 7 апреля 2021 г.

«Financial flows, however, undermine our endeavours for strong, sustainable and inclusive growth. They create an uneven playing field where criminals gain while legitimate business suffers».

«This is happening partly due to a widespread failure in effective supervision and compliance of anti-money laundering measures. That's why the FATF wants governments to re-think their regulatory culture in this area».

«Focusing on the real money laundering or terrorist financing risks will make a big difference. High-risk transactions should face tough checks».

Незаконные финансовые потоки подрывают наши усилия по обеспечению уверенного, устойчивого и инклюзивного роста. Они создают неравное игровое поле, на котором преступники выигрывают, а законный бизнес страдает.

Частично это происходит из-за повсеместного сбоя в эффективном надзоре и соблюдении мер по борьбе с отмыванием денег. Вот почему ФАТФ хочет, чтобы правительство переосмыслили свою культуру регулирования в этой области.

Сосредоточение внимания на реальных рисках отмывания денег или финансирования терроризма будет иметь большое значение. Транзакции с высоким риском должны подвергаться жесткой проверке.

Отмечу, что ФАТФ (Группа разработки финансовых мер борьбы с отмыванием денег) отводит кредитно-финансовым учреждениям (так называемому частному сектору) одну из главных ролей в системе выявления и нейтрализации рисков от незаконных финансовых операций.

Сегодня важно понимать, что отработка финансовой составляющей организованной преступной деятельности, включая наркобизнес, должна быть безусловным приоритетом.

Более того, финансовый след в раскрытии бесконтактных преступлений часто бывает единственным способом формирования доказательственной базы, потому что он всегда оставляет цифровые отпечатки.

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ)

ФАТФ – межправительственная организация, вырабатывающая мировые стандарты в сфере противодействия отмыванию преступных доходов и финан-сированию терроризма, а также осуществляющая оценки соответствия национальных систем ПОД/ФТ государств этим стандартам.

ФАТФ создана в 1989 году по решению стран «Большой семерки» и является основным международным институтом, занимающимся разработкой имплементацией международных стандартов в сфере ПОД/ФТ.

Членами ФАТФ являются 35 стран и 2 организации, наблюдателями – 20 организаций и 1 страна.

Региональные группы по типу ФАТФ (РГТФ):

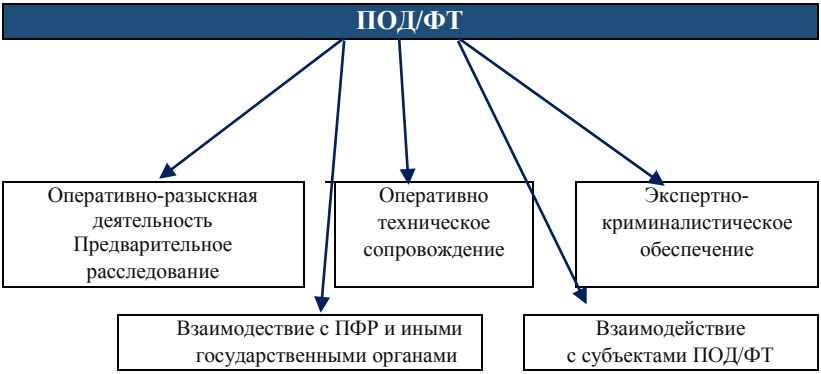
1. *Комитет экспертов Совета Европы по оценке мер противодействия легализации преступных доходов и финансированию терроризма (МАНИВЭЛ – MONEYVAL).*
2. *Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ – EAG).*
3. *Азиатско-Тихоокеанская группа борьбы с отмыванием денег (АТГ – APG).*
4. *Группа разработки финансовых мер борьбы с отмыванием денег государств Ближнего Востока и Северной Африки (МЕНАФАТФ – MENAFATF).*
5. *Группа разработки финансовых мер борьбы с отмыванием денег государств Латинской Америки (ГАФИЛАТ – GAFILAT).*
6. *Межправительственная группа по борьбе с отмыванием денег в Западной Африке (ГИАБА – GIABA).*
7. *Группа по борьбе с отмыванием денег государств Восточной и Южной Африки (ЕСААМЛГ – ESAAMLG).*
8. *Карибская группа разработки финансовых мер борьбы с отмыванием денег (СИФАТФ – CFATF).*
9. *Группа разработки финансовых мер борьбы с отмыванием денег в Центральной Африке (ГАБАК – GABAC).*

«Финансовый след» действий преступников

Доклад экспертной рабочей группы Парижского пакта при координации УНП ООН от 2014 года: «Именно финансовый след» действий преступников дает самые высокие шансы для изобличения и получения доказательств в отношении наиболее серьезных преступлений и пресечения самых значительных угроз в антинар-котической сфере».

Рекомендации Совета Европы К (80) 101: «Банковская система может играть существенную роль в предотвращении отмывания денег, а сотрудничество банков может способствовать борьбе правоохранительных органов с такими преступными явлениями».

Рекомендации ФАТФ (10,11,13,16)



То сам «финансовый след» мы ищем и находим, используя все возможности правоохранительной компетенции: и ведомственные механизмы, и ресурсы финансовой разведки, и информационное взаимодействие с частным сектором.

Нами наработана практика выявления предикатных составов к преступлениям, связанным с легализацией наркодоходов, с применением новой модели оперативного документирования: от расчетов за наркотики – к их изъятию.

Ее принцип заключается в проведении детального анализа финансовых операций по определению системы наркорасчетов и легализации наркодоходов с последующим установлением участников наркосбыта, в том числе координаторов и бенефициаров преступной деятельности, находящихся за рубежом.

В 2017 г. в России при непосредственном участии Центрального Банка создана ассоциация «ФинТех», членами которой стали ведущие российские банки. Взаимодействие с кредитно-финансовыми организациями осуществляется в порядке ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» (далее – ФЗ № 395-1).

Среди основных направлений работы Ассоциации – развитие технологий распределенного реестра, исследование и внедрение финансовых инноваций в ответ на вызов криптоиндустрии. В частности, Ассоциацией запущен пилотный проект по созданию и хранению «цифровых отпечатков».

Российские правоохранительные органы имеют доступ к данным из информационных хранилищ банков, активно используют в своей деятельности положения ст. 26 ФЗ № 395-1 о предоставлении сведений, составляющих банковскую тайну.

Такой инструмент является векторным в системе противодействия бесконтактным формам наркопреступности.

Примерный стандарт запрашиваемых данных, необходимых для начального анализа финансовой составляющей преступной деятельности, который следует запросить:

– движение денежных средств (входящие/исходящие транзакции) по счету (счетам) в банковских учреждениях либо по учетным записям в электронных платежных системах и сервисах (например, QIWI Кошелек);

– подключение услуг интернет-банкинга, привязанные к электронным платежным инструментам, номера телефонов, адреса электронной почты, IP-адреса, IMEI-коды используемого мобильного оборудования;

– биометрические данные, фото и видео изображения с устройств фиксации на банкоматах и платежных терминалах, геолакация субъектов финансовых операций;

– возможные обменные операции, связанные с виртуальными активами.

