

ТЕНДЕНЦИИ ПРОЯВЛЕНИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Д.В. Чернорук, 3 курс

Научный руководитель – Л.П. Володько, к.м.н., доцент

Полесский государственный университет

Стремительное внедрение цифровых технологий во все сферы жизни в начале XXI в. предопределило возникновение новых общественных отношений. Наибольшую значимость и распространенность имеет технология Интернет, которая дала человеку безграничные возможности в области передачи, распространения и рассылки информации, позволила выполнять финансово-банковские операции, несмотря на расстояния и границы. Вместе с тем, кроме положительного эффекта Интернет содержит ряд отрицательных моментов и негативных последствий. С одной стороны, Интернет позволил более эффективно и безнаказанно совершать ранее существовавшие традиционные преступления, с другой – породил новые, неизвестные еще совсем недавно виды общественно опасных посягательств, совокупность и система которых выражается в таком негативном социальном явлении как Интернет-преступность.

О том, что Интернет активно используется преступными элементами, свидетельствует широкое распространение в сети сайтов экстремистской направленности и других преступно ориентированных ресурсов. Много компьютерных преступлений совершается в России и Белоруссии с использованием возможностей, которые предоставляет своим пользователям сен Интернет.

По свидетельству экспертов самым привлекательным сектором белорусской экономики для преступников является кредитно-финансовая система. Динамика киберпреступности позволяет утверждать, что в Республике Беларусь, как и во всем мире, продолжается период ее роста: в 2005 году зарегистрировано 178 преступлений против информационной безопасности, в 2006 году – 334, в 2007 году – 996. Из них зарегистрировано особо тяжких и тяжких преступлений – 39 (2006 г. – 16), менее тяжких – 915 (277), не представляющих большой общественной опасности – 42 (41). При этом в структуре компьютерной преступности наблюдается значительное увеличение числа таких преступлений, как хищение путем использования компьютерной техники (897–239; +275,3%).

Наиболее распространенными являются компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей. В 2007г. белорусскими правоохранительными органами были выявлены 15 подобных преступлений, в ходе расследования которых установлены факты незаконного перевода 6,3 млрд рублей. В 2008 году в Беларуси более 500 человек были привлечены к уголовной ответственности за действия, направленные против информационной безопасности. Как свидетельствует официальная пресса, до 80% преступлений в сфере информационной безопасности компаний и банков происходит по вине или при непосредственном участии персонала данных фирм.

В Республике Беларусь активно работает подразделение по борьбе с компьютерными преступлениями министерства внутренних дел Беларуси, в прессе имеется информация, свидетельствующая об учащении случаев вымогательства денег через интернет. Подавляющее число преступлений против информационной безопасности совершаются не подростками, а взрослыми людьми. Компьютерные преступления имеют высокую латентность. Многие крупные компании, фирмы, банки не сообщают о преступлениях, совершенных хакерами в отношении них. Они не хотят признаваться, что в их информационной безопасности есть брешь.

За последнее время не отмечено ни одно компьютерное преступление, которое было совершено одним человеком. Более того, известны случаи, когда преступными группировками нанимались бригады из десятков хакеров, которым предоставлялось отдельное охраняемое помещение, оборудованное по последнему слову техники, для того чтобы они осуществляли хищение крупных денежных средств путем нелегального проникновения в компьютерные сети крупных коммерческих банков.

Органы внутренних дел стали фиксировать случаи вымогательства денежных средств через интернет. Злоумышленники совершают так называемое электронное нападение на компьютер, в результате чего блокируются программы. Потом пользователю приходят письма с предложениями разблокировать эти программы за определенное денежное вознаграждение. К сожалению, часто злоумышленники рассылают электронные письма, которые рассылают тысячи вирусов, блокирующих программы.

В России аналогичный вид компьютерных преступлений носит название «Синдром Робина Гуда». Удивительно, но для общественного мнения в России характерен данный синдром — преступники-хакеры представляются некими благородными борцами против толстосумов. Хакерство в России, по-видимому, просто обречено на дальнейшее развитие.

В условиях мирового финансового кризиса необходимо системное и последовательное исследование Интернет- преступности как в целом, так и отдельных наиболее распространенных ее видов, разработка эффективных мер борьбы и предупреждения преступлений в Глобальной сети. Однако ее высокая латентность и отсутствие официальной статистики, приводят к неэффективности мер предупреждения, которые к тому же нередко носят фрагментарный и характер, предопределяя трудности в противодействии и борьбе с данным видом общественно опасных деяний. Проведенный анализ Интернет – преступности позволил сделать следующие выводы:

1. С момента возникновения Интернет- преступности в ходе ее эволюции можно выделить 5 последовательных этапов развития. Эти этапы Интернет-преступность проходит в любой стране мира, меняется лишь скорость прохождения того или иного этапа, но порядок остается тем же. Этап быстрого количественного роста совершаемых Интернет-преступлений совпал с ростом популярности субкультуры хакеров.

2. Интернет-преступность является частью компьютерной преступности и соотносится с такими ее видами, как преступность в сфере компьютерной информации. Интернет-преступность отличается от других видов особыми свойствами: глобальностью, широкой распространенностью, крайне высокой латентностью и др., определяющими ее бурный рост и общественную опасность.

3. Общество негативно относится к отсутствию контроля над деятельностью и распространением информации в Интернет социально-опасного характера. В то же время некоторая часть населения склонна идеализировать образ Интернет-преступника и часто воспринимает его как «борца за свободу».

4. Сама природа сети Интернет, зачастую, является благоприятной для совершения преступлений, так как такие ее свойства, как глобальность, анонимность пользователей, охват широкой аудитории и их взаимозаменяемость создают преступникам, использующим Интернет, преимущества на всех этапах совершения преступления, а также позволяет эффективно скрываться от правоохранительных органов. Определяющими факторами, является специфическая криминальная субкультура.

Компьютерные преступления становятся общественно опасными, поэтому проблемы выработки защитных мер против всевозможных злоупотреблений в данной сфере дают импульс к разработке и введению в действие соответствующих норм уголовного законодательства.

Список использованных источников

1. Катаев С.Л. Социальные аспекты компьютерной преступности // Центр иссл. пробл. комп. преступн. – Киев, 2002.
2. Крылов В.Б. Информационные компьютерные преступления. – М.: ИНФРА-М-НОРМА, 1997.
3. Анип Б. Защита компьютерной информации. – СПб.: ВНУ, 2000.