ПРОФИЛАКТИКА ПРЕСТУПЛЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Крючкова Д.В. – студентка юридического факультета ВГУ имени П.М. Машерова

Государство и общество находятся в постоянном и непрерывном процессе развития. В таком же непрерывном процессе совершенствования и преобразования находятся информационные технологии. И если ранее момент появления и распространения их в обществе ассоциировался с безусловным прогрессом, новациями, шагом вперед, то позднее, когда в этой сфере стали совершаться противоправные деяния, в

отношении законопослушных граждан, положительное отношение к информационным технологиям и самому процессу информатизации общества перестало быть столь непреклонным и неизменчивым.

Следует отметить, что к преступлениям в области информационных технологий относятся не только преступления, предусмотренные гл. 31 Уголовного кодекса Республики Беларусь (далее УК) «Преступления против информационной безопасности», но и противоправные деяния, предусмотренные иными статьями и главами УК (список на отдельном листе). К числу преступлений в данной сфере относится и хищение с использованием компьютерной техники (ст. 212 УК), где компьютерная техника используется именно в качестве орудия совершения преступления.

Так, 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 «Back Orifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера.

В 2001 году руководство МВД республики проанализировало криминогенную ситуацию, складывающуюся в сфере компьютерной информации и телекоммуникаций в нашей стране, а также странах дальнего и ближнего зарубежья. Была изучена организация работы правоохранительных органов других государств по предупреждению преступлений данной категории, опыт борьбы с киберпреступностью российских коллег. Принимая во внимание правонарушения, зарегистрированные в 1998–2000 годах, вступление в действие нового Уголовного кодекса, 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.

Далее, 28 ноября 2002 года на основании приказа Министра внутренних дел, с целью совершенствования организации работы названных подразделений, в МВД было создано самостоятельное управление, осуществляющее практическую деятельность по раскрытию преступлений в сфере высоких технологий (Управление «К»).

Результат не заставил себя долго ждать. Если за три года (1998–2000) было возбуждено только три уголовных дела, связанных с использованием компьютерных технологий, то в период с 2001 по 2005 годы – уже 1813 таких дел. Что, безусловно, подчеркивает необходимость функционирования Управления по раскрытию преступле-

ний в сфере высоких технологий в качестве подразделения МВД Республики Беларусь.

Проанализировав первые результаты активного противостояния IT-жуликам, руководство Управления «К» пришло к выводу, что в республике за последние пять лет виды виртуального мошенничества претерпели значительные изменения. Если в 1998–2001 г. 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 хорошо организованные преступные группы.

За короткий промежуток времени, спектр преступлений в сфере высоких технологий значительно расширился и уже выходил 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%). Кстати, удельный вес привлеченных несовершеннолетних составлял на тот момент всего 6,0% от общего числа. В то же время, за период с 2005 по 2008 годы количество несовершеннолетних, совершивших преступления в сфере высоких технологий, уже увеличилось в пять раз.

Что же касается статистики за 2014 год, то число выявленных преступлений в сфере высоких технологий составило 2290 преступлений, в том числе по областям: 1. Минск – 708; 2. Гомельская – 351; 3. Минская – 273; 4. Витебская – 261; 5. Могилевская – 249; 6. Брестская – 243;7. Гродненская – 205. Доля хищений путем использования компьютерной техники (статья 212 УК) от общего числа выявленных по-прежнему велика (88,8 %) и составила 2033 преступления данной категории. Меньше зарегистрировано хищений с банковских пластиковых карт в особо крупном и крупном размерах (в 2014 г. – 34, в 2013 г. – 38), что является следствием активных действий Управления «К» по выявлению групп, специализирующихся на квалифицирован-

ных хищениях данной категории. Только за отчетный период выявлено четыре такие группы. Снизилось (-7,6%) количество выявленных преступлений против информационной безопасности (в 2014 г. – 257, в 2013 г. – 278), ответственность за которые предусмотрена 31 главой УК. Так, значительно уменьшилось количество выявленных фактов разработки и распространения вредоносных программ (-72,4%).В результате ОРМ выявлено 1006 лиц (-4,6 %). К уголовной ответственности привлечено 809 человек, в том числе 335, имевших судимость, 620 неработающих и 31 несовершеннолетний.

Как видно из предоставленных статистических данных за отчетный период – 2014 года, деятельность Управления по раскрытию преступлений в сфере высоких технологий имеет неоспоримые положительные результаты и направлена в будущем на максимальное снижение преступности в сфере информационных технологий. В рамках своей деятельности Управление «К» также значительное внимание уделяет вопросу предупреждения преступлений в сфере информационных технологий, путем осведомления граждан всевозможными способами о правилах безопасного пользования сетью Интернет, банковскими пластиковыми картами, о зарегистрированных фактах преступного воздействия на информационную безопасность граждан для уменьшения количества жертв подобных преступлений. Деятельность такого характера ведется как в сети Интернет – на официальном сайте МВД Республики Беларусь, так и по телевидению, в газетах.