Вместе с тем практика показывает, что объем информации, разрешенной к получению правоохраной, должен быть гораздо шире, поскольку в настоящее время кредитные учреждения, в том числе операторы платежных систем, обладают эксклюзивными программными комплексами, позволяющими получать и детализировать финансовую информацию, которая является оперативно-значимой для выявления и раскрытия тяжких и особо тяжких составов наркопреступлений, а также фактов легализации наркодоходов.

Данные о клиентах оцифровываются кредитно-финансовыми учреждениями с использованием все более совершенных программных продуктов.

Безусловно, кредитные организации практикуют новые технологии, прежде всего, в целях повышения безопасности своих активов.

Каждый желающий кредитоваться проверяется по нескольким методикам. В результате формируются некие «кредитные досье» с данными из целого спектра источников, которые могут быть значимыми и для правоохранительных органов.

Следует отметить, что сами клиенты уже продолжительный период времени являются главными поставщиками личной информации. Каждая транзакция по пластиковой карте отображает весомую часть жизненных предпочтений пользователя (потреби-

тельские детали, касающиеся места покупки, суммы чека, категории товара). Информация аккумулируется по большому числу параметров (с точки зрения рисков и с точки зрения их потребительских предпочтений).

Например, бонусные программы от банков. Они как раз созданы для сбора таких данных. Подобные аналитические ресурсы построены на технологиях big data. В таком формате действия клиента отслеживаются мгновенно и контролируются сотни параметров.

Банки постоянно совершенствуют практику сбора информации по «цифровым следам». Отслеживаются все действия в виртуальном пространстве (время присутствия на тех или иных сайтах, участие в различных группах в социальных сетях, используемые ссылки и т. д.) и на основе собранных данных составляет «диспозициональную модель личности человека», которая прогнозирует предрасположенность платить по долгам).

Кроме того, запускаются смежные проекты по социальным сервисам: онлайн-запись к врачам, оплата налогов, юридическая помощь и так далее. Все это также способствует получению информации о различных аспектах жизни человека.

Итог следующий: банковские приложения в гаджетах и пластиковая карточка «запоминают» электронные следы своего пользователя, что является колоссальным источником информации.

Масштабы данных о потребителях кредитно-финансовых услуг также разрастаются за счет солидарности с операторами мобильной связи (например, геолокация).

Для повышения информированности кредитно-финансовой сферы разрабатываются и другие «пилотные» направления, которые крайне важны и для правоохранительной деятельности. Например, система биометрической верификации клиентов по фотоизображению (распознавание происходит за две секунды).

В целях противодействия наркопреступлениям, совершаемым с использованием IT-технологий, разработаны и введены в

эксплуатацию специальные программные продукты, обеспечивающие поиск в медиасфере оперативно значимой информации.

С их помощью формируются аналитические срезы из даркнета о магазинах, территориях обслуживания, предлагаемых товарах и ценах, отзывах и комментариях покупателей. Такие отчеты имеют встроенную систему визуализации данных, а также возможность наблюдения за интересующими объектами в течение заданных периодов.

Использование преступниками электронных и цифровых средств существенно затрудняет нашу работу. Тем не менее мы совершенствуем свои приемы и методы.

В нашем арсенале имеются средства, позволяющие отслеживать финансовый профиль преступников, в том числе в криптосфере. Например, с помощью аналитического программного инструмента с онлайн-доступом «Прозрачный блокчейн», который разработан в результате совместного проекта Росфинмониторинга и Российской академии наук. Технология способна оценивать и анализировать связи участников криптовалютной среды с криминальными торговыми интернет-площадками.

Принимая во внимание трансграничный формат работы криптосервисов, особую актуальность приобретают вопросы, характеризующие международную позицию в отношении соответствующих рисков и угроз, включая сегмент правоохранительного сотрудничества.

Стандарты ФАТФ требуют, чтобы юрисдикции принуждали к регистрации на их территории провайдеров услуг в сфере виртуальных активов, и чтобы они собирали, хранили и предоставляли властям информацию о клиентах.

Какие сведения можно получить?
Регистрационные данные, идентификационные данные, журналы учетных записей пользователей, информация о криптокошельке, информация о сделках с криптоактивом, информация о рекламных объявлениях пользователей и информация о торговых чатах

Информация по биткойн-кошельку:
– баланс биткоин-кошелька;
– список адресов-получателей (все адреса, назначенные пользователем для получения биткойн-транзакций);
– список входящих транзакций (отметка времени UTC, адрес получателя, сумма, описание);
– список исходящих транзакций (отметка времени UTC, адрес получателя, сумма, описание)

Информация о биткойн-сделках:
– ID (уникальный ID-номер, присвоенный конкретной сделке);
– дата начала сделки;
– дата условного депонирования (дата, когда сделка завершена и биткойн отправлен покупателю);
– способ оплаты (наименование способа оплаты, только для онлайн-торгов);
– имя пользователя покупателя (имя пользователя учетной записи LocalBitcoins, покупающего биткойны);
– имя пользователя продавца (имя пользователя учетной записи LocalBitcoins, продающего биткойны);
– сумма сделки FIAT (сумма сделки, выраженная в валюте, указанной в объявлении);
– сумма сделки Bitcoin (сумма сделки в биткойнах);
– биткойн цена (цена биткойна, выраженная в валюте торговой сделки);
– валюта (трехбуквенный стандартный код ISO (международная организация по стандартизации)

Эта информация необходима правоохранительным органам для идентификации лиц, которые проводят операции с виртуальными активами, чтобы использовать ее для анализа, планирования мероприятий и как убедительное доказательство виновности преступников.

Недоработки юрисдикций в этом направлении могут негативно влиять не только на эффективность своих национальных систем, но и затрагивать международные интересы, принимая во

внимание транснациональный характер организованной преступности и террористической деятельности, а также трансграничность перемещения незаконных финансовых потоков.

В настоящее время в мире действуют различные режимы регулирования выпуска и оборота виртуальных активов и деятельности связанных с этими услугами провайдеров. Указанные обстоятельства порождают неравномерную доступность информации и неравные возможности для обмена информацией между юрисдикциями.

С учетом этого в 2018 г. ФАТФ предприняла согласованные со своими участниками меры для обновления международных стандартов в области ПОД/ФТ и распространила их действие на виртуальные активы и провайдеров услуг в сфере виртуальных активов. Обновленная версия руководства будет обсуждаться на пленарной сессии.

Но уже сейчас понятно, что определение поставщиков таких услуг будет расширено и под него подпадут компании независимо от используемых технологий, а исходя из критерия о деятельности по передаче и обмене виртуальных активов.

Отметим, что под это определение подходят и валюты видеоигр, которые можно обменять на внутриигровые товары, но также и на наличные деньги на определенных вторичных рынках. На первый взгляд это может показаться необоснованным, но власти некоторых государств уже имели дело с валютами видеоигр, которые использовались преступными группировками для отмывания денег.

Информационное взаимодействие с криптоплощадками в настоящее время возможно только в электронной форме и посредством функции обратной связи. Установление такого диалога обязательно для нужд правоохраны.

Спорным представляется вопрос о тайне информации о виртуальных активах в сравнении с банковской.

