СЕКЦИЯ 4
СОЦИАЛЬНО-ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЧЕЛОВЕКА, ОБЩЕСТВА И ГОСУДАРСТВА

УДК 349.2

А. П. Абрамович
Учреждение образования «Барановичский государственный университет», Барановичи

КИБЕРПРЕСТУПНОСТЬ В РЕСПУБЛИКЕ БЕЛАРУСЬ: СОСТОЯНИЕ И ПУТИ ПРОТИВОДЕЙСТВИЯ

Введение. Человечество вступило в эру глобального информационного общества, в котором информация и знания играют важнейшую роль во всех процессах жизнедеятельности. Республика Беларусь также встала на путь построения информационного общества.

Появляются новые особенности правового регулирования, которые должны идти в ногу со временем и постоянно совершенствоваться. Право оказывает значительное влияние на процесс мотивации человеческого поведения. Позиция государства «закладывается» в юридические нормы, которые становятся для личности главным источником правовой информации.

Развитие в Республике Беларусь, как и во всем мире, электронных технологий и телекоммуникационных сетей, всеобщая доступность в глобальной компьютерной сети Интернет различных информационных ресурсов способствовали появлению киберпреступности. Сегодня киберпреступность активно выходит на лидирующие позиции наравне с торговлей оружием, проституцией и наркоторговлей. Об этом все громче заявляют правоохранители различных стран мира. В настоящий момент мы наблюдаем, что в мировом сообществе пытаются навести порядок в данной сфере и в той или иной мере взять Интернет под контроль.

Актуальность темы исследования заключается в том, что, учитывая быстрые темпы компьютеризации населения и технологического развития общества, обществу необходима законодательная подкованность и защищенность в отношении информации, которая может пострадать в результате противоправных действий тех или иных лиц.

Основная часть. Преступления в сфере информационных технологий или киберпреступность — преступления, совершаемые в сфере информационных технологий.

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров банковских карт и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.п.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Предпосылки для совершения компьютерных преступлений проявляются в результате сочетания следующих факторов: 1) мотивация; 2) наличие возможности; 3) уязвимости в защите ПО; 4) отсутствие должного противодействия.

Опасность современной киберпреступности состоит в способности проникать во все сферы жизни общества, а также в быстрой приспосабливаемости к новым условиям.

Человек может загрузить практически любую информацию и поделиться с кем-либо, но не каждый сервис может гарантировать безопасность и защищенность своему пользователю. Антивирусные программы защищают компьютер от уже известных вредоносных программ, но ничто не мешает злоумышленникам создать более совершенную программу, которая сможет обойти защиту. Наряду с этим существует такое мнение, что самый защищенный компьютер тот, что не подключен к сети.

Киберпреступность является удобным способом причинения вреда злоумышленниками. Это объясняется тем, что, используя современные технологии, можно достаточно быстро и анонимно совершить преступления, находясь практически в любой точке Земли.

Преступления данной категории сложны тем, что зачастую являются международными, т. е. преступники находятся и совершают противоправные действия в одном государстве, а их жертвы находятся в другом. Для борьбы с такими преступлениями особое значение имеет международное сотрудничество, своевременный обмен информацией, а также умелое использование ресурсов для нахождения и поимки преступников.

Самыми распространёнными киберпреступлениями являются хищения путём использования компьютерной техники, неправомерный доступ к компьютерной информации, а также написание вирусов и их распространение. Первое высокотехнологичное преступление на территории нашей республики было зарегистрировано 20 ноября 1998 года. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием BackOrifice, злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера.

Принимая во внимание правонарушения, зарегистрированные в 1998—2000 годах, вступление в действие нового УК Республики Беларусь, предусматривающего ответственность за преступления против информационной безопасности, а также высокую степень вероятности дальнейшего распространения киберпреступности на территории нашей республики, было принято решение о создании подразделения, специализирующегося на профилактике и раскрытии злодеяний данной категории.

Управление по раскрытию преступлений в сфере высоких технологий (УРПСВТ) МВД Республики Беларусь является самостоятельным оперативно-розыскным подразделением министерства, непосредственно подчиненным первому заместителю министра внутренних дел — начальнику главного управления криминальной милиции. Для осуществления взаимодействия с иными правоохранительными органами и организациями применяется условное наименование «Управление “К”» МВД Республики Беларусь [1].

Проанализировав первые результаты активного противостояния ИТ-мошенникам, руководство «Управления “К”» пришло к выводу, что в Республике Беларусь за последние пять лет виды виртуального мошенничества претерпели значительные изменения.

