рамках осуществления правовой помощи или содействия расследованию фактов торговли людьми.

Таким образом, в настоящее время в рамках деятельности универсальных и региональных международных организаций принят целый ряд международных договоров, которые закрепляют соответствующие системы борьбы с торговлей людьми. Пристальное внимание мирового сообщества к указанной проблеме имеет свои положительные результаты, так как многие современные государства существенно изменили не только внутригосударственное отраслевое законодательство, но и правоприменительную практику с целью противодействия указанному преступному явлению. Однако в настоящее время все еще актуальной является проблема нежелания отдельных государств, в том числе и тех, на территории которых активно развиваются преступные группировки, занимающиеся торговлей людьми, ратифицировать вышеназванные международные нормативно-правовые акты и принимать на себя соответствующие обязательства, что создает существенные угрозы для международного мира и правопорядка.

Гаврилин Юрий Викторович,
начальник кафедры управления
органами расследования преступлений
Академии управления МВД России,
доктор юридических наук, доцент

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ, СОВЕРШЕННЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ОПЫТ АКАДЕМИИ УПРАВЛЕНИЯ МВД РОССИИ

Сегодня в юридической литературе и на научных форумах разного уровня очень много говорится о цифровой трансформации преступности. Цифровая трансформация преступности – это не просто фигура речи, научная абстракция. По итогам 2020 года каждое четвертое преступление в стране совершается с использованием информационных технологий. В Москве же этот показатель еще больше – почти 40%. При этом современные преступники активно применяют новейшие средства противодействия расследованию – технологии подмены телефонных номеров, IP-телефонию, совершают криминальные транзакции в цифровых валютах.

Первая тенденция выражается в развитии дистанционных способов совершения преступлений, при которых исключается непосредственный контакт соучастников как между собой, так и с потерпевшими.

Коммуникация при этом осуществляется с использованием социальных сетей, мессенджеров, электронной почты и иных Интернет-сервисов. Результаты применения дистанционных технологий управления протестной активностью ярко видны на примере разнообразных «цветных революций», инициируемых в разных точках Земли.

Вторая тенденция касается технологий сокрытия преступлений, основанных на использовании сервисов анонимизации личности в цифровом пространстве. Анонимизиция направлена на подмену либо блокирование информации, позволяющей установить лицо, совершившее Интернет-соединение (прежде всего, IP-адрес и MAC-адрес) и затрудняет установление лица, совершающего те или иные действия в виртуальном пространстве, включая противоправные. Именно возможности существования некой «приватности» в Интерент-пространстве как некого «естественного права» является питательной средой, создающей впечатление о ложной безнаказанности в цифровой среде.

Третья тенденция связана с использованием криптовалют в криминальных взаиморасчетах. Зачастую сокрытие следов криминальных финансовых транзакций осуществляется посредством конвертации денежных средств в виртуальную валюту, оборот которой не подконтролен для уполномоченных государственных органов. Цифровая валюта широко используется в финансировании экстремистской деятельности, что сегодня будет наглядно представлено в докладах выступающих.

Четвертая тенденция обусловлена ростом масштабов межрегиональной и трансграничной преступности, использованием при совершении преступлений сетевой инфраструктуры, расположенной за пределами Российской Федерации. Дистанционные способы совершения преступлений открывают широкие возможности для причинения ущерба гражданам России с территории стран СНГ, преимущественно Украины, уровень международного сотрудничества в правоохранительной сфере с которой находится на невысоком уровне, что превращает ее в своего рода криминальный анклав, чем активно пользуются преступники в своих противоправных целях.

Пятая тенденция выражается в формировании криминального рынка противоправных услуг в информационно-телекоммуникационной сфере, связанных с предоставлением доступа к частной переписке в мессенджерах, социальных сетях и посредством электронной почты. Данные услуги открыто рекламируются в мессенджере Telegram и обсуждаются на Darknet-форумах. Там же широкое распространение получили услуги по «пробиву», то есть получению сведений об интересующем лице из закрытых источников, в том числе из баз данных операторов связи, банков, правоохранительных органов и др.

Шестая тенденция наметилась в связи с развитием технологий искусственного интеллекта и возможностями их использования в

противоправной деятельности. Уже сегодня широкое распространение приобрели интеллектуальные технологии синтезирования речи, видеоизображений, с помощью которых можно создавать аудио- и видеозаписи для манипуляции людьми, распространения фальшивых новостей и видеосюжетов. Данные технологии могут быть применены и при совершении преступлений с использованием методов «социальной инженерии».

Все обозначенные тенденции в полной мере проявляются в отношении преступлений экстремисткой направленности.

Благоприятную среду для совершения подобных преступлений обеспечивает активное развитие технологий высокоскоростного доступа в сеть Интернет, программных средств мгновенного обмена сообщениями (мессенджеров), социальных сетей, и других цифровых технологий.

Однако сказанное выше не является основанием для отказа от прогресса, формирования цифровых фобий и панических настроений.

Неслучайно федеральный проект «Информационная безопасность» в рамках национальной программы «Цифровая экономика Российской Федерации» предусматривает свыше полусотни мероприятий, направленных на нейтрализацию приведенных выше угроз[1].

Оптимизм вызывают сообщения о создании Росфинмониторингом специального сервиса «Прозрачный блокчейн», обеспечивающего анонимизацию транзакций в криптовалюте. Сервис обеспечивает анализ транзакций с криптовалютами и выявление тех из них, которые имеют признаки нарушения закона, в частности тех, которые совершаются для оплаты незаконных товаров и услуг, например, для покупки наркотиков, а также для отмывания денег[2].