Вместе с тем категория тайны применительно к цифровым финансовым активам и цифровой валюте не конкретизирована. Кроме того, сведения, аккумулированные в информационных системах, формируются по правилам публичного блокчейна, то есть открытой сети, что позволяет любому участнику изучить историю транзакций, а также установить размер пересылаемых между адресами сумм.

В России Федеральный закон «О цифровых финансовых активах» вступил в силу с января 2021 г. Как в целом в мире, нам пока не удалось охватить регулированием все области данного явления.

МВД России является участником законотворческой деятельности по вопросам криптосферы.

Наше главное управление стало инициатором разработки механизма ареста и конфискации цифровых активов. В частности, параметров создания и функционирования так называемых «государственных криптокошельков».

Если кратко, то, по нашему мнению, наиболее практичной представляется «технология мультиподписи», которая выступает защитным инструментом, реализуемым в криптовалютных операциях.

Все кошельки с множеством подписей работают по одному и тому же принципу совместного использования закрытых ключей.

Это создает дополнительный уровень безопасности, поскольку к активам нельзя получить доступ, используя только один ключ.

В практике правоохранительных органов такой вид кошелька может быть использован на всех стадиях уголовного судопроизводства для включения участвующих в конкретном деле авторизаторов: оперативный сотрудник, следователь, курирующий прокурор.

Указанная модель позволит избежать сложной процедуры передачи установленных цифровых активов от одного участника процессуальной стадии другому, а также нивелировать коррупционные риски.

Стратегия государственной антинаркотической политики Российской Федерации на период до 2030 года
Угрозы национальной безопасности в сфере оборота наркотиков (п. 9) *г) появление новых форм противоправной деятельности организованных групп и преступных сообществ (преступных организаций), усиление ими конспирации каналов поставки и сбыта наркотиков с использованием инновационных коммуникационных и других новых технологий;* *е) использование новейших финансовых инструментов в целях легализации (отмывания) доходов, полученных в результате незаконного оборота наркотиков, а также применение новых способов оплаты приобретаемых наркотиков;* *ж) масштабное использование сети «Интернет» для пропаганды незаконного потребления наркотиков;* *к) использование доходов, полученных в результате незаконного оборота наркотиков, для финансирования деятельности международных террористических организаций*
Противодействие легализации (отмыванию) доходов, полученных в результате незаконного оборота наркотиков, является стратегической задачей антинаркотической политики (пп. г п. 11)
Меры направленные на сокращение количества преступлений и правонарушений, связанных с незаконным оборотом наркотиков (п. 16) *г) развитие механизмов выявления и пресечения преступлений, связанных с незаконным оборотом наркотиков и совершаемых с использованием современных информационных технологий, в том числе организованными группами и преступными сообществами (преступными организациями);* *д) противодействие легализации доходов, полученных в результате незаконного оборота наркотиков, в том числе совершенствование системы выявления финансовых операций в этой области, установление членов организованных групп и преступных*

сообществ (преступных организаций), действующих в финансовой сфере, а также субъектов экономической деятельности, используемых для легализации этих доходов;
е) укрепление взаимодействия между правоохранительными органами Федеральной службой по финансовому мониторингу и негосударственными организациями в целях дальнейшего совершенствования тактических приемов разрушения экономических связей наркопреступности;
ж) совершенствование мер, направленных на пресечение использования электронных платежных инструментов при совершении преступлений, связанных с незаконным оборотом наркотиков, включая введение внесудебного механизма блокировки банковских счетов (вкладов) и электронных средств платежа по инициативе субъектов оперативно-разыскной деятельности на срок до 30 суток для физических и (или) юридических лиц, в отношении которых имеются сведения об их причастности или достаточные основания подозревать их в причастности к незаконному обороту наркотиков (в том числе в целях финансирования терроризма);
з) усиление контроля за осуществлением финансовых операций по внесению денежных средств на банковские счета и электронные средства платежа, а также установление административной ответственности для лиц, передающих выпущенные (эмитированные) на их имя финансовые инструменты третьим лицам, в случае установления фактов использования таких инструментов в преступной деятельности, в том числе связанной с незаконным оборотом наркотиков

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО	
Конвенция Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма (Варшава 2005 год) (Глава IV) (Федеральный закон от 26 июля 2017 года № 183-ФЗ)	Рекомендации ФАТФ (36–38)
Второй дополнительный протокол Европейской конвенции о взаимной правовой помощи по уголовным делам (Страсбург, 2001 год) (Федеральный закон от 6 июня 2019 года № 120-ФЗ)	
Стороны в максимально возможной степени оказывают друг другу помощь в связи с проведением расследований, судебных преследований и сопутствующих процедур в отношении отмывания денег, предикатных преступлений и финансирования терроризма с целью определения и отслеживании орудий, доходов и другого имущества, подлежащего конфискации	

В России обсуждаемые сегодня риски закреплены в качестве угроз национальной безопасности в Стратегии государственной антинаркотической политики на период до 2030 г.

В завершение отмечу, что обсуждаемые сегодня проблемные вопросы требуют решения не только внутри отдельно взятого государства, а на международном уровне.

Необходимо перезагрузить формат нашего правоохранительного сотрудничества в условиях новых рисков и угроз.

Но, как говорят, чтобы началось что-то новое, что-то должно закончиться. Безусловно, это COVID-пандемия. В этом, я уверена, мы солидарны.

Будьте здоровы!

Харламов С. О.[1],
начальник кафедры конституционного и муниципального права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент

Егоров С. А.[2],
заместитель начальника кафедры конституционного и муниципального права Московского университета МВД России имени В.Я. Кикотя, кандидат юридических наук, доцент

Хрустов А. А.[3],
соискатель кафедры конституционного и муниципального права Московского университета МВД России имени В.Я. Кикотя

ПРАВОВЫЕ ОСНОВЫ МЕЖГОСУДАРСТВЕННОГО И ВНУТРИГОСУДАРСТВЕННОГО СОТРУДНИЧЕСТВА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОЙ МИГРАЦИИ

Незаконная миграция является широко распространенным явлением, несмотря на все национальные и глобальные усилия по противодействию ей. На постсоветском пространстве ее формации во многом способствуют процессы строительства независимых государств, созданных после распада СССР. Данные процессы сопровождаются рядом этнических и территориальных конфликтов, что в свою очередь приводит к постоянному реформированию миграционных институтов и попыткам международных преступных группировок использовать ситуацию в своих целях.

Основными странами назначения миграционных потоков внутри СНГ являются Россия и Казахстан, а за пределами Содружества – Европейский союз, куда постоянно растет миграция, в том числе незаконная. Благодаря существующему безвизовому режиму стран СНГ, Украины и Грузии друг с другом (за отдельными исключениями), большинство мигрантов въезжают на их территории законно в целях трудоустройства. Несмотря на развитую национальную нормативно-правовую базу в области противодействия незаконной миграции, незаконная занятость трудовых мигрантов является общей чертой в СНГ. За годы независимости страны СНГ построили систему коллективной ответственности в борьбе с этим явлением, однако большое число трудовых мигрантов все еще находится вне правового поля.

