Аппаратный кошелек – небольшое устройство, предназначенное для безопасного хранения приватных ключей, а также для проведения транзакций. Особенности передачи аппаратных кошельков (не подключенных к сети Интернет) заключаются в том, что при передаче физического носителя с доступом к криптокошельку, на котором хранится определенное количество криптовалюты, не остаются какие-либо цифровые следы, средства не имеют физического выражения, не отражаются в отчетности, а при возникновении угрозы разоблачения есть возможность уничтожения данного носителя в целях воспрепятствовать доказыванию получения взятки. Примером является кошелек для хранения криптовалют Ledger Nano X с поддержкой интегрированной платформы Ledger Live, которая предоставляет все необходимые пользователю стандартные функции, такие как проверка баланса или отправка и получение активов. Указанный кошелек внешне напоминает стандартную флеш-карту, особенность его использования заключается в том, что на нем не хранится криптовалюта, а всего лишь ключи доступа к ней.

В связи с чем следует отметить, что сотрудникам правоохранительных органов необходимо обладать специальными знаниями при выявлении и раскрытии взяточничества, совершаемого путем использования криптовалют, с целью борьбы с данным негативным явлением.

Таким образом, на основании вышеизложенного следует выделить новые способы дачи-получения взятки с использованием криптовалют: перевод криптовалют с одного кошелька на другой с использованием сети Интернет, а также передача аппаратных кошельков (не подключенных к сети Интернет).

УДК 343.97

Д.К. Григорян

АКТУАЛЬНЫЕ ВОПРОСЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ И ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Конец XX – начало XXI в. – время, характеризующееся резким скачком в развитии телекоммуникационных технологий, а также массовым внедрением новейшей системы цифровых технологий во все сферы человеческой жизни. Данный этап в развитии общества способствовал возникновению невероятных угроз и рисков для человека, общества и государства. Уже сегодня наибольшую значимость, даже некий приоритет, имеет интернет, который легко соединил людей по всей планете, сделал коммуникации беспрепятственными, открыл новые горизонты виртуальной реальности. Всемирная сеть подарила миру безграничные возможности в области накопления, передачи и распространения любой информации, помогла выполнять экономические операции в финансово-банковской сфере быстро и качественно, несмотря на дальние расстояния и границы, а также сплотила людей в устойчивые группы и организации в зависимости от их мировоззрения, интересов и увлечений.

Преступления в сфере высоких технологий характеризуются повышенной опасностью, так как в настоящее время информационно-телекоммуникационные технологии полностью преобразовали индустриальный социум в информационное общество, овладев жизнями миллионов людей.

Вышеуказанные аспекты являются примером того, насколько сильно интернет-пространство «поглощает» людей, что создает ряд достаточно серьезных проблем, сферы проявления которых весьма разнообразны. Так, за последние несколько лет мировое сообщество сотрясают проблемы распространения экстремизма и терроризма. «Невидимая война», как часто называют терроризм, все в больших масштабах затрагивает людей, активно воздействуя на их сознание. Наиболее часто используемый способ распространения экстремистских и террористических идей происходит через сеть Интернет. Злоумышленники стремятся нагонять страх и панику у населения, пытаясь овладеть еще не до конца сформированной психикой молодежи, а более взрослому поколению привить негативно устойчивые взгляды на происходящее в мировом сообществе. Так, можно утверждать, что телекоммуникационные сети достаточно часто негативно воздействуют на общество, формируя искаженное представление о действительности.

Вместе с тем возникает вопрос: что же толкает людей к занятию террористической и экстремистской деятельностью? Данный вопрос регулярно поднимается в ходе проведения круглых столов и научных совещаний, однако однозначного ответа на него все еще нет, но существуют несколько подходов. Первый – «биологический», его сущность состоит в том, что антиобщественное террористическое и экстремистское поведение присуще самой природе человека. Второй подход получил название «социальный», так как в нем причинами и условиями, способствующими совершению преступлений в данной области, выступают различные явления общественной жизни. Существует и третий подход, объединяющий в себе два предыдущих. Научное сообщество полагает, что условиями реализации террористических и экстремистских идей в обществе являются как внутренняя природа многогранной личности человека (психологические особенности), так и социальные явления. При этом социальные явления могут быть как негативные (безработица, религиозные разногласия, низкий уровень жизни населения), так и позитивные (широкий спектр социальных возможностей для саморазвития, информатизация общества, расширенный доступ к различной информации).

В Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, отмечается, что в нынешних условиях глобализации и информатизации социума экстремизм и терроризм изменяют формы своего существования, легко проникая в жизнь людей, принимая виртуальный характер и зарождаясь в глобальной сети. Так, возникает еще один тип коммуникаций – «объективная реальность – виртуальная реальность». На первых стадиях своего распространения он получает развитие в интернет-пространстве, а на последующих – выходит за пределы виртуальной реальности и превращается в проявления экстремистской и террористической направленности.

