получных районов и использование альтернативных маршрутов для перевозок также снижают риски.

Следует отметить, что помимо указанных мер немаловажных моментом будет являться налаженный момент взаимодействия между кампаниями и правоохранительными органами, что позволит сотрудникам легче получать интересующую их информацию, а также получать доступ к важным объектам, архивам, что существенно облегчит процесс раскрытия преступления или даже поспособствует выявлению причин и условий, способствовавших совершению преступления.

В завершение конечно же следует сказать о таком этапе раскрытия рассматриваемой категории преступлений, как стадию моделирования версий, в которых будут отображены возможные варианты совершения преступлений, пути отхода-подхода, определение хода мыслей преступников. Значимость данного этапа подтверждается в работе В.Л. Шаповникова, в который сказано, что «прежде, чем выдвинуть версию, необходимо тщательно проанализировать имеющуюся информацию, которая была получена в результате оперативно-розыскных мероприятий и следственных действий[1]».

Дырма С.В.

Академия управления МВД России (г. Москва)

Предупреждение вовлечения граждан в совершениях IT-преступлений

На рубеже XXI века использование передовых технических и программных достижений современных информационных технологий в повседневной жизни для каждого из нас стало в достаточной степени обыденным. Мало кто в современном обществе может представить свою жизнь без использования мобильного телефона с доступом в глобальную сеть Интернет, а также банковских карт или соответствующих финансовых онлайн-приложений[2]. Современные информационно-коммуникационные технологии, используемые при осуществ-

[1] Шаповников В.Л. Особенности раскрытия и расследования краж грузов, совершаемых на железнодорожном транспорте // Уголовный процесс, криминалистика: Ленинградский юридический журнал. Санкт-Петербург, 2015. URL: https://cyberleninka.ru/article/n/osobennosti-raskrytiya-i-rassledovaniya-krazh-gruzov-sovershaemyh-na-zheleznodorozhnom-transporte/viewer (дата обращения: 25.04.2025).

[2] Дырма С.В. Развитие IT-преступности как триггер совершенствования деятельности органов внутренних дел : сборник научных трудов V Всероссийской научно-практической конференции; под общ. ред. С.А. Буткевича. Симферополь, 2023. С.113-117.

лении межличностной социальной коммуникации, стерли барьеры времени и расстояния, что безусловно упрощает процессы информационного обмена между людьми, создавая комфортные условия для развития современного общества.

Вместе с тем в последние годы наблюдается активное использование современных информационно-коммуникационных технологий при совершении преступлений.

Так, согласно анализу статистических сведений в период с 2018 по 2024 год, при общем снижении количества преступлений, зарегистрированных в Российской Федерации, совершенных с использованием информационно-коммуникационных технологий[1] увеличилось более чем на 300 %[2].

Вышеуказанный анализ статистических сведений о состоянии преступности сделать вывод о том, что мы живем в эпоху цифровой трансформации преступности. В 2018 году доля IT-преступлений в общей структуре преступности в Российской Федерации составляла 8,8 %, а по итогам 2024 года указанная доля увеличилась до 40 %. Таким образом, в настоящее время четыре из десяти, совершаемых в стране преступлений, является IT-преступлениями.

Определяя главные отличительные особенности IT-преступлений от иных общественно опасных деяний, следует отметить, что программные и аппаратные средства информационных технологий (мобильные телефоны, Интернет и иные средства коммуникации) используются для реализации объективной стороны преступления. Например, при совершении IT-преступлений против собственности современные информационно-коммуникационные технологии используются для осуществления коммуникации злоумышленника с потенциальным потерпевшим, либо используются для хищения денежных средств с банковских счетов различными способами.

В структуре IT-преступности наибольшую долю составляют именно преступления против собственности, к числу которых относятся кражи и мошенничества. Доля подобных преступлений в структуре IT-преступности по итогам 2024 года составила 63,5 %.

С развитием различных средств мобильной коммуникации повсеместное распространение в теневом сегменте Интернета получила криминальная информация о способах совершения отдельных видов имущественных преступлений в киберпространстве, способах конспирации преступной детальности, использования программных средств анонимизации в сети и т. п.

Высокий уровень доступности подобного рода криминальной информации в глобальной сети создает условия для вовлечения в совершение краж и мошенничеств в киберпространства все новых и новых лиц, как в роли исполнителей преступлений, так и в роли пособников (например для обналичивания денежных средств, полученных преступным путем и их перевода через различ-

[1] Далее – IT-преступления.

[2] Согласно анализу статистических сведений ФКУ «ГИАЦ МВД России».