Вопросы противодействия нелегальной миграции нашли освещение в большом числе законодательных актов как национального, так и наднационального уровня. Совершенствование взаимодействия между государствами по вопросам противодействия трансграничной преступности является одним из приоритетных направлений деятельности правоохранительных структур различных стран мира. Такие факторы глобализационных процессов, как развитие коммуникаций и информационных технологий, рост открытости национальных границ, свободное перемещение товаров, услуг, капиталов и рабочей силы и др., облегчили распространение трансграничной преступности. Очевидно, что современная преступность имеет качественно новые формы, что требует адекватной реакции со стороны правоохранительных органов различных государств. Для достижения эффективности функционирования системы противодействия международной преступности, государства разрабатывают комплекс методов взаимодействия своих правоохранительных структур, которое может осуществляться в различных формах, а также совершенствуют законодательную базу в рассматриваемой сфере.

На наднациональном уровне следует выделить Конвенцию ООН против транснациональной организованной преступности (2000 г.). Основная цель этого документа состоит в аккумулировании усилий государств, направленных на противодействие транснациональной организованной преступности. Данный документ выступает правовым базисом для выстраивания системы актов, регулирующих, в том числе, и вопросы противодействия незаконной миграции.

Стоит отметить, к примеру, Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, который дополняет вышеназванный международный нормативный правовой акт. Протокол устанавливает меры, направленные на противодействие незаконному ввозу мигрантов различными способами. В данном акте отмечается необходимость объединения усилий государств в решении этой проблемы, актом предусмотрены механизмы международного сотрудничества, а также спектр мер, включая социально-экономические, которые надлежит реализовать государствам – участникам с целью противодействия незаконному ввозу мигрантов.

Предупреждение, расследование и уголовное преследование применительно к преступным деяниям, которые касаются незаконного ввоза мигрантов и носящим трансграничный характер при участии организованной преступной группы, опираются на положения рассматриваемого Протокола. Кроме того, данный международный нормативный правовой акт регулирует отношения по защите прав лиц, которые стали объектом таких преступлений. Понятийный аппарат Прокола применяется и в национальном законодательстве Российской Федерации, в частности, данный документ дает определения таким понятиям, как «незаконный ввоз мигрантов», а также «незаконный въезд». Применение этих понятий, закрепленных в действующем законодательстве государств – участников, способствует единообразию подходов в определении криминализируемых ими деяний.

Россия является участницей международных документов регионального уровня в сфере противодействия нелегальной миграции. В 2010 г. было подписано Соглашение о сотрудничестве по противодействию нелегальной трудовой миграции из третьих государств между Правительствами Российской Федерации, Республики Беларусь, Республики Казахстан (позднее присоединились Кыргызская Республика и Республика Армения). Данное соглашение выступает основным правовым базисом для совместной деятельности государств – участников в рассматриваемой сфере. Государства, подписавшие документ, согласованно подходят к установлению мер по противодействию незаконным миграционным потокам из третьих государств. Для этой цели они устанавливают правила выявления и учета трудовых мигрантов, осуществляющих трудовую деятельность без законных оснований, выявления и пресечения каналов и структур, которые занимаются организацией и содействием перемещению нелегальных трудовых мигрантов. Соглашением предусмотрен мониторинг численности нелегальных мигрантов, а также установлены правила применения отдельных мер принуждения к названной категории граждан. Государства – участники Соглашения совместными усилиями вырабатывают комплекс мер, которые ограничивают въезд нелегальных мигрантов для осуществления ими трудовой деятельности на территории государств – сторон, ранее применявших отдельные меры принуждения к таким лицам. Большая работа в рамках Соглашения проводится в отношении ограничения распространения недостоверной информации в рассматриваемой сфере. Посредством слаженной работы компетентных органов государств – участников Соглашения возможна реализация единой политики противодействия незаконным миграционным потокам.

Документ предусматривает основные организационно-правовые формы сотрудничества государств – участников Соглашения в сфере противодействия незаконно миграции. Наиболее распространенными формами сотрудничества являются:

– обмен информацией;

– обмен опытом работы;

– подготовка и повышение квалификации сотрудников правоохранительных структур государств;

– организация и проведение оперативно-профилактических мероприятий и специальных операций по противодействию нелегальной трудовой миграции;

– заключение соглашений о реадмиссии и др.

Следует подчеркнуть, что Россия является полноправным членом международного сообщества, принимающим активное участие в совместном с другими государствами поиске наиболее действенных путей и средств борьбы с нелегальной миграцией. Рассмотренное Соглашение предусматривает наиболее широкий спектр форм сотрудничества государств в решении данной проблемы.

Стоит подчеркнуть, что международное сотрудничество Российской Федерации в сфере противодействия незаконной миграции сосредоточено преимущественно на взаимодействии с государствами постсоветского региона, чему есть вполне логичное объяснение – Россия представляет собой крупнейший в регионе центр притяжения мигрантов из стран бывшего СССР, прежде всего, из Центральной Азии и Закавказья. Можно с уверенностью говорить о том, что национальная миграционная политика Российской Федерации выстраивает структуру и динамику миграционных процессов в регионе.

К примеру, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с пре-

ступностью 1998 г. регулирует вопросы сотрудничества в предупреждении, пресечении, выявлении, раскрытии и расследовании преступлений, связанных с незаконной миграцией.

Тем самым, правовая регламентация противодействия нелегальной миграции в качестве своих направлений имеет:

– совершенствование миграционного учета и контроля;

– совершенствование ответственности за нелегальную миграцию и стимулирование и поддержку законной миграции;

– скоординированную деятельность госструктур на федеральном, региональном и муниципальном уровнях по противодействию нелегальной миграции;

– обеспечение межгосударственного сотрудничества в сфере противодействия нелегальной миграции и др.

Таким образом, можно наблюдать определенную преемственность в вопросе определения ключевых направлений противодействия нелегальной миграции, которые отражены в рассмотренных выше актах. Соглашением 2010 г. установлен более широкий перечень направлений в сравнении с Концепцией, которая была принята в рамках СНГ в 2004 г. Это обеспечивает более эффективную координацию совместных усилий государственных структур стран-участников данного Соглашения в рассматриваемой сфере.

Стоит отметить и многочисленные двусторонние соглашения Российской Федерации по противодействию незаконной миграции. Если сравнивать такие соглашения с многосторонними международными правовыми актами, содержащими общие принципы взаимодействия государств, фиксирующими базовые программные положения, а также включающими отсылочные нормы к национальному законодательству, то они отличаются детализацией и конкретизацией в регулировании межгосударственных отношений с учетом специфики проявлений нелегальной миграции. Та-

кая особенность двусторонних соглашений позволяет рассматривать их в качестве более гибкого инструмента правового регулирования межгосударственных отношений.

Если рассматривать национальный уровень, то в полной мере задачи и направления борьбы с незаконной миграцией определены в Концепции государственной миграционной политики Российской Федерации на период до 2025 г.

