роста мошенничеств (ст. 159 УК РФ), совершаемых с использованием ИТТ, в 2021 г. в СФО составили 9,7%, в Российской Федерации – 13,4%.

Факторами роста рассматриваемых преступлений кроме обозначенных ранее причин являются растущая популярность виртуализации личной жизни, доступность и простота использования информационно-телекоммуникационных технологий, вовлечение в сферу цифровых экономических отношений лиц, мало информированных и не подготовленных к возможным угрозам кибербезопасности, наличие средств анонимизации пользователей и массовое внедрение криптографических средств безопасности в сети Интернет.

Тем не менее динамика изучаемых видов преступности не дает оснований утверждать о преобладании в дальнейшем способов совершения, связанных исключительно с использованием ИТТ. Наблюдается некоторое плато, которое может дать как незначительный рост, так и стабилизацию. В этом заслуга органов внутренних дел, которые на текущий момент уделяют особое внимание противодействию подобным преступлениям, основываясь на концепции подготовки квалифицированных кадров в области информационно-телекоммуникационных технологий, и правильная государственная политика в сфере кибербезопасности. Не остаются в стороне и коммерческие компании, внедрение в деятельность современных систем обеспечения кибербезопасности способствует скорейшему расследованию киберинцидентов и противостоянию киберугрозам. Внедрение Роскомнадзором технических средств противодействия угрозам (ТСПУ) способствует ограничению к обороту противоправной информации и доступу к ресурсам, ранее использующимся для осуществления преступной деятельности, например сети Tor. Начало действия закона о «приземлении» иностранных ИТ-компаний[1] с целью соблюдения законодательства России обеспечит эффективный механизм для профилактики и раскрытия преступлений, совершаемых с использованием сети Интернет.

Резюмируя, можно утверждать, что преступления, совершаемые с использованием информационно-телекоммуникационных технологий, являются обратной стороной цифровой трансформации общества, но в системе преступность-население-государство приобретают регулируемые формы и не способны масштабно криминализировать складывающиеся электронные экономические, общественные и социальные коммуникации.

Щербич Л.А.,

кандидат юридических наук, доцент
Университет прокуратуры Российской Федерации (г. Москва)

Щербич А.Н.

Информационно-аналитическое управление ГУНК МВД России (г. Москва)

Цифровизация наркобизнеса

Наркоситуация в Российской Федерации остается достаточно сложной, о чем свидетельствует количество зарегистрированных преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ[2]. В 2021 г. их количество составило 179,7 тыс., в 2020 г. – 189,9 тыс.[3] На протя-

[1] О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации : Федеральный закон от 01.07.2021 № 236-ФЗ.

[2] По тексту приведены данные статистической отчетности, формируемой ФКУ «ГИАЦ МВД России».

[3] Раздел 1 формы № 1-МВ-НОН (код 171).

жении последних десяти лет удельный вес наркопреступлений остается уровне 9-10% в общем массиве криминальных деяний, зарегистрированных в стране.

Особенностью незаконного оборота наркотиков в России за последние пять лет является широкое использование информационно-телекоммуникационных технологий (IT-технологии) для распространения практически всех видов подконтрольных веществ на пространстве субъектов Российской Федерации. Этот процесс быстро эволюционирует одновременно с увеличением пользователей цифровой техники и участников виртуальной среды, их психологической адаптацией к подобного рода коммуникации, чувством мнимой свободы и безнаказанности в Интернете.

Следует констатировать, что современные технологичные формы распространения наркотических средств и психотропных веществ не дали существенных преимуществ правоохранительным органам в борьбе с их предложением на черном рынке веществ, свободная реализация которых запрещена.

В целях своевременного реагирования на изменения состояния наркоситуации и обеспечения в стране правопорядка Генеральной прокуратурой Российской Федерации в 2017 г. была введена новая статистическая отчетность (по форме «4-ЕГС»), позволяющая организовать статистическое наблюдение за развитием этого процесса.

В 2021 г. на фоне общего снижения числа зарегистрированных на территории России преступлений (на 1,9%) на учет поставлены 517,7 тыс. уголовно наказуемых деяний, совершенных с использованием IT-технологий или в сфере компьютерной информации, из которых 52 тыс., или 10,1%, выявлены в сфере незаконного оборота наркотиков, что на 9,6% превышает данные за предшествующий год (по ст. 228.1, 228.2, 228.4, 230, 234 УК РФ)[1].

Остается актуальным вопрос: какие уголовные посягательства в сфере незаконного оборота наркотиков следует относить к наркопреступлениям, совершенным с использованием IT-технологий. После непродолжительной дискуссии специалистов совместным указанием Генеральной прокуратуры и МВД России от 29 декабря 2021 г. введены в действие обновленные перечни статей Уголовного кодекса РФ, используемые при формировании статистической отчетности. Согласно Перечню № 25 к наркопреступлениям, совершенным в сфере незаконного оборота наркотиков с использованием IT-технологий, относятся преступления при наличии соответствующего квалифицирующего признака, предполагающего использование в преступных целях информационно-телекоммуникационных сетей (в том числе сети Интернет), а также при наличии в статистической карточке отметки о способе совершения преступления, раскрывающего объективную сторону, например использование сети Интернет или Даркнет («теневая сеть»), технических и программных средств (средств мобильной связи) для передачи информации вне сети и др.