Если в 1998—2001 годах наиболее распространенными были компьютерные махинации (хищения пин-кодов), конечным итогом которых являлось завладение товарами зарубежных интернет-магазинов, то в 2005 году стали превалировать факты незаконного вторжения в процесс обмена электронными данными. На смену любителям-одиночкам пришли ОПГ.

За короткий промежуток времени спектр преступлений в сфере высоких технологий значительно расширился и уже вышел за рамки злодеяний, имеющих исключительно экономический подтекст. Все чаще совершались хакерские «атаки» на интернет-ресурсы государственного значения.

Объяснялось это тем, что ОПГ стали активнее использовать в своей противоправной деятельности новейшие достижения науки и техники. Новинки использовались как для непосредственной подготовки, совершения и сокрытия преступлений, так и для организации преступной деятельности в целом (обмен информацией на качественно новом технологическом уровне).

Изучая категории лиц, привлекаемых к уголовной ответственности за нарушения закона в области информационной безопасности, сотрудники «Управления “К”» пришли к выводу, что подавляющее большинство среди них составляют молодые люди в возрасте 18—29 лет (60,7%). Вторыми по массовости шли граждане от 30 лет и старше (33,3%) [1].

С учетом данной негативной тенденции уголовно-правовые нормы, касающиеся указанной категории правонарушителей, постоянно совершенствуются, в том числе путем снижения возраста, с которого наступает уголовная ответственность. С 4 апреля 2016 года вступили в силу изменения и дополнения уголовного законодательства, которые относятся к возрасту наступления уголовной ответственности для несовершеннолетних. За хищение с помощью компьютерной техники (ст. 212 УК Республики Беларусь) и уклонение от отбывания наказания в виде ограничения свободы (ст. 415) наказывать теперь будут с 14 лет, а не с 16, как это было раньше [2].

Заключение. Граждане государства, которые не посвящены в такие базовые сферы права, как гражданское, административное и уголовное право, имеют смутное понятие о том, какие права и обязанности они имеют и на что они могут рассчитывать при нарушении этих же самых прав.

Следует иметь в виду, что официальная статистика не отражает реальное количество преступлений. Объясняется это незнанием потерпевших о существовании ответственности за те или иные противоправные действия, совершенные в информационной среде, а также нежеланием отдельных жертв сообщать о преступных посягательствах во избежание подрыва репутации либо из-за опасений собственной ответственности (например, за использование установленного на персональном компьютере контрафактного программного обеспечения).

За последние годы законодательство Республики Беларусь претерпело ряд существенных изменений, в том числе и в информационной сфере. На данный момент оно предусматривает уголовную, административную и гражданско-правовую ответственность.

Исходя из изложенного, предлагается: 1) ввести в обязательную программу для изучения как школьниками, так и студентами университета, такую дисциплину, как «Правопонимание». Это позволит государству решить не только многие проблемы, связанные с необразованностью граждан в правовом аспекте, но и ряд моментов, касающихся совершения преступлений. Если граждане будут лучше понимать свои права и обязанности перед государством, то будет меньше проблем с их нарушениями; 2) организовать единое управление «К», которое будет направлено на международное сотрудничество. Предвидится упрощенный обмен опытом, информацией, а также ресурсами, которые могут быть полезны в раскрытии преступлений, связанных с нарушениями в Сети и в Республике Беларусь, и на территории зарубежных государств.

Список источников

1. Исторические вехи управление по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь , 2010 — 2017 [Электронный ресурс]. — Режим доступа: http://mvd.gov.by/main.aspx?guid=3291. — Дата доступа: 01.02.2017.

2. *Корзан, М. М.* Компьютерных преступлений стало больше [Электронный ресурс] / М. М. Корзан // Сайт районной газеты «Івацэвіцкі веснік», 2007—2017. — Режим доступа: http://www.ivatsevichy. by/zdaryenn/tyelefon-m-l-cy-102/-kompyuternyh-prestupleniistalo-bolshe.html . — Дата доступа: 01.02.2017.

3. *Сафонова, Т. В.* Информационное право Республики Беларусь [Электронный ресурс] / Т. В. Сафонова. — Режим доступа: http://lib.vsu.by /xmlui/bitstream/handle/123456789/2277/Информационное%20право%20РБ.pdf? sequence=3&isAl lowed=y . — Дата доступа: 03.02.2017.