Концепция определяет необходимость:

– совершенствования законодательства по вопросам борьбы с нелегальной миграцией;

– совершенствования мер ответственности за нарушение законодательства Российской Федерации в сфере миграции;

– создания и совершенствования системы иммиграционного контроля посредством фиксации данного термина в системе законодательных актов Российской Федерации, определения круга уполномоченных органов и их компетенции;

– совершенствования системы государственного контроля въезда и пребывания иностранных граждан на территории Российской Федерации;

– противодействия организации каналов нелегальной миграции, в том числе за счет повышения защищенности паспортно-визовых и иных документов, позволяющих идентифицировать личность;

– создания инфраструктуры для реализации процедуры реадмиссии и обеспечения региональными органами государственной власти функционирования специальных учреждений для содержания иностранных граждан и лиц без гражданства, подлежащих административному выдворению или депортации;

– совершенствования взаимодействия между полномочными ведомствами, в том числе информационного обмена на национальном уровне, а также с компетентными органами иностранных государств по вопросам противодействия нелегальной миграции;

– разработки и принятия программ борьбы с нелегальной миграцией, проведения совместных с другими государствами оперативно-профилактических мероприятий;

– усиления работы информационного и разъяснительного характера с гражданами – работодателем, в целях нивелирования рисков нарушений миграционного законодательства Российской Федерации.

Также следует отметить ряд документов стратегического характера, которые затрагивают сферу противодействия нелегальной миграции: Стратегия национальной безопасности Российской Федерации (2015 г.), Стратегия противодействия экстремизму в Российской Федерации до 2025 г., Концепция внешней политики Российской Федерации, Концепция общественной безопасности в Российской Федерации, Основы государственной пограничной политики Российской Федерации и др.

Все это позволяет выработать всесторонний подход к формулированию приоритетных задач и направлений борьбы с незаконной миграцией в России. В свою очередь определение направлений позволяет выработать законодательные меры противодействия незаконной миграции. В настоящее время комплекс таких мер определен на уровне большого количества законодательных актов федерального уровня, которые регулируют различные общественные отношения. В качестве примера можно привести Федеральный закон «О правовом положении иностранных граждан в Российской Федерации». Отдельные механизмы законодатель установил в Федеральных законах от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию», от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации», от 18 июля 2006 г. № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации», УК РФ, КоАП РФ и других.

Указанные механизмы, среди прочего, предполагают пресечение коррупционных проявлений, криминальных деяний в рамках осуществления государственной миграционной политики, незамедлительную реакцию на факты нарушений в этой сфере. Реагирование осуществляется посредством применения административной и уголовной ответственности. Такие механизмы также предполагают пресечение незаконной трудовой деятельности иностранцами и лицами без гражданства. К ним можно отнести, к примеру, порядок применения отдельных принудительных мер: депортации, выдворения и реадмиссии иностранных граждан, которые преступили закон. В числе таких механизмов можно выделить и установление запрета на въезд таких граждан в Российскую Федерацию на протяжении определенного временного периода в связи с нарушением ими российского законодательства. К числу рассматриваемых механизмов относится и обеспечение пограничного контроля, функционирование информационных систем учета иностранцев, включая тех, чье пребывание на территории страны является нежелательным, реализация контроля за совпадением цели въезда на территорию Российской Федерации реальным целям въезда и нахождения в стране.

В настоящее время административно-правовая система контроля пребывания иностранных граждан и лиц без гражданства на территории России определяется следующими нормативными правовыми документами.

1. Конституция Российской Федерации, которой принадлежит главенствующая позиция в иерархии нормативных правовых актов, ей должны соответствовать все остальные нормативные правовые акты. Конституция Российской Федерации характеризуется прямым действием на всей территории страны, являясь отправной точкой нормотворчества и правоприменения. Данный документ устанавливает основы правого положения личности, базовые принципы, на которых построена вся система рассмат-

риваемых правоотношений. Непосредственно для рассматриваемой категории лиц ч. 3 ст. 62 Конституции Российской Федерации разработан национальный режим пребывания в пределах государства с оговоркой о ряде исключений, определенных федеральными законами или международными договорами.

2. Федеральный закон от 25 июля 2002 г. № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации». Данный законодательный акт содержит ряд определений, являющихся базовыми для правоприменительной практики, в частности, в нем определены понятия «иностранный гражданин», «лицо, не имеющее гражданства». В нем представлены в обобщенном виде основания и порядок пребывания и проживания иностранцев на территории Российской Федерации. Сферой регулирования данным нормативным правовым актом является пласт отношений, связанных с перемещением указанной категории граждан по территории Российской Федерации, осуществлением ими трудовой деятельности, установлены права и ограничения в вопросах государственной и муниципальной службы. В данном законодательном акте также освещаются вопросы миграционного учета названной категории граждан и меры ответственности, предусмотренные за нарушения требований миграционного законодательства.

3. Федеральный закон от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию». Устанавливает режим пребывания рассматриваемых субъектов, в том числе указывает необходимый перечень документов, основания и условия их получения. Имеет статус специального законодательного акта, более подробно описывающего нормы основного закона государства и Федерального закона от 25 июля 2002 г. № 115-ФЗ. Кроме того, положениями этого закона устанавливаются ограничения, при которых лицу мо-

жет быть отказано в возможности покинуть или посетить Российскую Федерацию, также устанавливается особый порядок въезда и выезда, распространяемый на рассматриваемые группы лиц.

4. Федеральный закон от 18 июля 2006 г. № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации». Законом определяются права и обязанности иностранцев, связанные с данной процедурой, последовательность действий по осуществлению миграционного учета и основания снятия с миграционного учета (документы, сроки и т. д.), основы взаимодействия данной категории лиц с органами, осуществляющими учет, их полномочия, а также ответственность в случае несоблюдения порядка осуществления миграционного учета.

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ. Данный кодифицированный законодательный акт является основополагающим в области установления оснований и принципов административной ответственности и наказания, а также условий освобождения от административной ответственности и наказания. КоАП РФ устанавливает принципы законодательства об административных правонарушениях, перечень видов нарушений законодательства и мер ответственности, условия применения наказаний, субъектов, уполномоченных осуществлять производство по делам об административных правонарушениях. В КоАП РФ определен механизм обеспечения производства по такой категории дел, а также реализации актов уполномоченных органов в названной сфере. Что касается иностранцев, то они несут административную ответственность на одинаковых условиях с гражданами России, однако КоАП РФ содержит ряд составов административных правонарушений, специальным субъектом которых является только лицо, являющееся гражданином другой страны, или лицо,

которое не имеет гражданства. Также в КоАП РФ для иностранцев устанавливается специальный вид наказания – административное выдворение за пределы страны.

6. Уголовный кодекс Российской Федерации, в который включены специальные нормы, устанавливающие уголовную ответственность за совершение преступлений в сфере регулирования миграционных потоков (ст.ст. 322.1, 322.2 и 322.3). Социальная обусловленность ответственности за вышеназванные правонарушения (преступления) продиктована важными причинами. Все лица, фиктивно поставленные на учет по месту пребывания или зарегистрированные в жилом помещении, становятся бесконтрольными и могут совершить на территории населенного пункта различного рода правонарушения, в том числе и уголовные. Отсутствие сведений о месте нахождения лиц, фиктивно поставленных на учет, а также зарегистрированных и совершивших противоправные деяния, усложняет процесс их раскрытия и расследования.

