УДК 32 (575.2) (04)

СОВРЕМЕННОЕ СОСТОЯНИЕ КИБЕРПРЕСТУПНОСТИ (ПО МАТЕРИАЛАМ КЫРГЫЗСКОЙ РЕСПУБЛИКИ И РОССИЙСКОЙ ФЕДЕРАЦИИ)

Т.К. Салиева – студентка
Ошский государственный юридический институт

В данной статье освещаются существующие и возможные проблемы преступности в сфере использования компьютеров, анализируется современное состояние, также прогнозируется динамика развития данной преступности в ближайшем будущем.

В 1966 г. компьютер был впервые использован как инструмент для совершения кражи из Банка Миннесоты, США. Это был первый официально зарегистрированный случай использования компьютерной техники для совершения преступления, который ознаменовал наступле-

ние эры высокотехнологичной преступности[1]. С тех пор компьютерные преступления получили широкое распространение во многих сферах жизни общества, которые в 60-х годах еще даже не существовали.

До недавнего времени считалось, что преступность в сфере использования компьютерных технологий существует только в зарубежных странах, а в Кыргызской Республике или в странах СНГ по причине слабой информатизации общества ее практически нет. Недооценка возможностей компьютеризации страны и потенциала высококлассных специалистов-компьютерщиков привела к недостаточному изучению этой проблемы и, как следствие, к правовому вакууму в этой области. В данном случае речь идет о правовом вакууме в области уголовно-правовых и криминологических мер противодействия преступности в сфере использования компьютерных технологий. В Кыргызской Республике компьютерная преступность имеет высокую степень латентности[2].

В данное время не только на территории Кыргызстана, но и большинства постсоветских стран получили распространение разнообразные виды преступлений, совершаемых с использованием глобальной сети Интернет: мошенничество, детская порнография, торговля наркотиками и ограниченными в обороте лекарственными средствами, торговля огнестрельным оружием, алкоголем. Кроме того, одним из наиболее опасных видов преступлений было названо мошенничество при торговле ценными бумагами через глобальную сеть. Чрезвычайно разнообразны также компьютерные мошенничества: это ложные предложения товаров и услуг, услуги по организации хакерских атак, аферы с электронными платежными картами и счетами клиентов электронных платежных систем. Статистика показывает, что почти в 43% случаев жертвами компьютерных мошенников становятся участники онлайновых аукционов – когда покупатель отзывается на недобросовестное предложение приобрести какой-нибудь товар по очень низкой цене, но с предоплатой. До 10% потерпевших – это одинокие мужчины из развитых стран, которые верят в так называемых черных невест. Одно из таких преступлений было раскрыто сотрудниками МВД Российской Федерации. Группа мошенников от имени жительницы Йошкар-Олы вступила в переписку с искавшим через Интернет невесту инженером из Германии. Вместо фотографии "избранницы" ему выслали снимок известной балерины Анастасии Волочковой. Выманив под разными предлогами у будущего жениха 26 тысяч евро, "невеста" переписку прекратила. После того как инженер заявил о произошедшем в управление "К" МВД Республики Марий Эл, группа из девяти аферистов была разоблачена[3].

Растет количество фиктивных сделок через Интернет-магазины, где оплата производится с помощью системы Web Money Transfer. Появились и новые виды электронного вымогательства. Например, бывают случаи, когда в крупные авиакомпании по электронной почте приходят письма с угрозой провести теракт на их самолете, если на указанный счет не будет переведена крупная сумма.

Кроме отмеченных выше видов кибермошенничества, вполне реальна угроза так называемого кибертерроризма, под которым понимается использование Интернета в целях рекрутирования новых сторонников, размещения информации, направленной на разжигание межнациональной розни, расовой нетерпимости.

Следует отметить, что чаще всего поддержка сайтов террористической и экстремистской направленности осуществляется из-за рубежа. По статистике МВД РФ, 85% таких ресурсов находятся за пределами России. Создать сайт в Интернете на территории любого государства сегодня очень просто. На это уходит примерно 50 мин времени плюс средства, перечисляемые электронным платежом. Причем зарегистрировать сайт можно на любое имя и разместить на нем любую информацию. Например, в Интернете можно найти предложения даже об услугах киллеров, не говоря уже о способах изготовления наркотических веществ и взрывных устройств[4].

Как отмечают зарубежные криминалисты, опасность от применения вышеописанных схем

---

[1] Combating computer crime. Prevention. Detection. Investigation. Chantico publishing company, inc. 1990.

[2] *Бекбоев А.З.* Уголовно-правовые и криминологические меры противодействия преступности в сфере использования компьютерных технологий (по материалам Кыргызской Республики и отдельных стран СНГ): Автореф. дисс. … канд. юрид. наук. – Бишкек, 2007. – С. 4.

[3] По данным интервью зам. начальника Бюро специальных технических мероприятий (БСТМ) МВД РФ Константина Мачабели Gzt.ru.

[4] "ONLINE INVESTMENT FRAUD: NEW MEDIUM, SAME OLD SCAM" www.sec.gov.

мошенничества может резко возрастать при использовании в преступных целях компаний, учрежденных за границами государства, как правило, в оффшорных зонах, поскольку правоохранительные органы испытывают серьезные трудности при отслеживании и преследовании иностранных мошенников.

Рассмотрев типичные способы мошенничества с использованием сети Интернет в России и других постсоветских странах, необходимо отметить, что и Кыргызстан вынужден следовать общим тенденциям, происходящим в указанных соседних странах. Это означает, что при бурном росте Интернет-технологий в Кыргызстане ожидается появление и уже появляются идентичные способы мошенничества.

Однако, по нашему мнению, кыргызское общество остается незащищенным от подобного рода преступных посягательств. Среди обстоятельств, на которых мы основываем свое утверждение, могут быть названы: несовершенство кыргызского законодательства; отсутствие у кыргызских правоохранительных органов опыта и методик борьбы с подобного рода преступлениями; отсутствие системы взаимодействия в борьбе с компьютерной преступностью между различными государственными органами; отсутствие системы информирования общественности о совершенных преступлениях.

Вместе с тем компьютерное мошенничество, и вообще киберпреступность в целом, может представлять существенную опасность для информационной и финансовой безопасности Кыргызской Республики.

В целях борьбы с подобной преступной деятельностью в Кыргызстане должны быть предприняты определенные меры, которые, на наш взгляд, могут быть заимствованы из зарубежного, в частности американского, опыта. Среди них могут быть названы: создание системы взаимодействия различных правоохранительных органов для борьбы с компьютерным мошенничеством; создание системы информирования инвесторов о совершенных и раскрытых преступлениях, в частности через Интернет, а также разработка криминалистических методик расследования подобных преступлений.