Для понимания механизма совершения преступлений в сфере незаконного оборота наркотических средств и психотропных веществ (далее – наркотики) с использованием IT-технологий необходимо обратиться к положениям Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», статьей 2 которого определены понятия «информационные технологии» (это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов) и «информационная система» (это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств). Кроме того, здесь же дано определение информационно-телекоммуникационной сети, под которой понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к

[1] Разделы 1 и 9 формы «4-ЕГС» (код 494).

которой осуществляется с использованием средств вычислительной техники. В свою очередь, средства вычислительной техники – это совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Таким образом, «преступление в сфере незаконного оборота наркотиков, совершенное с использованием IT-технологий» является собирательным объемным понятием и по механизму его совершения должно содержать вышеперечисленные признаки технологического процесса обмена данными между субъектами преступления.

Исследовав характеристику взаимодействия субъектов преступной деятельности в цифровом пространстве, следует сказать о том, что она обусловлена следующими специфическими признаками.

Во-первых, цифровизация сбыта и приобретения наркотиков основана на несложных действиях по входу в виртуальную среду и сохранению там анонимности – «непрозрачный трафик», технологии по подмене IP-адресов и телефонных абонентских номеров, программы-коммуникаторы. Теперь нет необходимости в непосредственных контактах людей для совершения криминальных сделок в отношении наркотиков. Чтобы передать запрещенный товар, используют разнообразные тайники, распространен так называемый бесконтактный способ сбыта наркотиков, по желанию заказчика наркотики могут быть доставлены курьерской или почтовой связью, и, безусловно, вся эта деятельность достаточно тщательно конспирируется.

Во-вторых, Даркнет стал идеальной площадкой для незаконных операций, которые, как оказалось, могут удачно сочетаться с современными маркетинговыми технологиями по продвижению запрещенного товара. Поэтому вся эта деятельность вращается вокруг одной генеральной цели – получение сверхприбыли. Извлекается эта прибыль из аренды интернет-магазинов по продаже наркотиков, от администрирования криминальных ресурсов и обеспечения их технической поддержки и прочего. Основу материального обогащения прежде всего составляют финансовые потоки от продажи наркотиков. Но давайте разберемся, есть ли смысл прибегать к совершению наркопреступлений с использованием IT-технологий, если оплата за наркотики будет проходить в прозрачном контуре – ответ очевиден: нет. Поэтому в механизме совершения рассматриваемых преступлений всегда следует выделять признак, характеризующий технологию процесса расчетов между субъектами наркопреступлений.

На сегодняшний день развитие дистанционных платежных сервисов и платежных систем способствует расширению сферы безналичных расчетов и доступности услуг кредитных организаций. Одновременно с этим распространение наркотиков с использованием IT-технологий сопровождается совершенствованием обезличенных взаиморасчетов, разработкой многоуровневых и многообразных схем для соблюдения высокой конспирации финансовых следов, по которым возможно было бы выявить и связать между собой субъектов преступлений.

Финансовая составляющая преступности в сфере информационно-телекоммуникационных технологий (IT-преступность), след которой обнаруживается в сфере деятельности кредитных организаций, все чаще ведет в недостаточно регулируемые сферы финансового сектора. Здесь идет речь в том числе об обороте криптовалют, а при расчетах за наркотики – преимущественно биткоинов в связи с высокой степенью их анонимности. Большинство сервисов по обмену и продаже криптовалют расположены за пределами территории Российской Федерации.

Таким образом, совершение наркопреступлений с использованием IT-технологий имеет две равные по своей значимости стороны, одна из них связана с современными технологическими решения по организации коммуникации субъектов преступной деятельности, вторая – с проведением финансовых операций, связанных с оборотом наркотиков.

Решение первой из них, касающейся в том числе сбыта наркотиков с исполь-

зованием современных электронных технологий, начато давно. В частности, Федеральным законом от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"» установлен запрет использования на территории Российской Федерации информационно-телекоммуникационных сетей, информационных систем и программ для ЭВМ, предназначенных для получения доступа к информационным ресурсам, обращение к которым ограничено.

Федеральным законом от 29 июля 2017 г. № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона "Об информации, информационных технологиях и о защите информации"» предусматриваются идентификация пользователей мессенджеров и возможность ограничения рассылки и передачи сообщений, содержащих информацию, распространяемую с нарушением требований законодательства Российской Федерации.

На сегодняшний день накоплен значительный опыт противодействия совершению наркопреступлений с использованием IT-технологий в сфере оперативно-розыскной деятельности.