Таким образом, положения нормативных правовых актов наднационального уровня, международных соглашений, законодательных актов тех государств, правовая связь с которыми имеется у конкретного лица, являются базой формирования правового статуса иностранных граждан и лиц без гражданства. Кроме того, правовое положение иностранных граждан также определяется законодательством страны пребывания. Миграционный учет иностранных граждан и лиц без гражданства в Российской Федерации регулируется рядом специальных нормативных правовых актов.

В завершение следует подчеркнуть, что современные миграционные процессы подталкивают государства к координированным совместным действиям в вопросе противодействия этому негативному социальному явлению. Очевидно, что в настоящее время существует острая необходимость продолжения междуна-

родного диалога в выработке комплекса мер, которые эффективно будут предотвращать нелегальный въезд мигрантов в государства, позволят создать гибкую систему управления миграционными потоками. Для России приоритетными направлениями в контексте международного сотрудничества по вопросам противодействия нелегальной миграции должно стать поступательное развитие международных связей со специализированными международными организационными структурами, такими как УВКБ ООН, МОМ, ОБСЕ, ПРООН, государственными и негосударственными организациями. Помимо прочего существует необходимость активизации сотрудничества с европейскими государствами в области внешней трудовой миграции и ее контроля.

Список литературы

1. Конвенция Организации Объединенных Наций против транснациональной организованной преступности (принята в г. Нью-Йорке, 15 ноября 2000 г.) // НПП «Гарант-сервис». URL: https://base.garant.ru/2561303/.

2. Протокол против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности (принят в г. Нью-Йорке, 15 ноября 2000 г. Резолюцией 55/25 на 62-м пленарном заседании 55-й сессии Генеральной Ассамблеи ООН) // Бюллетень международных договоров. 2005. № 2. С. 34–46.

3. Соглашение о сотрудничестве по противодействию нелегальной трудовой миграции из третьих государств (принято в г. Санкт-Петербург, 19 ноября 2010 г.) // Собрание законодательства Российской Федерации. 2012. № 5. Ст. 541.

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступностью (Москва, 25 ноября 1998 года) // АО «Кодекс». URL: https://docs.-cntd.ru/document/901732327.

5. Соглашение между Правительством Российской Федерации и Правительством Республики Узбекистан об организованном наборе и привлечении граждан Республики Узбекистан для осуществления временной трудовой деятельности на территории Российской Федерации (заключено в г. Москве 5 апреля 2017 г.) // Собрание законодательства Российской Федерации. 2018. № 6. Ст. 802.

6. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // URL: http://www.pravo.gov.ru.

7. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 01.07.2021) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

8. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 01.07.2021) // Собрание законодательства Российской Федерации. 2002. № 1 (ч. 1). Ст. 1.

9. Федеральный закон от 15 августа 1996 г. № 114-ФЗ (ред. от 01.07.2021) «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию» // Собрание законодательства Российской Федерации. 1996. № 34. Ст. 4029.

10. Федеральный закон от 25 июля 2002 г. № 115-ФЗ (ред. от 02.07.2021) «О правовом положении иностранных граждан в Российской Федерации» // Собрание законодательства Российской Федерации. 2002. № 30. Ст. 3032.

11. Федеральный закон от 18 июля 2006 г. № 109-ФЗ (ред. от 24.02.2021) «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации» // Собрание законодательства Российской Федерации. 2006. № 30. Ст. 3285.

12. Безруков А. В., Невирко Д. Д. Современное состояние миграционного законодательства и роль судебных решений в защите прав мигрантов // Миграционное право. 2018. № 2. С. 35–39.

13. Бекяшев Д. К., Иванов Д. В. Международно-правовое регулирование вынужденной и трудовой миграции. М., 2013. С. 182.

14. Воздействие мирового экономического кризиса на трудовую миграцию из Кыргызстана в Россию: качественный обзор и количественное исследование. Бишкек, 2009. 110 с.

15. Жеребцов А. Н., Захарова В. А., Натхо Р. М. Проблема юридического определения понятия «миграция населения» в российском миграционном законодательстве, науке и практике // Современное право. 2019. № 11. С. 47–51.

16. Жеребцов А. Н., Малышева Е. А. Административная ответственность в миграционном праве Российской Федерации : материальные и процессуальные аспекты : научно-практическое пособие. М. : Юстицинформ, 2019. С. 56.

Ховавко С. М.[1]*,*
доцент кафедры
оперативно-разыскной деятельности и специальной техники
Крымского филиала Краснодарского университета МВД России,
кандидат юридических наук, доцент

ТЕХНИЧЕСКОЕ ОТОЖДЕСТВЛЕНИЕ ЛИЧНОСТИ В ОПЕРАТИВНО-РАЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Интенсивное развитие научно-технического прогресса и внедрение достижений науки и техники в оперативно-розыскную деятельность дает основание утверждать о наличии относительно новой формы отождествления личности – техническое отождествление личности на основе биометрической идентификации. Техническое отождествление личности основано на компьютерном анализе биометрических персональных данных.

Биометрические персональные данные в соотв. с ч. 1 ст. 12 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» , это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 ст. 152.

Физиологические особенности человека условно делятся на две группы:

– статические: папилярный рисунок пальца; венозный рисунок пальца или руки; сетчатка глаза; радужная оболочка глаза; изображение лица;

– динамические: голос; рукописный почерк; клавиатурный почерк; цифровой почерк; походка; сердечный ритм; распознавание жестов.

Из биологических особенностей человека для целей биометрической идентификации подходит на современном этапе ДНК.

Техническое отождествление личности осуществляется с применением аппаратно-программных средств, которые включают в себя технические средства фиксации биометрических данных лица, представляющего оперативный интерес (технические средства фото-, видео-, аудиофиксации) и специализированных программ (распознавания по геометрии лица, распознавания по походке, распознавания по голосу и др.). Такое отождествление возможно даже при отсутствии потерпевших и очевидцев преступления, а также материальных следов преступления – отождествление личности происходит практически без участия человека исключительно аппаратно-программными средствами, которые анализируют статические и динамические признаки личности, зафиксированные на фото-, видео- или аудиозаписях, оказавшихся в распоряжении оперативных подразделений (записи телефонных переговоров, аудио-, фото-, видео-и файлы, размещенные в сети Интернет, записанные АПК «Безопасный город» или обнаруженные при проведении других оперативно-разыскных мероприятий).

Техническое отождествление личности на основе биометрической идентификации существенно расширяет возможности органов, осуществляющих оперативно-розыскную деятельность, так как осуществляется достаточно оперативно и исключительно аппаратно-программными средствами, а оперативный сотрудник лишь оценивает результаты такого отождествления.

