количество заявлений о мошенничестве (хищение с обманом жертвы) выросло на 5,1 %, превысив 249 тыс. Однако количество заявлений о возбуждении уголовных дел в связи с компьютерными преступлениями со взломом сократилось на 10,6 %, до 157 тыс. Около четверти преступлений было связано с другими составами, в том числе незаконной организацией и проведением азартных игр. Эксперты оценили ущерб России от действий хакеров в 150 млрд р. по итогам 2021 г. В интернете имеется также статистика о распространении киберугроз по всему миру. Согласно данной информации Россия стала лидером по объему теневых операций с криптовалютой.

В мировой практике право на соблюдение конфиденциальной информации стало неотъемлемой частью процесса реализации основополагающих прав человека в период активного развития различного рода компьютерных технологий, прежде всего – право на конфиденциальность приватной жизни, право на свободу выражения собственного мнения. Данные аспекты затрудняют законодательное ограничение использования программ, скрывающих или шифрующих настоящую личность пользователей. В этом состоит парадокс. Так как в современном мире «право на анонимность» прямо не указано ни в одном акте международного характера, который подлежит обязательному исполнению странами. Встречаются лишь рекомендации независимых международных организаций и стейкхолдеров (это физическое либо юридическое лицо, которое прямо или косвенно воздействует на работу организации или располагает определенными ожиданиями от результатов ее деятельности), и большинство процессов опираются на судебную практику.

Например, в Соединенных Штатах Америки в первой поправке к Конституции 1787 г. закреплено право на высказывание мнения анонимно, а фундаментальная необходимость в защите этого права была признана Верховным судом США.

Однако в России некоторые правоотношения по этому поводу регулируются. Например, в 2014 г. российское законодательство затронуло анонимные платежи. В соответствии с Федеральным законом Российской Федерации от 5 мая 2014 г. № 110 «О внесении изменений в отдельные законодательные акты Российской Федерации» максимальная планка анонимных интернет-платежей стала 15 000 р., что позволило сократить объем транзакций, проводимых киберпреступниками.

Но даже некоторые ограничения не повлияли на распространение киберугроз. В 2022 г. появилась информация об утечке личных данных пользователей из сервиса «Яндекс.Еда». В эти данные входили Ф.И.О. заказчиков еды, их адрес проживания, вплоть до квартиры, номер их телефона, сумму которую они потратили за полгода. Как следствие – сервис оштрафовали лишь на 50 000 тыс. р., что невероятно мало за такую утечку информации.

Количество киберпреступлений и преступников неизбежно будет увеличиваться. Дешевая составляющая киберпреступлений и сложность обнаружения и сбора доказательств создают стимулы для потенциальных преступников. Виртуальный интеллект, транстерриториальность и высокий уровень латентности киберпреступлений затрудняют обнаружение и расследование случаев. С другой точки зрения, киберпреступность превосходит нынешние возможности государственных органов по контролю за правопорядком. Риски и затраты в киберпреступности ниже, чем в традиционной преступности, а выгода выше. Эта рентабельность еще больше укрепляет намерения преступника совершить киберпреступление.

Подводя итог вышеизложенному, можно отметить, что киберанонимность оказывает большое влияние на возникновение киберпреступлений, в основном снижая потенциальную вероятность обнаружения и, следовательно, связанные с этим затраты. На самом деле, анонимность может в какой-то степени побудить потенциальных преступников пойти на риск. Огромной проблемой является также то, что отсутствует нормативная база, которая следит и регулирует деятельность людей в интернете. Это приводит к увеличению количества киберпреступлений, ведь преступники могут руководствоваться тем, что если законодатель четко не определил рамки дозволенного в киберпространстве, то они могут делать что и как угодно. Следовательно, необходимо создать полную нормативную базу, которая затрагивала бы все сферы интернет-отношений, устанавливала бы юридическую ответственность за интернет-мошенничество, нелегальный спам, кражу криптовалюты и т. п.

