чем как в формате реального присутствия, так и в режиме онлайн-конференций. Главная их цель – в преддверии летних каникул довести до обучающихся основные виды киберугроз и меры по защите от них.

В целом проведение указанного комплекса профилактических мероприятий позволило достичь поставленных целей, всесторонне и качественно довести необходимую информацию до населения (в особенности до молодежи). С высокой степенью эффективности были задействованы заинтересованные государственные органы и организации, предприятия, социальная, транспортная и спортивная инфраструктура, мобильные операторы сотовой связи.

Как свидетельствует статистика, проведение данных широкомасштабных профилактических мероприятий весьма существенным образом сказываются на формировании положительной динамики в противодействии киберпреступности. Массированным информированием граждан всеми доступными способами о самых актуальных способах хищений денежных средств правоохранительные органы достигают главной цели: обеспечение превентивной самозащиты населения от преступных киберпосягательств. Вместе с тем важнейшее значение в противодействии киберпреступности имеет консолидация и партнерские отношения между правоохранительными органами, организациями государственного и частного секторов, образовательными и научными учреждениями.

Таким образом, профилактическая работа, направленная на правовое просвещение населения, и впредь должна носить системный характер с привлечением всех заинтересованных структур органов государственного управления.

УДК 343.9.01

И.С. Митряев

ВЛИЯНИЕ КИБЕРПРОСТРАНСТВЕННОЙ АНОНИМНОСТИ НА МОТИВАЦИЮ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ IT-ТЕХНОЛОГИЙ

Совершенствование информационных систем упрощает доступ к информации, предлагает ее разновидности. В то время как безопасность личных данных подвергается высокому риску, анонимность, невидимость и сокрытие следов преступления становятся большой проблемой в сфере интернет-отношений между людьми.

Киберпреступность во многом отличается от традиционных преступлений, в том числе универсальностью и сложностью, в частности

анонимностью, сокрытием и незаметностью. Анонимность киберпространства делает отслеживание личности серьезной проблемой, которая создает препятствия для обнаружения и расследования.

Анонимизация киберпространства делает отождествление личности глобальной проблемой, которая создает препятствия для расследования данного рода преступлений и поимки преступников.

Киберанонимность оказывает влияние на преступную мотивацию и явление виктимизации, которое представляет из себя процесс или конечный результат превращения в жертву преступного посягательства лица или группы лиц, поэтому решать эту задачу необходимо на разных уровнях, включая технологии и правоохранительные органы.

Анонимное общение – отличительная особенность интернет-пространства. При использовании интернета анонимность может сохраняться от начала до конца. Но при этом данный тип общения может нести достаточно серьезную угрозу конфиденциальности личных данных пользователей, организаций. Интернет повсюду. Но достаточно часто его используют в торговых центрах, ресторанах, барах, аэропортах и т. п. Из-за особенности распространения интернета злоумышленники часто пользуются этим, взламывая средства связи обычных пользователей, которые подключены к одной общественной сети.

Существуют специальные программы и сервисы, которые позволяют полностью сохранить свою анонимность в сети Интернет. Этот механизм затрудняет установление личности пользователя. Ведь посредником может являться программа. Но вполне реально отследить данный путь посредством следования процессам прямо противоположным передачам.

Анонимное подключение представляет собой фундаментальное субъективное право, необходимое каждому посетителю интернета. В определенных случаях это отдельные компьютерные сети, созданные для достижения анонимности в сети Интернет. Особенность таких сетей в том, что они сочетают в себе определенную степень защищенности пользователя, легкость использования и наличие «прозрачности» для конечного пользователя.

Наиболее известным примером программ для обеспечения анонимности является браузер Tor и VPN, что позволяет добиться полной анонимности в сети Интернет. Следует отметить, что использование данных программ законодательно не регламентируется, то пользоваться такими программами может любой желающий.

Статистика о количестве киберпреступлений в России за 2021 г. говорит о 518 тыс. киберпреступлений, что на 1,4 % больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 г. В частности,

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.