Условиями достоверности результатов технического отождествления личности на основе биометрической идентификации с применением аппаратно-программных средств является в первую очередь научность и объективность применяемых компьютерных

программ распознавания биометрии и технических средств фиксации анализируемых признаков отождествляемого лица, что должно подтверждаться соответствующей сертификацией. Также необходимым условием технического отождествления личности на основе биометрической идентификации является наличие интегрированных с аппаратно-программными средствами объективных банков биометрической информации (фото, видео-, аудиоучеты органов, осуществляющих оперативно-розыскную деятельность, других государственных органов, а также единая биометрическая система и биометрические системы коммерческих банков). В единой биометрической системе для идентификации используются одновременно два параметра – голос и лицо (фотоизображение лица человека) [3]. Наряду с единой биометрической системой и независимо от нее многие крупные банки (Сбербанк», Альфа-банк и др.) достаточно давно внедряют собственные биометрические системы, а счет образцам биометрии, собранной коммерческими банками, может идти на миллионы [4; 5].

В ближайшей перспективе Министерством внутренних дел Российской Федерации планируется создание централизованного банка биометрических данных россиян и иностранцев. Новая система позволит устанавливать личности людей по отпечаткам пальцев и изображению лица. Создать Федеральную информационную систему биометрических учетов планируется в рамках опытно-конструкторской работы до 2023 г. За это время предполагается разработать программное обеспечение, необходимое для ведения и использования централизованного банка данных биометрических параметров граждан Российской Федерации, иностранных граждан и лиц без гражданства.

Предполагается, что технология позволит идентифицировать личность, а также неопознанные тела по дактилоскопической информации, изображению лица и геномной информации. Разработка будет взаимодействовать с объединенной поисковой федеральной системой генетической идентификации.

Впервые идея создания общей информационной системы с биометрическими данными граждан была высказана главой МВД Владимиром Колокольцевым в 2014 г. Тогда он говорил о необходимости объединить ресурсы дактилоскопической и фоноскопической информации, лабораторий ДНК-анализа, комплексов биометрической идентификации личности и фиксации передвижения транспортных средств. Кроме того, МВД готовит распознавание преступников не только по лицу, но и голосу, радужке глаза, татуировкам и, возможно, по походке.

Комплексное распознавание лица по различным биометрическим параметрам, безусловно, будет способствовать повышению степени достоверности результатов такого отождествления. При оценке результатов технического отождествления личности на основе биометрической идентификации нельзя исключать возможные объективные ошибки и умышленное искажение злоумышленниками своих биометрических параметров (например, применение компьютерных программ изменения голоса при общении по техническим средствам связи или умышленное изменение походки при передвижении в поле зрения камер наружного наблюдения, использование грима, силиконовых или медицинских масок для сокрытия лица и т. п.). Поэтому результаты технического отождествления личности на основе биометрической идентификации не могут расцениваться как абсолютно достоверные, а требуют всесторонней оценки и проверки со стороны оперативного сотрудника.

Таким образом, дальнейшее совершенствование и использование в деятельности оперативных подразделений технического отождествления личности на основе биометрической идентификации является перспективной и эффективной формой отождествления личности, которая может существенно улучшить работу оперативных подразделений по выявлению, пресечению и раскрытию преступлений, розыску скрывающихся преступников и выполнению других задач оперативно-разыскной деятельности.

Список литературы

1. Маляров Е. А. Структурный анализ оперативно-разыскного мероприятия «отождествление личности» // Алтайский юридический вестник. 2020. № 3 (31). С. 136–140.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/.

3. Оперативно-розыскная деятельность : учебник для студентов вузов, обучающихся по направлению подготовки «Юриспруденция» / [А. В. Богданов и др.]. 5-е изд., перераб. и доп. М., 2020.

4. Официальный сайт единой биометрической системы // URL: https://bio.rt.ru.

5. Пятков И. Цена вопроса // Коммерсантъ. URL: https://kommersantru.turbopages.org/turbo/kommersant.ru/s/doc/4096563.

6. Еремина А., Ястребова С., Астапенко А. Сбербанк собрал биометрические данные миллиона людей // Ведомости. URL: https://vedomostiru.turbopages.org/turbo/vedomosti.ru/s/finance/articles/2018/12/13/789277-sberbank-biometricheskie-dannie.

7. Кузьмин Н. А. К вопросу о понятии и содержании коррупции // Вестник Московского университета МВД России. 2020. № 6. С. 128–131.

8. Кузьмин Н. А. К вопросу о необходимости закрепления в действующем законодательстве понятия «коррупционное преступление» // Вестник Московского университета МВД России. 2020. № 2. С. 196–198.

9. Квалификация взяточничества (по материалам судебной практики): научно-практическое пособие / [М. Г. Жилкин и др.]. М., 2019.

Чекунов И. Г.[1],
заместитель генерального директора
по юридическим вопросам и безопасности
«Лаборатории Касперского»,
кандидат юридических наук

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Компетенции на линии «следователь – оперативный сотрудник» в сфере работы с цифровыми следами схожи, различие скорее процессуальное: следователь собирает доказательства в рамках полномочий, данных УПК, деятельность оперативного работника регламентирована в первую очередь ФЗ «Об ОРД». И те, и другие должны обладать определенными базовыми знаниями и навыками, иначе даже при привлечении специалистов им будет затруднительно понять методы и результаты собирания и исследования цифровых следов.

Разделение проходит по линии следователь/оперативник и специалист /эксперт».

Следователь/оперативный сотрудник должен владеть методикой и тактикой осуществления расследования уголовных дел в сфере компьютерной информации и по иным делам, по которым осуществляется поиск, сбор и исследование цифровых следов, а также владеть базовыми знаниями по компьютерным и сетевым технологиям.

Следователь/оперативный сотрудник обязан знать:

– общие принципы работы компьютерных устройств, осведомленность об основных компонентах и их функциях. Наиболее распространенные виды вычислительных устройств: компьютеры, мобильные устройства, игровые устройства, «умные» вещи (IoT), серверы;

[1] © Чекунов И. Г., 2022.

– общие принципы устройства электронных носителей информации, их виды, а также осведомленность о способах хранения информации, например, на сервере в RAID-массиве;

– общее понятие о файловой системе как средстве для хранения и поиска данных;

– осведомленность о возможных проблемных ситуациях в криминалистическом исследовании различных видов устройств и носителей информации;

– принципы построения локальных сетей, понимание того, как устроен интернет (на аппаратном уровне передачи сетевого трафика и общее понимание сетевых протоколов);

– общее понимание задач информационной безопасности как состояния защищенности компьютерной информации, таких ее свойств как конфиденциальность, целостность, доступность, подлинность, подотчетность, неотказуемость и достоверность способов и методов ее обеспечения.

Следователь должен:

– повышать осведомленность об использовании в следственной практике технико-криминалистических средств и средств программного обеспечения, предназначенных для обнаружения, фиксации и исследования цифровых следов, взаимодействовать с организациями, осуществляющими экспертную поддержку судопроизводства;

– повышать осведомленность о возможности использования электронных ресурсов, содержащих базы данных о вредоносных программах и информацию об их использовании, а также иные сведения, имеющие значение для расследования (WhoIs, Virustotal, Securlist);

– обеспечивать эффективное взаимодействие между следователями, отдельными подразделениями органов, осуществляющих оперативно-разыскную деятельность в сфере противодействия компьютерным преступлениям;

– владеть компьютерной и другой оргтехникой, необходимым программным обеспечением, уметь пользоваться справочными информационными системами.