УДК 343.97

А.В. Морозов

АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ПРОФИЛАКТИКИ И ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Наиболее проблематичным в современном мире считается именно сложность того, что в действительности достаточно тяжело не только отклонить существующие угрозы различного уровня, но даже предотвратить их в информационной области. И это глобальная проблема XXI в. не только на национальном, но и на международном уровне.

Под национальной и информационной безопасностью следует понимать базовые определения складывающихся современных общественных отношений не только на внутригосударственном уровне, но и на международном.

Сегодня киберпреступность, которая, по сути, перестала иметь уже государственные границы в рамках конкретного государства, является реальной угрозой первостепенной важности, которая направлена прежде всего на урегулирование вопросов национальных интересов и безопасности в рамках взаимодействия различных государств. Но в существующих условиях взаимодействия мировое информационное пространство не может не являться ареной для конфликтных ситуаций разных государств, юридических и физических лиц.

В научном сообществе киберпреступления, в широком смысле, обозначены как общественно опасные деяния, посягающие, помимо компьютерных систем, на иные объекты, к основным из которых относятся: национальная и мировая безопасность (кибертерроризм), имущество, имущественные права индивидов и их коллективных образований (это и кражи, и мошенничество, совершенные посредством компьютерных систем или в киберпространстве, а также посягательства на авторские права (плагиат и киберпиратство), на личную безопасность (явления кибербуллинга и секстинга, груминга и троллинга) и пр. [1, с. 6].

Цифровую грамотность можно определить как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктах и услугах, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

В Указе Президента Республики Беларусь от 29 июля 2021 г. № 292 «Об утверждении программы социально-экономического развития Республики Беларусь на 2021–2025 годы» определена цифровая трансформация белорусского государства. Инструментом выполнения поставленных задач станет реализация Государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы, иных государственных программ и программ социально-экономического развития административно-территориальных единиц, региональных комплексов мероприятий в части мероприятий в сфере информатизации.

В свою очередь, например, в 2022 г. в Российской Федерации уже запущена долгосрочная программа повышения цифровой грамотности жителей страны. В рамках данной программы будут созданы новые образовательные сервисы для различных групп граждан, в том числе для студентов, пенсионеров и детей.

Представляется необходимым с учетом имеющегося российского опыта принятие Государственной программы Республики Беларусь «Цифровая грамотность», поскольку на сегодня личная цифровая грамотность становится важным условием работы в онлайн-среде.

Прежде всего необходимо определить и законодательно закрепить понятие «цифровая грамотность». В связи с чем предлагается определить «цифровую грамотность населения» как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктах и услугах, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

Недостаточность законодательства, регулирующего борьбу с преступлениями в сети Интернет, отвечающего современным потребностям правоприменения, не позволяет объективно оценивать масштабы киберпреступности, связанной с новыми коммуникационными технологиями.

Помимо несовершенной законодательной основы противодействия киберпреступности одной из основных проблем является недостаточность компетентных лиц, выявляющих и предотвращающих киберпреступления. Часто осведомленность преступников в сети Интернет превышает осведомленность сотрудников правоохранительных органов [2, с. 142].

Деятельность государственных органов по предупреждению преступлений, совершаемых в сфере цифровой экономики, должна носить многоуровневый характер и учитывать проблемы квалификации таких преступных посягательств. Во-первых, необходимо научное обеспечение деятельности по предупреждению преступности, т. е. использование результатов научно-исследовательской работы в правоприменительной практике. Во-вторых, целесообразно методическое обеспечение деятельности по предупреждению преступности, состоящее в совершенствовании подзаконных актов, которые способствуют оперативному реагированию на ситуации совершения преступлений в сфере цифровой экономики и эффективному применению законодательных актов. В-третьих, необходимо принятие организационно-управленческих мер, состоящих в подготовке сотрудников правоохранительных органов и в переходе от территориального принципа их работы к функциональному.

Таким образом, целесообразно определить и законодательно закрепить понятие «цифровая грамотность», дополнив Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» статьей, определяющей понятие «цифровая

грамотность», определив ее как способность эффективно управлять личными цифровыми ресурсами; разбираться в особенностях различных информационных продуктов и услуг, иметь актуальную информацию о ситуации на информационном пространстве; принимать обоснованные решения в отношении безопасности использования информационных ресурсов.