Однако, для предотвращения преступлений в IT-сфере, нельзя забывать и о роли самих пользователей информационными технологиями, которые могут, соблюдая некоторые правила рекомендации, не стать жертвами подобных преступлений, а значит, непременно снизят количество преступных деяний в данной сфере.

К таким правилам следует отнести:

1. Не следует соглашаться покупать SIM-карты на свои паспортные данные для малознакомых людей;

2. Нельзя предоставлять неизвестным конфиденциальные сведения, размещенные на Вашей SIM-карте;

3. Не переходите по ссылкам, указанным в СМС - сообщениях, приходящих на Ваш мобильный телефон от незнакомого абонента; не скачивайте картинки содержащиеся в такого рода сообщениях;

4. Знайте, что органы МВД не уведомляют посредством сети интернет или мобильной связи о необходимости уплаты электронных штрафов;

5. Знайте об опасностях загрузки из сети Интернет различных программных продуктов! Внимательно читайте онлайновые объявления! Не нажимайте «ок», если точно не знаете, с чем вы соглашаетесь;

6. Не общайтесь в социальных сетях, посредством электронной

почты с незнакомыми Вам людьми, так как в последнее время все чаще именно такой способ используется для вербовки в террористические организации;

7. Берегитесь программ, которые позволяют вашему модему осуществлять набор номера для доступа в интернет! Если на экране вашего компьютера появляется диалоговое окно с информацией о том, что идет набор номера, который вы не поручали ему набирать, немедленно аннулируйте соединение. Если вы все-таки услышали (по характерному звуку), что модем произвольно устанавливает соединение – прервите процедуру (вплоть до отключения модема от телефонной сети). Проверьте настройки «удаленного соединения по умолчанию», наличие новых соединений и наличие программ (ссылок, ярлыков), которые вами не создавались и не устанавливали;

8. Не указывайте открыто свой e-mail адрес при размещении своих сообщений комментариев к статьям и т.д. на различных интернет-форумах, в гостевых книгах и чатах.

9. Никогда не открывайте письма, поступившие от неизвестного отправителя, тем более прикрепленные файлы, которые могут содержать вредоносные программы.

10.Ни при каких условиях не следует отвечать на письма (другие сообщения и послания) сомнительного содержания от неизвестных пользователей, показывая тем самым, что ваш e-mail реально существует.

11. Перед тем, как снять деньги посредством использования банкомата, убедитесь в отсутствии установленного на него «скимера». Злоумышленники взламывают компьютерные системы банков, откуда воруют информацию о реквизитах банковских карт клиентов или при помощи специальной накладки («скимера») на клавиатуру банкомата, снимают данные с магнитных полос карточек. Похищенные сведения записывают при помощи специального устройства на фальшивые кредитки. С помощью такой подделки в банкомате снимают деньги или заказывают дорогостоящие товары в интернет-магазинах;

12. Также, перед тем, как снять деньги посредством использования банкомата, убедитесь в отсутствии на клавиатуре самого банкомата металлической накладки, посредством которой преступники имеют реальную возможность узнать пароль от карты;

13. Опять же, перед тем, как снять деньги посредством использования банкомата, убедитесь в отсутствии «ливанской петли». Используя специальное устройство («ливанская петля» – капроновая нить с металлической скобой), злоумышленники блокируют карточку в картоприемнике банкомата. При возникновении затруднений с возвратом карточки, стоящий сзади человек предлагает пострадавшему повторно набрать пин-код. Благодарный гражданин теряет бдительность и, не таясь, набирает код повторно. Конечно, кредитка не воз-

вращается и рассерженный клиент отправляется в банк, в то время как «добровольный советчик» извлекает карточку и снимает деньги.

14. Получив подозрительное сообщение, ни при каких обстоятельствах не вводите логин и пароль интернет-банка. Подобные махинации («фишинг») направлены на хищение паролей и персональных данных пользователей интернет-банков.Фишер (от англ. «fish» – рыба) – категория виртуальных мошенников, которая создает в сети Интернет копии сайтов, например, банковского учреждения. После этого начинается «рыбалка». Рассылаются рекламные сообщения с завлекающим текстом, на которые некоторые пользователи клюют, заходят на сайты-ловушки и оставляют там свои реквизиты (пин-код, номер счета). В скором времени банковские счета доверчивых людей пустеют.

Безусловно, нельзя говорить о полном искоренении преступности в сфере информационных технологий, так как с развитием самих технологий, развиваются преступники, и способы совершения преступления, и технические средства для совершения преступлений. Однако, можно с уверенностью утверждать, что своевременная профилактика таких преступлений Управлением по раскрытию преступлений в сфере высоких технологий, а также бдительность самих граждан снизит уровень преступности в сфере информационных технологий.