Дальнейшие эффективные и адекватные решения по нейтрализации криминальных вызовов и угроз в сфере борьбы с наркоугрозой стране должны строиться с учетом цифровизации процессов сбора и обмена информацией на основе современных программных комплексов в целях обеспечения компетентных органов справочной и оперативно-розыскной информацией, завершение формирования нормативной правовой и технологической базы по деанонимизации виртуального пространства, блокировки звонков с подменой номера, переходов с территории иностранных государств, создание условий для полноценной возможности функционирования Рунета. Необходима проработка вопроса о создании национального центра по координации противодействия IT-преступности.

Несмотря на принимаемые меры, легализация доходов от незаконного оборота наркотиков в России в большинстве своем продолжает носить латентный характер. Например, в 2021 г. количество предикатных легализации наркопреступлений составило порядка 1,1 тыс.[1], следовательно, эффективность уголовно-правовых средств по борьбе с указанными криминальными проявлениями недостаточна.

Назовем основные, на наш взгляд, причины. Одна из них связана с отсутствием возможности контроля за оборотом децентрализованной криптовалюты, в которую конвертируются фиатные средства (к примеру, есть криптовалюты, для которых конфиденциальность – это главный принцип).

Другие причины лежат в уголовно-процессуальном поле. Так, наряду с доказыванием фактических обстоятельств легализации наркодоходов существует проблема установления (доказывания) специальной цели у лица, совершившего финансовую операцию или сделку, по приданию ей правомерного вида, то есть видимость законности владения, пользования и распоряжения денежными средствами или иным имуществом, полученным в результате незаконного оборота наркотиков. В большинстве своем финансовые операции, связанные с совершением предикатных преступлений и свойственные бесконтактному сбыту наркотиков, расцениваются в качестве способа конспирации преступной деятельности и (или) получения дохода от распространения наркотиков.

Кроме того, как правило, наркопреступления, совершаемые с использованием IT-технологий, ведутся уже в автоматизированном режиме, что влечет разрыв причинно-следственной связи между конкретным фактом сбыта (продажи) наркотика и полученными (поступившими) за него расчетными средствами.

Таким образом, в целях ликвидации экономических основ преступности в сфере незаконного оборота наркотиков необходимы дальнейшие шаги по совер-

[1] Раздел 3 формы «5-Л» (код 475).

шенствованию действующего законодательства в рассматриваемой сфере, направленные на криминализацию действий, связанных с сокрытием незаконно полученных доходов от преступной деятельности.

Безгачев Ф.В.

Сибирский юридический институт МВД России (г. Красноярск)

Особенности обеспечения кибербезопасности посредством технологий искусственного интеллекта

Цифровые и информационные технологии (ИТ) – это важнейшая часть современных систем управления, находящихся во всех отраслях экономики на сегодняшний день. Следствием данного фактора является появление новых киберугроз и кибератак, совершаемых в областях, в основе которых функционируют различные информационные системы и иные информационные технологии[1]. В современном мире складывается тенденция роста количества попыток совершения киберпреступлений на объектах критически важной информационной инфраструктуры (КИИ) с помощью использования информационно-коммуникационных технологий (ИКТ)[2].

Множественные удачные попытки подобного рода преступлений свидетельствуют о том, что посредством ИКТ действительно можно нанести колоссальный как физический, так и информационный ущерб. Необходимо отметить, что при нахождении киберпреступником уязвимости в одном из компонентов информационной системы на критически важных объектах представляется возможным осуществление целенаправленных нападений на объекты по всему миру. Исходя из этого, на современных объектах КИИ особую актуальность приобретают задачи, решение которых направлено на своевременное обновление базовых компонентов систем управления[3]. Также стоит отметить, что на сегодняшний день не только со стороны производителей, но и со стороны самих потребителей не всегда уделяется должное внимание вопросу кибербезопасности. Совокупность данных факторов приводит к развитию новых методов и угроз нарушения безопасности[4].

Одним из наиболее перспективных и актуальных инструментов обеспечения кибербезопасности объектов КИИ является технология искусственного интеллекта (ИИ). Посредством интеллектуальных средств представляется возможность производить анализ большого объема данных с быстрой скоростью. Именно это и позволяет обнаруживать угрозы кибербезопасности и прогнозировать их в дальнейшем посредством самообучения модели ИИ и моделирования рисков в целом. На сегодняшний день существует ряд интеллектуальных решений применительно к кибербезопасности.

Одним из основных направлений использования искусственного интеллекта при решении задач из данной области

[1] Ковалев А.А., Балашов А.И. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник Поволжского института управления. 2018. Т. 18. № 5. С. 105-114.

[2] Лебедь В.Н., Терещенко Б.И., Восканян К.А. Управление процессами обеспечения кибербезопасности как фактор международной стабильности // Коммуникология: электронный научный журнал. 2017. Т. 2. № 4. С. 30-37.

[3] Афанасьева Д.В. Применение искусственного интеллекта в обеспечении безопасности данных // Известия Тульского государственного университета. Технические науки. 2020. № 2. С. 151-154.

[4] Горян Э.В. Зарубежный опыт использования технологий искусственного интеллекта в обеспечении информационной безопасности банковского сектора // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11, № 4. С. 62-73.