Считаем целесообразным с учетом имеющегося российского опыта принятие Государственной программы Республики Беларусь «Цифровая грамотность», поскольку на сегодня личная цифровая грамотность становится важным условием работы в онлайн-среде. Посещение небезопасных сайтов, невозможность распознать откровенно мошеннические действия и фейковую информацию в сети Интернет приносят серьезные неприятности пользователю и тем самым создают дополнительную нагрузку на правоохранительные органы.

Список использованных источников

1. Абламейко, М.С. Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика : автореф. дис… канд. юрид. наук : 12.00.14 / М.С. Абламейко ; Белорус. гос. ун-т. – Минск, 2012. – 28 с.

2. Жуков, А.З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права / А.З. Жуков // Проблемы экономики и юрид. практики. – 2019. – № 4. – С. 141–143.

УДК 343

Р.Р. Насыров

О ПРОТИВОДЕЙСТВИИ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ И ИХ АНАЛОГОВ

Информационные технологии внедряются во все сферы жизни человека, и преступная сфера не является исключением. Информационно-телекоммуникационная сеть Интернет и информационные технологии позволили наркобизнесу выйти на новый уровень и привлечь внимание огромного количества людей.

Информационно-телекоммуникационные технологии на современном этапе развития активно способствуют развитию и модернизации наркосети, посредством которой осуществляется розничная и оптовая продажа наркотических средств, психотропных веществ и их аналогов. К тому же преступный элемент постоянно повышает меры конспирации, зашифрованность электронных терминалов и сетевых ресурсов, которые служат для перевода денежных средств за наркотики. К наиболее распространенным интернет-площадкам и мессенджерам относятся DarkNet, LegalRC, Iklad, DarkWeb, AlphaBay Market, Daffy Duck, Silkkitie, AS, Lambo, Ramp, Dream Market, Silk Road, Hansa, BigRC.biz, Telegram.

Рассматривая маркетплейсы в теневом сегменте сети Интернет, стоит отметить, что на них перевод денежных средств между продавцом и покупателем допускается посредством платежных систем (например, Яндекс.Деньги, Qiwi, WebMoney и др). Как правило, в Qiwi открывается несколько счетов, на которых аккумулируются денежные средства. Впоследствии данные счета используются для проведения финансовых операций по приобретению различных криптовалютных форм в рублевом эквиваленте на Ethereum, Биткоин, Monero, Litecoin, Zcash, Ripple, Dash. Криптовалюта активно используется лицами, осуществляющими незаконную продажу наркотиков в теневом сегменте сети Интернет. Она обладает огромными преимуществами, так как под ней понимаются виртуальные денежные средства, не имеющие материального выражения и физической формы. Тем самым для криптовалюты характерен уровень анонимности, независимость от национальной валюты, защищенность, необратимость операций, автономность и условность.

Ко всему этому в противодействии криптовалютной наркоторговле большое значение приобретает проблема отсутствия у сотрудников правоохранительных органов необходимых знаний, касающихся криптовалюты и работы с ней. На практике возникает немало вопросов обнаружения и изъятия виртуальных цифровых денежных средств. Именно поэтому важно повышать знания и подготовку сотрудников в области информационных технологий и программирования. Следствием вышеуказанных проблем является отсутствие зарегистрированных случаев изъятия криптовалюты в качестве нелегального дохода от сбыта запрещенных в гражданском обороте средств и веществ.

В Стратегии Государственной антинаркотической политики Российской Федерации на период до 2030 года указано, что возникновение новых и модернизация уже имеющихся способов совершения преступлений организованными группами с использованием инновационных коммуникационных технологий и сетей выступает одной из самых злободневных угроз национальной безопасности в сфере контроля и противодействия незаконному обороту наркотических средств, психотропных веществ и их аналогов (Указ Президента Российской Федерации от 23 ноября 2020 г. № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года».