ные платежные системы с целью противодействия процессу расследования преступления).

Средства мобильной коммуникации достаточно активно используются и при осуществлении взаимодействия между участниками преступных групп, совершающих IT-преступления.

Рассматривая термин «вовлечение» с позиции уголовного права, отметим, что статьей 150 Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за вовлечение несовершеннолетнего в совершение преступления. По мнению Г.А. Решетниковой, данный запрет обусловлен объективными потребностями общества в уголовно-правовой охране интересов семьи и несовершеннолетних[1], что в целом не вызывает никаких сомнений.

В данной статье вовлечение будет рассматриваться не с позиции указанной нормы права, а как деятельность отдельных субъектов, направленная на побуждение мотивации у граждан (не всегда несовершеннолетних) к совершению IT-преступлений.

Вовлечение как совокупность активных действий лица (лиц), направленных на привлечение лица к совершению IT-преступлений, по нашему мнению, состоит из двух основных элементов:

1. Создание позитивных или негативных мотивирующих факторов для лица, привлекаемого в качестве исполнителя или пособника для совершения IT-преступлений.

2. Использование позитивных или негативных мотивирующих факторов для склонения лица к совершению IT-преступлений.

Как уже ранее было отмечено, существенную долю в структуре IT-преступности составляют кражи и мошенничества. В связи с чем одним из наиболее распространенных мотивов к совершению подобных преступлений является корыстный. Как правило, лица, вовлекающие в совершение имущественных IT-преступлений, обещают гражданам быстрый и сравнительно высокий уровень заработка при минимальном риске быть привлеченным к уголовного ответственности. Например, гражданин в социальной сети находит предложения о работе «курьером», основная функция которого состоит в получении наличных денежных средств от граждан с последующим их зачислением на различных банковские счета или электронные кошельки. При этом злоумышленник инструктирует вовлекаемое в преступную деятельность лицо о мерах конспирации (автоматическое удаления архива сообщений в мессенджере, определенная линия поведения при задержании сотрудниками правоохранительных органов и т. п.).

В ряде случаев при вовлечении граждан в совершение отдельных имущественных IT-преступлений злоумышленники в качестве гаранта требуют от гражданина снять видео с изображением своего лица, паспорта, места прожи-

[1] Решетникова Г.А. Вовлечение несовершеннолетнего в совершение преступления: поиск оптимальной нормы // Судебная власть и уголовный процесс. 2022. № 1. С. 64-71.

вания, либо заснять видеоролик, содержащий информацию о дискредитации Вооруженных Сил Российской Федерации, действующих в целях защиты интересов Российской Федерации и ее граждан. В дальнейшем злоумышленники с использованием полученных компрометирующих материалов могут вовлекать граждан в совершение не только IT-преступлений, но и правонарушений экстремистского характера.

Так, злоумышленники, располагающие подобными компрометирующими материалами на гражданина могут склонить его к нарушению норм статьи 20.3.3 Кодекса Российской Федерации об административных правонарушениях, предусматривающей административную ответственность за публичные действия, направленные на дискредитацию исполнения Вооруженными Силами Российской Федерации и другими госорганами своих полномочий за пределами РФ, так и к совершению преступлений, предусмотренных статьей 275 Уголовного кодекса Российской Федерации (Государственная измена).

По нашему мнению, реализация мер профилактики вовлечения граждан в совершения IT-преступлений должна базироваться на следующих направлениях:

1. Осуществление информационно-пропагандистской работы с привлечением средств массовой информации и освещением фактов вовлечения граждан в совершения различных видов IT-преступлений, в том числе фактов совершения указанными лицами в последующем правонарушений экстремистского характера.

2. Повышение общего уровня цифровой грамотности населения в части использования некоторых программных продуктов информационных технологий в своей повседневной деятельности путем проведения информационно-просветительских акций с различными категориями населения.

3. Проведение целевых профилактических мероприятий в образовательных организациях с целью формирования высокого уровня правосознания у несовершеннолетних.

Гайбашев Р.Н.

Академия управления МВД России (г. Москва)

Системное управление рисками при проведении оперативно-розыскных мероприятий в сфере незаконного оборота наркотиков

В условиях роста масштабов и усложнения форм преступной деятельности в сфере незаконного оборота наркотиков (НОН) оперативно-розыскные мероприятия (ОРМ) становятся все более рискованными для личного состава органов внутренних дел (ОВД). Помимо прямой угрозы жизни и здоровью сотрудников, операции в данной сфере сопряжены с повышенными процессуальными рис-