Роскомнадзор приступил к использованию технологий искусственного интеллекта для повышения скорости и точности выявления противоправной информации в сети Интернет. Новое программное обеспечение системы мониторинга позволяет проверять около 12 млн. текстовых материалов в сутки и выявлять незаконную информацию с точностью не ниже 85%. Применение нейросетей позволяет повысить производительность работы экспертов более чем в 14 раз[3].

В этих условиях как никогда важна роль образовательных организаций, обеспечивающих подготовку кадров, способных эффективно

---

[1] Паспорт федерального проекта «Информационная безопасность». URL: https://digital.ac.gov.ru/poleznaya-informaciya/material/ (дата обращения: 01.06.2021).

[2] Встреча Президента Российской Федерации В.В. Путина с директором Росфинмониторинга Ю.А. Чиханчиным. URL: https://www.fedsfm.ru/releases/4939 (дата обращения: 01.06.2021).

[3] Технологии искусственного интеллекта повышают оперативность и эффективность выявления незаконной информации в интернете. URL: https://rkn.gov.ru/ news/rsoc/ news73266.htm (дата обращения: 01.06.2021).

противодействовать новым вызовам и угрозам, а также разрабатывающих научно-теоретические основы противодействия киберпреступности. Обозначенное направление на протяжении ряда лет является приоритетным для Академии управления МВД России и реализуется на системной основе, включая в себя проведение всероссийских онлайн-семинаров, включение в образовательный процесс профильных учебных дисциплин, а также соответствующие научные исследования.

С 2019 года в рамках цикла «Противодействие преступности в условиях развития информационного общества» в Академии проводятся всероссийские онлайн-семинары, посвященные отдельным аспектам противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий, включая вопросы выявления, раскрытия и расследования кибермошенничеств, дистанционного сбыта наркотиков, использования криптовалют в финансировании экстремистской деятельности и пр.[1] К проведению подобных мероприятий привлекаются наиболее авторитетные специалисты правоохранительных органов, органов государственной власти, а также негосударственных организаций – субъектов цифровой инфраструктуры, компетенции которых получили широкое признание: Лаборатория Касперского, Группа АйБи, Сбербанк и др.

С 2020 года в образовательный процесс по учебным планам магистратуры включена дисциплина «Организация противодействия преступления, совершенным с использованием информационно-телекоммуникационных технологий», направленная, в зависимости от направления подготовки, на формирование у обучаемых следующих компетенций:

– организация участия в формировании основных направлений деятельности органов внутренних дел в сфере киберпреступности;

– обеспечение совершенствования нормативно-правового регулирования отношений в рассматриваемой сфере;

– организация внутреннего и внешнего взаимодействия участников расследования;

– материально-техническое, ресурсное и кадровое обеспечение и др.

Существенное внимание уделяется основным направлениям государственной политики в области развития информационного общества; принятию и классификации информационно-телекоммуникационных технологий; правовому регулированию

[1] Гаврилин Ю.В., Парадников А.Г. Совершенствование выявления, раскрытия и расследования хищений, совершенных с использованием информационных банковских технологий (по итогам всероссийского онлайн-семинара) // Труды Академии управления МВД России. № 2 (54). 2020. С. 123–130; Гаврилин Ю.В. Противодействие цифровой трансформации наркопреступности (по итогам Всероссийского онлайн-семинара) // Труды Академии управления МВД России. 2020. № 4 (56). С. 122–130.

отношений в данной сфере; уголовно-процессуальной и криминологической характеристике преступлений, совершенных с использованием информационно-телекоммуникационных технологий; уголовно-процессуальным, криминалистическим и организационным основам их выявления, раскрытия и расследования. Второй раздел учебной дисциплины посвящен особенностям противодействия отдельным видам преступлений, совершенных с использованием информационно-телекоммуникационных технологий: против личности, против собственности, экономической направленности, в сфере незаконного оборота наркотиков, экстремистской направленности и пр.

Научное обеспечение включает в себя подготовку и защиту диссертационных исследований А.А. Балашовой[1], Г.З. Гаспаряном[2], Е.П. Шульгиным[3] и др., а также проведение ряда международных научно-практических конференций: «Криминалистика и новые вызовы современности» (58-е криминалистические чтения); «Криминалистика в условиях информационного общества» (59-е ежегодные криминалистические чтения); «Стратегическое развитие системы МВД России: состояние, тенденции, перспективы»; «Противодействие преступлениям, совершенным с использованием Интернет-технологий: правовые, криминалистические и организационные аспекты» (61-е ежегодные криминалистические чтения); «Развитие учение о противодействии расследованию и мерах по его преодолению в условиях цифровой трансформации преступности» (62-е ежегодные криминалистические чтения). Исследования в данном направлении активно и научный поиск ответов на новые вызовы современности активно продолжаются.

[1] Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании. Дис. … к.ю.н. по специальности 12.00.09 – уголовный процесс.

[2] Гаспарян Г.З. Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий. Дис. … к.ю.н. по специальности 12.00.12 – криминалистика, судебно-экспертная деятельность, оперативно-розыскная деятельность.

[3] Шульгин Е. П. Правовые и организационные основы деятельности органов досудебного расследования МВД Республики Казахстан, осуществляющих производство в электронном формате. Дис. … к.ю.н. по специальности 12.00.11 – судебная деятельность, прокурорская деятельность, правозащитная и правоохранительная деятельность.