

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.

В этих условиях актуализируются вопросы обеспечения кибербезопасности, защиты информационной инфраструктуры от посягательств извне и внутри страны, а также обеспечения стабильного развития сферы ИКТ.

Киберпреступность является феноменом, сформированным в процессе научно-технического и технологического прогресса. Чем более развитым является государство, тем активнее в нем идет процесс цифровизации. Однако цифровизация, бурный рост технологий, инновационные достижения создают дополнительные риски и угрозы, в том числе криминогенного характера. Преступники быстрее адаптируются к меняющимся условиям, осваивают новые технологии и используют их в противоправных целях. Стремительный прогресс и процессы глобализации еще больше усложняют проблемы, связанные с противодействием преступности. Отсутствие границ в киберпространстве обуславливает международный характер киберпреступности. В этой связи киберпреступность представляет собой серьезную проблему.

На протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений, поэтому необходимо осуществлять прогнозирование развития имеющихся в информационном пространстве тенденций и возникновения новых угроз, а также разработать и внедрить единую систему обеспечения кибербезопасности.

Так, стратегия кибербезопасности Республики Беларусь закреплена в Концепции национальной безопасности, утвержденной постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1. В нормативном правовом акте указано, что «национальная система обеспечения кибербезопасности должна реализовывать весь возможный комплекс правовых, организационных и технических мер по обеспечению безопасности национальной информационной инфраструктуры, в том числе информационных систем, обеспечивать конфиденциальность, доступность и целостность информации, а также легко трансформироваться и адаптироваться в изменяющейся обстановке за счет постоянного анализа на предмет соответствия актуальным рискам кибербезопасности. В первую очередь необходимо обеспечить киберустойчивость национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем, эффективное противодействие киберпреступлениям».

В ходе анализа зарубежных доктрин в сфере информационной безопасности (Великобритания, Казахстан, Литва, Польша, Российская Федерация, Чехия) установлено, что в Концепции национальной безопасности Республики Беларусь учтены передовые зарубежные подходы, опыт подготовки и совершенствования подобного рода документов доктринального характера.

Однако необходимо дальнейшее развитие концептуальных, правовых и организационных основ обеспечения кибербезопасности Республики Беларусь.

По нашему мнению, в новой редакции Концепции национальной безопасности Республики Беларусь необходимо отразить следующие положения:

усилить кибербезопасность государственных органов, так как недостаточная защищенность информации, составляющая государственную тайну, создает угрозу национальной безопасности Республики Беларусь, поэтому необходимо оперативно предоставлять информацию об угрозах и уязвимостях всем без исключения государственным органам;

осуществить расстановку приоритетов по устранению рисков для критически важной инфраструктуры в сфере безопасности, необходимо создать новые подходы в сфере кибербезопасности с использованием новейших технологий, улучшением обмена информацией и управления рисками;

инвестировать в инфраструктуру следующего поколения, необходимо взаимодействовать с представителями частного сектора в целях содействия развитию и обеспечению безопасности 4G- и 5G-сетей, а также проанализировать возможность использования новых технологий.

УДК 336.7 + 346.7

А.В. Дешук

СОВЕРШЕНСТВОВАНИЕ ФИНАНСОВОЙ БЕЗОПАСНОСТИ БАНКОВСКОЙ СИСТЕМЫ В СФЕРЕ БЕЗНАЛИЧНОГО ДЕНЕЖНОГО ОБРАЩЕНИЯ

Важнейшей целью современного государства является устойчивое развитие национальной экономики. Для этого необходимы внедрение высокоэффективной системы денежного обращения и использование современных платежных инструментов. Система безналичных расчетов является ключевым условием существования денежно-кредитной сферы, способствующим реализации монетарной политики государства. По мере уменьшения доли наличных денег в структуре денежного предложения снижается общая потребность в эмиссии денег Национальным банком Республики Беларусь для удовлетворения спроса экономики, одновременно нейтрализуются потенциальные риски коммерческих банков по управлению собственной ликвидностью. В этой связи приоритет отдается развитию системы безналичных расчетов по розничным платежам и поступательной замене расчетов наличными денежными средствами среди населения их безналичной формой.

Начиная с 2000-х гг. в систему национальных платежей вошли новые платежные инструменты – банковские платежные карточки, которые из сугубо имиджевого предмета превратились в технологический инструмент предложения широкого спектра розничных банковских услуг. Число банковских платежных карточек, находящихся в Беларуси в обращении, на 1 января 2022 г. превысило 15,7 млн, прирост количества банковских платежных карточек в обращении за пять лет составил 25,2 %. На основе действующих платежных систем в страну пришли мобильные платежные сервисы, получившие широкое распространение в мире. Использование таких мобильных платежных сервисов, как Apple Pay, Samsung Pay, Google Pay, предоставляющих пользователю мобильного устройства возможность проводить безналичные розничные платежи без физического использования банковских платежных карточек, вывело рынок банковских платежных карточек на новый уровень.