Используя механизмы информационного воздействия, террористические и экстремистские организации с легкостью оказывают влияние на индивидуальное, групповое и общественное сознание населения, нагнетая религиозную или этническую ненависть, пропагандируя экстремистскую идеологию, привлекая все большее число сторонников в террористическую деятельность. Например, в марте 2022 г. платформа Meta была признана Тверским районным судом Москвы организацией, осуществляющей экстремистскую деятельность, а к социальным сетям Instagram и Facebook, действующим на ее основе, ограничили доступ на территории России. Как известно, данная корпорация официально разрешила пользователям размещать информацию, в которой содержатся призывы к насилию в отношении российских военных.

На данный момент в связи с блокировкой вышеуказанных социальных сетей, безусловно, уменьшилось количество преступных посягательств, однако, не следует забывать о таком мессенджере, как Telegram. Это новый этап современного уровня проникновения в сознание людей. Начиная с 2015 г. через данное приложение незаконно сбываются наркотические средства и психотропные вещества, оружие и многие другие предметы, ограниченные в обороте на территории РФ. Существуют также десятки телеграм-каналов представителей запрещенных группировок.

Согласно открытым данным совокупность пользователей, подписанных на вышеуказанные каналы, составляет примерно 25 000. Особому влиянию подвергаются именно женщины, потому что в силу психологических и физиологических особенностей они более подвержены влиянию со стороны преступников-террористов. Всем известны случаи вербовки женщин в международные террористические организации. Это связано в первую очередь с тем, что женщина воспринимается обществом как «мать – хранительница домашнего очага» и не может представлять опасность. В силу разных жизненных обстоятельств женщины совершают особо тяжкие преступления рассматриваемой тематики: кто-то из-за ложной любви, кто-то из-за чувства страха, а кто-то просто по глупости. Примером может служить история, которая произошла в декабре 2017 г. с группой молодых людей, среди которых были представительницы женского пола: 17-летняя Аня Павликова и 19-летняя Маша Дубовик. Они объединились в телеграм-чат для обсуждения политики в стране, в какой-то момент к ним в сообщество внедрился более взрослый активист, который предложил из виртуального общества объединиться в реальную организацию, именуемую «Новое величие». Позднее в марте 2018 г. 10 участников данного преступного объединения были задержаны.

Проблемы распространения экстремизма и терроризма актуализируются день за днем, именно поэтому требуют особого контроля. В системе Министерства внутренних дел Российской Федерации в сентябре 2008 г. было создано главное управление по противодействию экстремизму, которое как реализует нормативно-правовое регулирование в сфере противодействия экстремизму и терроризму, так и разрабатывает комплексную профилактику для борьбы с ними.

На основании вышеизложенного полагаем целесообразным внести ряд предложений по совершенствованию методов борьбы и мер профилактики преступлений экстремистской и террористической направленности:

создание и распространение новой системы медиаматериалов с целью профилактики и предупреждения распространения экстремизма и терроризма в современном обществе;

проведение научных форумов в рамках работы с молодежью на базе Национального центра информационного противодействия терроризму и экстремизму;

улучшение межведомственного взаимодействия среди силовых структур и ведомств как в Российской Федерации, так и на международном уровне.

Таким образом, работа по улучшению указанных выше направлений позволит вести более эффективную политику борьбы с экстремистскими направленностями и террористической деятельностью.

УДК 343.985

Е.И. Давидович

НЕКОТОРЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

На современном этапе развития цивилизации информационная сфера приобретает определяющее значение для гармоничного развития личности, общества и государства. Вместе с тем трансформация социума, стремительное и повсеместное внедрение информационно-коммуникационных технологий (ИКТ) в различных сферах общественной жизни помимо позитивных эффектов порождают и широкий перечень уязвимостей.

Одним из важнейших условий высокоэффективного обеспечения кибербезопасности является разработка концептуальных основ, отражающих систему взглядов на сущность и содержание национальной безопасности в информационной сфере. Указанное обстоятельство повышает практическую значимость в изучении передового зарубежного опыта в сфере регулирования кибербезопасности.

В Республике Беларусь наблюдаются опережающее развитие ИКТ и правового регулирования этой новой сферы правоотношений, а также активное внедрение информационных технологий в деятельность государственных органов. Создаются различные электронные информационные ресурсы, которые содержат как открытые, так и закрытые сведения.

Развитие ИКТ становится важным и неотъемлемым элементом структурных преобразований и подъема экономики страны, роста деловой и интеллектуальной активности населения, укрепления авторитета страны в международном сообществе, поэтапного формирования информационного общества. Надежно защищенное информационное пространство является, с одной стороны, важным обязательным признаком и предпосылкой успешного формирования информационного общества, необходимым условием вхождения в мировое информационное сообщество, глобализации общественных отношений, с другой – выступает как системообразующий признак современного государства, как главное условие сохранения информационного суверенитета страны и укрепления государственности.