Специалист должен обладать следующими компетенциями:

– познания в архитектуре вычислительных систем;

– опыт администрирования компьютеров под управлением различных операционных систем (Windows, Linux, MacOS, iOS, Android и т. д.);

– познания в сфере сетевых технологий (локальных и глобальной сетей, сетевого оборудования, сетевых протоколов);

– знание языков программирования;

– навыки обратной разработки и исследования вредоносного кода;

– владение тактическими приемами и методами производства следственных действий;

– осведомленность в правоприменительной практике и в криминальных тенденциях в сфере компьютерной информации.

Общепрофессиональные компетенции:

– способность к прогнозированию развития ситуаций и выработке сценариев поведения;

– отраслевая и межотраслевая коммуникация.

Также необходимо обладать определенными личностными качествами – выдержкой, дисциплинированностью, целеустремленностью, инициативностью и организаторскими качествами.

Помимо вышесказанного и с учетом разнообразия компьютерных экспертиз (например, программно-компьютерные, аппаратно-компьютерные, компьютерно-сетевые и т. п.) эксперт должен знать, понимать и владеть внутренней архитектурой и принципами работы ЭВМ; навыками использования операционной системы, сетевых технологий, средств разработки программного обеспечения.

Эксперт должен обладать способностью к формализации в предметной области с учетом ограничений используемых методов исследования и готовностью обосновать принимаемые решения, осуществлять постановку и выполнение экспериментов по проверке корректности и эффективности.

Важным качеством для специалиста в данной области является владение навыками моделирования, анализа и использование формальных методов деконструирования программного обеспечения и методами чтения, понимания и выделения главной идеи прочитанного исходного или дизассемблированного кода.

В связи с вышесказанным, я хотел бы отметить, что осенью 2019 г. в «Лаборатории Касперского» появился проект Kaspersky Antidrone, который на сегодняшний день не имеет аналогов в России. Сегодня эксперты Kaspersky Antidrone обладают патентами в сфере защиты от гражданских беспилотных летательных аппаратов в Российской Федерации и уже реализовали ряд проектов для критической инфраструктуры, масштабных публичных мероприятий, а также частной собственности.

Так, например, зимой прошлого года система противодействия БПЛА была испытана на Челябинском трубопрокатном заводе, одном из крупнейших промышленных объектов региона.

В ходе эксперимента система успешно отразила попытки несанкционированного проникновения гражданских дронов через охраняемый периметр.

Kaspersky Antidrone представляет собой масштабируемую модульную платформу на базе искусственного интеллекта для обнаружения и защиты от дронов гражданского назначения.

Гибкий программный интерфейс Kaspersky Antidrone позволяет интегрировать различные типы устройств от ведущих мировых производителей и поставлять их в качестве единого комплекса, конфигурация которого уникальна для каждого заказчика.

Уникальное решение позволяет защищать воздушное пространство объектов любого масштаба, а модульная архитектура системы поддерживает масштабирование, что позволяет говорить о создании в будущем единой системы защиты от БПЛА.

Kaspersky Antidrone состоит из программно-аппаратного комплекса (ПАК), рабочего места оператора, средств классификации дронов и модуля нейтрализации, который прерывает каналы управления летательного аппарата. Kaspersky Antidrone обнаруживает беспилотник еще до того, как тот достигнет защищаемого периметра, и определяет расположение его пилота на земле. При этом используется комбинация различных технологий:

– радиочастотное-сканирование (радиус обнаружения до 5000 м);

– оптические и инфракрасные-камеры (радиус обнаружения до 1500 м);

– радары (радиус обнаружения до 2000 м);

– лазерные сканеры (радиус обнаружения до 1000 м);

– микрофоны и др.

Все данные поступают на сервер и обрабатываются с использованием нейросетей в реальном времени. Поддерживается также широкий перечень устройств нейтрализации, заставляющих дрон вернуться на точку взлета за счет подавления управляющего сигнала пульта пилота: конструктивно практически любой гражданский беспилотник при потере управления возвращается в зафиксированную при старте точку взлета, используя бортовую навигационную систему.

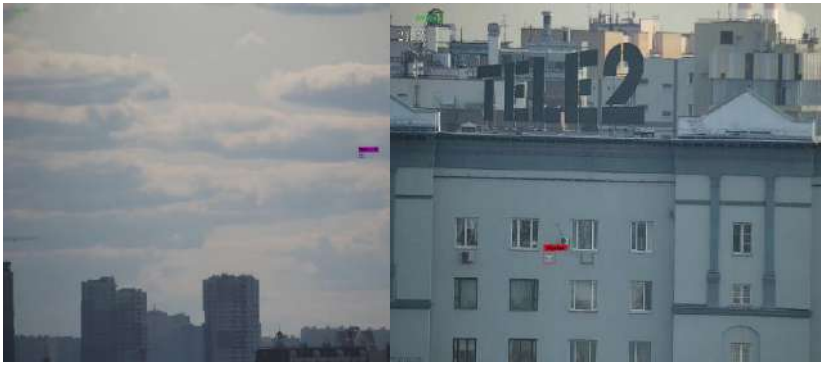
В самом крайнем случае (и при наличии соответствующего разрешения от регулирующих органов) в Kaspersky Antidrone могут быть интегрированы средства принудительного приземления дронов.

Ключевыми преимуществами комплекса являются программное обеспечение, модульность, автономность и полностью автоматический режим работы. Кроме того, компания готова адаптировать конфигурацию программно-аппаратного комплекса под индивидуальные нужды заказчика.

Надо выделить, что Kaspersky Antidrone Neural Network – это специально обученная нейронная сеть, которая позволяет определить тип и модель беспилотника, а также исключает возможность срабатывания системы на птиц и прочие объекты. На данный момент нейронная сеть определяет: беспилотные летательные аппараты, птиц, самолеты и вертолеты.

Благодаря запатентованным технологиям и широкому набору используемых признаков, искусственный интеллект распознает даже новые или самодельные виды беспилотных летательных аппаратов.

Нейронная сеть не только осуществляет классификацию целей в автоматическом режиме, но и поддержку оператора в принятии решении об уровне угрозы или о последующих действиях по нейтрализации.



Нейронная сеть уделяет особое внимание обнаружению малых объектов в условиях ограниченной видимости, при этом делает это быстрее и лучше, чем любой оператор-человек на практически любых типах камер и при сложной освещенности.

Сборник тезисов выступлений

СТРАТЕГИЧЕСКИЕ АСПЕКТЫ СОТРУДНИЧЕСТВА ОРГАНОВ ВНУТРЕННИХ ДЕЛ (ПОЛИЦИИ) СТРАН СОДРУЖЕСТВА В ПРОТИВОДЕЙСТВИИ ТРАНСНАЦИОНАЛЬНОЙ ПРЕСТУПНОСТИ В КОНТЕКСТЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА ПОД ЭГИДОЙ СОВЕТА МИНИСТРОВ ВНУТРЕННИХ ДЕЛ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

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