АКТУАЛЬНЫЕ ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

О. В. Дудко, В. В. Осипенко

В XXI в. человечество вышло на новый уровень научно-технического прогресса. С подобным стремительным развитием особенно важным является его использование в правильных целях. Однако, облегчив одни сферы общественной жизни, научно-технический прогресс также усложнил другие, создавая все новые и новые вызовы для мирового сообщества. Так на сегодняшний день инновационные технологии активно используются для совершения преступлений, которые получили особое название – киберпреступность.

Понятие «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в ее рамках или против нее, то есть любое преступление в компьютерном пространстве. Киберпреступность имеет различные проявления. В связи с тем, что «полем» для совершения киберпреступлений является глобальная компьютерная сеть Интернет, то последняя становится способом налаживания наркотрафика, инструментом политической дестабилизации, способом хищения денежных средств с электронных счетов и кошельков, финансирования терроризма, платформой для торговли оружия и т.д.

Киберпреступность появилась практически одновременно с созданием компьютерных технологий – в 80-е гг. прошлого века, тогда преступники действовали в основном путем рассылок вредоносных программ на электронную почту пользователей. В 1990-е гг. появление веб-браузеров имело следствием распространение так называемых «вирусов», представляющих собой вредоносные программы, внедряющиеся в систему компьютера. На современном этапе киберпреступления совершаются путем хищения личных данных пользователей. Таковыми преступлениями являются «фишинг», который состоит в противоправном завладении конфиденциальной информацией пользователей Интернета, и вишинг (мошенничество путем телефонных коммуникаций преступников с жертвами, в итоге которых жертвы сами сообщают свои конфиденциальные данные). К сожалению, для киберпреступников существенно упрощен поиск потенциальных жертв в связи с популярностью социальных сетей, где содержится необходимая для них информация.

Киберпреступность становится одним из самых распространенных преступлений и вопросы противодействия приобретают мировой характер. Так, 23 ноября 2001 г. В Будапеште была принята Конвенция «О компьютерных преступлениях», которая определила виды преступления в компьютерной сфере как незаконный доступ («хакерство»), незаконный перехват, вмешательство в данные, систему, использование девайсов не по назначению, компьютерный подлог, мошенничество путем использования компьютерных технологий, преступления в сфере детской порнографии, авторских и смежных прав и др.

Данный вид преступления является одним из самых распространенных в виду того, что вся преступная деятельность происходит в Интернет-пространстве, где становится проблематичным отследить начальный и конечный пути перемещения вредоносных программ и, впоследствии, утечки данных. Также, практически невозможно установить место совершения преступления – оно происходит в Интернете, который не имеет материально-вещественной формы. Более того, изобличение лиц, совершающих подобные преступления, становится еще более сложным в виду того, что они могут находится под юрисдикцией другого государства. На пути к борьбе с киберпреступностью Республике Беларусь следует выстроить четкую стратегию и систему институтов в данной сфере, потому как подобные меры позволят снизить количество потенциальных жертв данных преступлений. Стратегия должна базироваться на двух направлениях: повышение правовой грамотности самих граждан путем проведения профилактической работы, чтобы не стать жертвами преступления, и повышения квалификации сотрудников органов внутренних дел (к примеру, прохождение повышения квалификации, привлечение внештатных специалистов с определенными знаниями).

Важно проводить профилактические мероприятия, направленные на предупреждение кибермошенничества: соответствующие рубрики в телевизионных передачах, предупреждения в радиотрансляциях, общественном транспорте, отделениях банка и почты. Более того, если данных мер недостаточно, предлагается повысить их эффективность путем личных профилактических бесед сотрудников органов внутренних дел с наиболее уязвимыми слоями населения (пенсионерами), так как доверие к государственному служащему в форменной одежде существенно выше, а восприятие информации эффективнее. Также эффективным представляется почтовая и телефонная рассылка, чтобы информация об опасности мошенничества по телефону всегда была при гражданах в виде памятки.

Говоря о младшем поколении необходимо отметить, что в школах должны проводиться уроки по компьютерной и финансовой грамотности, чтобы у граждан с детства формировалось осторожное поведение в Интернет-пространстве.

Помимо вышеперечисленных мер предлагается специалистам банков использовать новейшее антивирусное программное обеспечение в интернет-банкингах, чтобы минимизировать сомнительное движение денежных средств со счетов.

Как известно, чтобы повысить эффективность в части, касающейся именно расследования киберпреступлений, требуется создание специальных подразделений в структуре органов внутренних дел и органов государственной безопасности, привлекая и подготавливая грамотных специалистов в области информационных технологий. Данные меры существенно облегчат предупреждение и расследование киберпреступлений. Следует отметить, что Республика Беларусь уже предпринимает меры по улучшению качества расследования киберпреступлений, так, создан и функционирует специализированное управление – Управление по противодействию

киберпреступности (Управление К). Понимая, мировой характер проблемы, Республика Беларусь является активным членом различных соглашений, которые позволяют наладить сотрудничество в области борьбы с киберпреступностью (например, Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года.

Что касается противостояния киберпреступности, упомянутое Управление К проводит профилактические мероприятия путем опубликования тематических статей на его официальном сайте, сотрудников Управления приглашают на различные телевизионные (новостные) передачи. Управлением предлагаются пошаговые действия, которые позволят минимизировать количество жертв кибермошенников: сохранение конфиденциальных данных о личности и, в частности, о банковских счетах пользователей в тайне, то есть, несообщение их по телефону ни одному лицу, даже «сотрудникам банка»; установление родительского контроля в мобильных устройствах детей и пенсионеров; использование различных банковских счетов, созданных для различных целей (покупок, накоплений и т. д).

Следственный комитет Республики Беларусь также проводит подобные мероприятия в рамках предупреждения кибермошенничества. В частности, публикуются данные о расследовании соответствующих уголовных дел в целях популяризации компьютерной грамотности всеми возрастными группами населения. При этом информируется, что наибольшую трудность в расследовании киберпреступлений представляет поиск и изобличение лиц, их совершивших. На современном этапе это действительно является проблемным вопросом привлечения виновных лиц к ответственности, так как мошенники могут находиться на другом конце планеты, а вопросы выдачи с тем или иным государством в достаточной степени не урегулированы. В связи с данным обстоятельством целесообразным будет снова подчеркнуть важность международных соглашений о сотрудничестве в сфере киберпреступлений.

Прокуратура Республики Беларусь также проводит тематические профилактические мероприятия и, в частности, координационные совещания, итогом которых является информирование субъектов хозяйствования о недопустимости разглашения конфиденциальной информации, потому как данные субъекты также становятся жертвами кибермошенничества. Учитывая вышеизложенное следует отметить, что в Республике Беларусь создана соответствующая правовая база и функционируют специализированные субъекты для борьбы с киберпреступностью.

В заключение необходимо подчеркнуть, что единственно правильного и наиболее эффективного способа предупреждения киберпреступности на данный момент не существует. Сотрудники правоохранительных органов и финансовых учреждений делают все возможное, чтобы минимизировать число жертв кибермошенничества, но, к сожалению, для этого необходимы и усилия самих граждан. Только грамотный симбиоз правоохранительной и самостоятельной деятельности позволит минимизировать риски стать жертвами фишинга и вишинга.